Szladik Míra

Az Európai Unió kiberbiztonsági lépései

1. Bevezetés

A közlekedés, energetika, pénzügyi ágazatok, egészségügy egyre inkább függenek a digitális technológiától. Az utóbbi évtizedekben ez függőség még nagyobb méretűvé vált. Az Európai Unióban is számos lehetőséget nyújtotta digitalizáció árnyoldalaival is jelen lett. Ahogy az infrastruktúra, gépipar is fejlődik, úgy modernizálódnak a kibertérben elkövetett bűncselekmények is. A kibertámadások és a kiberbűncselekmények Európa szerte egyre gyakoribbakká váltak. Nem csak a gazdaság, de a társadalom is kiberfenyegetéseknek lett kitéve. Az újszerű kihívások és problémák minden ország/szervezet számára megkívánja védelmi stratégiájuknak megreformálását, illetve új alternatívák felmutatását.

Az Európai Unió az elmúlt 20 évben igyekezett a kiberbiztonsággal kapcsolatban olyan jogi környezetet alkotni, mely mindenki számára biztonságot teremt. Több fronton is dolgozik a kiberreziliencia előmozdításán, a kiberbűnözés elleni küzdelemben, illetve a kiberdiplomácia kiszélesítésében. Ezen tanulmány keretein belül bemutatom az Európai Unió fontosabb jogi lépéseit a kiberbiztonság megteremtésére.

2. Az Európai Unió kiberbiztonsági stratégiái

Az Európai Unió az elmúlt évtizedben három kiberbiztonsági stratégiát alkotott meg. Főbb elemzési pontjai a megelőzés,

reagálás, nemzetközi együttműködés, digitális biztonsági infrastruktúra, kiberbiztonsági tudatosság és az innováció.

2.1. 2013-as kiberbiztonsági stratégia

Az Európai Unió 2013-ban kezdte meg első kiberbiztonsági stratégiájának kidolgozását, ami „Az EU kiberbiztonsági stratégiája digitális évtizedre" címmel jelent meg, még ugyanabban az évben. A stratégiát az EU külügyi és biztonságpolitikai főképviselője és az Európai Bizottság dolgozta ki.[1] A 2013-as stratégia számít az első átfogó dokumentumnak, amelyet az EU a kiberbiztonság területén megalkotott. Összekapcsolta a belső biztonság kérdéseit és a külső biztonság kihívásait is. A dokumentum célul tűzte ki az egységes digitális piac létrehozását, amelyben a gazdasági növekedés kulcsát is látta, ami szorosan összefügg az emberek az internetes műveletek kapcsán tanúsított bizalmának növelésével is, ami azonban elképzelhetetlen a kibertér kockázatmentesítése nélkül.

A dokumentum öt stratégiai prioritást határoz meg a tagállamok számára. Rendelkezzenek a tagállamok rugalmas reagálási képességgel, csökkentsék a kiberbűnözés jelenségét, kibervédelmi politikát és képességeket alakítsanak ki, ipari és technológiai erőforrásokat hozzanak létre, amik szükségesek a kiberbiztonság megteremtéséhez, végül uniós szintű koherens nemzetközi kiberpolitika kialakítása.[2]

A stratégia három nagy területen tartja szükségesnek az intézkedések meghozatalát. A nemzeti szinten, ahol az állami és

---

1 Bihaly Barbara: A kibervédelem szerepe az Európai Unió közös biztonsági és védelmi politikájában, *Hadtudományi szemle,* 2021/3. 49. o.

2 Gazdag Ferenc – Remek Éva: *A biztonsági tanulmányok alapjai,* In: Hautzinger Zoltán (szerk.): *Studia Universitatis Communia,* Budapest, Dialóg Campus Kiadó, 2018. 134. o.

a magánszektor összefogása, a kapacitások hatékony fejlesztése a feladat. Az uniós szint, ahol kiemelt szerepe van az ENISA-nak a határokon átnyúló incidenskezelés fejlesztése céljából. A jogalkotás területén, amelynek ki kell terjedni arra, hogy a tagállamok egy nemzeti stratégiát alkossanak és megalakíthatók legyenek a CERT-ek.[3]

A dokumentum az kibertér kiépítésében felismerte a magánszektor szerepének fontosságát, azonban leszögezte, hogy egyre nő az igény a biztonságra, transzparenciára, valamint az elszámoltathatóságra, amelyet csak magasabb szinteken lehet eredményesen megvalósítani. Ennek tükrében fogalmazta meg általános éllel azokat az alapelveket, amelyeken a közös kiberbiztonsági stratégia nyugszik: az Európai Unió alapértékei ugyanolyan mértékben vonatkoznak a digitális világra, mint a fizikaira; a hozzáférés mindenki számára biztosított kell, hogy legyen; az érdekelt felek bevonásával történő demokratikus és hatékony irányítás; biztonság, mint közös felelősség.[4]

Szerepkörét tekintve már a dokumentum megalkotásakor is egyértelmű volt, hogy a kérdés összetettsége és az érintettek sokfélesége miatt központi felügyeleti rendszer kialakítására nem lesz lehetőség. Így a kibertámadások megelőzése és kivédésének rendszere alapvetően nemzeti szinten kell, hogy működjön, ami aztán adott esetben az uniós szintű beavatkozás által kerülhet kisegítésre. Ennek három fő pillére a NIS, a bűnüldözés és a védelem területe lesz.[5]

---

3 Kovács László: *Kiberbiztonság és -stratégia,* Budapest, Dialog Campus Kiadó, 2018. 88. o.

4 Európai Bizottság: Közös Közlemény az Európai Parlamentnek, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának, Az Európai Unió kiberbiztonsági stratégiája, 2013.02.7., https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:52013JC0001&from=EN (Letöltés: 2023.02.11.)

5 Az Európai Unió kiberbiztonsági stratégiája (2013) 20. o.

2.2. 2017-es kiberbiztonsági stratégia

Az Európai Bizottság és a tagállamok döntéshozói számára is hamar világossá vált, hogy a 2013-as kiberbiztonsági stratégia az új technikai, politikai, gazdasági változások miatt felülvizsgálatra szorul. A tagállamokban a 2013-as stratégia végrehajtása sem ment zökkenőmentesen, ez is egy ok volt, amiért a stratégia újításra szorult. 2013 óta a kiberbűnözés, fenyegetések aránya erősen megnövekedett, ami szintén egy intő jel volt, egy erősebb stratégia megalkotására.[6]

A 2017-es stratégiában nagyobb hangsúlyt kap a nemzetközi együttműködés fejlesztése, amely egy digitális egységes piac, globális stratégia, európai biztonsági stratégia, hibrid fenyegetésekkel szembeni fellépés közös kerete kialakítását könnyítené meg. Ezekkel a témákkal az Unió már korábban is foglalkozott, viszont a 2017-es stratégia elérkezettnek látta az időt, hogy ezeket a munkafolyamatokat összefogják. A 2013-as stratégiában megfogalmazott fő célok és elvek (megbízható, biztonságos és nyitott kiber-ökoszisztéma elősegítése) a 2017-es startégiában is aktuálisak, viszont nagyobb és több erőre van szükség ahhoz, hogy az egyre súlyosodó fenyegetésekkel szembe lehessen nézni.[7]

A 2017-es stratégia felhívja a figyelmet arra, hogy a kibertámadásokkal szembeni ellenállóképesség eléréséhez, illetve a stratégiai függetlenség kiépítéséhez egy olyan erős és egysége piac, nagyobb uniós technológiai fejlesztések és képzett szakemberek

6 Európai Bizottság: Közös közlemény az Európai Parlamentnek és a Tanácsnak: Ellenálló képesség, elrettentés, védelem: az Unió erőteljes kiberbiztonságának kiépítése 2017. 09. 13. 2. o.

