THE BURDEN OF CYBER DEFENSE IN THE COMMON SECURITY AND DEFENCE POLICY OF THE EU

A KIBERVÉDELEM TÉRHÓDÍTÁSA AZ EU KÖZÖS BIZTONSÁG- ÉS VÉDELEMPOLITIKÁJÁBAN

KERSÁNSZKI Tamás[1]

Abstract

The European Union, which has been building its instruments for peace for almost 80 years, still plays a key role in maintaining regional and world peace. Today, this European Union faces terrorism, hybrid threats, climate change, economic crises, energy security and migration, which pose significant challenges for its member states and at the EU central level. Therefore, today Europe's policy and the basis of its collective security are determined by the action guidelines for security, defense, the fight against terrorism, cyber security, energy security, and strategic communication. The article highlights the main political decisions and declarations of the EU, which led to the creation of the Strategic Compass from transatlantic cooperation. It specifically addresses the political and strategic decisions related to cyber defense, which are becoming more and more prominent, which are gaining an increasingly important role in geopolitical security and defense decisions.

Keywords

European Union, cyber security, strategic compass, security policy

Absztrakt

Az Európai Unió mely már közel 80 éve a békére építette fel instrumentumait és mai napig kulcs szerepet játszik a régió és a világbéke fenntartásában. Ez az Európai Uniós ma a terrorizmussal, hibrid fenyegetésekkel, éghajlatváltozásokkal, gazdasági válságokkal, energiabiztonsággal és migrációval néz szembe mely jelentős kihívásokat jelent tagállamainak és uniós központi szinten is. Ezért ma Európa politikáját és a kollektív biztonságának alapját a biztonság, védelem, a terrorizmus elleni küzdelem, és a kiberbiztonság, energiabiztonság, stratégiai kommunikáció cselekvési irányvonalak határozzák meg. A cikk kiemeli az EU főbb politikai döntéseit és nyilatkozatait, ami Transzatlanti együttműködésektől a Stratégiai Iránytű megalkotáshoz vezetett. Külön kitér az egyre hangsúlyosabbá váló kibervédelemmel kapcsolatos politikai és stratégiai döntésekre, mely egyre fontosabb szerephez jut a geopolitikai biztonsági és védelemi döntésekben.

Kulcsszavak

Európai Unió, kiberbiztonság, stratégiai iránytű, biztonságpolitika

[1] kersanszki@uni-obuda.hu | ORCID: 0000-0002-4268-9892 | head, Obuda University STEM Office | PhD student, Obuda University Doctoral School for Safety and Security Sciences | vezető, Óbudai Egyetem STEM Iroda | PhD hallgató, Óbudai Egyetem Biztonságtudományi Doktori Iskola

BEVEZETÉS

Európa tagállamai közel 80 éve a békére fektetve kezdték el megalapozni az együttműködésüket. A NATO és az EU ma már kulcs szerepet játszik a régió és a világbéke fenntartásában, akkor amikor a bipoláris világrendszer felbomlott.

Európai Unió, terrorizmussal, hibrid fenyegetésekkel, éghajlatváltozásokkal, gazdasági válságokkal, energiabiztonsággal és migrációval néz szembe, mely kihívásokat jelent tagállami és uniós szinten is egyaránt. Európa kollektív biztonsága az elmúlt évtizedben terrorizmus elleni unión belüli és kívüli terrorizmus elleni küzdelem, a kiber-, energiabiztonság, közös nacionális és transznacionális fellépések köré szerveződött.

A hibrid hadviseléssel járó új megközelítést és stratégiai szemlélet a kibervédelem fontosságát újból előtérbe helyzete. Az Európai Unió ezért több területen kezdett el fejlesztéseket kiberrezisztencia biztosítása érdekében. A kiberfenyegetések sokszor több államot érintenek egyszerre, és a társadalom és gazdaság számára fontos kritikus infrastruktúrát érinthetik, ezért az azt felügyelő uniós és kormányzati szervek megerősítése, újak létrehozásra, stratégiai irányvonala meghatározásra és az ezzel kapcsolatos haderőfejlesztések fokozásra elengedhetetlenül szükség volt.

Mindez úgy valósult meg, hogy a hagyományos területvédelmet háttérbe szorította a válság- és konfliktus megelőzés tudva azt, hogy az érdekellentétek hosszú távon jelen lesznek a bel és külpolitikai szinten. A tagállamok és az uniós szervezetek és politikák részéről ez egy közös stratégiai problémamegoldást kíván, úgy, hogy közben a nemzeti szuverenitás önkéntelenül korlátozódik.

