DERES PETRONELLA

Kiberbiztonság, kiberbűnözés – Helyzetkép a Covid–19-pandémia időszakából

A tanulmány megkísérli vázolni a kiberbiztonság és kiberbűnözés aktuális nemzetközi, európai fejleményeit: tárgyalja az Európai Bizottság biztonsági unióra vonatkozó új stratégiája alapján meghatározott legújabb irányvonalakat, a teljesség igénye nélkül áttekinti a pandémiás időszak főbb mérföldköveit a kiberbűnözés elleni küzdelem terén, ismerteti a budapesti egyezmény második kiegészítő jegyzőkönyvének rendelkezéseit, érintve a 2021. évi Octopus-konferencia, továbbá az Internet Organised Crime Threat Assessment (IOCTA) 2021. évre vonatkozó egyes megállapításait.

Európai Unió – A biztonsági unió stratégiája

Az Európai Bizottság a 2020 és 2025 közötti időszakra a *biztonsági unióra* vonatkozó új stratégiát terjesztett elő.[1] A stratégia *meghatározza azokat az eszközöket és intézkedéseket,* amelyeket a következő öt évben kell kidolgozni fizikai és digitális környezetünk biztonságának garantálása érdekében.

Kiemelt területek:
- a *terrorizmus és a szervezett bűnözés* elleni küzdelem;
- *a kiberbűnözés* és a hibrid fenyegetések megelőzése és felderítése;
- a *kritikus infrastruktúrák védelme és rezilienciájának növelése,* a *kiberbiztonság* előmozdítása;
- a kutatások és innovációk támogatása.

A stratégia az uniós szintű fellépés négy stratégiai prioritását határozza meg:[2]

1) *Időtálló biztonsági környezet*
   A kritikus infrastruktúrák, továbbá a nyilvános terek védelme, kiberbiztonság, a drónokra vonatkozó szabályozás, intézkedések.

[1] European Commission: Communication from the Commission on the EU Security Union Strategy. COM(2020) 605 final. Brussels, 24.7.2020. https://eur-lex.europa.eu/legal-content/EN/-TXT/?qid=1596452256370&uri=CELEX:52020DC0605

[2] https://ec.europa.eu/info/strategy/priorities-2019-2024/promoting-our-european-way-life/european-security-union_hu

2) *A változó fenyegetések kezelése*
   Kiberbűnözés, továbbá a hibrid fenyegetések elleni küzdelem, korszerű bűnüldözés, a jogellenes online tartalmak elleni küzdelem.
3) *Az európaiak védelme a terrorizmussal és a szervezett bűnözéssel szemben*
   A radikalizálódás elleni küzdelemhez (korai felismerés, rezilienciaépítés és kivonulás, valamint rehabilitáció és a társadalomba való visszailleszkedés) illeszkednek a határbiztonsági jogszabályok megerősítését és a meglévő adatbázisok jobb felhasználását célzó lépések. A nemzetközi szervezetekkel és az unión kívüli országokkal való együttműködés szintén kulcsfontosságú a terrorizmus elleni küzdelemben, például a terrorizmusfinanszírozás valamennyi forrásának felszámolása érdekében.[3]
4) *Erős biztonsági ökoszisztéma*
   A kormányoknak, a bűnüldöző hatóságoknak, a vállalkozásoknak, a szociális szervezeteknek és az Európában élő polgároknak közös felelősségük a biztonság erősítése.

A készségek és a fokozott tudatosság mind a bűnüldözés, mind a polgárok számára előnyös lehet. Még a biztonsági fenyegetésekre és az ellenük való küzdelem módjára vonatkozó alapvető ismeretek is érzékelhető hatást gyakorolhatnak a társadalom rezilienciájára.

A szolgáltatók általi a kibertámadások leküzdéséhez biztosított védelem mellett szükség van a kiberbűnözés kockázataival kapcsolatos tudatosság növelésére és a kibertámadásokkal szembeni védelemhez szükséges alapkészségek elsajátítására is.

[3] A szervezett bűnözés és kiberbűncselekmények kapcsolatáról lásd részletesen Gyaraki Réka: A kiberbűncselekmények megjelenése és helyzete napjainkban – Különös tekintettel a szervezett bűnözéssel kapcsolatos kérdésekre. In: *A bűnügyi tudományok és az informatika.* PTE ÁJK–MTA TK, Pécs–Budapest, 2019, 83–103. o. A kiberterrorizmus jelenségével, a kiberterrorista magatartások büntetőjogi megítélésének vizsgálatával részletesen foglalkozik Bőczné Neparáczki Anna Viktória: A kiberterrorizmus büntető anyagi jogi megítélése. *Ügyészek Lapja,* 2020/1., 71–85. o.; illetve Dornfeld László: Kiberterrorizmus – A jövő terrorizmusa? In: Mezei Kitti (szerk.): *A bűnügyi tudományok és az informatika.* PTE ÁJK–MTA TK, Budapest–Pécs, 2019, 46–63. o.; valamint Szabó Imre: Az informatikai terrorizmus veszélyei. *Belügyi Szemle,* 2011/2., 5–20. o.

Főbb mérföldkövek a kiberbűnözés elleni küzdelem terén a Covid–19-pandémia alatt (2019–2021)

„A jövőben minden bűncselekménynek lesz információtechnológiai vonzata."
(Octopus-konferencia, 2019)[4]

Alapvetések

Az Európai Unióban jelenleg több mint tízmilliárd (2024-re kb. 22 milliárd) összekapcsolt digitális eszköz van (*„Internet of Things"*: dolgok, avagy eszközök internete). A mai információs[5] és kommunikációs technológiai rendszerek ugyanakkor súlyos károkat szenvedhetnek biztonsági események (például üzemzavarok, vírusok) miatt.[6] A kibertámadások becslések szerint éves szinten ma már évi 600 milliárd dolláros kárt okoznak globálisan (2014-ben ez 445 milliárd dollár volt).[7] Az elmúlt évek tapasztalatai alapján minden szinten szorosabb együttműködésre van szükség a biztonság terén.