7 Kelemen Roland: Az Európai Unió kiberbiztonsági stratégiájának evolúciója az elmúlt évtizedben. In: Bódiné Beliznai Kinga – Gosztonyi Gergely (szerk.): *Jogtörténeti Parerga III: Ünnepi tanulmányok Mezey Barna 70. születésnapja tiszteletére,* Budapest, ORAC Kiadó Kft., 2023. 182. o.

kellenek, amellyel egy átfogóbb és a szakpolitikákon átívelő megközelítést ér el.[8]

Az ENISA állandó megbízatást kapott az Bizottságtól feladatainak minél hatékonyabb ellátása érdekében. Lehetővé tette, hogy az ENISA képes legyen támogatni a tagállamokat, uniós intézményeket és vállalkozásokat olyan területeken, mint például a hálózati és információs rendszerek biztonságáról szóló irányelv, vagy a kiberbiztonsági tanúsítási keretrendszer. Az európai felkészültséget azzal is fokoznák, hogy éves összeurópai kiberbiztonsági gyakorlatokat szerveznek. Továbbá az ENISA-nak támogatnia kell az információs és kommunikációs technológiák (IKT) uniós szakpolitikáinak kidolgozását.[9]

A kiberbiztonsági piac növekedését az EU-ban számos tényező visszafogja. A termékekbe való magasabb fokú ellenálló képesség kialakítása céljából a Bizottság javaslatot nyújtott be egy uniós kiberbiztonsági tanúsítási keretrendszer létrehozásáról.

Az EU létrehozott egy olyan EU egészére érvényes tanúsítási keretrendszert, ami az információs és kommunikációs technológiai termékek, szolgáltatások és eljárások kiberbiztonsági tanúsítására vonatkozik. Az új mechanizmust az ipar például intelligens orvostechnikai eszközök tanúsítására használhatná.[10]

A rendszer szabályok, műszaki követelmények, szabványok és eljárások formájában valósul meg, ami csökkenti a piac széttagoltságát, felszámolja a szabályozási akadályokat és – amennyiben a tagállamok ténylegesen alkalmazzák őket – megkönnyíti

8 Közös közlemény az Európai Parlamentnek és a tanácsnak, Ellenálló képesség, elrettentés, védelem: az Unió erőteljes kiberbiztonságának kiépítése 3. o.

9 Közös közlemény az Európai Parlamentnek és a tanácsnak 2017.

10 Az EU közös kiberbiztonsági tanúsítási keretrendszert hoz létre és megerősíti ügynökségét – A Tanács kialakította álláspontját https://www.consilium.europa.eu/hu/press/press-releases/2018/06/08/eu-to-create-a-common-cybersecurity-certification-framework-and-beef-up-its-agency-council-agrees-its-position/ (Letöltés: 2022.10.12.)

a határokon átnyúló kereskedelmet, javítva a belső piac működésének feltételeit. A kiberbiztonsági tanúsítási rendszerek stratégiai prioritásait a Bizottság által közzétett uniós gördülő munkaprogram tartalmazza, amelyben megtalálhatók azon IKT-termékek, szolgáltatások és folyamatok, amelyek alkalmasak arra, a tanúsítási rendszer hatálya alá tartozzanak.[11]

A termékek, szolgáltatások és folyamatok jelentette kiberbiztonsági veszélyék alapján a tanúsítvány három megbízhatósági szintet – alap", „jelentős", valamint „magas" – különböztet meg. Ezek alapján határolható be, hogy rendeltetésszerű használatuk mekkora valószínűséggel, és milyen mértékű, illetve hatású veszélyt jelenthet. A gyakorlatban ez azt jelenti, hogy az a termék, amely „magas" biztosítási tanúsítványi szint szerint kerül besorolásra, az megfelelt a legmagasabb szintű biztonsági teszteknek.[12] Az ez alapján kiállított bizonyítvány elismerésre kerül az összes tagállamban, amely megkönnyíti a forgalmazását és növeli a termék, szolgáltatás, vagy folyamat megbízhatóságát.

A nemzetközi együttműködés erősítése az Európa kibertérbeli stratégiai autonómiájához való hozzájárulást szolgálja. Mivel világszerte a nemzetbiztonságra leselkedő egyik legnagyobb veszély a kibertámadás, ezért az országok érdeke egy erős szövetség és partnerség fenntartása, annak érdekében, hogy ezeket a támadásokat elhárítsák. Az Unió támogatja azt az álláspontot, miszerint a nemzetközi jog a kibertérben is érvényesüljön. A globális kiberstabilitás alapja az országok helyi és nemzeti képessége a kiberincidensek megelőzésére, azokra való reagálása. Az Unió 2013 óta vezető szerepet tölt be a nemzetközi kiberkapacitás-építésében. A 2017-es stratégia szerint továbbra is

11 Az Európai Parlament és a Tanács (EU) 2019/881 rendelete az ENISA-ról (48).

12 Az Európai Parlament és a Tanács (EU) 2019/881 rendelete az ENISA-ról (84).

a jogokon alapuló kapacitásépítési modellt fogja előmozdítani, a digitálisan a fejlődésért megközelítésnek megfelelően.[13]

Az EU a NATO-val is el fogja mélyíteni az együttműködést a kiberbiztonság, hibrid fenyegetések és a védelem terén. Továbbá támogatni fogják a kutatási és innovációs együttműködést is.

Főbb intézkedéseit tekintve: teljes körű végrehajtása a hálózati és információs rendszerek biztonságáról szóló irányelvnek, európai tanúsítási keretrendszer meghatározásáról szóló rendelet elfogadása, közös bizottsági/iparági kezdeményezés a termékek/szoftverek sebezhetőségének csökkentése érdekében, hatásvizsgálat végzése, melynek során létrehozzák az Európai Kiberbiztonsági Kutatási és Kompetenciaközpontot, tagállamok fellépése a kiberbiztonsági képzési programokba.

Összefoglalva az Unió kiberfelkészültsége központi jelentőségű az egységes digitális piac, illetve a biztonsági és védelmi unió szempontjából. A 2017-es stratégia meghatározza a kihívások nagyságrendjét és azokat az intézkedéseket, amelyeket az Európai Unió megtehet a biztonság létrehozása érdekében. Olyan célzott intézkedések javaslatait foglalja magába, melyek a tagállamok és az érintett uniós szervek együttműködésével, azok hatásköreit és feladatköreit tiszteletben tartva.

2.3. 2020-as kiberbiztonsági stratégia

2020 év végén az Európai Uniónak új kiberbiztonsági stratégiája lett Az EU kiberbiztonsági stratégiája a digitális évtizedre címmel.[14] A stratégia kiemeli, hogy a közlekedés, az energiaügy, a telekommunikáció, a pénzügy, a biztonság, az űrpolitika, a védelem és a demokratikus folyamatokat egyre inkább befolyásolja

13 Közös Közlemény az Európai Parlamentnek és a Tanácsnak 2017.

14 European Commission: The EU's Cybersecurity Strategy for the Digital Decade (2020. december 16.).

a hálózati és információs rendszerek.[15] Felvázolja, hogy az EU-nak nincs meg a kollektív helyzetismerete a kiberfenyegetésekkel kapcsolatban, ezért a kiberbiztonság javítása elengedhetetlen. Az új kiberbiztonsági stratégia meghatározza, hogyan fogja megvédeni az Európai Unió lakóit a kibertámadásoktól, illetve milyen nemzetközi együttműködéseket köt a biztonság érdekében.

A 2020-as startégiában nagy szerepet kap a globális gondolkodás és az európai cselekvés, ennek elérése érdekébe szükséges egy globális és nyílt internetet. Ezt úgy kívánja biztosítani, hogy 1. megteremti a rezilienciát, a technológiai szuverenitást, 2. az operatív kapacitásépítést a megelőzés, elrettentés és reagálás érdekében, és 3. előmozdítja a globális nyílt kiberteret.[16]

Az EU ennek a stratégia melletti elköteleződés érdekében elfogadta a Digitális Európa programot is, amelynek keretében 2021-2027-ig soha nem látott mértékű uniós digitális átállási beruházásokat tervez az új technológiai és ipari szakpolitikák, illetve a helyreállítási menetrend részeként. A Digitális Európa program célja, hogy elérhetővé tegye a vállalkozások, a polgárok és a közigazgatási intézmények számára a technológiát. Továbbá fel szeretné gyorsítani a gazdasági fellendülést és az európai társadalom és gazdaság digitális átállását is. Ez a program mindenki számára kedvező különösen a kis- és középvállalkozásoknak. Öt területet foglal magába, melyeket támogat a program: szuper-számítástechnika, mesterséges intelligencia, kiberbiztonság, fejlett digitális készségek, a digitális technológiák alkalmazása és hozzáférhetősége.[17]

15 Közös közlemény az Európai Parlamentnek és a Tanácsnak: Az EU kiberbiztonsági stratégiája a digitális évtizedre, 1. o.

