Hadtudományi Szemle
15. évfolyam (2022) 4. szám 37–49. • DOI: 10.32563/HSZ.2022.4.3

Bihaly Barbara[1]

Kibervédelem a NATO-ban és az EU-ban

Cyber Defence in NATO and in the EU

Absztrakt

Az elmúlt több mint két évtizedben a növekvő hibrid és jelentős kiberbiztonsági fenyegetettség egyaránt kihatott az Európai Unió (EU) és az Észak-atlanti Szerződés Szervezetének (NATO) tagállamaira és saját rendszereire is. Az európai kormányoknak lépéseket kellett tenniük a nemzeti szintű kiberbiztonsági politikák kidolgozására, miközben egyidejűleg egyesítették szuverenitásukat az Észak-atlanti Szerződés Szervezetén és az Európai Unión keresztül védelmük megerősítése érdekében. Gyakran felmerül a kérdés, hogy mi a különbség és mi a hasonlóság a két szervezet között, illetve szükséges-e mindkét szervezet, ha vannak átfedések? Jelen publikáció célja bemutatni, hogyan hatnak a kiberbiztonsági fenyegetések az EU és a NATO szervezeti struktúrájára és stratégiai környezetére.

Kulcsszavak: *kibervédelem, NATO, Európai Unió*

Abstract

Over the past two decades, the growing hybrid and significant cyber security threat has affected both the Member States of the European Union (EU), the North Atlantic Treaty Organization (NATO) and their own systems. European governments had to take steps to develop cyber security policies at national level, while simultaneously pooling their sovereignty through the North Atlantic Treaty Organization and the European Union to strengthen their protection. The question often arises as to what is the difference and the similarity between the two organizations, and is it necessary for both if there are overlaps? The purpose of this publication is to show how cyber

[1] Doktori hallgató, Nemzeti Közszolgálati Egyetem Katonai Műszaki Doktori Iskola, e-mail: b.bihaly@gmail.com

security threats affect the organizational structure and strategic environment of the EU and NATO.

Keywords: *cyber defence, NATO, European Union*

Bevezetés

A kiberbiztonsági fenyegetések kihívások elé állítják az egyéneket, a vállalatokat, az államokat és a kormányközi szervezeteket egyaránt. E fenyegetések megjelenése a nemzetközi biztonsági együttműködést is nehéz feladatok elé állítja. Ez a cikk azt elemzi, hogyan hatnak a kiberbiztonsági fenyegetések az Európai Unió (EU) és az Északatlanti Szerződés Szervezetének (NATO) struktúrájára és milyen stratégiai hátteret dolgoztak ki ezek kezelésére.

Habár a NATO fő erőfeszítései továbbra is a katonai védelemre összpontosulnak, felismerte a polgári hálózatok fontosságát és a velük szemben támasztott kockázatokat, különösen a hibrid fenyegetésekkel kapcsolatos munkája révén, de nem rendelkezik olyan jogi vagy szakpolitikai eszközökkel, amelyek e kérdések közül sokat közvetlenül megválaszolhatnának. Itt lép be az Európai Unió. Az EU számos területen felülírta vagy kiegészítette a tagállami politikákat, beleértve a gazdasági, igazságügyi és belügyi területeket is. Ennek megfelelően Európa jogi környezetének nagy része uniós jogszabályokból áll, vagy azon alapul. Míg a nemzeti kormányok őrzik szuverenitásukat a védelem és a külpolitika területén, az EU korlátozott jogkörrel rendelkezik ezeken a területeken. Valójában az EU jelentős szerepet játszik az európai kiberbiztonsági környezet alakításában, elsősorban a gazdasági szabályozással, az egyéni jogokkal és a belső biztonsággal kapcsolatos jogszabályokkal.

Ezek a szabályozások elsősorban a köz- és a magánszféra közötti információmegosztás gyorsaságának, rendszerességének és központosításának növelésére irányulnak. Az EU szerény kül- és védelempolitikai mandátuma ellenére jelentős szerepet kezdett játszani a külpolitika alakításában, és lassan saját katonai-védelmi struktúrája is kialakult (EUMC, EU MPCC). Ennek megfelelően a NATO és az EU kibervédelmi törekvései, stratégiái és szervezetei részben párhuzamos szerepeket töltenek be, részben kiegészítik egymást.

Stratégiai és doktrinális háttér

Annak ellenére, hogy a NATO korábban is foglalkozott már a kibertérben végrehajtott támadásokkal, az Észtországot ért 2007-es kibertámadások rávilágítottak a NATO tevékenységeinek elégtelenségére, és politikai elkötelezettségének, valamint hadműveleti képességeinek jelentős növekedését idézték elő ezen a területen. Az észt incidens segített a NATO számára élesebb perspektívába hozni a kiberfenyegetések tétjét.[2]

A kiberfenyegetések kihívások elé állították a NATO imázsát és hírnevét, a szövetség által végrehajtott katonai műveleteket támogató biztonságos kommunikáció

[2] Abrial 2011.

biztosításának képességét, a hatékony működés képességét, amikor a kibertér a katonai konfliktusok új csataterét vagy területét jelenti, valamint a NATO-tagok azon képességét, hogy hozzájáruljanak a Szövetség célkitűzéseinek teljesüléséhez és küldetéseinek végrehajtásához.