A 2020-ban kirobbant *koronavírus okozta válság* az európai biztonságot is előtérbe helyezte:

- tesztelte Európa kritikus infrastruktúrájának ellenálló képességét;
- a válsághelyzetekre való felkészültséget; és
- a válságkezelési rendszereket.

A pandémia alatt megsokasodtak az egészségügyi intézmények elleni kibertámadások[8], e jelenség is megmutatta, mennyire fontos az infrastruktúrák vé-

[4] Octopus 2019: Cooperation against Cybercrime, 20–22 November 2019, Council of Europe, Strasbourg, France. https://www.coe.int/en/web/cybercrime/octopus-interface-2019

[5] Az információs társadalomról lásd bővebben Jobbágy Szabolcs: Az információs társadalom, az informatika és a távközlés konvergenciája. Múlt, jelen, jövő. *Hadmérnök*, 2009/1., 184–196. o.

[6] Simon Béla: Az EU rendészeti szerveinek együttműködése a kiberbűnözés ellen. *Nemzetbiztonsági Szemle*, 2018/4., 21–47. o.

[7] James Lewis: *Economic Impact of Cybercrime – No Slowing Down.* CSIS, 2018. https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/economic-impact-cybercrime.pdf

[8] 2020 őszén Németországban következett be az első olyan dokumentált klinikai ellátási esemény, amely halálos kimenetellel járt, és közvetlen összefüggésbe hozható egy zsarolóvírus-támadással. A Düsseldorfi Egyetemi Kórházat egy DoppelPaymer zsarolóvírussal támadták meg. A ransomware-t használó, nem egészségügyi szektorra specializálódott kiberbűnözői csoport eredetileg az egyetemet szándékozott megtámadni, azonban „félrement" a támadás, amely miatt 2020. szeptember 11-én leállt az egyetemi kórház sürgősségi osztálya. A beérkező kritikus állapotú beteget a leállás miatt a harminckét kilométerre levő wuppertali kórházba kellett volna szállítani, ami az azonnali ellátást egy órával késleltette, ezt a beteg már nem élte túl. A haláleset miatt ismeretlen tettes ellen nyomozást indítottak a német hatóságok. Lásd

delme.[9] Ez is fontos szerepet játszott abban, hogy amikor az Európai Unió 2020 decemberében a digitális tér átfogó megújítására hirdetett programot, akkor a programcsomag két jogszabálytervezete (a digitális szolgáltatásokról[10] és a digitális piacról[11]) mellett átfogó koncepciót terjesztett elő a mind veszélyeztetettebbnek számító kiberdomén hatékony védelmére is.[12]

Néhány mérföldkő az elmúlt három évből (2019–2021)

Az Európai Tanács *2019. április 17-én* rendeletként elfogadta az úgynevezett *kiberbiztonsági jogszabályt (Cybersecurity Act)*[13], amely többek között bevezeti az Európai Uniós Kiberbiztonsági Ügynökséget, amely bővített hatáskörrel átveszi a jelenlegi Európai Hálózat- és Információbiztonsági Ügynökség (ENISA) szerepét.

Az Európai Tanács *2019. május 17-én* létrehozta azt *a jogszabályi keretet* (KKBP-határozat és EU tanácsi rendelet)[14], amely lehetővé teszi az Európai Unió számára, hogy célzott korlátozó intézkedéseket vezessen be az olyan kibertámadásoktól való elrettentés és az azokra való reagálás érdekében, amelyek külső fenyegetést jelentenek az EU vagy annak tagállamai számára, beleértve a harmadik államok vagy nemzetközi szervezetek ellen irányuló kibertámadásokat is. A határozat a rossz szándékú és szándékos kibertevékenységekkel szembeni közös uniós korlátozó intézkedések alkalmazhatóságáról dönt, a rendelet pedig a jelentős hatású kibertámadások esetén szankciók alkalmazását teszi lehetővé az EU részéről.

---

erről: Palicz Tamás – Bencsik Balázs – Szócska Miklós: Kiberbiztonság a koronavírus idején – a COVID–19 nemzetbiztonsági aspektusai. *Scientia et Securitas,* 2021/2., 84. o.

[9] Nyáry Gábor: A digitális tér átfogó megújítására hirdetett programot az EU. *Ludovika cyberblog,* 2020. december 18. https://www.ludovika.hu/blogok/cyberblog/2020/12/18/a-digitalis-ter-atfogo-megujitasara-hirdetett-programot-az-eu/

[10] https://ec.europa.eu/commission/presscorner/detail/hu/QANDA_20_2349

[11] https://ec.europa.eu/commission/presscorner/detail/en/QANDA_20_2348

[12] https://hirlevel.egov.hu/2021/03/29/a-heten-olvastuk-kiberbiztonsag-2021-marcius-29/

[13] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU). No 526/2013. Official Journal of the European Union, 7.6.2019, L 151/15–69. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0881&from=EN

[14] A tanács 2019/796 határozata az uniót vagy annak tagállamait fenyegető kibertámadások elleni korlátozó intézkedésekről. https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=uriserv:OJ.LI.2019.129.01.0001.01.HUN&toc=OJ:L:2019:129I:TOC; a Tanács 2019/796 rendelete az uniót vagy annak tagállamait fenyegető kibertámadások elleni korlátozó intézkedésekről. https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=uriserv:OJ.LI.2019.129.01.0001.01.HUN-&toc=OJ:L:2019:129I:TOC

Ez a jogszabályi keret most első alkalommal teszi lehetővé az EU számára, hogy szankciókat vessen ki

- olyan személyekre vagy szervezetekre, akik, illetve amelyek kibertámadásokért vagy megkísérelt kibertámadásokért felelősek;
- akik, illetve amelyek pénzügyi, technikai vagy anyagi támogatást nyújtanak ilyen támadásokhoz;
- vagy akik, illetve amelyek azokban egyéb módokon működnek közre.

Szankciók vethetők ki továbbá az ilyen személyekkel és szervezetekkel kapcsolatban álló személyekre és szervezetekre is.