16 Közös közlemény az Európai Parlamentnek és a Tanácsnak: Az EU kiberbiztonsági stratégiája a digitális évtizedre, 5. o.

17 Digital Europe: https://culture.ec.europa.eu/hu/node/1179 (Letöltés: 2023.03.28.)

A stratégia értelmében fokozni kell valamennyi érintett gazdaság és a társadalom szempontjából fontos feladatot ellátó ágazat kiberrezilienciáját.[18] A hálózati és információs rendszerek biztonságára vonatkozó szabályok alapján fokozni kell az érintett gazdaság és a társadalom szempontjából fontos feladatot ellátó ágazatok kiberrezilienciáját. Ahhoz, hogy a kifinomultabb kibertámadásokkal szemben fel lehessen lépni a Bizottság javaslatára kiépítik a biztonsági műveleti központok uniós hálózatát, amely egy kiberbiztonsági pajzsként fog funkcionálni az EU számára.[19] A hálózati és számítógépes rendszerek folyamatos nyomon követése és elemzése végett, sok nemzeti hatóság, állami szervezet számítógépes-biztonsági eseményekre reagáló csoportokat (CSIRT) és biztonsági műveleti központokat (SOC) hozott létre.[20]

Az új kiberbiztonsági stratégia értelmében a kiberbiztonság beépülne az ellátási lánc valamennyi elemébe és négy kiberbiztonsági szektoron – belső piac, bűnüldözés, diplomácia, védelem területén – átívelve még szorosabban összekapcsolná az uniós tevékenységeket.

---

18 Farkas Ádám: II.6. A kibertér állami-társadalmi-egyéni biztonsági szintjeinek metszéspontja: a reziliencia, In: Farkas Ádám – Kelemen Roland: *Nemzeti biztonság és kibertér,* Budapest, Médiatudományi Intézet, 2023. 104–110. o.; Vikman László: A közműszolgáltatások és a reziliencia egyes kérdései, különös tekintettel a kiberbiztonságra, *Védelmi-biztonsági Szabályozási és Kormányzástani Műhelytanulmányok,* 2021/14.; Kelemen Roland – Mihály Laura Dominika: A kibertér és a psziché ütközéspontjai mint a 21. századi reziliencia kulcskérdése. *Védelmi-biztonsági Szabályozási és Kormányzástani Műhelytanulmányok.* 2022/14.

19 Közös közlemény az Európai Parlamentnek és a Tanácsnak: Az EU kiberbiztonsági stratégiája a digitális évtizedre, 8. o.

20 Közös közlemény az Európai Parlamentnek és a Tanácsnak: Az EU kiberbiztonsági stratégiája a digitális évtizedre, 7. o.

3. Szabályozások átalakulása 2010 után

3.1. NIS 1. irányelv

A 2013-as Stratégia megalkotásával már lehetett látni, hogy kell egy kiegészítés, ami annak esszenciális második feleként is értelmezhető biztonsági intézkedésekről szóló irányelv lesz. 2016-ban került elfogadásra a NIS-irányelv, ami a sebezhetőség csökkentése érdekében jött létre a Kiberbiztonsági Stratégia követelményeinek megfelelően.

A dokumentum teljes címe az Európai Parlament és a Tanács (EU) 2016/1148 irányelve a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről.[21] Ahogy a címből is kiderül, a NIS-irányelv már egy konkrét jellegű jogi jellegű intézkedéseket tartalmaz, ami az Európai Unió egészére kiterjedő kiberbiztonság területén hozott szabályozás, melynek célja a kiberbiztonság mértékének növelése.

A NIS-irányelv elsősorban a nemzeti keretek kialakítását szorgalmazta, ami kiemelte, hogy a nemzeti stratégia foglalkozzon a felkészültség, reagálás, helyreállítás körében tehető intézkedések azonosításával, kockázatértékelési terv készítésével, rendszerek biztonságára vonatkozó célok és prioritások kijelölésével, a nemzeti stratégiák vonatkozásában szervezett oktatási, tájékoztató és képzési programok megjelölésével, illetve a nemzeti stratégiák végrehajtásában érintett szereplők jegyzékével.[22]

---

21 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, https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX%3A32016L1148 (Letöltés: 2023.02.11.)

22 Európai Parlament és a Tanács 2016/1148 irányelve 7. cikk (1).

Az irányelv kötelezővé teszi a tagállamok számára, hogy kijelöljenek egy vagy több számítógép-biztonsági eseményekre reagáló csoportot (CSIRT), amelyek az adott szektor történéseiért felelős. Annak érdekében, hogy az egész EU területén közösségi szintű együttműködés jöhessen létre, az irányelv létrehozta az Együttműködési Csoportot, ami a hatóságok együttműködésére szolgál, illetve a CSIRT hálózatot, ami a CSIRT-ek együttműködését biztosítja.[23]

Kiépítésére került egy olyan együttműködési csoport is, amely a tagállamok, a Bizottság és az ENISA (Európai Uniós Hálózat- és Információbiztonsági Ügynökség) képviselőiből állt. Feladata az államok közötti stratégiai együttműködés, az információcsere támogatása, illetve a hálózati és információs rendszerek biztonságának megteremtése.[24]

3.2. NIS 2. irányelv

A kibertér rohamos változását mutatja, a jogalkotás területén fellépő intézkedése, ugyanis hat évvel a NIS 1. irányelv elfogadását követően 2023. január 16-án a Tanács és az Európai Parlament életbe léptette a NIS 2. irányelvet, amely az Unió egész területén egy egységes és magas szintű kiberbiztonsági környezetet kíván megteremteni. A célja az irányelvnek a NIS 1-hez hasonló, azt fejleszti tovább: javítani kíván a köz- és a magánszektor kiberrezilianciáján, illetve a kiberbiztonsági eseményekre való reagálási képesség növelésén.

A NIS 2. preambuluma is kiemeli, hogy „A hálózati és információs rendszerek a mindennapi élet központi jellemzőjévé fejlődtek a társadalom gyors digitális átalakulásával és összekapcsolódásával, beleértve a határokon átnyúló információ-

23 Európai Parlament és a Tanács 2016/1148 irányelve 11. cikk, 12. cikk.
24 Európai Parlament és a Tanács 2016/1148 irányelve 11. cikk.

megosztást is. Ez a fejlődés a kiberfenyegetettség bővüléséhez vezetett, új kihívások támasztásával, amelyek minden tagállamban kiigazított, összehangolt és innovatív reagálást igényelnek."[25]

3.2.1. Mi a különbség a NIS 2. és a NIS 1. irányelv között?

A NIS 2. irányelv tágabb hatállyal rendelkezik. Sokkal több ágazatra kiterjed a hatálya, így a korábban fókuszban lévő ágazatok mellett (energetika, közlekedés) kibővült a szolgáltatások köre is, melyet az irányelv két csoportra bont szét: a korábbi „alapvető szolgáltatásokat nyújtó" szereplők és a „digitális szolgáltatók" helyett fontos és alapvető szervezeteket határoz meg, melyeket kiemelten kritikus ágazatokhoz és egyéb kritikus ágazatokhoz sorol.[26]

Kiemelten kritikus ágazatok csoportjában átfedéseket mutat a NIS 1. irányelvvel, viszont a digitális infrastruktúra körében érintett szolgáltatások köre kiszélesedett, illetve több új elemet is beemelt az ágazati körébe (például: világűr, IKT szolgáltatások irányítása).

