Parti Katalin

Összefoglaló

CEPOL Research and Science Conference: Cybersecurity, cybercrime and social networks Madrid, 2011. június 28-30.

Az Európai Rendőrakadémiát, a CEPOL-t (*Collège Européen de Police vagy European Police College*) 2005-ben hozta létre az Európai Bizottság a határokon túli rendőri együttműködés és eszmecsere élénkítése és elősegítése céljából.[1] Céljának teljesülése érdekében a CEPOL évente 60-100 konferenciát, szemináriumot, tréninget és találkozót szervez a tagállamok rendőrhatóságai részére, az Európai Unió különböző helyszínein. Központja a Londontól 70 km-re fekvő Bramshill. A tagállamok általában rendőrképző felsőoktatási intézményeiken keresztül tartják a kapcsolatot a központi szervvel. A magyarországi kapcsolattartó a Rendőrtiszti Főiskola. A CEPOL képzéseire a nyomozó hatóságok szabadon delegálhatnak résztvevőket, a nemzeti kapcsolattartón keresztül. A CEPOL rendezvényeiről vagy a honlapon,[2] vagy a kapcsolattartón[3] keresztül lehet tájékozódni.

A CEPOL igazgatója 2009 és 2013 decembere között **dr. Bánfi Ferenc**, aki korábban az ENSZ Fejlesztési Programjának Moldováért és Ukrajnáért felelős Európai uniós határforgalmi együttműködési irányítójaként, valamint a Dél-Kelet-Európai Együttműködési Kezdeményezés (SECI) transznacionális bűnözés elleni regionális vezetőjeként szerzett tapasztalatokat a rendőri szakigazgatás területén. 1997 és 1998 között országos rendőrkapitány-helyettes.

A két és félnapos konferencia második-harmadik napján voltam jelen, szakértőként/előadóként. A konferencia a madridi Kongresszusi Központban, 90 fős hallgatósággal és 20 szakértővel folyt.

A konferencia témája az internetes bűnözés volt, központi kérdései pedig, hogy hogyan hasznosíthatóak a tudományos kutatások eredményei a mindennapi rendőri munkában, illetve hogyan működhet közre az ipar (pl. telekommunikációs szolgáltatók, szoftvergyártók) a felderítés és a nyomozás feladataiban, valamint a nyomozási együttműködés megkönnyítésében.

A konferencián számos szakértőt hallhattunk a **közösségi oldalak nyomozásban betöltött szerepéről.** Kanadával, az Egyesült Államokkal és az Egyesült Királysággal szemben az európai nyomozó hatóságok nem kapnak kormányzati támogatást arra, hogy megismerjék az online közösségi kommunikációs színtereket – amilyen a Facebook, a MySpace vagy a Twitter –, így kevésbé jellemző ezeknek a kommunikációs és információszerző lehetőségeknek a napi munkába való integrálása is. Míg példának okáért az Egyesült Királyságban 450 rendőrtiszt használja napi rendszerességgel, felderítési eszközként a Facebook-ot, addig **Michael Wirz (Zurich Police Office, Svájc)** kutatása szerint Zürich város rendőrtisztjeinél a közösségi online média integrálása csak most kezdődött meg. Míg Zürich

[1] COUNCIL DECISION 2005/681/JHA of 20 September 2005 establishing the European Police College (CEPOL) and repealing Decision 2000/820/JHA. OJ L256/63

[2] http://www.cepol.europa.eu

[3] dr. Kiss Rita, rita.kiss@rtf.hu; +36 1 39 23 573

lakosságának 20%-a, addig a rendőrtiszteknek csak mintegy 1%-a használja a Facebookot és a Twittert szakmájához kapcsolódóan. A zürichi rendőrség felállított egy tanácsadó/irányítóközpontot (center of excellence), aminek a fő feladata a prevenció. Ennek keretében az online közösségi oldalak rendőri munkában való hasznosítását – amilyen a lakossági-rendőri információcsere, a lakossági tájékoztatás és felvilágosítás – oktatják helyi keretek között a rendőröknek. A közösségi oldalakon megjelenő rendőrség közelebb hozza a prevenciót a lakossághoz, erősíti a rendőri szervezetbe vetett bizalmat, az incidensekre közvetlen és prompt reagálást biztosít, valamint transzparencia-érzést kelt. A bűnüldöző hatóságok átlátható és ellenőrizhető működése növeli a bizalmat, a hatóság tekintélyét, és ezzel együtt a hatékonyságot is. Ugyanakkor biztosítja a bűnüldözés és bűnmegelőzés különböző szereplőivel – jogalkotók, jogalkalmazók, szoftver- és biztonságtechnikai fejlesztők – való együttműködést, a közvetlen párbeszédet is. Emellett, az incidenskezelés gördülékenységének biztosítására szükség lenne belső protokollok kidolgozására is. Ezek a protokollok angolszász bűnüldözési területen ugyan adottak, de korántsem biztos, hogy azokat egy az egyben át lehetne ültetni az európai gyakorlatba.

