Az EU rendészeti szerveinek együttműködése a kiberbűnözés ellen[1]

Cooperation between EU law enforcement agencies against cybercrime

dr. Simon Béla[2]

Absztrakt:

Jelen tanulmány célja, hogy kiberbűnözés elleni fellépés aspektusából az Európai Unió tagállamainak rendészeti együttműködési platformjait és azok működését bemutassa annak érdekében, hogy áttekintést adjon a jelenlegi helyzetről, illetve lehetőséget teremtsen a fejlesztési lehetőségek feltárására. A vizsgálat módja az Európai Unió és a tagállamok intézményrendszereinek, illetve funkcióinak áttekintése jellemzően az ehhez kapcsolódó joganyagok, közlemények, tudományos munkák, illetve a GENVAL[3] kölcsönös értékelő jelentéseinek segítségével. Eredménye pedig a fő feladatok, célok, trendek körülírása közösségi és tagállami szinten.

Kulcsszavak: rendészeti szervek, kiberbűnözés, együttműködés

[1] A mű a KÖFOP-2.1.2-VEKOP- azonosítószámú, „A jó kormányzást megalapozó közszolgálat-fejlesztés” elnevezésű kiemelt projekt keretében működtetett Ludovika Kiberbiztonsági Kiemelt Kutatóműhely keretében, a Nemzeti Közszolgálati Egyetem felkérésére készült. The work was created in commission of the National University of Public Service under the priority project KÖFOP-2.1.2-VEKOP- titled „Public Service Development Establishing Good Governance” in the Ludovika Cyber Security Workshop.

[2] Nemzeti Közszolgálati Egyetem, Rendészettudományi Kar, ORCID azonosító: 0000-0002-1555-3690

[3] GENVAL: Az EU Tanácsa előkészítő szervei közé tartozó Általános ügyekkel és értékeléssel foglalkozó munkacsoport. Azokat az intézkedéseket koordinálja, amelyek célja a szervezett bűnözés megelőzése és felszámolása (kivéve a belügyminiszterek munkacsoportjába tartozó kérdésekben) Ennek 7. körös országokat érintő értékelése vonatkozott a kiberbűnözésre. Bővebben: https://www.coe.int/en/web/octopus/blog/-/blogs/genval-evalutation-reports-on-cybercrime/

Abstract:

The purpose of this paper is to demonstrate the police cooperation platforms and their operation in the field of cybercrime in order to give an overview of the current situation and provide opportunities for exploration of development possibilities. The method of analysis is an overview of the institutional systems and functions of the European Union and of the Member States, typically through the related legal material, publications, scientific works and GENVAL Mutual Evaluation Reports. The result of the analysis is to describe the main tasks, goals and trends on Community and Member State level.

Keywords: Hungarian law enforcement agencies, cybercrime, cooperation

Bevezetés

Jelen tanulmány célja – terjedelmi okok folytán - s em lehet az, hogy az Unió teljes rendészeti és igazságszolgáltatási együttműködés intézményrendszerét áttekintse át, hanem az, hogy a kiberbűncselekmények megelőzésével, felderítésével, bizonyításával összefüggő funkciókat, intézményeket megvizsgálja. Ennek során nem tudja a teljes palettát bemutatni az EU-s szinten sem, hiszen számos közösségi intézménynek van a kiberbűnözés ellen ható tevékenysége[4], de ezek leglényegesebb elemeit áttekintve megvizsgálja, hogy azokhoz miként lehetne a leghatékonyabban igazodni, azokat miként lehetne hatékonyabban kiaknázni.
Az kétségtelen, hogy az Európai Unió kiemelten foglalkozik a digitális egységes piaci stratégia[5] teljeskörű végrehajtásával és annak egyik fő eleme a kiberbiztonság prioritást élvez.

Az EU egyre nagyobb kiberbiztonsági kihívásokkal kényszerül szembenézni. A mai IKT[6]-rendszerek ugyanakkor komoly károkat szenvedhetnek biztonsági problémák, például üzemzavarok vagy vírusok miatt. Ezek az események, amelyeket gyakran hálózat- és információbiztonsági (NIS[7]) eseményeknek neveznek, egyre sűrűbben fordulnak elő, és egyre nehezebb őket elhárítani.[8]

E veszélyeket az Európai Unió Tanácsa már rég felismerte és ennek egyik eredménye volt, hogy az Előkészítő Szervek[9] közt működő Általános ügyekkel és értékeléssel foglalkozó munkacsoport (GENVAL) is készített egy értékelést, melynek

[4] Hiszen az Európai Bizottságnak és számos szervének, mint például OLAF (Office européen de lutte antifraude) az EU csalás elleni hivatalának is számos olyan vizsgálata volt, melynek eredményeként a kiberbűncselekmények száma csökkent

[5] Bővebben: http://www.consilium.europa.eu/hu/policies/digital-single-market/ (letöltés ideje: 2017.11.02.)

[6] Információ- és kommunikáció-technológiai

[7] Network and information systems – hálózati és információs rendszerek – melyhez kapcsolódik a NIS Directive – NIS irányelv (az Európai Parlament és a Tanács (EU) 2016/1148 irányelve)

[8] https://www.consilium.europa.eu/hu/policies/cyber-security/ (letöltés ideje: 2017.11.02.)

[9] A Tanácsot feladatai ellátásában egyrészt az európai uniós tagállami kormányok Állandó Képviselőinek Bizottsága (a Coreper), másrészt több mint 150 szakosított munkacsoport és bizottság, az úgynevezett tanácsi előkészítő szervek segítik. – bővebben: https://www.consilium.europa.eu/hu/council-eu/preparatory-bodies/?Page=5 (letöltés ideje 2017.11.02.)

célja a kiberbűnözés európaihelyzetének feltárása[10] volt. A jelentés átfogó képet nyújt az Európai Unió tagállamaiban a kiberbűnözés elleni küzdelem, a határokon átnyúló együttműködés és az érintett uniós ügynökségekkel folytatott együttműködés jogi és operatív vonatkozásairól.

Az Előkészítő Szervek között a hálózatbiztonság és a kiberbűnözés elleni fellépés máshol is megjelenik. Kiemelten az alábbiaknál:

- Belső Biztonságra Vonatkozó Operatív Együttműködéssel Foglalkozó Állandó Bizottság (COSI)[11]
- A büntető anyagi jogi munkacsoport (DROIPEN)[12]
- A büntetőügyekben folytatott rendőrségi és igazságügyi együttműködés területén működő koordinációs bizottság (CATS)[13]
- A bűnüldözési munkacsoport (LEWP) [14]
- Biztonsági Bizottság[15]

Az Európai Unión belül sem állnak meg ezek a kérdések a büntetőjogi tényállások határán, hanem a kiberterrorizmussal, kiberhadviseléssel összefüggésben megjelennek a közös kül- és biztonságpolitika terén is. Ezek szintén meghaladják e tanulmány terjedelmi korlátait.

A NIS irányelv hatása a kiberbűncselekmények elleni együttműködésre

Az Európai Bizottság 2013. február 7-én fogadta el „Az Európai Unió Kiberbiztonsági Stratégiája: Nyílt, megbízható és biztonságos kibertér" című közleményét

[10] korábbi értékelések fókuszában jellemzően a szervezett bűnözés megelőzése és felszámolása volt, valamint az utas-nyilvántartási adatállomány (PNR-adatok) összegyűjtése és felhasználása, az emberkereskedelem, a korrupció elleni küzdelem.

[11] Standing Committee on Operational Cooperation on Internal Security - http://www.consilium.europa.eu/en/council-eu/preparatory-bodies/standing-committee-operational-cooperation-internal-security/

[12] Working Party on Substantive Criminal Law http://www.consilium.europa.eu/en/council-eu/preparatory-bodies/working-party-substantive-criminal-law/

[13] Coordinating Committee in the area of police and judicial cooperation in criminal matters http://www.consilium.europa.eu/en/council-eu/preparatory-bodies/coordinating-committee-area-police-judicial-cooperation-criminal-matters/

[14] Law Enforcement Working Party http://www.consilium.europa.eu/en/council-eu/preparatory-bodies/law-enforcement-working-party/

[15] Security Committee http://www.consilium.europa.eu/en/council-eu/preparatory-bodies/security-committee/

melynek részeként, egyik fő intézkedéseként szintén elfogadta a hálózat- és információbiztonságnak az egész Unióban egységesen magas szintjére vonatkozó intézkedésekről szóló közleményét (NIS irányelv[16]).[17]

A rendelkezések értelmében minden tagállamnak ki kell jelölnie egy vagy több CSIRT[18]-et, mely az incidenskezelésért felelős a meghatározott szektorban és részt vesz a CSIRT-ek hálózatának munkájában. A döntés értelmében létre kell hozni egy Együttműködési Csoportot, amelynek tagjai a tagállamok képviselői, a Bizottság, valamint az Európai Uniós Hálózat- és Információbiztonsági Ügynökség (ENISA) és fő feladata a hálózati és információs rendszerek biztonsága tekintetében a tagállamok között folytatott stratégiai együttműködés támogatása és elősegítése. Tehát itt operatív együttműködésről és adatszolgáltatási kötelezettségről nem beszélhetünk.