Ennek megoldására rendszerezni kellett a kibervédelemmel kapcsolatos kérdéseket és definíciókat, valamint ki kellett adni a megfelelő direktívákat, amelyek segítik összehangolni a kiberfenyegetések elleni védekezést a Szövetségen belül.

Az Allied Joint Publication-3 (AJP 3), másnéven Összhaderőnemi Műveleti Doktrína[3] alapján készült el 2020-ban a NATO műveleti architektúrájának részeként az Összhaderőnemi Kibertér Műveleti Doktrína (AJP 3.20.),[4] és előtte 2009-ben az Összhaderőnemi Információs Műveleti Doktrína (AJP 3.10.).[5]

Az előbbi, az Összhaderőnemi Kibertér Műveleti Doktrína a szövetséges közös doktrína a kibertérműveletekhez, egy NATO-doktrína, amely a szövetséges közös műveletek összefüggésében tervezi, hajtja végre és értékeli a kibertérműveleteket (*cyberspace operations,* CO).

Ehhez hasonlatosan, az Összhaderőnemi Információs Műveleti Doktrína célja annak elmagyarázása, hogy az információs műveletek (*information operations,* IO) miként támogatják a műveletek tervezését, lebonyolítását és értékelését.

A két műveleti doktrínán kívül még nagy jelentőségű dokumentum a Joint Air Competence Center (JAPCC) által kiadott *NATO Joint Air Power And Offensive Cyber Space Operations,*[6] amely a légierő kibertámadásokra való kivételes érzékenysége miatt kiadott doktrína a támadó kibertérműveletekről.

A NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), a NATO oktatási és fejlesztési feladatokat ellátó szervezete 2012-ben kiadta a *Nemzeti kiberbiztonsági keretrendszer kézikönyv*et *(Tallinn Manual)*,[7] amelynek célja, hogy mind az akadémikusok, mind a döntéshozók számára mélyreható vizsgálatot nyújtson a kiberbiztonság nemzetbiztonsági kontextusban való kezelésének lényeges tényezőiről. Az alkalmazott elméleti keretek célja, hogy segítsék a kérdés különféle aspektusainak további megértését, de nem írnak elő politikai vagy fejlődési utat. Ugyanis a nemzeti kiberbiztonság kérdése túlontúl bonyolult, így egyetlen egyéni megközelítésre sem lehet általános érvényű megoldásként tekinteni.

Az EU sem tétlenkedett az elmúlt években a jogszabályalkotás terén, hiszen már több ízben is adott ki kiberbiztonsági stratégiát, az elsőt 2013-ban,[8] a legfrissebbet pedig 2020 végén.[9]

Az EU 2013-as kiberbiztonsági stratégiájától kezdve az EU koherens és holisztikus nemzetközi kiberpolitikát dolgozott ki. Partnereivel kétoldalú, regionális és nemzetközi szinten együttműködve globális, nyitott, stabil és biztonságos kiberteret mozdított elő, amelyet az EU alapvető értékei vezérelnek, és amely a jogállamiságon alapul. Ezen túl az EU támogatta a harmadik országokat abban, hogy növeljék a kiberbűnözés

[3] *Allied Joint Publication-3. Allied Joint Doctrine for the Conduct of Operations.* 2019.
[4] *Allied Joint Publication 3.20. Allied Joint Doctrine for Cyberspace Operations.* 2020.
[5] *AJP-3.10 Allied Joint Doctrine for Information Operations.* 2009.
[6] MacKenzie 2017.
[7] Klimburg 2012.
[8] *Az Európai Unió kiberbiztonsági stratégiája: Nyílt, megbízható és biztonságos kibertér.* 2013.
[9] European Commission 2020.

elleni küzdelmet, és a 2017-es uniós kiberdiplomáciai eszköztárat arra használta, hogy továbbra is hozzájáruljon a kibertér nemzetközi biztonságához és stabilitásához.[10]

Az EU jelentős előrehaladást ért el a kibervédelmi együttműködés terén is, beleértve a kibervédelmi képességeket, nevezetesen a kibervédelmi politikai keretrendszert (CDPF), valamint az állandó strukturált együttműködést (PESCO).[11]

A kiberbiztonsági stratégiák kiterjednek az olyan alapvető szolgáltatások biztonságára, mint a kórházak, az energiahálózatok és a vasút, valamint az otthonunkban, irodáinkban és gyárainkban folyamatosan növekvő számú összekapcsolt objektum, a nagyobb kibertámadásokra adott válaszok kollektív képességeinek kiépítése és a világ minden részén működő partnerekkel való együttműködés.

Mindezek mellett, a 2020-as Stratégia leírja, hogy az EU hogyan tudja kihasználni és megerősíteni eszközeit és erőforrásait annak érdekében, hogy technológiailag szuverén legyen. Azt is leszögezi, hogy az EU hogyan erősítheti meg együttműködését azokkal a partnereivel a globális szintéren, akik osztják a demokrácia, a jogállamiság és az emberi jogok értékeit.

