DOI:10.38146/bsz-ajia.2012.v60.i6.pp87-107

SZALÁRDI GÁBOR

A csúcstechnológiai bűnözés elleni küzdelem támogatása

A világháló használata és az abból fakadó előnyök a huszonegyedik század emberének ma már természetes dolog. Megtalálható az otthonokban, munkahelyeken és a szórakozóhelyeken is. A vezeték nélküli hálózat lehetővé tette azt is, hogy mostanra akár a nyílt utcán vagy utazás közben is elérhetők legyünk. Végfelhasználók milliói osztják meg magánügyeiket biztonságosnak vélt csatornákon keresztül ismerőseikkel, miközben a számítógépen futó programok és az internetes alkalmazások automatikusan adatok halmazát gyűjtik rólunk. Ez a halmaz az átlagember számára értéktelen és nem is elérhető.

Tény azonban, hogy az internethasználóknak van egy olyan, egyre bővülő köre, amelynek tagjai autodidakta módon, tanulmányaik során, illetve munkájukból adódóan magasabb szinten kezelik a számítógépeket, az internetet, és a megszerzett tudásukat személyes adatok illegális gyűjtésére, valamint szándékos károkozásra, illetve anyagi haszonszerzésre használják (botnet[1], malware, vírusok stb.). A következő jellemző bűncselekmények fordulnak elő:

– személyazonosság-lopás;
– internetes banki ügyintézés adatainak másolása;
– elektronikus kereskedelemmel összefüggő csalások;
– elektronikus pénzmosás.

Az elkövetők elfogása és bíróság elé állítása hihetetlenül bonyolult feladat, hiszen a hatóságok sem automatikusan szereznek tudomást a bűncselekményről, gyakran ugyanis a sértettben sem tudatosul az áldozattá válás ténye. Továbbá az elkövető azonosítása is rendkívül nehéz feladat, hiszen fizikailag nem kell Magyarországon lennie annak, aki betör egy titkosított hálózat tagjaként működő kormányzati számítógépbe, vagy indít az interneten automatikusan továbbműködő károkozót.

1 Vírussal fertőzött számítógépek hálózata, amelyekkel a felhasználó tudta nélkül lehet támadást indítani információs rendszerek ellen (az eddigi legnagyobb botnet 24 óra alatt kb. ötvenezer fertőzött számítógéppel állt fel).

Gyermekek szexuális kizsákmányolása

Az internet térnyerésével előtérbe került egy olyan bűncselekményi kategória, amely mára a csúcstechnológiai bűnözés egyik, a társadalomra legveszélyesebb részévé vált.

A gyermekek szexuális kizsákmányolására irányuló, azokat ösztönző, anyagi forrással ellátó bűncselekmények viszonylagos latenciája és anonimitása miatt vonzó az azonos érdeklődési körű emberek között.

Ezek a bűncselekmények

- pornográf tartalmú (ingyenesen és térítés ellenében letölthető) internetes oldalak üzemeltetése, használata (letöltés és feltöltés);
- pornográf témájú közösségi oldalak, fórumok létrehozása, fenntartása és használata.

Mindkét elkövetési módszer magától értődő módon a gyermekek szexuális kizsákmányolását *(Child Sexual Exploitation; CSE)* erősíti, újabb és újabb potenciális elkövetőt teremtve. Az internetes le- és feltöltő oldalak addig szaporodnak, amíg a rajtuk megjelenő videókra, képekre van kereslet.

A feltöltött anyagok iránt érdeklődők sokszor úgy gondolják, hogy nem ártanak senkinek, holott ennek éppen a fordítottja igaz. Az érdeklődés, a gyakori letöltés újabb film vagy kép elkészítéséhez vezet. Természetesen ezen oldalak látogatása most még térítés ellenében történik.

A bevétel sok esetben szervezett bűnözői csoportokhoz kerül, amelyek ebből a pénzből finanszíroznak súlyos, országhatárokon átnyúló bűncselekményeket (terrorizmus, kábítószer-kereskedelem, fegyverkereskedelem, embercsempészés, emberkereskedelem stb.).

A pornográf témájú közösségi oldalak, fórumok általában egyetlen célt szolgálnak: olyan platformot fenntartani és használni, amelynek segítségével a „témában érintett" vagy még „csupán érdeklődő" személyek tapasztalatokat, információkat cserélhetnek.

Együttműködés

Az Európai Unió bűnüldözési információs rendszere és a Nemzetközi Bűnügyi Rendőrség Szervezete keretében megvalósuló együttműködésről és információcseréről szóló 1999. évi LIV. törvény felhatalmazása alapján az *ORFK Nemzetközi Bűnügyi Együttműködési Központ (Nebek)* jogosult a két-

és többoldalú nemzetközi szerződésben részes állammal folytatott együttműködés során adat-, információtovábbításra, illetve adatok és információk igénylésére. Feladatait a rendelkezésre álló információs csatornák (Europol[2], Interpol[3], SIS/SIRENE[4], SELEC[5]) használatával látja el, ebben kiemelt szerepet vállal az Europol Nemzeti Irodához tartozó és Hágába kihelyezett Europol Magyar Összekötő Iroda.

A Nebek a csúcstechnológiai bűnözés és a gyermekek szexuális kizsákmányolása vonatkozásában elsősorban a következő három nyomozó szervvel működik együtt:

– Nemzeti Nyomozó Iroda Bűnügyi Főosztály Csúcstechnológiai Bűnözés Elleni Osztály,
– Budapesti Rendőr-főkapitányság Gazdaságvédelmi Főosztály Gazdaságvédelmi Osztály I. Számítógépes Bűnözés Elleni Alosztály,
– Budapesti Rendőr-főkapitányság Bűnügyi Főosztály Gyermek- és Ifjúságvédelmi Osztály.

