Fekete-Karydis Klára t. őrnagy – Lázár Bence főhadnagy:

A KIBERVÉDELMI STRATÉGIÁK FEJLŐDÉSE, KIBERVÉDELMI KIHÍVÁSOK, AKTUALITÁSOK (2.)

Az Európai Unió kiberbiztonsági szabályozása 2013-tól napjainkig

ÖSSZEFOGLALÓ: *A kibervédelem aktualitása hazai és nemzetközi szinten is megkérdőjelezhetetlenné vált, ami a jelenség körüli stratégiák, képzési programok és szakmai fórumok számának gyors növekedésében is megmutatkozik. Az illegális tevékenységek és a terrorizmus új kapcsolódási pontjai egyúttal azt is megkövetelik a kormányzattól, annak illetékes szerveitől, ügynökségeitől és tisztviselőitől, hogy csak egy kevesek által értett technológia által megtestesített jelenséget szabályozzanak, és továbbfejlesszék a gyorsan változó technológiákkal szembeni védelmet és társadalmi ellenállást. A tanulmány második részében a szerzők közelebbről is bemutatják a kibertér, a kibertérből érkező fenyegetések típusait és az ott zajló trendeket. Vizsgálják a kibervédelem területén jelentkező fő kockázatokat, kihívásokat és fenyegetéseket, illetve hogy mi szükséges egy a kibertámadásokra hatékonyan reagáló nemzeti és nemzetközi rendszer működtetéséhez.*

KULCSSZAVAK: *kiberstratégia, kritikus információs infrastruktúra, terrorizmus, kiberbiztonság, NATO, Európai Unió, kibertámadás, hibrid hadviselés, haderőfejlesztés, kibervédelem, Magyar Honvédség*

BEVEZETÉS

A technológiai forradalom, az információs és a kommunikációs rendszerek példátlanul gyors fejlődése és a posztmodern társadalmi és üzleti kapcsolattartás és a közösségi média eszköztára új alapokra helyezte a nemzeten belüli és a nemzetközi érintkezés platformjait. A 21. századi ember végleg szakítani látszik a hagyományos kommunikációs csatornákkal, és legyen szó társas vagy üzleti kapcsolatokról, részben a költséghatékonyság szempontjainak, részben a megváltozott szokásoknak megfelelően egyre inkább áttevődik mindennapi életünk a kibertérbe. Ez azonban azt is jelenti, hogy mindennapi biztonságunk egy jelentős hányada is e szférába került, hiszen elektromosság és internet nélkül egyszerűen nem működne a ma ismert világunk. Ez természetesen nem jelenti azt, hogy a hagyományos fenyegetések típusai vagy pusztító ereje lecsökkent volna. Ez azt jelenti, hogy a konvencionális veszélyforrások mellett egy új dimenzió nyílt, így biztonságunk és az annak védelmére hivatott erők feladatköre még komplexebbé – és sebezhetőbbé – vált.

A kiberbiztonság azokat a biztosítékokat és intézkedéseket jelenti, amelyek segítségével mind a polgári, mind a katonai területeken egyaránt megvédhető a virtuális tér azoktól a fenyegetésektől, amelyek azok összefüggő hálózataival és információs infrastruktúráival kapcsolatosak, vagy amelyek károsíthatják ezeket. A kiberbiztonság célja a hálózatok és

az infrastruktúra rendelkezésre állásának és integritásának, valamint a benne lévő információk titkosságának megőrzése.

AZ EURÓPAI UNIÓ KIBERVÉDELMI SZABÁLYOZÁSA 2013-TÓL

2013 mérföldkő volt az EU kibervédelmi építkezésében, ekkor született meg a „kibervédelmi törvény" néven is ismert dokumentum, az Európai Bizottság és az Európai Unió közös kül- és biztonságpolitikájának főképviselőjének közös közleménye (2013. február 07.). Az Európai Unió Kiberbiztonsági Stratégiája: egy nyílt, biztonságos és megbízható kibertér (JOIN/2013/01),[1] melynek fő tartalmi elemei között már robusztusan megjelennek a kibervédelem katonai és műveleti vonatkozásai is. A kiberbiztonsági alapelvek legfontosabb mondanivalója, hogy stratégiailag azonos szintre helyezi a digitális teret a fizikai térrel, valamint a rájuk vonatkozó jogi szabályozás, védelem és irányítás kérdéseinek fontosságát. Az uniós jövőképet öt, a kiemelt kihívásokra reagáló stratégiai prioritásban foglalja össze:

1. a kibertámadásokkal szembeni ellenálló képesség elérése a tudatosság javításán keresztül;
2. a számítástechnikai bűnözés drasztikus csökkentése, a dokumentum ennek érdekében szigorú és hatékony jogszabályok bevezetését és hatékonyabb uniós szintű koordinációt sürget;
3. a kibervédelmi politika és képességek kifejlesztése a közös biztonság- és védelempolitika (KBVP) tekintetében;
4. a kiberbiztonsági ipari és a technológiai erőforrások fejlesztése kiemelten a kibervédelmi termékek egységes piacának előmozdítása és a kutatás-fejlesztési célú beruházások és az innováció ösztönzése révén;
5. összefüggő nemzetközi szakpolitika létrehozása a kibertér vonatkozásában az Európai Unió számára és az Unió alapértékeinek támogatása;[2] ennek érdekében beemeli a kibertérrel kapcsolatos kérdéseket az Unió külkapcsolataiba és a közös kül- és biztonságpolitikába, ideértve az Európa Tanácsot, a Gazdasági Együttműködési és Fejlesztési Szervezetet (OECD[3]), az ENSZ-t, az EBESZ-t, a NATO-t, az Afrikai Uniót (AU), a Délkelet-ázsiai Nemzetek Szövetségét (ASEAN[4]) és az Amerikai Államok Szervezetét (OAS[5]), valamint előirányozza a kiberbiztonsággal kapcsolatos kapacitásépítést és az ellenállóképes információs infrastruktúrák fejlesztését harmadik országokban.