A felmerülő informatikai incidensek természetesen nem csak kiberbűncselekményekre és kiberterrorizmusra vonatkoznak, de statisztikai elemzések nélkül is belátható, hogy egy információs rendszerrel kapcsolatos incidenssel összefüggésben az esetek túlnyomó többségében felvetődik a kiberbűncselekmény elkövetésének gyanúja.[19]

A CSIRT-ek közti hálózat és az Együttműködési Csoport működése azonban számos kérdést vet fel.

E tanulmány szerzője azt már korábban kifejtette[20] a magyarországi Kormányzati Eseménykezelő Központ (GovCERT) és az LRLIBEK[21] működésével összefüggésben, hogy bűnüldözői szempontból hátrányos az, hogy a nyomozóhatóságok az

---

[16] AZ EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2016/1148 IRÁNYELVE (2016. július 6.) a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről http://eur-lex.europa.eu/legal-content/HU/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.HUN&toc=OJ:L:2016:194:TOC

[17] http://www.katasztrofavedelem.hu/letoltes/kkb/4_20160429-KKB-hatarozat-kibervedelem.pdf (letöltés ideje 2017.11. 02.)

[18] Computer Security Incident Response Team (számítógép-biztonsági incidenskezelő csoport) kifejezésből képzett mozaikszó. A CSIRT kifejezést elsősorban Európában használják a CERT levédett kifejezés helyett, amelyet a CERT Coordination Center (CERT/CC) jegyeztetett be az Amerikai Egyesült Államokban.

[19] Egy természeti katasztrófa, vagy egy berendezés meghibásodása is előidézhet incidenseket, de például különösen utóbbi esetében a mulasztással összefüggő felelősség vizsgálata is indokolt lehet.

[20] Dr. Simon Béla: Rendészeti szervek együttműködése a kiberbűnözés ellen in Nemzetbiztonsági Szemle – kézirat időpontjában megjelenés alatt

[21] BM Országos Katasztrófavédelmi Főigazgatóság szervezetén belül működő Létfontosságú Rendszerek és Létesítmények Informatikai Biztonsági Eseménykezelő Központja - az állam és önkormányzat által üzemeltetett létfontosságú rendszerek és létesítmények

esetek túlnyomó többségében nem szereznek információt olyan incidensekről, amelyekben e szervezetekkel kapcsolatban álló szereplők érintettek. A megtámadott, károsított, vagy annak kísérletével érintett szereplők – ilyen módon sértettek – nem tesznek feljelentést a nyomozóhatóságoknál és olyan együttműködési platform sem került kialakításra, ami az incidensekből kinyerhető adatokat, adatbázisokat a nyomozóhatóságok rendelkezésére bocsátja, ezért a nyomozóhatóságok azokat más ügyekben sem tudják hasznosítani.[22]

Több olyan jogi megoldás született az egyes jogrendszerekben[23], hogy a különféle szereplőket (tipikusan informatikai rendszereket, kritikus informatikai infrastruktúrákat üzemeltetőket) az őket érintő informatika incidensekkel kapcsolatban bejelentés tételére kötelezték. A címzettek ezen kötelezettségeiknek sok esetben ellenszegültek és nem tettek eleget bejelentési kötelezettségeiknek.[24] Ez jellemzően reputációs okokra vezethető vissza. Az érdekek tehát a legtöbb esetben a sértetti oldalon a büntetőeljárás megindítása ellen hatnak, ugyanakkor ez a gyakorlat súlyosan sérti az legalitás és az officialitás elveit, tehát az állam a büntető igényét nem tudja érvényesíteni arra hivatott hatóságai által, mivel a jelenlegi rendszer lehetővé teszi, hogy a sértettek döntsenek a büntetőeljárás kezdeményezéséről.[25] Tárgyalt témánk vonatkozásában azonban fontos volna a büntető eljárások prevenciós hatásának elérése is, továbbá a feljelentések megtételének elmulasztása nem csak piaci szereplők esetében jellemző, hanem állami, önkormányzati aktorok esetében is.

A bűncselekmény elkövetésének gyanújával összefüggésben a NIS irányelv leglényegesebb feladat meghatározása:
„A biztonsági események hátterében bűncselekmények is állhatnak, ezek megelőzését, kivizsgálását és büntetőeljárás alá vonását elősegíti, ha az alapvető szolgáltatásokat nyújtó szereplők, a digitális szolgáltatók, az illetékes hatóságok és a bűnüldöző hatóságok koordinálják tevékenységeiket és együttműködnek egymással.

---

kivételével - ellátja a nemzeti létfontosságú rendszerek és létesítmények védelmével kapcsolatos hálózatbiztonsági tevékenységet.

[22] Emellett persze nem kell elrendelni eleve reménytelen büntetőeljárásokat sem, de lehetőség sincs kiválasztani olyanokat, melyek a siker reményével kecsegtetnek

[23] Például: Incident Prevention, Warning, and Response (ipwar) manual bővebben: https://www.directives.doe.gov/directives-documents/200-series/0205.01-DManual-1/@@images/file

[24] Ez vélelmezhető például abból az adatból, hogy 2017. évben a Létfontosságú Rendszerek és Létesítmények Informatikai Biztonsági Eseménykezelő Központ mindösszesen 3 darab incidensről kapott bejelentést. (2017.10.26-án az Országos Katasztrófavédelmi Főigazgatóságon tartott konferencián elhangzottak)

[25] Ez természetesen más bűncselekmény típusoknál is lehetséges: például a zsebtolvajlás sértettje nem kíván feljelentést tenni.

Amennyiben egy biztonsági esemény gyaníthatóan uniós vagy nemzeti jog szerinti súlyos bűncselekményekhez köthető, a tagállamoknak arra kell ösztönözniük az alapvető szolgáltatásokat nyújtó szereplőket és a digitális szolgáltatókat, hogy a gyaníthatóan súlyos bűncselekmény jellegét öltő biztonsági eseményt jelentsék az érintett bűnüldöző hatóságok felé. Adott esetben ajánlott, hogy a Számítástechnikai Bűnözés Elleni Európai Központ (Europol EC3) és az ENISA elősegítse a különböző tagállamokban működő illetékes hatóságok és bűnüldöző hatóságok közötti koordinációt."[26]

Tehát az eddigi állami rendelkezések önmagukban is rendre a címzett szereplők ellenállásába ütköztek, így a különösen összetett kérdés, hogy a NIS irányelv címzettjei miként fognak a közösség tagállamai irányába is információt szolgáltatni. A bűncselekmények megelőzése, megszakítása és az elkövetők kilétének megállapítása azonban ezek nélkül nem megoldható.

Az irányelv a bűncselekményekkel összefüggésben az alábbi rendelkezéseket tartalmazza:

A 8. pontban rögzítésre került, hogy az irányelv nem sértheti a tagállamok számára biztosított azon lehetőséget, hogy megtegyék az alapvető biztonsági érdekeik védelméhez, a közrend és a közbiztonság megóvásához, valamint a bűncselekmények kivizsgálásának, felderítésének és a büntetőeljárások lefolytatásának lehetővé tételéhez szükséges intézkedéseket. Az Európai Unió működéséről szóló szerződés (EUMSZ) 346. cikke értelmében egyetlen tagállam sem köteles olyan információt szolgáltatni, amelynek közlését ellentétesnek tartja alapvető biztonsági érdekeivel.

Az irányelv meghatározásában amennyiben az Együttműködési Csoport bűnüldözési hatóságokkal folytat együttműködést olyan hálózat- és információbiztonsági kérdések tekintetében, amelyek azok munkájára esetlegesen hatást gyakorolhatnak, tiszteletben kell tartania a meglévő információs csatornákat és hálózatokat.

A megfogalmazás több helyen is a „súlyos bűncselekmények" kifejezést használja, ami azt mutatja, hogy az Európai Parlament és a Tanács sem látja indokoltnak a büntetőjogilag ugyan értékelhető, de mennyiségénél fogva nehezen üldözhető cselekmények elleni fellépést, mivel azok és az officialitás elvének érvényre juttatása a bűnüldöző hatóságok számára felesleges terhet jelentene.

A tagállamok büntetőjogi és nemzetbiztonsági autonómiájának védelmében azonban a NIS irányelv is rögzíti, hogy *„nem érinti azokat az intézkedéseket, ame-*

[26] Az Európai Parlament és a Tanács (Eu) 2016/1148 irányelve (2016. július 6.) A hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről (62.) pont

lyeket a tagállamok az alapvető állami funkcióik védelme, és különösen a nemzetbiztonság védelme érdekében hoznak, ideértve az olyan információk védelmét szolgáló intézkedéseket is, amelyek közlését a tagállamok ellentétesnek tartják alapvető biztonsági érdekeikkel, továbbá a közrend fenntartása, és különösen a bűncselekmények kivizsgálásának, felderítésének és büntetőeljárás alá vonásának lehetővé tétele érdekében hozott intézkedéseiket."