TRANSZATLANTI EGYÜTTMŰKÖDÉSEK A VÉDELEM ÉS BIZTONSÁG TERÜLETÉN

Az Európai Unió sikeres külpolitikáját és azon belül is a védelemét és biztonságát a mai napig a transzatlanti partnerség adja. A transzatlanti kapcsolatok már 1953-ben lekezdődtek, az akkor még Szén és Acél Közösséggel, melynek formalizálása 1990-ben történt a Transzatlanti nyilatkozat aláírásával. Ebben már megjelentek a biztonsággal, védelemmel kapcsolatos elköteleződések, mint a béke megőrzése és a nemzetközi biztonság előmozdítása másokkal együttműködve az agresszió és a kényszer ellen, hozzájárulva ezzel a konfliktusok békés rendezéséhez a világban. [1]

Az együttműködésnek azonban új területei váltak szükségszerűvé a globális kihívások és a gazdasági kapcsolatok erősítése miatt, mely így, a korábbi gazdasági, oktatási, tudományos és kulturális területek mellett a politika lépett be a béke, biztonság, demokrácia és a fejlődés előmozdítása érdekében. Az Új Transzatlanti Napirend (1995) aláírásával egyben elfogadták az EU-USA Közös akciótervet és rendszeres találkozókról döntöttek az USA elnöke, az Európai Bizottság, az Európai Unió Tanácsának soros elnöke, illetve az EU közös külügyi és biztonságpolitikai képviselőjének részvételével. [2]

Az Új Transzatlanti Napirend biztonságpolitikai szempontból egy hosszútávú együttműködés alapjait rakta le, mely egy új európai biztonsági architektúra felépítését tűzi ki célul, melynek központi elemeként a NATO-t jelöli meg. Fontos elemként jelent meg, hogy az új tagok csatlakozásnak az EU-hoz és a NATO-hoz nemcsak a jólétet, de egyben a biztonságot és stabilitást is szolgálniuk kell. A Partnerség a Békéért az Együttműködési

Tanács, valamint a NATO és Oroszország közötti biztonsági partnerség létrehozása, továbbá a NATO és Ukrajna közötti együttműködés az EBESZ megerősítése a régió desatbiljzációjának megelőzése érdekében szoros és hosszútávú elköteleződés alapjait fektette le az államok között.

Az EU jövőképét a gazdasági válságból való kilábalás után erősebb Európában és globális stratégiában látta, ahogy ezt a 2017-ben megjelentetett Közös jövőkép, közös fellépés: erősebb Európa című stratégiai dokumentum és ennek gyakorlati értékelését tartalmazó Az EU kül- és biztonságpolitikára vonatkozó globális stratégiája a gyakorlatban megfogalmazta. [3]

A dokumentum középpontjában továbbra is a katonai képességek és a terrorizmus elleni küzdelem áll, de emellett megjelenik a foglalkoztatás kérdésköre, az inkluzív társadalmak és az emberi jogok. Kiemeli, hogy továbbra is a békeépítés a legfontosabb szempont mindezt a "puha erő" alkalmazásával. A globális szó túllép a földrajzi értelmezésen és már szakpolitikák széles skáláját tartalmazza államokon átívelően.

Az uniós biztonsági és védelmi politikának már rugalmasnak és összefogónak kell lennie, a Lisszaboni Szerződésben lefektetett elvek mentén kell megvalósulnia, miszerint el kell mélyíteni a tagállamok közötti együttműködést és a külső szakpolitikákban határozottabb összefogásra van szükség a tagállamok, az uniós intézmények között. A dokumentum külön kitér a fenntarthatóság célok mellet a terrorizmus elleni közdelem, migráció, biztonság, mint kiemelt területekre az együttműködés területén. [4] [5]

Az EU-nak legfőbb stratégiai partnere ezen a téren az USA, melyet Joe Biden beiktatása után az Európa Tanács megerősített azzal, hogy az éghajlatváltozás elleni küzdelem, klímasemlegesség, a COVID-19 által érintett gazdaság helyreállítása és a globális nonproliferációs leszerelési és fegyverzetellenőrzési rendszer megerősítése mellett való közös kiállással a terrorizmus elleni küzdelem, nemzetközi bűnözés, migráció, energiaügyek területén szorosabb együttműködést tervez. [6]