A Stratégia értelmében az EU technológiai szuverenitásának az összes kapcsolódó szolgáltatás és termék rugalmasságán kell alapulnia. Mind a négy „kiberközösségnek" – a belső piaccal, a bűnüldözéssel, a diplomáciával és a védelemmel foglalkozóknak – szorosabban kell együttműködnie a fenyegetések közös tudatosítása érdekében, továbbá készen kell állniuk arra, hogy kollektíven reagáljanak, ha egy támadás megvalósul.

Másrészről, a Stratégia célja kollektív képességek kiépítése a nagyobb kibertámadásokra való reagáláshoz.[12] Azt is felvázolja, hogy a nemzetközi együttműködés szükséges és elengedhetetlen a nemzetközi biztonság és stabilitás megteremtéséhez a kibertérben. Ezen túlmenően felvázolja, hogy a Joint Cyber Unit hogyan tudja a leghatékonyabb választ adni a kiberfenyegetésekre a tagállamok és az EU rendelkezésére álló kollektív erőforrások és szakértelem felhasználásával.

Az EU digitális évtizedre vonatkozó új kiberbiztonsági stratégiája kulcsfontosságú eleme az Európa digitális jövőjének alakításáról kiadott dokumentumának,[13] a Bizottság európai fellendülési tervének[14] és a Biztonsági Unió 2020–2025-ös stratégiájának.[15]

Mivel a kiberbiztonsági fenyegetések szinte mindig határokon átnyúlók, és az egyik ország kritikus létesítményeit érintő kibertámadás kihatással lehet az EU egészére, az EU-tagállamoknak erős kormányzati szervekkel kell rendelkezniük, amelyek felügyelik az országukban a kiberbiztonságot, különösen a társadalmunk szempontjából kritikus ágazatokban. Ezeknek az intézményeknek folyamatos információcsere révén együtt kell működniük a más tagállamokban működő társintézményekkel. Ennek szabályozására jött létre a NIS-direktíva 2016-ban,[16] majd 2020-ban a felülvizsgálati eljárás eredményeként a Bizottság előterjesztette az Unió egész területén magas

[10] European Commission 2020.
[11] *Towards a More Secure, Global and Open Cyberspace: The EU Presents Its New Cybersecurity Strategy*. 2020.
[12] European Commission 2020.
[13] *Shaping Europe's Digital Future.* 2019.
[14] *Recovery Plan for Europe.* 2021.
[15] *European Security Union.* 2020.
[16] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016.

szintű kiberbiztonságot célzó intézkedésekre vonatkozó irányelvre irányuló javaslatot (NIS2-irányelv).[17]

A hálózat- és információbiztonságról szóló (NIS-) irányelv az első uniós szintű kiberbiztonsági jogszabály, amely 2016-ban jelent meg, konkrét célja a kiberbiztonság magas szintű, közös elérése volt a tagállamokban. Miközben növelte a tagállamok kiberbiztonsági képességeit, végrehajtása nehéznek bizonyult, ami a belső piac különböző szinteken való széttagoltságát eredményezte. A digitalizáció jelentette növekvő fenyegetésekre és a kibertámadások számának növekedésére való reagálás érdekében a Bizottság javaslatot nyújtott be a NIS-irányelv felváltására és ezáltal a biztonsági követelmények megerősítésére, az ellátási láncok biztonságának kezelésére, a jelentési kötelezettségek egyszerűsítésére és szigorúbb szabályok bevezetésére. A NIS2 hatályának javasolt kibővítése – több szervezet és ágazat intézkedésre való tényleges kötelezése révén – hosszú távon hozzájárulna a kiberbiztonság szintjének növeléséhez Európában.

Európa digitális jövőjének alakításához szorosan hozzáfűződik a Cyber Security Act,[18] az EU kiberbiztonsági törvénye, amely megújítja és megerősíti az EU kiberbiztonsági ügynökségét (ENISA), és létrehozza a digitális termékek, szolgáltatások és folyamatok uniós szintű kiberbiztonsági tanúsítási keretrendszerét.

Intézmények

A következőkben bemutatom a főbb kibertéri ráhatással rendelkező NATO felsőszintű bizottságokat, valamint azon szervezeteket, amelyek szakterületi munkájuk során közvetlen vagy közvetett hatást gyakorol(hat)nak a kibertérre és a kapcsolódó területekre.

Politikai szinten az NAC (North Atlantic Council, Észak-atlanti Tanács) és természetesen a védelmi tervező és erőforrás-elosztással foglalkozó bizottságok foglalkoznak a kibervédelem kérdésével.

