

37. Országos Tudományos Diákköri Konferencia
Had- és Rendészettudományi Szekció
Budapest, 2025. április 22–24.
Nemzeti Közszolgálati Egyetem
Hadtudományi és Honvédtisztképző Kar

Az Európai Unió kiberbiztonsági szabályozása evolúciójának másfél évtizede

Jelige: SZM268

Pályamunka lezárásának időpontja: 2023. április

2023.

Tartalom

I. Bevezetés	1
II. Alapfogalmak.....	3
2.1. Kibertér	3
2.2. Kibervédelem, kiberbiztonság, kiberbűnözés.....	4
III. Európai Unió és a kiberbiztonság	7
3.1 Az Európai Unió hatályos szabályozásainak előzményei	7
3.2. Kiberbiztonsági stratégiák	10
3.2.1. 2013-as kiberbiztonsági stratégia.....	10
3.2.2. 2017-es kiberbiztonsági stratégia.....	12
3.2.3. 2020-as kiberbiztonsági stratégia.....	15
3.2.4. Közös biztonság és védelempolitika	16
3.3. Szabályozások átalakulása 2010 után.....	17
3.3.1. NIS 1-irányelv.....	17
3.3.2. NIS 2-irányelv.....	18
3.3.3. DORA rendelet	21
3.3.4. CER irányelv.....	22
3.4. Intézmények.....	24
3.4.1. Európai Unió Hálózat- és Információbiztonsági Ügynökség.....	24
3.4.2. Europol Számítástechnikai Bűnözés Elleni Központ (EC3).....	27
3.5. Kiberdiplomácia	29
3.5.1. Kiberdiplomácia megjelenése az Európai Unióban.....	29
IV. Összegzés.....	32
V. Mellékletek.....	36
VI. Irodalomjegyzék.....	37

I. Bevezetés

Az elmúlt évszázad rengetek újítás hozott technikai forradalomnak köszönhetően az emberek életének mindennapjaiba. Manapság már elképzelhetetlennek tartanánk, azt, hogy ne létezenek számítógépek, amik a társadalom napjainak lényeges segédeszköze. Az emberek többségének a megszokás részévé vált az online térben dolgozni, kikapcsolódni és szociális életet élni. Az élet sokkal egyszerűbb lett digitális technológia elterjedésének köszönhetően. Vagy nem? A 21. század sok mindenben hozott újítást, könnyebbséget, azonban sok kihívással kell szembenéznie az embereknek, amik a biztonságukat fenyegetik: háborúk, járványok, terrorizmus, nemzetközi bűnözés, és a kibertérben elkövetett támadások. Ahogy az infrastruktúra, gépipar is fejlődik, úgy modernizálódnak a kibertérben elkövetett bűncselekmények is. Az újszerű kihívások és problémák minden ország/szervezet számára megkívánja védelmi stratégiájuknak megreformálását, illetve új alternatívák felmutatását. A kibertér tehát mára egyértelmű részévé vált nem csupán az ember magánéletének, hanem a gazdaságnak, a politikának, és a kultúrának is. Tehát a kibertér majdnem minden területen megjelenik és magában hordozza a túlságosan nagymértékű függőség kialakulását is, amely abban ölt testet, hogy a kibertér nyújtotta szolgáltatások hibája, vagy kiesése nem csak anyagi károk bekövetkezésével járhat, hanem közvetlenül is fenyegetheti az emberi életet. A kibertér biztonságának megteremtése azonban annak ellenére, hogy részben feltétlenül nemzeti feladat, már csak jellege miatt is elképzelhetetlen, hogy ne feltételezzon nemzetközi, vagy regionális együttműködési szinteket.

A kiberbiztonság megteremtése biztonságunk és jólétünk szempontjából egyaránt teljes fontossággal bír. A kibertérben elkövetett fenyegetések, bűncselekmények sokfélék lehetnek: A kibertérben bűnözők könnyedén el tudnak érni személyes adatokat, banki adataikat, vagy éppen cégek üzleti titkait. A kiberbűnözők adataikat lopják, hamisítják, vagy zsarolják az áldozatokat. Az adatlopások, az adathalászat, és a vírusok terjesztése az egész világra kiterjedő problémákat okozhat. Ezek a veszélyek csak néhány példa a kibertérre vonatkozóan, és azokat folyamatosan növelik az új technológiák fejlődésével és az online tevékenységek növekedésével. Azonban a megfelelő kibervédelmi intézkedések, a felhasználók és a vállalkozások kiberbiztonsági tudatosságának növelése segíthet a veszélyek elkerülésében és az online biztonság növelésében.

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.

II. Alapfogalmak

A kibertér, a kiberbiztonság és –védelem, a kibertámadás, valamint a kiberterrorizmus. Azok a kifejezések, amelyek a 21. században mindenki számára ismert fogalmakká váltak, anélkül, hogy azok valós, mélységi tartalmát ismernék. Életünk jelentős részét a kibertérben végzett cselekmények határozzák meg. A 2000-es évek eleje forradalmi változásokat hozott az emberiség történelmében: digitalizáció, okoseszközök, mesterséges intelligencia megjelenésével és egyre jelentősebb térhódításával. Joggal mondhatjuk, hogy a negyedik ipari forradalom időszakát éljük, ami magában hordozza a társadalom átalakulását is. Kérdéses, hogy a kibertér rohamosan fejlődő szintjeivel hogyan tud lépést tartani a társadalom, és főként a jogi szabályozás? Hogyan hat az egyénre, a gazdaságra és magára az államra? A továbbiakban ezeket a kérdéseket igyekszem megválaszolni, annak érdekében, hogy rámutassak arra, hogy a kibertér biztonsága és védelme a hálózati biztonságnál jóval összetettebb és mélyebb fogalmakat takar.

2.1. Kibertér

A kibertér fogalmának definiálására számos elmélet született, amely mind a saját tudományterületből kiindulva próbálja definiálni azt, legtöbbször figyelmen kívül hagyva annak multiszisztecinális jellegét. Ezt a NATO Kibervédelmi Kiválósági Központ jegyzéke is jól bemutatja, ugyanis több mint negyven kibertér definíció kerül benne értelmezésre, amely más-más szinteken elemzi a fogalmat. A hadtudományhoz kapcsolódóan Munk Sándor definíciója szerint: *„A kibertér napjainkban különböző alkalmazási területek, szakmai körök, sőt a mindennapi közbeszéd gyakran használt, népszerű kifejezése. A fejlett információtechnológia eredményeként kialakuló hálózatok egy olyan szolgáltatási, virtuális működési környezetté, sőt >>életkörnyezetté<< váltak, amelyek mindenki számára érzékelhető virtuális térként, világként megélhető környezetet alkotnak. Ebben a >>térben<< szereplők tevékenykednek, folyamatok zajlanak, események történnek, amelyek pozitív hatással, vagy negatív (káros, vagy akár pusztító erejű) következményekkel vannak a >>hagyományos<< világ szereplőinek életére, tevékenységére.”¹*

Fontos leszögezni, hogy a kibertér definiálásában nagy jelentőséggel bír az a tényező, hogy milyen megközelítésben, illetve ki határozza meg a fogalmat. A kibertér használatával kapcsolatban többféle felhasználói dimenziót kell szem előtt tartani: állami és nem állami

¹ MUNK Sándor: A kibertér fogalmának egyes, az egységes értelmezést biztosító kérdései. *Hadtudomány*, 2018/1. szám, 113-114. o.

szereplők, gazdasági szereplők, katonai szféra, magánszféra és közsféra. A különböző dimenziók szem előtt tartása azért fontos, hogy a kibertérben tevékenykedő szereplők sokszínűségét szemléltessék. Megkülönböztetünk aktív és passzív feleket a kibertérben. Aktív fél a kibertérben elkövetett támadásért felelős személy, míg a passzív fél az elszenvedője a támadásoknak.²

2.2. Kibervédelem, kiberbiztonság, kiberbűnözés

A kibertér fogalmához szorosan kapcsolódik a kiberbiztonság és a kibervédelem. Az Ibtv. meghatározása szerint a kiberbiztonság a következőképpen definiálható: „*a kibertérben létező kockázatok kezelésére alkalmazható politikai, jogi, gazdasági, oktatási és tudatosságnövelő, valamint technikai eszközök folyamatos és tervszerű alkalmazása, amelyek a kibertérben létező kockázatok elfogadható szintjét biztosítva a kiberteret megbízható környezetté alakítják a társadalmi és gazdasági folyamatok zavartalan működéséhez és működtetéséhez*”³

Ahogy a kibertér fogalmánál is többféle felhasználó található, a kiberbiztonság körét sem szabad kizárólagosan az állami és kormányzati rendszerekre szűkíteni, ugyanis a biztonságos használat igénye a kibertérben minden magánszereplő és gazdasági szereplő részéről fennáll. Az államok szerepe nyilvánvalóan erősebb, ugyanis szabályozó joghatósága és jelentős erőforrásai az állami szereplők és a nagy nemzetközi szervezetek kezében vannak. Például az Európai Unió és a NATO.⁴

A kibervédelem minden eszköz és tevékenység összessége, amelynek célja, hogy az infokommunikációs eszközöket, rendszereket, technológiákat megvédjék azoktól a támadásoktól, amik az adatok, illetve az információk bizalmasságát, sérthetlenségét és működőképességét veszélyeztetik. Többféle védelmi feladatot lehet megkülönböztetni, aszerint, hogy milyen kihívások, illetve fenyegetések érik a kiberteret: információvédelem, kiberbűnözés elleni védelem, katonai hálózatok védelme. Problémások azok az esetek, amikor a támadások, a kormányzati közigazgatási rendszerek ellen, irányulnak, amik az állami szereplők intézményeinek biztonságát és ezáltal a teljes társadalmat fenyegethetik. Ugyanis ezekben az esetekben az egyes államoknak kötelessége bizonyos válaszlépéseket tenni-védelmi elhárításokat bevezetni. Egyes államok döntéseiben eltérnek abban, hogy milyen mértékűnek határozzák meg a támadásokat és hogyan reagálnak rá. Ugyancsak probléma merül fel a

² GAZDAG Ferenc-REMEK Éva (2018): A biztonsági tanulmányok alapjai. In Hautzinger Zoltán (szerk.) *Studia Universitatis Communia*, Budapest, Dialóg Campus Kiadó, 127.o.