A korlátozó intézkedések személyek esetében az EU-ba való *beutazási tilalma*t, illetve személyek és szervezetek esetében egyaránt *vagyonieszköz-befagyasztás*t foglalnak magukban. Emellett *uniós személyeknek és szervezeteknek tilos pénzeszközöket* a jegyzékbe vett személyek és szervezetek *rendelkezésére bocsátani* (például WannaCry, NotPetya, Operation Cloud Hopper néven ismert támadások).

Az Európai Bizottság európai digitális átalakulást szorgalmaz az unióban. *2020. február 19-én* a testület három dokumentumban tette közzé az adatkezeléssel és a mesterséges intelligenciával kapcsolatos stratégiáját:

- *Shaping Europe's Digital Future* (Európa digitális jövőjének megtervezése)[15];
- *A European Strategy for Data* (Európai adatstratégia)[16];
- *White Paper on Artificial Intelligence – A European approach to excellence and trust* (Fehér könyv a mesterséges intelligenciáról: a kiválóság és a bizalom európai megközelítése)[17].

Az Európai Uniós Kiberbiztonsági Ügynökség (ENISA) *2020 áprilisában* tette közzé *Ütemterv a számítógépbiztonsági-incidenskezelő csoportok és a bűnüldöző, igazságszolgáltatási szervek közötti együttműködéshez*[18] című dokumentumát.

---

[15] https://ec.europa.eu/info/sites/default/files/communication-shaping-europes-digital-future-feb-2020_en_4.pdf

[16] https://eur-lex.europa.eu/legal-content/HU/TXT/?qid=1593073685620&uri=CELEX%3A520-20D-C0066

[17] https://ec.europa.eu/commission/future-europe/white-paper-future-europe-and-way-forward_hu

[18] Roadmap on the cooperation between CSIRTS and LE. https://www.enisa.europa.eu/publications/support-the-fight-against-cybercrime-roadmap-on-csirt-le-cooperation/@@download/-fullReport; továbbá ehhez kapcsolódóan: An overview on enhancing technical cooperation between CSIRTs and LE. https://www.enisa.europa.eu/publications/support-the-fight-against-cybercrime-tools-for-enhancing-cooperation-between-csirts-and-le/@@download/fullReport. Minderről lásd bővebben Deres Petronella: Digitális tér – Kiberbűnözés. Aktuális helyzetkép. In: Vókó György (szerk.): *Kriminológiai Tanulmányok 58*. OKRI, Budapest, 2021, 63–64. o.

Az uniós vezetők az Európai Tanács *2020. októberi* rendkívüli ülésén a digitális transzformáció kérdésével is foglalkoztak. A digitalizáció egyike a Covid–19-válság utáni uniós helyreállítás két fő pillérének, kulcsszerepe van a növekedés új formáinak előmozdításában és az EU rezilienciájának erősítésében.

Az unió számos olyan szakpolitika kialakításán dolgozik, amelyek hozzájárulnak a digitális transzformációhoz, ezek közül témánk szempontjából kettő kiemelésre méltó:

- az uniós vezetők rámutattak arra, hogy javítani kell az EU azon képességét, hogy megvédje magát a kiberfenyegetésekkel szemben, s ehhez igazságszolgáltatási és bűnüldözési célokból biztosítsa az adatokhoz való hozzáférést;
- biztonságos kommunikációs környezetet kell teremteni; mivel egyre több bűnöző használ fel technológiát a bűncselekmények megtervezéséhez és elkövetéséhez, így a bűnüldözés során a hatóságok is egyre nagyobb mértékben hagyatkoznak az elektronikus bizonyítékokra.

Az igazságszolgáltatás digitalizációja

Az igazságszolgáltatás digitalizációja arra irányul, hogy könnyebbé váljon az igazságszolgáltatás igénybevétele, javuljon az igazságszolgáltatás hatékonysága, és az igazságszolgáltatási rendszerek reziliensebbé váljanak az olyan válságok idején, mint például a Covid–19-világjárvány.

A tanács rámutatott arra, hogy jelenleg is folyamatban vannak a mesterséges intelligenciának az igazságügyi ágazatban való alkalmazásával kapcsolatos kutatások és fejlesztések, és elismeri, hogy az javíthatja az igazságszolgáltatási rendszerek működését.

A tagállamokat ösztönözni kell arra, hogy a bírósági eljárások során alkalmazzanak nagyobb mértékben digitális eszközöket; az igazságszolgáltatási ágazatban fejleszteni kell a digitális készségeket, hogy a bírák, ügyészek, igazságügyi alkalmazottak és más igazságszolgáltatási szakemberek hatékonyan, ugyanakkor az igazságszolgáltatási szervekhez fordulók jogait és szabadságait kellő tiszteletben tartva tudják használni a digitális eszközöket.

Néhány uniós tagállam már megkezdte a digitális eszközök alkalmazását az igazságszolgáltatás területén, például a következőket:

- digitális bírósági eljárások lefolytatása;
- elektronikus kommunikáció a felek között;
- okmányok elektronikus továbbítása;

– videókapcsolat révén lefolytatott meghallgatás és videokonferencia alkalmazása.[19]

Az e-CODEX-rendszer (e-igazságügyi kommunikáció online adatcsere révén) egy olyan digitális technológiai megoldás, amely lehetővé teszi a bíróságok közötti határokon átnyúló kommunikáció korszerűsítését.[20] 2021. december 8-án a tanács elnöksége és az Európai Parlament ideiglenes megállapodásra jutott az e-CODEX-rendszerről szóló rendeletjavaslatra vonatkozóan.

Az Európai Bizottság és az Európai Külügyi Szolgálat *2020 decemberében új uniós kiberbiztonsági stratégiát* terjesztett elő. A stratégia célja, hogy megerősödjön Európa kiberfenyegetésekkel szembeni kollektív ellenálló képessége, valamint hogy minden polgár és vállalkozás megbízható szolgáltatásokat és digitális eszközöket vehessen igénybe, és ezek előnyeit teljes mértékben ki tudja használni. A dokumentum három területen konkrét intézkedési javaslatokat is megfogalmaz:

– Reziliencia, technológiai szuverenitás és vezető szerep.
– Operatív kapacitás kiépítése: a megelőzés, elrettentés és reagálás elősegítése.
– A globális és nyitott kibertér kiépülésének és működésének támogatása.