---

[1] Közös közlemény az Európai Parlamentnek, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának – Az Európai Unió kiberbiztonsági stratégiája: Nyílt, megbízható és biztonságos kibertér /* JOIN/2013/01 final */ https://eur-lex.europa.eu/legal-content/hu/TXT/?uri=CELEX:52013JC0001 (Letöltés időpontja: 2019. 03. 22.)

[2] Uo. 2. bek.

[3] Organisation for Economic Co-operation and Development.

[4] Association of Southeast Asian Nations.

[5] Organization of American States.

Szintén ebben az évben az Európai Parlament és a Tanács az információs rendszerek elleni támadásokról adott ki egy irányelvet,[6] melynek célja egyrészt a kritikus infrastruktúra védelmének erősítése volt az által, hogy a bűncselekmények tényállására és vonatkozó szankcióikra vonatkozó minimumszabályok megállapítása révén közelítse a tagállamok büntetőjogát az információs rendszerek elleni támadások terén. Másrészt azt is célul tűzte ki, hogy javítsa a tagállamok illetékes hatóságai, így a rendőrség és az egyéb bűnüldözési szakszolgálatok, valamint az Unió illetékes szakosított ügynökségei és szervei – például az Eurojust, az Europol és annak a számítástechnikai bűnözés elleni európai központja –, valamint az Európai Hálózat- és Információbiztonsági Ügynökség (ENISA[7]) közötti együttműködést.

Megjelent továbbá a Tanács határozata is az EU-minősített adatok védelmét szolgáló biztonsági szabályokról[8] azzal a céllal, hogy egyenértékű védelem valósuljon meg a Tanács tulajdonában lévő EU-minősített adatok tekintetében annak más uniós intézményekkel, szervekkel, hivatalokkal és ügynökségekkel való megosztása során, valamint a tagállamok illetékes hatóságai és azok szerződéses vállalkozói tekintetében. Az Eurobarométer annuális kiberbiztonsági kérdőíveinek ismétlődő kérdései alapján kirajzolódó idősorok növekvő tendenciát mutattak a kiberbűnözéssel kapcsolatos aggodalmak terén. 2014-ben[9] már az uniós polgárok 85%-a vélte úgy, hogy növekszik a kiberbűnözésnek való kitettség, vagyis kiberbűnözők áldozatává válhat, így az Európai Parlament és a Tanács közös rendeletet bocsátott ki a belső piacon történő elektronikus tranzakciókhoz kapcsolódó elektronikus azonosításról és bizalmi szolgáltatásokról.[10] Nem volt tehát meglepetés, hogy az Unió 2015-ös biztonsági agendájának három prioritása közül az egyik a kiberbiztonság volt. A dokumentum ugyanabban a felfogásban és szerkezetben tárgyalja a kiberbűnözést, mint a NATO 2011-es kibervédelmi koncepciója, vagyis a terrorizmussal, a szervezett bűnözéssel és a hibrid fenyegetésekkel is összefüggésben.

2016-ban két kulcsfontosságú dokumentumot fogadtak el Brüsszelben: az EU új biztonsági stratégiáját *Közös jövőkép, közös fellépés: erősebb Európa – globális stratégia az Európai Unió kül- és biztonságpolitikájára vonatkozóan*[11] címmel, valamint a hálózati és információs rendszerekkel (NIS[12]) kapcsolatos direktívát. Az Állam- és Kormányfők Európai Tanácsa 2016. június 28-án fogadta el a Federica Mogherini felügyelete alatt készült új, globális európai biztonsági stratégiát, melynek alig van olyan pontja, mely ne említené

[6] Az Európai Parlament és a Tanács Irányelve (2013. augusztus 12.) az információs rendszerek elleni támadásokról és a 2005/222/IB tanácsi kerethatározat felváltásáról. https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:32013L0040&from=fr (Letöltés időpontja: 2019. 03. 25.)

[7] European Network and Information Security Agency.

[8] A Tanács határozata (2013. szeptember 23.) az EU-minősített adatok védelmét szolgáló biztonsági szabályokról (2013/488/EU). https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:274:0001:0050:HU:PDF (Letöltés időpontja: 2019. 03. 25.)

[9] Special Eurobarometer 423 on Cyber Security. Report, 02. 2015. http://ec.europa.eu/commfrontoffice/publicopinion/archives/ebs/ebs_423_en.pdf (Letöltés időpontja: 2019. 03. 22.)

[10] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC. https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX:32014R0910 (Letöltés időpontja: 2019. 03. 05.)

[11] Shared Vision, Common Action: A Stronger Europe. A Global Strategy for the European Union's Foreign and Security Policy. http://eeas.europa.eu/archives/docs/top_stories/pdf/eugs_review_web.pdf (Letöltés időpontja: 2019. 03. 25.)

[12] Network and Information Systems.

a kibervédelmet. A kiberbiztonság a dokumentum által meghatározott öt prioritás közül négyben jelenik meg explicit módon, nevezetesen a 3. rész 1. (Uniónk biztonsága), 2. (Állami és társadalmi ellenálló képesség az Uniótól keletre és délre), 4. (Együttműködésen alapuló regionális berendezkedések) és 5. (Globális kormányzás a 21. században) pontjában, valamint a 4. (Az elképzeléstől az intézkedésig) részben.

