

SZONGOTH RICHÁRD – VETTER DÁNIEL

Nemzetközi bűnügyi együttműködés a kiberbűnözés területén

A nemzetközi bűnügyi együttműködés napjaink igen dinamikusán változó területe, hiszen a szolgáltatások más országból való elérésének, az állampolgárok más országokba való mozgásának megkönnyítésével kapcsolatos vívmányokat a bűnelkövetők is figyelemmel kísérik, és ki is használják. Megfigyelhető a bűnözés szervezettségének növekedése, a bűnözés határon átnyúló jellege, amely olykor kiemelten nehéz feladat elé állítja a rendvédelmi szervek munkatársait.

A kiberbűnözés utóbbi időben tapasztalt felfutása és egyre szerteágazóbbá válása megkívánta a speciális rendőri egységek közötti kapcsolat szorosabbra fűzését, a beszerzett információk más országgal történő megosztását. A többéves számítógépes bűnözési nyomozati tapasztalattal, valamint a nemzetközi bűnügyi együttműködésben jártassággal bíró szerzőpáros célja annak bemutatása, hogy a kiberbűnözés területén milyen együttműködési lehetőségek találhatók, és azok milyen módon képesek támogatni a kiberbűnözés elleni küzdelmet, a hazai eljárásokat. Terjedelmi okok miatt a tanulmányban azon nemzetközi szervezetek, kapcsolattartási formák kifejtésére kerül sor, amelyekkel kapcsolatban kézzelfogható, rendszeresen visszatérő tapasztalatok állnak rendelkezésre.

Az Europol-együttműködés

Az Europol

Az Europol az Európai Unió bűnüldöző hatósága, amely segíti a tagállamok bűnüldöző hatóságainak munkáját. Az Europolnak nincs önálló nyomozati jogköre, de központi szerepet játszik az Európa biztonságával foglalkozó uniós és nemzeti szervek között, ennek keretében bűncselekményekkel kapcsolatos információs csatornaként működik, és egyike a legnagyobb bűnüldözési elemzési kapacitással felruházott szervezeteknek.

A hazai rendvédelmi szervek napi rendszerességgel küldenek és fogadnak bűnügyi információkat az Europol biztonságos információcserét kiszolgáló hálózatán (SIENA rendszer), így segítve a gyors és hatékony adatcserét a nemzetközi szervezett bűnözés elleni küzdelem terén. Az „Europol-csatorna”

leginkább az uniós tagállamokkal, az európai országokkal, illetve az operatív szerződéssel bíró harmadik tagállamokkal (például Amerika, Kanada, Ausztrália stb.) folytatott bűnügyi információcsere terén aktív.

Az EC3 és az elemzői projektek

Az Europol kiberbűnözéssel foglalkozó szervezeti egysége az European Cybercrime Centre¹ (EC3 – Európai Kiberbűnözés Elleni Központ), amely 2013-ban kezdte meg működését. A központban a kiberbűnözés három fő területéhez – kibertámadások, gyermekek szexuális kizsákmányolása és készpénz-helyettesítő fizetési eszközökkel kapcsolatos bűncselekmények – kötődő munka úgynevezett elemzői projektek (*analyst project*) keretében valósul meg. A projektek működéséhez szükséges információkat alapvetően a tagállamok szolgáltatják a nyomozásaik során felvetődő adatok és információk megosztásán keresztül, amely adatok összesítése és elemzése történik az elemzői projekt keretén belül.

A Készenléti Rendőrség Nemzeti Nyomozó Irodán keresztül hazánk tagja mindhárom kiberbűnözéssel foglalkozó elemzői projektnak, így az AP CYBORG-nak (kiberbűncselekményekkel foglalkozó elemzőprojekt), az AP TWINS-nek (gyermekek szexuális kizsákmányolásával foglalkozó elemzőprojekt) és az AP TERMINAL-nak (készpénz-helyettesítő fizetési eszközökkel történő visszaélésekkel foglalkozó elemzőprojekt). Az elemzői projektek² célja az adott bűnügyi szakterületen végzett folyamatos, naprakész és a nyomozásokat ténylegesen segítő adatcserék és elemzések. (Az elemzőprojektek segítségével megvalósuló munka szorosan kötődik a későbbiekben bemutatandó EMPACT feladatrendszerhez is.) Az elemzői projektek gyakorlatilag egy közös területet kínálnak az adott bűnügyi területhez kötődő információcsere egy mederbe tereléséhez, illetve az Europol szakemberei által az információk tematikus elemzésére.

Az AP CYBORG célja az Európai Unió területén működő informatikai hálózatok, kritikus infrastruktúrák ellen irányuló kibertámadásokkal kapcsolatos nyomozások támogatása, különös tekintettel a profitorientált szervezett bűnözői csoportok elleni fellépésre. Ennek keretében a rosszindulatú számítógépes programok, zsarolóvírusok, hackertevékenység mellett az adatlopás, a személyiséglopás és az internetes csalások elleni fellépésben is szerepet játszik.