Az egyéb kritikus ágazatok között megjelenik a vegyszerek gyártása, digitális szolgáltatók, futárszolgáltatások stb.

Azok a szervezetek, melyek a kiemelten kritikus, vagy az egyéb kritikus ágazatokhoz tartoznak, de nem sorolhatók az alapvető szervezetek köréhez, azok fontos szervezetnek minősülnek. A tagállamok feladatköréhez sorolja a fontos és az alapvető szervezetek listájának összeállítását.[27]

A szabályok hatályára vonatkozólag is változást hozott a NIS 2. irányelv. Míg a NIS 1. irányelv alapján a tagállamok

25 Az Európai Parlament és a Tanács 2022/2555 irányelve.

26 Az Európai Parlament és a Tanács 2022/2555 irányelve 1. 2. melléklet.

27 Domokos Márton – Bertók Gábor – Huszár Daniella: *NIS 2. – az EU új kiberbiztonsági irányelve*, https://www.jogiforum.hu/hir/2023/01/03/nis2-az-eu-uj-kiberbiztonsagi-iranyelve/ (Letöltés: 2023.03.14.)

feladata, volt az, hogy melyik szervezetek felelnek meg annak a kritériumoknak, melyek alapján alapvető szolgáltatásokat nyújtó szereplőknek minősülnek. Az új irányelv megteremti a méretkorlátra vonatkozó szabályt, amely általános szabályként terjed ki a hatálya alá tartozó ágazatokban működő, illetve a hatálya alá tartozó minden közepes és nagyméretű szervezetre, amelyek szolgáltatásokat nyújtanak.[28] A NIS 2. irányelv megalkotja a jogi koherenciát más szektorspecifikus szabályokkal, mint pl. a DORA rendelet, ennek értelmében ezen szabályoknak ugyanolyan szintű védelmet kell biztosítani, mint a NIS 2. irányelvnek.[29]

A tagállamoknak, ahogyan minden uniós irányelvet, természetesen a NIS 2. irányelvet is át kell ültetniük a nemzeti jogukba. Azonban számos más kötelezettséget is előír az irányelv, többek között ki kell jelölni a tagállamoknak illetékes hatóságokat és egyedüli kapcsolattartó pontokat, nemzeti kiberbiztonsági stratégiákat és szakpolitikákat kell elfogadniuk, kiberbiztonsági válságkezelési keretek kialakítása szükséges, továbbá létre kell hozni a számítógép-biztonsági eseményekre reagáló csoportokat (CSIRT)

A tagállami átültetés alapján a nemzetközi jogban is megjelenik az érintett alapvető és fontos szervezetek számára meghatározott kötelezettség. Ilyen kötelezettség például az, hogy minden olyan eseményről, amely jelentős hatással van a szolgáltatásaik nyújtására (alapvető és fontos szervezetek),

28 EU Tanácsa: *A kiberbiztonság és -reziliencia megerősítése az EU egész területén – Ideiglenes megállapodás a Tanács és az Európai Parlament között*, 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/ (Letöltés: 2023.03.14.)

29 Domokos Márton – Bertók Gábor – Huszár Daniella: *NIS 2. – az EU új kiberbiztonsági irányelve*, https://www.jogiforum.hu/hir/2023/01/03/nis2-az-eu-uj-kiberbiztonsagi-iranyelve/ (Letöltés: 2023.03.14.)

értesíteniük kell a CSIRT-jüket vagy az illetékes hatóságot.[30] A kötelezettségeket, már a NIS 1. irányelv is magába foglalta, viszont a NIS 2. szabályai jóval részletesebben kitér a kötelezettségi pontokra.

Az irányelv kiemeli a nemzetközi együttműködés nagyfokú szerepét is és ennek érdekében együttműködési csoportok létrehozását írja elő.[31] Kialakítja a nemzeti CSIRT-hálózatot, amely a tagállamok közötti gyors és hatékony együttműködést szolgálja. Létrehozták az Európai Kiberválságügyi Kapcsolattartó Szervezetek Hálózatát (EU-CyCLONe), amely a tagállamok, az Unió, ügynökségek, hivatalok közötti releváns információk rendszeres és hatékony cseréjét szolgálák.[32]

Az irányelv szabályozásai nem terjednek ki az olyan területekre, mint a védelem vagy a nemzetbiztonság, a közbiztonság, bűnüldözés és az igazságszolgáltatás. Továbbá nem terjed ki az irányelv hatálya a parlamentek és a központi bankokra sem.[33] A közigazgatási szervekre való tekintettel (mivel gyakran szerepelnek a kibertámadások célpontjai között) a NIS 2. irányelv rájuk alkalmazandó lesz.

Az EU kiberbiztonsági ügynökségének (ENISA) szerepét az irányelv növelte, magasabb szinten kell elvégeznie a meglévő feladatait. Feladatai közé tartozik az európai sérülékenység-adatbázis fenntartása, Unió kiberbiztonsági helyzetéről jelentéskészítés, DNS-szolgáltatók, a doménnév-nyilvántartási szolgáltatásokat nyújtó szervezetek, a felhőszolgáltatók, az adatközpont-szolgáltatók, a tartalomszolgáltató hálózati szolgáltatók, az irányított szolgáltatók és az irányított biztonsági szolgáltatók, valamint az

30 Az Európai Parlament és a Tanács 2022/2555 irányelve 21. cikk (1).
31 Az Európai Parlament és a Tanács 2022/2555 irányelve 14. cikk III. fejezet.
32 Az Európai Parlament és a Tanács 2022/2555 irányelve 16. cikk (1).
33 Az Európai Parlament és a Tanács 2022/2555 irányelve (8).

online piacterek, az online keresőprogramok és a közösségimédia-szolgáltatási platformok szolgáltatói nyilvántartása.[34]

A tagállamoknak a NIS 2. irányelvet, 2024. október 17-ig kell elfogadniuk és kihirdetniük. A NIS 2. irányelv elfogadása mellett sor került a pénzügyi ágazat digitális működési rezilienciájáról szóló rendelet (DORA rendelet) elfogadására. Folyamatban van a kiberreziliencia rendelet elfogadása is.

3.3. DORA rendelet

2020. szeptember 24-én az Európai Bizottság közzétette a Digital Operational Resilience Act első tervezetét (DORA rendelet). Miért volt szükség erre a rendeletre? A pénzügyi szektorban létező szervezetek egy erős kölcsönös függőségeken alapuló rendszerekben működnek, amelyek nem egységesek EU-s szinten, nehezen összeegyeztethetők az kibertérben felmerülő kockázatok kezelésére megalkotott törvényi szabályozások. Az Európai Bizottság ezért, közösségi szinten is fontosnak tartotta, hogy az informatikai kockázatokat és fenyegetéseket egységesen kezeljék. Így megszületett a DORA rendelet, amely segítségével átláthatóbb lesz a törvényi szabályozás.[35] Tehát az elsődleges cél, az IKT (információs és kommunikációs technológia) ellenállóképességének megerősítése a pénzügyi szolgáltatások terén.

A rendelet 20 pontban, tételesen felsorolja, mit kell pénzügyi szervezet alatt érteni, de a rendelet hatálya kiterjed a harmadik fél IKT-szolgáltatók körére is (adatelemzési szolgáltatásokat kínáló szolgáltatók, felhőalapú számítástechnikai

34 Az Európai Parlament és a Tanács 2022/2555 irányelve 6. cikk (34).

35 Szőllősi Zoltán: *DORA (Digital Operational Resilience Act) rendet tesz a pénzügyi kibertérben*, https://www2.deloitte.com/hu/hu/pages/kockazat/articles/dora.html (Letöltés: 2023.03.27.)

szolgáltatások.[36]) A szervezeteknek rendelkezniük kell egy ellenálló képességgel, illetve egy helyreállító képességgel az IKT-incidensek kezelése végett.

A DORA a kiberbiztonsági előírásokat öt fő területen szabályozza.[37]

— IKT kockázatkezelés;
— IKT-val kapcsolatos események kezelése, osztályozása, jelentése;
— digitális működési reziliencia tesztelése;
— harmadik féltől eredő IKT kockázat kezelése;
— információk megosztására vonatkozó megállapítások.