Mindenhez az EU-nak egy asszertívabb, erősebb és egységesebb külföldi és belpolitikára van szüksége, melyben válaszokat kell adni Kína egyre erősödő jelenlétére, a gazdaság, kiberbiztonság területén. ennek tudatában az EU-nak újra kellett gondolni a transzatlanti kereskedelmi kapcsolatokat, a NATO és WTO-ben rejlő előnyök kihasználását, a hybrid fenyegetésekre való határozottabb fellépéseket és a globális környezetvédelmi (EU–USA éghajlat-politikai munkacsoport létrehozása), gazdasági és egészségügyi problémák hatékonyabb kezelését, mint például a WHO reformját. Ennek érdekében a már meglévő kapcsolatok és párbeszédek "sűrítését" irányozta elő az agytrösztök és a civil társdallamom felé történő aktívabb kommunikáció kialakítását, melyek kiegészültek például speciálisan Kínával foglalkozó szervekkel. [7]

A védelmi és biztonsági területen ezen cselekvések feltételeznek, egyfajta közös stratégiai ambíciót, autonómiát és kultúrát a tagállamok részéről, mely feltételezi, hogy fejlesztik védelmi képességeiket, ami a NATO tagok esetében a felelősségvállalásaik betartását jelenti, ezzel válthatnak az USA egyenrangúbb partnerévé. [8]

Az új partnerséggel járó kihívások

Az amerikai előválasztások körüli politikai megszólalások újra ráirányítják a figyelmünket a Joe Biden és Ursula Von der Leyen elnök új "A globális változásra irányuló új EU–USA program" -ra mely a globális változásokra való egységes fellépésre szólít fel azon

két ország tekintetében, melyek a világ GDP-jének és kereskedelmének közel egyharmadát és a közvetlen külföldi befektetések 60%-át adják. [8] Az új elnökség szakít a Donald Trump status quo ante megközelítésével és egy új partnerség megközelítését helyezi előtérbe. A két hatalomnak olyan szilárd együttműködést kell kialakítani az egészségügy, a biztonság, az éghajlatváltozás, a kereskedelem, a technológiáról, és a szabályokon alapuló multilaterális rendszerek tekintetében, mely ellenállnak az önkényuralmi hatalmak destabilizációs törekvéseinek, melyek az elmúlt időszak geopolitikai hatalmi átrendeződései, az országok közötti kétoldalú feszültségek és az egyoldalú politikákhoz való visszatérés is erősített.

Az ezen kihívásokra és elköteleződésre létrejött új transzatlanti program alapelve, hogy a a transzatlanti partnerségnek és a multilaterális rendszerek kölcsönösen erősítik, nem pedig kölcsönösen kizárják egymást. [10]

A transzatlanti partnerség alapelvei, hogy az államoknak a globális közjavak előmozdításán kell munkálkodniuk, úgy, hogy erősebb többoldalú fellépés vár el az intézmények részéről. Az EU és az USA közös érdekeire alapozva határozottan kell kiállni közös stratégiai prioritásaink tekintetében, azzal együtt, hogy tiszteletben tartják közös értékeket, mint a méltányosságot, a nyitottságot és a versenyt, akkor is, ha kétoldalú különbségek állnak fenn.

Az Együttműködés egy biztonságosabb, virágzóbb és demokratikusabb világért alfejezet fő gondolata a nemzetközi biztonság iránti közös elköteleződés, különösen annak a fényében, hogy Kína és Oroszország eltérő stratégiai és gazdasági érdekek mentén politizál, melynek kapcsán 2022 elején Oroszország látványos lépést tett az ukrajnai háború megindításával kapcsolatosan.

Az EU határozott lépeseket tett a védelmi szerepének megszilárdítását többek között a képességfejlesztési beruházások támogatása révén, mely előnnyel jár a NATO és a transzatlanti együttműködés számára. Kitér arra is, hogy az EU-nak és az USA-nak együtt kell működnie egy határozottabb nemzetközi fegyverzet-ellenőrzési és leszerelési menetrend előmozdítása érdekében. Az utóbbi az ukrán háború miatt felülvizsgálatra szorul a felek részéről. [8]

A szorosabb biztonsági és védelmi partnerségi megállapodás újabb fejezete a 2021. Brüsszelben megrendezett EU-USA csúcstalálkozó nyilatkozat a Towards a Renewed Transatlantic Partnership volt, melyben a Párizsi Megállapodásban lefektetett célok végrehajtásáról, a transzatlanti kereskedelmi és gazdasági kapcsolatok elmélyítését (Pittsburgh Statement), a meglévő kereskedelmi rendszer reformjáról (Kereskedelmi és Technológiai Tanács felállítása) és biztonsági, védelmi kérdésekről döntöttek. Ennek geopolitikai szempontból legfontosabb felajánlása az EU részéről történt, melyben felajánlotta az USA csatlakozását a PESCO-hoz (Permanent Structured Cooperation) [10] [11]