A NIS irányelv azonban nem önmagában álló rendelkezés, hanem egy nagy rendszer része, amelyben fontos előremutató rendelkezések szerepelnek.
Ilyen például[27] az Európai Bizottság ajánlása a nagyszabású kiberbiztonsági eseményekre és válsághelyzetekre való összehangolt reagálásról[28].
Ebben találjuk meg az uniós szintű kiberbiztonsági esemény megfogalmazását, amiről akkor beszélhetünk, ha:

- az esemény által okozott zavar túlságosan kiterjedt ahhoz, hogy egy érintett tagállam önállóan kezelje; vagy
- két vagy több tagállamot technikailag, vagy politikailag széleskörűen érint; és
- időszerű koordinációt és reagálást igényel uniós politikai szinten.

Az EU szintjén a jelentős kiberbiztonsági eseményekre és válságokra adott hatékony válasz gyors és eredményes együttműködést igényel valamennyi érdekelt fél között és erősen támaszkodik az egyes tagállamok felkészültségére és képességeire, valamint az uniós képességek által támogatott összehangolt közös fellépésre. Az eseményekre történő azonnali és hatékony válaszadás csak a már korábban megtervezett és lehetőség szerint jól bevált együttműködési eljárások és mechanizmusok esetén lehetséges, amelyekben a kulcsfontosságú szereplők nemzeti és uniós szintű szerepe és felelőssége egyértelműen meghatározott.

A NIS-irányelv azonban nem ír elő uniós együttműködési keretet nagyszabású kiberbiztonsági események és válságok esetére.

Uniós szinten a kiberbiztonsági válságokra adandó válaszokban kulcsszerepet játszó szereplők közé tartoznak a NIS-irányelvben nevesített Számítógép-biztonsági Incidenskezelő Csoport (CSIRT) hálózata, valamint az érintett ügynökségek és

[27] Említhető még a Bizottság közleménye az Európai Parlamentnek, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának: Európa kibertámadásokkal szembeni ellenálló képességének erősítése, valamint a versenyképes és innovatív kiberbiztonsági ágazat támogatása címmel – bővebben: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52016DC0410

[28] A Bizottság (EU) 2017/1584 számú ajánlása (2017. szeptember 13.) a nagyszabású kiberbiztonsági eseményekre és válsághelyzetekre való összehangolt reagálásról

szervek, nevezetesen az Európai Unió (Europol / EC3), az EU Hírszerző Elemző Központja (INTCEN), az EU Katonai Törzsének Hírszerzési Osztálya (EUMS INT) és az EU helyzetelemző szolgálata (SITROOM), mint a SIAC (az egységes iformációelemzési kapacitás), az EU-hibrid fúziós cellák (az INTCEN-ben), az EU intézményeinek hálózatbiztonsági vészhelyzeteket elhárító csoportja (CERT-EU) és a sürgősségi reagálási koordinációs központ az Európai Bizottságban.

A NIS-irányelv az esetlegesen bekövetkező kiberbiztonsági események kapcsán a legtöbb feladatot a CSIRT-ek hálózatához delegálja. A CSIRT-hálózatok feladatai közé tartozik az operatív együttműködés további formáinak megvitatása, feltárása és azonosítása is, beleértve a kockázatok és biztonsági eseményekkel kapcsolatos korai figyelmeztetéseket, a kölcsönös segítségnyújtást, az együttműködés elveit és módjait, határokon átnyúló kockázatokat és eseményeket. Az Együttműködési Csoport pedig az együttműködésben is mint stratégiai szereplő jelenik meg.

Az ajánlás fontos feladatként jelöli a kommunikációt, hiszen az európai polgárok és vállalkozások bizalma a digitális szolgáltatásokban alapvető fontosságú a virágzó digitális egységes piac számára. Ezért a válságkommunikáció különösen fontos szerepet játszik a kiberbiztonsági incidensek és válságok negatív hatásainak mérséklésében.

A tagállamoknak teljes körűen ki kell használniuk az Európai Hálózatfinanszírozási Eszköz (Connecting Europe Facility[29]) Kiberbiztonsági Digitális Szolgáltatási Infrastruktúrája (CyberSecurity Digital Service Infrastructures[30], DSI) által kínált lehetőségeket, és együtt kell működniük a Bizottsággal annak biztosítása érdekében, hogy a jelenleg fejlesztés alatt álló alapvető szolgáltatási platform együttműködési mechanizmusa biztosítsa a szükséges funkcionalitást és kielégítse az együttműködési követelményeket a kiberbiztonsági válságok során is.[31]

A NIS irányelv magyarországi implementálása a 2018. május 10-én hatályba lépett bejelentés-köteles szolgáltatást nyújtókról szóló 410/2017. (XII. 15.) Korm. rendeletben történt meg. Eszerint eseménykezelő központként a Belügyminisztérium Országos Katasztrófavédelmi Főigazgatóság került kijelölésre. A feladat nem csekély. Nem csak a nemzetközi kapcsolattartás lehetőségéhez, a működéshez szükséges infrastrukturák kiépítése, az ellenőrzési, eseménykezelési, bírságolási folyamatok jogi kimunkálása nehezen megvalósítható e szűkös időkereten belül. Ha figyelembe vesszük, hogy ha szükségesek fejlesztések, akkor technikai oldalon

[29] Bővebben: https://ec.europa.eu/inea/en/connecting-europe-facility

[30] Bővebben: https://ec.europa.eu/digital-single-market/en/news/connecting-europe-facilities-cybersecurity-digital-service-infrastructure valamint http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=4634

[31] http://ec.europa.eu/transparency/regdoc/rep/3/2017/EN/C-2017-6100-F1-EN-MAIN-PART-1.PDF letöltés időpontja: 2017.11.02.

– különösen közbeszerzésen keresztül történő – lebonyolítása, a személyi oldalon pedig az állomány pályáztatása, nemzetbiztonsági ellenőrzése, kinevezése, felkészítése nehezen tudott megvalósulni a rendelet megalkotása és hatályba lépése közti 5 hónap alatt[32].

A Kiberbiztonsági Ügynökség szerepe a kiberbűncselekmények elleni együttműködésben

Az EU fontos lépést tett a kiberbiztonság érdekében, amikor döntött a Kiberbiztonsági Ügynökség (Cybersecurity Agency)[33] létrehozásáról.

A meglévő Európai Hálózat- és Információbiztonsági Ügynökségre (ENISA) építve az Ügynökség állandó megbízatást kap, hogy segítse a tagállamokat a számítógépes támadások hatékony megelőzésében és reagálásában. A Kiberbiztonsági Ügynökség az EU kiberbiztonsági reagálási készségét az éves páneurópai kiberbiztonsági gyakorlatok szervezésével, a fenyegetési információk és ismeretek jobb megosztásával, valamint az információmegosztási és elemzési központok létrehozásával fogja javítani. Az Ügynökség a tervek szerint segíteni fogja a hálózat- és információs rendszerek biztonságáról szóló irányelv végrehajtását is.

A Bizottság javaslatára a Kiberbiztonsági Ügynökség segítséget nyújt továbbá az EU egészére kiterjedő infokommunikációs termékek és szolgáltatások tanúsítási keretrendszerének létrehozásához és végrehajtásához.

A 2018. év elejének fejleményei közé tartozott az is, hogy Bizottság javaslata szerint kísérleti programként 2018. évben létre kell hozni egy Kiberbiztonsági Kutatási és Kompetencia Központot (European Cybersecurity Research and Competence Centre). Az új intézmény a tagállamokkal együttműködve elősegítheti a folyamatosan változó fenyegetések elleni fellépéshez szükséges eszközök és technológiák kifejlesztését és fejlesztését, valamint elősegíti, hogy kibervédelmi eszközök korszerűbbek legyenek, mint a számítógépes bűnözők által használt eszközök[34]. Ez kiegészíti a kapacitásépítési erőfeszítéseket ezen a területen uniós és nemzeti szinten.

A bizottság megállapítása szerint a számítógépes bűnözők felderítésére, nyomon követhetőségére és üldözésére összpontosító hatékonyabb bűnüldözési válasz központi szerepet játszik az ilyen bűncselekmények elkövetésének hatékony

[32] Jelen tanulmány a hatálybalépést megelőzően született, de a megjelenést megelőző időszakban folyik a feladatok és hatáskörök átalakítása

[33] Bővebben: http://europa.eu/rapid/attachment/IP-17-3193/en/Cybersecurity-EU%20agency%20and%20certification%20framework.en.pdf

[34] https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/european-agenda-security/20180124-progress-report-13-towards-effective-and-genuine-security-union.pdf - letöltés időpontja 2018. január 28.

elhárítására. A Bizottság ezért javasolja az elrettentés fokozását a csalás és a nem készpénzes fizetőeszközök hamisítása elleni új intézkedések révén.