¹ <https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3>

² <https://www.europol.europa.eu/crime-areas-trends/europol-analysis-projects>

A kibertámadások fogalmi körébe elsődlegesen a különböző kártékony programok – így a zsarolóvírusok, kémprogramok –, a túlterheléses, úgynevezett DoS-, DDoS-támadások, az adathalászatok, a szerverek adatbázisait érintő adatlopási tevékenységek vagy a weboldalak felületeit megváltoztató, úgynevezett deface támadások, továbbá a folyamatosan, elnyújtottan, célzottan és összehangoltan, egy előre kiválasztott konkrét célpont ellen végrehajtott, úgynevezett ATP- (*Advanced Persistent Threat*) támadások tartoznak. Az egység a klasszikus elemzői és koordinációs feladatai mellett speciális malware-, illetve virtuális valutákkal kapcsolatos elemzési tevékenységet is végez. Az előbbieken túl forenzikus tevékenysége keretében helyszíni adatmentésekben, adattárakban való ellenőrzésekben tud segítséget nyújtani a tagállamok együttműködő rendvédelmi szervezetei számára.

Az AP CYBORG, igazodva az internetes bűnözés folyamatosan változó körülményeihez, valamint a tagállamok részéről felvetődő igényekhez, a szervezetét, továbbá az általuk nyújtott támogatások, szolgáltatások körét igyekszik folyamatosan fejleszteni, azokat innovatív megoldásokkal ellátni, így az elemzői projektektől elvárta, a beküldött adatok más ügyben való egyezőségének megállapításán és az egyedi ügyek mélyebb, több módszerrel, eszközzel való elemzésén túl a következő kapacitások jellemzik.

A napjainkban egyre nagyobb nehézséget jelentő káros számítógépes programok, úgynevezett malware-ek és azok közül is az Európában a legnagyobb fenyegetést jelentő zsarolóvírusok elleni küzdelem vonatkozásában kiemelendő a kifejezetten a kártékony programok elemzésére létrehozott Európai malware-elemző rendszer (*European Malware Analyst System; EMAS*), amely jelentős segítséget tud nyújtani a tagállamok számára. A 2013 óta működő és folyamatosan fejlesztett, úgynevezett sandbox technológiára épülő rendszerbe a további vizsgálatok elvégzése érdekében a rendvédelmi szervek elektronikus úton feltölthetik az ügyekben felkutatott malware-mintázatokat, valamint az azokkal összefüggésben keletkezett adatokat, majd az egység az általa megállapítottakat részletes jelentésben küldi vissza az azt kérőnek. A készített jelentés választ adhat az adott kártékony program malware-családjáról, a kiforduló IP-címeiről, az úgynevezett *command and control* szerverekről, valamint a kód lefutásáról.

Az utóbbi években egyre nagyobb népszerűségnek örvendő virtuális valuták a legális tevékenységeken túl a bűnözői körök által végrehajtott műveletekben is igen nagy szerepet játszanak, így a specializált kiberbűnözés elleni egységek is egyre érdeklődőbbé váltak a terület iránt. Az AP CYBORG az online elérhető adatbázisok és az elemzőszoftverek együttes alkalmazásával

hatékonyan képes támogatni a tagállami nyomozásokat. A részükre megküldött, virtuális fizetőeszközöket tartalmazó pénztárcák, úgynevezett *wallet*ek vizsgálata során elvégzik a hozzájuk kapcsolható, azzal összefüggésbe hozható további tárcák felderítését, valamint automatikusan ellenőrzést végeznek az Europol nyilvántartásában annak megállapítása érdekében, hogy az elemzésre megküldött egyedi azonosító nem szerepelt-e a korábbi eljárásokban. Az esetleges találatokról, valamint az elvégzett vizsgálatról jelentést készítenek, amelyet továbbítanak a megkereső félnek. Fontos megjegyezni, hogy a rendszerek segítségével összeállított anyagok a büntetőeljárások során bizonyítékként felhasználhatók, valamint a common law jogrendszer követelményeit figyelembe véve megállapításaikról az egység szakemberei szükség esetén az eljáró bíróság előtt is beszámolnak.

Az elemzői projekt feladatai évről évre bővülnek, ezt jól szemlélteti, hogy 2016-ban 4221 jelzést kellett feldolgozniuk, amelyből 107 egyezőségi, 32 operatív elemzői jelentést készítettek, továbbá 52 műveletben vettek részt, míg 2017-ben már 4254 feladatot dolgoztak fel, amelyből 108 egyezőségi, 52 operatív elemzői beszámolót készítettek, valamint 82 művelet támogatását látták el.

Az AP TWINS a gyermekek szexuális kizsákmányolásához és bántalmazásához kötődő valamennyi online és offline cselekmény elleni küzdelmet és bűnmegelőzési tevékenységet támogatja. Ez felöleli a gyermekek szexuális kizsákmányolását ábrázoló felvételek készítése, terjesztése, kereskedelme elleni fellépést, de a szorosan kapcsolódó úgynevezett *grooming* vagy beszerzési tevékenység, a szexuális zsarolás, az élőképes bántalmazás és az utazó szexuális bűnözők elleni küzdelmet is.

