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

A KIBERVÉDELMI STRATÉGIÁK FEJLŐDÉSE, KIBERVÉDELMI KIHÍVÁSOK, AKTUALITÁSOK (1.)

AZ Európai Unió kiberbiztonsági szabályozása 2013-ig

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 szerzők tanulmányuk első részében felvázolják a kiberbiztonsági stratégiák kialakulásának folyamatát, bemutatják a szabályozási környezet kronológiai fejlődését és annak aktualitásait. Részletes képet nyújtanak a nemzetközi biztonsági architektúrák kiberbiztonsági előírásairól, a releváns magyar jogszabályokról, a kibervédelmi intézményrendszerről, illetve ezek céljairól és követelményeiről.*

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, a posztmodern társadalmi és üzleti kapcsolattartás, valamint 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. 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 ELSŐ IRÁNYELVTŐL A KRITIKUS INFORMÁCIÓS INFRASTRUKTÚRAVÉDELMI AKCIÓTERVIG

Az első, a kiberbiztonság szempontjából releváns irányelv az adatvédelem területén született 1995-ben a személyes adatok feldolgozása vonatkozásában, az egyének védelméről és az ilyen adatok szabad áramlásáról.[1] A közös európai kibervédelem kialakításának a 2001. június 6-án a *Hálózati és Információs Biztonság: Javaslat egy európai szakpolitikai megközelítésre* című közlemény adott aztán impetust, melyben az Európai Bizottság egyszerre adresszálta az Európai Unió Tanácsát, az Európai Parlamentet, az Európai Gazdasági és Szociális Bizottságot, valamint a Régiók Tanácsát.[2]

A Budapesti Konvenció[3] (Európa Tanács, 2001. november 23.) a számítógépes hálózatokon, vagyis főként az interneten elkövetett bűncselekményekről szóló első nemzetközi egyezmény. Az Egyezmény Preambulumában megfogalmazott fő cél a bűnözés elleni küzdelemre irányuló közös büntetőpolitika kialakítása, különösen a megfelelő jogszabályok elfogadásával és a nemzetközi együttműködés előmozdításával. A Konvenció főként a szerzői jog, a számítógéppel elkövetett csalás, a gyermekpornográfia és a hálózati biztonság területein elkövetett jogsértésekre vonatkozik, valamint olyan jogköröket és eljárásokat tartalmaz, mint például a számítógépes hálózatok keresése és a lehallgatás, illetve a kiberbűnözésre vonatkozó jogharmonizáció, a nyomozati tevékenység és a vádemelés elősegítése, továbbá egy gyors és hatékony nemzetközi együttműködési rendszer felállítása.

2002. január 28-án megszületett a Tanács 2002/C 43/02 számú határozata a közös álláspontról és a különleges intézkedésekről a hálózati és az információbiztonság területén,[4] március 7-én az Európai Parlament és a Tanács 2002/21/EK keretirányelve az elektronikus hírközlő hálózatok és elektronikus hírközlési szolgáltatások közös keretszabályozásáról,[5] majd az elektronikus hírközlési ágazatban a személyes adatok kezeléséről, feldolgozásáról és a magánélet védelméről július 12-én,[6] 2003. február 08-án pedig a Tanács 2003/C

---

[1] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Official Journal L 281, 23. 11. 1995. P. 0031 – 0050. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:31995L0046&from=en (Letöltés időpontja: 2019. 02. 23.)

[2] Commission of the European Communities, Brussels, 06. 06. 2001., (COM(2001) 298), Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of Regions, Network and Information Security: Proposal for A European Policy Approach. https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2001:0298:FIN:EN:PDF (Letöltés időpontja: 2019. 02. 23.)

[3] Convention on Cybercrime, Council of Europe, European Treaty Series No. 185.

[4] Council Resolution of 28 January 2002 on a common approach and specific actions in the area of network and information security. Official Journal C 043, 16. 02. 2002. P. 0002 – 0004. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32002G0216%2802%29 (Letöltés időpontja: 2019. 02. 23.)

[5] 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 (Framework Directive). Official Journal L 108, 24. 04. 2002. P. 0033 – 0050. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32002L0021&from=en (Letöltés időpontja: 2019. 02. 18.)

[6] 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 (Directive on privacy and electronic communications). Official Journal L 201, 31. 07. 2002. P. 0037 – 0047. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32002L0058&from=EN (Letöltés időpontja: 2019. 02. 23.)

48/01 számú, *A hálózati* és *az információbiztonság-kultúra európai megközelítése*[7] című határozata.