2021. március 22-én a tanács úgynevezett Következtetésekben *(Conclusion)* foglalta össze álláspontját az új kiberbiztonsági stratégiáról.[21] A dokumentum kijelöl bizonyos intézkedési területeket, és azokkal kapcsolatban megbízást ad egy másik uniós testületnek (az Európai Bizottságnak, továbbá a kül- és biztonságpolitikai főmegbízottnak) arra, hogy direkt szakpolitikai intézkedési terve-

[19] A tanács a bizonyításfelvételre, illetve az iratkézbesítésre vonatkozó két átdolgozott rendeletet fogadott el, amelyek célja a hatóságok közötti, határokon átnyúló információcsere javítása a digitalizáció révén. Az új szabályok célja annak ösztönzése is, hogy a bizonyításfelvétel során gyakrabban alkalmazzanak videókonferenciát vagy más távközlési technológiát, hogy ezáltal valamely másik tagállamban tartózkodó tanútól, féltől vagy szakértőtől is lehessen meghallgatás útján bizonyítékot felvenni. https://www.consilium.europa.eu/hu/press/press-releases/2020/11/04/digital-europe-council-adopts-new-rules-to-modernise-judicial-cooperation-in-taking-of-evidence-and-service-of-documents/

[20] Az e-CODEX-rendszer különböző szoftverösszetevőkből álló csomag, amely lehetővé teszi a nemzeti rendszerek egymással való összekapcsolását; segítségével a felhasználók (vagyis az illetékes igazságügyi hatóságok, a gyakorló jogászok és a polgárok) a dokumentumokat, jogi űrlapokat, bizonyítékokat és egyéb információkat gyorsan és biztonságosan, elektronikus úton küldhetik el, illetve fogadhatják. Az e-CODEX már most is megteremti a hátteret az elektronikus bizonyítékok digitális cseréjére szolgáló rendszerhez, valamint támogatja az európai nyomozási határozatokkal és a büntetőügyekben folytatott igazságügyi együttműködés területén nyújtott kölcsönös jogsegéllyel kapcsolatos információcserét.

[21] A tanács következtetései a digitális évtizedre vonatkozó uniós kiberbiztonsági stratégiáról. https://data.consilium.europa.eu/doc/document/ST-6722-2021-INIT/hu/pdf

ket dolgozzon ki, konkrétan kiemelve a következő évekre vonatkozó cselekvési területeket, ahová a kiberbiztonság európai megerősítését célzó fejlesztéseknek koncentrálniuk kell. Ezek, többek között[22]:

- úgynevezett *biztonsági műveleti központok hálózatának* létrehozása EU-szerte a hálózatok elleni támadásokra utaló jelek nyomon követésére és előre jelzésére;
- *közös kiberbiztonsági egység* kialakítása;
- az *uniós 5G eszköztár* intézkedéseinek alkalmazása és végrehajtásának gyors befejezése;
- az *erős titkosítás fejlesztésének* támogatása, ezáltal annak biztosítása, hogy a bűnüldöző és igazságügyi hatóságok – akár online, akár offline – gyakorolni tudják hatásköreiket;
- a *kiberdiplomáciai eszköztár* hatékonyságának és eredményességének növelése (a rendszerszintű hatású kibertámadások megelőzése és leküzdése érdekében);
- *kiberhírszerzéssel foglalkozó munkacsoport* létrehozása az EU általános célú hírszerző szervezetének (EU INTCENT) megerősítésére;
- a nemzetközi szervezetekkel és a partnerországokkal folytatott *együttműködés megerősítése* e területen.

2021. április 20-án a tanács zöld jelzést adott a bukaresti székhelyű Kiberbiztonsági Kompetenciaközpont létrehozására.[23]

2021. április 29-én nem hivatalos megállapodás született az Európai Parlamentben az ideiglenes szabályokról a gyermekek online zaklatása elleni küzdelem terén.

2021. május 17-én a kibertámadásokat illetően a tanács további egy évvel meghosszabbította a már említett, *2019. május 17-én* létrehozott szankciós keretet.

2021. október 19-én a tanács Következtetéseket fogadott el a közös kiberbiztonsági egységben rejlő lehetőségek feltárásáról.

A tanács *2021. december 3-án* megállapodott az új kiberbiztonsági irányelvre vonatkozó álláspontjáról: elfogadta az EU egész területén egységesen kimagasló szintű kiberbiztonságot biztosító intézkedésekkel kapcsolatos álláspontját. Az intézkedések célja, hogy tovább javuljon az állami és a magánszektor mel-

[22] https://www.consilium.europa.eu/hu/press/press-releases/2021/03/22/cybersecurity-council-adopts-conclusions-on-the-eu-s-cybersecurity-strategy/

[23] Európai Kiberbiztonsági Ipari, Technológiai és Kutatási Kompetenciaközpont (ECCC); https://www.consilium.europa.eu/hu/policies/cybersecurity/seat-selection-cybersecurity-centre/

lett az unió egészének kiberrezilienciája és a kiberbiztonsági eseményekre való reagálási képessége.[24]

A javaslat alapján – annak elfogadása után – az új, NIS 2-irányelv[25] lép a jelenlegi, a hálózati és információs rendszerek biztonságáról szóló NIS-irányelv helyébe. E módosított irányelv célja, hogy megszüntesse a kiberbiztonsági követelmények és a kiberbiztonsági intézkedések végrehajtása terén a különböző tagállamok között fennálló eltéréseket. Az új irányelv kapcsán kiemelendő, hogy létrehozzák az Európai Kiberválságügyi Kapcsolattartó Szervezetek Hálózatát (EU-CyCLONe), amely összehangolja a nagyszabású kiberbiztonsági események kezelését.

Az Európai Unió jelenleg dolgozza ki az *elektronikus bizonyítékok könnyebb és gyorsabb elérését lehetővé tevő új szabályokat*. Ennek előzményeként, az uniós tagállamok miniszterei már 2019 októberében egy olyan, az Europol égisze alatt létrehozandó innovációs laboratórium megalapításáról tárgyaltak, amely figyelemmel kísérné az új technológiai fejleményeket és ösztönözné az innovációt a belső biztonság területén.