A stratégia tartalmilag és szerkezetileg is a nemzetközi biztonsági architektúrákban már kialakult módon tárgyalja a kiberbiztonság és a kibervédelem tárgykörét, új elemként hangsúlyozva, hogy támadás esetén az Unió segítséget nyújt tagállamainak a gyors helyreállításban.[13] A dokumentum „előretekintő kiberszereplőként" *(forward-looking cyber player)* adresszálja az EU-t, mely a digitális világban is megvédi értékeit, és egy szabad és biztonságos globális internetet promotál.[14] Ezen értékek közé emeli be az információ szabad áramlását a személyek, valamint a termékek és szolgáltatások szabad áramlása mellé, s egyben felelős viselkedést biztosító egyezményeket is sürget az államok részéről.[15] Mindezekhez természetesen átfogó feladatrendszert delegál, mely a kritikus (információs) infrastruktúra, az adatvédelem, az állampolgárok és a szektorális szereplők védelmén túl a kiberdiplomáciára, a globális együttműködésre és a multilaterális digitális kormányzásra is kiterjed.[16]

A technológiai fejlődés tekintetében új együttműködést hirdet a dokumentum a versenyszférával,[17] miszerint a megcélzott képességek akkor érhetők el és tarthatók fenn, ha a védelmi együttműködést normának tekintjük, és az önkéntes megközelítés valós elköteleződéssé alakul. Aláhúzza továbbá, hogy az európai stratégiai autonómiához és a KKBP hitelességéhez elengedhetetlen egy fenntartható, innovatív és versenyképes európai védelmi ipar. Nyolc nappal később fogadta el az Európai Parlament a kiberbiztonsági szabályozás letéteményesének számító irányelvet, mely 2016 augusztusában lépett hatályba. A NIS Direktíva[18] széles körű javaslatcsomagot fogalmaz meg a hálózati és információs rendszerek biztonsági szintjének növelésére irányuló intézkedésekre az Unió gazdasága és társadalma szempontjából létfontosságú szolgáltatások biztosítása érdekében. Az irányelvet a tagállamoknak 2018. május 9-ig kellett átültetniük saját jogrendszerükbe, a kiberbiztonsággal kapcsolatos alapvető szolgáltatások szereplőinek beazonosítására pedig 2018. november 9. volt a határidő.

A NIS direktíva adja az EU kiberbiztonságának növeléséhez szükséges intézkedések jogi keretét, de gyakorlati útmutatással[19] is szolgál, például a legjobb gyakorlatok bemutatása és bizonyos bekezdések értelmezése, magyarázata. Az intézkedéscsomag három pillére a tagállamok:

---

[13] Shared Vision Common Action: i. m. 21.

[14] Uo. 21., 42.

[15] Uo. 42.

[16] Uo.

[17] Uo. 45.

[18] The Directive on security of network and information systems (NIS Directive), Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, Official Journal of the European Union, L 194/1, 19. 07. 2016. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC (Letöltés időpontja: 2019. 03. 22.)

[19] NIS Toolkit.

– *felkészültsége* – az illetékes hatóságok kijelölése, a számítógép-biztonsági eseményekre reagáló csoportok, vagyis a CSIRT-ek[20] és kompetens hálózati és információbiztonsági hivatalok felállítása,[21] valamint a nemzeti kiberbiztonsági stratégiák elfogadása és a nemzeti kapcsolattartó pont kijelölése (amennyiben egynél több illetékes hatóság van).

Az illetékes hatóságok felelősségi körébe utalja:
- az alapvető szolgáltatásokat nyújtók (kiber)biztonsági szabályzatainak értékelését;
- a digitális szolgáltatók felügyeletét;
- a részvételt az együttműködési csoport munkájában (melynek tagjai a tagállamok illetékes hálózati és információbiztonsági hatóságai, az Európai Bizottság és az ENISA;
- szükség esetén a nyilvánosság tájékoztatását (a bizalmas adatkezelés szabályainak betartásával);
- a kötelező érvényű utasítások kiadását a kiberbiztonság folyamatos szinten tartása és fejlesztése érdekében.

A CSIRT felelősségi körébe utalja:
- a kiberbiztonsági események nyomon követését és a rájuk történő reagálást;
- a kockázat- és eseményelemzést;
- az együttműködést a CSIRT-ek között és a privát szférával;
- a szabványosított gyakorlatok alkalmazásának szorgalmazását a biztonsági események és a kockázatok kezelésében, valamint az információk osztályozása tekintetében.[22]

– *együttműködése* – melyben minden tagállam részt vesz, s mely kiterjed:
- a stratégiai együttműködésre;
- az információmegosztásra;
- a műveleti együttműködésre;
- a műszaki együttműködésre;
- útmutatás biztosítására a CSIRT felé;
- segítségnyújtásra a tagállamok kiberbiztonsági képességei kiépítésében;
- a jó gyakorlatok átadására;
- a biztonsági eseményekkel kapcsolatban tett bejelentések alapján hozott szabályok megvitatására.[23]

– *interszektorális biztonsági kultúrája* – mely egyaránt fontos a polgárok és a gazdaság szempontjából, főként az energetikai, a közlekedési, a vízi és a pénzügyi szektorban,[24] ahol egy kibertámadás az alapvető szolgáltatás zavarát okozhatja. A kulcsfontosságú szolgáltatóknak meg kell felelniük az irányelvben meghatározott biztonsági és jelentési követelményeknek, továbbá kötelezettséget kell vállalniuk arra vonatkozóan, hogy megfelelő biztonsági intézkedéseket hozzanak és tájékoztassák az érintett nemzeti hatóságokat a súlyos eseményekről. Az irányelv ezen része összességében igyekszik előmozdítani a kockázatkezelés kultúráját.