A kiberbiztonság fogalma olyan, egyébként kapcsolódó területeken kiadott hivatalos dokumentumokban is megjelent, mint a terrorizmus elleni küzdelem és a kritikus infrastruktúra védelme. Ezek közül legfontosabb az első hivatalos EU-közlemény, melyben megemlítésre kerül a kibertámadás és a kiberterrorizmus fogalma, az Európai Bizottság által 2004. október 20-án elfogadott *A létfontosságú infrastruktúrák védelme a terrorizmus elleni küzdelemben,*[8] mely az EU terrortámadásokkal és a kritikus infrastruktúrával kapcsolatos prevenciós, készenléti, eseményreagálási képességeinek megerősítésére vonatkozó intézkedésekre tesz javaslatot, valamint a később erre épülő programok:

- a program implementációjának támogatására kiadott Zöld Könyv *(Green Paper on a European Programme for Critical Infrastructure Protection);*[9]
- a létfontosságú infrastruktúrák figyelmeztető információs hálózatának *(Critical Infrastructure Warning Information Network – CIWIN)*[10] a felállítása;
- a létfontosságú infrastruktúrák védelmére vonatkozó európai program[11] *(European Programme for Critical Infrastructure Protection – EPCIP),*[12] melyben az Európai Bizottság kijelöli a program végrehajtásához szükséges elveket és eszközöket;
- a kritikus infrastruktúrák védelméért felelős európai hálózat *(European Reference Network for Critical Infrastructure Protection – ERNCIP)*[13] létrehozása, mely hozzávetőleg 140 tagintézménnyel működik együtt.

Az európai uniós kiberbiztonság két pillérét képező hálózati és információbiztonsági *(network and information security – NIS)* direktíva,[14] illetve a kritikus információs infrastruktúra-védelem[15] kialakulásához hosszú út vezetett, melynek során párhuzamosan folyt az uniós struktúrák fejlesztése, a tagállami intézkedésekre és vállalásokra történő javaslatok kidolgozása, illetve a kibervédelem beillesztése a közös, uniós védelmi együttműködésbe.

---

[7] Council Resolution of 18 February 2003 on a European approach towards a culture of network and information security. Official Journal C 048, 28. 02. 2003. P. 0001 – 0002. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32003G0228%2801%29 (Letöltés időpontja: 2019. 02. 14.)

[8] Critical infrastructure protection. Communication from the Commission to the Council and the European Parliament of 20 October 2004 – Critical Infrastructure Protection in the fight against terrorism COM(2004) 702. https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=LEGISSUM:l33259 (Letöltés időpontja: 2019. 02. 23.)

[9] Az Európai Közösségek Bizottsága, Brüsszel, 2005. 11. 17., COM(2005) 576. Zöld Könyv a létfontosságú infrastruktúrák védelmére vonatkozó európai programról. https://eur-lex.europa.eu/legal-content/GA/TXT/?uri=celex:52005DC0576 (Letöltés időpontja: 2019. 02. 23.)

[10] https://ec.europa.eu/home-affairs/what-we-do/networks/critical_infrastructure_warning_information_network_en (Letöltés időpontja: 2019. 02. 14.)

[11] A Bizottság 2006. december 12-i közleménye a létfontosságú infrastruktúrák védelmére vonatkozó európai programról, COM(2006) 786. Az Európai Unió Hivatalos Lapja, C 126, 2007. 06. 07. https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=LEGISSUM:l33260&from=EN (Letöltés időpontja: 2019. 03. 14.)

[12] https://ec.europa.eu/home-affairs/content/european-programme-critical-infrastructure-protection-epcip_en (Letöltés időpontja: 2019. 03. 14.)

[13] https://erncip-project.jrc.ec.europa.eu/ (Letöltés időpontja: 2019. 02. 23.)

[14] Directive on Security of Network and Information Systems/NIS Directive. Az Európai Unió és a Tanács (EU) 2016/1148 Irányelve (2016. 06. 06.) a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről. Az Európai Unió Hivatalos Lapja, L 194/1, 2016. 07.19. https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:32016L1148&from=EN (Letöltés időpontja: 2019. 02. 18.)

[15] Critical Information Infrastructure Protection – CIIP.

Ennek az építkezésnek az első eleme az Európai Hálózat- és Információbiztonsági Ügynökség *(European Network and Information Security Agency – ENISA)* létrehozása[16] volt 2004-ben, mely nagymértékben hozzájárul az EU hálózati és információbiztonsági kultúrájának fejlesztéséhez és az internetpiac megfelelő működéséhez, szoros együttműködésben a tagállamokkal és a privát szférával.