A rendelet mindegyik területre részletes szabályozásokat hozott meg. Az IKT kockázatkezelés kapcsán előírja az IKT-rendszerek és eszközök beállítását és karbantartását, hogy ezzel minimalizálják az IKT-kockázatok hatását. Ha felmerül IKT-kockázat, akkor ezeknek a forrását folyamatosan azonosítani kell és védelmi, illetve megelőzési intézkedéseket kell kidolgozni az elhárítás érdekében. Katasztrófa- és helyreállítási terveket kell bevezetni, amelyek biztosítják az IKT-val kapcsolatos incidensek utáni gyors helyreállítást.

A digitális működési reziliencia érdekében az IKT kockázatkezelési keretrendszer elemeinek felkészültségét időszakonként tesztelni kell. Ha gyengeségek, hiányosságok fordulnak elő a rendszerben, azokat azonosítani kell, és azonnal megszüntetni.[38]

A harmadik féltől eredő IKT kockázatok kezelése érdekében biztosítani kell a külső IKT-szolgáltatókra való támaszkodásból származó kockázatok alapos nyomon követését. A szolgáltatások kulcsfontosságú elemeit harmonizálni kell. A kritikus vagy

36 Az Európai Parlament és a Tanács 2022/2554 rendelete 63. szakasz.
37 Az Európai Parlament és a Tanács 2022/2554 rendelete 1. cikk (1) (a).
38 Az Európai Parlament és a Tanács 2022/2554 rendelete 24. cikk (1-6).

fontos funkciókat támogató IKT-szolgáltatások esetén a pénzügyi szervezeteknek kilépési stratégiát kell bevezetniük.[39]

Az információmegosztás ösztönzi az együttműködést más pénzügyi szervezetek megbízható közösségei között. Az ilyenfajta együttműködés fokozza a pénzügyi szervezetek digitális működési rugalmasságát, illetve felhívja a figyelmet az IKT-kockázatokra. Továbbá egy ösztönzés a pénzügyi szervezetek részére, hogy a kibertér fenyegetéseivel kapcsolatos információkat megosszák egymással.[40]

3.4. CER irányelv

Az Európai Bizottság 2020. december 16-án terjesztette elő a kritikus szervezetek ellenálló képességéről szóló irányelvjavaslatát (The Critical Entities Resilience Directive – CER). A tagállamoknak 2024. októberig kell beültetni az irányelvet a hazai jogba. A javaslat szakít a korábbi rendszerelem védelmére fókuszáló szemlélettel és helyére a kritikus fontosságú szervezetek működésének ellenálló képesség kialakítása kerül. Elfogadását követően az irányelv hatályánkívül helyezte a 2008-ban elfogadott, az európai kritikus infrastruktúrák azonosításáról és kijelöléséről szóló jelenlegi irányelvet. Ennek az volt az oka, hogy míg a 2008-as irányelv nem volt felkészülve azokra az új kihívásokra, amik a 2010-es években érték a világot. Például a digitális gazdaság térnyerésére, terrorveszélyre, Covid-19 világjárványra. Ezek mind rávilágítottak arra, hogy az uniós tagállamok között globális szinten is nagyfokú kölcsönös függőség áll fenn, tehát igény volt egy új, aktuális irányelv megalkotására.[41]

39 Az Európai Parlament és a Tanács 2022/2554 rendelete 28. cikk (8).

40 Az Európai Parlament és a Tanács 2022/2554 rendelete 45. cikk.

41 Az Eu Tanácsa: *Az EU rezilienciájának erősítése*, https://www.consilium.europa.eu/hu/press/press-releases/2021/12/20/strengthening-eu-resilien-

Az irányelv kilenc ágazatot sorol fel, amelyeket kritikus fontosságú szervként jelöl meg: közlekedés, energia, egészségügy, ivóvíz, szennyvíz, digitális infrastruktúra, űrágazat, banki szolgáltatások, pénzügyi piaci infrastruktúrák.[42] Az itt felsorolt ágazatoknak képesnek kell lenniük például a Covid19, terrorizmus, természeti katasztrófák megelőzésére, védelem biztosítására és az ellenálló képesség kialakítására.

A tagállamok számára is előír kötelezettségeket az irányelv. Négyévente kockázatértékelést kell végezniük és azonosítaniuk kell az alapvető szolgáltatásokat nyújtó, kritikus fontosságú szervezeteket, olyan releváns kockázat értékelése érdekében, melyek zavart okozhatnak.[43]

Az irányelv azonosítja a különös európai jelentőségű kritikus szervezeteket is. Akkor minősülhet egy szervezet kiemelt európai jelentőségű, kritikus fontosságú szervezetnek, ha a tagállamok közül hat vagy több állam számára nyújt alapvető szolgáltatásokat. A tagállamok ebben az esetben felkereshetik a Bizottságot, hogy az tanácsadó missziókat az érintett szervezetek kötelezettségeinek teljesítése érdekében bevezetett intézkedések értékelése céljából.[44]

Létrehoz az irányelv egy kritikus szervezetek rezilienciájával foglalkozó csoportot is, aminek a célja az, hogy segítse a tagállamok közötti együttműködést és az információcserét ezen irányelvvel kapcsolatban.[45]

---

ce-council-adopts-negotiating-mandate-on-the-resilience-of-critical-entities/

42 Az Európai Parlament és a Tanács (EU) 2022/2557 irányelve a kritikus szervezetek rezilianciájáról (5).

43 Az Európai Parlament és a Tanács (EU) 2022/2557 irányelve a kritikus szervezetek rezilianciájáról III. fejezet 12. cikk (1).

44 Az Európai Parlament és a Tanács (EU) 2022/2557 irányelve a kritikus szervezetek rezilianciájáról 18. cikk (1).

45 Az Európai Parlament és a Tanács (EU) 2022/2557 irányelve a kritikus szervezetek rezilianciájáról 19. cikk.

A CER és a NIS 2. irányelv kapcsán a tagállamok hangsúlyozzák, hogy a két irányelvet össze kell hangolni egymással. Tehát a kritikus fontosságú szervezetek rezilienciájáról szóló irányelv hatálya alá tartozó ágazatok a NIS 2. irányelv hatálya alá is tartozzon.[46]

4. Intézmények

4.1. Európai Uniós Hálózat- és Információbiztonsági Ügynökség

A hírközlő hálózatok és az információs rendszerek is a társadalmi fejlődés alapvető elemeivé váltak. Mindenhol jelen vannak: vízellátás, villamos energia stb. Alapvető prioritás ezeknek a rendszereknek a biztonságos működése, ugyanis egy esetleges baleset, támadás során ezeknek az infrastrukturális rendszereknek a meghibásodása óriási problémákat tudnak okozni a polgárok számára. Szükségessé vált egy olyan európai szintű szakértői központ létrehozása, amely iránymutatást és tanácsot ad, segítséget nyújt. Ezen igények kielégítése céljából az Európai Parlament és a Tanács a 460/2004/EK rendeletével létrehozta az Európai Hálózat- és Információbiztonsági Ügynökséget (továbbiakban: ENISA).[47]

Alapfeladatai között megjelenik a tagállamoknak való tanácsadás a tudatosság növelése érdekében, ugyanis a hálózati és információs rendszerek iránti bizalom biztosítása miatt szükséges

46 Az Eu Tanácsa: *Az EU rezilienciájának erősítése*, https://www.consilium.europa.eu/hu/press/press-releases/2021/12/20/strengthening-eu-resilience-council-adopts-negotiating-mandate-on-the-resilience-of-critical-entities (Letöltés: 2023.04.03.)