---

[20] Computer Security Incident Response Team.

[21] Ideértve a NIS tekintetében illetékes hatóságokat és az adatvédelmi hatóságokat is.

[22] Hálózati és információs rendszerek kiberbiztonsága – Összefoglaló az alábbi dokumentumról: (EU) 2016/1148 irányelv – hálózati és információs rendszerek kiberbiztonsága. https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=LEGISSUM:4314915&from=HU (Letöltés időpontja: 2019. 03. 05.)

[23] Hálózati és információs rendszerek kiberbiztonsága. https://eur-lex.europa.eu/legal-content/HU/ALL/?uri=LEGISSUM:4314915 (Letöltés időpontja: 2019. 03. 22.)

[24] Beleértve a bankokat, a pénzintézeteket, a pénzpiacokat és a pénzügyi piaci infrastruktúrát.

A direktíva nagy hangsúlyt fektet az oktatási, tájékoztató és képzési programokra, a kutatás és fejlesztés tervezésére, valamint a kockázatok azonosítására és előrejelzésére, továbbá hatékony, arányos és visszatartó erejű szankciókat helyez kilátásba a direktíva feltételei alkalmazásának biztosítása érdekében. Az Európai Bizottság elkötelezett az irányelv implementációjáért, és periodikusan szabályozza a végrehajtás menetét és egyes aspektusait.[25, 26, 27]

2017 szeptemberében értékelték a 2013-as kiberbiztonsági stratégia eredményeit,[28] megszületett a nagyszabású kiberbiztonsági eseményekre és válsághelyzetekre történő összehangolt reagálásról szóló bizottsági ajánlás,[29] valamint az Unió külügyi és biztonságpolitikai főképviselőinek közös közleménye az Európai Parlamentnek és a Tanácsnak *Ellenálló képesség, elrettentés és* védelem – *Az Unió erőteljes kiberbiztonságának kiépítése* címmel.[30] Ez a közös közlemény a közös megközelítés és a holisztikus szemlélet jegyében íródott, átfogó javaslatcsomagot tartalmaz egyfelől az uniós intézmények, a tagállamok, a privát szféra és a társadalom, másfelől a gazdaság, a digitális egységes piac, a demokrácia, a szabadságjogok és az európai értékek kibertámadásokkal szembeni védelmére azzal a céllal, hogy a kiberbiztonság az Európai Unió digitális társadalmában központi szerepet kapjon.

Mindezt annak figyelembevételével, hogy:

– a kiberbiztonsági eszközök a nemzetbiztonsági struktúrák részeként tagállami kézben vannak;
– a kibertámadások határokon átnyúló jellege miatt e téren alapvető szükséglet a nemzetközi együttműködés;
– az állami szereplők (is) egyre gyakrabban alkalmaznak diszkrétebb kibereszközöket a hagyományos katonai eszközök helyett geopolitikai céljaik elérésére;
– az internetet használó polgári lakosság majdnem egésze érzékel rosszindulatú kibertevékenységet;

---

[25] A Bizottság (EU) 2017/179 végrehajtási határozata (2017. február 1.) a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről szóló (EU) 2016/1148 európai parlamenti és tanácsi irányelv 11. cikkének (5) bekezdése értelmében az együttműködési csoport működéséhez szükséges eljárásrend megállapításáról. HL L 28., 2017. 02. 02., 73–77. https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX:32017D0179 (Letöltés időpontja: 2019. 03. 25.)

[26] A Bizottság közleménye az Európai Parlamentnek és a Tanácsnak: A kiberbiztonsági irányelv maximális kihasználása – a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről szóló 1148/2016/EU irányelv hatékony végrehajtása felé (COM(2017) 476 final 2, 2017. 10. 04.). https://eur-lex.europa.eu/legal-content/hu/TXT/?uri=CELEX%3A52017DC0476 (Letöltés időpontja: 2019. 03. 22.)

[27] A Bizottság (EU) 2018/151 végrehajtási rendelete (2018. január 30.) a hálózati és információs rendszerek biztonságát fenyegető kockázatok kezelése céljából a digitális szolgáltatók által figyelembe veendő elemek és a biztonsági események hatása jelentőségének megállapítására szolgáló paraméterek pontosabb meghatározása tekintetében az (EU) 2016/1148 európai parlamenti és tanácsi irányelv alkalmazására vonatkozó szabályok meghatározásáról (HL L 26., 2018. 01. 31., 48–51.). https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:32018R0151&from=BG (Letöltés időpontja: 2019. 03. 22.)

[28] Commission Staff Working Document, Assessment of the EU 2013 Cybersecurity Strategy, European Commission, Brussels, 13. 09. 2017. SWD(2017) 295 final. http://ec.europa.eu/transparency/regdoc/rep/other/SWD-2017-295-F1-EN-0-0.PDF (Letöltés időpontja: 2019. 03. 25.)

[29] Commission Recommendation (EU) 2017/1584 of 13 September 2017 on coordinated response to large-scale cybersecurity incidents and crises. https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=celex:32017H1584 (Letöltés időpontja: 2019. 03. 22.)

[30] Joint Communication to the European parliament and the Council: Resilience, Deterrence and Defence: Building strong cybersecurity for the EU, European Commission, Brussels, 13. 09. 2017. JOIN(2017) 450 final. https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A52017JC0450 (Letöltés időpontja: 2019. 03. 09.)