A projekten keresztül megvalósuló információcsere és az elemzések segítségével a tagállamok és az Europol a gyermekek szexuális kizsákmányolásáról készített felvételek klasszikus megosztási platformjai (például „Peer to Peer” fájlcsere) mellett az újabb típusú platformok (például darknet piacterek, online chatszobák stb.) elleni fellépést is igyekszik hatékonyabbá tenni.

Az új típusú bűnelkövetési formák, mint a szexuális zsarolás és a beszerzés, olyan próbatételek elé állítják a rendvédelmi szerveket, amiket csak rendkívül gyors, rugalmas és áldozatközpontú nemzetközi együttműködéssel lehet teljesíteni. Akármelyik bűnelkövetési forma ellen küzdenek is a szakemberek, a legfontosabb cél mindig az áldozatok azonosítása és lehetséges megmentése, kimentése, ideális esetben a valós áldozattá válás megelőzése.

A projekt kiemelt kezdeményezése az áldozatazonosítást elősegítő Áldozatazonosítási Munkacsoport (*Victim Identification Task Force*) kezdeménye-

zés, amelynek keretében a részt vevő tagországok szakemberei évente több alkalommal, hosszabb, akár többhetes időszakig együtt, összehangolva igyekeznek elemezni az ismeretlen áldozatokat ábrázoló képfelvételeket az Europol központjában.

Ki kell emelni továbbá, hogy az elemzői projekten keresztül érkeznek az amerikai NCMEC-jelentések (*National Center for Missing & Exploited Children*; Eltűnt és kizsákmányolt gyermekek nemzetközi központja). A szervezet kormányzati felhatalmazás alapján, konkrét állami feladatokat hajt végre az Egyesült Államokban a gyermekvédelem területén. A hazánkat érintő jelentések az amerikai szolgáltatók (Microsoft, Google, Facebook stb.) által észlelt magyarországi kötődésű gyermekek online szexuális kizsákmányolásával kapcsolatos információkat tartalmazzák. A Magyarországra érkező, évi kb. ezerötyszáz-kétezer jelentés elsődleges elemzését a Készenléti Rendőrség Nemzeti Nyomozó Iroda kiberbűnözés elleni főosztálya végzi, a jelentések alapján évente több tíz büntetőeljárás megindítására is sor kerül.

Az AP TERMINAL a készpénz-helyettesítő fizetési eszközökkel kapcsolatos nyomozások támogatását szolgálja. A tradicionális elkövetési módszerek (például bankkártyamásolás) mellett az új típusú elkövetési módszerekre (például ATM-hackelés) is fókuszál. A készpénz-helyettesítő fizetési eszközökhöz kapcsolódó adatokra és tranzakciókra vonatkozó elemzői tevékenység mellett a projekt célja a széles körű bűnmegelőzési tevékenység is.

Még mindig népszerű elkövetési formák a klasszikus bankkártya-hamisításhoz kötődő bűncselekmények, mint a bankkártyaadatok megszerzését célzó, ATM- és POS-terminálok elleni cselekmények, valamint a hamis bankkártyák elkészítése és felhasználása.

Emellett azonban az internetes vásárlás lehetőségeinek elterjedésével egyenes arányban növekedett az online vásárláshoz szükséges bankkártyaadatok megszerzését célzó adathalász és más csalárd jellegű tevékenységek száma. A megszerzett bankkártyaadatoknak óriási, jellemzően a darknethez kötődő piaca van, így akár több tízezer illegálisan megszerzett bankkártyaadatot is lehet vásárolni az illegális piacokon.

Az EC3 legújabb szervezeti átalakulásaként említhető, hogy a korábbi kezdeményezések eredményeként az idei évtől megkezdte működését az Europol Darkweb Elleni Nyomozó Csoportja is, amely a kibertámadások, a gyermekek online szexuális kizsákmányolása, az online bankkártyás csalások, az emberkereskedelem és a hamisítások területén jártas szakemberekből, valamint a terrorelhárítás, a kábítószer- és a fegyverkereskedelem terén tapasztalt elemzőkből fog állni. A csoport a legnagyobb támogatást az évente

megrendezendő CyberPatrol elnevezésű, a darkneten elérhető illegális tartalmak és szolgáltatások célzott felderítését szolgáló EMPACT-műveletben fogja nyújtani. A csoport célja a darkneten üzemelő illegális piactereken megvalósuló, az említett bűnügyi területekhez kötődő rendvédelmi fellépés fokozása.

Európai kiberbűnözés elleni akciócsoport

Az elemzői projektekhez szorosan kapcsolódik az Europol-tagállamok kiberbűnözés elleni szakegységek vezetőit tömörítő, stratégiai tervezési, véleményezési és tanácsadási feladatokat ellátó Európai kiberbűnözés elleni akciócsoport (*European Cybercrime Task Force; EUCTF*), amelyben a Készenléti Rendőrség Nemzeti Nyomozó Iroda képviseli hazánkat. Az akciócsoport ülésein az önálló kezdeményezések mellett az elemzői projektek keretében keletkezett információk, feladatok megvitatása és a későbbiekben bemutatandó EMPACT-együtműködés támogatása is fontos szerepet játszik.