2006. május 31-én fogadták el *Az Európai Bizottság stratégiája egy biztonságos információs társadalomért – dialógus, partnerség, megerősítés* című közleményt,[17] mely a kockázatkezelési intézkedések átfogó sorozatát kínálja az elektronikus kommunikációhoz kötődő reziliencia kiépítésének jegyében. 2007-ben a Tanács adott ki egy állásfoglalást a biztonságos európai információs társadalomra irányuló stratégiáról,[18] 2008-ban pedig meghosszabbították az ENISA mandátumát.[19]

A 2009-es kritikus információs infrastruktúra-védelmi akcióterv megalkotásának elsődleges célja Európa megvédése volt a jelentős kibertámadásoktól és megszakításoktól. A biztonságot és az ellenálló képességet jelölte meg a védelem első vonalaként, aláhúzva az ez irányú nemzetközi együttműködés fontosságát, és kiemelte az EU készenléti és eseményreagálási képességének, illetve a konzisztens megelőző, felismerő, vészhelyzeti és helyreállítási intézkedések elfogadásának fontosságát. A Bizottság öt célt fogalmazott meg a dokumentumban:

1. a tagállamok közti együttműködés és a jó (szakpolitikai) gyakorlatok átadásának elősegítése;
2. a kritikus információs infrastruktúra biztonságát és ellenálló képességét szolgáló európai szintű Public Private Partnership kialakítása;
3. az eseményreagálási képesség támogatása az Európai Unióban;
4. a nemzeti és EU-s kibervészhelyzeti tervek és jelentős hálózatbiztonsági incidenseket szimuláló gyakorlatok előmozdítása;
5. a nemzetközi együttműködés megerősítése a globális problémák kezelésére, kiemelten az internet stabilitása és az ellenálló képesség tekintetében.

[16] Az Európai Parlament és a Tanács 460/2004/EK rendelete (2004. 03. 10.) az Európai Hálózat- és Információbiztonsági Ügynökség létrehozásáról. Hivatalos Lap L 077, 13. 03. 2004. o. 0001 – 0011. https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:32004R0460&from=EN (Letöltés időpontja: 2019. 03. 14.)

[17] Communication from the Commission of 31 May 2006: A strategy for a Secure Information Society – Dialogue, partnership and empowerment COM(2006) 251. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM%3Al24153a (Letöltés időpontja: 2019. 02. 18.)

[18] Council Resolution of 22 March 2007 on a Strategy for a Secure Information Society in Europe (2007/C 68/01). https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:32007G0324(01)&from=EN (Letöltés időpontja: 2019. 02. 23.)

[19] Regulation (EC) No 1007/2008 Of the European Parliament and of the Council of 24 September 2008 amending Regulation (EC) No 460/2004 establishing the European Network and Information Security Agency as regards its duration. https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:293:0001:0002:EN:PDF (Letöltés időpontja: 2019. 03. 03.)

A fenti célok elérése érdekében az akcióterv az alábbi öt pillérre épül:

1. Felkészültség és prevenció:
   a) európai fórum, ahol a tagállamok megoszthatják információs és szakpolitikai gyakorlataikat;[20]
   b) európai Public Private Partnership az ellenálló képességért;[21]
   c) alapvető képességek és szolgáltatások a nemzeti/kormányzati CERT-eknek.
2. Felismerés és reagálás:
   a) egy európai információmegosztási és riasztórendszer[22] kialakítása;
   b) a polgárokat és a kisvállalkozásokat támogató európai információmegosztási és riasztórendszer.
3. Kárenyhítés és helyreállítás:
   a) nemzeti vészhelyzeti tervezés és gyakorlatok;
   b) páneurópai jelentős internetes incidenskezelő gyakorlatok;
   c) megerősített együttműködés a nemzeti/kormányzati CERT-ek között.
4. Nemzetközi együttműködés:
   a) a hosszú távú ellenálló képességet és az internet tartós stabilitását támogató európai prioritások, alapelvek és útmutatók meghatározása;
   b) az alapelvek és az útmutatók globális promóciója;
   c) globális együttműködés a jelentős internetes incidenskezelő gyakorlatokon.
5. Az európai kritikus infrastruktúra fogalomkörének definiálása az információs és kommunikációs technológia szektorában.