³ Ibtv. 1.§ (1) 26.

⁴ GAZDAG-REMEK (2018), 128. o.

felelősség kérdésében is. Sok esetben a nemzetközi szabályozások nem térnek ki arra, hogy az állami vagy nem állami szereplőkkel szemben, milyen módon lehet fellépni. Továbbá alapvető technológiai hiányosság, hogy a kibertérben elkövetett támadások nehezen visszakövethetők. Például a támadás egy emailben elküldött rosszindulatú fájlön keresztül valósul meg.⁵

Általános értelemben a kiberbűnözés olyan bűncselekmények elkövetését jelenti, amit interneten keresztül, számítógép segítségével követnek el. Az elkövető olyan károkat okoz, amelyek a fizikai világban testesülnek meg. Például: csalások, személyes adatokkal való visszaélés. Az emberek nem fordítanak elég figyelmet az internet használatából adódó veszélyekre. A felhasználók gyanútlanul használják a világháló által biztosított felületeket. Ahogy nő az internethasználók száma- úgy nőnek a személyazonossággal való visszaélések is. Az utóbbi években sok olyan kibertámadás történt, amelyek nemcsak egyéneket, hanem országokat is fenyegettek. Az ilyen jellegű támadások mára már képesek akár nukleáris üzemeket, légvédelmi rendszereket, elektromos hálózatokat is leállítani, így elengedhetlenné válik a nemzetbiztonsági kockázat körébe sorolása.

A számítógépes vírusok története egészen a szűkebb értelemben vett számítógépes hálózatok koráig nyúl vissza. Neumann János már az 1940-es években megjósolta lehetőségüket és potenciális veszélyüket, az első ilyen vírus megteremtésére azonban az 1970-es évekig várni kellett. Az internet korai létszakaszában – az ARPANET idején – jelent meg az első ilyen jellegű, fenyegetést egyelőre nem jelentő program, az ún. „Creeper vírus”, amely nem csinált mást, mint az egy hálózathoz kapcsolódó számítógépek között önmagát sokszorozítva terjedt és a képernyőn egy egyszerű üzenetként jelent meg amelyről nevét is kapta. A megjelenő üzenet „*I’m the creeper, catch me if you can!*” volt.⁶

Ahogy az számítógépek közötti kapcsolat mértéke nőtt, a vírusok is egyre bonyolultabbá és veszélyesebbé váltak, olyannyira, hogy a biztonsági rendszerek jelentős lépéshátrányba kerültek.

Az 1980-as években kezdődött el a kiberhadviselés kora, amikor az akkori Szovjetunió egy német hackert, Marcus Hess-t bízta meg az Egyesült Államok hadi titkainak megszerzésével,

⁵ GAZDAG-REMEK, 129-130. o.

⁶ The Creeper Worm, the First Computer Virus <https://www.historyofinformation.com/detail.php?entryid=2860> (Letöltés dátuma: 2023.02.02.)

amelynek során Hess több, mint 400 katonai számítógépet – köztük a Pentagonhoz tartozókat is – feltört, hogy a megszerzett információkat aztán továbbítsa.⁷

Az információbiztonság történetének egyik fordulópontját jelentette az 1988-as Morris vírus is, amely nevét megalkotójáról, Robert Morrisről kapta. A vírus gyors tempóban sokszorozódott az érintett rendszerekben, amelynek következtében azok, teljesen leálltak, vagy használhatatlanságig lassultak. Ezt számítják az első Denial-of-Service (DoS), azaz infrastruktúrát megbénító támadásnak.⁸

Amint egyre nagyobb tömegek számára vált elérhetővé az internet, az online felületekre feltöltött személyes adatok száma is egyre nőtt, ami magával hozta a szervezett bűnözés megjelenését is a kibertérben. A hálózatok biztonságát érintő fenyegetések exponenciális növekedése hívta életre a tűzfalak és egyéb vírusölő programok megalkotását és tömeggyártását.

A korai időszakban ezt a területet általában a vírusok és hackerek lépéselőnye jellemezte, amely a 2000-es évek elejével fordult meg. A nemzeti szabályozások körülbelül ekkorra lettek képesek valamelyest utolérni a probléma által szült kihívásokat, és az ilyen jellegű támadásokat egyre súlyosabb büntetésekkel (hosszúidős szabadságvesztés, magas összegű pénzbüntetések).

Az előbbi tendencia azonban mégsem volt képes meggátolni az elmúlt évtized és egyben a kibertér történetének legnagyobb bűncselekményeit, amelyek meghatározó jelleggel hatottak a kiberbiztonság egészére.

2013-ban az egykori CIA alkalmazott, Edward Snowden olyan titkosított NSA (Az Egyesült Államok Nemzetbiztonsági Ügynöksége) dokumentumokat hozott nyilvánosságra, amelyek fényében egyértelművé vált, hogy a kormányzatok világszerte megfigyelik az embereket, például a telefonhívások, valamint az online kapcsolattartás terén.⁹

⁷ Tim MATTHEWS: A Brief History of Cybersecurity, Cyberinsiders, 2019. <https://www.cybersecurity-insiders.com/a-brief-history-of-cybersecurity/> (Letöltés dátuma: 2023.02.06.)

⁸ Caleb TOWNSEND: A Brief and Incomplete History of Cybersecurity, *United States Cybersecurity Magazine*, <https://www.uscybersecurity.net/history/> (Letöltés dátuma: 2023.02.06.)

⁹ Dakota MURPHEY: A history of information security, *IFSEC GLOBAL*, <https://www.ifsecglobal.com/cyber-security/a-history-of-information-security/> (Letöltés dátuma: 2023.02.06.)

A történelem legnagyobb kaliberű, legtöbb felhasználót érintő támadása a 2013-14-es „*Yahoo! data breach*” volt, amely a Yahoo – egyébként csak utólagosan tett – nyilatkozata alapján 3 milliárd felhasználói fiókot és az azokhoz kapcsolódó adatot veszélyeztetett.¹⁰

Érdemes megemlíteni továbbá a „*WannaCry*” néven 2017-ben felbukkant zsarolóvírust, amely a megfertőzött számítógépeken zárolta az ott tárolt fájlokat és az újbóli hozzáférést pénzügyi megfizetéséhez kötötte. A vírus több 99 országban, 28 nyelven jelent meg és összesen több mint 230 ezer számítógépet érintett. Jelentőségét növelte, hogy az érintett rendszerek között olyan szervezetek számítógépes hálózatai is szerepeltek, mint az angol és skót National Health Service kórházai, és az ott található MRI szkenner, valamint vértároló hűtőberendezések. Az Europol beszámolójában úgy fogalmazott, hogy ilyen jellegű és mértékű támadás eddig precedens nélküli volt az Európai Közösség történelmében.¹¹

III. Európai Unió és a kiberbiztonság

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. A kibertámadások és a kiberbűncselekmények Európa szerte egyre gyakoribbakká váltak. Nem csak a gazdaság, de a társadalom is kiberfenyegetéseknek lett kitéve.

Ebben a fejezetben megvizsgálom és bemutatom az Európai Unió kiberbiztonsággal kapcsolatos intézkedéseit, az előzményektől kezdve, kiberbiztonsági stratégiákon, irányelveken, rendeleteken át. Megvizsgálom a NIS 1, NIS 2 irányelvet, a DORA rendeletet, illetve a CER irányelvet is. Kitérek azokra az intézményekre is, melyek a kiberreziliencia megteremtésében nagy szerepet játszanak (ENISA, Europol) Igyekezem egy átfogó és komplex képet bemutatni az Európai Unió erőteljes kiberbiztonsági intézkedésiből.

3.1 Az Európai Unió hatályos szabályozásainak előzményei

Az első kiberbiztonság terén hozott irányelv 1995-ben született a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról¹².

¹⁰ Robert MCMILLAN-Ryan KNUTSON: Yahoo Triples Estimate of Breached Accounts to 3 Billion, Wall Street Journal, 2017. <https://www.wsj.com/articles/yahoo-triples-estimate-of-breached-accounts-to-3-billion-1507062804> (Letöltés dátuma: 2023.01.25.)

¹¹ BBC: Cyber-attack: Europol says it was unprecedented in scale, 2017. <https://www.bbc.com/news/world-europe-39907965> (Letöltés dátuma: 2023.01.25.)

¹² Directive 95/46 EC of the European Parliament and of the Council

Ezt követte a Budapesti Konvenció¹³, amely ugyan nem kifejezetten az Európai Unióhoz köthető – tekintve, hogy az Európa Tanács égisze alatt került elfogadásra – mégis fontos forrása a nemzetközi büntetőpolitika kiberbűnözéssel kapcsolatos területének.

A 2000-es évek elején irányelvek sokasága foglalkozott az információs infrastruktúravédelem területével, amelyek közül a legfontosabbak: a Tanács 2002/C 43/02 közös álláspontról és a különleges intézkedésekről a hálózati és az információbiztonság területén¹⁴, az Európai Parlament és a Tanács 2002/21 EK keretirányelv (Framework Directive) az elektronikus hírközlő hálózatok és elektronikus hírközlési szolgáltatások közös keretszabályozásáról¹⁵, az Európai Parlament és a Tanács 2002/58 EK irányelv az elektronikus hírközlési ágazatban a személyes adatok kezeléséről, feldolgozásáról és a magánélet védelméről¹⁶, a Tanács 2003/C48/01 számú határozata a hálózati és az információbiztonság-kultúra európai megközelítéséről¹⁷.