STRATÉGIAI IRÁNYTŰ ÉS A KIBERVÉDELEM EU STRATÉGIÁJA

Az Unió védelemmel kapcsolatos stratégiájának koncepcióját az Európai Bizottság 2016-os „Út egy hatékony és valódi biztonsági unió felé vezető út előkészítése” című közleményében jelentette meg, mely a 2015-ös európai biztonsági menetrendet vette alapul. A javaslat az Európai Unió és az uniós országok közötti megosztott felelősségen alapul az európai polgárok biztonsága érdekében. Azt ezt követő stratégia a 2020 és 2025 közötti

időszakon belül azokra a kiemelt területekre összpontosít, ahol az EU segítheti a tagállamokat az Európában élők biztonságának előmozdításában, miközben tiszteletben tartja európai értékeinket és elveinket.

A Tanács 2022 március 24-25. ülésén hivatalosan jóváhagyta az EU első biztonsági és védelmi fehér könyvét, a Stratégiai Iránytűt, amely olyan nagyívű cselekvési tervet jelent, megalapozza az elkövetkezendő tíz évben Európai Unió biztonság- és védelempolitikáját. [12]

A stratégiai iránytű az EU meglévő biztonsági és védelemi elemzi és a bizonytalan globális helyzet miatt fennálló fenyegetésekre ad iránymutatást közös értékelését. A stratégiai dokumentum négy alappillére, a lépjünk partnerségre, cselekedjünk, ruházzunk be és védjük meg magunkat olyan javaslatokat és ütemtervet tartalmaz, hogy az uniós és társult tagországok közösen fel tudjanak lépni a válság, háború idején megvédve ezzel az polgáraikat. Ilyen például egy uniós gyorstelepítésű kapacitást, mely válságok esetén 5000 katona bevetését teszi lehetővé, vagy a közös biztonság- és védelempolitika keretébe tartozó polgári missziós kétszáz fős szakértői csapat, mely a hybrid hibrid fenyegetéseket kivédésben és kezelésében nyújt segítséget erősítve ezzel is az uniós kibervédelmi politikát.

1. ábra: Az Európai Unió Biztonsági Uniós stratégiája
Forrás: https://ec.europa.eu/info/sites/default/files/chart_honeycomb_contrast_resized_0.png

A kibervédelmi politikai keret 2018-ben történő felülvizsgálatának megállapításai bekerültek a Stratégiai iránytű értékelésbe, miszerint az EU kibervédelmi politikájának

hozzá kell járulnia ahhoz, hogy az EU képes legyen megvédeni, észlelni és elrettenteni a kibertámadásokat. Ennek hatására már megfogalmazásra kerültek azok az irányelvek, hogy fokozni kell a kibervédelmi képességek fejlesztését, amit az EU ipari bázisának támogatásával, valamint az oktatás, a képzés és a szakmai gyakorlatok további ösztönzésével lehet elérni. További célként jelöltek meg a polgári-katonai szinergiák fokozását és a kibervédelem szerves integrálását az EU biztonság- és védelempolitikájának szélesebb területeibe, az uniós intézmények és a tagállamok közötti fokozott együttműködés és koordináció révén.

A kibertér mára már geopolitikai verseny színterévé vált, ezért határozott és gyors válaszokkal kell reagálnia a rosszindulatú kibertevékenységekre. Az EU-nak ezért nagy hangsúlyt kell helyeznie a megelőzésre, védelemre, korai észlelésre és elhárításra mind katonai, polgári és politikai szinten.

2022. májusában az Európa Tanács elfogadta a Kibervédelmi berendezkedés tervét. A Kibervédelmi berendezkedés célja, hogy demonstrálja az EU határozottságát abban, hogy mind azonnali és hosszú távon is válaszokat tudjon adni a fenyegetés különböző szereplőinek, akik meg akarják fosztani az EU-tól a biztonságos és nyílt hozzáférést a kibertérhez, és korlátozzák stratégiai érdekeit vagy partnerei biztonságát. [13]

A Kibervédelmi berendezkedés a közös uniós diplomáciai válasz mellyel az EU kiberdiplomáciával kapcsolatos megközelítését definiálta. A célja az tagállamok közötti együttműködés ösztönzése, az azonnali és hosszú távú veszélyek mérséklésének elősegítése, valamint a potenciális agresszorok viselkedésének hosszú távú befolyásolása. Az EU rosszindulatú kibertevékenységekre adott diplomáciai válaszai teljes mértékben támogatják a közös kül- és biztonságpolitikán belüli intézkedéseket (politikai nyilatkozatok, diplomáciai lépések és párbeszéd), beleértve a szükséges szankciókat is. [14]