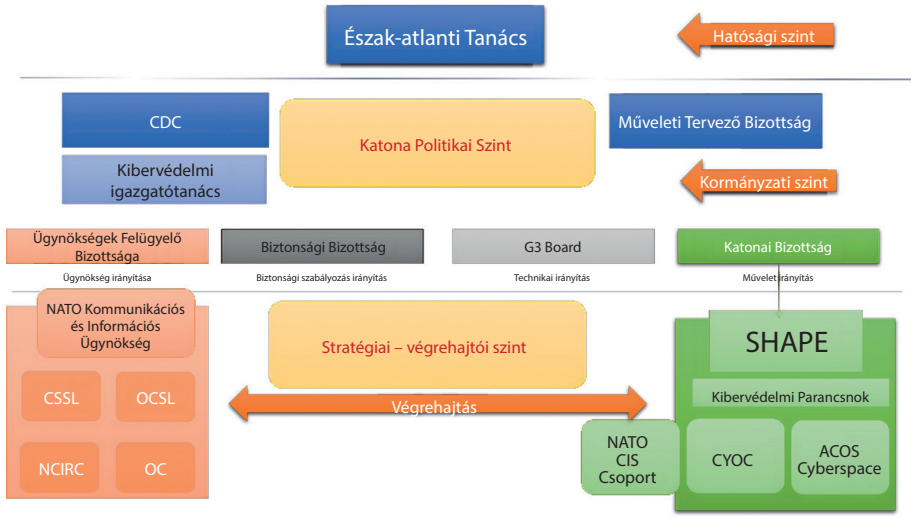
Az NAC alá tartozó szervezeti elemek horizontálisan katonai, civil és ügynökség kategóriákra bonthatók, vertikálisan pedig stratégiai, taktikai és műveleti szintre.

Katonai-stratégiai szinten a legfontosabb elemek a Military Committee (MC) és az alá tartozó MC Policy Working Group (katonapolitikai, stratégiai-hadműveleti szintű kérdések, érintőlegesen kibertéri feladatokkal foglalkozik) és az MC CIS (híradó informatikai kérdések, érintőlegesen foglalkozik kibertéri feladatokkal).

Viszont funkcionális szakterületi (főbizottság) szinten a Cyber Defence Committee (CDC) és a Cyber Defence Management Board (CDMB) – amely mivel Management és nem Policy Board, a CDMB szintje alatta kell(ene) hogy legyen – támogatják a politikai döntéshozatalt a kibervédelem területén.

Az NAC-nak alárendelt CDC a politikai kormányzás és általában a kibervédelmi politika vezető bizottsága. Munkacsoporti szinten a CDMB felelős a kibervédelem koordinálásáért a NATO polgári és katonai testületei között. A CDMB a NATO politikai, katonai, műveleti és műszaki testületeinek vezetőiből áll, akik felelősek a kibervédelemért.

[17] European Parliament 2022.
[18] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019.



1. ábra: A NATO kiberhez kapcsolódó szervezetei

Forrás: a szerző szerkesztése

Kiberhez szakterületileg csatlakozó testületek továbbá a C3B (Consultation, Command & Control Board), amely politikai kérdésekben tesz javaslatokat az NAC-nak; a DPPC (Defence Policy and Planning Committee), amely védelmi kérdésekben tölt be tanácsadói szerepet; és a RPPB (Resource Policy and Planning Board), amely a NATO erőforrásainak kezeléséért felelős.

Végrehajtói szinten a NATO Konzultációs, Ellenőrzési és Vezérlési Testülete (NC3) alkotja a kibervédelem technikai és végrehajtási szempontjaival kapcsolatos konzultáció fő bizottságát. A NATO Katonai Hatóság (NMA) és a NATO Kommunikációs és Információs Ügynökség (NCIA) specifikus felelősséget viselnek a műveleti követelmények kimutatásáért, a NATO kibervédelmi képességeinek megszerzéséért, megvalósításáért és működtetéséért. A Szövetséges Transzformációs Parancsnokság (ACT) felelős az éves Cyber Coalition gyakorlat tervezéséért és lebonyolításáért.[19]

Továbbá az NCIA a belgiumi Monsban található NCIRC Műszaki Központon keresztül felelős a technikai kiberbiztonsági szolgáltatások nyújtásáért az egész NATO-ban. Az NCIRC kulcsszerepet játszik a NATO-t érintő kiberincidensek megválaszolásában. Kezeli és jelenti az incidenseket, és terjeszti az incidensekkel kapcsolatos fontos információkat a rendszerbiztonsági menedzsment és a felhasználók felé. Az NCIRC Koordinációs Központ a NATO-n belüli és a tagországokkal folytatott kibervédelmi tevékenységek koordinálásáért, valamint a CDMB személyzeti támogatásáért felelős személyzeti egység.[20]

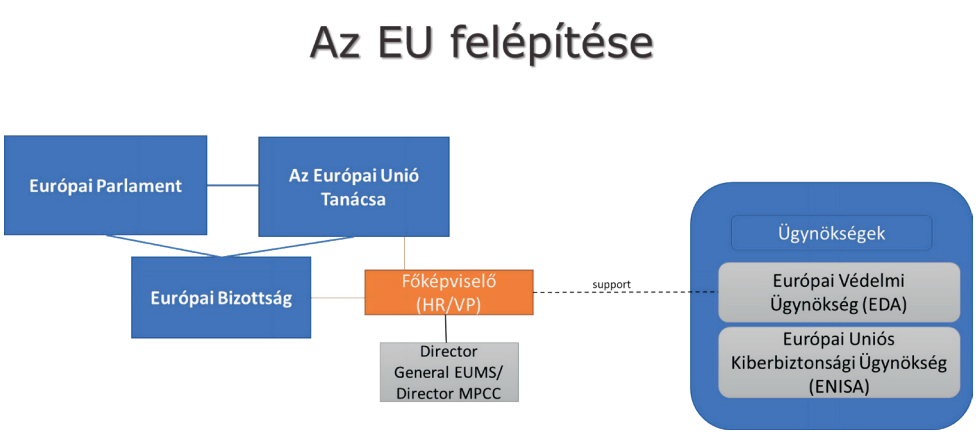
[19] NATO 2021.
[20] NATO 2021.