Valamennyi tagország nyomozó szervének a nyomozások során egyetlen célja lehet: az interneten fellelt pornográf tartalmú kép vagy videó alapján eljutni a szexuális erőszakot elszenvedő áldozathoz, az elkövető személyhez és felszámolni a bűnözői hálózatot.

Az információtechnológia hihetetlen léptékű fejlődése és az internet gyors előretörése miatt a szervezett bűnözői hálózatok elleni hatékony küzdelem csak szoros együttműködéssel valósítható meg, elsősorban az igazságügyi szervek, az informatikai iparág szereplői, az internetszolgáltatók, a banki szektor és a nem kormányzati szervezetek között.
A megoldásra törekvés adott, ezt a Nebek teljes mértékben támogatja.

Európai Unió

Az EU legtöbb polgára napi szinten használja valamely információtechnológiai vagy kommunikációs csatornát, amelyet természetes módon biztonságosnak és megbízhatónak gondol. A kommunikációs csatornák biztonsága

2 Európai Rendőrségi Hivatal.
3 Nemzetközi Bűnügyi Rendőrség Szervezete.
4 Schengeni Információs Rendszer/Kiegészítő információ kérése a nemzeti bevitel szintjén.
5 Délkelet-európai Rendészeti Központ.

fontos tényező, a magánélethez és a szólásszabadsághoz fűződő alapjogok tiszteletben tartása azonban még fontosabb.

Európa elkötelezett híve az internet felhasználásával – különösen a gyermekek sérelmére – elkövetett bűncselekmények elleni küzdelemnek, és mindent megtesz a bűnözés visszaszorításáért.

A gyermekek sérelmére elkövetett szexuális zaklatás és a szexuális kizsákmányolásra irányuló bűncselekmények különösen nagy károkat okoznak a gyermekek fizikai és pszichológiai fejlődésében, megnehezítik a társadalomba való beilleszkedés folyamatát.

Az internet rendkívül gyors terjedése mellett a bűnügyi szervek korlátozott lehetőségei is a bűncselekmények elkövetését segítő tényezők. Továbbá kiemelt problémaként kezelendő a sértetti kör bizonyos fokú ismeretlensége: az áldozatok, félve a megaláztatástól, bizonytalanok a megfelelő segítségnyújtást és támogatást illetően, ezért nem tesznek feljelentést.

Uniós irányelvek

Cybercrime

Az Európai Parlament és a Tanács közös irányelvjavaslatot dolgozott ki *az információs rendszerek védelme érdekében*[6]. A javaslattal párhuzamosan számos egyéb programot indítottak útjára, illetve terveznek elindítani pályázat kiírásával:

– bűnmegelőzési és bűnüldözési program *(Prevention of and Fight against Crime; ISEC)*;
– büntető igazságszolgáltatás program *(Criminal Justice; JPEN)*;
– biztonságosabb internet program *(Safer Internet Programme; SIP)*.

Az irányelvjavaslat célja olyan, az információtechnológiát érintő és felhasználó tevékenységek egységes büntetőjogi ágba való bevonása, amelyek eddig a nemzeti szinteken való jogszabályi háttér különbözőségei miatt szankciók nélkül maradó cselekmények voltak. Ilyenek az információs rendszerekbe való jogosulatlan belépés, illegális adat- és rendszerművelet, e műveletekre való felbujtás, segítségnyújtás és ezek kísérlete.

6 Az információs rendszerek elleni támadások visszaszorítása és a 2005/222/JHA tanácsi kerethatározat hatályon kívül helyezéséről szóló COM(2010) 517. számú irányelvjavaslat (2010).

A javaslat egy új büntetőjogi kategóriát is bevezet, a jogosulatlan információszerzést. A tevékenység magában foglal minden olyan magatartást, amely egy információs rendszer használatával, nem nyilvános csatornán keresztül továbbított számítógépes adat céleszközzel történő megszerzésére irányul.

Legfontosabb célja az eddig ismertté vált, de nem szankcionált számítógépes támadások (botnet), valamint a bűncselekményhez használt speciális eszközök gyártásának, árusításának, terjesztésének és megszerzésének büntethetővé tétele, illetve a nemzetközi ügyek kapcsán végzett nyomozások és bírósági eljárások könnyebbé tétele, gyakorlat kialakítása.

Az irányelvjavaslat érint egy csupán részben rendészeti, igazságügyi területet is. A javaslat kidolgozói és a javaslatot bírálók szerint is szükség van ugyanis a rendőri szervek és a magánszektor közötti együttműködés erősítésére a 24 órás elérhetőségű rendőri kapcsolattartó pontok számának növelésével, hatáskörének bővítésével, illetve egy rendőr–civil EU-hálózat létrehozásával, amelynek tagjai szakértők és hatóság. Szükség van a rendőri szervek és az internetszolgáltatók, nagyobb szervertulajdonosok közötti együttműködést ösztönző, uniós szintű megállapodásra.

Gyermekek szexuális kizsákmányolása

A bűnözés elleni hatékony fellépés érdekében 2010. március 29-én Brüsszelben elfogadták a gyermekek szexuális zaklatása, szexuális kizsákmányolása és a gyermekpornográfia elleni küzdelemről szóló, az Európai Parlament és a Tanács közös irányelvjavaslatát, amely azonban nem az első európai szintű kísérlet a probléma kezelésére. Felismerve az internet, az információtechnológia és a gyermekek szexuális kizsákmányolására irányuló bűncselekmények közötti kapcsolatot, a tanács 2000 óta számos határozatot hozott az információs rendszerek és a gyermekek védelme érdekében.

Az uniós irányelv főbb vívmányai a 2004/68/IB[7] kerethatározat integrálása után a következők[8]:

– Büntethetővé nyilvánítja a gyermekek szexuális zaklatásának és kizsákmányolásának azokat a súlyos formáit, amelyek jelenleg nem tartoznak az uniós

7 A gyermekek szexuális kizsákmányolása és a gyermekpornográfia elleni küzdelemről szóló 2004/68/IB tanácsi kerethatározat (2003. 12. 22.).