Ugyanebben az évben további öt, az internet védelmével, a kritikus (információs) infrastruktúra védelmével, valamint a tagállamok adatvédelmi együttműködésével kapcsolatos dokumentumot fogadtak el:

– a Bizottság közleménye az Európai Parlamentnek és a Tanácsnak: „Az internet szabályozása”;[23]
– a Bizottság Közleménye az Európai Parlamentnek, a Tanácsnak, az Európai Gazdasági és Szociális bizottságnak, valamint a Régiók Bizottságának a kritikus informatikai infrastruktúrák védelméről: „Európa védelme a nagyszabású számítógépes támadások és hálózati zavarok ellen: a felkészültség, a védelem és az ellenálló képesség fokozása”;[24]
– a Tanács **á**llásfoglalása a hálózat- és információbiztonság együttműködésre építő európai megközelítéséről;[25]

[20] European Forum for MS – EFMS.

[21] European Public Private Partnership for Resilience – EP3R.

[22] European Information Sharing and Alert System – EISAS.

[23] Communication from the Commission to the European Parliament and the Council – Internet governance: the next steps. Az Európai Közösségek Bizottsága, Brüsszel, 2009. 06. 18., COM(2009) 277. https://eur-lex.europa.eu/legal-content/HU/ALL/?uri=CELEX:52009DC0277 (Letöltés időpontja: 2019. 03. 18.)

[24] Opinion of the European Economic and Social Committee on the ’Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Critical Information Infrastructure Protection. Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience. COM(2009) 149, 22. 09. 2010. HU. Az Európai Unió Hivatalos Lapja, C 255/98. https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX:52009AE1948 (Letöltés időpontja: 2019. 03. 18.)

[25] 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/HU/TXT/HTML/?uri=CELEX:-32009G1229(01)&from=EN (Letöltés időpontja: 2019. 03. 18.)

– elnökségi következtetések a kritikus információs infrastruktúra védelméről szóló miniszteri értekezletről;[26]
– az Európai Parlament és a Tanács 2009/140/EK irányelve az elektronikus hírközlő hálózatok és elektronikus hírközlési szolgáltatások közös keretszabályozásáról szóló 2002/21/EK irányelv, az elektronikus hírközlő hálózatokhoz és kapcsolódó eszközökhöz való hozzáférésről, valamint azok összekapcsolásáról szóló 2002/19/EK irányelv és az elektronikus hírközlő hálózatok és az elektronikus hírközlési szolgáltatások engedélyezéséről szóló 2002/20/EK irányelv módosításáról.[27]

Ezek közül a második volt az, amely létrehozta az állam és a versenyszféra közti partnerséget a nemzeti kiber ellenálló képesség javítása érdekében. Olyan javaslatokat fogalmazott meg a digitális kommunikáció nagymértékű zavaraira reagálandó, melyek ösztönözték az együttműködést a legfontosabb erőforrások, szolgáltatások és eszközök tekintetében, valamint a köz- és a versenyszférára is érvényes követelményeket fogalmazott meg, és megteremtette az együttműködés és a működési mechanizmusok alapjait. 2010-ben megszületett az európai digitális menetrend[28] és az ENISA modernizációjának koncepciója.[29] Az Európai Unió és az Amerikai Egyesült Államok novemberi csúcstalálkozóján létrehoztak egy munkacsoportot,[30] melynek feladata együttműködési megközelítések kialakítása volt kiberbiztonsági és számítástechnikai bűnözéssel kapcsolatos kérdésekben.

INTÉZKEDÉSEK 2011-TŐL 2013-IG

2011 a korábbi stratégiák és állásfoglalások frissítésének, átdolgozásának éve volt, és kiadásra került a Bizottság közleménye az Európai Parlamentnek, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak, valamint a Régiók Bizottságának a kritikus informatikai infrastruktúrák védelméről: „Eredmények és következő lépések: a globális kiberbiztonság felé”,[31] melyet a 10299/11. sz. tanácsi következtetésekben hagytak jóvá. Megjelent a Bizottság közleménye az Európai Parlamentnek, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak, valamint a Régiók Bizottságának a kritikus informatikai infrastruktúrák

[26] Presidency Conclusions of the Ministerial Conference on Critical Information Infrastructure Protection, Tallin (EE).

[27] Directive 2009/140/EC of the European Parliament and of the Council of 25 November 2009 amending Directives 2002/21/EC on a common regulatory framework for electronic communications networks and services, 2002/19/EC on access to, and interconnection of, electronic communications networks and associated facilities, and 2002/20/EC on the authorisation of electronic communications networks and services. https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0037:0069:HU:PDF (Letöltés időpontja: 2019. 02. 23.)

[28] https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0245:FIN:HU:PDF (Letöltés időpontja: 2019. 02. 23.)