AZ EU KÜLSŐ TEVÉKENYSÉGEI A KIBERBIZTONSÁG TERÜLETÉN

A Stratégiai Iránytű megfogalmaz olyan útmutatásokat, melyek segítségével az EU megerősítheti azon képességeit, hogy megelőzze, elrettentse és reagáljon a kibertámadásokra. Az EU határozott terve egy globális, nyitott, stabil és biztonságos kibertér kialakítása és védelme mellett, mely hozzájárul ahhoz, hogy az EU állampolgárai biztonságos digitális életet élhessen. A kiberbiztonsággal kapcsolatos politikák és fejlesztések közvetve is hozzájárulnak ahhoz, hogy az EU ellenálló, zöld és digitális Unióvá váljon.

Az EU kiberbiztonsági stratégiája jelentős szerepet tölt be ellenálló képesség megteremtésében és fenntartásában, ezzel a megőrzi a technológiai szuverenitást, ami megerősíti az EU vezető szerepét a működőképes felépítés, a rosszindulatú kibertevékenységek elleni küzdelem területén; valamint az együttműködés előmozdítását a globális és nyitott kibertér érdekében.

A 2021 novemberében megjelent Stratégiai iránytű -közvetlenül hozzájárul a versailles-i menetrend végrehajtásához- első változatát, 27 uniós tagállam hírszerzési szolgálatai és az uniós intézmények szakértői részvételével alkották meg. 2022 februárjában és márciusában újabb kiegészítések készültek hozzá, amelyek már tartalmazta a tagállamok közötti egyeztetések eredményeit, melyet a Bizottság beépítette a 2022. február 15-én közzétett védelem- és űrpolitikai csomagjába, valamint figyelembe vették az aktuális külpolitikai fejleményeket, köztük különösen az Ukrajna elleni orosz katonai agressziót.

EU KIBERBIZTONSÁGI POLITIKÁJA

A növekvő kiberfenyegetésekkel és incidensekkel szemben Európai Bizottság prioritásként kezeli, hogy minden európai polgár és vállalkozás megfelelő online és offline védelemben részesüljön.

A Cybersecurity Ventures információbiztonsági kutató és elemző cég "Kiberbiztonság – a digitális világunk alapja, európai perspektíva" 2020-as felmérése alapján globális szinten minden 11. másodpercben zsarolóvírus támadás ér egy szerveztet. A kiberbűnözéssel kapcsolatos kár 2021-ben elérte 5.5 milliárd eurót. [15] A sikeres támadások leggyakoribb célpontjai a digitális termékek, melyek közül csupán egyetlen terméket érő kiberbiztonsági támadások is kihathatnak a teljes ellátási láncra, ami gazdasági és társadalmi tevékenységek zavarához vezethet, vagy akár a biztonságot, életeket is veszélyeztethet.

2. ábra: Fontosabb kiberfenyegetések
Forrás: https://www.eeas.europa.eu/eeas/cybersecurity-eu-external-action_en

2020 decemberében a Bizottság és az Unió külügyi és biztonságpolitikai képviselője elfogadta az EU kiberbiztonsági stratégiáját, amely már holisztikus megközelítést alkalmaz a kiberbiztonsági szempontokra vonatkozóan, és ennek tükrében javasolta a hálózati és információs rendszerek biztonságáról szóló irányelv (NIS) lefektetett jelenlegi szabályok felülvizsgálatát. [16] Az új NIS2-irányelv, mely 2022 májusában az Európai Parlament és az EU-tagállamok között létrejött politikai megállapodást, mely már az Unión belüli magas szintű kiberbiztonságot szolgáló intézkedésekről szól, ami alapját a digitalizáció rapid elterjedése és a különböző állami és magán szektorok érő kiberfenyegetettség fokozódása miatt vált szükségessé. A NIS 2 irányelv minimumszabályokat állapít meg a szabályozásokkal kapcsolatosan és jogorvoslatokról és szankciókról is rendelkezik egyben. Az első 2016-ban elfogadott NIS irányelv leginkább a digitális szektorokban működő vállalkozások és szervezetek tekintetében írt elő jogszabályi kötelezettségeket, addig a NIS 2 irányelv esetében a korábbi kritikus szektorokba (energia, pénzügy, egészségügy, közlekedés stb.) bevonta az élelmiszeripari, gyógyászati cégek gépgyártói és hulladékkezelő cégek is. Az említett cégeknek szervezeti és technológiai változtatások mellet kötelező kiberbiztonsági auditot is elő kell írnak a nemzeti szabályozásoknak. A NIS 2 irányelv a központi kormányzatok közigazgatási szerveire és a regionális szintű közigazgatási szervekre is kötelezően kell alkalmazni. [17]