8 A gyermekek szexuális zaklatása, szexuális kizsákmányolása és a gyermekpornográfia elleni küzdelemről, valamint a 2004/68/IB kerethatározat hatályon kívül helyezéséről szóló COM(2010)94 javaslat (2010. 03. 29.).

jogszabályok hatálya alá (szexuális bűncselekmények elkövetése céljából szervezett utazás, különösen gyermekszexturizmus).
– Emeli a büntetőjogi szankciók mértékét a visszatartó erő növelése érdekében.
– Büntethetővé nyilvánítja a szexuális zaklatás és kizsákmányolás új, az informatika alkalmazásával lehetővé vált formáit (online pornográf előadások, gyermekpornográf anyaghoz való tudatos hozzáférés).
– Új bűncselekmények meghatározása (grooming, azaz szexuális kapcsolatra való felhívás és letöltés nélküli pornográf tartalmú kép vagy videó megtekintése).
– A nyomozások és a vádemelések elősegítése érdekében rendelkezések.
– Módosítja a jogszabályokat annak érdekében, hogy a gyermekek szexuális zaklatásának és kizsákmányolásának az unióból származó elkövetői (állampolgárok és állandó lakosok) akkor is eljárás alá vonhatók legyenek, ha bűncselekményeiket az EU-n kívül követik el.
– Új rendelkezések az áldozatok jogorvoslatainak elérhetősége érdekében.
– A gyermekpornográfiához való internetes hozzáférés korlátozása.

Uniós programok, projektek

Biztonságos internet program[9]

Az internetet és egyéb kommunikációs technológiát használó gyermekek védelme érdekében létrehozott többéves közösségi program[10] keretében egy hármas tagozódású pályázat kiírására került sor olyan projektek fogadása és elbírálása céljából, amelyek fő törekvése a gyermekek védelme. A befogadott projekt szakmai elemzésére szaktudással bíró, szintén pályázati úton bekerülő cég felkérésére kerül sor. A projekt megvalósítása a pályázat harmadik szintje. A biztonságos internet program a következő négy elemre épül:
– ismeretterjesztés;
– illegális tartamú oldalak elleni elkötelezett harc;
– biztonságosabb online környezet hirdetése;
– tudásközpont megvalósítása.

Fő célkitűzése olyan biztonságos internetközpontok *(Safer Internet Centres; SIC)* létrehozása Európa-szerte, amelyek a koordinátori szerepkörüknél fog-

9 http://ec.europa.eu/home-affairs/policies/crime/crime_sexual_en.htm
10 Multi-annual Community Programme on protecting children using the Internet and other communication technologies.

va lehetővé teszik az illegális tartalmú oldalak elleni küzdelemhez nélkülözhetetlen tudás terjesztését. Efféle központok jelenleg harminc országban találhatók, ellátják felvilágosító tevékenységüket, bejelentik az illegális adattartalmú oldalakat és segítséget nyújtanak a családoknak.

Az illegális tartalmú oldalak elleni eredményes küzdelem érdekében a biztonságos internet program keretén belül sor került az Internet-hotline-ok Nemzetközi Szövetsége *(International Assosiation of Internet Hotlines; INHOPE)* elnevezésű hálózat, a segítségnyújtás, valamint az állandó elérhetőség érdekében pedig a Felvilágosító Központok Európai Hálózata *(European Network of Awareness Centres; INSAFE)* megalapítására.

CIRCAM-projekt[11]

Az Európai Rendőri Vezetők Munkacsoportja *(European Police Chief Task Force; EPCTF)* által 2004-ben életre hívott és a rendőrség átfogó műveleti stratégiai tervezése *(Comprehensive Operational Strategic Planning for the Police; COSPOL)* elnevezésű projekt célja a rendőri szervek szervezett és súlyos bűncselekmények felderítésére irányuló stratégiai tervezésének elősegítése az EU valamennyi szintjén megvalósuló koordinációval és a felek közötti kommunikációval.

A COSPOL valójában egy többoldalú, a rendőri szerveket segítő eszköz, amelyet terroristák, szervezett bűnözői hálózatok és csoportok vezetőinek elfogására és a szervezet felszámolására irányuló rendőri akciók és nyomozások támogatása érdekében hoztak létre. A COSPOL-projekten belül megvalósuló együttműködés alapfeltétele az Europol nyújtotta lehetőségek kihasználása.

Számos bűncselekmény-kategóriát (kábítószer, csúcstechnológiai bűnözés stb.) érintő projekt fut a COSPOL égisze alatt.

A CIRCAM- *(COSPOL Internet Related Child Abuse Material)* projektet az Európai Rendőri Vezetők Munkacsoportja 2004-ben indította útjára az interneten terjesztett illegális, pornográf tartalmú anyagok visszaszorítása érdekében. A projekt kiemelkedő sikereket ért el a gyermekek szexuális kizsákmányolására irányuló anyagok terjesztését akadályozó szűrő *(Child Sexual Abuse Anti Distribution Filter; CSAADF)* tagországok közötti terjesztésében, amelynek alapja az érintett domén blokkolása. A projekttagok folyamatosan elemzik a célterülettel érintett bűnözés várható irányait és a beavatkozás le-

11 http://circamp.eu

hetséges eszközeit, a megvalósításhoz magasabb szintű műveleti megközelítés szükséges.
A projekt műveleti és elemzői támogatást kap az Europoltól és az Interpoltól.
A CIRCAM-hálózat céljai a következők:

– pornográf anyagok készítésére és terjesztésére specializálódott bűnözői hálózatok és szervezetek azonosítása és felszámolása, az elkövetők elfogása és segítségnyújtás az áldozatoknak;
– együttműködés az internet használatára vonatkozó általános gyakorlat kialakítása érdekében;
– európai szintű segítségnyújtás a pornográf tartalmú anyagok terjesztése elleni küzdelemben;
– a szervezett bűnözői csoportok által üzemeltetett fizetős oldalak azonosítása és felszámolása.