Az Egyesült Királyság rendőrségeinek fejlesztő ügynöksége **(National Policing Improvement Agency, Home Office)** azon dolgozik, hogy közelebb hozza az internetes csatornákat a nyomozó hatósághoz. **Nick Keane** szerint erre azért is szükség van, mert az angol lakosság 45%-a már legszívesebben Twitteren keresztül kommunikál a rendőrséggel. Az online hírforrások megbízhatósági mutatói folyamatos emelkedést mutatnak: míg a lakosságnak csupán 44%-a tartja megbízhatónak a hagyományos média (pl. televízió) híreit, addig az online tájékoztatás a megkérdezettek 58%-a szerint megbízhatóbb, mint a hagyományos. Persze egy online megjelenő hírnek nem azért lesz nagy a hírértéke, mert megbízható a forrása, hanem mert sokan rákattintanak (tweetelik). Ezt a logikát követve az online média remekül felhasználható a lakossági, elsődleges prevenció, valamint a biztonságérzet növelésére.

Számos kutatás igazolja a biztonságérzet szubjektív, belső érzékelés-vezérelt mivoltát (pl. Kó, 2004; Kerezsi, 2004; Barabás, 2004; Korinek, 1995). A biztonságérzet két irányba fejti ki hatását: egyrészt nagyobb biztonságban érezzük magunkat, ha a körülöttünk élők (szomszédaink, munkatársaink, vagy akár a média) szerint a bűnözés alacsony mértékű, másrészt viszont puszta pszichológiai (viktimológiai) tények miatt ténylegesen nagyobb lesz a biztonság akkor, ha nyugodtak, kiegyensúlyozottak vagyunk, de legalábbis ismerjük a prevenció eszközeit és tudjuk, honnan, kitől kérhetünk segítséget. Ezt a logikát követve a rendőrség online kommunikációja hasznosítható a lakosság elődleges biztonságérzetének – és tényleges biztonságnak – a növelésére is. Némileg ez ellen ható tényező, hogy a rendőrség kommunikációja olyan nyilvánvalóan félrevezető információkat tartalmaz, mint például a londoni vagy madridi metrótámadások után az adott városok töretlen biztonságának hangsúlyozása. Ezek a kijelentések, amelyeknek elsődleges célja a pánik elkerülése, hiteltelenítik a nyomozó hatóság (illetve a belügyi irányítás) munkáját, amely csak nagyon lassan és óriási erőfeszítésekkel hozható újra megfelelő szintre. Terrorhelyzetben a lakosság az információs űrt a nem hivatalos online fórumok (blogok, wikipedia, youtube videocsatorna stb.) böngészésével igyekszik kitölteni. Ezeket a fórumokat – a véleményformálásban elfoglalt szerepüket felismerve – sikerrel hasznosította például számos észak-afrikai kormány, amikor 2011 tavaszán felkeléseket, rebellis politikai hangokat kellett elcsitítani. Az érintett országokban (Tunézia, Egyiptom, Algéria, sőt, Kína) hatalom ellenbloggereket bérelt fel, akiknek a feladata az, hogy – magukat tisztes állampolgárnak kiadva, saját blogjaikban, fórum-hozzászólásaikban – lejárassák a felkelést szítókat. De

hasonló véleményformálási taktikának lehetünk tanúi sokkal jelentéktelenebb kérdésekben is, amilyen például a szaúd-arábiai női vezetés kérdése.

A nyomozó hatóság tagjainak el kell sajátítaniuk többek között az online nyelvezetet, folyamatosan jelen kell lenniük – és ezt demonstrálniuk is kell – az online közösségi oldalakon, az online kommunikáció felépítésének, irányainak megfelelő stratégiai gondolkodás képességét (előre tervezés, szereplők összekapcsolása stb.). Valamint – és talán ez a legnehezebb feladat – illeszkedniük kell az önszabályozó szervezetek alulról építkező rendszerébe. Ez a gyakorlatban azt jelenti, hogy alapvetően meg kell hagyni az online közösségek saját irányítását, de fel kell ismerni azt a pontot, amikor már külső, rendészeti eszközökkel szükséges beavatkozni a rend helyreállítása – vagy legalábbis a rendbontó erők manipulálása – érdekében.