– 2020-ra a dolgot internetét[31] alkotó több tízmilliárd eszköz fog csatlakozni az internethez;
– az uniós kiberbiztonsági piac bővülése akadályokba ütközik, melyek közül legjelentősebb az egységes kiberbiztonsági tanúsítási keretrendszer hiánya;
– egyes ágazatok egyedi problémákkal szembesülnek;
– az új digitális technológiák felelősségi kérdéseket vetnek fel;
– elemi fontosságú egy gyors és hatékony vészhelyzeti reagálórendszer kiépítése;
– elengedhetetlen a kiberbiztonsági képességek tagállami és uniós megerősítése;
– a kiberhigiéniának minden életkorban, minden szektorban, minden szinten és minden szakterületen biztosítottnak kell lennie;
– a kiberbiztonsági eszközöknek elérhetőknek kell lenniük a vállalkozások és a magánszemélyek számára is;
– a kiberbűncselekmények kivizsgálásának, illetve a kiberbűnözők büntető eljárás alá vonásának lépést kell tartaniuk a kiberbűnözés növekedési ütemével és fejlődésével;
– nagy a kiber- és a hibrid fenyegetések metszete;
– a nemzetközi jog és különösen az ENSZ Alapokmánya a kibertérben is érvényesül.

A dokumentum összehangolt módon erősíti tovább az Európai Unió kiberbiztonsági struktúráit és kapacitásait a következő eszközökkel:

– az ellenálló képesség kialakításának érdekében a köz- és a privát szféra mellé a társadalmat is beemeli a nemzeti és az uniós kiberbiztonsági együttműködésbe;
– lehetővé teszi a stratégiai függetlenség és a reziliencia kialakítását;
– egységes keretbe foglalja a kiberellenálló képesség munkafolyamatait, rendszerezi azokat a szakterületeket, melyekkel korábban is foglalkozott az EU és kiegészíti azokat;
– az EU áttér a reaktív megközelítésről a proaktív megközelítésre;
– lendületet ad a kiberbiztonsági termékek és szolgáltatások Unión belüli előállításának és az egységes kiberbiztonsági piacnak;
– kiterjeszti az ENISA mandátumát,
– elősegíti az Unión belüli információcserét;
– előirányoz egy uniós kiberbiztonsági tanúsítási keretrendszert;
– ágazatspecifikus stratégiákat szorgalmaz az általános kiberbiztonsági stratégiák kiegészítésére, különösen a pénzügyi szolgáltatások, a szállítás és az energetika területén;
– szorgalmazza a kiberbiztonság beépítését a kereskedelmi és beruházási szakpolitikákba, különös tekintettel a kritikus technológiákkal kapcsolatos külföldi felvásárlások és befektetések szűrésére, valamint a külkereskedelem szabályozásának modernizálására;
– felvállalja, hogy megvizsgálja egy kiberbiztonsági vészhelyzet-elhárítási alap létrehozásának lehetőségét;
– tervezetben ismerteti, hogy hogyan illeszthető be a kiberbiztonság a meglévő válságkezelési mechanizmusokba, meghatározva a tagállamok közötti, illetve a tagállamok és az uniós szervek, szervezeti egységek együttműködésének mikéntjét;
– javaslatot tesz egy európai kiberbiztonsági kutatási és kompetenciaközpont létrehozására;
– javasolja a kutatási erőfeszítések összevonását;
– előirányozza a digitális piacon használt termékek és szolgáltatások titkosításának felmérését szolgáló kapacitás kialakítását;
– előmozdítja a biztonságos internetes kereskedelmet;

[31] Internet of Things – IOT.

– az IKT-szakembereken túl kiterjeszti a kiberhigiéniai képzést a többi ágazatban dolgozókra, a közszférában dolgozókra és az iskolákra, lendületet adva a kiberbiztonsági tananyag fejlesztésének;
– elősegíti a kibertudatosság fejlesztését;
– javaslatot tesz egy egyablakos tájékoztató portál kialakítására, a kiberbiztonsági eszköztár bővítésére az e-kormányzásban, illetve tájékoztató kampányokra;
– előirányozza egy kibervédelmi képzési és oktatási platform létrehozását;
– előmozdítja a bűnözésre történő reagálás fokozását;
– szorgalmazza a bilaterális és multilaterális együttműködést;
– támogatja a kiberbiztonsági fejlesztési együttműködést harmadik országokkal;
– elősegíti a kibertámadások elhárítását a tagállami védelmi kapacitások szinergiájának növelésére vonatkozó javaslatokkal;
– biztosítja a kibervédelem érvényesülését a KBVP-műveletekben;
– megerősíti az Unió kiberbiztonsági kapacitásbővítési képességét;
– biztosítja a fokozott EU–NATO kibervédelmi együttműködést;
– előirányozza az állandó strukturált együttműködési (PESCO[32]) kezdeményezések és az Európai Védelmi Alapnak (EDF[33]) a felhasználását a kibervédelmi projektek támogatására.

Globális összehasonlításban megkérdőjelezhetetlen Európa vezető szerepe (lásd 1. táblázat), fontos azonban megjegyezni, hogy az Egyesült Államok, Kanada és Brazília szigetet képeznek az amerikai kontinensen kibervédelmi szempontból, és a kontinens átlaga messze alulmúlja e három ország képességeit.