Europol számítástechnikai bűnözés elleni közös akció-munkacsoport

Szintén ki kell emelni a 2014 szeptemberében alakult, a kiberbűnözéssel kapcsolatos EMPACT-prioritások műveleti karjának is tekinthető számítástechnikai bűnözés elleni közös akció-munkacsoportot (J-CAT). Tagjai a tagállamok, valamint az Europollal operatív együtműködési megállapodást kötő országok rendvédelmi szervei által kifejezetten ebbe az egységbe delegált, kiberbűnözés területén jártas összekötő tisztjei, akik az EC3 szakmai iránymutatása mellett támogatják az országaik által folytatott, továbbá az országaikat érintő nyomozásokat, továbbá az Europol által legfontosabbnak kezelt műveleteket. A korábban két évre alapított, majd két évvel meghosszabbított munkacsoport működése azóta állandó mandátumot kapott, valamint az abban részt vevő tagállamok mellett lehetőség van a munkacsoporthoz egy adott időszakra, kifejezetten egy adott ügy vagy ügyek megoldásának időtartamára csatlakozni. A munkacsoport felállítása óta először 2017 novemberében két hét időtartamra, négy nyomozás támogatására, EMPACT-finanszírozásból Románia delegált egy szakértőt, aki a J-CAT-tagokkal együtműködve hatékonyan tudta támogatni a folyamatban lévő eljárásokat.

A munkacsoport pozitívumai közé tartozik, hogy az egységbe delegált tagállami összekötők egymáshoz közeli irodákban látják el feladataikat, így az információk megosztása, valamint az informális csatornák kialakítása a

leghatékonyabban megoldható. Az egység 2015-ben nyolc, 2016-ban húsz, míg 2017-ben negyvenegy műveletet támogatott a napi szintű – a tagállami összekötő irodákat érintő és azokat az ebbe a csoportba delegált összekötő révén tehermentesítő – megkeresések, adatkérések, koordinációs feladatok ellátása mellett, továbbá tavaly már két közös nyomozó csoportban is feladatokat vállalt.

Az Europol nemzeti összekötő irodák szerepe

Az Europol szervezetében a saját alkalmazásában lévő szakemberek, elemzők és egyéb munkakört ellátó szakértők mellett megtalálhatók a tagállamok és az Europollal operatív együttműködési megállapodást kötő országok összekötő irodái is, amelyek a feladatkörük alapján ellátják a nemzetközi bűnügyi együttműködésből rájuk delegált tevékenységeket, valamint képviselik hazájukat a különböző országok, szervezetek, intézmények előtt. Magyarország vonatkozásában az ORFK Nemzetközi Bűnügyi Együttműködési Központ szervezeti elemeként az Europol Magyar Összekötő Iroda végzi és felügyeli a rendőri együttműködés keretében megvalósuló információcserét, a megkeresések kiküldését, azok – a hazai nyilvántartások ellenőrzését, szükség esetén az eljárást folytató egységekkel való egyeztetést követő – megválaszolását. Fontos fejlesztés, hogy a biztonságos adatcserét lehetővé tevő, úgynevezett SIENA-hálózat kiépítése után jelenleg – az Europol által működtetett Európai Biztonságos Hálózat alkalmazásainak felhasználásával megvalósuló együttműködés és információcsere rendjéről szóló 23/2016. (IX. 15.) BM–NGM együttes utasítás végrehajtásáról szóló 25/2017. (VIII. 17.) ORFK utasításnak megfelelően – a hazánkban SIENA-végponttal bíró szervezeti egységek közvetlenül bekapcsolódtak a nemzetközi információcserébe, így gyakran már a hazai nyomozók készítik és fordítják a megkereséseket, és továbbítják vázlatként az összekötő irodának, ahol annak ellenőrzését és az esetleges hibák javítása, javíttatása után küldik el a címzetteknek.

A 23/2016. (IX. 15.) BM–NGM együttes utasításban foglaltak alapján – a megkeresések és a válasziratok tartalmi és formai színvonala miatt – több egység is teljes jogosultságot kapott, így a kiberbűnözés esetében a Készenléti Rendőrség Nemzeti Nyomozó Iroda kiberbűnözés elleni főosztály végpont felhasználói közvetlenül, az összekötő iroda érintése nélkül képesek akár a társszervekkel együttműködést folytatni.

Az összekötő iroda tehát az egyszerűbb megítélésű, az adattárakban való ellenőrzést követően, többletinformáció nélkül megválaszolható, részükre

megküldött megkereséseket önállóan – a szakmai relevanciától függően, esetleg a kiberbűnözés elleni főosztályt később tájékoztatva – megválaszolják, míg az összetettebb vagy egy konkrét ügyre vonatkozó adatkéréseket a főosztálynak a további intézkedések megtétele céljából megküldik.