Az EU kiberbiztonsági stratégiája geopolitikai szempontból is erősíti az Unió azon pozícióját, mely a nemzetközi normák és szabványok terén a kibertérben, és hozzájárul a világon a globális, nyitott, stabil és biztonságos kibertér megteremtése érdekében. Mindez hozzájárul a jogállamiság, az emberi és az alapvető szabadságjogok és demokratikus értékek megőrzéséhez.

Az új stratégia, a korábbi stratégiák eredményeket követően a három eszköz alkalmazását javasolja. Szabályozási, ahol a rugalmasság, technológiai szuverenitás és vezető szerep; a beruházási, ahol a működési kapacitás a megelőzésre, elrettentésre és reagálásra; és a politikai együttműködés a globális és nyitott kibertér előmozdítása érdekében.

Az új kiberbiztonsági stratégia kulcsfontosságú eleme az Európa digitális jövőjének alakítása, a Bizottság Európai Fellendülési Tervének és a 2020–2025 közötti időszakra szóló Unió Biztonsági Stratégiának.

A Bizottság legutóbb, 2022 szeptemberében javaslatot terjesztett elő egy a kiberrezilienciáról szóló jogszabályra, amely megerősíti az EU kiberbiztonsági törvényében körvonalazott kiberbiztonsági tanúsítási keretrendszert.

A javaslat kötelező kiberbiztonsági követelményeket vezet be azon termékekre vonatkozóan, melyek digitális elemeket tartalmaznak és ezen követelményeket a teljes életciklusuk alatt teljesíteniük kell. Az új jogszabálytervezet nagyon felelőséget ró a gyártókra, és egyben előny a digitális termékeket használók számára, hogy átláthatóbbak lesznek a digitális elemeket tartalmazó termékek biztonsági jellemzői, így nagyobb védelmet biztosítva a magánélet és személyes adat védelmének. [18]

Kiberbiztonság és készségfejlesztés

A biztonságos kibertér biztosításhoz elengedhetetlenek a megfelelő képzések és készségekkel rendelkező szakemberek. Az EU Kiberbiztonsági Ügynöksége (ENISA) kidolgozta a kiberbiztonsági készségek keretrendszerét, mely meghatározta azokat a releváns szerepeket és kompetenciákat, melyek szükségesek a kibervédelmi munkakörök betöltéséhez. A keretrendszer kialakításánál cél volt a területhez köthető releváns szerepek, kompetenciák, készségek és ismeretek definiálása. Ezek segítenek abban, hogy a kiberbiztonság mint önálló terület elkülönüljön a ICT-ben elvárt általános készségektől, és egyben segítséget adjon az intézményi és rövid ciklusú képzésekés tervezésénél. A keretrendszerben 12 kiberbiztonsággal kapcsolatos szerepkör került azonosításra. Az egyes szerepkörök esetében részletesen leírja az adott személy felelősségét, elvárt készségeit és a szinergiákat. Például egy Kiber incidensekért felelős tisztviselő feladata: figyelni és értékelni a rábízott rendszerek kiberbiztonsági állapotát. Elemzni, értékelni és mérsékelni a kiberbiztonsági incidensek hatását. Azonosítani kell tudnia a kiberincidensek kiváltó okait és rosszindulatú szereplőket. Az adott szervezet incidens-elhárítási terve alapján vissza tudja állítani a rendszerek és folyamatok funkcionalitását a korábbi működőképes állapotba, továbbá dokumentálnia kell a bizonyítékokat és a megtett intézkedéseket. [19]

A kiberbiztonsági és kibervédelmi kutatás-fejlesztést és a kiberbiztonsági készségek a Bizottság digitális készségekre vonatkozó általános menetrendje alá tartoznak. A fejlesztések a Horizont 2020, a Horizont Európa és a Digitális Európa program forrásaiból valósulnak meg.

A 2023-as évet a Bizottság a készségek évének nevezte ki. Az Európai Kiberbiztonsági Készségek Keretrendszerére alapozva, a kiberbiztonsággal foglalkozó szakemberek számának növelése érdekében kerül kialakításra a Kiberbiztonsági Akadémia, mely koordináló, ernyőszervezetként fog működni és európai és nemzeti szinten már meglévő kezdeményezéseket, és koordinációt, integrációt és ezek közötti közös kommunikációt fog biztosítani.