A szabályozás két jogalkotási javaslatból tevődik össze: 1) egy rendeletből, amely a büntetőügybeli elektronikus bizonyítékokra vonatkozó, közlésre és megőrzésre kötelező európai határozatokról szól, s amelynek célja, hogy gyorsabban hozzá lehessen jutni az elektronikus bizonyítékokhoz, függetlenül attól, hogy az adatokat hol tárolják; és 2) egy irányelvből, amely jogi képviselők kinevezésére kötelezné a nem az Európai Unióban letelepedett, de ott szolgáltatásokat nyújtó szolgáltatókat; e képviselők feladatkörébe a határozatok átvétele, az azoknak való megfelelés és azok végrehajtása tartozna.

Az EU a jelenlegi és jövőbeli online és offline kockázatok kezelése érdekében további két jogszabály megalkotásán fáradozik: a hálózati és információs rendszerek hatékonyabb védelmét szolgáló aktualizált irányelven, valamint a kritikus fontosságú szervezetek rezilienciájáról szóló új irányelven.

[24] Javaslat – Az Európai Parlament és a Tanács irányelve az unió egész területén egységesen magas szintű kiberbiztonságot biztosító intézkedésekről, valamint az (EU) 2016/1148 irányelv hatályon kívül helyezéséről – Általános megközelítés. https://data.consilium.europa.eu/doc-/document/ST-14337-2021-INIT/hu/pdf

[25] A NIS 2-irányelv meghatározza a kiberbiztonságikockázat-kezelési intézkedések és bejelentési kötelezettségek alapját az irányelv hatálya alá tartozó valamennyi ágazatra nézve, így az energiaügy, a közlekedés, az egészségügy és a digitális infrastruktúra területén.

A számítástechnikai bűnözésről szóló budapesti egyezményhez csatolt második kiegészítő jegyzőkönyv

Összefoglalás a budapesti egyezményről[26]

Az egyezményt jelenleg 66 ország ratifikálta. Az egyezmény célja

1) a számítógépes bűnözéssel kapcsolatos nemzeti jogszabályok összehangolása;
2) e bűncselekmények kivizsgálásának támogatása; és
3) a nemzetközi együttműködés erősítése a számítógépes bűnözés elleni küzdelemben.

Az egyezmény modellként szolgál a kiberbűnözéssel kapcsolatos nemzeti jogszabályok megfogalmazásához, és a nemzetközi együttműködés bázisát biztosítja e területen (komplexen kezelve az anyagi, az eljárásjogi és a nemzetközi büntetőjogi kérdéseket).

Az egyezmény bűncselekményi tipológiája:

- Számítástechnikai rendszer és számítástechnikai adat hozzáférhetősége, sértetlensége és titkossága elleni bűncselekmények (jogosulatlan belépés; számítástechnikai adat, számítástechnikai rendszer megsértése, eszközökkel való visszaélés).
- Számítógéppel kapcsolatos bűncselekmények (számítógéppel kapcsolatos hamisítás, illetve csalás).
- Számítástechnikai adatok tartalmával kapcsolatos bűncselekmények (gyermekpornográfiával kapcsolatos bűncselekmények).
- Szerzői vagy szomszédos jogok megsértésével kapcsolatos bűncselekmények.
- Számítástechnikai rendszerek útján megvalósított rasszista és idegengyűlölő cselekmények.

Az egyezmény nem tartalmazott azonban több más „kiberténnyállást", így például a személyiség-/személyazonosság-lopást, a groomingot, a kiberterrorizmust.

Az egyezmény a számítógépes bűncselekményekkel kapcsolatos nemzetközi szabályozás egyik kiindulópontja, folyamatos fejlesztés alatt áll, az Európa Tanács számos útmutatót adott ki az egyes szakaszok értelmezésével kapcsolatban.[27]

[26] 2004. évi LXXIX. törvény az Európa Tanács Budapesten, 2001. november 23-án kelt Számítástechnikai Bűnözésről szóló Egyezményének (a továbbiakban: egyezmény) kihirdetéséről. *Magyar Közlöny,* 11064–11096. o.

[27] Lásd továbbá Krasznay Csaba: Húsz év a globális kiberbűnözés elleni küzdelemben – A Budapesti Egyezmény értékelése. *Külügyi Szemle,* 20. (Különszám), 2021, 211. o.

Az első kiegészítő jegyzőkönyv

Az egyezmény első kiegészítő jegyzőkönyve a számítástechnikai rendszerek útján megvalósított rasszista és idegengyűlölő cselekmények büntetendővé nyilvánításáról szól.[28] Az egyezmény kiegészítő jegyzőkönyve kriminalizálja a rasszista és faji megkülönböztetést, a bántalmazást, valamint a népirtás és az emberiesség elleni bűncselekmények tagadását, következményeinek minimalizálását, elfogadását, illetve támogatását.[29]

A második kiegészítő jegyzőkönyv

Az Európa Tanács 2017 szeptemberében megkezdte a számítástechnikai bűnözésről szóló budapesti egyezmény *második kiegészítő jegyzőkönyvének kidolgozását*.[30] A jegyzőkönyv célja, hogy meghatározza

- a hatékonyabb kölcsönös bűnügyi jogsegély-mechanizmusra irányuló rendelkezéseket;
- az egyezmény egyéb részes államainak szolgáltatóival való közvetlen együttműködésre vonatkozó rendelkezéseket;
- a lekérdezések határokon átnyúló kiterjesztésére vonatkozó keretet és biztosítékokat.

A jegyzőkönyv szigorú biztosítékokat és adatvédelmi követelményeket foglal magában. Egy ilyen megállapodás előnye abban rejlik, hogy *az egész világon alkalmazható lehet.*

A budapesti egyezmény az internethasználat nagymértékű növekedése, a felhőalapú számítástechnika fejlődése és az interakciók szinte minden formájának digitalizálódása előtt íródott (amikor a bűnügyi nyomozás szempontjából kritikus digitális [és egyéb] bizonyítékok túlnyomó többsége saját területi határokon belül volt). Ezek a változások az elektronikus bizonyítékokat szinte minden bűncselekmény számára fontossá tették – ebből a szempontból az összes bűnözést kiberbűnözéssé változtatták, és óriási feladatok elé is állították a bűnüldözést, többek között az internet globális jellegére figyelemmel. A bűncselekmények nyomozásához, a büntetőeljárás megindításához kapcsolódó és

[28] https://rm.coe.int/168008160f

[29] Sorbán Kinga: Az informatikai bűncselekmények elleni fellépés nemzetközi dimenziói. *Themis*, 2015/6., 16. o.