A Bizottság 2018. évben alkotni javasol egy irányelvet, mely meg fogja erősíteni a bűnüldöző hatóságok képességeit azáltal, hogy kiterjeszti az információs rendszerekhez kapcsolódó bűncselekmények alkalmazási körét valamennyi fizetési műveletre, beleértve a virtuális pénznemeken keresztül történő ügyleteket is. A jogforrás továbbá közös szabályokat vezet be a büntetések mértékére, és tisztázza a tagállamok joghatóságát az ilyen bűncselekmények tekintetében.

A számítógépes bűnözés hatékony kivizsgálásának és büntetőeljárásának fokozására a Bizottság 2018 elején javaslatokat fog előterjeszteni az elektronikus bizonyítékok határokon átnyúló hozzáférésének megkönnyítésére. Ezen túlmenően 2018. októberben a Bizottság bemutatja válaszát a bűnügyi nyomozásokat akadályozó titkosítások kezelésére. [35]

Az Unió tagállamainak kiberbűnözés elleni együttműködésére vonatkozó további lehetséges területei:

- Konkrét ügyekhez kapcsolódó nyomozóhatósági együttműködés
- Konkrét ügyekhez kapcsolódó ügyészi együttműködés
- Konkrét ügyekhez kapcsolódó megkeresések harmadik országok irányába
- Közös akciók, gyakorlatok
- Jogalkotási együttműködés
- Együttműködés K+F területen
- részvétel olyan büntetőeljárások lefolytatásában, amelyre hatáskörrel nem rendelkezik az állam (EU Cybercrime Task Force (EUCTF)

Terjedelmi korlátok miatt azonban jelen tanulmánynak ezek nem képezik részét.

Az EU határain kívüli jó gyakorlatok

A gyermekek online szexuális kizsákmányolásának minden mozzanata jellemzően nem marad egy kontinensen belül. Fontos kitekintést tenni az Európai Unió határain kívül is működő[36] legjobb nemzetközi gyakorlatokról:

- Interpol Baseline: lehetővé teszi a köz- és magánszféra partnerei számára, hogy felismerjék, beszámoljanak és eltávolítsák a gyermekek szexuális zaklatásának anyagát hálózataikról.[37]
- Az Egyesült államokban működő Munkacsoport a Gyermekek Elleni Nemzetközi Bűncselekményekre (International Crimes Against Children Task

[35] http://europa.eu/rapid/press-release_IP-17-3193_en.htm letöltés ideje 2017.11.02.

[36] Természetesen az EU igazságszolgáltatási, rendészeti együttműködési rendszere is működik az EU határain kívül (pl Europol működésében harmadik országok delegáltjai)

[37] https://www.interpol.int/Crime-areas/Crimes-against-children/Internet-crimes

Force Program) - elnevezésű szervezet (– amely 61 koordinált munkacsoport nemzeti hálózata, amely több mint 4500 szövetségi, állami és helyi bűnüldöző és ügyészi ügynökséget képvisel. Ezek az ügynökségek proaktív és reaktív vizsgálatokat, törvényszéki vizsgálatokat és büntetőeljárásokat folytatnak és működtetnek egy Gyermekvédelmi Rendszert (Child Protection System CPS)[38] adatbázist

- Az ENSZ Transznacionális Szervezett Bűnözés Elleni Egyezménye (United Nations Convention against Transnational Organized Crime and the Protocols Thereto) UNTOC Az ENSZ nemzetközi együttműködési felülete leginkább jogalkotói, jogalkalmazói segítséget nyújt tagjainak a bűncselekmények e körével szemben is[39], illetve képzéseket indít és támogat a bűnüldöző szervek tagjai részére[40].

Európai szintű együttműködés

- ECTEG (European Cybercrime Training and Education Group) – Számítástechnikai Bűnözés Elleni Európai Képzési és Oktatási Csoport, amely az Európai Unió és az Európai Gazdasági Térség tagállamainak csatlakozott bűnüldöző szervezeteiből, nemzetközi szervezeteiből, tudományos központokból, magániparból és szakértőkből áll és célja különféle oktatások tartása, képzések fejlesztése.
- EUCTF (European Union Cybercrime Task Force) – egy olyan ügynökségi csoport, amelyet a nemzeti számítógépes bűnözés elleni egységek vezetőiből alakítottak ki[41].
- IFOREX (Internet és Forenzikus Szakértői Csoport - Internet and Forensics Experts CIRCAMP - A COSPOL (Comprehensive Operational Strategic Planning for the Police - Rendészeti Műveleti Stratégiai Tervező Egység) gyermekek szexuális kizsákmányolását bemutató anyagok internetes terjesztését felgöngyölítő projekt (COSPOL Internet-related Child Abusive

[38] Internet Crimes Against Children Task Force Program – gyermekek sérelmére elkövetett internetes bűncselekmények elleni program https://www.icactaskforce.org/ Child Protective Services – gyermekvédelmi szolgálatok

[39] Például Thaiföld esetében: http://www.unodc.org/documents/southeastasiaandpacific //Publications/2015/childhood/2015_Series_1-UNODC_Working_Paper-Amendments_to_the_Criminal_Code_of_Thailand.pdf

[40] Például Dél Amerikában: http://www.unodc.org/ropan/en/IndexArticles/Cybercrime/unodc-ropan-contribuye-a-combatir-la-pornografia-infantil-facilitada-por-internet.html

[41] Szerepel az EU kiberbiztonsági stratégiájában is mint együttműködő testület: https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:52013JC0001&qid=1541349123773&from=EN – letöltés ideje 2018. 11. 04.

Material Project - CIRCAMP) olyan szűrési technológiák használatát népszerűsíti az uniós tagállamokban, amelyek blokkolják a felhasználók hozzáférését a gyermekek kizsákmányolásával kapcsolatos kereskedelmi weboldalakhoz.[42]

A Belső Biztonságra Vonatkozó Operatív Együttműködéssel Foglalkozó Állandó Bizottság (COSI)[43] az Unió belső biztonságával kapcsolatban a tagállamok által kifejtett operatív tevékenységek koordinálását segíti, ösztönzi és erősíti.
Az elmúlt időszakban a COSI elsősorban

- a nagy károkozással járó, online és bankkártyás fizetéssel összefüggő; továbbá
- az áldozatok részére komoly hátránnyal járó – például gyermekek sérelmére elkövetett – számítógépes bűncselekmények; valamint
- a kritikus infrastrukturát és számítógépes rendszereket érintő kiber-bűncselekmények tekintetében kívánt hatékony lépéseket tenni a kialakítandó védekezés érdekében.[44]

EMPACT

A fejlődés egyik kiemelt motorja lehet a rendészeti szervek irányába az EMPACT (European Multidisciplinary Platform against Criminal Threats) a nemzetközi szervezett bűnözés elleni hatékony fellépés érdekében kialakított feladatrendszer, amelynek keretében több különböző prioritást (például: informatikai bűncselekmények, emberkereskedelem, szintetikus drogok, illegális migráció stb.) érintően végeznek közös munkát a kijelölt EMPACT nemzeti szakértők az EUROPOL segítségével.

Az EMPACT előre meghatározott célok elérését szolgáló ad hoc menedzsment környezet. A tagállamok, az EU ügynökségei és intézményei, a harmadik államok, valamint az állami és magán szervezetek olyan strukturált multidiszciplináris együttmőködési platformja, amely a prioritásként meghatározott súlyos és szervezett nemzetközi bűncselekmények ellen küzd, így pl a kiberbűnözés ellen is.[45]

---

[42] https://www.europol.europa.eu/sites/default/files/documents/hu_europolreview.pdf letöltés ideje 2017.12.10.

[43] A COSI (Standing Committee on Internal Security) szerepéről és összetételéről az Európai Unió működéséről szóló szerződés 71. cikke rendelkezik

[44] Az Európai Unió Belső Biztonsági Állandó Bizottsága által meghatározott stratégiai célok a kiber-bűnözés elleni harc bővebben: http://www.cert-hungary.hu/node/211

[45] Az Európai Unió Tanácsa 14518/2012 számú dokumentuma 2. pont, Brüsszel, 2012. október 3.

A kiberbűnözés elleni fellépés prioritás keretében a cél a számítógépes bűnözés, valamint az internet bűnözési célú használata elleni harc. A prioritáson belül a bankkártyabűnözést, a kibertámadások és gyermekek online szexuális kizsákmányolása elleni küzdelmet fogják össze.[46]

Az EMPACT működése még nem tekint vissza hosszú múltra. A kiberbűnözés visszaszorításának egyik hátráltató tényezőjeként említjük, hogy tengerentúli tech óriás vállalatok (például: Google, Microsoft, Apple) együttműködési hajlandósága, adatközlési gyakorlata nem megfelelő. Ha a nyomozóhatóságok közti kölcsönös segítségnyújtás nem elegendő, akkor be kell látni, hogy uniós szintű kényszerítő mechanizmusok kimunkálása volna célszerű. Annak eldöntése, hogy ezeket politikai, gazdasági, diplomáciai eszközök igénybevételével lehet megvalósítani, amely már a tagállamok kiberbűnözéssel foglalkozó egységeinek munkatársai, vezetői kompetenciakörét meghaladja. Ebből két dolog következik. Egyrészt ezeket a kérdéseket magasabb szintre kell emelni (nem véletlen, hogy a Bizottság is ígéretet tett az elektronikus bizonyítékok határokon átnyúló hozzáférése megkönnyítésének előmozdítására). Másrészt az egyes tagországoknak – így Magyarországnak is – jelentős személyi ráfordításokat kell allokálnia e célra.