További nem bizottsági és nem nemzeti képviseleti szervezetek, amelyek érintik a kibervédelmet:

- NATO (HQ) ESCD (Emerging Security Challenges Division);
- NATO (HQ) Operations Division;
- A NAC és az MC munkáját segítő Nemzetközi Titkárság (IS), a Nemzetközi Katonai Törzs (IMS);
- CTAC – Cyber Threat Assessment Cell (a CDMB alatt);
- SHAPE (BE) (benne végrehajtói szinten: Cyberspace Operations Centre [CyOC]);
- ACT (US) (van egy kiberosztály szintű szerve);
- NIFC (UK) (NATO Intelligence Fusion Centre).

A NATO-n belül léteznek kutatás/fejlesztésért és kiképzésért felelős szervezetek, amelyek közül kiemelendő a tallinni székhelyű NATO Cooperative Cyber Defence Centre of Excellence (CCD COE), amelynek küldetése, hogy egyedülálló interdiszciplináris szakértelemmel támogassa a tagországokat és a NATO-t a kibervédelmi kutatások, képzések és gyakorlatok területén, amelyek a technológia, a stratégia, a hadműveletek és a jog fókuszterületeit lefedik.[21]

Az Európai Unió eredeti célja – szemben a NATO-val, amelynek célja eredetileg is, azóta is a védelmi és katonai együttműködés – a gazdasági, majd később a politikai szintű összehangolt, koherens együttműködés. Ennek a politikai együttműködésnek a biztonság- és védelempolitikai oldala lassan alakult ki, és még mindig van hova fejlődni. A fenti okokból kiindulva az Európai Unió intézményi felépítése is másként alakult.



2. ábra: Az EU releváns vezetői szerveinek felépítése és kapcsolata
Forrás: a szerző szerkesztése

Az EU közös biztonság- és védelempolitikájának központi eleme a Főképviselő (High Representative, HR), aki alakítja és irányítja az EU közös kül- és biztonságpolitikáját

[21] CCD COE. Lásd: https://ccdcoe.org/about-us/

(CSFP), beleértve a közös biztonság- és védelempolitikát (CSDP); elnököl a Külügyi Tanácsban (FAC); az Európai Védelmi Ügynökséget (European Defence Agency, EDA) vezeti; valamint az Európai Bizottság egyik alelnöke.[22]

A HR munkáját támogatja és a CSDP-t végrehajta az EDA és az ENISA (Az Európai Unió Hálózat- és Információbiztonsági Ügynöksége). Az EDA katalizátorként működik, elősegíti az együttműködéseket, új kezdeményezéseket indít és megoldásokat vezet be a védelmi képességek javítására. Ez az a szervezet, ahol a tagállamok készek együttműködési képességeket fejleszteni. Az Unió közös biztonság- és védelempolitikájának alátámasztásához szükséges képességek fejlesztésében is kulcsfontosságú előmozdító erő, többek között kiberképességek fejlesztésével is foglalkozik, ennek értelmében alájuk tartozik a PESCO is.[23]

Az ENISA az EU kiberbiztonsági ügynökségeként funkcionál, tehát támogatást nyújt a tagállamoknak, az EU intézményeinek és a vállalkozásoknak olyan kulcsfontosságú területeken, mint például a NIS-irányelv végrehajtása.[24]