[29] Európai Bizottság, Brüsszel, 2010. 09. 30., COM(2010) 521, 2010/0275 (COD). Javaslat: Az Európai Parlament és a Tanács Rendelete az Európai Hálózat- és Információbiztonsági Ügynökségről (ENISA) {SEC(2010) 1126} {SEC(2010) 1127} https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:52010PC0521&from=EN (Letöltés időpontja: 2019. 03. 18.)

[30] European Commission, MEMO, Brussels, 05. 12. 2012., Declaration on the Launch of the Global Alliance against child sexual abuse online. http://europa.eu/rapid/press-release_MEMO-12-944_en.htm (Letöltés időpontja: 2019. 02. 03.)

[31] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Critical Information Infrastructure Protection. 'Achievements and next steps: towards global cyber-security' COM(2011) 163. https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:52011DC0163&from=EN (Letöltés időpontja: 2019. 03. 18.)

védelméről is: „Európa védelme a nagyszabású számítógépes támadások és hálózati zavarok ellen: a felkészültség, a védelem és az ellenálló képesség fokozása”,[32] valamint másodszor is meghosszabbították az ENISA mandátumát.[33]

2012 elején a gyermekvédelem került az EU döntéshozóinak fókuszpontjába, és a Bizottság kiadta a gyermekek számára jobb és biztonságosabb internethasználatot biztosító európai stratégiáját.[34] Márciusban külön felmérést készített az Eurobarométer a kiberbiztonságról, melynek eredményeit 2012 júliusában publikálta,[35] és az Európai Bizottság kiadott egy közleményt a Tanácsnak és az Európai Parlamentnek *Küzdelem digitális korunk bűnözésével: számítástechnikai bűnözés elleni európai központ létrehozása* címmel,[36] ami az EU és benne az Europol válasza volt a határok nélküli kibertérben zajló bűnözéssel szemben. Szinte napra pontosan 11 év telt el a Budapesti Konvenció óta, mire megszületett az Európai Parlament 2012. november 22-i állásfoglalása a kiberbiztonságról és -védelemről,[37] mely hangsúlyozza, hogy:

– a számítástechnikai fenyegetések és a kormányzati, közigazgatási, katonai és nemzetközi szervek elleni támadások az EU-ban és világszerte egyre nagyobb veszélyt jelentenek, egyre gyakrabban fordulnak elő, és komoly aggodalomra ad okot, hogy az állami és nem állami szereplők, különösen a terror- és bűnszervezetek megtámadhatják az uniós intézmények és tagállamok kritikus információs és kommunikációs struktúráit és infrastruktúráit, és jelentős – akár működésképtelenséggel járó – károkat okozhatnak;[38]
– e kihívásokkal szemben globális, összehangolt megközelítésre van szükség uniós szinten, egy olyan átfogó uniós kiberbiztonsági stratégia kidolgozásával, amely gondoskodik a kiberbiztonság és -védelem közös fogalommeghatározásáról, továbbá annak meghatározásáról, hogy mi minősül a védelemmel kapcsolatos számítógépes támadásnak, illetve egy közös műveleti koncepcióról, és amelynek figyelembe kell vennie

[32] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Critical Information Infrastructure Protection. „Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience” {SEC(2009) 399} {SEC(2009) 400} COM/2009/0149. https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:52009DC0149&from=EN (Letöltés időpontja: 2019. 03. 18.)

[33] Regulation (EU) No 580/2011 of the European Parliament and of the Council of 8 June 2011 amending Regulation (EC) No 460/2004 establishing the European Network and Information Security Agency as regards its duration. https://www.enisa.europa.eu/media/news-items/extension-of-enisa2019s-mandate-published-1 (Letöltés időpontja: 2019. 02. 23.)

[34] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions European Strategy for a Better Internet for Children. European Commission, Brussels, 02. 05. 2012., COM(2012) 196 final. https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0196:FIN:EN:PDF (Letöltés időpontja: 2019. 03. 04.)

[35] 390. sz. Eurobarométer különfelmérés a kiberbiztonságról, 2012. http://ec.europa.eu/commfrontoffice/publicopinion/index.cfm/Survey/getSurveyDetail/yearFrom/1974/yearTo/2012/surveyKy/1058 (Letöltés időpontja: 2019. 02. 23.)

[36] Communication from the Commission to the Council and the European Parliament, Tackling Crime in our Digital Age: Establishing a European Cybercrime Centre /* COM/2012/0140 final */. https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=celex:52012DC0140 (Letöltés időpontja: 2019. 02. 23.)