Magyarország képviselői eddig a kiberbűnözés elleni fellépés terén nem vállaltak EMPACT prioritáshoz kapcsolódó irányító szerepet, de ez a későbbiekben jelentősen előmozdíthatná e téren nemzetközi elismertségünket, a szakmai kapcsolatok kialakulását, valamint a szakmai fejlődést is, hiszen a projekthez kapcsolódó szakmai munkában történő nagyobb számú kolléga is jelentős tapasztalatot gyűjtene.

Az EMPACT jelentősége abban áll, hogy SOCTA által feltárt problémákat a COSI és az Europol közreműködésével, együttműködésével a prioritások és a kapcsolódó projektek segítségével a stratégiai elképzeléseket operatív cselekvésekké alakítják át. Az EMPACT a gyakorlati együttműködés fokmérőjévé vált. Az EMPACT keretén belül végzett rendőri akciók további hatással lesznek a nemzeti rendőrségek operatív tevékenységeire, ahogy azok is hatást gyakorolnak majd az egész EU operatív bűnügyi együttműködésére. Az eddigi magyarországi aktivitásokat – például tudatosságnövelő kiadványokat és akciókat[47] – jó eséllyel további hatékonyságnövelő intézkedések, gyakorlatok fogják követni.

[46] Sorbán Kinga: Az informatikai bűncselekmények elleni fellépés nemzetközi dimenziói http://epa.oszk.hu/02300/02363/00023/pdf/EPA02363_THEMIS_2015_jun_343-375.pdf letöltés dátuma 2017.12.10.

[47] http://saferinternet.hu/a-gyerekek-online-zsarolasatol-ved-az-orfk-kampanya-videoval-es-tanacsokkal-szolnak-a-fiatalokhoz

A GENVAL 12711/1/17 jelentése a „A számítástechnikai bűnözés megelőzését és az ellene folytatott küzdelmet érintő európai szakpolitikák gyakorlati végrehajtása és működése:

A GENVAL értékelésekből levonható következtetések:

Evidencia, hogy az informatika és az ahhoz kapcsolódó visszaélések fenyegetése teljesen átszővik életünket. Mint látható ez az EU intézményeiben is nagyon sok esetben felmerül. Vizsgálatunkat azonban szűkítsük a rendészeti együttműködésre.

A kiberbűnözés kifejezés a bűncselekmények széles körét öleli fel, a GENVAL ország értékelések kezdeti időszakában is megállapodás született, hogy az értékelés középpontjába azok a bűncselekmények kerülnek, amelyek a tagállamok megítélése szerint különös figyelmet érdemelnek. Az értékelés ezért is az alábbi problémakörökre terjedt ki:

- az informatikai támadásokra,
- a gyermekek online szexuális bántalmazására/az internetes gyermekpornográfiára és
- az online bankkártyacsalásra

Ahhoz, hogy a tagállamok előrelépést érhessenek el a számítástechnikai bűnözés elleni küzdelemben, minden országban magas szintű politikai akaratra, költségvetési erőfeszítésekre, valamint az emberi és technikai erőforrásokba való jelentős beruházásokra van szükség.

Az értékelésből az derül ki, hogy a számítástechnikai bűnözés elleni küzdelmet az összes tagállam komolyan veszi, és erre a célra struktúrákat hoztak létre, erőforrásokat különítettek el és intézkedéseket hoztak. Az elkötelezettség és a hatékonyság szintje azonban eltérő az egyes tagállamokban, és bizonyos esetekben több szempontból is van még mit javítani a számítástechnikai bűnözés elleni küzdelemre alkalmazott általános megközelítésen. Ugyanakkor több közös problémát és kihívást is sikerült azonosítani.

A tagállamok többsége már elfogadott nemzeti kiberbiztonsági stratégiákat, melyek keretet nyújtanak a nemzeti prioritások meghatározásához, valamint a fontosabb koordinációs struktúrák stratégiai és operatív szintű létrehozásához. Egyes tagállamok a nemzeti kiberbiztonsági stratégiájuk végrehajtásához cselekvési tervet is elfogadtak.

A tagállamok többsége már aláírta és megerősítette a számítástechnikai bűnözésről szóló 2001. évi Európa tanácsi egyezményt[48] (Budapesti Egyezmény), valamint annak a számítástechnikai rendszerek útján megvalósított rasszista és idegengyűlölő cselekmények büntetendővé nyilvánításáról szóló kiegészítő jegyzőkönyvét.

A tagállamoknak a kiberbűnözésre és a kiberbiztonságra vonatkozó statisztikai adatai elégtelenek, széttagoltak, és nem teszik lehetővé az összehasonlítást sem a tagállamok különböző régiói, sem pedig az egyes tagállamok között. Ennek egységeshez közeli kialakítása azért fontos, hogy a tendenciák alakulása megfigyelhető legyen és megnyíljon a lehetőség az összehangolt fellépésre. Ezen túlmenően az is fontos adalék, hogy csak olyan folyamatokat lehet menedzselni, amiket számszerűsíteni tudunk.[49]

A kiberbűncselekmények – mint problémakör – annyi részterületeket foglal magába, hogy szükséges a specializáció. Az értékelés megállapítása szerint ez a bűnüldöző hatóságok esetében jellemzően megvalósult, de igazságügyi alkalmazottak körében növelni szükséges a szakosodás mértékét.

Kiemelten fontos a képzés és továbbképzés e területen, melyhez összehangolt oktatási programok szükségesek. Ebben részt vesznek a Számítástechnikai Bűnözés Elleni Európai Központ (EC3)/Europol, az ECTEG, az Eurojust, az OLAF és a CEPOL is.

A hatékonyság növeléséhez nem csak a rendészeti szervek egymás közti, hanem a piaci szereplőkkel (pénzügyi intézményekkel/bankokkal, a távközlési vállalatokkal, internetszolgáltatókkal, nem kormányzati szervezetekkel, tudományos szervezetekkel, vállalkozásokkal, szakmai egyesületekkel) való kooperáció is szükséges. A köz- és a magánszektorbeli érdekeltek között többszereplős megközelítésen alapuló, szoros és hatékony intézményközi koordináció és együttműködés szükséges stratégiai és operatív szinten is. Ajánlásként fogalmazódott meg ilyen jellegű fúziós központok kialakítása a tagállamok szintjén.

Egyes tagállamokban a nemzeti jogszabályok lehetővé teszik az alapvető előfizetői információknak a külföldi szolgáltatóktól való közvetlen beszerzését, más tagállamokban viszont be kell tartani a kölcsönös jogsegély eljárásait, melyeket gyorsabbá és hatékonyabbá kellene tenni. Az Európai Unió tagállamai számára fontos, hogy gondoskodjanak arról, hogy a nemzeti jogszabályaik elég rugalmasak legyenek az elektronikus bizonyítékok elfogadhatóságának elősegítéséhez, azon

[48] Aktuális adatok: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=dvMo444p

[49] http://ttk.nyme.hu/fmkmmk/tamop412/Documents/Tananyagok/%C3%81tkonvert%C3%A1lt%20tananyagok%20pdf-exportja/Innov%C3%A1ci%C3%B3s%20 folyamatmenedzsment.pdf

esetek vonatkozásában is, amikor az elektronikus bizonyíték másik országból, illetve közvetlenül az internetszolgáltatótól került beszerzésre.

Az Együttműködés további szükséges területei

A bűnüldözés – amikor a szükséges információk megszerzéséhez dekriptálnia kell - a kriptográfia eszközeivel felvértezett bűnelkövetőkkel vívott küzdelmében hátrányból indul. Az ehhez szükséges számítási kapacitás működtetése tagállami szinten nagyon költséges vállalás volna. Számos tagállam igénybe veszi az Europol, pontosabban a Számítástechnikai Bűnözés Elleni Európai Központ (EC3) dekódoló platformját. A titkosításból fakadó kihívásokat részben ellensúlyozni lehetne a kutatás-fejlesztés erősítésével és új módszerek kidolgozásával, valamint a különböző érintett hatóságok, piaci szereplők és a tudományos műhelyek közötti megfelelő együttműködéssel.

A kiberbűncselekmények jellegükből adódóan nagyon sok esetben több joghatóságot érintenek. A nemzetközi bűnügyi jogsegélyben beszerzett bizonyítékok felhasználhatósága a digitális világgal nem érintett eljárások során is sok esetben problémát jelent.[50] Az elektronikus bizonyítékok, azaz az adatok elfogadhatóságukkal kapcsolatban még több gondot okoznak. Az Unió számos tagállamában az elektronikus bizonyítékok gyűjtésére egyedi előírások vannak érvényben annak érdekében, hogy azok a bíróságok előtt bizonyítékként elfogadhatóak legyenek. Számos tagállamban az eljárásjog technológiasemleges, azaz a bizonyítékok beszerzésére általános szabályokat és elveket alkalmaznak. Ilyen esetekben a jogrendszerek átvilágítása szükséges ahhoz, hogy az egymás bizonyítékai kölcsönösen elfogadhatók legyenek.