1. táblázat *A világ régióinak kiberbiztonsági értékelése*[34]

Régió	Jogi	Technikai	Szervezeti	Kapacitás-fejlesztés	Együtt-működés	Átlag
Afrikai államok	0,29	0,18	0,16	0,17	0,25	0,21
Amerikai államok	0,40	0,30	0,24	0,28	0,26	0,30
Arab államok	0,44	0,33	0,27	0,34	0,29	0,33
Ázsia és a Csendes-óceán térsége	0,43	0,38	0,31	0,34	0,39	0,37
Független Államok Közössége	0,58	0,42	0,37	0,38	0,40	0,43
Európai térség	0,61	0,60	0,45	0,49	0,46	0,52
Átlag	0,46	0,37	0,30	0,33	0,34	0,36

[32] Permanent Structured Cooperation.
[33] European Defence Fund.
[34] Global Cybersecurity Index (GCI) 2017. 25. Fig. 6.1. https://www.itu.int/dms_pub/itu-d/opb/str/d-str-gci.01-2017-pdf-e.pdf (Letöltés időpontja: 2019. 03. 22.)

2018 első félévében három, második félévében két területen történt előrelépés a kibervédelemben. Januárban adta ki a Bizottság a digitális oktatási cselekvési tervről szóló Közleményét,[35] melynek segítségével ismét a gyermekek és a fiatalkorúak védelme került az Unió fókuszába olyan kihívásokkal szemben, mint az internetes zaklatás[36] és a radikalizáció, és olyan kompetenciák kialakítása kapcsán, mint a kiberhigiénia és az online biztonság. Áprilisban az online dezinformációs kampányok kezeléséről jelent meg egy bizottsági közlemény[37] a kibertérben folytatott információs hadviseléssel szembeni védelem érdekében, melyben már gyakorlati szempontból jelenik meg a kibertámadások és a hibrid hadviselés metszete, illetve ezek kombinációja.

Az EU vezetőinek májusi, informális találkozóján is elhangzott közlemény,[38] mely a digitális egységes piac adatvédelméről szól, szorgalmazva a NIS Direktíva maradéktalan implementációját minden tagállamban, és javasolva, hogy a kibervédelem hatékony elrettentéssel párosuljon. Ősztől a kutatás, a technológia, az innováció és az ipari együttműködés került az EU csúcsszerveinek napirendjére két olyan javaslattal, melyek a kiberbiztonsági szaktudás eredményorientált fókuszálására és a gazdasági értelemben is mérhető kibervédelmi ipari fejlesztésre irányultak. Utóbbi azért is elemi fontosságú, mert az élenjáró kiberbiztonsági termékek és szolgáltatások Unión belüli előállítása nem pusztán gazdasági, de biztonsági szempontból is elemi fontosságúak. Az első javaslat a Digitális Európa Program[39] elindítására, a második egy Európai Kibervédelmi Ipari, Technológiai és Kutatási Kompetenciaközpont és a kapcsolódó nemzeti koordinációs központok létrehozására irányul.[40]

---

[35] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on the Digital Education Action Plan, {SWD(2018) 12 final}. European Commission, Brussels, 17. 01. 2018. COM(2018) 22 final. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2018%3A22%3AFIN (Letöltés időpontja: 2019. 03. 22.)

[36] Cyber bullying.

[37] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Tackling online disinformation: a European Approach, COM/2018/236 final, European Commission, Brussels, 26. 04. 2018. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52018DC0236 (Letöltés időpontja: 2019. 03. 05.)

[38] Communication from the Commission, Completing a trusted Digital Single Market for all The European Commission's contribution to the Informal EU Leaders' meeting on data protection and the Digital Single Market in Sofia on 16 May 2018. European Commission, Brussels, 15. 05. 2018. COM(2018) 320 final. https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A52018DC0320 (Letöltés időpontja: 2019. 03. 09.)

[39] Proposal for a Regulation of the European Parliament and of the Council establishing the Digital Europe programme for the period 2021–2027, {SEC(2018) 289 final} {SWD(2018) 305 final} {SWD(2018) 306 final} – Outcome of the European Parliament's proceedings (Strasbourg, 10 to 13 December 2018), COM/2018/434 final – 2018/0227 (COD), ST 15317 2018 INIT. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2018%3A434%3AFIN (Letöltés időpontja: 2019. 03. 22.)

[40] Proposal for a Regulation of the Parliament and the Council establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres. A contribution from the European Commission to the Leaders' meeting in Salzburg on 19–20 September 2018. {SEC(2018) 396 final} – {SWD(2018) 403 final} – {SWD(2018) 404 final}. European Commission, Brussels, 12. 09. 2018, COM(2018) 630 final, 2018/0328 (COD). https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-establishing-european-cybersecurity-industrial-technology-and-research (Letöltés időpontja: 2019. 03. 22.)

2019 első negyedévében is gyorsult az ütem a szabályozás terén. Egyfelől az uniós intézmények biztonságát szolgáló határozat született a személyes adatok védelme tekintetében,[41, 42] illetve folyamatban van az ENISA mandátumának újabb felülvizsgálata,[43] továbbá megjelent a biztonsági unió megvalósítására vonatkozó legfrissebb, 18. helyzetjelentés,[44] illetve kidolgozás alatt van a terrorista tartalmak online terjesztésének prevencióját célzó szabályozás is.[45]

2. táblázat *Az EU-tagállamok osztályozása a GCI értéke szerint*[46]

< 40%	40–50%	50–60%	60–70%	70–80%	80–90%
(3)	(2)	(7)	(10)	(4)	(2)
			7. LV		
			8. DE		
			9. IE		
		17. HR	10. BE		
		18. RO	11. AT		
		19. BG	12. IT		
		20. HU	13. PL	3. UK	
26. MT		21. ES	14. DK	4. NL	
27. SK	24. CY	22. PT	15. CZ	5. FI	1. EE
28. SL	25. GR	23. LT	16. LU	6. SE	2. FR

[41] Commission Decision (EU) 2019/236, of 7 February 2019, laying down internal rules concerning the provision of information to data subjects and the restriction of certain of their rights in the context of the processing of personal data by the European Commission for the purposes of internal security of the Union institutions. https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1553600741335&uri=CELEX:32019D0236 (Letöltés időpontja: 2019. 03. 22.)