A hálózat a rendőri szervek munkájának támogatása érdekében a 2006-ban kiadott akciótervnek megfelelően jár el a következők szerint:

– szűrő terjesztésével a tagországok nemzeti szabályozásaira figyelemmel blokkolja az illegális, pornográf anyagokat tartalmazó weboldalak elérését;
– azonosítja és lezárja a pornográf anyagok terjesztésével összefüggésben elérhető fizetési rendszereket;
– azonosítja és elfogja az ilyen bűncselekmények elkövetésében érintett személyeket.

A projekt vezetője a Norvég Bűnügyi Szolgálat (Kripos) és az Egyesült Királyság Gyermekek szexuális kizsákmányolása elleni online védelmi központ *(UK Child Exploitation and Online Protection Center; CEOP).*
Hazánk nem tagja a CIRCAM-hálózatnak.

A CIRCAM-projekt másik hasznos eszköze a *Nemzetközi domén-feketelista (International „Worst of"-list of domains),* ez elsősorban azon országok támogatása céljából jött létre[12], amelyek megfelelő jogszabályi vagy technikai háttér hiányában nem képesek felvenni a harcot a rohamosan szaporodó illegális tartalmú oldalak ellen. A lista segítségével a nemzeti hatóságok számára

– azonosíthatóvá válnak az esetleges ellenőrzés tárgyát képező internetes oldalak,
– az internetszolgáltatók blokkolhatják a domének elérését.

12 http://i247.ip/I247/Public/THB/default.asp

A CIRCAM-projekt kiemelkedő partnereként működő Interpol szolgáltatja a feketelistát és a figyelmeztető oldalt a saját biztonságos, 24 órás elérhetőséget nyújtó belső rendszerén[13] keresztül a tagországok kapcsolattartó pontjainak.

Európai Pénzügyi Koalíció

A szervezet *(European Financial Coalition; EFC)* célja az illegális tartalmú, fizetős internetes oldalak mögött lévő gazdasági háttér felszámolása. A legnagyobb pénzügyi, internetszolgáltató és információtechnológiai cégek a nemzetközi rendőri szervekkel, az Európai Bizottsággal és civilszervezetekkel együttműködve azonosítják és fagyasztják be az illegális tartalmú weboldalakhoz kapcsolt pénzügyi vonalakat, számlákat. Az Europol szoros kapcsolatot tart fenn az Egyesült Királyságban működő online védelmi központtal, az Eltűnt és kihasznált gyermekek nemzetközi központjával *(International Center for Missing and Exploited Children; ICMEC)* és az Olasz Rendőrséggel.

Az Europol a 2009 márciusában létrejövő szervezetet a kezdetek óta támogatja.

SIP-BENCH–II projekt

A biztonságosabb internet program égisze alatt működő projekt *(Safer Internet Programme Benchmark II)* célja az internetes szűrőalkalmazások és szolgáltatások teljesítményének teljes körű felmérése. A projekt eredményeinek megismerésével és terjesztésével azoknak a szülőknek és intézményeknek kívánnak ajánlást nyújtani, akik, illetve amelyek elsősorban beépített szűrők alkalmazásával igyekeznek megvédeni a gyermekeket az ártalmas tartalmú internetes oldalaktól.

Az elemzés alapján felállított és szakértők által kidolgozott lista ismeretében a szülők eldönthetik, hogy melyik program, alkalmazás vásárlása, telepítése szolgálja legjobban az érdekeiket.

FIVES-projekt

A rendőrségi nyomozások során sokszor probléma a nagyszámú tárolóeszközök lefoglalása és a tartalom teljes körű elemzése. A projekt a lefoglalt kép- és hanganyagok igazságügyi vizsgálatát hivatott támogatni egy saját fejlesz-

13 Interpol I-24/7

tésű, könnyen kezelhető, nagy adattartalom gyors és hatékony elemzésére kifejlesztett alkalmazással[14].

Egy átlagos nyomozás során is több terrabyte-nyi[15], eltérő kiterjesztésű adat lefoglalására kerül sor, ezek elemzése nagyon lassú folyamat.

A vizsgálati másolat és a videofelvételek támogatása *(Forensic Image and Video Examination Support; FIVES)* alkalmazás a rendőri és igazságügyi szervek számára lehetővé teszi

– a nagy adattartalom gyors és mélyreható elemzését, a már feltárt illegális tartalmú adatok és az új adatok megkülönböztetését;
– az azonosítási folyamatba épített automatizmusok segítségével az emberi beavatkozás minimalizálását;
– különböző képeken és videókon látható bűncselekmények azonos helyszíneinek jelzését képfelismerő és tárgypont-azonosító eszköz futtatásával.

Európai civilszervezetek összefogása
a gyerekek biztonságos internetezésért

Az internetes gyermekvédelem körében a *European NGO Alliance for Child Safety Online (ENACSO)* projekt célja egy civilszervezetekből álló dinamikus hálózat kiépítése és fejlesztése, amely a témában képviseli az uniós civilszervezeteket, illetve hozzájárul egy Európában egységes gyermekvédelmi koncepció kialakításához és igyekszik hatással lenni a nemzeti, európai és nemzetközi szakpolitikák és stratégiák létrehozására.
A projekt tagja a Kék Vonal Gyermekkrízis Alapítvány.

Rendvédelmi Szervezetek Szövetsége

A *Virtual Global Taskforce (VGT)* célja egy erős és hatékony nemzetközi rendőri hálózat létrehozása, amely képes felvenni a harcot a bűnözői csoportok ellen.

Céljaik között szerepel az internet biztonságosabbá tétele, az áldozatok és lehetséges áldozatok azonosítása és segítségnyújtás, az elkövetőkről naprakészen tartott adatbázis működtetése.
Hazánk nem tagja a szervezetnek.