47 Az Európai Parlament és a Tanács 460/2004/EK rendelete az Európai Hálózat- és Információbiztonsági Ügynökség létrehozásáról (11).

az egyének, vállalkozások, közigazgatási szervek megfelelő tájékozottsága. Nemcsak a tagállamoknak nyújthat tanácsokat, hanem az Európai Parlament, a Bizottság, az európai szervek is részesülhetnek a segítségében. Tevékenységeivel elő kell segítenie a belső piac zavartalan működését, azzal, hogy kifejleszti a hálózat- és információbiztonság kulturáját. Szorgalmazza az együttműködést a Bizottság és a tagállamok között is, hogy megelőzzék a hálózat- és információbiztonsággal kapcsolatos problémákat, illetve azokra hatékonyan reagáljanak. Előmozdítja a kockázatértékelési tevékenységet (veszély meghatározása, a veszély jellemzése, a veszélyeztetettség mértékének felmérése és a kockázat jellemzése) és a megelőzés-kezelési megoldásokkal kapcsolatos kutatásokat a köz- és a magánszektorban működő szervezeteken belül. [48]

Az ENISA feladatkörének és céljainak teljesítése során nem sértheti a tagállamok hálózat- és információbiztonsággal kapcsolatos hatásköreit, illetve a közbiztonsággal, avédelemmel, a nemzetbiztonsággal kapcsolatos tevékenységeket sem.[49]

Az ENISA-t szervezetileg három rész alkotja: az igazgatóság, az ügyvezető igazgató, az érdekeltek állandó csoportja. Az igazgatóság a tagállamok egy-egy képviselőjéből, a Bizottság által kinevezett három képviselőből, a Tanács által kinevezett három képviselőből áll. Az igazgatóság fogadja el az ENISA belső működési szabályzatát, amit nyilvánosságra kell hozni. Az ügyvezető igazgató az ENISA vezetője, aki a feladatok ellátásában független. Az igazgatóság nevezi ki a Bizottság javaslata alapján, maximum öt évre. Az érdekeltek állandó csoportja az információ- és hírközléstechnológiai iparágat, a fogyasztói csoportokat és a hálózat- és információbiztonsággal foglalkozó tudományos szakértőket képviseli. A csoport tanácsokkal

48 Az Európai Parlament és a Tanács 460/2004/EK rendelete 3. cikk.
49 Az Európai Parlament és a Tanács 460/2004/EK rendelete 1. cikk (3).

láthatja el az ügyvezető igazgatót a meghatározott feladatainak ellátásához.[50]

Az ENISA létrehozása óta rengetek technológia változás, társadalmi-gazdasági folyamatok, piaci fejlemények történtek, melyek szükségessé tették a 2004-es rendelet átreformálását. AZ Európai Parlament és a Tanács 526/2013/EU rendeletének a célja, hogy megerősítsék az ENISA-t annak érdekében, hogy még nagyobb sikerrel járulhasson hozzá az uniós intézmények és a tagállamok olyan erőfeszítéseihez, amelyekkel európai kapacitást szándékoznak létrehozni a hálózat- és információbiztoság területén jelentkező kihívások kezelésre.[51] A 2013-as rendelet kiemeli, hogy a digitális gazdaság méretére való tekintettel, meg kell növelni az Ügynökség számára elkülönített pénzügyi és emberi erőforrásokat. Továbbra is tanácsokkal kell ellátnia a Bizottságot, a tagállamokat, a hivatalokat, az uniós intézményeket.

Az uniós hálózat- és információbiztonság magas szintjének biztosítása érdekében a számítógép-biztonsági és incidenskezelő csoportok (CSIRT) és a hálózatbiztonsági vészhelyzetekkel elhárító csoportok (CERT) közötti együttműködést ösztönöznie kell.[52]

Az ENISA-ról hozott két rendelet nem tudta hatékonyan felvenni a kibertámadásokkal való harcot, mert a megbízatása korlátozta. Felül kell vizsgálni az ENISA megbízatását a megváltozott kiberbiztonsági helyzetben, annak érdekében, hogy hatékonyabban tudjon hozzájárulni a kiberbiztonsági kihívásokra uniós szinten. Az Európai Parlament és a Tanács 2019/881 rendeletében egy még erősebb intézkedécsomagot fogadtak el

50 Az Európai Parlament és a Tanács 460/2004/EK rendelete 6–8. cikk.

51 Az Európai Parlament és a Tanács 526/2013/EU rendelete az Európai Uniós Hálózat és Információbiztonsági Ügynökségről (ENISA) és a 460/2004/EK rendelet hatályon kívül helyezéséről (11).

52 Az Európai Parlament és a Tanács 526/2013/EU (31).

az ENISA-ról. A 2019-es rendelet értelmében minden eddigi ENISA-ról hozott rendeletben meghatározott feladatát továbbra is el kell látnia. Az ENISA-nak segítenie kell az (EU) 2016/1148 irányelvben foglaltak megvalósítását. (NIS 1. irányelv).[53]

A reform keretében az ENISA a korábbi mandátumához képest állandó megbízást kapott, amely egyébként kiterjedt a szintén újításként megteremtett tanúsítási rendszerek kidolgozásában való közreműködésre is.[54]

Az ENISA-nak együtt kell működni a a különböző nemzetközi szervezetekkel, az OECD-vel, az EBESZ-szel és a NATO-val. Az együttműködés kiterjedhet közös kiberbiztonsági gyakorlatokra, illetve biztonsági eseményekre való reagálás közös koordinációjára is. Továbbá támogatnia kell a CSIRT-ek és a CERT-EU operatív együttműködését.[55]

Feladatkörét tekintve három területre lehet szétosztani. Elsősorban gyakorlati tanácsokkal és megoldásokkal szolgál, amely támogatja a tagállamokat a nemzeti kiberbiztonsági stratégiák kidolgozásában. Másrészt tanulmányokat és jelentéseket készít. Végül pedig közreműködik a hálózat- és információbiztonságra vonatkozó uniós szakpolitikák és jogszabályok megszövegezésében.[56]

Tevékenységét éves munkaprogramok határozzák meg. Az ENISA szoros együttműködésben áll az Európai Rendőrségi Hivatallal (EUROPOL) és a Számítástechnikai Bűnözés Elleni Európai Központtal is.[57]

---

53 Az Európai Parlament és a Tanács (EU) 2019/881 rendelete az ENISA-ról és az információs és kommunikációs technológiák kiberbiztonsági tanúsításáról, valamint az 526/2013/EU rendelet hatályon kívüli helyezéséről (16).

54 COM (2017) 477.

55 Az Európai Parlament és a Tanács (EU) 2019/881 rendelete.

56 Az Európai Parlament és a Tanács 2019/881 rendelete, https:// eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:32019R0881&from=EN (Letöltés: 2022.10.12.)

57 Az Európai Parlament és a Tanács 526/2013/EU rendelete (28).

A 2019-es rendelet átalakította az ENISA struktúráját. Az igazgatótanács, a felügyelőtestület, az ügyvezető igazgató, az ENISA tanácsadó csoportja és a nemzeti kapcsolattartó tisztviselők hálózata alkotja a szervezetét. Az igazgatótanács tagállamonként egy, a Bizottság által kijelölt két tagból áll. Feladatuk az ENISA működésének irányát meghatározni, elfogadni a költségvetést, felügyelni a működést. Az egyik újítás a 2013-as rendelethez képest a szervezeti felépítésben a felügyelőtestület bevezetése. A felügyelőtestület segíti az igazgatótanács munkáját, illetve elkészíti az igazgatótanács által elfogadandó határozatokat. A felügyelőtestület öt tagból áll. Az ügyvezető igazgató vezeti az ENISA-t. A másik új elem az ENISA tanácsadó csoportja. A csoport releváns érdekelt felekből (pl. IKT-ágazatot, nyilvánosan elérhető elektronikus hírközlési szolgáltatások nyújtóit, kiberbiztonság területén tevékenykedő tudományos szakembereket), képviselő elismert szakértőkből, illetékes hatóságokból, európai szabványügyi szervekből, bűnüldözői hatóságokból és adatvédelmi felügyeleti hatóságokból áll. Ahogy a nevéből is látszik feladata a tanácsadás az ENISA feladatainak ellátásával kapcsolatban. A harmadik új szervezeti elem a nemzeti kapcsolattartó tisztviselők hálózata, mely a tagállamok képviselőiből áll. Feladatuk, hogy megkönnyítsék az ENISA és a tagállamok közötti információcserét.[58]

4.2. Europol Számítástechnikai Bűnözés Elleni Központ (EC3)

Az Europol 1999. július 1-jén kezdte meg a működését, miután a tagállamok ratifikálták az Europol-egyezményt. 2010 januárjában az Europol új jogi kerettel és kiterjesztett feladatkörrel rendelkező, teljes jogú uniós ügynökséggé vált. (Európai Rendőr-

58 Az Európai Parlament és a Tanács (EU) 2019/881 rendelete az ENISA-ról 13–23. cikk.

ségi Hivatal (Europol) létrehozásáról szóló 2009. április 6-i, 2009/371/IB számú tanácsi határozat alkotta meg.)[59] Hivatalos ügynökséggé válása után az integráltabb együttműködés kialakítása volt a fő feladata.