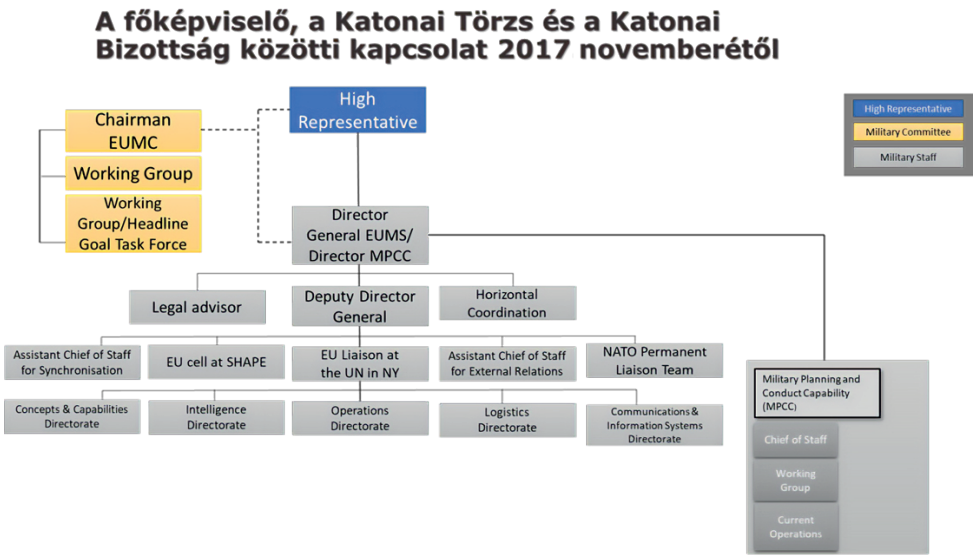
Többek között a Közös Kutatóközpont (JRC), az Európai Bizottság közös kutatóközpontja is aktívan hozzájárul az EU kiberbiztonságához. Például a JRC dolgozta ki a kiberbiztonsági taxonómiát. Ez összehangolja a kiberbiztonságban használt terminológiát, hogy tisztább áttekintést kaphassunk az EU kiberbiztonsági képességeiről.[25] Gazdasági oldalról pedig az Információmegosztó és Elemző Központok (ISACs) segíti a magán- és közszféra együttműködését a kiberbiztonság területén. Az ISAC-ek továbbfejlesztése mind uniós, mind nemzeti szinten a Bizottság prioritása. Az ENISA-val együttműködve elősegíti új ISAC-ek létrehozását azokban az ágazatokban is, ahol ilyen nincs. A Bizottság által felügyelt „Empowering EU ISACs konzorcium" jogi, technikai és szervezeti támogatást nyújt az ISAC-ek számára.[26]

Illetve, a NIS-irányelv értelmében az EU-tagállamoknak biztosítaniuk kell, hogy jól működő számítógépes biztonsági eseményekre reagáló csapataik (CSIRT-ek) legyenek, más néven számítógépes vészhelyzeti reagálási csapatok (CERT-ek). Ezek a csapatok a kiberbiztonsági eseményekkel és kockázatokkal foglalkoznak a gyakorlatban. EU-szinten együttműködnek egymással, és együttműködnek a magánszektorral is. A CERT-EU a főbb uniós intézmények informatikai biztonsági szakértőiből áll és együttműködik a tagállamok többi CERT-jével, valamint speciális IT-biztonsági cégekkel az információbiztonsági incidensekre és a kiberfenyegetésekre való reagálás érdekében.[27]

Ami a kiberbiztonság és -védelem szempontjából viszont igazán fontos, az az, ahogy már korábban említettük: az EU politikai és gazdasági szervezet, a NATO viszont katonai. Ezért több kérdés is felmerült az EU története során azzal kapcsolatban, hogy egy esetleges agresszió esetén hogyan tud fellépni – hisz nem minden EU-tagállam NATO-tagállam is –, és elégségesek-e a NATO által ajánlott biztonsági garanciák. Ennek ellenére, vagy épp ezért, a közös kül- és biztonságpolitika fejlődése,

[22] Lásd: https://eur-lex.europa.eu/summary/glossary/high_representative_cfsp.html
[23] Lásd: https://eda.europa.eu/who-we-are/Missionandfunctions
[24] Lásd: www.enisa.europa.eu/about-enisa
[25] Nai-Fovino et al. 2019.
[26] www.isacs.eu/
[27] https://cert.europa.eu/cert/plainedition/en/cert_about.html

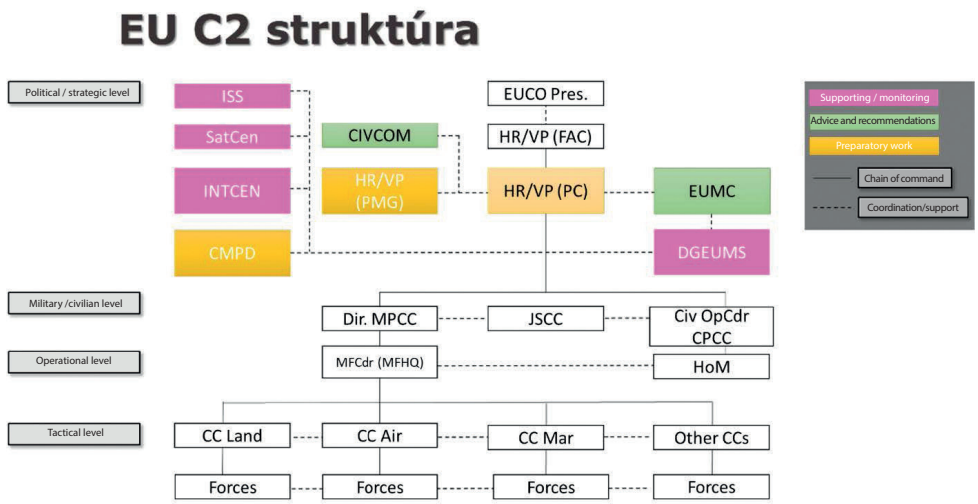
továbbá a NATO-n belül kezdeményezett Európai Biztonság és Védelmi Identitás (ESDI) megjelenése mintegy életre hívta az első katonai-védelmi irányú szervezetet, az EU Katonai Tanácsát (EUMC) 2000-ben, majd az Európai Unió Katonai Törzsét (European Union Military Staff, EUMS) 2004-ben.