A kibertér védelmének kialakítására való törekedés Uniós szinten egyébként más, általánosabb jellegű dokumentumokban is megjelent, ezek közül jelentős az Európai Bizottság által 2004-ben kiadott a terrorizmus elleni védelem körében a létfontosságú infrastruktúra védelméről szóló javaslat¹⁸, amelyet a Bizottság a Tanács felkérésére készített el. Ennek kiemelt jelentősége abban áll, hogy későbbi programok egész sora tekintetében szolgált alapul.

2005-ben kiadták az Európai Bizottság Zöld Könyvét, ami 11 szektorra és 37 termékre osztotta fel Európa kritikus infrastruktúráit. A Zöld Könyv alapján lefolytatott tárgyalásokat követően a Miniszterek Tanácsa elé 2006 decemberében irányelv-javaslatot terjesztettek.¹⁹

¹³ The Budapest Convention (ETS No. 185) and its Protocols

<https://www.coe.int/en/web/cybercrime/the-budapest-convention> (Letöltés dátuma: 2023.01.28.)

¹⁴ Council resolution of 28 January 2002 on a common approach and specific actions in the area of network and information security,

[https://eur-lex.europa.eu/legalcontent/EN/TXT/PDF/?uri=CELEX:32002G0216\(02\)&from=EN](https://eur-lex.europa.eu/legalcontent/EN/TXT/PDF/?uri=CELEX:32002G0216(02)&from=EN)

(Letöltés dátuma: 2023.01.28.)

¹⁵ Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services, <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32002L0021&from=en> (2023.01.29.)

¹⁶ Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32002L0058&from=EN> (2023.01.29.)

¹⁷ Council Resolution of 18 February 2003 on a European approach towards a culture of network and information security,

<https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:C:2003:048:FULL&from=HU> (2023.01.29.)

¹⁸ Communication from the Commission to the Council and the European Parliament of 20 October 2004 – Critical Infrastructure Protection in the fight against terrorism, <https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=LEGISSUM:l33259> (Letöltés dátuma: 2023.01.29.)

¹⁹ Prof. Dr. KOVÁCS László mk. ezredes, 38.o.

Az európai unió kiberbiztonság két pillérének általában a Hálózati és Információbiztonsági Direktívát, valamint a Kritikus Információs Infrastruktúra-Védelmet tartják.²⁰ Ezek kialakulása azonban hosszú folyamat eredménye volt, melynek első lépése az Európai Hálózat- és Információbiztonsági Ügynökség (European Network and Information Security Agency – ENISA) 2004-es létrehozása (majd mandátumának 2008-as meghosszabbítása) volt.²¹

A kibertámadások kivédését és megszakítását célzó 2009-es akciótervben a Bizottság öt pillért fogalmazott meg: felkészültség és prevenció; felismerés és reagálás; kárenyhítés és helyreállítás; nemzetközi együttműködés; az információs és kommunikációs technológia szektorában kidolgozni a kritikus infrastruktúra kritériumrendszerét²²

Ezt követően folyamatosan került sor a tagállamok közötti adatvédelmi együttműködés elmélyítésére, amelynek során egy sor újabb dokumentum került elfogadásra. Ezek körében említhetők az internet szabályozásáról szóló Bizottsági közlemény²³, Tanácsi állásfoglalás a hálózat- és információbiztonság együttműködésre építő európai megközelítésről²⁴, továbbá az Európai Parlament és a Tanács 2009/140EK²⁵ irányelve, amely három különböző, de a kiberbiztonság területéhez tartozó dokumentum módosításáról rendelkezett.

2010-ben megjelent az Európai Digitális Menetrend²⁶, ami az Európa 2020 Stratégia részét képezi. Sor került továbbá az ENISA modernizációjára²⁷ is.

²⁰ FEKETE-KARYDIS Klára-LÁZÁR Bence: A Kibervédelmi Stratégiák Fejlődése. Kibervédelmi Kihívások, Aktualitások, *Honvédségi Szemle*, 2019/4.

²¹ FEKETE-KARYDIS. 41. o.

²² Communication from the Commission to the European Parliament, The Council, The European Economic and Social Committee and the Committee of Regions on Critical Information Infrastructure Protection, <https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0149:FIN:EN:PDF> (Letöltés dátuma: 2023.02.01.)

²³ Communication from the Commission to the European Parliament and the Council - Internet governance <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52009DC0277> (Letöltés dátuma: 2023.02.01.)

²⁴ Council Resolution of 18 December 2009 on a Collaborative European Approach to Network and Information Security(2009/C321/01)

<https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:C:2009:321:FULL&from=EN> (Letöltés dátuma: 2023.02.01.)

²⁵ Az Európai Parlament és a Tanács 2009/140/EK irányelve <https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0037:0069:HU:PDF> (Letöltés dátuma: 2023.02.02.)

²⁶ Európai Bizottság: Az európai digitális menetrend <https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0245:FIN:HU:PDF> (Letöltés dátuma: 2023.02.01.)

²⁷ Az Európai Tanács és Európai Parlament Rendelete az Európai Hálózat- és Információbiztonsági Ügynökségről <https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:52010PC0521&from%20=EN>, (Letöltés dátuma: 2023.02.01.)

Az évtized elején az európai kiberbiztonsági szabályozás gyermekvédelmi dimenzióval is bővült, amikor az Európai Bizottság elfogadta a gyermekek biztonságosabb internethasználatát elősegítő európai stratégiáját.²⁸

Nagy jelentőséggel bírt az Európai Parlament 2012-ben elfogadott ajánlása a kiberbiztonságról és védelemről. Főbb programpontjai: saját nemzeti kiberbiztonsági- és védelmi stratégiák kialakítása, saját nemzeti kibervédelmi veszélyhelyzeti tervek és válságkezeléshez szükséges képességek létrehozása, kiberbiztonság fenntartásához szükséges jogszabályok beépítése a nemzeti jogrendekbe, továbbá a kutatásfejlesztési tevékenységet tegyék alappillérré a kiberbiztonság megteremtése céljából.²⁹

3.2. Kiberbiztonsági stratégiák

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. A következőkben tehát a 2013-as, a 2017-es és a 2020-as stratégiának a főbb pontjait mutatom be.

3.2.1. 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.³⁰ 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

²⁸ A Bizottság közleménye az Európai Parlamentnek, a Tanácsnak <https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:52012DC0196&from=EN> (Letöltés dátuma: 2023.02.01.)

²⁹ GAZDAG-REMEK, 134. o.

³⁰ BIHALY Barbara: A kibervédelem szerepe az Európai Unió közös biztonsági és védelmi politikájában *Hadtudományi szemle*, 2021/14. évf. 3. szám, 49. o.

hozzanak létre, amik szükségesek a kiberbiztonság megteremtéséhez, végül uniós szintű koherens nemzetközi kiberpolitika kialakítása.³¹

A stratégia három nagy területen tartja szükségesnek az intézkedések meghozatalát. A nemzeti szinten, ahol az állami és 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.³²

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 élel 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 felelősség³³

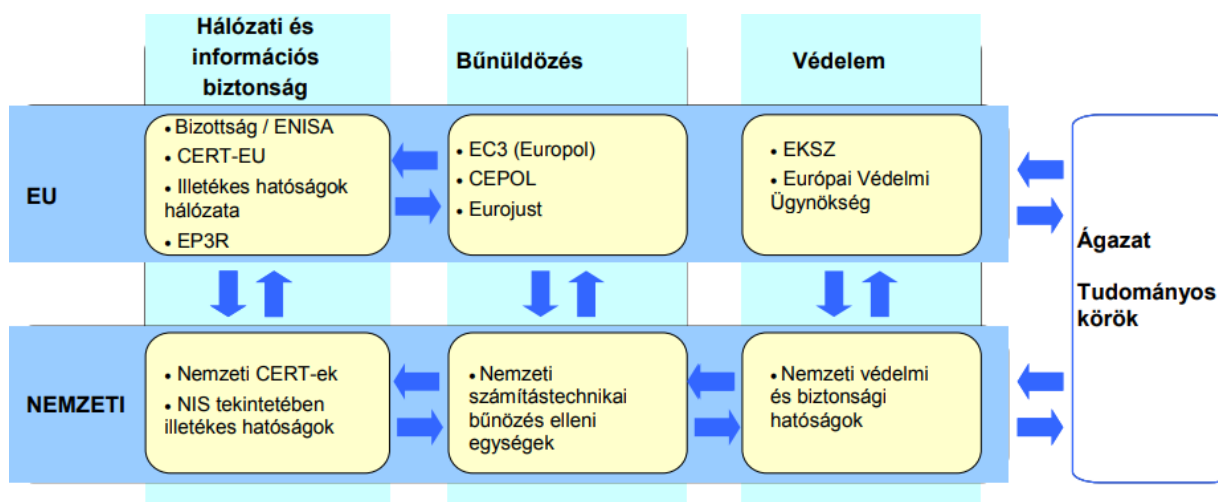
Szerepkörét tekintve már a dokumentum megalkotásakor is egyértelmű volt, hogy a kérdés összetettsége és az érintettek sokfélesége miatt központi felügyeleti rendszer kialakítására nem lesz lehetőség. Így a kibertámadások megelőzése és kivédésének rendszere alapvetően nemzeti szinten kell, hogy működjön, ami aztán adott esetben az uniós szintű beavatkozás által kerülhet kisegítésre. Ennek három fő pillére a NIS, a bűnüldözés és a védelem területe lesz.³⁴

³¹ GAZDAG-REMEK (2018) 134. o.

³² KOVÁCS (2018) 88. o.

³³ 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 dátuma: 2023.02.11.)

³⁴ Az Európai Unió kiberbiztonsági stratégiája (2013) 20. o.