14 http://i247.ip/I247/Public/Children/Default.asp
15 1 Terrabyte = 1024 Gigabyte = 1 048 576 Megabyte

PIN-művelet[16]

Az akció elindításakor létrehoztak egy rendőri szervek által irányított weboldalt, amely illegális tartalmú anyagok elhelyezésének lehetőségét és megtekintését kínálta.

A belépni szándékozók internetes azonosítóját lekövették, és az illető szembekerült egy figyelmeztető oldallal, amely tájékoztatta, hogy egy rendőri portálon van, és az azonosítóit átadják az illetékes nyomozó szerveknek további intézkedésre. A művelet 2003. decemberi indulása óta számos ország állampolgárainak azonosító adatai felkerültek, olyanokéi, akik szándékosan kerestek az interneten illegális pornográf tartalmú weboldalakat.

A művelet valódi célja azonban a bűnmegelőzés és a magukat megfoghatatlannak hívők elbizonytalanítása. Az akció az évek folyamán már bebizonyította érdemeit, és a hatékonyabb visszatartó erő érdekében a szervezők újabb és újabb internetszolgáltatókat és cégeket vonnak be.

A VGT ugyanakkor a szülők és nevelők részére segítséget is nyújt a gyermekvédelem terén. Felvilágosítást adnak a veszélyes weboldalak online bejelentésének lehetőségeiről. A szervezet évente nagyjából háromszáz jelentést kap a szülőktől.

Europol

Elemzői munkafájlok[17]

Az Európai Rendőrségi Hivatal (Europol) bűnözésfinanszírozás és csúcstechnológiai bűnözés elleni osztálya a tagországok kompetens nyomozó szerveinek támogatása céljából működteti a CYBORG és a TWINS elemzői munkafájlokat *(Analysis Work File; AWF)*.

A 2009. április 29-én megnyitott munkafájl célja az Europol mandátumkörébe eső internetes és információtechnológiai bűnözéssel kapcsolatos tagállami nyomozások támogatása a munkafájlok alaprendeltetése és a nyitóparancsban meghatározottak szerint.

Magyarország tagja a CYBORG AWF-nek, a kapcsolattartó szerv a Nemzeti Nyomozó Iroda Bűnügyi Főosztály Csúcstechnológiai Bűnözés Elleni Osztály.

16 http://www.virtualglobaltaskforce.com
17 http://europs.europolhq.net/Europs/DesktopDefault.aspx

Az Europol mandátumkörébe eső és a pornográf tartalmú anyagok készítésére, terjesztésére és kereskedelmére irányuló bűnözői hálózatok felderítése érdekében tett tagállami erőfeszítések elősegítésére indította el 2001. augusztus 16-án az Europol a TWINS munkafájlt.
Az Europol a következő célok elérésében nyújt segítséget:

– elkövetők azonosítása;
– a határon átnyúló elkövetési módszerek és a kapcsolattartás módjának (rejtett, meghívásos módon működő privát csatornák) azonosítása;
– sértettek azonosítása az esetlegesen folyamatban lévő bűncselekmények megszakítása érdekében;
– hálózati azonosító elrejtéséhez használt programok azonosítása;
– ismételt áldozattá válás megakadályozása;
– az Europol összekötő tiszti hálózat *(Europol Liaison Officers Network; ELO)* igénybevételével a műveleti szintű együttműködés hatékonyságának növelése;
– stratégiai és műveleti elemzői támogatás nyújtásával a bűncselekmény változásainak követése;
– információ- és tapasztalatcsere érdekében szakértői (műveleti és stratégiai) találkozók szervezése.

Hazánk a kezdeti tagság után kilépett a munkafájlból.

Csúcstechnológiai bűnözés elleni központ

A *High Tech Crime Center (HTCC)* a tagországok szervezett bűnözés elleni küzdelmében kíván támogatást nyújtani a közvetlen és közvetett igények lehetőség szerinti kielégítésével elsősorban magasan képzett szakértők közreműködésével végzett koordinációval, műveleti támogatással és képzésekkel.

A HTCC a koordinátor szerepét tölti be a csúcstechnológiai bűnözéshez kapcsolódó tevékenységek vonatkozásában, és a következő eszközökkel igyekszik hatékonyabbá tenni a tagországok közötti együttműködést:

– legjobb gyakorlat (a nyomozó szervek leghatékonyabb nyomozási taktikáinak azonosítása és elemzése a nyomozás eredményességének növelése érdekében);
– kutatás és fejlesztés (az információtechnológia fejlődésének nyomon követésével fenyegetettségértékelés);
– szakértői csoport;
– kommunikációs platform (a tagországok nyomozó szerveinek kapcsolattartásra alkalmas eszköze);

– képzések (a bűnözés fejlődési irányához és a tagországok internet-információtechnológiai specifikus igényeihez igazodva dolgozzák ki a képzési anyagokat, és egy 2007 óta működő munkacsoport keretében tart fenn állandó kapcsolatot rendészeti szervekkel, nemzetközi szervezetekkel, magánszektorral és iskolákkal).

A központ képzett szakértői az adott jogszabályi keretek között speciális szaktudást igénylő kérdésekben segíthetnek választ adni a hozzájuk kéréssel forduló tagországnak akár eseti jelleggel, akár közös nyomozó csoport *(Joint Investigation Team; JIT)* keretében. Lehetőség van lefoglalt számítógép merevlemezeinek speciális programmal való átvizsgálásra, valamint az Europol tisztviselői számára elérhető internet account használatával biztonságos online információcserére.

A központ a csúcstechnológiai bűnözés tendenciáinak azonosítása érdekében folyamatosan elemzi a tagországok által szolgáltatott és a terület által érintett információkat, valamint adatot szolgáltat az Europol által készített szervezettbűnözés-fenyegetettségi értékeléshez *(Organized Crime Threat Assessment; OCTA),* és saját, területspecifikus fenyegetettségértékelést készít.