Az Europol az Európai Unió bűnüldöző hatósága, melynek fő feladat az EU biztonságosabbá tétele. Feladatkörébe tartozik az EU-tagállamok hatóságainak támogatása, a kölcsönös információmegosztás a nemzeti rendőrségekkel és a bűnügyi adatok szakszerű elemzése. A nagy kiterjedésű bűnszervezetek és terrorista hálózatok fenyegetése miatt erősebb szabályozásokra volt szükség, ezért 2016 májusában hatályon kívül helyezték a 2009/371/IB tanácsi határozatot és új lépéseket kellett bevezetnie az Europolnak.[60]

2012 márciusában nyújtotta be az Európai Bizottság a javaslatát a számítástechnikai bűnözés elleni küzdelem európai központjának létrehozására (továbbiakban EC3), amely a Stockholmi Program egyik fontos eleme.[61] Az EC3-at Hágában az Európai Rendőrségi Hivatalon belül hozták létre, működését 2013. január 11-én kezdte. Céljaiban kitűzte, hogy egy kapcsolattartó pontként működjön a számítástechnikai bűnözés elleni küzdelemben, részt vegyen az unión belüli rendészeti koordinációban, operatív támogatással segítse a tagállami rendészeti szerveket a konkrét nyomozások során.

---

59 Tájékoztató az EUROPOL rendszerről, https://www.naih.hu/europol/tajekoztato-europol-rendszerrol (Letöltés: 2023.04.02.)

60 Az Európai Parlament és a Tanács (EU) 2016/794 rendelete a Bűnüldözési Együttműködés Európai Uniós Ügynökségéről (Europol), valamint a 2009/371/IB, a 2009/934/IB, a 2009/935/IB, a 2009/936/IB és a 2009/968/IB tanácsi határozat felváltásáról és hatályon kívül helyezéséről.

61 Az Európai Tanács tájékoztatása. A Stockholmi Program 2010. https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=LEGISSUM%3Ajl0034 (Letöltés: 2023.04.03.)

A számítástechnikai bűnözés három fő területére is kitér: 1. a szervezett bűnözői csoportok által elkövetett számítástechnikai bűncselekmények 2. olyan számítástechnikai bűncselekmények, amelyek súlyos kárt okoznak az áldozataiknak pl. gyermekek szexuális kizsákmányolása 3. olyan számítástechnikai bűncselekmények, melyek az Unión belüli kritikus infrastruktúrákat és információs rendszereket érintik.[62]

Az EC3-nak öt feladatkörét említeném: 1. Adatokat gyűjt a számítógépes bűnözésről: ezeket az adatokat feldolgozzák a tagállami nyomozó hatóságok részére. 2. Támogatja a közös nyomozócsoportok létrehozását a tagállamok számára, ezzel is koordinálva a tagállamok közötti együttműködést a számítógépes bűncselekmények nyomozásában. Az Eurojusttal és az Interpollal is szoros együttműködésben áll. 3. Elemzi a kibertérből érkező fenyegetéseket és ezekből igyekszik előrejelezni a számítógépes bűnözés alakulását. 4. CERT-ekkel kapcsolattartás a minél hatékonyabb fellépések érdekében 5. Szorosan együttműködik a tagállamok nyomozó hatóságaival és igazságügyi szervezeteivel.[63]

5. Közös biztonság és védelempolitika

Az Európai Unió közös biztonság és védelempolitikája (Common Security an Defence Policy, CSDP) elengedhetetlen szerepet tölt be a nemzetközösség együttes kül- és biztonságpolitikájában. A 2009-es lisszaboni szerződés vezette be a CSDP fogalmát és

62 Bizottság közleménye a Tanácsnak és az Európai Parlamentnek: Küzdelem digitális korunk bűnözésével: Számítástechnikai Bűnözés Elleni Európai Központ létrehozása 2012. 03. 28.

63 Gyaraki Réka: A nemzetközi intézmények szerepe a kiberbiztonságban, In: Török Bernát (szerk.) *Információ-és kiberbiztonság*, Budapest, 2020. 192–193. o.

létrehozta a kölcsönös védelmi záradékot (Treaty on European Union Article 42).[64]

A 2013. évi kiberbiztonsági stratégia (melyet a korábbi fejezetben kifejtettem). A stratégia releváns a közös biztonság és védelempolitika tekintetében is, ugyanis a belső biztonság kérdéseit a külső biztonság kihívásaival egyeztette össze, tehát az Európai Unió biztonságvédelmének két szintjét kapcsolta össze. [65]

2014-ben az Európai Tanács elfogadta az első kibervédelmi politikai keretrendszert. A keretrendszer kibervédelmi és nemzetközi kiberpolitikai célokat tűzött ki az EU tagállamai számára, mint például: a tagállamok CSDP-vel kapcsolatos kibervédelmi képességeinek fejlesztése, CSDP kommunikáció hálózatainak védelme, oktatási, továbbképzési lehetőségek fokozása, erősíteni a nemzetközi partnerekkel való együttműködést.[66]

Mivel a 2013. évi kiberbiztonsági stratégia nem hozta meg a kívánt eredményeket, ezért arra ösztönözte az Európai Uniót, hogy újabb erőfeszítéseket tegyen a védelem érdekében. 2017-ben el is fogadták az új kiberbiztonsági stratégiát. A CSDP szempontjából ez a stratégia a kiberbiztonsági elrettentés kiépítésére összpontosít a tagállamok védelmi képességeinek felhasználásával.

2017. évi stratégia alapján az EU közös kiberbiztonsági tanúsítási keretrendszerét (Cyber Defence Policy Framework) 2018-ban frissítették. Ezt a kiberképességek fejlesztése és a CSDP támogatása miatt kezdeményezték.

---

64 Kölcsönös védelmi záradék, https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=LEGISSUM:mutual_defence (Letöltés: 2023.03.12.)

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

66 Council Of the European Union: EU Cyber Defence Policy Framework (2014. november 18.).

Fontos leszögezni, hogy a CSDP kibervédelmének katonai koncepciója a tagállamok képességein és együttműködésén alapszik. A biztonság és védelem területén a tagállamok nemzeti érdekeket támasztanak.[67]

2020-ban jelent meg az EU új kiberbiztonsági stratégiája (EU kiberbiztonsági stratégiája a digitális étvizedre)[68]. Az új stratégia szerint a tagállamoknak növelniük kell a kiberfenyegetések megelőzésére és azokra való reagálás képességét. A kiberbiztonsági stratégiával összhangban a CDSP számára a következő stratégiai pontok váltak meghatározóvá: Az EU-nak tovább kell folytatnia a vonatkozó CSDP-struktúrák csatlakozását a NATO szövetségi missziói hálózatához, a CSDP katonai missziói és műveletei számára az EU katonai elképzelésének és stratégiájának kidolgozása a kibertérben, a polgári CSDP-paktum keretében a polgári CSDP-missziók hozzájárulhatnak az EU szélesebb körű munkájához a kiberbiztonsági kihívások leküzdésében.[69]

6. Kiberdiplomácia

6.1. Kiberdiplomácia meghatározása

A kiberdiplomáciának – ahogyan az a kibertér fogalmának esetére is igaz – nincsen pontos tudományos meghatározása. A kiberdiplomácia a kibertérben folytatott diplomáciaként definiálható,