1. ábra: Az Európai Unió 2013-as stratégiájának szerepkörei és felelősségekerei
(Forrás: Az Európai Unió kiberbiztonsági stratégiája (2013))

3.2.2. 2017-es kiberbiztonsági stratégia

Az Európai Bizottság és a tagállamok döntéshozói számár 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.³⁵

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 stratégiában is aktuálisak, viszont nagyobb és több erőre van szükség ahhoz, hogy az egyre súlyosodó fenyegetésekkel szembe lehessen nézni.

A 2017-es stratégia felhívja a figyelmet arra, hogy a kibertámadásokkal szembeni ellenállóképesség eléréséhez, illetve a stratégiai függetlenség kiépítéséhez egy olyan erős és

³⁵ Európai Bizottság: Közös közlemény az Európai Parlamentnek és a Tanácsnak: Ellenálló képesség, elrettentés, védelem: az Unió erőteljes kiberbiztonságának kiépítése 2017.09.13. 2.o.

egysége piac, nagyobb uniós technológiai fejlesztések és képzett szakemberek kellenek, amellyel egy átfogóbb és a szakpolitikákon átívelő megközelítést ér el.³⁶

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 fokozná, hogy éves összeurópai kiberbiztonsági gyakorlatokat szerveznek. Továbbá az ENISA-nak támogatnia kell az információs és kommunikációs technológiák (IKT) uniós szakpolitikáinak kidolgozását.³⁷

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 orvostechikai eszközök tanúsítására használhatná.³⁸

A rendszer szabályok, műszaki követelmények, szabványok és eljárások formájában valósul meg, ami csökkenti a piac széttagozottságát, felszámolja a szabályozási akadályokat és – amennyiben a tagállamok ténylegesen alkalmazzák őket – megkönnyíti 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.³⁹

A termékek, szolgáltatások és folyamatok jelentette kiberbiztonsági veszélyek alapján a tanúsítvány három megbízhatósági szintet – alap”, „jelentős”, valamint „magas” – különböztet meg. Ezek alapján határolható be, hogy rendeltetésszerű használatuk mekkora valószínűséggel,

³⁶ Közös közlemény az Európai Parlamentnek és a tanácsnak, Ellenálló képesség, elrettentés, védelem: az Unió erőteljes kiberbiztonságának kiépítése 3.o.

³⁷ Közös közlemény az Európai Parlamentnek és a tanácsnak 2017.

³⁸ 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 dátuma: 2022.10.12.)

³⁹ Az Európai Parlament és a Tanács (EU) 2019/881 rendelete az ENISA-ról (48)

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.⁴⁰

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 a jogokon alapuló kapacitásépítési modellt fogja előmozdítani, a digitálisan a fejlődésért megközelítésnek megfelelően.⁴¹

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.

⁴⁰ Az Európai Parlament és a Tanács (EU) 2019/881 rendelete az ENISA-ról (84)

⁴¹ Közös Közlemény az Európai Parlamentnek és a Tanácsnak 2017.

3.2.3. 2020-as kiberbiztonsági stratégia

2020 év végén az Európai Uniónak új kiberbiztonsági stratégiája lett Az EU kiberbiztonsági stratégiája a digitális évtizedre címmel.⁴²

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 a hálózati és információs rendszerek.⁴³ 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 stratégiában nagy szerepet kap a globális gondolkodás és az európai cselekvés, ennek elérése érdekében szükséges egy globális és nyílt internetet. Ezt úgy kívánja biztosítani, hogy 1. megteremtse a rezilienciát, a technológiai szuverenitást, 2. az operatív kapacitásépítést a megelőzés, elrettentés és reagálás érdekében, és 3. előmozdítja a globális nyílt kibertérrel.⁴⁴

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.⁴⁵

A stratégia értelmében fokozni kell valamennyi érintett gazdaság és a társadalom szempontjából fontos feladatot ellátó ágazat kiberrezilienciáját.

⁴² European Commission: The EU's Cybersecurity Strategy for the Digital Decade (2020. december 16.).

⁴³ Közös közlemény az Európai Parlamentnek és a Tanácsnak: Az EU kiberbiztonsági stratégiája a digitális évtizedre, 1.o.

⁴⁴ Közös közlemény az Európai Parlamentnek és a Tanácsnak: Az EU kiberbiztonsági stratégiája a digitális évtizedre, 5.o.

⁴⁵ Digital Europe: <https://culture.ec.europa.eu/hu/node/1179> (Letöltés dátuma: 2023.03.28.)

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.⁴⁶ 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.⁴⁷

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.

3.2.4. Közös biztonság és védelempolitika

Az Európai Unió közös biztonság és védelempolitikája (Common Security and Defence Policy, CSDP) elengedhetetlen szerepet tölt be a nemzetközösség együttes kül és biztonságpolitikájában.

A 2009-es lisszaboni szerződés vezette be a CSDP fogalmát és létrehozta a kölcsönös védelmi záradékot (Treaty on European Union Article 42).⁴⁸

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 egyeztetette össze, tehát az Európai Unió biztonságvédelmének két szintjét kapcsolta össze.⁴⁹

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

⁴⁶ Közös közlemény az Európai Parlamentnek és a Tanácsnak: Az EU kiberbiztonsági stratégiája a digitális évtizedre 8.o.

⁴⁷ Közös közlemény az Európai Parlamentnek és a Tanácsnak: Az EU kiberbiztonsági stratégiája a digitális évtizedre 7.o.

⁴⁸ Kölcsönös védelmi záradék: https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=LEGISSUM:mutual_defence (Letöltés dátuma: 2023.03.12.)

⁴⁹ RAMSES A. Wessel: Towards EU Cybersecurity Law. Regulating a New Policy Field. In Nicholas Tsagourias – Russell Buchan (szerk.): *Research Handbook on International Law and Cyberspace*. H. n., Edward Elgar Publishing, 2015. 403–426.

fejlesztése, CSDP kommunikáció hálózatainak védelme, oktatási, továbbképzési lehetőségek fokozása, erősíteni a nemzetközi partnerekkel való együttműködést.⁵⁰

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.

Fontos leszögezni, hogy a CSDP kibervédelmének katonai koncepciója a tagállamok képességein és együttműködésén alapszik. A biztonság és védelem területén a tagállamok nemzeti érdekeket támasztanak.⁵¹

2020-ban jelent meg az EU új kiberbiztonsági stratégiája (EU kiberbiztonsági stratégiája a digitális étvizedre)⁵². 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 hálózatahoz, 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.⁵³

3.3. Szabályozások átalakulása 2010 után

3.3.1. 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.

⁵⁰ Council Of the European Union: EU Cyber Defence Policy Framework (2014. november 18.)

⁵¹O . MOSKALENKO-V. STRELTSOV: Shaping a 'hybrid' CFSP to face 'hybrid' security challenges. *European Foreign Affairs Review* 22. (2017), 4. 513–532 o.

⁵² European Commission: The EU's Cybersecurity Strategy for the Digital Decade

⁵³ BIHALY Barbara: A kibervédelem szerepe az Európai Unió közös biztonsági és védelmi politikájában. *Hadtudományi Szemle*, 2021/14. évf. 3. szám, 52. o.

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.⁵⁴ 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.⁵⁵

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.⁵⁶

Kiépítésére került egy olyan együttműködési csoport is, amely a tagállamok, a Bizottság és az ENISA (Európai Unió Hálózat- és Információbiztonsági Ügynökség) képviselőiből állt. Feladata az államok közötti stratégiai együttműködés, az információcsere támogatása, illetve a hálózati és információs rendszerek biztonságának megteremtése.⁵⁷

3.3.2. 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

⁵⁴ 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 dátuma: 2023.02.11.)

⁵⁵ Európai Parlament és a Tanács 2016/1148 irányelve 7. cikk (1)

⁵⁶ Európai Parlament és a Tanács 2016/1148 irányelve 11. cikk, 12. cikk

⁵⁷ Európai Parlament és a Tanács 2016/1148 irányelve 11. cikk

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 információmegosztást is. Ez a fejlődés a kiberfenyegetettség bővüléséhez vezetett, új kihívások támasztásával, amelyek minden tagállamban kiigazított, összehangolt és innovatív reagálást igényelnek.”⁵⁸

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.⁵⁹

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.⁶⁰

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

⁵⁸ Az Európai Parlament és a Tanács 2022/2555 irányelve

⁵⁹ Az Európai Parlament és a Tanács 2022/2555 irányelve 1. 2. melléklet

⁶⁰ dr. DOMOKOS Márton-dr. BERTÓK Gábor-dr. HUSZÁR Daniella: NIS 2 – az EU új kiberbiztonsági irányelve <https://www.jogiforum.hu/hir/2023/01/03/nis2-az-eu-uj-kiberbiztonsagi-iranyelve/> (Letöltés dátuma: 2023.03.14.)

nagyméretű szervezetre, amelyek szolgáltatásokat nyújtanak.⁶¹ 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.⁶²

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), értesíteniük kell a CSIRT-jüket vagy az illetékes hatóságot.⁶³ 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.⁶⁴ 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 szolgálják.⁶⁵

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.⁶⁶ A közigazgatási szervekre való

⁶¹ 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 dátuma: 2023.03.14.)

⁶² dr. DOMOKOS Márton-dr. BERTÓK Gábor-dr. HUSZÁR Daniella: NIS 2 – az EU új kiberbiztonsági irányelve <https://www.jogiforum.hu/hir/2023/01/03/nis2-az-eu-uj-kiberbiztonsagi-iranyelve/> (Letöltés dátuma: 2023.03.14.)