3. ábra: A főképviselő, a Katonai Törzs és a Katonai Bizottság közötti kapcsolat 2017 novemberétől
Forrás: www.eeas.europa.eu/sites/default/files/impetus_24_dp_final_1.pdf

Az EUMS az Európai Külügyi Szolgálat (EKSZ) egyik főigazgatósága, amely hozzájárul a CSDP-hez, azáltal, hogy stratégiai tanácsokkal látja el a HR-t, és katonai szolgálatán keresztül irányítja a műveleteket. Másrészről, a 2017-ben alapított Military Planning and Conduct Capability (MPCC) hadműveleti központja.[28] Az EUMS jelent az EUMC-nek, ami a HR és a Politikai és Biztonsági Bizottság alá tartozik.

[28] *The Military Planning and Conduct Capability (MPCC).* 2018.



4. ábra: EU C2-struktúra
Forrás: https://data.consilium.europa.eu/doc/document/ST-8798-2019-INIT/en/pdf

Az organigramokból látszik, hogy explicit nincs még beillesztve a kiberkomponens (se hibrid komponens) az EU védelmi gyakorlatába, sem a C2-struktúrába, viszont a dinamikusan változó biztonsági környezet miatt a már meglévő politikai irányelvek és stratégiák mellé a műveleti szintű (akár támogató, akár önálló komponensként) kibererőket szükséges lesz rövidesen bevezetni, bármilyen irányba is fejlődjön tovább az EU önálló védelmi struktúrája.

Összegzés

Társadalmunk és gazdaságunk erősen függ az információs technológiától. Minél nagyobb ez a dependencia a kibertér és a modern technológia adta lehetőségekre, annál inkább figyelembe kell vennünk az új típusú biztonsági kihívásokat is, amelyek jelentősen befolyásolhatják mindennapi életünket, a kritikus infrastruktúrák működését, a különböző szolgáltatásokhoz való hozzáférést. A teljes körű, kibertérre is kiterjedő védelempolitikai gondolkodás megjelenik a NATO és az EU által kiadmányozott stratégiákban is.

Már a 2013 elején, az EU külügyi és biztonságpolitikai főképviselője és az Európai Bizottság által közösen kidolgozott új EU Kiberbiztonsági Stratégia meghatározta a kiberkorszak jövőjét az EU-ban. A stratégia nagyon világos célokat és prioritásokat határozott meg az EU kiberpolitikájára vonatkozóan, ideértve a szabadság és a nyitottság előmozdítását, a megfelelést, a kiberbiztonsági képességeket és a kibertérrel kapcsolatos nemzetközi együttműködést.

Ezzel a stratégiával és a NIS-irányelvvel az EU határozott és közös irányt szab tagállamai számára a kiberbiztonság területén. Bár a NATO-nak számos közös fellépése

van az Európai Unióval a kiberbiztonság területén, a Szövetségnek saját kiberbiztonsági politikája és stratégiája van.

De a két szervezet alapvető céljaiban való eltéréseknek megfelelően, a stratégiák és a gondolkodás köré épített intézményrendszer – bár már vannak átfedések – igen különböző. A jövőre nézve a valódi kérdés az, hogy az EU megelégszik-e ezekkel az átfedésekkel és a NATO által nyújtott biztonsági garanciákkal, vagy elindul a saját haderőfejlesztés útján a jelenlegi labilis világpolitikai helyzetben.

Az EU–NATO-együttműködés mindig is kihívást jelentett az egyes szervezetek tagságának összetételében mutatkozó különbségek miatt. Ugyanakkor a kapcsolatok folyamatosan épülnek, különösen mióta az EU és a NATO 2016 februárjában technikai megállapodást írt alá az NCIRC és a CERT-EU közötti információmegosztás fokozására. Ezen túlmenően két nem NATO-tag EU-ország tagja a CCD COE-nek, az EU-n és a NATO-n kívüli országok pedig különféle NATO-val kapcsolatos kibergyakorlatokon vesznek részt megfigyelőként.

Végső soron számos előnnyel járna a szorosabb EU–NATO-együttműködés, ahol a szövetségesek együtt dolgozhatnának a NATO-n belül a közös kibervédelmi képességek és stratégiák továbbfejlesztésén. Az EU és a NATO egyidejűleg kétoldalúan dolgozhatna közös célok elérése érdekében más kiberbiztonsági kérdésekben. A két szervezet közös politikai napirendje magában foglalhatja a kibertermékekre és -szolgáltatásokra vonatkozó uniós szövetséges biztonsági szabványok konvergenciáját, beleértve a közös beszerzéseket a kevésbé érzékeny területeken; együttműködési gyakorlatokat; strukturáltabb információmegosztást; a kiberbűnözés elleni nemzetközi rendszerek folyamatos fejlesztését; valamint következetes és gyakorlatias adatvédelmi előírásokat. Ennek elérése érdekében a szövetséges és uniós államoknak hozzá kell járulnia a NATO és az EU közös kiberműveleteihez, ami kohézióként szolgálhat e két szervezet egymáshoz való közelítésében.