Az eredményes együttműködés és a stratégiai célok megvalósítása érdekében az Europol létrehozta az Europol csúcstechnológiai bűnözés elleni platformot *(Europol Cyber Crime Platform; ECCP),* amely a következőket foglalja magában:

– internetbűnözés online értesítési rendszer *(Internet Crime Reporting Online System; I-CROS),* amelynek célja a tagországok és egyes esetben a (műveleti megállapodással bíró) harmadik partnerek által az internetes bűncselekményekről szolgáltatott információk továbbítása közvetlenül az Europol Információs Rendszerbe *(Europol Information System; EIS);*
– CYBORG AWF;
– internet igazságügyi szaktudás *(Internet Forensic Expertise; I-FOREX)* platform az említett I-CROS és CYBORG AWF kiegészítésére szolgál, magában foglalva minden egyéb, nem személyes vagy műveleti információt. Ezek az adatok általában rendőrségi legjobb gyakorlatokra és képzésekre vonatkoznak.

Akciónapok[18]

Az Europol évről évre különböző méretű, technikai támogatottságú és célú akciók szervezésével igyekszik segíteni a tagországok nyomozó hatóságainak felderítő munkáját.

TYPHON

A művelet nyomán tizenkilenc országban tartottak házkutatást a hatóságok, és a korábban azonosított 286 elkövető közül 118-at letartóztattak. Az osztrák hatóságok által vezetett nyomozás során sikerült azonosítani egy pornográf tartalmú anyagokat terjesztő internetszolgáltatót. A lefoglalt anyagok alapján az Europol több minősített tartalmú információs csomagot és elemző jelentéseket állított össze. Az akció során kiderült, hogy a munkakörénél fogva jó néhány elkövető a gyermekek állandó közelségében dolgozott.

Az osztrák hatóságok által vezetett nyomozás végén sikerült azonosítani és biztonságba helyezni öt, különböző állampolgárságú, négy és tizenkét év közötti gyermeket.

VENICE CARNIVAL

A velencei Olasz Postai és Kommunikációs Rendőrség által vezetett művelet során az Europolnak sikerült azonosítania számos, malware-rel fertőzött weboldal URL-jét. A malware volt a felelős az internetfelhasználó illegális, pornográf oldalakra való átirányításáért. A malware-t tartalmazó szerver tulajdonosa nem tudott a fertőzésről. A beszerzett adatok alapján valószínűsíthető volt, hogy ugyanaz a bűnözői szervezet állt a fertőzés hátterében, amelyik az illegális tartalmú képek reklámozásáért volt felelős.

A művelet nyomán számos tagországban működő weboldal-tulajdonost értesítettek, ők pedig elvégezték a szükséges vizsgálatokat és a törléseket.

HAVEN

Az Europol Műveleti Főosztály TWINS AWF szervezésében Németországgal, Hollandiával, Svédországgal és az Egyesült Királysággal együttműkö-

18 Child Sexual Exploitation 2010 Fact Sheet
http://europs.europolhq.net/europs/desktopmodules/search/getDMSDoc.aspx?id=520193&ext=pdf

désben, 2011 márciusában került sor a HAVEN elnevezésű közös európai akciónap megrendezésére.

Az akciónap célja az érintett tagországok által megjelölt és a gyermekek szexuális szolgáltatásairól elhíresült országokból érkező repülőjáratok utasainak ellenőrzése (szükség esetén csomagok átvizsgálásával együtt) a legnagyobb cél- és tranzitállomás bevonásával, mint például a frankfurti vagy a Schiphol repülőtér, de részt vett számos brit és svéd nemzetközi repülőtér is.

Az Europol három Mobile Office kitelepítésével és egy ügyeletes kapcsolattartó személy kijelölésével segítette a tagországok hatóságainak munkáját.

Interpol

Az Interpol együttműködik a tagországok kapcsolattartó pontjaival, ezzel téve lehetővé a nyomozó szervek számára a hatékonyabb bűnmegelőzést és bűnüldözést nemzeti és nemzetközi szinten egyaránt.[19]

A nyomozó szervek támogatása terén tapasztalt szakértőket felvonultató munkacsoportjain keresztül az Interpol évek óta kiemelt szerepet vállal a csúcstechnológiai bűnözés elleni küzdelemben. Jelenleg négy, területi eloszlású munkacsoport létezik:

- Európai Csúcstechnológiai Munkacsoport *(European Working Party on Information Technology Crime; EWP ITC);*
- Afrikai Regionális Csúcstechnológiai Munkacsoport *(African Regional Working Party on ITC; ARWP ITC);*
- Ázsiai–Dél-óceáni Csúcstechnológiai Munkacsoport *(Asia-South Pacific Working Party on ITC; A-SPWP ITC);*
- Dél-amerikai Csúcstechnológiai Munkacsoport *(Latin America Working Party on ITC; LAWP ITC).*

Az Európai Csúcstechnológiai Munkacsoport évente háromszor rendez találkozót, 2010 szeptemberében tartotta az Interpol Főtitkárság *(Interpol Secretariat General; IPSG)* az 58. munkacsoporti ülést.

A munkacsoport már eddig is számos elemzéssel, gyakorlati útmutatóval és ajánlással segítette a rendőri szerveket. Egyebek között a következőkkel segít:

19 http://i247.ip/I247/Public/Children/Default.asp

– Csúcstechnológiai bűnözés nyomozása *(Information Technology Crime Investigation Manual; ITCIM)* című útmutató (szaktudással felvértezett nyomozók tapasztalatainak, iránymutatásainak gyűjteménye, megjelenik CD-n);
– botnetadatbázis;
– képzések (szakértők bevonásával, például Microsoft).