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

68 European Commission: The EU's Cybersecurity Strategy for the Digital Decade.

69 Bihaly Barbara: A kibervédelem szerepe az Európai Unió közös biztonsági és védelmi politikájában, *Hadtudományi Szemle*, 2021/3. 52. o.

vagyis a diplomáciai erőforrások felhasználása, illetve a diplomáciai funkciók ellátása a kibertérben a kibertérrel kapcsolatos nemzeti érdekek biztosítása érdekében.[70] A kibertér számos olyan jellemzőt halmozott fel, amelyek az érdekelt felek közötti diplomáciai kötelezettségvállalást jelentik. Először is, ez egy globális terület, amely összeköti a világ országait/nemzeteit és polgárait, ahol különböző módokon kölcsönhatások és súrlódások keletkeznek közöttük. Egy ilyen nagy globális közös javaknak a mindenki számára való hozzáférés biztosítása és a konfliktusok elkerülése érdekében szükség van minimális szabályokra és előírásokra, amelyeket csak a diplomáciai tárgyalások eredményeként lehet létrehozni.[71]

6.2. Kiberdiplomácia megjelenése az Európai Unióban

2015-ben látott napvilágot az a dokumentum, amely először használta a kiberdiplomácia kifejezést az Európai Unióban. Ezen dokumentum célnak tűzte ki, hogy megvédi az emberi jogokat és biztosítja, hogy az internettel ne lehessen visszaélni , de továbbra is a szabad véleménynyilvánítás fóruma maradjon. Továbbá az uniós diplomácia és a jogi eszközök segítségével igyekszik megakadályozni a kiberbiztonsági fenyegetéseket és hozzájárul a nemzetközi kapcsolatok stabilitásának növekedéséhez.[72]

Az Európai Unión belüli szakpolitikák mélyülése megkövetelte, hogy a diplomáciai eszköztárat megerősítsék. A nagyobb védelem érdekében az Európai Unió Tanácsa 2017-ben

70 André Barrinha – Thomas Renard: Cyber-diplomacy: the making of an international society in the digital age, Global Affairs, 2017. 3:4–5, 353–364.

71 S. J. Buck: *The global commons: An introduction*, Washington DC, Island Press, 1998. 6. o.

72 Az Európai Unió Tanácsa, 2015. A Tanács következtetései a kiberdiplomáciáról.

megegyezett abban, hogy az Unió politikai, biztonsági és gazdasági érdekeinek széleskörű védelme érdekében kialakít egy közös uniós diplomáciai keretrendszert az állami és nem állami szereplők által végrehajtott rosszindulatú és szándékos kibertevékenységek ellen. Ez a megállapodás létrehozta a kiberdiplomáciai eszköztárat (EU Cyberdiplomacy Toolbox)[73] A Tanács azt szerette volna megvalósítani a Toolboxxal, hogy a közös uniós diplomáciai intézkedések keretében előmozdítsák a veszélyek csökkentését. Továbbá döntöttek arról is, hogy a kibertámadások körében alkalmazni fogják a közös kül-és biztonságpolitika területéhez tartozó intézkedéseket is, vagyis akár az esetleges szankciós intézkedéseket is. A szankcióknak a nemzetközi joggal összefüggésben arányosnak kell lenniük a kibertevékenység által okozott hatásokkal.[74]

A Politikai és Biztonsági Bizottság 2017 októberében végrehajtási iránymutatásokat fogadott el a kiberdiplomáciai eszköztárra vonatkozóan. Öt kategóriát sorol fel a dokumentum:

– megelőző intézkedések;
– együttműködési intézkedések;
– stabilitást szolgáló intézkedések;
– korlátozó intézkedések;
– lehetséges uniós támogatás a tagállamok jogszerű válaszaihoz.[75]

Az Európai Unió tagállamait fenyegető kibertámadásokkal szemben 2019-ben kiadták a KKBP-határozatot[76] és egy új

73 13007/17 – Implementing guidelines for the Framework on a Joint EU Diplomatic Response to Malicious Cyber Activities.

74 Council of the European Union (2017a): Draft implementing guidelines for the Framework on a Joint EU Diplomatic Response to Malicious Cyber Activities – approval of the final text, Brussels, 9 October 2017.

75 Agnes Kasper – Anna-Maria Osula – Anna Molnár: *EU cybersecurity and cyber diplomacy*, 2021. 8. o.

76 Tanács (KKBP) 2019/797. határozata.

tanácsi rendeletet.[77] Ezen dokumentumok a rossz szándékú és a szándékos kibertevékenységekkel szembeni közös uniós korlátozó intézkedések alkalmazhatóságának kérdéséről döntött és a kibertámadásokra válaszul adott szankciók alkalmazását teszik lehetővé. Ezzel a jogi aktussal tehát az Európai Uniónak lehetősége lett szankciókat kivetni (például utazási tilalom, bizonyos eszközök befagyasztása).[78] 2020. júliusában valósult meg először gyakorlatban a szankciók alkalmazása 6 személy és 3 szervezet ellen, akikről kiderült, hogy az uniós tagállamok elleni különböző kibertámadásokért felelősek.[79]

7. Összegzés

A 2000-es évek elején a digitalizáció és az IKT-eszközökkel kapcsolatos kérdésköröket az Európai Unió jogalkotói és döntéshozói csupán gazdasági oldalról közelítették meg. A 2013-as kiberbiztonsági stratégia mondható egy fontos állomásnak az EU kiberbiztonsági intézkedéseinek körében, ugyanis innentől kezdve álltak neki biztonságiasítani a kiberteret.

A Cyberdiplomacy Toolboxban foglalt korlátozó intézkedések aktiválása egy mérföldkővé vált az EU kibertérben folytatott rosszindulatú tevékenységekre való reagálás közös megközelítésének kialakításában. A szankciórendszer hasznos lehet a tagállamok közötti együttműködés fellendítésére is, ugyanis az ilyenfajta korlátozó intézkedések meghozatalára az Európai Unió Tanácsára van szükség. Az egyes államok ellenállóképes-

77 Tanács (EU) 2019/796 rendelete.

78 Kelemen Roland: III.2. Az Európai Unió szerepe a kibertér biztonsági aspektusaiban, In: Farkas Ádám – Kelemen Roland: *Nemzeti biztonság és kibertér,* Budapest, Médiatudományi Intézet, 2023. 134., 137–138. o.

79 Regulation EU 2020/1124 of 30 July 2020.

ségének javításában és ezzel előmozdítva a releváns uniós jogszabályoknak (például NIS-irányelv) való megfelelést is szolgálja. Természetesen nem teljesen kikövetkeztethető, hogy a szankciók 100%-ig beválnak és a jövőbeli kiberfenyegetéseket sikerül elrettenteni, de az EU mindenesetre megadta az eszközt, hogy sikeresebben lehessen kezelni ezeket a helyzeteket. A tanulmányban említett dokumentumok elemezve világossá válik az Európai Unió törekvése, egy olyan Európa létrehozása, amely ellenáll és megvédi az egyéneket, államokat a kibertérben előforduló támadások, fenyegetésekkel szemben. Olyan stratégiákat alakít ki, amely gyors reagálási képességet és erősebb védelmet alakít ki. A rendelkezések mind olyan intézkedéseket kívánnak létrehozni, amelyek összehangolják a tagállamokat, így tovább erősítve az Unió kiberbiztonságát. Az EU kiberbiztonsági szabályozásai biztonságosabb online környezetet biztosítanak mindenkinek, az internetes adatvédelem és a személyes adatok védelme érdekében. Az EU által hozott kiberbiztonsági szabályozások összességében azt mutatják, hogy az EU kiemelten fontosnak tartja a kiberbiztonság javítását és a kiberbiztonsági fenyegetések elleni küzdelmet, valamint a digitális gazdaság és társadalom védelmét. Az EU arra törekszik, hogy a kiberbiztonsági szabályozások folyamatosan fejlődjenek, és a jövőbeli kiberbiztonsági kihívásokra is hatékony válaszokat adjanak.