Sebastian Denef a német **Fraunhofer Institute** által végzett trendanalízist mutatta be, amely szerint anyagi támogatás és kellő létszám hiányában nagyon nehéz motiválni a nyomozó hatóságot arra, hogy képezzék magukat. A projekt első riportja a közösségi média rendőri gyakorlatban való alkalmazhatósága mellett egyébként az intelligens adatfeldolgozó rendszerek, a mobilszámítástechnika és a megfigyelési technológiák alkalmazását, valamint a digitális biometrikus azonosítórendszerek bevethetőségét és társadalmi elfogadottságát is vizsgálja.[4]

Detlef Nogala, a CEPOL Kutatás- és Tudásbázis Menedzsment vezetője ezen a ponton felhívta a figyelmet arra, hogy a CEPOL, felismerve a közösségi média jelentőségét a rendőri reagálásban, 2011 őszén tréninget tervez, amelynek célja a rendvédelmi szervek képzése az online közösségi magatartás dekódolására és manipulálására.

Wouter Stol (Police Academy, Belügyminisztérium, valamint University of Applied Sciences, Hollandia) bemutatta a CYREN (Cybersafety Research and Education Network) programot.[5] A CYREN olyan online csomópont, amely összeköttetést teremt az ipari fejlesztők, valamint a bűnmegelőzés között. A köz- és a magánszektornak találkoznia kell az online bűnözés üldözésében. A kezdeményezés hiányossága, hogy egyetemek nem lehetnek a tagjai. Keretében kezelési stratégiák születtek a phishing támadások elhárítására, az online gyermekabúzus jeleinek felismerésére, az online gyermekpornográf anyagok azonosítására, valamint olyan aktuális problémák kezelésére, amilyen az online kortárs bántalmazás (cyberbullying), az extrémista weboldalak és online közösségek leszerelése.

Az **ENSFI (European Network of Forensic Science Institutes)** tevékenysége,[6] amelyet **Erwin van Eijk** ismertetett, hasonló a CYREN-éhez. Az ENFSI nem egy specifikus szervezetnek dolgozik, hanem több nyomozó szervvel áll kapcsolatban, összesen 58 tagja van 35 országban. Tanulmányozzák a tipikus eseteket, majd esettanulmányokat és megoldási metódusokat dolgoznak ki („mock cases”), amelyet aztán körbeküldenek, hogy a tagok véleményezhessék és további ötleteket adhassanak hozzá. Egyik érdekes példájuk, hogy mi történik nagy elektronikus adathalmaz („big data”) esetén – hogyan kezelendők, rögzítendők, tárolandók a nagyméretű adathalmazok.

A konferencián a szakértők hasonlóképpen nyilatkoztak a következő kérdésekről:

- A nyomozó hatóság ismeretei az online bűnözésről hiányosak.
- Jellemző az előkészületi jellegű cselekmények – amilyen például a gyermekpornográf weboldalak letöltés nélküli elérése, valamint a gyermekkel való online

[4] A projektről bővebben lásd: www.composite-project.eu
[5] www.cybersafety.nl
[6] http://www.enfsi.eu/page.php?uid=54

kapcsolatteremtés offline szexuális abúzus céljára – kriminalizálására törekvés,[7] amelyek felismerése és azonosítása nehézséget okoz a nyomozó hatóságnak (fejtette ki **David Wall (Durham University, Egyesült Királyság);** hasonló gondolatokat fogalmaztam meg előadásomban). Ehhez kapcsolódó probléma, hogy nem tisztázott, melyik az a pont, az a mozzanat, amely gyanúsítottá tesz valakit. Ezt az online bűncselekmények esetében szigorúan tisztázni kell (fejtette ki **Wouter Stol**, l. korábban).