⁶³ Az Európai Parlament és a Tanács 2022/2555 irányelve 21. cikk (1)

⁶⁴ Az Európai Parlament és a Tanács 2022/2555 irányelve 14. cikk III. fejezet

⁶⁵ Az Európai Parlament és a Tanács 2022/2555 irányelve 16. cikk (1)

⁶⁶ Az Európai Parlament és a Tanács 2022/2555 irányelve (8)

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 sérülékenységszint 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 online piacterek, az online keresőprogramok és a közösségimédia-szolgáltatási platformok szolgáltatói nyilvántartása⁶⁷

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.

3.3.3. 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.⁶⁸ 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 szolgáltatások.⁶⁹) A szervezeteknek rendelkezniük kell egy ellenálló képességgel, illetve egy helyreállító képességgel az IKT-incidensek kezelése végett.

⁶⁷ Az Európai Parlament és a Tanács 2022/2555 irányelve 6. cikk (34)

⁶⁸ SZÖLLŐSI Zoltán: DORA (Digital Operational Resilience Act) rendet tesz a pénzügyi kibertérben <https://www2.deloitte.com/hu/hu/pages/kockazat/articles/dora.html> (Letöltés dátuma: 2023.03.27.)

⁶⁹ Az Európai Parlament és a Tanács 2022/2554 rendelete 63.szakasz

A DORA a kiberbiztonsági előírásokat öt fő területen szabályozza.⁷⁰

1. IKT kockázatkezelés
2. IKT-val kapcsolatos események kezelése, osztályozása, jelentése
3. Digitális működési reziliencia tesztelése
4. Harmadik féltől eredő IKT kockázat kezelése
5. 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.⁷¹

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 fontos funkciókat támogató IKT-szolgáltatások esetén a pénzügyi szervezeteknek kilépési stratégiát kell bevezetniük.⁷²

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.⁷³

3.3.4. 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

⁷⁰ Az Európai Parlament és a Tanács 2022/2554 rendelete 1. cikk (1) (a)

⁷¹ Az Európai Parlament és a Tanács 2022/2554 rendelete 24. cikk (1-6)

⁷² Az Európai Parlament és a Tanács 2022/2554 rendelete 28. cikk (8)

⁷³ Az Európai Parlament és a Tanács 2022/2554 rendelete 45. cikk

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, Covid19 -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.⁷⁴

Az irányelv kilenc ágazatot sorol fel, amelyeket kritikus fontosságú szervként jelöl meg: közlekedés, energia, egészségügy, ivóvíz, szennyvíz, digitális infrastruktúra, úragazat, banki szolgáltatások, pénzügyi piaci infrastruktúrák.⁷⁵ 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.⁷⁶

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.⁷⁷

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.⁷⁸

⁷⁴ 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/>

⁷⁵ Az Európai Parlament és a Tanács (EU) 2022/2557 irányelve a kritikus szervezetek rezilienciájáról (5)

⁷⁶ Az Európai Parlament és a Tanács (EU) 2022/2557 irányelve a kritikus szervezetek rezilienciájáról III. fejezet 12. cikk (1)

⁷⁷ Az Európai Parlament és a Tanács (EU) 2022/2557 irányelve a kritikus szervezetek rezilienciájáról 18. cikk (1)

⁷⁸ Az Európai Parlament és a Tanács (EU) 2022/2557 irányelve a kritikus szervezetek rezilienciájáról 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.⁷⁹

3.4. Intézmények

3.4.1. Európai Unió 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).⁸⁰

Alapfeladatai között megjelenik a tagállamoknak való tanácsadás a tudatosság növelése érdekében, ugyanis a hálózati és információs rendszerek iránti bizalom biztosítása miatt szükséges 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.⁸¹

⁷⁹ 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 dátuma: 2023.04.03.)

⁸⁰ Az Európai Parlament és a Tanács 460/2004/EK rendelete az Európai Hálózat- és Információbiztonsági Ügynökség létrehozásáról (11)

⁸¹ Az Európai Parlament és a Tanács 460/2004/EK rendelete 3. cikk

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.⁸²

Az ENISA-t szervezetiileg 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 láthatja el az ügyvezető igazgatót a meghatározott feladatainak ellátásához.⁸³

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 erőfeszítéseikhez, amelyekkel európai kapacitást szándékoznak létrehozni a hálózat- és információbiztoság területén jelentkező kihívások kezelésére.⁸⁴ 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.⁸⁵

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

⁸² Az Európai Parlament és a Tanács 460/2004/EK rendelete 1. cikk (3)

⁸³ Az Európai Parlament és a Tanács 460/2004/EK rendelete 6-8. cikk

⁸⁴ Az Európai Parlament és a Tanács 526/2013/EU rendelete az Európai Unió Hálózat és Információbiztonsági Ügynökségről (ENISA) és a 460/2004/EK rendelet hatályon kívül helyezéséről. (11)

⁸⁵ Az Európai Parlament és a Tanács 526/2013/EU (31)

2019/881 rendeletében egy még erősebb intézkedéscsomagot fogadtak el 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)⁸⁶

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.⁸⁷

Az ENISA-nak együtt kell működni 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.⁸⁸

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.⁸⁹

Tevékenységét éves munkaprogramok határozzák meg. Az ENISA szoros együttműködésben áll az Európai Rendőrségi Hivatallal (EUROPOL) és a Számítástechnikai Bűnözés Elleni Európai Központtal is.⁹⁰

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

⁸⁶ 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)

⁸⁷ COM (2017) 477.

⁸⁸ Az Európai Parlament és a Tanács (EU) 2019/881 rendelete

⁸⁹ 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 dátuma: 2022.10.12.)

⁹⁰ Az Európai Parlament és a Tanács 526/2013/EU rendelete (28)

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.⁹¹

3.4.2. Europol Számítástechnikai Bűnözés Elleni Központ (EC3)

Az Europol 1999. július 1-én 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 Rendőrségi Hivatal (Europol) létrehozásáról szóló 2009. április 6.-i, 2009/371/IB számú tanácsi határozat alkotta meg.)⁹² Hivatalos ügynökséggé válása után az integráltabb együttműködés kialakítása volt a fő feladata.

Az Europol az Európai Unió bűnüldöző hatósága, melynek fő feladata az EU biztonságosabbá tétele. Feladatkörébe tartozik az EU-tagállamok hatóságainak támogatása, a kölcsönös információmegosztás a nemzeti rendőrségekkel és a bűnügyi adatok szakszerű elemzése. Továbbá segíti a tagállamok közös nyomozó csoportjait (Joint investigation teams), ahol a speciális eszközrendszer és információ segítségével még hatékonyabb bűntényfeltárást alkot meg.⁹³ Olyan bűncselekmények ellen segíti az EU tagállamok munkáját mint például a terrorizmus, embercsempészet, emberkereskedelem, pénzmosás, iparjogvédelmi jog megsértése, tiltott kábítószer-kereskedelem.⁹⁴

Az Europol munkatársai között megtalálhatók a rendőrség tagjai, határőrség, csendőrség, biztonsági szolgálat, vám- és pénzügyőrség. Fontos, hogy a tisztviselők nem rendelkezhetnek elletartóztatást közvetlenül. Csupán megfigyelő és elemző tevékenységben játszanak szerepet.⁹⁵

⁹¹ Az Európai Parlament és a Tanács (EU) 2019/881 rendelete az ENISA-ról 13-23. cikk

⁹² Tájékoztató az EUROPOL rendszerről <https://www.naih.hu/europol/tajekoztato-europol-rendszerrol> (Letöltés dátuma: 2023.04.02.)

⁹³ <https://www.eurojust.europa.eu/judicial-cooperation/instruments/joint-investigation-teams> (Letöltés dátuma: 2023.04.05.)

⁹⁴ Europol: Crime Areas&Trends <https://www.europol.europa.eu/crime-areas> (Letöltés dátuma: 2023.04.05.)

⁹⁵ Europol: Careers&Procurement <https://www.europol.europa.eu/careers-procurement> (Letöltés dátuma: 2023.04.27.)

Technikailag nagyon fejlett intézményről van szó, mely hatékonyan és megbízhatóan működik. Folyamatosan fejlesztik és biztonságos-számítástechnikai infrastruktúrával szerelik fel. Sokkal egyszerűbbé teszik az operatív és stratégiai információk tárolását, elemzését, illetve a tagállamokkal való megosztását is. 3 részből áll:

1. SIENA⁹⁶, ami egy biztonságos információcserét lehetővé tevő hálózati alkalmazás
2. EIS⁹⁷, ami az Europol Információs Rendszer
3. EPE⁹⁸, ami az Europol szakértői platformja

Az Europol alapvető tevékenységéhez tartozik az operatív és stratégiai elemzések, melyeket a legmodernebb módszertanok alapján visznek véghez és segítséget nyújtanak a tagállamok nyomozásaiban. 3 féle elemzési formát különböztethetünk meg:

1. OC-SCAN⁹⁹ fenyegetéséről szóló értesítések: korai előrejelzések a szervezett bűnözés általi új fenyegetettségekkel szemben.
2. TE-SAT¹⁰⁰, ami az EU aktuális terrorhelyzetéről ad tájékoztatást
3. EU SOCTA¹⁰¹, ami a súlyos és a szervezett bűnözésre vonatkozó EU-s fenyegetésértékelést mutatja be

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.¹⁰²

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.¹⁰³ Az EC3-at Hágában az Európai Rendőrségi Hivatalon belül

⁹⁶ Europol: Secure Information Exchange Network Application (SIENA) <https://www.europol.europa.eu/operations-services-and-innovation/services-support/information-exchange/secure-information-exchange-network-application-siena> (Letöltés dátuma: 2023.04.05.)

⁹⁷ Europol: Europol Information System <https://www.europol.europa.eu/operations-services-and-innovation/services-support/information-exchange/europol-information-system> (Letöltés dátuma: 2023.04.05.)

⁹⁸ Europol: Europol Platform for Experts <https://www.europol.europa.eu/operations-services-and-innovation/services-support/information-exchange/europol-platform-for-experts> (Letöltés dátuma: 2023.04.05.)