[30] Előzmények: 2012-ben a feladatok elismeréseként munkacsoportot hoztak létre a kérdések megvizsgálására, a csoport átalakult az úgynevezett „Cloud Evidence Group"-ba, amely kiegészítés elfogadását javasolta egy második kiegészítő jegyzőkönyv formájában. A tárgyalások 2017 szeptemberében kezdődtek, amelyek eredményeként öt ideiglenes rendelkezésszöveget készítettek, amelyek célja a nehézségek kezelése.

ezek szempontjából kardinális számos elektronikus bizonyítékot egyre több esetben – az egyes elkövetők azonosítására használt alapvető előfizetői információktól kezdve az e-mailek tartalmáig – egy másik országban tárolnak vagy vizsgálnak, mint ahol a bűncselekményt elkövették. A bizonyítékok globalizációja tehát jelentős feladatok elé állítja bűnüldözést.

A Budapesti Egyezmény Bizottság – e jelenségre válaszul – egy második jegyzőkönyvet javasolt a budapesti egyezményhez, amelynek célja többek között a már említett nehézségek kezelése. A bizottság az elmúlt évek során öt rendelkezés ideiglenes szövegét ismertette. (Ezekről a rendelkezésekről több vitát folytattak, többek között a 2019. novemberi Octopus-konferencián[31].)

Az Európai Bizottság 2018-as jelentése megállapította, hogy *„az összes vizsgálat több mint fele határokon átnyúló kérelmet tartalmaz az [elektronikus] bizonyítékokhoz való hozzáférésről"*[32]. Az államok területi joghatósága és az adatok országhatárokon át történő mozgásának és tárolásának módjai jelentős nehézségeket jelentenek a bűnüldözés számára, előfordul, hogy a bűnüldöző szervek nem is tudhatják, hol található az adat vagy az adatok birtokában lévő és ellenőrző entitás – és így fogalmuk sincs arról, hogy hová kell fordulniuk a kérés benyújtásához[33].

Amint az a biztonsági unióra vonatkozó 2020. évi uniós stratégiában, a digitális évtizedre vonatkozó 2020. évi uniós kiberbiztonsági stratégiában és a szervezett bűnözésre vonatkozó 2021. évi uniós stratégiában is szerepel, a bizottság elkötelezte magát a jegyzőkönyvről folytatott tárgyalások gyors és sikeres lezárása mellett. Az Európai Parlament a digitális évtizedre vonatkozó uniós kiberbiztonsági stratégiáról szóló 2021. évi állásfoglalásában szintén elismerte, hogy le kell zárni a jegyzőkönyvvel kapcsolatos munkát.

Az Európai Unió Tanácsának határozatával összhangban a bizottság az Európai Unió nevében részt vett a jegyzőkönyvre vonatkozó tárgyalásokon. A bizottság következetesen konzultált az uniós álláspontról a tárgyalással foglalkozó tanácsi különbizottsággal.

Az Európai Parlament és az Európai Bizottság közötti kapcsolatokról szóló keretmegállapodással összhangban a bizottság írásbeli jelentések és szóbeli előadások útján is tájékoztatta az Európai Parlamentet a tárgyalások állásáról.

---

[31] https://www.coe.int/en/web/cybercrime/octopus-interface-2019; https://itki.uni-nke.hu/hirek/2019/11/26/octopus-2019-a-jovoben-minden-buncselekmenynek-lesz-informaciotechnologiai-vonzata

[32] https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=SWD:2018:0119:FIN:HU:PDF

[33] https://www.crossborderdataforum.org/budapest-convention-what-is-it-and-how-is-it-being-updated/

A 2021. május 28-i plenáris ülésen a számítástechnikai bűnözésről szóló egyezmény bizottsága saját szintjén jóváhagyta a jegyzőkönyv tervezetét, és azt elfogadás céljából továbbította az Európa Tanács Miniszteri Bizottságának.

Az Európa Tanács Miniszteri Bizottsága 2021. november 17-én (lásd a *2021. évi Octopus-konferencia* alcím alatt) elfogadta a jegyzőkönyvet.

A közel négy évig tartó tárgyalások és a 2021. november 17-i hivatalos jóváhagyás után a számítógépes bűnözésről szóló budapesti egyezmény 2. kiegészítő jegyzőkönyvét az Európa Tanács 2022. május 12-én, Strasbourgban, a megerősített együttműködésről és az elektronikus bizonyítékok nyilvánosságra hozataláról szóló nemzetközi konferencia keretében nyitják meg aláírásra az egyezmény részes felei számára.

A legutolsó verzió nyolc fő rendelkezésre összpontosít:

1) Nyelv.
2) Videókonferencia.
3) Közös nyomozó csoportok és közös nyomozások.
4) Az előfizetői információkhoz történő közvetlen hozzáférés.
5) Külföldi határozatok érvényre juttatása az adatok gyors előállítása érdekében.
6) Doménnév-regisztrációval kapcsolatos információk kérése (ÚJ).
7) A tárolt számítógépes adatokhoz történő gyors hozzáférés vészhelyzet esetén (ÚJ).
8) Sürgősségi kölcsönös jogsegély *(Emergency Mutual Legal Assistance).*

Noha az egyezmény és a második kiegészítő jegyzőkönyv jelentősége a kiberbűncselekmények nemzetközi harmonizációjának előmozdításában vitathatatlan, számos kritika fogalmazható meg az egyes rendelkezések kapcsán.[34]

A 2021. évi Octopus-konferencia[35]

Az Octopus-projekt az Európa Tanács projektje: a számítógépes bűnözésről szóló egyezmény (budapesti egyezmény) részes államainak és megfigyelőinek, egyéb szervezeteknek, a kiberbűnözéssel foglalkozó szakértőknek az önkéntes hozzájárulásán alapul, *célja* az egyezmény, annak jegyzőkönyvei és a kapcsolódó előírá-

[34] Lásd többek között Krasznay Csaba: i. m. 191–214. o.