Az összekötő iroda a napi szintű SIENA-üzenetek kezelésén túl kapcsolatot tart az EC3 és a J-CAT munkatársaival, valamint szükség esetén – amennyiben a hazai eljárást folytató szerv akadályoztatva van, vagy az idő rövidsége indokolja – részt vesznek az Europol vagy más tagállam által szervezett műveleti találkozókban, amelyeken az előzetes egyeztetések alapján képviselik a hazai érdekeket, majd pedig annak végeztével tájékoztatják az eljáró szerveket. Az összekötő iroda által ellátott további tevékenységként említhető, hogy ha egy kiemelt jelentőségű ügyben azonnal szükséges az információ beszerzése, akkor személyesen, közvetlenül veszik fel a kapcsolatot más országok összekötőivel, ezzel segítve a bűnfelderítési célok hatékony megvalósulását.

Interpol

A jelenleg 192 tagországot soraiban tudó lyoni székhelyű Interpol a kiberbűnözés elleni küzdelemben főként a harmadik országokkal való nemzetközi bűnügyi együttműködésben nyújt segítséget hazánknak.

Az Interpol a már jól ismert adatkérésekkel, személy- és tárgyközvetésekkel, kiadatásokkal, eljárási jogsegélyekkel kapcsolatos feladatainak ellátása mellett az utóbbi időben kiemelt figyelmet fordít a terrorelhárítás és a klaszszikus szervezett bűnözés területein kívül a kiberbűnözés elleni küzdelemre. A célkitűzés súlyát és a feladat fontosságát jelzi, hogy a szervezet 2015-ben megnyitotta a szingapúri globális innovációs komplexumát, amelynek fő feladata a tudomány és technológia területén kiemelt szakértelemmel bíró szervezetekkel együttműködve a kiberbűnözés mértékének visszaszorítása, az alkalmazható technológiák kifejlesztése, megosztása, valamint a rendvédelmi szervek munkatársainak képzése.

Az Interpolnál több olyan, a bűnügyi munkát, illetve a bűnmegelőzést támogató projekt van, amelyek nagyban segítik a tagállamok munkáját. A gyermekek sérelmére elkövetett szexuális kizsákmányolás területén kiemelendő az Interpol gyermekek sérelmére elkövetett szexuális bűncselekmények nemzetközi képi adatbázisa (*International Child Sexual Exploitation*). A 2009 márciusában létrehozott adatbázishoz 49 országnak van hozzáférése, köztük a Ké-

szenléti Rendőrség Nemzeti Nyomozó Irodán keresztül hazánknak is. Az adatbázis több százezer képfelvételt tartalmaz, köztük több mint tízezer már azonosított gyermek áldozattal kapcsolatos felvételt. Az adatbázis fő célja az abba feltöltött, ismeretlen áldozatokat ábrázoló felvételekkel kapcsolatos elemzési tevékenység támogatása, ezzel az áldozatazonosítások és -megmentések számának növelése. A rendszer segítségével hazánkban az elmúlt években több sikeres áldozatazonosítás és gyanúsított felelősségre vonás is történt.

Itt kell megemlíteni az Interpol *Worst of List* kezdeményezését, a szervezet által karbantartott és rendszeresen frissített linkgyűjteményt, adatbázist, amely a nyílt interneten keresztül elérhető, a gyermekek szexuális kizsákmányolását ábrázoló felvételeket tartalmazó linkekre vonatkozik. Az adatbázis segítségével már akár közvetlenül az internetszolgáltatókon keresztül is elérhetővé lehet tenni ezeket a linkeket az internet-előfizetők számára, csökkentve ezzel a képfelvételeken szereplő gyermekek minden egyes megtekintéssel megvalósuló ismételt áldozattá válását. Hazánkban jelenleg folyamatban van az adatbázis alkalmazásának jogszabályi háttérét megteremtő egyeztetés az érintett állami, civil és gazdasági szereplők közreműködésével.

Természetesen az „Interpol-csatorna” a legfontosabb olyan információcserét elősegítő csatorna, amelyen keresztül hazánk jellemzően a nem európai uniós országokkal szükséges rendvédelmi információcserét bonyolítja le. A csatorna alkalmas konkrét bűnügyi információk, személyi adatok megosztására, illetve a rendőri együttműködés keretein belül megvalósítható, konkrét nyomozásokhoz köthető kérések továbbítására is az Interpol által üzemeltetett I–24/7 globális rendőri kommunikációs csatornán keresztül. Az Interpol Magyar Nemzeti Iroda az ORFK Nemzetközi Bűnügyi Együttműködési Központ keretein belül működik.

24/7 kiberbűnözés elleni kapcsolattartási pontok

Az úgynevezett 24/7 kapcsolattartási pontok lényege, hogy a hálózatban részt vevő országok folyamatos, nonstop ügyeleti rendszert működtetnek a megkezesések fogadása és kiküldése érdekében. Magyarországot érintően három azonos célt szolgáló, de alapvetően különböző eredetű 24/7 kiberbűnözés elleni kapcsolattartási pontról beszélhetünk.