- A hagyományos rendőri együttműködésre már vannak bevett eszközök és eljárások, ám ezek nem alkalmazhatók a határokon átnyúló online bűnözés területén. Különösen jellemző ez a kis súlyú vagyon elleni vagy gazdasági bűnözésre, amelynek online példája az egy centes phishing csalás, amelynek során az elkövető minden sértettől csak egy-egy centet emel le.
- Az online bűnelkövetők egy speciális, meghatározó csoportja a fiatalkorú elkövetőké („digitális bennszülöttek"), akiknek motivációi sokszor eltérnek az anyagi haszonszerzésre törekvő felnőttekétől (Shannon, 2007).
- A fiatalkorú elkövetők növekvő száma – és ezen belül az online elkövetésre specializálódott csoportok megjelenése – eddig nem tapasztalt terhet ró a nyomozó hatóságokra: szükségessé válik speciális ifjúsági bűnmegelőzési és bűnüldözési csoportok felállítása.
- Az online bűnözés eszköztára kiegészül olyan, könnyen kezelhető, tömegesen elterjedt és intelligens eszközökkel, amilyen pl. az okostelefon. Ezek könnyebbé teszik a bűncselekmények megvalósítását, de az áldozattá válási kockázatot is közelebb hozzák a felhasználókhoz.
- További kockázatot és felderítési nehézséget jelent az anonimizáló szolgáltatás, az internet kávézók, a wifi hotszpotok, a US3 technológiák, a live CD-k és DVD-k, valamint a felhőalkalmazások.
- Az online környezet-adta anonimitás, valamint a társadalmi kapcsolatokban való eligazodás képességének fölöslegessé válása az online térben olyan társadalmi tényezők, amelyek szintén elősegítik az online devianciák megjelenését és elszaporodását.
- Az elektronikus kommunikációs csatornák és eszközök által generált óriási adatmennyiség, az adatok dekódolása, bizonyítékként való felhasználása kihívás elé állítja mind az ipar, mind pedig a rendőrség képviselőit. Erről hallhattunk **Fernando Fernandez (Tech Investigation Unit, National Police, Spanyolország)** előadásában.
- Az online bűnözés felderítésének és nyomozásának szabályozatlan közegében a rendőrség stratégiája, hogy az eljárásban mindent szabad, amit jogszabály kifejezetten nem tilt. Ez azonban könnyen a magánszféra és a bűnmegelőzés egyensúlyvesztéséhez vezethet, a magánszféra rovására – ahogy azt **Francisco Luis (Judicial Police, Igazságügy Minisztérium, Portugália)** kiemelte. (L. bővebben a 2006/24/EK adatrögzítési irányelv implementálása nyomán felmerült társadalmi vitát és aggályokat.)[8]

[7] 2010.3.29. COM(2010)94 végleges javaslat: az Európai Parlament és a Tanács Irányelvének megalkotására a gyermekek szexuális zaklatása, szexuális kizsákmányolása és a gyermekpornográfia elleni küzdelemről, valamint a 2004/68/IB kerethatározat hatályon kívül helyezéséről. Elérhető:
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52010PC0094:EN:NOT

[8] Az Európai Parlament és a Tanács 2006/24/EK Irányelve (2006. március 15.) a nyilvánosan elérhető elektronikus hírközlési szolgáltatások nyújtása, illetve a nyilvános hírközlő hálózatok szolgáltatása keretében

- Hiányoznak a módszertani segédletek a nyomozó hatóság hatékony és jogszerű eljárásához az online bűncselekmények ügyében.

A konferencia másik nagy kérdésköre a magán- és a közszféra együttműködési modelljei (a továbbiakban PPP mint Public Private Partnership) volt, természetesen az online bűnözéssel összefüggésben. A szakértők – **Manel Medina (Deputy Head of Technical Competence Department, ENISA); Manuel Carpio (Director of Information Security and Fraud Prevention, Telefónica); Santiago Segarra (Industry Business Development Team, IBM, Spanyolország); Adam Palmer (Norton Lead Cybersecurity Advisor, Symantec, Pittsburg)** – a következőkre mutattak rá:

- Ki kell építeni az alapvető bizalmi légkört a kormány és a privát cégek között, mert ez az alapja az információcserének és a kölcsönös fejlődésnek.
- Ahol csak lehet, alkalmazni kell a PPP együttműködéseket.
- A magán- és a közszféra közti információcsere biztonságos és adatvédelmi szempontból támadhatatlan kell hogy legyen.
- A PPP szereplői közös akcióterveket kell hogy kidolgozzanak.
- A kormányoknak teljes mértékben el kell ismerniük és minden eszközzel támogatniuk kell az ipart.
- A partnerség egyenlőségen, ne pedig alá-fölérendeltségen alapuljon. Az ebben a szellemben született jelmondat: Kooperációt felülről jövő szabályozás helyett (cooperate, not regulate)!

Irodalom

Barabás T. (2004) Általános viktimológia, latencia. In: Irk F. (szerk.) Áldozatok és vélemények I. OKRI: Budapest pp. 157-199

Kerezsi K. (2004) A bűnmegelőzés különböző dimenzióinak megjelenése az attitűdvizsgálatban. In: Irk F. (szerk.) Áldozatok és vélemények I. OKRI: Budapest pp. 121-157

Korinek L. (1995) Félelem a bűnözéstől. Közgazdasági és Jogi Könyvkiadó: Budapest

Kó J. (2004) A bűnözéstől való félelem. In: Irk F. (szerk.) Áldozatok és vélemények I. OKRI: Budapest pp. 57-85

Shannon, D. (2007) The online sexual solicitation of children by adults in Sweden. In: English summary of Bra Report No. 2007: 11, Stockholm: The Swedish National Council of Crime Prevention

Parti Katalin

Budapest, 2011. július 5.

előállított vagy feldolgozott adatok megőrzéséről és a 2002/58/EK irányelv módosításáról. Elérhető: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:HU:PDF;
Legfrissebb: http://ec.europa.eu/home-affairs/policies/police/police_data_en.htm