[35] „Octopus Conference 2021 – Cooperation against Cybercrime". https://www.coe.int/en/web/cybercrime/octopus-interface-2021

sok, normák végrehajtásának támogatása, valamint a 2020-tól a *pandémia következményeként* előtérbe került további nehézségek kezelése.

- Az évente-másfél évente megrendezett *Octopus-konferencia* a világ egyik legnagyobb kiberbűncselekményekkel foglalkozó nemzetközi szakmai rendezvénye: több mint száz országból érkeznek miniszterek, magas szintű kormányzati képviselők, nemzetközi szervezetek képviselői, kutatók, de részt veszek az információtechnológiai ipar képviselői is, hogy e tanácskozáson megtárgyalják a *kiberbűnözés és az online térben elkövetett visszaélések aktuális trendjeit.*
- A 2021. évi eseménynek különös jelentőséget adott, hogy ebben az évben van a számítógépes bűnözésről szóló egyezmény (budapesti egyezmény) elfogadásának huszadik évfordulója.
- A konferencián elfogadták a dokumentum második kiegészítő jegyzőkönyvét a kibővített együttműködésről és az elektronikus bizonyítékok közzétételéről.

A 2021. évi online közvetítésű konferencia (amelyen részt vehettem) nyitónapja egy különleges eseménnyel kezdődött: a résztvevőket *Marija Pejčinović Burić,* az Európa Tanács főtitkára és *Pintér Sándor* belügyminiszter, majd – a világ minden tájáról – miniszterek, főügyészek és más magas rangú tisztviselők köszöntötték; a konferencián körülbelül százhúsz ország nagyjából ezerkétszáz kiberbűnözési szakértője vett részt.

A plenáris nyitónap *(High-level Special Event)* után két nap alatt majd húsz szekció, illetve workshop fogta át a kiberbűnözés valamennyi – büntető anyagi jogi és -eljárásjogi, kriminológiai, informatikai, biztonságpolitikai – szegmensét, magas szintű elméleti és gyakorlati szakemberek prezentációja, tanácskozása segítségével. Ilyen meghirdetett workshop volt többek között

- A Covid–19 és a kiberbűnözés *(COVID-19 and cybercrime).*
- Bűnözés és kriptovaluták *(Crime and cryptocurrencies).*
- A kiberbűnözéssel kapcsolatos jogszabályok globális helyzete *(Global state of cybercrime legislation).*
- A gyermekek szexuális kizsákmányolását rögzítő anyag automatizált felderítése *(Automated detection of child sexual abuse materials).*
- Zsarolóvírusok *(Ransomware).*
- Kiberbűnözés, elektronikus bizonyítékok és mesterséges intelligencia *(Cybercrime, e-evidence and artificial intelligence).*
- Kapacitásépítés-workshopok *(Capacity-building workshops).*
- Kiberbűnözés: Áldozatok *(Cybercrime: Victims).*
- Kiberbűnözés: Bűnelkövetők *(Cybercrime: Offenders).*

A konferencia összefoglaló következtetéseiben ösztönzi az államokat, hogy csatlakozzanak a budapesti egyezményhez és írják alá a második kiegészítő jegyzőkönyvet, amint az megnyílik aláírására (2022. május 12.), továbbá kiemeli, hogy a felmerülő új nehézségek miatt folytatódik a megoldások keresése például a mesterséges intelligenciával vagy a kriptovalutákkal[36] kapcsolatban.

Néhány kiemelt „kiberfenyegetés" jellemzői a világjárvány időszakában a 2021. évi IOCTA-jelentés és az Octopus-konferencián elhangzottak alapján

„A kiberbűnözés nem forradalom, hanem evolúció;
az idő múlásával a kiberbűnözés »kibereleme« szinte minden bűnözési formába beépül"
(IOCTA-jelentés, 2020)

A technológiával „támogatott" bűnözés folyamatosan fejlődik, mind a technológiai változás függvényében, mind az új technológiákkal való társadalmi interakció tekintetében.[37] A Covid–19-válság szemléltette, hogy a bűnözők hogyan használják ki a társadalom legkiszolgáltatottabb helyzetét.

A bűnözők a kiberbűnözés már létező formáit úgy módosították, hogy illeszkedjenek a világjárvány „narratívájához", a szervezett bűnözői csoportok is gyorsan kihasználták a Covid-19-járvány által kiváltott válságot, tevékenységeiket és módszereiket az új helyzethez igazítva.

Az IOCTA-dokumentumok hangsúlyozzák, hogy a Covid–19 számos területen a már fennálló problémák felerősödését okozta, ezt tovább súlyosbította az otthon dolgozó emberek számának jelentős növekedése.

Ugyanakkor 2020 folyamán változott a Covid–19 bűnözésre gyakorolt hatása, a nagyobb tudatosság csökkentette a bűnözés egyes típusainak hatását.

---

[36] Az Európai Bizottság 2021. július 20-án tette közzé jogalkotásijavaslat-csomagját, amely az EU pénzmosás és terrorizmus finanszírozása elleni keretrendszerének megerősítését tűzte ki célul. Erről lásd részletesen Csongrádi Erika – Miskó Judit: *A pénzmosás leáldozó csillaga – átvilágított kriptovaluták.* https://www.mnb.hu/kiadvanyok/szakmai-cikkek/felugyelet/dr-csongradi-erika-dr-misko-judit-a-penzmosas-lealdozo-csillaga-atvilagitott-kriptovalutak. 2021 végén a tanács álláspontjában bevezetett módosítások egyszerűsítik és pontosítják a bizottság javaslatát. https://data.consilium.europa.eu/doc/document/ST-14259-2021-INIT/en/pdf

[37] Urbas Gregor – Kim-Kwang Choo: *Resource Materials on Technology-enabled Crime, Technical and Background Paper No. 28.* Australian Institute of Criminology, 2008, p. 5.