⁹⁹ Europol: OC-SCAN Threat Notice <https://www.europol.europa.eu/publications-events/publications/oc-scan-threat-notice-europol-launches-scan-system-for-strategic-notice> (Letöltés dátuma: 2023.05.10.)

¹⁰⁰ Europol: EU Terrorism Situation & Trend Report <https://www.europol.europa.eu/publications-events/main-reports/tesat-report> (Letöltés dátuma: 2023.05.10.)

¹⁰¹ Europol: Serious and Organised Crime Threat Assessment <https://www.europol.europa.eu/publications-events/main-reports/socta-report> (Letöltés dátuma: 2023.05.10.)

¹⁰² Az Európai Parlament és a Tanács (EU) 2016/794 rendelete a Bűnüldözési Együttműködés Európai Unió's 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

¹⁰³ Az Európai Tanács tájékoztatása. A Stockholmi Program 2010. <https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=LEGISSUM%3Ajl0034> (Letöltés dátuma: 2023.04.03.)

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.

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.¹⁰⁴

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.¹⁰⁵

3.5. Kiberdiplomácia

3.5.1. Kiberdiplomácia megjelenése az Európai Unióban

A kiberdiplomácia, ahogyan az a kibertér fogalmának esetére is igaz, nincsen pontos tudományos meghatározása. A kiberdiplomácia a kibertérben folytatott diplomáciaként definiálható, vagyis a diplomáciai erőforrások felhasználása, illetve a diplomáciai funkciók ellátása a kibertérben a kibertérrel kapcsolatos nemzeti érdekek biztosítása érdekében.¹⁰⁶ A kibertér számos olyan jellemzőt halmazott 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 sűrűlódások keletkeznek közöttük. Egy ilyen nagy globális közös javaknak a mindenki számára való hozzáférés biztosítása és a konfliktusok elkerülése érdekében szükség van minimális

¹⁰⁴ Bizottság közleménye a Tanácsnak és az Európai Parlamentnek: Küzdelem digitális korunk bűnözésével: Számítástechnikai Bűnözés Elleni Európai Központ létrehozása 2012.03.28.

¹⁰⁵ GYARAKI Réka: A nemzetközi intézmények szerepe a kiberbiztonságban. In: Török Bernát (szerk.) *Információ- és kiberbiztonság*, Budapest, 2020, 192-193.o.

¹⁰⁶ André BARRINHA-Thomas RENARD (2017) Cyber-diplomacy: the making of an international society in the digital age, *Global Affairs*, 3:4-5, 353-364,

szabályokra és előírásokra, amelyeket csak a diplomáciai tárgyalások eredményeként lehet létrehozni.¹⁰⁷

2015-ben látott napvilágot az a dokumentum, amely először használta a kiberdiplomácia kifejezést az Európai Unióban. Ezen dokumentum céljaként 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.¹⁰⁸

Az Európai Unió belüli szakpolitikák mélyülése megkövetelte, hogy a diplomáciai eszköztárat megerősítsék. A nagyobb védelem érdekében az Európai Unió Tanácsa 2017-ben 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)¹⁰⁹ A Tanács azt szeretne volna megvalósítani a Toolboxsal, 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.¹¹⁰

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

1. Megelőző intézkedések
2. Együttműködési intézkedések
3. Stabilitást szolgáló intézkedések
4. Korlátozó intézkedések
5. Lehetséges uniós támogatás a tagállamok jogszerű válaszához.¹¹¹

¹⁰⁷ BUCK, S. J. (1998). The global commons: An introduction. Washington, DC: *Island Press*, 6. o.

¹⁰⁸ Az Európai Unió Tanácsa, 2015, A Tanács következtetései a kiberdiplomáciáról

¹⁰⁹ 13007/17 – Implementing guidelines for the Framework on a Joint EU Diplomatic Response to Malicious Cyber Activities

¹¹⁰ 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

¹¹¹ 2021, Agnes KASPER-Anna-Maria OSULA-Anna MOLNÁR- EU cybersecurity and cyber diplomacy, 8. o.

Az Európai Unió tagállamait fenyegető kibertámadásokkal szemben 2019-ben kiadták a KKBP-határozatot¹¹² és egy új tanácsi rendeletet.¹¹³ 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)

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.¹¹⁴

¹¹² Tanács (KKBP) 2019/797 határozata.

¹¹³ Tanács (EU) 2019/796 rendelete.

¹¹⁴ Regulation EU 2020/1124 of 30 July 2020

IV. Összegzés

Az utóbbi évtizedekben az internet és a hálózat szerepe óriásit nöött a társadalom életében. A mindig több és több információ megszerzése értékke vált, így az információszolgáltatás a legfőbb területe lett a mindennapjainknak. A legtöbb tevékenység elvégzése lehetetlen lenne a számítógépes-technikai eszközök nélkül. A kibertér sokkal összetettebb jelenség annál, hogy csupán egyoldalúan, informatikai szempontból közelítsük meg. A dolgozat első része alapján láthatóvá vált, hogy az egyéni tudatosság a megfelelő biztonság megteremtése céljából elengedhetetlen. A rohamosan fejlődő világban a digitális eszközök kényelmet, de egyben kiszolgáltatottságot is teremtenek. A kiberbiztonság multidiszciplináris szempontú megközelítése által azonban a káros következmények csökkenthetők vagy kiiktathatók.

A számítógépes rendszereknek a megbízható működése és biztonsága a gazdaság, a társadalom és az állam szempontjából óriási jelentőséggel bír. Az elmúlt időszakokban azonban ez a biztonság megingott, rengeteg információs rendszereket érintő/veszélyeztető események történtek, melyek újabb kihívások elé állították akár az Európai Uniót, akár a tagállamokat.

A fogalmi tisztázások terén elmondható, hogy nincsenek egységesen kimondott definíciók a kibertér, kiberbiztonság, kibervédelem, kiberterrorizmus terminusokra. Különböző államok különböző értelmezéssel elemzik az egyes fogalmakat, melyek nemzetközi szinten értelmezési problémákhoz vezethetnek. Tehát a kiberbiztonság területén a fogalmi keretek tisztázása a legnehezebb feladat nemzetközi szinten.

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 kibernetikai biztonság előmozdításán, a kibertérben előforduló támadások, illetve a kiberterrorizmus elleni küzdelemben, illetve a kibertudományok fejlesztésében.

Számos irányelv, rendelet, stratégia került megalkotásra az Európai Unió által az elmúlt húsz évben. Ezek közül is kiemelném az Európai Parlament és a Tanács (EU) 2019/881 rendeletét az ENISA-ról, a NIS 1, NIS 2, CER irányelvet és a DORA rendeletet. Ezeket a dokumentumokat elemezve világossá válik az Európai Unió törekvése, miszerint, egy olyan Európa létrehozása, amely ellenáll és megvédi az egyéneket, államokat a kibertérben előforduló támadások, fenyegetésekkel szemben. Olyan stratégiákat alakít ki, amely gyors reakálási képességet és erősebb védelmet alakít ki. A rendelkezések mind olyan intézkedéseket kívánnak létrehozni, amelyek összehangolják a tagállamokat, így tovább erősítve az Unió kiberbiztonságát.

A 2013-as kiberbiztonsági stratégia az akkori időszakban az Európai Unióban tapasztalható kiberfenyegetésekre és kockázatokra összpontosított. A stratégia célja az európai kiberbiztonság erősítése és a digitális gazdaság és társadalom biztonságának javítása volt. A stratégia öt fő prioritást határoz meg: 1. Kibervédelem: Az EU az egyes tagállamokkal együttműködve létrehozta a Kibervédelmi Ügynökséget, amelynek feladata a kiberbiztonság terén tapasztalható fenyegetések és kockázatok értékelése, valamint a tagállamok és az EU intézményeinek segítése a kibertámadások elleni védekezésben. 2. Biztonságos e-kereskedelem: Az EU javította az elektronikus kereskedelmi infrastruktúrák biztonságát, és a fogyasztók jogainak védelmét szolgáló jogszabályokat hozott létre az elektronikus tranzakciókra vonatkozóan. 3. Nemzetközi együttműködés: Az EU erősítette nemzetközi kapcsolatait a kiberbiztonság terén, beleértve a nemzetközi szervezetekkel, más országokkal és az iparral való együttműködést is. 4. Kibertér gyakorlati kérdései: Az EU kiemelt figyelmet fordított a kiberbiztonsági gyakorlati kérdéseire, például a kiberbiztonsági oktatásra, a kiberbiztonsági szakértők képzésére, valamint a kibertámadások megelőzésére és kezelésére szolgáló technológiák fejlesztésére. 5. Kiberbiztonsági ipar: Az EU segítette az európai kiberbiztonsági ipar fejlődését és versenyképességét, beleértve az innovációt és a kutatást is.

A 2017-es kiberbiztonsági stratégia négy fő területre tér ki: 1. Erős és innovatív európai kiberbiztonsági ipar: A stratégia célja az európai kiberbiztonsági ipar erősítése, az innováció támogatása, valamint az európai vállalkozások versenyképességének növelése. 2. Biztonságos európai kiberteret létrehozása: Ez a prioritás az EU digitális környezetének biztonságának javítására irányul. Magában foglalja az új jogszabályok kidolgozását, a kiberbiztonsági tudatosság növelését és a nemzetközi együttműködés erősítését. 3. Hatékony eszközök kialakítása a kiberbűnözés elleni küzdelemre: A stratégia célja a hatékony kiberbűnözés elleni küzdelem és a szervezett bűnözés megelőzése, valamint a hatékony büntetőeljárások kidolgozása. 4. Az EU globális szerepvállalása a kiberbiztonság terén: Ez a prioritás az EU globális kiberbiztonsági szerepvállalására összpontosít, amely magában foglalja a nemzetközi szabványok kidolgozásához és a nemzetközi partnerségek megerősítéséhez való hozzájárulást.