[37] P7_TA(2012)0457 Kiberbiztonság és -védelem. Az Európai Parlament 2012. november 22-i állásfoglalása a kiberbiztonságról és -védelemről (2012/2096(INI)) (2015/C 419/22). Az Európai Unió Hivatalos Lapja, C 419/145, 2015. 12. 16. https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX%3A52012IP0457 (Letöltés időpontja: 2019. 03. 08.)

[38] Uo. 1. bek.

a meglévő ügynökségek és szervek jelentette hozzáadott értéket, valamint a nemzeti stratégiával már rendelkező tagállamok bevált gyakorlatait és a levont tanulságokat;
- egy ilyen stratégiának biztosítania kell a rugalmasságot, és azt rendszeresen aktualizálni kell annak érdekében, hogy alkalmazkodni tudjon a kibertér gyorsan változó természetéhez;[39]
- elengedhetetlen egy, a kibervédelemről szóló Fehér Könyv kidolgozása, amely egyértelmű fogalommeghatározásokat állapít meg és meghatározza a polgári és katonai szférában elkövetett számítógépes támadások szintjeinek kritériumait e támadások motivációjának és hatásának, továbbá a válaszlépések szintjeinek – többek között az elkövetők kivizsgálásának, felderítésének és büntetőeljárás alá vonásának – megfelelően.[40]

A kibervédelem más, fontos katonai vetületei több területen is kiemelten jelennek meg a dokumentumban, úgymint:
- a különböző katonai és polgári kezdeményezések, programok és tevékenységek ötvözésének elősegítése a koordináció és az uniós szintű szinergiák kialakítása érdekében;[41]
- az Európai Unió működéséről szóló szerződés[42] 222. cikkének (Szolidaritási Záradék) végrehajtására vonatkozó megoldásokkal kapcsolatos javaslat kidolgozásának szükségessége egy tagállamot érő súlyos kibertámadás esetére, illetve, bár még mindig várat magára a nemzetbiztonságot fenyegető kibertámadások közös terminológiával való meghatározása, az Európai Unióról szóló szerződés[43] 42. cikkének (7) bekezdése (Kölcsönös Védelmi Záradék) kiterjedhetne az ilyen támadásokra is;[44]
- a közös biztonság- és védelempolitikának (KBVP) biztosítania kell, hogy az uniós katonai műveletekben és polgári missziókban részt vevő erők védelmet kapjanak a számítógépes támadásokkal szemben, hangsúlyozván, hogy a kibervédelemnek a KBVP aktív képességének kell lennie;[45]
- jogszabályi szinten megfelelő különbséget kell tenniük a polgári és a katonai szintű számítástechnikai incidensek között.[46]

A dokumentum az EU kibervédelmének minden szintjére vonatkozóan megfogalmaz ajánlásokat:
- az Unió szintjén;
- az Európai Védelmi Ügynökség vonatkozásában:
  - sürgeti a tagállamokat, hogy működjenek együtt nagyobb mértékben az Ügynökséggel katonai téren is – a kibervédelem területén;[47]

[39] Uo. 2. bek.
[40] Uo. 7. bek.
[41] Uo. 2. bek.
[42] Az Európai Unió működéséről szóló szerződés egységes szerkezetbe foglalt változata. https://eur-lex.europa.eu/resource.html?uri=cellar:2bf140bf-a3f8-4ab2-b506-fd71826e6da6.0007.02/DOC_2&format=PDF (Letöltés időpontja: 2019. 05. 09.)
[43] Az Európai Unióról szóló szerződés egységes szerkezetbe foglalt változata. https://eur-lex.europa.eu/resource.html?uri=cellar:2bf140bf-a3f8-4ab2-b506-fd71826e6da6.0007.02/DOC_1&format=PDF (Letöltés időpontja: 2019. 05. 09.)
[44] P7_TA(2012)0457 Kiberbiztonság és -védelem. 3. bek.
[45] Uo. 4. bek.
[46] Uo. 6. bek.
[47] Uo. 22. bek.