Interpol-tájékoztatók

Az Interpol mindenki számára elérhető tájékoztatókat készít és publikál, így figyelmeztet az információtechnológia hordozta veszélyekre.

Vezeték nélküli technológia

A rádióalapú kommunikációra épülő technológia *(Wireless Local Area Network; WLAN)* adattovábbítási metódusa és biztonsági szintje alapjaiban különbözik a kábelalapú kommunikációtól. Az adatok rádióhullámok segítségével lépnek ki a rádióadón keresztül.
A WLAN-kommunikációt számos veszély fenyegeti:
– jogosulatlan személy használhatja az internet-hozzáférést, ami nagy fokú anonimitást garantál számára, így tevékenységének akár pénzügyi vagy büntetőjogi vonzata is lehet;
– a teljes kommunikáció ellenőrizhető (jogosulatlan személy által);
– adatlopás;
– jogosulatlan adatmódosítás.

3G mobiltelefonok

A hírközlési telekommunikációs szolgáltatók új, nagyobb és merőben más információs forgalom lebonyolítására képes technológiát dolgoztak ki harmadik generáció, azaz 3G néven. Új információs forgalmon a videoletöltés nélküli megtekintést *(Video streaming; VS),* a videokonferencia-hívást, a videohívásokat, az e-mail-kommunikációt és a webes böngésző szolgáltatásokat értem.

Ez a technológia a bűnözők számára is új lehetőségeket teremtett, külön kiemelendők a következő tevékenységek:
– a 3G technológiával ellátott telefonokra nagyon széles feketepiac alakult ki, az így létrejövő keresletet jól mutatja a telefonlopások számának ugrásszerű növekedése;

– a VS térnyerése és a képküldő multimédia-szolgáltatás bevezetése újabb lökést adott a gyermekek szexuális kizsákmányolásával, illegális pornográf anyagok kereskedelmével érintett, valamint az illegális megfigyeléssel foglalkozó bűnözői tevékenységnek;
– a trójai típusú támadások[20] elterjedése is megfigyelhető, ezek során személyes adatokat igyekeznek gyűjteni a mobiltelefon memóriájából vagy az adatforgalomból;
– az elektronikus szavazások bevezetésével egy teljesen új bűncselekmény megjelenése várható, amikor az erre szakosodott szervezett bűnözői csoportok klónozott[21] vagy másolt mobiltelefonokkal adnak le további szavazatokat, így befolyásolva a választási eredményeket;
– A 3G technológia nyújtotta internetelérési lehetőség újabb vírusok megjelenését generálta.

A tagországok nyomozó szervei egyrészt a megfelelő jogszabályi háttér hiánya, másrészt a technikai és szaktudás terén csak nehezen tudják felvenni a versenyt az új technológiára épülő bűnözéssel. Az Interpol a következő tanácsokkal segíti a rendőrség munkáját:
– szükség van egy olyan jogszabályi háttér kialakítására, amely lehetővé teszi az elektronikus nyomkövetéssel gyűjtött adatok bizonyítékként történő felhasználását;
– együttműködés a technológiát használó, a szaktudásukat átadni képes cégekkel;
– együttműködés a szolgáltatókkal az illegális tartalmú oldalak hatékony blokkolása érdekében;
– együttműködés a gyártóval és a szolgáltatókkal a lopás és csalás elleni védelemi technológia és eljárás kialakítása céljából (kártyaletiltás, szolgáltatónál történő letiltás);
– a 3G technológiára épülő rendőri kapcsolattartó hálózat kialakítása.

Multimédiaüzenet-küldés

Az MMS-szolgáltatás lassan felváltja az SMS-t, vagyis az utóbbi a szöveges üzenet mellett kiegészült hang- és képüzenettel. Formátuma és a szinkronizálási eljárás következtében a legtöbb mobiltelefon már összekapcsolható a

20 Álcázott malware programba való bejuttatása és elrejtése, ez a továbbiakban nem igényel különösebb beavatkozást, önállóan végzi az adatok gyűjtését.
21 Valódi mobiltelefon azonosító adatainak eltulajdonítása, és úgynevezett üres készülékre áthelyezése.

számítógépekkel. A technikai lehetőségeket kihasználva a bűnözői csoportok a vírusok terjesztésén felül a nagy mennyiségű adatforgalom miatt szinte ellenőrizhetetlen módon terjeszthetik az illegális pornográf tartalmú kép- és videoanyagokat.

Virtuális pénz

A valódi pénz olyan elektronikusan tárolt és titkosított kódformája, amely a hozzárendelt érték alapján részt vesz a kereskedelemben. Valójában ugyanazon az elven működik, mint a papírpénz, csak elektronikusan. Számtalan internetes pénzügyi tranzakciót bonyolítanak le a világon naponta bankkártyákkal és hitelkártyákkal.
A virtuális pénznek két fajtája ismert:

– azonosított virtuális pénz *(Identified Virtual Money; IVM),* amely tartalmaz személyes információkat, így a tulajdonos beazonosítható;
– azonosító nélküli virtuális pénz vagy digitális készpénz *(Anonymous Virtual Money; AVM),* ennek nyomon követése vagy a tulajdonos visszakövetése a pénzköltés után nem lehetséges.

A bűnözői körök számára széles távlatokat nyit a virtuális pénz használatának elterjedése:

– virtuális pénz jogosulatlan készítése, felhasználása;
– az információs rendszerbe való illegális behatolás után a számlák manipulációja;
– a kiszolgáló információs rendszer támadása, amely a bizalomhiány következtében a virtuális pénz forgalmának csökkenéséhez vezet;
– a rendszer használatával való visszaélés bűncselekmények elkövetése céljából (pénzmosás);
– egyes bűncselekmények elkövetésének megkönnyítésére való felhasználás (emberrablás vagy zsarolás esetén a követelt pénzösszeg átadása elektronikus formában).