A magyar büntetőeljárásról szóló törvényben[51] információs rendszerben tárolt adatok megőrzésére kötelezés - amelyet a budapesti Cybercrime Egyezmény[52] tárolt számítástechnikai adat gyors megőrzése néven említ - a jelenlegi joggyakorlatban nem működik megfelelően. Az egyik probléma, hogy több tagállamban (a magyar és jellemzően a kelet- közép-európai államoktól eltérően) nagyon rövid,

[50] Magyar eljárásjog szerint lefolytatott bírói engedélyhez kötött eszközök alkalmazása – pl magánlakás átkutatása titkos információgyűjtés - során beszerzett, majd nyílttá tett iratok mennyiben használhatóak fel egy angliai bírósági eljárásban? Vagy egy olyan jogrendszerben, ahol ügyészi engedélyhez kötött a nyílt házkutatás végrehajtása – még ma is gondot okozhat egy, magyar szabályok szerint lefolytatott eljárási cselekmény eredményeinek felhasználása.

[51] 1998. évi XIX. törvény 158/A. §

[52] Az Európa Tanács Budapesten, 2001. november 23-án kelt Számítástechnikai Bűnözésről szóló Egyezményének kihirdetéséről szóló 2004. évi LXXIX. törvény

vagy egyáltalán nincs a szolgáltatóknak kötelezettsége az internet kapcsolat létesítésével, fenntartásával kapcsolatos előzmény adatok megőrzésére. Ez jellemzően azokban az országokban tipikus, ahol a magánélet, magántitok sérthetetlensége nagyobb súllyal esik a latba jogalkotási és alkotmányos kérdések során. Ezekben az országokban reálisan kevésbé várható el, hogy uniós bűnüldözési érdekből az előzmény adatokat hosszabb ideig tárolják. A részleges megoldást az jelentené, ha megkereső hatóságok kérése a megkeresett ISP (Internet Service Provider- internetszolgáltató) irányába egységes módon és rövid határidővel, szinte azonnalosan meg tudna valósulni. Az unió tagállamai számára fel kell tárni az ezt hátráltató tényezőket és megoldást kell találni azok elhárítására.

A határon átnyúló bűnelkövetői magatartások ellen a nemzetközi bűnügyi együttműködés újabb eszközeit is igénybe kell venni. Erre példa a nemzetközi közös nyomozócsoportok (Joint Investigation Teams - JIT-ek[53]) létrehozása. Bár ez a jogintézmény legjobban a huzamosabb ideig működő szervezett jegyeket mutató bűnelkövetés ellen a leghatékonyabb (emberkereskedelem, kábítószer kereskedelem, jövedéki termékek csempészete, stb), de egyes kiberbűncselekményekkel szembeni felderítést és a nyomozások eredményességét is fokozná, illetve fokozhatná.

A gyermekek szexuális bántalmazása és kizsákmányolása elleni küzdelem területén számos standard intézkedés, illetve eszköz áll rendelkezésre. Ezek között szerepel a - már korábban említett - Interpol gyermekek szexuális kizsákmányolásával kapcsolatos nemzetközi adatbázisa (ICSE-DB[54]). Ezen túlmenően néhány tagállam előremutató intézkedéseket tett. Ilyenek például az alábbiak:

- kialakítottak az áldozatok azonosítására szolgáló külön nemzeti adatbázist[55], amellett, hogy az INTERPOL adatbázisához adatszolgáltatóként kapcsolódnak[56].

---

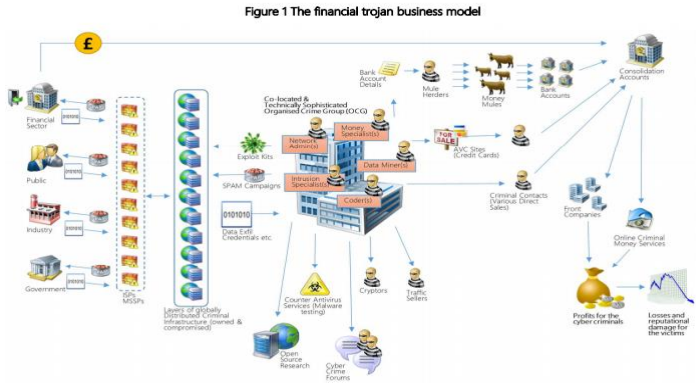
[53] Bővebben: https://www.europol.europa.eu/activities-services/joint-investigation-teams

[54] International Child Sexual Exploitation Data Base, amely az igazoltan jogsértő felvételek hash adatbázisát tartalmazza. A 2017. évi adatok szerint segítségével 10 000 áldozat és 4 900 elkövető volt azonosítható Forrás: https://www.interpol.int/en/News-and-media/Publications2/Fact-sheets/Databases/ (letöltés: 2017. 10.22)

[55] például Nagy Brittania Child Abuse Image Database (CAID) – bővebben: https://www.gov.uk/government/publications/child-abuse-image-database

[56] ezen túlmenően az európai nyomozóhatóságok nagy mennyiségben kapnak értesítéseket bűncselekmény gyanús felvételek terjesztőiről a National Center for Missing & Exploited Children nevű szervezettől - bővebben: https://www.gov.uk/government/publications/child-abuse-image-database

- intézkedéseket tettek a gyermekek újbóli áldozattá válásának megakadályozása céljából. Egyes esetekben például a gyermekek szexuális bántalmazásával kapcsolatos ügyekben folytatott büntetőeljárás során az áldozatok és a tanúk védelmét szolgáló intézkedésekkel[57].
- a bűnüldöző hatóságok, a forróvonalak, a nem kormányzati szervezetek és az internetszolgáltatók közötti jó együttműködés keretében nem csak ad-hoc kapcsolatot, hanem intézményesített formájú együttműködést hoztak létre konkrét feladatokkal, felelősökkel, hatáskörökkel[58].



1. számú ábra: Egy pénzügyi trójai program üzleti modellje[59]

[57] A tanú és áldozatvédelem, minden uniós tagállam jogrendszerében megjelenik, de egyes államokban differenciáltan és kiemelten a gyermekek szexuális áldozattá válásával kapcsolatban. Például Svédországban is számos intézkedést tettek. Bővebben: https://www.government.se/contentassets/fb78975ee42f41349f782189fbee929a/national-action-plan-for-safeguarding-children-from-sexual-exploitation https://www.government.se/4a18d0/contentassets/81ce0fcf0eaa4d09a9f807b5c0017f21/about-what-must-not-happen.pdf

[58] Például Nagy Britannia: Cyber-security Information Sharing Partnership (CiSP) bővebben: https://www.ncsc.gov.uk/cisp

[59] Cyber crime: Understanding the online business model https://www.ncsc.gov.uk/file/2390/download?token=kZc2hbea - letöltés ideje: 2018. 11. 03.

A technológiai fejlődés eredményeit a kriminális oldal szereplői is saját céljaik előmozdítására használják. Bár például a TOR böngésző[60] fejlesztése is elsődlegesen nemzetbiztonsági célokat szolgált,[61] de használatát az illegális szereplők is gyorsan átvették. Amilyen folyamatok megfigyelhetők a legális területen, - nagy valószínűséggel hasonló tényezők hasonló folyamatokat generálnak a bűnözői oldalon.

Az elmúlt időszakban a számítógép és internet felhasználók száma exponenciálisan emelkedett, miközben a szakértő személyek speciális ismerete egyre szűkebb területekre korlátozódott. Jellemzően a kibertérben bűncselekményt elkövetők sem képesek önállóan végrehajtani illegális tevékenységüket. Az egyes részterületekre mind több specialista igénybevétele szükséges.

A legális szereplők tevékenységét jellemzően az anyagi érdekeltség mozgatja és az anyagi érdekek által nem motivált szereplők (pl: open source programok írói) csak abban az esetben képesek célokat elérni, ha valamilyen ernyő szervezet összefogja a tevékenységüket (pl: Linux Foundation).
Ilyen módon, két fő tendencia látható:

- tőkével rendelkező személyek megkeresik a speciális ismeretekkel rendelkező személyeket és anyagi ellenszolgáltatásért rábírják különféle kiberbűncselekmények részfeladataira
- tőke hiányában vagy ideológiai alapon, vagy a várható anyagi haszon érdekében csoportosulások jönnek létre különféle kiberbűncselekmények elkövetésére.

Mindkét esetben az látható, hogy a személyek közti közvetlen fizikális kapcsolat nem szükséges, így mindkét fő fejlődési ág alkalmat ad az elkövetőknek határokon átnyúló együttműködésre.

Ezek a szervezett tevékenységek kiemelt veszélyt jelentenek a kibertér biztonságára és szükségessé teszik a közös adatbázisok létrehozatalát legalább az Európai Unió, de célszerűen minden ország nyomozóhatóságai közt.