– a tagállamokat illetően:
  - ösztönzi a tagállamokat, hogy katonai struktúrájukon belül hozzanak létre külön kiberbiztonsági és kibervédelmi egységeket a más uniós tagállamokon belüli hasonló szervekkel történő együttműködés céljából;[48]
– a köz- és a magánszféra együttműködésére nézve;
– a nemzetközi együttműködés tekintetében, különös tekintettel a EU-nak a NATO-val[49] és az Amerikai Egyesült Államokkal[50] folytatott együttműködésére:
  - ösztönzi a kiberbiztonság területén a BRICS-országokkal és más, feltörekvő gazdasággal bíró országokkal az egyre elterjedtebb számítógépes bűnözésre, kiberfenyegetésre és számítógépes támadásokra adandó közös válaszok feltárásának céljával folytatott ismeretek cseréjét polgári és katonai szinten egyaránt;[51]
  - arra sürgeti az Európai Külügyi Szolgálatot és a Bizottságot, hogy a vonatkozó nemzetközi fórumok és szervezetek, nevezetesen az ENSZ, az EBESZ, az OECD és a Világbank keretében tanúsítson proaktív hozzáállást annak érdekében, hogy elérje a hatályos nemzetközi jog alkalmazását, valamint a kiberbiztonság és -védelem területén a felelős állami viselkedésre vonatkozó normákról szóló konszenzust, összehangolva a tagállamok álláspontjait azzal a céllal, hogy a kiberbiztonság és -védelem területén előmozdítsa az alapvető uniós értékeket és szakpolitikákat.[52]

ÖSSZEGZÉS

A kibervédelemi 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 definíciója, az állami és a nem állami szereplők által végzett tevékenységek formái, és a kezdeti konfúzió után letisztultak az információs és a kiberműveletek közti határok. Az információs és kommunikációs technológiai szektor és a rossz szándékú kiberműveletek rohamos terjedése és robbanásszerű fejlődése négy különböző, ugyanakkor összefüggő területen:

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 hatálybaléptetését;
2. együttműködés – ami egyenesen következik a kibertér globális, határokon átnyúló jellegéből, és 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,

[48] Uo. 27. bek.
[49] Uo. 49–51. bek.
[50] Uo. 52–55. bek.
[51] Uo. 45. bek.
[52] Uo. 46. bek.

valamint az, hogy a belső piac ez 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. (A tanulmány 2., befejező részét folyóiratunk 2019/5. számában közöljük.)

FELHASZNÁLT IRODALOM

390. sz. Eurobarométer különfelmérés a kiberbiztonságról, 2012. http://ec.europa.eu/commfrontoffice/publicopinion/index.cfm/Survey/getSurveyDetail/yearFrom/1974/yearTo/2012/surveyKy/1058

A Bizottság 2006. december 12-i közleménye a létfontosságú infrastruktúrák védelmére vonatkozó európai programról, COM(2006) 786. Az Európai Unió Hivatalos Lapja, C 126, 2007. 06. 07. https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=LEGISSUM:l33260&from=EN

Az Európai Közösségek Bizottsága, Brüsszel, 2005. 11. 17., COM(2005) 576. Zöld Könyv a létfontosságú infrastruktúrák védelmére vonatkozó európai programról. https://eur-lex.europa.eu/legal-content/GA/TXT/?uri=celex:52005DC0576

Az Európai Parlament és a Tanács 460/2004/EK rendelete (2004. 03. 10.) az Európai Hálózat- és Információbiztonsági Ügynökség létrehozásáról. Hivatalos Lap L 077, 13. 03. 2004. o. 0001 – 0011. https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:32004R0460&from=EN

Az Európai Unió működéséről szóló szerződés egységes szerkezetbe foglalt változata. https://eur-lex.europa.eu/resource.html?uri=cellar:2bf140bf-a3f8-4ab2-b506-fd71826e6da6.0007.02/DOC_2&format=PDF

Az Európai Unióról szóló szerződés egységes szerkezetbe foglalt változata. https://eur-lex.europa.eu/resource.html?uri=cellar:2bf140bf-a3f8-4ab2-b506-fd71826e6da6.0007.02/DOC_1&format=PDF

Commission of the European Communities, Brussels, 06. 06. 2001., (COM(2001) 298), Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of Regions, Network and Information Security: Proposal for A European Policy Approach. https://ccdcoe.org/sites/default/files/documents/EU-010606-NISProposal.pdf

Communication from the Commission of 31 May 2006: A strategy for a Secure Information Society – Dialogue, partnership and empowerment COM(2006) 251. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM%3Al24153a

Communication from the Commission to the Council and the European Parliament, Tackling Crime in our Digital Age: Establishing a European Cybercrime Centre /* COM/2012/0140 final */. https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=celex:52012DC0140

Communication from the Commission to the European Parliament and the Council – Internet governance: the next steps. Az Európai Közösségek Bizottsága, Brüsszel, 2009. 06. 18., COM(2009) 277. https://eur-lex.europa.eu/legal-content/HU/ALL/?uri=CELEX:52009DC0277

Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Critical Information Infrastructure Protection. 'Achievements and next steps: towards global cyber-security' COM(2011) 163. https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:52011DC0163&from=EN

Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Critical Information Infrastructure Protection. „Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience" {SEC(2009) 399} {SEC(2009) 400} COM/2009/0149. https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:52009DC0149&from=EN

Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions European Strategy for a Better Internet for Children. European Commission, Brussels, 02. 05. 2012., COM(2012) 196 final. https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0196:FIN:EN:PDF

Convention on Cybercrime, Council of Europe, European Treaty Series No. 185.