A rendőri szervek számára elengedhetetlen feladat a virtuálispénz-szolgáltatók által használt szerverek földrajzi helyének azonosítása és a jogalkotókra, norma-előkészítőkre való nyomásgyakorlás egy egységes nemzetközi jogszabályi környezet kialakítása érdekében.

Sértett felkutatását és a bűncselekmény felderítését segítő adatbázis

A gyermekek sérelmére elkövetett szexuális bűncselekmények az interneten a lefényképezéstől a brutális szexuális bűncselekmények vizuális rögzítéséig terjed. Tekintettel az internet széles körű elérhetőségére, a gyermekek sérelmére elkövetett szexuális bűncselekményekkel kapcsolatos anyagok online elhelyezése is bűncselekménynek számít és globális, összehangolt együttműködést igényel.

Az Interpol koordinálja a több tagállamot is érintő nagy volumenű nyomozásokat, ezenkívül képzést és elemzői-technikai segítséget nyújt. A szervezet arra buzdítja a tagállamokat, hogy zöld sarkos körözéseket[22] bocsássanak ki, amellyel fel tudják hívni a nemzetközi rendőri szervezetek figyelmét a gyermekek sérelmére súlyos bűncselekményeket elkövető személyekre, különösen a bűnismétlőkre.

A korbban említettek szerint az Interpol számos más szervezettel dolgozik együtt, beleértve a CIRCAM-ot és a gyermekek szexuális kizsákmányolása ellen létrehozott VGT-t.

ICSE-adatbázis

Gyermekek sérelmére elkövetett szexuális bűncselekmények nemzetközi képi adatbázisa 2009 márciusában indult, és a korábbi interpolos *(Interpol Child Abuse Image Database; ICAID)* adatbázist váltotta fel. Rendeltetése, hogy a tagállamok illetékes nyomozó szervei közvetlenül megoszthassák egymással az ilyen bűncselekménnyel összefüggésbe hozható adatokat, információkat, fényképeket. Az adatbázis egy kifinomult kép-összehasonlító algoritmus alapján képes kapcsolatokat találni az áldozatok és az elkövetési helyek között, valamint segítséget nyújt az elkövetők azonosításában. Ebben az esetben a rendszer jelzi a lekérdező félnek, ha egy kép már ismert elemeket tartalmaz, illetve ha már nyomozás van folyamatban.

Az adatbázis a G8-tagországok kezdeményezésére, az Európai Bizottság finanszírozásával jött létre és az Interpol üzemelteti. Eddig a 190-ből 25 állam csatlakozott a rendszerhez: Kanada, Csehország, Dánia, Franciaország, Németország, Norvégia, Svédország, Egyesült Királyság, Ukrajna, Spanyol-

22 Az Interpol figyelmeztető üzenete, amellyel felhívják a tagországok figyelmét egy adott személyre, aki cselekményét más országban is elkövetheti. Tipikusan pedofilia, gyermekpornográf szolgáltatás céljából utazó bűnöző esetében alkalmazzák.

ország, Brazília, Japán, Románia, Lengyelország, Ausztria, Svájc, Egyesült Államok, Fehéroroszország, Litvánia, Ciprus, Andorra, Írország, Ausztrália, Belgium, Chile.

Magyarország csatlakozása folyamatban van, az állomány képzése 2011 decemberében megtörtént.

Összegzés

A számítástechnika és információtechnológia rohamos fejlődése miatt a rendvédelmi szervek nehéz helyzetben vannak, az állandósulni látszó lépéshátrány demoralizálja a nyomozó szervek munkatársait. További probléma, hogy ahogyan más kiemelt bűncselekmények nyomozása során, úgy a csúcstechnológiai bűnözés elleni küzdelemben sem lehet megállni az országhatároknál.

A könnyű pénzszerzési lehetőség reményében folytatott internetes adathalászat, illetve szolgáltatók elleni támadások, valamint a deviáns indíttatású tiltott pornográf oldalak nézegetése és a „tapasztalat- és fájlcsere" más személyekkel gyakran olyan szerverek és álcázott számítógépek segítségével történik, amelyek sok esetben még csak nem is az Európai Unió területén vannak. Könnyen belátható, hogy a kölcsönösségen alapuló nemzetközi bűnügyi együttműködés hiányában a hatóságok nem vehetik fel a versenyt a bűnelkövetőkkel, így e jól felfogott érdeket képviselve az Európai Unió megkezdte a hatékony kooperációt megteremtő irányelvek kidolgozását.

Az Europol és az Interpol kifejezetten a csúcstechnológiai bűnözés elleni küzdelem céljából hozott létre adatbázisokat, amivel a bűnüldözés élére álltak. Természetesen az adatbázisok semmit nem érnek adatszolgáltatások, adatok nélkül. Jól felfogott érdeke valamennyi ország nyomozó szervének, hogy minden rendelkezésre álló eszközt, így az adatbázisokat is megragadja a bűnüldözés folyamán. A lehetőség immár mind jogszabályi vonatkozásban, mind technikailag is adott a hatékony beavatkozásra.

A megfelelő hasznosítás és az eszközök igénybevételének mértéke már a tagországok dolga, vagy ahogyan az Europolnál mondják: *„Minél többet adsz, annál többet kapsz."*[23]

23 Az Europol egyik jelmondata: „The more you share the more you get."

FORRÁSOK

http://circamp.eu
COM(2010) 94. irányelvjavaslat
COM(2010) 517. irányelvjavaslat
EC 2005/222/JHA számú kerethatározat
EC 2004/68/IB számú kerethatározat
http://ec.europa.eu/home-affairs/policies/crime/crime_sexual_en.htm
http://europs.europolhq.net/Europs/DesktopDefault.aspx
http://europs.europolhq.net/europs/desktopmodules/search/getDMSDoc.aspx?id=520193&ext=pdf
http://i247.ip/I247/Public/Children/Default.asp
http://i247.ip/I247/Public/THB/default.asp
http://www.virtualglobaltaskforce.com