A 2020-es kiberbiztonsági stratégia négy fő pilléren alapszik: 1. Ellenállóképesség: A régió ellenálló képességének javítására összpontosít a kiberbiztonsági fenyegetésekkel szemben. Magába foglalja a kockázatkezelés és a felkészültség előmozdítását, valamint a káresetekre való reagáló és helyreállító képesség kifejlesztését. 2. Megfigyelés és védelem: Ez a pillér az EU képességeinek erősítésére irányul, hogy megelőzzék, megfigyeljék és válaszoljanak a kibertámadásokra. Tartalmazza a kiberfenyegetésekkel kapcsolatos közös

kiberfenyegetésekkel kapcsolatos közös megértés kialakítását, az együttműködés javítását a tagállamok között, valamint az EU védelmi képességeinek javítását. 3. Kiberbiztonsági kapacitások és készségek fejlesztése: Ez a pillér a régió kiberbiztonsági készségeinek és kapacitásainak fejlesztésére törekszik. Magába foglalja az oktatás, a képzés és a tanúsítási programok előmozdítását annak érdekében, hogy az EU rendelkezzen egy magasan képzett és képes kiberbiztonsági munkaerővel. 4. Globális és nyitott internet előmozdítása: A globális kiberbiztonsági szabványok és legjobb gyakorlatok elterjedésének elősegítésére összpontosít. Magában foglalja az egy nyitott, átlátható és globális internet előmozdítását, miközben biztosítja, hogy tiszteletben tartsák az alapvető jogokat és értékeket.

A NIS1 és NIS 2 irányelv az Európai Unió kiberbiztonsági jogszabályainak kulcsfontosságú elemei. A NIS 1 irányelvet 2016-ban fogadták el, míg a NIS 2 irányelvet 2021-ben. Az irányelvek célja a kritikus infrastruktúrák és szolgáltatások védelme a kibertámadások ellen. A NIS 1 irányelv hatálya kiterjed a kritikus infrastruktúrákra és szolgáltatásokra, például az energia- és vízellátó rendszerekre, közlekedési infrastruktúrákra, pénzügyi szolgáltatásokra és egészségügyi rendszerekre. A NIS 2 irányelv tovább bővíti a NIS 1 hatályát, és a digitális szolgáltatásokra is kiterjed. Mind a NIS 1, mind a NIS 2 irányelv előírja, hogy az érintett szervezeteknek biztonsági intézkedéseket kell hozniuk, valamint hogy együtt kell működniük az illetékes hatóságokkal, hogy hatékonyan védekezzenek a kibertámadások ellen.

A Digital Operational Resilience Act (DORA) az Európai Bizottság által 2021-ben javasolt uniós jogszabály, amelynek célja a digitális szolgáltatások és infrastruktúrák operatív ellenállóképességének biztosítása, valamint a kibertámadásokkal és más digitális fenyegetésekkel szembeni védelem javítása. Számos szektorra kiterjed, beleértve a pénzügyi szektort, a digitális szolgáltatásokat, az e-kereskedelmet, az online piactereket, a felhőalapú szolgáltatásokat és az internetes közösségi média platformokat.

A Critical Entities Resilience Directive (CER) előírja, hogy a tagállamoknak javítaniuk kell az infrastruktúrák ellenállóságát és megelőzni a kritikus infrastruktúrák meghibásodását vagy bármilyen támadását. A tagállamoknak meg kell határozniuk a kritikus infrastruktúrák és szolgáltatások listáját, és védelmi intézkedéseket kell kidolgozniuk a kritikus rendszerek biztonságának fenntartására

Az ENISA (Európai Unió Hálózat- és Információbiztonsági Ügynökség) és az EC3 (Europol Kiberbűnözési Központja) fontos szerepet játszanak az Európai Unió kiberbiztonságának erősítésében. Bár az ENISA és az EC3 különböző szervezetek, az Európai Unió kiberbiztonsági

stratégiájának megfelelően szorosan együttműködnek, hogy elősegítsék a kiberbiztonsági fenyegetések kezelését és csökkentsék a kiberbűnözést. Az ENISA feladatai közé tartozik az Európai Unió hálózat- és információbiztonságának javítása, a kiberbiztonsági fenyegetések elemzése és az Európai Unió tagállamainak támogatása a kiberbiztonsági rendszerek fejlesztése és a biztonsági kultúra fejlesztése terén. Az EC3 a kiberbűnözés elleni küzdelemre összpontosít, és feladatai közé tartozik a kiberbűnözők azonosítása és üldözése, valamint a kiberbiztonsági fenyegetésekkel kapcsolatos információk és adatok gyűjtése, elemzése és megosztása az Európai Unió tagállamaival és más nemzetközi partnerekkel.

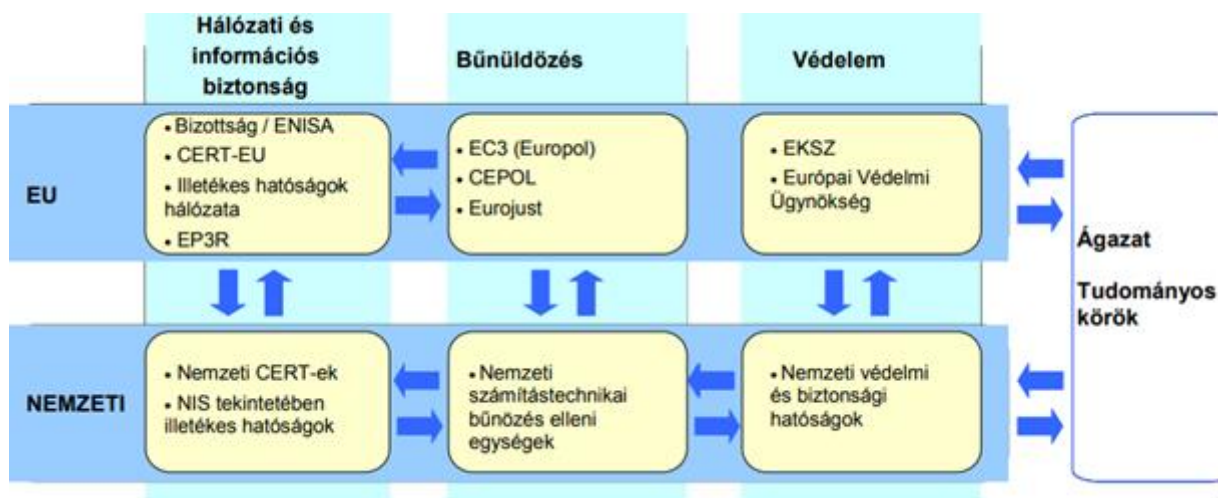
A kiberbiztonsági szabályozások betartása nem csak az európai szervezetek és állami szervek számára fontos, hanem az egyének számára is, akik folyamatosan kapcsolatban állnak az internettel és a digitális világgal.

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 ellenállóképességének 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 sikerebben 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 reakálási 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.

V. Mellékletek

1. ábra: Az Európai Unió 2013-as stratégiájának szerepkörei és felelősségkörei



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 dátuma: 2023.02.11.]

VI. Irodalomjegyzék

Összefoglaló kötetek:

1. GAZDAG Ferenc-REMEK Éva (2018): *A biztonsági tanulmányok alapjai*. In Hautzinger Zoltán (szerk.) *Studia Universitatis Communia*, Budapest, Dialóg Campus Kiadó 125-137. o.
2. GYARAKI Réka (2020): A nemzetközi intézmények szerepe a kiberbiztonságban. In: Török Bernát (szerk.) *Információ-és kiberbiztonság*, Budapest, 192-193.o.
3. KOVÁCS László (2018): *Kiberbiztonság és –stratégia*, Budapest, Dialog Campus Kiadó, 15-95. o.
4. MOSKALENKO-V. STRELTSOV (2017): *Shaping a 'hybrid' CFSP to face 'hybrid' security challenges*. *European Foreign Affairs Review* 22., 4. 513–532 o.
5. Ramses A. WESSEL (2015): *Towards EU Cybersecurity Law. Regulating a New Policy Field*. In Nicholas Tsagourias – Russell Buchan (szerk.): *Research Handbook on International Law and Cyberspace*. H. n., Edward Elgar Publishing, 403–426
6. TÁLAS Péter (2006): *A terrorizmus anatómiája*. Budapest, Zrínyi Kiadó, 5-42.o.

Tanulmányok, folyóiratok, cikkek:

1. 2021, Agnes KASPER-Anna-Maria OSULA-Anna MOLNÁR- EU cybersecurity and cyber diplomacy, 8. o.
2. André BARRINHA-Thomas RENARD (2017) Cyber-diplomacy: the making of an international society in the digital age. In: *Global Affairs*, 3:4-5, 353-364. o.
3. BIHALY Barbara: A kibervédelem szerepe az Európai Unió közös biztonsági és védelmi politikájában. In: *Hadtudományi szemle* 14. évfolyam, 2021/ 3. szám, 49. o
4. BUCK, S. J. (1998). The global commons: An introduction. Washington, DC. In: *Island Press*, 6. o.
5. FEKETE-KARYDIS Klára-LÁZÁR Bence: A Kibervédelmi Stratégiák Fejlődése, Kibervédelmi Kihívások, Aktualitások. In: *Honvédségi Szemle*, 2019/4.szám
6. KELEMEN Roland: Cyberfare state-Egy hibrid állammodell 21. századi születése. In: *Military and and Intelligence Cybersecurity Research Paper*, 2022/1. szám
7. MUNK Sándor: A kibertér fogalmának egyes, az egységes értelmezést biztosító kérdései. In: *Hadtudomány*, 2018/1.szám, 113-114. o.