Az első a 2004. évi LXXIX. törvénnyel kihirdetett, az Európa Tanács Budapesten, 2001. november 23-án kelt számítástechnikai bűnözésről szóló egyezményéhez (budapesti egyezmény vagy cybercrime egyezmény) kapcsolódó, az

Európa Tanács szervezete által karbantartott, úgynevezett COE 24/7 hálózat. Ennek a hálózatnak az egyezményhez csatlakozó államok a tagjai, jelenleg összesen 52 ország. Az európai országok között jellemzően ez a leggyakrabban alkalmazott sürgősségi csatorna.

A második a G7 együttműködési fórumhoz kapcsolódó, az Egyesült Államok igazságügyi minisztériuma által karbantartott úgynevezett G7 24/7 hálózat. Ennek 71 ország a tagja. A nem európai országok között jellemzően ez a leggyakrabban alkalmazott sürgősségi csatorna.

A harmadik lehetséges csatornaként természetesen meg kell említeni az Interpol-együttműködéshez köthető, az Interpol által üzemeltetett úgynevezett I-24/7 globális rendőri kommunikációs csatornát. Ennek a hálózatnak az Interpol-tagországok a tagjai, több mint 190 állam.

Magyarország képviselőjében az ORFK Nemzetközi Bűnügyi Együttműködési Központ a kijelölt 24/7-es kapcsolattartási pont valamennyi hálózatban, de a Készenléti Rendőrség Nemzeti Nyomozó Iroda kiberbűnözés elleni főosztálya is meg van jelölve valamennyi hálózatban mint kijelölt szakmai kapcsolattartási pont.

A 24/7 hálózatokon keresztül jellemzően olyan, a rendvédelmi együttműködéshez köthető megkeresések érkeznek, mint az elektronikus adatok megőrzésére vonatkozó kérelem, későbbi igazságügyi jogsegélykérelemhez kötődő kérdések, kérések, de akár késedelmet nem tűrő más, kiberbűnözéshez kötődő információk átadása is megvalósulhat, vagy halasztást nem tűrő, azonnali intézkedések végrehajtására vonatkozó kérések is érkezhetnek.

Gyakorlati példaként említhető meg a Készenléti Rendőrség Nemzeti Nyomozó Iroda kiberbűnözés elleni főosztályán folyamatban lévő nyomozás, amelynek keretében egy európai tagország területén található szerveren tárolt adatok soron kívüli megőrzésére, majd lefoglalására volt szükség annak érdekében, hogy ha a szabadlábon lévő, még el nem fogott elkövetők a szerver tartalmát esetleg távolról törölnék, az a későbbiekben rendelkezésre álljon. Az adatok megmaradása érdekében a COE 24/7 hálózaton keresztül megkeresés kiküldésére került sor az adott országba, amelynek a rendőri szervei néhány órán belül lehetővé tették a külföldi tárhelyszolgáltatón keresztül az adatok megőrzését, ezeket később európai nyomozási parancs megküldésével foglalták le.

Az EMPACT feladatrendszer

Hazánk az Készenléti Rendőrség Nemzeti Nyomozó Irodán, illetve a Nemzeti Adó- és Vámhivatalon keresztül tevékenyen részt vesz az Europol támogatása mellett folyamatban lévő EMPACT-munkában (*European Multidisciplinary Platform Against Criminal Threats*; Európai multidiszciplináris platform a bűnügyi fenyegetettség ellen). Az EMPACT egy olyan ad hoc menedzsmentkörnyezet, amely azért fejleszt ki egyes cselekvéseket, hogy elősegítse az előre meghatározott közös bűnügyi célok elérését.³ A tagállamok, az EU ügynökségei és intézményei, a harmadik államok, valamint az állami és magánszervezetek olyan strukturált multidiszciplináris együttműködési platformja, amely a sürgősként meghatározott súlyos és szervezett nemzetközi bűncselekmények ellen küzd.

A munka lényegében az Európai Unió égisze alatt, a nemzetközi szervezett bűnözés elleni hatékony fellépés érdekében kialakított feladatrendszer, amelynek keretében több, különböző prioritást (például emberkereskedelem, szintetikus drogok, illegális bevándorlás, kiberbűnözés stb.) érintően végeznek közös munkát a kijelölt EMPACT nemzeti szakértők az Europol segítségével. A különböző bűnügyi területeken végzendő, összeurópai rendvédelmi tevékenység érdekében évente úgynevezett operatív akcióterveket (*Operational Action Plan*; *OAP*) hoznak létre, amelyek összehangolják az adott területen végrehajtandó feladatokat.

A feladatok rendkívül sokfélék lehetnek. A leggyakoribbak az összehangolt, közös akciók, akciónapok, végrehajtások megszervezése, amely valamennyi részt vevő tagországtól konkrét operatív felderítések és/vagy nyomozások lefolytatását, összehangolt házkutatások, elfogások végrehajtását várja. Emellett természetesen akár közös képzések és konferenciák megszervezése, bűnmegelőzési kampányok lefolytatása, kutatások kezdeményezése, civil partnerekkel történő együttműködések kialakítása is a feladatrendszer része lehet.