[42] Regulation of the European Parliament and of the Council amending Regulation (EU, Euratom) No 1141/2014 of the European Parliament and of the Council as regards a verification procedure related to infringements of rules on the protection of personal data in the context of elections to the European Parliament. https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1553600033549&uri=CONSIL:PE_14_2019_INIT (Letöltés időpontja: 2019. 04. 10.)

[43] Proposal for a Regulation of the Parliament and the Council on ENISA, the „EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification („Cybersecurity Act'') – Outcome of the European Parliament's first reading (Strasbourg, 11 to 14 March 2019), ST 6938 2019 INIT. https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1553599477720&uri=CONSIL:ST_6938_2019_INIT (Letöltés időpontja: 2019. 03. 22.)

[44] Communication from the Commission to the European Parliament, the European Council and the Council, Eighteenth Progress Report towards an effective and genuine Security Union, COM/2019/145 final. https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1553599828872&uri=CELEX:52019DC0145 (Letöltés időpontja: 2019. 03. 29.)

[45] Proposal for a Regulation of the European Parliament and of the Council on preventing the dissemination of terrorist content online = Opinion of the European Economic and Social Committee, ST 15729 2018 INIT. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_15729_2018_INIT&qid=1553600033549&from=EN (Letöltés időpontja: 2019. 03. 29.)

[46] Global Cybersecurity Index (GCI) 2017. 56–57.

ÖSSZEGZÉS

A kibervédelmi koncepciók, stratégiák kialakulása, illetve a kiberbiztonsági szabályozás kezdetben az adatvédelem, a gyermekvédelem, a bűnüldözés, a terrorizmus elleni küzdelem, a kritikus infrastruktúra védelme és a hálózati biztonság területén kezdett formát ölteni, egymástól elszigetelt intézkedések révén. Az idő előrehaladtával rohamosan bővült a kiberbiztonság fogalomtára, kialakult például a kritikus információs infrastruktúra fogalma, differenciálódott a kibertámadások és azok elkövetőinek a definíciója, az állami és a nem állami szereplők által végzett tevékenységek formái, valamint a kezdeti konfúzió után letisztultak az információs és a kiberműveletek közti határok.

Az IKT-szektor és a rossz szándékú kiberműveletek rohamos terjedése és robbanásszerű fejlődése négy különböző, ugyanakkor egymással összefüggő területen jelentős.

1. Holisztikus szemlélet – ami szükségessé tette az egyre szofisztikáltabb ágazati kiberbiztonsági stratégiák és az átfogó, a kibervédelem összes aspektusát strukturáltan kezelő keretdokumentumok, önkéntességen alapuló ajánlások és törvényerejű szabályzók kidolgozását és hatályba léptetését.
2. Együttműködés – ami egyenesen következik a kibertér globális, határokon átnyúló jellegéből, valamint kiemelten fontos az euroatlanti térség biztonsága szempontjából.
3. Védelmi ipari kutatás, fejlesztés, innováció és a belső piac fejlesztése – amit egyenlőképp indokol az iparág exponenciálisan gyorsuló fejlődése, az a fundamentális követelmény, hogy az Unió nem alapozhatja biztonságát döntő többségében harmadik, esetenként az euroatlanti térségen kívül eső országokból importált eszközökre, valamint az, hogy a belső piac ilyen irányú fejlesztése gazdasági szempontból is nagy jelentőséggel bír egy digitális társadalomban.
4. Oktatás-képzés – ami azon a felismerésen alapul, hogy a kiberbiztonság szerves eleme a felhasználó kiberhigiéniai képessége, így nemzetbiztonsági, sőt vállalatgazdasági szempontból is kritikus fontosságúvá vált a dolgozók képzése és a szakemberek továbbképzése, sőt az is, hogy digitális társadalmunkban minden polgár tájékoztatást kapjon e tekintetben, hogy megvédhessük materiális és immateriális értékeinket és gyermekeinket, szem előtt tartva, hogy a felnövekvő nemzedékek már egy szinte minden tekintetben digitalizált világban fognak élni.

FELHASZNÁLT IRODALOM

A Bizottság (EU) 2017/179 végrehajtási határozata (2017. február 1.) a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről szóló (EU) 2016/1148 európai parlamenti és tanácsi irányelv 11. cikkének (5) bekezdése értelmében az együttműködési csoport működéséhez szükséges eljárásrend megállapításáról. HL L 28., 2017. 02. 02., 73–77. https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX:32017D0179

A Bizottság (EU) 2018/151 végrehajtási rendelete (2018. január 30.) a hálózati és információs rendszerek biztonságát fenyegető kockázatok kezelése céljából a digitális szolgáltatók által figyelembe veendő elemek és a biztonsági események hatása jelentőségének megállapítására szolgáló paraméterek pontosabb meghatározása tekintetében az (EU) 2016/1148 európai parlamenti és tanácsi irányelv alkalmazására vonatkozó szabályok meghatározásáról (HL L 26., 2018. 01. 31., 48–51.). https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:32018R0151&from=BG