Jogi szabályozások:

1. 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 dátuma: 2022.10.12.]
2. 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 dátuma: 2022.10.11.]
3. Az Európai Parlament és a Tanács (EU) 2016/794 rendelete a Bűnüldözési Együttműködés Európai Unió 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
<https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:32016R0794&from=HU>
[Letöltés dátuma: 2023.03.27.]
4. 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
<https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:32019R0881&qid=1680858329461&from=EN>
[Letöltés dátuma: 2023.03.20.]
5. Az Európai Parlament és a Tanács (EU) 2022/2557 irányelve a kritikus szervezetek rezilienciájáról
6. Az Európai Parlament és a Tanács 2013/40/EU irányelve 2013.
<https://eur-lex.europa.eu/legalcontent/HU/TXT/HTML/?uri=CELEX:32013L0040&from=EN>
[Letöltés dátuma: 2022.10.04.]

7. 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 dátuma: 2022.10.12.]
8. Az Európai Parlament és a Tanács 2022/2555 irányelve
9. Az Európai Parlament és a Tanács 460/2004/EK rendelete az Európai Hálózat- és Információbiztonsági Ügynökség létrehozásáról
<https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:32004R0460&from=HU>
[Letöltés dátuma: 2023.03.20.]
10. Az Európai Parlament és Tanács 2009/140/EK irányelve
<https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0037:0069:HU:PDF>
[Letöltés dátuma: 2022.10.08.]
11. Az Európai Tanács és Európai Parlament Rendelete az Európai Hálózat- és Információbiztonsági Ügynökségről
<https://eurlex.europa.eu/legalcontent/HU/TXT/HTML/?uri=CELEX:52010PC0521&from%20=EN>,
[Letöltés dátuma: 2022.10.10.]
12. Az Európai Tanács tájékoztatása. A Stockholmi Program 2010.
<https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=LEGISSUM%3Ajl0034>
[Letöltés dátuma: 2023.04.03.]
13. Bizottság közleménye a Tanácsnak és az Európai Parlamentnek: Küzdelem digitális korunk bűnözésével: Számítástechnikai Bűnözés Elleni Európai Központ létrehozása 2012.03.28.
<https://eur-lex.europa.eu/HU/legal-content/summary/european-cybercrime-centre-at-europol.html>
[Letöltés dátuma: 2023.01.28.]
14. COM (2017) 477
15. Communication from the Commission to the Council and the European Parliament of 20 October 2004 – Critical Infrastructure Protection in the fight against terrorism
<https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=LEGISSUM:133259>
[Letöltés dátuma: 2022.10.10.]

16. Communication from the Commission to the European Parliament and the Council - Internet governance
<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52009DC0277>
[Letöltés dátuma: 2022.10.08.]
17. Communication from the Commission to the European Parliament, The Council, The European Economic and Social Committee and the Committee of Regions on Critical Information Infrastructure Protection
<https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0149:FIN:EN:PDF>
[Letöltés dátuma: 2022.10.08.]
18. Council Of the European Union: EU Cyber Defence Policy Framework (2014. november 18.)
19. Council Resolution of 18 December 2009 on a Collaborative European Approach to Network and Information Security (2009/C 321/01)
<https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:C:2009:321:FULL&from=EN> [Letöltés dátuma: 2022.10.11.]
20. Council Resolution of 18 February 2003 on a European approach towards a culture of network and information security
<https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:C:2003:048:FULL&from=HU> [Letöltés dátuma: 2022.10.10.]
21. Council resolution of 28 January 2002 on a common approach and specific actions in the area of network and information security
[https://eurlex.europa.eu/legalcontent/EN/TXT/PDF/?uri=CELEX:32002G0216\(02\)&from=EN](https://eurlex.europa.eu/legalcontent/EN/TXT/PDF/?uri=CELEX:32002G0216(02)&from=EN) [Letöltés dátuma: 2022.10.10.]
22. Council resolution of 28 January 2002 on a common approach and specific actions in the area of network and information security,
[https://eur-lex.europa.eu/legalcontent/EN/TXT/PDF/?uri=CELEX:32002G0216\(02\)&from=EN](https://eur-lex.europa.eu/legalcontent/EN/TXT/PDF/?uri=CELEX:32002G0216(02)&from=EN)
[Letöltés dátuma: 2023.01.28.]
23. Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services, <https://eur-lex.europa.eu/legal->

- [content/EN/TXT/PDF/?uri=CELEX:32002L0021&from=en](https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32002L0021&from=en) [Letöltés dátuma: 2022.10.11.]
24. Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector,
<https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32002L0058&from=EN> [Letöltés dátuma: 2022.10.10.]
25. Directive 95/46 EC of the European Parliament and of the Council
26. Európai Bizottság: Közös közlemény az Európai Parlamentnek és a tanácsnak.
Ellenálló képesség, elrettentés, védelem: az Unió erőteljes kiberbiztonságának kiépítése
2017.09.13
27. 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 dátuma: 2022.10.11.]
28. European Commission: The EU's Cybersecurity Strategy for the Digital Decade (2020. december 16.).
29. European Commission: The EU's Cybersecurity Strategy for the Digital Decade (2020. december 16.).
30. General Secretariat of the Council: 13007/17 – Implementing guidelines for the Framework on a Joint EU Diplomatic Response to Malicious Cyber Activities
31. Ibtv. 1.§ (1) 26.
32. Kölcsönös védelmi záradék
https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=LEGISSUM:mutual_defence
[Letöltés dátuma: 2023.03.12.]
33. Közös közlemény az Európai Parlamentnek és a Tanácsnak: Az EU kiberbiztonsági stratégiája a digitális évtizedre
34. Regulation EU 2020/1124 of 30 July 2020
<https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:32020R1124>
[Letöltés dátuma: 2024.03.14.]

35. Tanács (EU) 2019/796 rendelete.
<https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:32019R0796&from=EN>
[Letöltés dátuma: 2024.03.14.]
36. Tanács (KKBP) 2019/797 határozata
<https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:32019D0797>
[Letöltés dátuma: 2024.03.14.]
37. The Budapest Convention (ETS No. 185) and its Protocols
<https://www.coe.int/en/web/cybercrime/the-budapest-convention>
[Letöltés dátuma: 2023.01.28.]

Internetes források:

1. 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 dátuma: 2023.04.03.]
2. Caleb TOWNSEND: A Brief and Incomplete History of Cybersecurity, *United States Cybersecurity Magazine*
<https://www.uscybersecurity.net/history/>
[Letöltés dátuma: 2023.02.06.]
3. Dakota MURPHEY: A history of information security, *IFSEC GLOBAL*,
<https://www.ifsecglobal.com/cyber-security/a-history-of-information-security/>
[Letöltés dátuma: 2023.02.06.]
4. dr. DOMOKOS Márton-dr. BERTÓK Gábor-dr. HUSZÁR Daniella: NIS 2 – az EU új kiberbiztonsági irányelve
<https://www.jogiforum.hu/hir/2023/01/03/nis2-az-eu-uj-kiberbiztonsagi-iranyelve/>
[Letöltés dátuma: 2023.03.14.]
5. 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 dátuma: 2023.03.14.]

6. Eurojust: Joint investigation teams
<https://www.eurojust.europa.eu/judicial-cooperation/instruments/joint-investigation-teams> [Letöltés dátuma: 2023.04.05.]
7. Europol: Careers&Procurement
<https://www.europol.europa.eu/careers-procurement>
8. Europol: Crime Areas&Trends
<https://www.europol.europa.eu/crime-areas>
[Letöltés dátuma: 2023.04.05.]
9. Europol: EU Terrorism Situation & Trend Riport
<https://www.europol.europa.eu/publications-events/main-reports/tesat-report>
[Letöltés dátuma: 2023.05.10.]
10. Europol: Europol Information System
<https://www.europol.europa.eu/operations-services-and-innovation/services-support/information-exchange/europol-information-system>
[Letöltés dátuma: 2023.04.05.]
11. Europol: Europol Platform for Experts
<https://www.europol.europa.eu/operations-services-and-innovation/services-support/information-exchange/europol-platform-for-experts>
[Letöltés dátuma: 2023.04.05.]
12. Europol: OC-SCAN Threat Notice
<https://www.europol.europa.eu/publications-events/publications/oc-scan-threat-notice-europol-launches-scan-system-for-strategic-notices>
[Letöltés dátuma: 2023.05.10.]
13. Europol: Secure Information Exchange Network Application (SIENA)
<https://www.europol.europa.eu/operations-services-and-innovation/services-support/information-exchange/secure-information-exchange-network-application-siena>
[Letöltés dátuma: 2023.04.05.]
14. Europol: Serious and Organised Crime Threat Assessment
<https://www.europol.europa.eu/publications-events/main-reports/socta-report>
[Letöltés dátuma: 2023.05.10.]
15. Jogharmonizációs ügyek intézése
<https://eujog.im.kormany.hu/jogharmonizacios-ugyek-intezese>
[Letöltés dátuma: 2023.03.04.]

16. Rendeletek, irányelvek és más jogi aktusok
https://european-union.europa.eu/institutions-law-budget/law/types-legislation_hu
[Letöltés dátuma: 2023.03.04.]
17. SZÖLLŐSI Zoltán: DORA (Digital Operational Resilience Act) rendet tesz a pénzügyi kibertérben
<https://www2.deloitte.com/hu/hu/pages/kockazat/articles/dora.html>
[Letöltés dátuma: 2023.03.27.]
18. Tájékoztató az EUROPOL rendszerről
<https://www.naih.hu/europol/tajekoztato-europol-rendszerrol>
[Letöltés dátuma: 2023.04.02.]
19. The Creeper Worm, the First Computer Virus
<https://www.historyofinformation.com/detail.php?entryid=2860>
[Letöltés dátuma: 2023.02.02.]
20. Tim MATTHEWS: A Brief History of Cybersecurity, Cyberinsiders, 2019.
<https://www.cybersecurity-insiders.com/a-brief-history-of-cybersecurity/>
[Letöltés dátuma: 2023.02.06.]