2021-ben hozták létre Bukarestben az Európai Kiberbiztonsági Kompetencia Központot (ECCC), hogy növelje Európa kiberbiztonsági kapacitásait és versenyképességét, és együttműködik a Nemzeti Koordinációs Központok Hálózatával (NCC) egy erős kiberbiztonsági közösség felépítésén. Az európai központ és a nemzeti hálózatok támogatják a digitális egységes piac védelmét, mint az elektronikus kereskedelem, az intelligens mobilitás és az IOT, továbbá hozzájárulnak az Unió kiberbiztonság terén fennálló autonómiáját.

Kiber network az EU-ban

Az Európai Unió Kiberbiztonsági Ügynöksége az ENISA a legmagasabb szintű ügynökség mely támogatja a tagországokat, az uniós intézményeket és a vállalati szektort, tudásmegosztást, kapacitásfejlesztést végez és segít felkészülni Európának az új kibertérben történő kihívásokra.

Az ENISA-val működnek együtt az információmegosztó és elemző központok (ISAC), melyek feladat a gazdasági szereplők és a kiberbiztonsági közösségek közötti együttműködés támogatása.

A NIS-irányelv is meghatározza, hogy a tagállamoknak működtetniük kell úgynevezett Computer Security Incident Response Teams (CSIRT-eket), más néven Computer Emergency Response Teams (CERT-eket). Ezek a csapatok uniós szinten is együttműködnek kapcsolatba vannak a magánszektorral is. A szektoriálisan kialakított CSIRT-eknek feladatuk, reagálás az eseményekre és azok nemzeti szintű nyomon követése, a kockázatokkal és incidensekkel kapcsolatos korai figyelmeztetések, azok elemzése, riasztások, bejelentések és egyéb információk biztosítása az érintett érdekelt felek számára.

Az Európai Kiberbiztonsági Szervezetet (ECSO) 2016-ban hozták létre, hogy a 2016-tól 2020-ig tartó időszakban a Bizottság megfelelőjeként működjön a Horizont 2020 keretprogramot lefedő köz- és magánszféra közötti szerződéses partnerségben és különféle támogató tevékenységeket végezzen, a közösségépítés és az iparfejlesztés területén. Az ECSO 250 tagot számlál, melyek között vannak a kiberbiztonsági ágazathoz tartozó, kutatási, akadémiai intézmények és a közszféra szereplői, keresletoldali iparágak.

2021-ben az Európai Védelmi Ügynökség (European Defense Agency, EDA) négyoldalú együttműködést alakított ki a kibervédelemmel érintett uniós ügynökségekkel: Európai Unió Kiberbiztonsági Ügynökség (ENISA), Európai Unió Ügynöksége Rendészeti együttműködés (Europol) és a Infokommunikációs Sürgősségi Reagálócsoport az Uniós intézmények, Szervek és Ügynökségek (CERT-EU) részéről valamint a Hibrid Kiválósági Központ (CoE). A Hibrid Kiválósági Központ (CoE) és az Európai Biztonság és Védelemi Kollégium (ESDC) közreműködésével az Európai Védelmi Ügynökség (EDA) kifejlesztett egy új kiber/hibrid tanfolyamot katonai és civil művelettervezők részére a kiberfenyegetések kezelése hibrid környezetben témakörben. A Joint Cyber Unit platform pedig azzal a céllal hozták létre, hogy a nagyszabású kiberincidensekre és válságokra adott uniós koordinált válaszadás biztosítása, valamint segítséget nyújt e támadások utáni kilábaláshoz.

ÖSSZEFOGLALÓ

A második világháborút követő időszakban a Marshall-terv segítségével épültek újjá az európai közösségek és gazdaságok. A rendszerváltás követően az Észak-atlanti Szerződés Szervezet (NATO) a csatlakozott országok számára garantálta kollektív biztonságunkat.

Az egyre feszültebb geostratégiai környezet azonban látható veszélyt kezdett jelenteni a jólét és a biztonság instrumentumaira. Különösen igaz ez az EU határai mentén megjelenő orosz fenyegetettségre, mely EU történetében először mozgatott meg jelentős erőforrásokat a védelmi együttműködésének előmozdítása érdekében. A védelemmel és biztonsággal kapcsolatos miniszteri megbeszélések és egyeztetések hatására többek között létrejött a Stratégiai Iránytű, a PESCO és az Európai Védelmi Alap (EFA), mely közös irányokat és célokat jelöltek ki a közösség számára.