A Bizottság közleménye az Európai Parlamentnek és a Tanácsnak: A kiberbiztonsági irányelv maximális kihasználása – a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről szóló 1148/2016/EU irányelv hatékony végrehajtása felé (COM(2017) 476 final 2, 2017. 10. 04.). https://eur-lex.europa.eu/legal-content/hu/TXT/?uri=CELEX%3A52017DC0476

A Tanács határozata (2013. szeptember 23.) az EU-minősített adatok védelmét szolgáló biztonsági szabályokról (2013/488/EU). https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:274:0001:0050:HU:PDF

Az Európai Parlament és a Tanács Irányelve (2013. augusztus 12.) az információs rendszerek elleni támadásokról és a 2005/222/IB tanácsi kerethatározat felváltásáról. https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:32013L0040&from=fr

Commission Decision (EU) 2019/236, of 7 February 2019, laying down internal rules concerning the provision of information to data subjects and the restriction of certain of their rights in the context of the processing of personal data by the European Commission for the purposes of internal security of the Union institutions. https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1553600741335&uri=CELEX:32019D0236

Commission Recommendation (EU) 2017/1584 of 13 September 2017 on coordinated response to large-scale cybersecurity incidents and crises. https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=celex:32017H1584

Commission Staff Working Document, Assessment of the EU 2013 Cybersecurity Strategy, European Commission, Brussels, 13. 09. 2017. SWD(2017) 295 final. http://ec.europa.eu/transparency/regdoc/rep/other/SWD-2017-295-F1-EN-0-0.PDF

Communication from the Commission, Completing a trusted Digital Single Market for all The European Commission's contribution to the Informal EU Leaders' meeting on data protection and the Digital Single Market in Sofia on 16 May 2018. European Commission, Brussels, 15. 05. 2018. COM(2018) 320 final. https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A52018DC0320

Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on the Digital Education Action Plan, {SWD(2018) 12 final}. European Commission, Brussels, 17. 01. 2018. COM(2018) 22 final. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2018%3A22%3AFIN

Communication from the Commission to the European Parliament, the European Council and the Council, Eighteenth Progress Report towards an effective and genuine Security Union, COM/2019/145 final. https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1553599828872&uri=CELEX:52019DC0145

Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Tackling online disinformation: a European Approach, COM/2018/236 final, European Commission, Brussels, 26. 04. 2018. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52018DC0236

Global Cybersecurity Index (GCI) 2017. 25. Fig. 6.1. https://www.itu.int/dms_pub/itu-d/opb/str/d-str-gci.01-2017-pdf-e.pdf

Hálózati és információs rendszerek kiberbiztonsága. https://eur-lex.europa.eu/legal-content/HU/ALL/?uri=LEGISSUM:4314915

Hálózati és információs rendszerek kiberbiztonsága – Összefoglaló az alábbi dokumentumról: (EU) 2016/1148 irányelv – hálózati és információs rendszerek kiberbiztonsága. https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=LEGISSUM:4314915&from=HU

Joint Communication to the European parliament and the Council: Resilience, Deterrence and Defence: Building strong cybersecurity for the EU, European Commission, Brussels, 13. 09. 2017. JOIN(2017) 450 final. https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A52017JC0450

Közös közlemény az Európai Parlamentnek, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának – Az Európai Unió kiberbiztonsági stratégiája: Nyílt, megbízható és biztonságos kibertér /* JOIN/2013/01 final */ https://eur-lex.europa.eu/legal-content/hu/TXT/?uri=CELEX:52013JC0001

Proposal for a Regulation of the European Parliament and of the Council establishing the Digital Europe programme for the period 2021–-2027, {SEC(2018) 289 final} {SWD(2018) 305 final} {SWD(2018) 306 final} – Outcome of the European Parliament's proceedings (Strasbourg, 10 to 13 December 2018), COM/2018/434 final – 2018/0227 (COD), ST 15317 2018 INIT. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2018%3A434%3AFIN

Proposal for a Regulation of the Parliament and the Council establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres. A contribution from the European Commission to the Leaders' meeting in Salzburg on 19–20 September 2018. {SEC(2018) 396 final} – {SWD(2018) 403 final} – {SWD(2018) 404 final}. European Commission, Brussels, 12. 09. 2018, COM(2018) 630 final, 2018/0328 (COD). https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-establishing-european-cybersecurity-industrial-technology-and-research

Proposal for a Regulation of the Parliament and the Council on ENISA, the „EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification („Cybersecurity Act'') – Outcome of the European Parliament's first reading (Strasbourg, 11 to 14 March 2019), ST 6938 2019 INIT. https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1553599477720&uri=CONSIL:ST_6938_2019_INIT

Proposal for a Regulation of the European Parliament and of the Council on preventing the dissemination of terrorist content online = Opinion of the European Economic and Social Committee, ST 15729 2018 INIT. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_15729_2018_INIT&qid=1553600033549&from=EN

Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC. https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX:32014R0910

Regulation of the European Parliament and of the Council amending Regulation (EU, Euratom) No 1141/2014 of the European Parliament and of the Council as regards a verification procedure related to infringements of rules on the protection of personal data in the context of elections to the European Parliament. https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1553600033549&uri=CONSIL:PE_14_2019_INIT

Shared Vision, Common Action: A Stronger Europe. A Global Strategy for the European Union's Foreign and Security Policy. http://eeas.europa.eu/archives/docs/top_stories/pdf/eugs_review_web.pdf

Special Eurobarometer 423 on Cyber Security. Report, 02. 2015. http://ec.europa.eu/commfrontoffice/publicopinion/archives/ebs/ebs_423_en.pdf

The Directive on security of network and information systems (NIS Directive), Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, Official Journal of the European Union, L 194/1, 19. 07. 2016. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC