AZ EUROPOL KÖZÖS PARLAMENTI ELLENŐRZŐ CSOPORTJÁNAK 15. TALÁLKOZÓJA

III. TEMATIKUS NAPIRENDI PONT: A KIBERBŰNÖZÉS ELLENI KÜZDELEM, KÜLÖNÖSEN A MESTERSÉGES INTELLIGENCIA ALKALMAZÁSÁVAL ELKÖVETETT BŰNCSELEKMÉNYEKKEL SZEMBENI FELLÉPÉS; A TUDÁSMEGOSZTÁS LEHETŐSÉGEI A CEPOL BEVONÁSÁVAL

A növekvő digitalizációban rejlő versenyelőny, az összekapcsolt hálózati és informatikai infrastruktúrák, továbbá az elmúlt évek válsághelyzetei felerősítették a kiberbiztonság európai igényét [JOIN(2020) 18 final, COM(2021) 170 final]. A mesterséges intelligencia (MI) a digitális adathalmazban való eligazodás eszközeként a mindennapok részévé vált. Folyamatos tanulást kíván, hogy nyomon követhessük kapcsolatát a kiberbűnözéssel [COM(2023) 665 final], és hogy a kockázatokra adott válaszok is naprakészek lehessenek.

Az Európai Multidiszciplináris Platform a Bűnügyi Fenyegetettség Ellen (EMPACT) a tagállami együttműködés eszköze, a súlyos és szervezett bűnözés elleni prioritásokat az Európai Unió Tanácsa határozza meg. Ezek egyike a kiberbűnözés elleni küzdelem.

Az Europol és annak Európai Kiberbűnözési Központja (EC3) operatív és stratégiai jelentések széles skáláját készíti. Az egyik ilyen jelentés feltérképezi, hogyan használhatják az MI-t a bűnözők (Europol-jelentés 2020); ilyen például az MI által támogatott jelszókitalálás, a CAPTCHA-törés (vagyis az a teszt, amely képes megkülönböztetni az emberi felhasználót a gépitől), a titkosítási és pszichológiai manipulációval végrehajtott (ún. social engineering) támadások, valamint a mélyhamisítás (deepfake) és az intelligens asszisztensekkel való visszaélés.

Az EC3 központ minden évben kiadja az Internetes Szervezett Bűnözés Fenyegetettség Felmérés-ét (IOCTA). A 2023-as IOCTA a kiberbűnözés különböző tipológiáira vonatkozó összefoglaló megállapításokat ismertet. A jelentést kiegészítő, kibertámadásokról szóló anyag például felvázolja az elkövető bűnszervezetek típusait, és rávilágít arra, hogy azok hogyan használják ki a geopolitikai változásokat; vizsgálja továbbá a rosszindulatú szoftverek által okozott támadások jellegét. Az online csalással foglalkozó kiegészítő jelentés kiemeli a bűnözők nagyfokú alkalmazkodókészségét, a társadalmi-gazdasági tendenciák és aktuális válsághelyzetek mentén alakított módszereiket. A 2024-es IOCTA aláhúzza az MI-n alapuló eszközök és szolgáltatások szélesedő elterjedését a kiberbűnözésben.
A legfrissebb Az MI és a rendfenntartás (2024) című jelentés, amely az adattorzítás, a magánélet, az elszámoltathatóság és az emberi jogok védelmének kérdéseivel foglalkozik az MI-jogszabály [COM(2021) 206 final] hatálybalépése kapcsán.

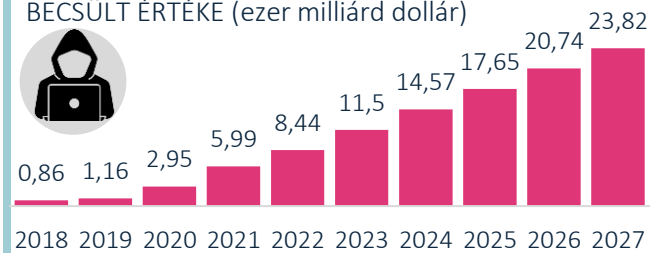
A 2021-ben indított AP4AI projekt célja, hogy a rendészet, a biztonság és az igazságszolgáltatás területén megalkossa az MI elszámoltathatóságának validált keretrendszerét. Reflektálva a lezajlott szabályozási vitákra és a 30 országban lefolytatott polgári konzultáció eredményeire született meg „Az MI elszámoltathatósági elvei a biztonság területén” (2022) című jelentés a bűnüldözésben és igazságszolgáltatásban részt vevő belső biztonsági szakemberek számára. A polgárokkal folytatott konzultáció szerint a kiszolgáltatott csoportok és a társadalom védelme, továbbá a jövőbeli bűnmegelőzés terén nyílna lehetőség az MI alkalmazására. A jelentést folyamatos együttműködés követi a szakértői csoportokkal, hogy az elszámoltathatósági elveket megvalósítható lépésekké alakítsák, jogi megfontolásokkal és gyakorlati példákkal szolgálva a jövőben.

Az Europol aktualizált stratégiai prioritásainál (2023) előtérbe került a jogérvényesítés és a kutatás, különös tekintettel az adatfeldolgozó eszközök MI-vel történő fejlesztésére. Az Europol 2022-es és 2023-as konszolidált éves tevékenységi jelentései ezért említik az AIDA projektet, amely célja egy leíró és előrejelző elemzési platform létrehozása, hogy a bűnüldöző szervek számára valós adatok feldolgozását tegye majd lehetővé operatív környezetben. Az Europol 2024–2026-ra vonatkozó többéves programozási dokumentumtervezete számos ponton érinti az MI-t. Említi például az európai adatvédelmi jogi és mesterséges intelligencia szabályozási keretek bűnüldözési tevékenységekre gyakorolt hatását, vagy az MI-ben rejlő lehetőségek kiaknázását az illegális online tartalom ellen küzdő uniós platform továbbfejlesztésével.

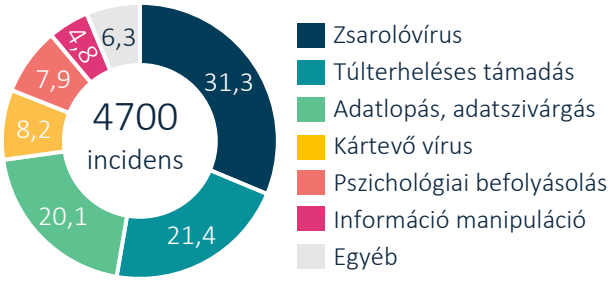
Ylva Johansson belügyi biztos az Europol Közös Parlamenti Ellenőrző Csoportjának 2024. februári genti ülésén kiemelte, hogy az Europolnak küzdenie kell az MI rosszindulatú felhasználása ellen, mert az elősegítheti a dezinformációs kampányokat, a csalást és a gyermekek szexuális zaklatását. Hangsúlyozta, hogy ehhez a bűnüldöző hatóságoknak hatékony MI-eszközöket kell fejleszteniük. ◆

1 A KIBERBŰNCSELEKMÉNYEK FŐ TÍPUSAI

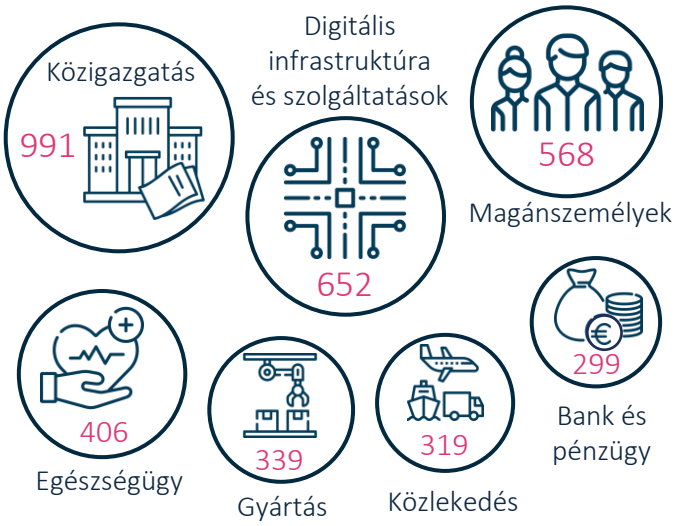
2 A KIBERBŰNÖZÉS ÁLTAL OKOZOTT GLOBÁLIS KÁR BECSÜLT ÉRTÉKE (ezer milliárd dollár)



3 AZ EU KIBERBIZTONSÁGI ÜGYNÖKSÉGÉNEK (ENISA) JELENTETT INCIDENSTÍPUSOK MEGOSZLÁSA, 2022.VII.–2023.VI. (százalék)

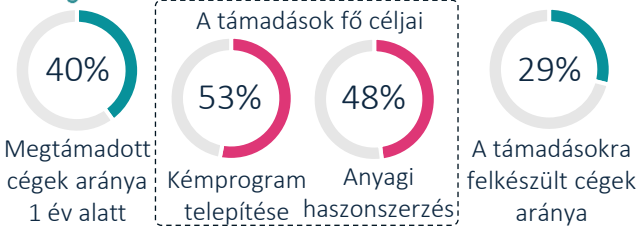


4 AZ ENISA ÁLTAL VIZSGÁLT KIBERINCIDENSEK A FŐBB TÁMADOTT SZEKTOROK SZERINT, 2022.VII.–2023.VI. Darab

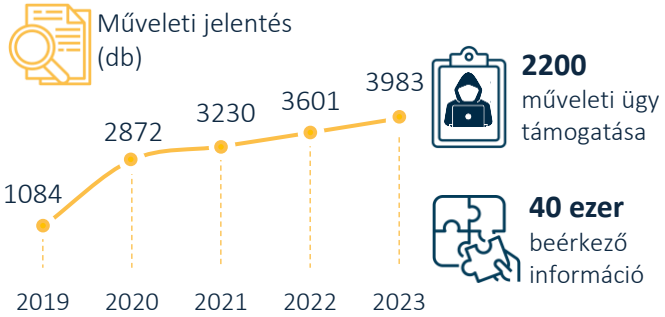


5 AZ EURÓPAI PIACOK KIBERBIZTONSÁGA, 2024

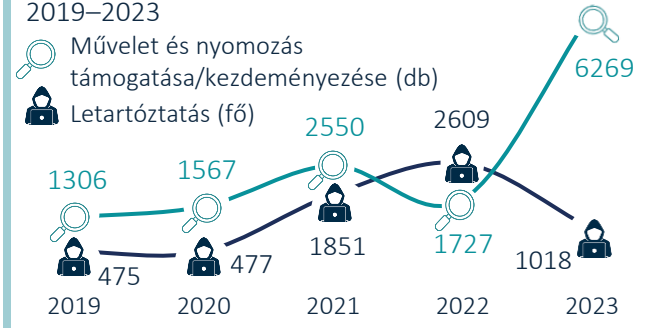
4261 cég és szervezet adatai (BE, CZ, CH, DE, ES, DK, FR, IT, NL, NO, PL, SE, UK)



6 AZ EUROPOL EC3 MŰVELETI TÁMOGATÁSAI, 2019–23



7 ONLINE CSALÁS ELLENI EMPACT EREDMÉNYEK, 2019–2023



FORRÁSOK

1 Európa Tanács: A Számítástechnikai Bűnözésről szóló Egyezmény, 2001; European Commission, 2024 | 2 Statista, 2024
3 | 4 ENISA, 2023 | 5 Cloudflare, 2024 | 6 Europol, CAAR 2019–2023 | 7 European Commission: EMPACT