Már jelenleg is nagy hatékonysággal működnek az Europol elemző projektjei. Számos gyermekpornográfia elkövetésével összefüggő nyomozás azáltal tud eredményes lenni, hogy a korábbi realizálások során összegyűjtött nicknevek, IP címek, szerver nevek, fórumbeszélgetések felhasználásra kerülnek a jelenleg folyó nyomozásokban és lehetővé teszik olyan személyek kilétének megállapítását, akik szigorú konspirációjának feltárása ezen adatok nélkül elképzelhetetlen lenne.

[60] bővebben: https://www.torproject.org/projects/torbrowser.html.en

[61] Fagoyinbo, Joseph Babatunde (28 May 2013). The Armed Forces: Instrument of Peace, Strength, Development and Prosperity. AuthorHouse. ISBN 978-1-4772-2647-6. pp. 262.

Fontos egy készletező adatgyűjtés, mivel a jelen kor script kiddie[62]-jei a holnap fekete kalapos hekkerei[63] lesznek. Nem csak a fórumbeszélgetések, személyi kapcsolatok, kell, hogy ezen adatbázisok részesei legyenek, hanem akár az egy felhasználó által használt jelszavak is.

A 8-10, vagy több karakterből és speciális jelszó-policy-nak megfelelő kódokból az emberek nem képesek sokat megjegyezni és ki ne cserélte volna fel már életében akár csak egyetlen egyszer a céges és a privát email címének, vagy hálózati hozzáférésének jelszavát. Ezek a jelszavak és jelszó próbálkozások az egyes szolgáltatók log fájljaiban hosszú ideig megtalálhatók. Természetesen nem szöveges formában, hanem a belőle generált hash kulcsok formájában. Jelentős segítséget nyújthat például az elkövető kilétének megállapításához, ha ugyanazt a 12 szám-kis-nagy-betű-speciális karakterből álló jelszót évekkel korábban egy hozzá egyértelműen köthető email címhez használta, mint amit például egy mostani vizsgált ügyben szereplő fórum belépési jelszóként használt.

Az ilyen jellegű adatbázisok létrehozásához a jogszabályi környezeten megteremtésén túl természetesen kell az állami és privát szektor összefogása, de elengedhetetlen a nemzetközi együttműködés.

Az is igaz, hogy adatvédelmi aggályokat is felvetnek ezek a kérdések és számos technika teszi bonyolulttá az adatbázisok létrehozatalát (jelszavak sózása[64]), de ha a bűnüldöző szervek nem építenek ki információs bázisokat, pozíciókat e téren, akkor ez a lemaradás egyre nagyobb lesz.

A másik nagyon fontos nemzetközi együttműködésre is támaszkodó feladat a bűnüldöző szervek számára operatív pozíciók kialakítása. Számos olyan – tipikusan gyermekek online szexuális kizsákmányolásával összefüggő – realizálás volt az elmúlt időszakban, amelyben az illegális szerver üzemeltetői jogokhoz hozzáfértek a nyomozóhatóság tagjai és igazságügyi engedéllyel, de bűncselekményt elkövetve fenntartották az illegális hálózatot és kapcsolatokat az eredményesebb realizálás érdekében[65].

Az operatív pozíciók kiépítése, fedett nyomozók alkalmazása nem csak a gyermek online szexuális kizsákmányolásával összefüggésben lehetséges. Fontos, hogy

---

[62] Jellemzően mélyebb szaktudással nem rendelkező fiatal gyermek, aki hackerek által megalkotott eljárások alapján mások által megírt programokat („szkripteket") használ arra, hogy számítógépekhez, hálózatokhoz illegális hozzáférést szerezzen.

[63] Feketekalapos hackernek nevezzük azokat a hackereket, akik magas szintű tudásukkal visszaélve, jogosulatlanul számítógépbe illetve számítógép-hálózatokba törnek be haszonszerzés vagy károkozás céljából.

[64] A jelszavak sózásáról bővebben: https://www.refaktor.hu/biztonsagos-jelszotarolas/

[65] Bővebben: https://www.theguardian.com/society/2017/oct/07/australian-police-sting-brings-down-paedophile-forum-on-dark-web letöltés ideje:2018. 11. 03.

a kiberbűncselekmények területén is legyenek a nyomozóhatóságoknak informátorai, bizalmi személyei, együttműködői.

Összességében tehát az együttműködés legfontosabb jellemzői az alábbiak kell legyenek:

- széleskörű: tagállamok nyomozóhatóságai, CSIRT-ek, piaci és állami IKT szereplők (internet-, tartalom, szolgáltatók, stb) pénzügyi szolgáltatók között
- speciális: a tudományos szereplőkkel
- folyamatos és azonnali (7/24)
- közös adatbázisok létrehozatala
- egységes gyakorlat a bűnügyileg releváns információs igény érvényesítésére az EU-n kívüli szolgáltatóktól

Összegzés, javaslatok

A fentiek alapján elmondható, hogy az Európai Unió a kiberbiztonság javítása érdekében a piac önszabályozó szerepében már kevésbé bízik és ehelyett hatékony adminisztratív intézkedéseket tesz a résztvevők motiválására (NIS irányelv, GDPR). Ezen túlmenően láthatjuk, hogy például a Belső Biztonság Alap is jelentős erőforrásokat delegál a kiberbűnözés elleni fellépésre[66]

Szükséges a szakmai angolt kiválóan beszélő munkatársak foglalkoztatása e téren. A rendészeti szervek által delegált szakértők jellemzően aktív végrehajtói és parancsnoki állományból kerülnek ki a bűnüldöző területről és megszerzett szakmai tapasztalataikat egy másik foglalkozás: a diplomáciai tisztviselő ismereteivel kell kibővíteniük.

Integrálni kell a rendőri felsőoktatásba – jellemzően rendészeti vezető mester szakon, illetve doktori iskolában, - vagy a vezetőképzésbe olyan ismereteket, amelyek hatékonyabbá teszik a rendőri szakembereket a nemzetközi diplomáciai együttműködésre, a projekt szemléletű ügyintézésre, pályázatok benyújtására, végrehajtására, pénzügyi elszámolására. Ki kell alakítani egy olyan tudásbázist, amely nem csak az Europol-hoz delegált Magyar Összekötő Iroda munkatársai és gyakornokai számára ad segítséget, hanem minden nemzetközi együttműködésben, JIT[67]-ben, kooperációban részt vevő személy és rendőri vezetők számára is segítséget nyújt.

[66] 2017. novemberében közzétett pályázat 8 M EUR összegben https://ec.europa.eu/research/participants/portal/desktop/en/opportunities/isfp/topics/isfp-2017-ag-cyber.html

[67] nemzetközi közös nyomozócsoport – joint investigation team

Rendőri állományú személyként részt venni az EU szerveivel történő együttműködésben mindenképp szakmai siker. Ugyanakkor a tapasztaltabb személyeknek, vezetőknek már nem mindig vonzó a feszes ütemtervben megvalósított szakmai utazás az Europol megbeszéléseire. Indokolt volna a valamilyen akár anyagi elismeréssel (pl.: napidíjak emelésével, vagy más módon) vonzóvá tenni az együttműködésben való részvételt. Ha ezen lehetőségek megszerzéséért, megatartásáért az állomány tagjai közt kialakulna egy egészséges verseny, az a hatékonyság javulását eredményezné.

Magyarországon a piaci szereplők (pl: pénzintézetek) megítélését nem érinti annyira hátrányosan egy több órás szolgáltatás leállás, mint a nyugat-európai tagállamokban. A vállalkozások kitettsége sok esetben nem olyan nagy az IT infrastruktúrák irányába, emellett a bűnügyi statisztikák sem mutatnak riasztó képet hazánkban,[68] de az elmúlt év zsarolóvírus kampányai is rávilágítottak arra, hogy az állampolgárok elégedettségét, biztonságérzetét és a gazdaság termelékenységét is nagyon gyorsan és nagyon hatékonyan tudja erodálni egy kártékony kód, ha az állami és piaci szereplők nem tudnak összehangoltan és gyorsan hatékony lépéseket tenni a károk megelőzésére, enyhítésére, felszámolására.

Magyarország Nemzeti Kiberbiztonsági Stratégiája jelentős megújításra szorul[69] és a kiberbűnözés elleni fellépés vonatkozásában indokolt volna részletes akcióterv kibocsátása. Ezek végrehajtása koordinálásával megbízott külön szerv létrehozása szintén indokolt volna.

Felhasznált irodalom

- BÁNYÁSZ Péter: Kiberbűnözés és közösségi média, In. Nemzetbiztonsági Szemle, 2017/4., pp. 55-74., 2017.
- BELÁZ Annamária – BERZSENYI Dániel: Kiberbiztonsági Stratégia 2.0 A kiberbiztonság stratégiai irányításának kérdései in Stratégiai Védelmi Kutatóközpont Elemzések 2017/3.
- KOVÁCS Zoltán: Biztonság vs. törvényes ellenőrzés az internet alapú kommunikációban ellentétes vagy egymással megférő követelmények Hadmérnök. 2016. december
- KOVÁCS Zoltán: Felhő alapú rendszerek törvényes ellenőrzési módszerei vizsgálata I –II. Hadmérnök VIII. évf. 2013. 3.sz.
- MUHA Lajos – NÉGYESI Imre. Nyílt forráskódú rendszerek alkalmazása. Budapest, NT Nonprofit Közhasznú Társaság. 2013.