A 2021. év bizonyíték arra, hogy amellett, hogy a 2020. évi megállapítás *(„cybercrime is an evolution not a revolution")*[38] továbbra is irányadó a hosszú (napjainkban is fennálló) pandémiás időszak rendkívüli körülményei *felgyorsították e fejlődést:*

1) a zsarolóprogram-csoportok *(ransomware)* továbbra is kulcsfontosságú fenyegetést jelentenek, az elkövetők egyre inkább kihasználják a széles körben elterjedt távmunkát, otthoni munkavégzést (VPN sebezhetőségek szemmel tartása stb.);
2) az online vásárlás veszélyei továbbra is mérvadók (adathalász csali);
3) a mobilbankolás népszerűségének növekedése miatt a mobilbanki trójaik is jelen vannak;
4) a kiskorúak még több időt töltenek otthon, megnőtt az *online grooming* („szexuális becserkészés") előfordulások száma, továbbá nagyobb eséllyel készítenek és osztanak meg a kiskorúak saját magukról készített anyagokat online (hírnév vagy anyagi haszonszerzés céljából, avagy kényszerítés miatt);
5) a *ransomware műveletek* inkább a nagy értékű támadásokra összpontosítanak: szervezetek és „ellátási láncok" ellen, míg az úgynevezett social engineering támadások a felső vezetőkre irányulnak, az elkövetők egyre könyörtelenebbek és módszeresebbek (*„ransomware crews"* – modern zsarolóprogramok), ilyen zsarolási módszerek például: az áldozatok adatainak kiszivárogtatása, azok közzétételével való fenyegetéssel (például Vice Society: azt a kettős technikát alkalmazza, hogy nemcsak titkosítja áldozata adatait, hanem azzal is fenyegetőzik, hogy nyilvánosságra hozza az ellopott információkat, ha a célpont nem fizeti ki a váltságdíjat egy meghatározott határidőn belül):
   - 2021-ben a kényszerítési módszerek arzenálja tovább bővült: újságírók, továbbá az áldozatok ügyfeleinek, üzleti partnereinek és alkalmazottainak hideghívásával (úgynevezett *cold-calling:* adatbázisokból jutnak személyes adatokhoz az elkövetők),
   - emellett a leghírhedtebb zsarolóprogramok közül DDoS-támadásokat is bevetnek az elkövetők áldozataik ellen, hogy nyomást gyakoroljanak rájuk a váltságdíj-követelés teljesítése érdekében.

2021-ben ezek a *modi operandi*k egyre népszerűbbek a *befektetési csalásokat végrehajtó bűnözők* körében is, amely az európai bűnüldöző szervek jelentése szerint a legfontosabb fenyegetések közé tartozik.

[38] A 2021. évi IOCTA-jelentés megállapításairól lásd bővebben Deres Petronella: i. m. 59–63. o.

Több ízben előfordul, hogy amint egy személy rájön, hogy a befektetéseit ellopták, a csalók újra felveszik az áldozatokkal a kapcsolatot azzal az ürüggyel, hogy képviselik őket, ügyvédi irodák vagy bűnüldöző szervek nevében, és felajánlják, hogy hogy segítenek visszaszerezni a pénzüket. Ilyen befektetési csalásokra példa

- a Ponzi-rendszer: egyfajta piramisjáték, ahol a korábbi befektetőket az újonnan érkezett befektetők pénzéből fizetik ki, egészen a rendszer összeomlásáig (ponzi-séma-gyanús altcoinok: *BST, The Billion Coin, Gemcoin, Bitconnect*);
- a *„pump and dump"* csalás: olyan részvénycsalás, amely során a bűnözők általában kis cégek részvényeiről olyan hamis híreket közölnek (például spam üzenet formájában), amelyből az áldozatok tévesen úgy gondolják, emelkedni fognak az adott cég papírjai (ehhez hasonló jellegű volt a War on Rugs nevű szervezet által 2021-ben „lebonyolított akció").

Következtetések

1) Az információs technológia *új fejleményei az elkövetők számára is új lehetőségeket* kínálnak, e probléma folyamatos küzdelmet jelent a büntetőjogi rendszer számára, veszélyt jelent hazánk *nemzetbiztonságára és infrastruktúrájára.*
2) Az „okoseszközöket" és adatokat célzó új bűncselekmények egyre gyakoribbá váltak, sőt a *hagyományos bűncselekményeket is ösztönzik* az új (kiber-) lehetőségek.
3) A *technológia a bűnözés, a bűncselekmények, valamint az igazságszolgáltatás folyamatának szinte minden aspektusát átalakítja,* számos nehézséggel kell szembesülnünk *a technológiával összefüggő bűnözés és igazságszolgáltatás* megértése során.
4) A számítógépes bűnözők elleni hatékony küzdelem érdekében *nemzetközi szintű együttműködésre* van szükség (az országok kiberbűnüldözésre fordított költségvetése csak a töredéke annak, amely az ilyen típusú bűnözésben mozog, ezt a hátrányt pedig csak összefogás révén lehet kiküszöbölni). A kiberbűnözéssel kapcsolatos kihívások hatékonyabb megválaszolása érdekében az *információk megosztása* áll a stratégiai, taktikai és operatív válaszok középpontjában a kiberbűnözés konkrét típusától függetlenül.
5) Fontos, hogy a kiberbűnözés elleni küzdelem ne csak az államok feladata legyen, hanem *a piac szereplői is* magukénak tudják, hiszen azok, akik a legújabb technológiákat fejlesztik, rengeteget tehetnek a megelőzés és a bűnüldözés hatékonyságának javítása érdekében.
6) Kiemelten fontos az *elektronikus bizonyítékok* hatékony gyűjtése, megőrzése és átadása.

7) A hatékony reagálás további kulcselemei: a *megelőzés* (egyének és szervezetek képzése), a *tudatosság és a kapacitásépítés* (a bűncselekmények különböző területein a bűnüldöző szervek képesek lesznek megérteni és reagálni a bűncselekmények kiberelemére), az Europol közös számítógépes bűnözés elleni munkacsoportja (J-CAT).