A rendőrséget érintő valamennyi prioritás területén a Készenléti Rendőrség Nemzeti Nyomozó Iroda képviseli Magyarországot. A kiberbűnözéshez kötődően a gyermekek szexuális bántalmazása/kizsákmányolása (child sexual exploitation/abuse EMPACT CYBER – CSA/CSE), az információs rendszerek elleni támadások (EMPACT CYBER AAIS; attacks against information systems), illetve készpénz-helyettesítő fizetési eszközökkel való visszaélés

³ Hegyaljai Máttyás: Az EMPACT mint rendészeti válasz az európai bűnözésre. In: Gaál Gyula – Hautzinger Zoltán (szerk.): Tanulmányok a „Biztonsági kockázatok – rendészeti válaszok” című tudományos konferenciáról. Pécs, 2014, 127–134. o. [Pécsi Határőr Tudományos Közlemények XV.]

(EMPACT Non-cash payment) munkacsoportokban folyik az összehangolt munka. Csak hogy érzékeltessük a munka jelentőségét és hasznosságát, néhány példa az egyes szakterületek által végrehajtott közös feladatokról az elmúlt évekből.

Kiváló példa a konkrét műveleti munka és a bűnmegelőzés összekapcsolására az EMPACT CYBER AAIS együttműködés keretében végrehajtott egyik közös akció, amelynek célja a közepesen felkészült, információs rendszerek elleni támadásokat végrehajtó, alapvetően fiatalabb bűnelkövetők felderítésére és elfogására irányuló nyomozások lefolytatása és az elkövetők elszámoltatása mellett egy olyan bűnmegelőzési kampány indítása volt, amely az informatikában jártas fiatalokat célozta.

Az akció keretében több olyan, jellemzően fiatalos vagy fiatal felnőtt elkövető beazonosítása és elfogása történt meg, akik weblapok elleni túlterheléses, vagy különböző, adatlopásokat megvalósító támadásokat hajtottak végre.

Az akcióhoz kapcsolódó, *Cyber Crime vs. Cyber Security: What will you choose?* (Kiberbűnözés vagy kiberbiztonság: Mít választasz?) elnevezésű kampány⁴ arra biztatta a fiatalokat, hogy a kiberbűnözői életmód helyett a civil szférában, informatikai vállalatoknál vagy akár a kiberbűnözés ellen küzdő rendvédelmi szerveknél kamatoztassák a számítástechnikai tudásukat.

Az EMPACT Non-cash payment együttműködés keretében minden évben az éves feladatrendszer része, az úgynevezett Globális repülőtéri akciónapok (*Global Airport Action Days*) elnevezésű operatív akciósorozat, amelynek célja a lopott bankkártyaadatok felhasználásával vásárolt repülőjegyekkel kapcsolatos visszaélések elleni összehangolt fellépés. A 2017-ben⁵ tizedik alkalommal megrendezett akcióban 61 ország – köztük hazánk – és 63 légitársaság vett részt, 226 repülőteret érintve világszerte. Az akciónak köszönhetően 298 gyanús tranzakció feltárására került sor, és 195 személyt számoltattak el. Az akciósorozat az európai tagországok egymás közötti együttműködése mellett remek példa a harmadik országokkal történő együttműködésre is.

A gyermekek online szexuális kizsákmányolása és bántalmazása elleni EMPACT-összefogás keretén belül talán a legtöbb a bűnmegelőzési jellegű feladat. Tisztán bűnmegelőzési jellegű, ám a témából fakadóan igen érzékeny területet érintő közös kampány volt a *Say No!* (Mondj nemet!) kampány,

4 <https://www.europol.europa.eu/activities-services/public-awareness-and-prevention-guides/cyber-crime-vs-cyber-security-what-will-you-choose>

5 <https://www.europol.europa.eu/newsroom/news/195-individuals-detained-result-of-global-crack-down-airline-ticket-fraud>

amelynek célja az online szexuális zsarolásokra történő figyelemfelhívás, illetve az áldozattá válás megelőzésének lehetőségei. A kampány keretében egy részletes ismertető anyag⁶ elkészítése mellett grafikákkal és a részt vevő tagországok nyelvére – így magyarra is – lefordított kisfilmmel⁷ igyekeztek a részt vevő rendvédelmi egységek felhívni a figyelmet a szexuális zsarolás veszélyeire.

Bilaterális együttműködések

A kétoldalú együttműködések a nemzetközi bűnügyi kooperáció igen jelentős szeletei, amelynek költségeit szükség esetén az Europol részben fedezi. Az ügynökség épületébe szervezett műveleti találkozók megtartásához szükséges utazási költségek lehívására két mód áll rendelkezésre, a kisebb összegű támogatások, illetve a nagyobb összegű támogatások rendszere. A legalább két tagállam részvételével megtartandó munkamegbeszélés költségeinek viselése kapcsán benyújtott kisebb összegű támogatások rendszerébe eső pályázat engedélyezése akár két hét alatt is megtörténhet, így a bűnmegelőzési, büntelítési érdekek még inkább biztosíthatóvá válnak.

A kétoldalú együttműködést támogatja továbbá az Eurojust is, amely nagy súlyt fektet a kiemelt kibertámadások során rövid időn belül összeállítható JIT-megállapodás mintáinak megszerkesztésére. Megfigyelhető, hogy a rendelkezésre álló pénzügyi keret évről évre növekszik, valamint hogy 2017-ben az Eurojust összesen kétszáz JIT-et támogatott, amelyek közül 87 aláírására tavaly került sor.