[68] Simon Béla: Kiberbűnözés aktuális trendjei in Magyar Rendészet 2018/1. pp. 164–166

[69] Beláz Annamária, Berzsenyi Dániel: Kiberbiztonsági Stratégia 2.0 A kiberbiztonság stratégiai irányításának kérdései in Stratégiai Védelmi Kutatóközpont ELEMZÉSEK 2017/3.

- MUHA Lajos: A kritikus információs infrastruktúrák védelme. Budapest: Reinet Technológia Kft, 2015.
- NAGY Zoltán András – MEZEI Kitti: Az informatikai bűncselekmények - egyetemi jegyzet Pécs, Magyarország: PTE Állam- és Jogtudományi Kar (2017)
- SIMON Béla: Rendészeti szervek együttműködése a kiberbűnözés ellen, 2018/1. szám.
- SIMON Béla: Kiberbűnözés aktuális trendjei in Magyar Rendészet 2018/1. pp 164-166
- SORBÁN Kinga: Az informatikai bűncselekmények elleni fellépés nemzetközi dimenziói http://epa.oszk.hu/02300/02363/00023/pdf/EPA02363_THEMIS_2015_jun_343-375.pdf letöltés dátuma 2017.12.10.
- Az Európai Unió Belső Biztonsági Állandó Bizottsága által meghatározott stratégiai célok a kiber-bűnözés elleni harcról: http://www.cert-hungary.hu/node/211 letöltés ideje: 2017. 11. 03.
- Bizottság (EU) 2017/1584 számú ajánlása (2017. szeptember 13.) a nagyszabású kiberbiztonsági eseményekre és válsághelyzetekre való összehangolt reagálásról https://ec.europa.eu/inea/en/connecting-europe-facility letöltés ideje: 2017. 11. 03.
- Bizottság közleménye az Európai Parlamentnek, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának: Európa kibertámadásokkal szembeni ellenálló képességének erősítése, valamint a versenyképes és innovatív kiberbiztonsági ágazat támogatása címmel – http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52016DC0410 letöltés ideje: 2017. 11. 03.
- Connecting Europe facilities — cybersecurity digital service infrastructure https://ec.europa.eu/digital-single-market/en/news/connecting-europe-facilities-cybersecurity-digital-service-infrastructure letöltés ideje: 2017. 11. 03.
- Coordinating Committee in the area of police and judicial cooperation in criminal matters http://www.consilium.europa.eu/en/council-eu/preparatory-bodies/coordinating-committee-area-police-judicial-cooperation-criminal-matters/
- Cyber crime: Understanding the online business model https://www.ncsc.gov.uk/file/2390/download?token=kZc2hbea letöltés ideje: 2017. 11. 03.
- Cyber-security Information Sharing Partnership (CiSP) https://www.ncsc.gov.uk/cisp

- Digital Service Infrastructures http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=4634 letöltés ideje: 2017. 11. 03.
- Európai Parlament és a Tanács 2016/1148 IRÁNYELVE (2016. július 6.) a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről, http://eur-lex.europa.eu/legal-content/HU/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.HUN&toc=OJ:L:2016:194:TOC letöltés ideje: 2017. 11. 03.
- Fagoyinbo, Joseph Babatunde (28 May 2013). The Armed Forces: Instrument of Peace, Strength, Development and Prosperity. AuthorHouse. ISBN 978-1-4772-2647-6.
- GENVAL: 7. körös országokat érintő értékelése https://www.coe.int/en/web/octopus/blog/-/blogs/genval-evalutation-reports-on-cybercrime/ letöltés ideje: 2017. 11. 03.
- http://ec.europa.eu/transparency/regdoc/rep/3/2017/EN/C-2017-6100-F1-EN-MAIN-PART-1.PDF letöltés időpontja: 2017.11.02.
- http://europa.eu/rapid/attachment/IP-17-3193/en/Cybersecurity-EU%20agency%20and%20certification%20framework.en.pdf letöltés ideje: 2017. 11. 03.
- http://europa.eu/rapid/press-release_IP-17-3193_en.htm letöltés ideje 2017.11.02.
- http://saferinternet.hu/a-gyerekek-online-zsarolasatol-ved-az-orfk-kampanya-videoval-es-tanacsokkal-szolnak-a-fiatalokhoz letöltés ideje: 2017. 11. 03.
- http://ttk.nyme.hu/fmkmmk/tamop412/Documents/Tananyagok/%C3%81tkonvert%C3%A1lt%20tananyagok%20pdf- exportja/Innov%C3%A1ci%C3%B3s%20folyamatmenedzsment.pdf letöltés ideje 2017.11.02.
- http://www.consilium.europa.eu/hu/policies/digital-single-market/
- http://www.unodc.org/ropan/en/IndexArticles/Cybercrime/unodc-ropan-contribuye-a-combatir-la-pornografia-infantil-facilitada-por-internet.html letöltés ideje 2017.11.02.
- https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/european-agenda-security/20180124-progress-report-13-towards-effective-and-genuine-security-union.pdf - letöltés időpontja 2018. január 28.
- https://ec.europa.eu/research/participants/portal/desktop/en/opportunities/isfp/topics/isfp-2017-ag-cyber.html letöltés ideje 2017.11.02.
- https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=dvMo444p letöltés ideje 2017.11.02.

- https://www.consilium.europa.eu/hu/council-eu/preparatory-bodies/?Page=5
- https://www.consilium.europa.eu/hu/policies/cyber-security/ letöltés ideje: 2017.11.02.
- https://www.europol.europa.eu/activities-services/joint-investigation-teams letöltés ideje 2017.11.02.
- https://www.europol.europa.eu/sites/default/files/documents/hu_europolreview.pdf letöltés ideje 2017.12.10.
- https://www.government.se/4a18d0/contentassets/81ce0fcf0eaa4d09a9f807b5c0017f21/about-what-must-not-happen.pdf letöltés ideje 2017.11.02.
- https://www.government.se/contentassets/fb78975ee42f41349f782189fbee929a/national-action-plan-for-safeguarding-children-from-sexual-exploitation letöltés ideje 2017.11.02.
- https://www.interpol.int/Crime-areas/Crimes-against-children/Internet-crimes letöltés ideje 2017.11.02.
- https://www.theguardian.com/society/2017/oct/07/australian-police-sting-brings-down-paedophile-forum-on-dark-web letöltés ideje: 2018. 11. 03.
- https://www.torproject.org/projects/torbrowser.html.en letöltés ideje 2017.11.02.
- Incident Prevention, Warning, and Response (ipwar) manual bővebben: https://www.directives.doe.gov/directives-documents/200-series/0205.01-DManual-1/@@images/file letöltés ideje 2017.11.02.
- International Child Sexual Exploitation Data Base - https://www.interpol.int/en/News-and-media/Publications2/Fact-sheets/Databases/ (letöltés: 2017. 10.22)
- Internet Crimes Against Children Task Force Program – gyermekek sérelmére elkövetett internetes bűncselekmények elleni program https://www.icactaskforce.org/ Child Protective Services – gyermekvédelmi szolgálatok
- Katasztrófavédelmi Koordinációs Tárcaközi Bizottság 4/2016 (IY.29) határozata http://www.katasztrofavedelem.hu/letoltes/kkb/4_20160429-KKB-hatarozat-kibervedelem.pdf (letöltés ideje 2017.11. 02.)
- Law Enforcement Working Party http://www.consilium.europa.eu/en/council-eu/preparatory-bodies/law-enforcement-working-party/
- Nagy Brittania Child Abuse Image Database (CAID) – https://www.gov.uk/government/publications/child-abuse-image-database letöltés ideje 2017.11.02.

- National Center for Missing & Exploited Children nevű szervezet https://www.gov.uk/government/publications/child-abuse-image-database
- Security Committee http://www.consilium.europa.eu/en/council-eu/preparatory-bodies/security-committee/ letöltés ideje 2017.11.02.
- Standing Committee on Operational Cooperation on Internal Security - http://www.consilium.europa.eu/en/council-eu/preparatory-bodies/standing-committee-operational-cooperation-internal-security/ letöltés ideje 2017.11.02.
- UNODC – Child Sex Offenders http://www.unodc.org/documents/southeastasiaandpacific//Publications/2015/childhood/2015_Series_1-UNODC_Working_Paper-Amendments_to_the_Criminal_Code_of_Thailand.pdf letöltés ideje 2017.11.02.
- Working Party on Substantive Criminal Law http://www.consilium.europa.eu/en/council-eu/preparatory-bodies/working-party-substantive-criminal-law/letöltés ideje 2017.11.02.