Körülbelül egy évtizeddel ezelőtt kezdték el az európai döntéshozók felismerni, hogy a számítógépes támadások és a számítógépes bűnözés által okozott fenyegetés eredendően határokon átnyúló probléma, amely határokon átnyúló megoldásokat igényel. A NATO-hoz és az EU-hoz tartozó európai államok növekvő támogatásával ezek a nemzetközi entitások ki tudták építeni szervezeti és működési struktúrájukat és kapacitásaikat. Az EU és a NATO óriási előrehaladást ért el azon képességének kiépítésében, hogy tagjai között koordinálja a kiberbiztonsági és védelmi tevékenységeket. Ígéretes fejlemény, hogy a közelmúltban is tapasztalható, hogy e szervezetek egyre inkább hajlandóak egymással és a nemzetközi partnerekkel való szorosabb együttműködésre. Az összehangolt védelmi politikák közelmúltbeli sikerei csak akkor érik el teljes potenciáljukat, hogy pozitív hatást fejtsenek ki, tehát ha a NATO és az EU az ebből a területből levont tanulságokat a szélesebb kiberpolitikai kérdésekben is alkalmazza.

Összességében elmondható, hogy a kiberfenyegetéseknek való kitettség a nemzeti kormányokat és a nemzetközi szervezeteket a nagyobb transzatlanti biztonsági együttműködés felé tereli. A nemzetállami szereplők – köztük Oroszország – növekvő jelentősége az új hadszíntéren megmutatta, hogy a kinetikus műveletek a kibertérben jelentkező agresszióval párosulnak, így egyre nagyobb szükség van a biztonsági együttműködésre Európában és szerte a világon.

A NATO és az EU eddigi lépései a kiberfenyegetések kezelése érdekében ígéretesek, de végső soron csak alapvetőek. Ezeknek a szervezeteknek erre az alapra kell építeniük azáltal, hogy folyamatos az információmegosztás, a képességépítés és a védekezési stratégiák határokon átnyúló integrációja, ha a kiberteret előnyükre akarják valaha is használni az ellenérdekelt felekkel szemben.

Felhasznált irodalom

Abrial, Stéphane (2011): NATO Builds Its Cyberdefenses. *New York Times,* 2011. február 27. Online: www.nytimes.com/2011/02/28/opinion/28iht-edabrial28.html

Allied Joint Publication 3.10 Allied Joint Doctrine for Information Operations. 2009. november 23. Online: https://info.publicintelligence.net/NATO-IO.pdf

Allied Joint Publication-3. Allied Joint Doctrine for the Conduct of Operations. 2019. február 11. Online: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/797323/doctrine_nato_conduct_of_ops_ajp_3.pdf

Allied Joint Publication 3.20. Allied Joint Doctrine for Cyberspace Operations. 2020. január 29. Online: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/899678/doctrine_nato_cyberspace_operations_ajp_3_20_1_.pdf

Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. Online: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC

European Commission (2020): The EU's Cybersecurity Strategy for the Digital Decade. 2020. december 16. Online: https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0

European Parliament (2021): *The NIS2 Directive: A High Common Level of Cybersecurity in the EU.* 2022. Online: www.europarl.europa.eu/RegData/etudes/BRIE/2021/689333/EPRS_BRI(2021)689333_EN.pdf

European Security Union. 2020. Online: https://ec.europa.eu/info/strategy/priorities-2019-2024/promoting-our-european-way-life/european-security-union_en

Klimburg, Alexander (2012): *National Cyber Security Framework Manual*. Tallinn. Online: www.ccdcoe.org/uploads/2018/10/NCSFM_0.pdf

Közös közlemény az Európai Parlamentnek, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának az Európai Unió kiberbiztonsági stratégiája: Nyílt, megbízható és biztonságos kibertér. 2013. Online: https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:52013JC0001&from=HU

MacKenzie, Paul J. (2017): *NATO Joint Airpower And Offensive Cyber Space Operations.* 2017. Online: www.japcc.org/wp-content/uploads/JAPCC_OCO_screen.pdf

Nai-Fovino, I. et al. (2019): A Proposal for a European Cybersecurity Taxonomy. Luxembourg: Publications Office of the European Union. Online: https://doi.org/10.2760/106002

NATO (2021): *Cyber Defence.* 2021. július 2. Online: www.nato.int/cps/en/natohq/topics_78170.htm

Recovery Plan for Europe. 2021. Online: https://ec.europa.eu/info/strategy/recovery-plan-europe_en

Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on Information and Communications Technology Cybersecurity Certification and Repealing Regulation (EU) No 526/2013 (Cybersecurity Act). Online: https://eur-lex.europa.eu/eli/reg/2019/881/oj

Shaping Europe's Digital Future. 2019. Online: https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/shaping-europe-digital-future_en

The Military Planning and Conduct Capability (MPCC). 2018. november. Online: www.eca.europa.eu/sites/eca-audit-defence/EN/Documents/MPCC.pdf

Towards a More Secure, Global and Open Cyberspace: The EU Presents its New Cybersecurity Strategy. 2020. december 16. Online: https://eeas.europa.eu/headquarters/headquarters-homepage/90623/towards-more-secure-global-and-open-cyberspace-eu-presents-its-new-cybersecurity-strategy_en