A kiberbűnözés országhatárokon átnyúló jellege, valamint az elkövetői csoportok vegyes összetétele miatt a számítógépes bűnözés elleni egységek és így a Készenléti Rendőrség Nemzeti Nyomozó Iroda kiberbűnözés elleni főosztály napi munkavégzésében is hangsúlyos szerepet kap a más országok bűnüldöző hatóságaival való együttműködés, a megszerzett információk megosztása. Különösen intenzív és hatékony a főosztály együttműködése az Egyesült Államok szövetségi rendvédelmi szerveivel, így a Szövetségi Nyomozóirodával (*Federal Bureau of Investigation*) és a Belbiztonsági Nyomozó Irodával (*Homeland Security Investigation*), illetve a Német Szövetségi Bűnügyi Hivatallal (*Bundeskriminalamt*).

⁶ <https://www.europol.europa.eu/publications-documents/online-sexual-coercion-and-extortion-form-of-crime-affecting-children-law-enforcement-perspective>

⁷ <https://www.youtube.com/watch?v=ufTgIJ2zKTE&feature=youtu.be>

Pozitív példaként említhető, hogy hatóságunk az Egyesült Államok bevándorlási és vámhivatal belbiztonsági nyomozóegységének (*United States Immigration and Customs Enforcement Homeland Security Investigations*) bűnügyi jelzése alapján nyomozást rendelt el gyermekpornográfia büntett gyanúja miatt, mivel a társszerv jelzése, illetve a nyomozás során beszerzett adatok szerint megalapozott gyanú merült fel arra, hogy az elkövetők egy olyan weboldalt üzemeltettek, amelyen keresztül az oda regisztráló, főleg külföldi személyek tömegesen osztottak meg tizennyolc évesnél fiatalabb személyekről készült, a nemiséget súlyosan szeméremsértő nyíltsággal ábrázoló fénykép- és videófelvételeket.

Az Egyesült Államok bevándorlási és vámhivatal bécsi regionális képviseletével (*United States Immigration and Customs Enforcement Regional Attaché Vienna, Austria*), illetve a belbiztonsági nyomozóegység charlestoni irodájával (*Homeland Security Investigations Charleston, South Carolina*) folytatott kiterjedt bűnügyi együttműködés következtében hatóságunk házkutatást tartott az elkövetők lakásaiban, majd az eljárás eredményes lefolytatása nyomán a két személy tekintetében az illetékes ügyészség vádemelési javaslatot tett gyermekpornográfia büntettének elkövetése miatt.

További pozitív példa az Amerikai Egyesült Államok és Magyarország között elsőként megkötött közös nyomozó csoport felállításáról szóló megállapodás, amelynek célja egy a darkneten elérhető, főként kábítószereket és illegálisan megszerzett személyazonosító adatokat kínáló oldalt kiszolgáló szerverrel, valamint annak adminisztrátorával kapcsolatos minden lehetséges adat beszerzése, továbbá az érintett eszközökön tárolt adatok lefoglalása volt. A bevezetett nyomozati cselekmények után a Szövetségi Nyomozóiroda munkatársainak részvételével házkutatás keretében sor került az érintett szerveren tárolt adatok lefoglalására, majd az amerikai fél a nyomozása során korábban beszerzett adatok alapul vételével megkezdhette a kiszolgáló szerveren tárolt információk elemzését, vizsgálatát.

A bemutatott nemzetközi együttműködési lehetőségek alapján látható, hogy a rendvédelmi szervek elsőrendűként tekintenek a kiberbűnözés területére, valamint hogy egy adott ügy megoldása során a beszerezni kívánt adatok és más ország rendvédelmi szerveivel való közvetlen együttműködés szükségessége alapján mérlegelni kell az alkalmazható kommunikációs csatornákat, majd megválasztani az alkalmazandót.

Végezetül fontos megemlíteni az együttműködés normatív hátterét. A kiberbűnözés területén folytatott nemzetközi együttműködés jogszabályi alapjait a bűnüldöző szervek nemzetközi együttműködéséről szóló 2002. évi

LIV. törvény teremti meg, amelynek célja, hogy – a felderítés hatékonyságának növelése érdekében – szabályozza a magyar bűnüldöző szerveknek a bűnmegelőzés és a bűnüldözés során külföldi hatóságokkal folytatott együttműködését.

Az Európai Unió tagállamaival folytatott együttműködés területén kiemelt jelentőségű továbbá az Európai Unió tagállamaival folytatott bűnügyi együttműködésről szóló 2012. évi CLXXX. törvény, amelynek célja az uniós tagországok közötti együttműködés gyorsítása és egyszerűsítése.

Természetesen a büntetőeljárások során a nemzetközi bűnügyi jogsegélyről szóló 1996. évi XXXVIII. törvény rendelkezéseit is figyelembe kell venni az eljárási jogsegélyek kérése és végrehajtása során.