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/HU/TXT/HTML/?uri=CELEX:32009G1229(01)&from=EN

Council Resolution of 18 February 2003 on a European approach towards a culture of network and information security. Official Journal C 048, 28. 02. 2003. P. 0001 – 0002. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32003G0228%2801%29

Council Resolution of 22 March 2007 on a Strategy for a Secure Information Society in Europe (2007/C 68/01) https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:32007G0324(01)&from=EN

Council Resolution of 28 January 2002 on a common approach and specific actions in the area of network and information security. Official Journal C 043, 16. 02. 2002. P. 0002 – 0004. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32002G0216%2802%29

Critical infrastructure protection. Communication from the Commission to the Council and the European Parliament of 20 October 2004 – Critical Infrastructure Protection in the fight against terrorism COM(2004) 702. https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=LEGISSUM:l33259

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 (Framework Directive). Official Journal L 108, 24. 04. 2002. P. 0033 – 0050. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32002L0021&from=en

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 (Directive on privacy and electronic communications). Official Journal L 201, 31. 07. 2002. P. 0037 – 0047. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32002L0058&from=EN

Directive 2009/140/EC of the European Parliament and of the Council of 25 November 2009 amending Directives 2002/21/EC on a common regulatory framework for electronic communications networks and services, 2002/19/EC on access to, and interconnection of, electronic communications networks and associated facilities, and 2002/20/EC on the authorisation of electronic communications networks and services. https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0037:0069:HU:PDF

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Official Journal L 281, 23. 11. 1995. P. 0031 – 0050. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:31995L0046&from=en

Directive on Security of Network and Information Systems/NIS Directive. Az Európai Unió és a Tanács (EU) 2016/1148 Irányelve (2016. 06. 06.) a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről. Az Európai Unió Hivatalos

Lapja, L 194/1, 2016. 07. 19. https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:32016L1148&from=EN

Európai Bizottság, Brüsszel, 2010. 09. 30., COM(2010) 521, 2010/0275 (COD). Javaslat: Az Európai Parlament és a Tanács Rendelete az Európai Hálózat- és Információbiztonsági Ügynökségről (ENISA) {SEC(2010) 1126}{SEC(2010) 1127} https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:52010PC0521&from=EN

European Commission, MEMO, Brussels, 05. 12. 2012., Declaration on the Launch of the Global Alliance against child sexual abuse online. http://europa.eu/rapid/press-release_MEMO-12-944_en.htm

Opinion of the European Economic and Social Committee on the 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Critical Information Infrastructure Protection. Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience. COM(2009) 149, 22. 09. 2010. HU. Az Európai Unió Hivatalos Lapja, C 255/98. https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX:52009AE1948

P7_TA(2012)0457 Kiberbiztonság és -védelem. Az Európai Parlament 2012. november 22-i állásfoglalása a kiberbiztonságról és -védelemről (2012/2096(INI)) (2015/C 419/22). Az Európai Unió Hivatalos Lapja, C 419/145, 2015. 12. 16. https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX%3A52012IP0457

Presidency Conclusions of the Ministerial Conference on Critical Information Infrastructure Protection, Tallin (EE).

Regulation (EC) No 1007/2008 Of the European Parliament and of the Council of 24 September 2008 amending Regulation (EC) No 460/2004 establishing the European Network and Information Security Agency as regards its duration. https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:293:0001:0002:EN:PDF

Regulation (EU) No 580/2011 of the European Parliament and of the Council of 8 June 2011 amending Regulation (EC) No 460/2004 establishing the European Network and Information Security Agency as regards its duration. https://www.enisa.europa.eu/media/news-items/extension-of-enisa2019s-mandate-published-1

https://ec.europa.eu/home-affairs/content/european-programme-critical-infrastructure-protection-epcip_en

https://ec.europa.eu/home-affairs/what-we-do/networks/critical_infrastructure_warning_information_network_en

https://erncip-project.jrc.ec.europa.eu/

https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0245:FIN:HU:PDF