A digitális biztonságunk világa a kibertér, mint új hadviselési tér egyre hangsúlyosabb szerepet kapott a modern hadviselésben. Az EU kibertér elleni védelme ma már az Európai Védelmi Ügynökség, az ENISA, az Europol és a Bizottság védelmi iparért felelős főigazgatósága tevékenységein keresztül valósul meg. Szervezeti és irányelvi szinten az EU felzárkózott a világhatalmak sorába, a működtetéshez azonban hatékony és megfelelő kiberbiztonsági munkaerő kell, melynek képzési programjai és az elvárt készségek meghatározása csak most születtek meg.

Az EU stratégiai kapacitása intézményi, anyagi és politikai alapokon nyugszik, melyből az intézményi és beruházási területen hathatós előrelépéseket tett az unió az aktuálisan fennálló fenyegetettségek hatására. Az európai stratégiai kultúrákat változatossága azonban nehezít a közös vélemények kialakítását, melyek veszélyeztethetik az európai és globális védelmi és biztonsági ügyekkel kapcsolatos célok megvalósítást.

FELHASZNÁLT IRODALOM

[1] Transzatlanti Nyilatkozat. [Online]. Elérhető: https://www.europarl.europa.eu/cms-data/124320/trans_declaration_90_en.pdf

[2] European External Action Service, *Közös jövőkép, közös fellépés : erősebb Európa : globális stratégia az Európai Unió kül- és biztonságpolitikájára vonatkozóan*, Publications Office, 2017, https://data.europa.eu/doi/10.2871/695883

[3] A közös kül- és biztonságpolitika végrehajtása – 2020. évi éves jelentés. [Online]. Elérhető: https://www.europarl.europa.eu/doceo/document/TA-9-2021-0012_HU.html

[4] Liszaboni Szerződés. [Online]. Elérhető: https://www.europarl.europa.eu/ftu/pdf/hu/FTU_1.1.5.pdf

[5] P. Fábián, *Az Európai Unió terrorizmusellenes stratégiája és rendelkezései*, Biztonságtudományi Szemle, Évf. 1 szám 3., 2019

[6] Európai Parlament, Uniós Külső Politikák Főigazgatósága, Schaik, L., Dams, T., *No way back : why the transatlantic future needs a stronger EU : in-depth analysis*, European Parliament, 2020, https://data.europa.eu/doi/10.2861/026248

[7] *Grevi*, G. (2020), *Fostering Europe's Strategic Autonomy.* A *Question of Purpose* and *Action*, EPC and KAS Policy Paper, December 2020.

[8] Közös közleménye az európai parlamentnek, az európai tanácsnak, 2020, https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:52020JC0022&from=hu
[9] Soare, R. Simona (2020), Turning the tide: how to rescue transatlantic relations. EUIIS. DOI 10.2815/097304
[10] Towards a Renewed Transatlantic Partnership: https://www.whitehouse.gov/briefing-room/statements-releases/2021/06/15/u-s-eu-summit-statement/
[11] PESCO: https://www.pesco.europa.eu/
[12] Stratégiai Iránytű, https://www.consilium.europa.eu/hu/press/press-releases/2022/03/21/a-strategic-compass-for-a-stronger-eu-security-and-defence-in-the-next-decade/
[13] Cyber posture, https://www.consilium.europa.eu/en/press/press-releases/2022/05/23/cyber-posture-council-approves-conclusions/
[14] Cybersecurity: how the EU tackles cyber threats: https://www.consilium.europa.eu/en/policies/cybersecurity/
[15] Saphing Europe's Digital Future: https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/shaping-europe-digital-future_en
[16] European Comission: The EU's Cybersecurity Stratgey for the Digital Decade (2020 december 16.)
[17] NIS 2 irányelv. https://www.consilium.europa.eu/hu/press/press-releases/2022/05/13/renforcer-la-cybersecurite-et-la-resilience-a-l-echelle-de-l-ue-accord-provisoire-du-conseil-et-du-parlement-europeen/
[18] Kiberreziliencia, https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act
[19] Az EU kiberbiztonsági stratégiája a digitális évtizedre, https://eur-lex.europa.eu/legal-content/hu/TXT/PDF/?uri=CELEX:52020JC0018
[20] Katonai mobilitásról szóló cselekvési terv: https://eur-lex.europa.eu/legal-content/HU/ALL/?uri=CELEX:52019JC0011