dr. Virág György
dr. Parti Katalin

BESZÁMOLÓ
a
Számítógépes bűnözéssel foglalkozó kormányközi munkacsoport (Intergovernmental Expert Group on Cybercrime) üléséről, (Bécs, 2011. január 17-21.) és az ennek kapcsán felmerült kérdésekről

A Bécsi Magyar ENSZ Képviselet felkérése alapján szakértőként vettünk részt az ENSZ Kábítószer-ellenőrzési és Bűnmegelőzési Hivatala (United Nations Office on Drugs and Crime, a továbbiakban UNODC) által megrendezett számítógépes bűnözés elleni kormányközi munkacsoport első ülésén. A munkacsoport ülését Dél-Afrika bécsi ENSZ Nagykövete elnökölte, az első alelnök Brazília ENSZ Nagykövete, míg a jelentéstevő a kanadai Christopher Ram volt.

I. Előzmények

Az ENSZ Bűnmegelőzési és Igazságszolgáltatási tárgyú 20. kongresszusa 2010 augusztusában, San Salvadorban a számítástechnikai és internetes bűnözés vetületeit tárgyalta, és úgy döntött, hogy felkéri a Bűnmegelőzési és Igazságszolgáltatási Bizottságot (CCPCJ) arra, hívja össze az ENSZ-tagállamok kormányközi ülését. A munkacsoport mandátumát a Salvadori Deklaráció 42. paragrafusa határozta meg. *"To conduct a comprehensive study of the problem of Cybercrime and responses to it by Member States, the international community and the private sector, including the exchange of information on national legislation, best practices, technical assistance and international cooperation, with a view to examining options to strengthen existing and to propose new national and international legal or other responses to Cybercrime."*
A kormányközi munkacsoport első ülésre került sor 2011. január 17. és 21. között Bécsben. Az ülés feladatai a következők voltak:

- megvitatni a 2001. november 23-án, Budapesten aláírt, a számítástechnikai bűnözésről szóló Európa Tanácsi Egyezmény (Convention on Cybercrime, ETS. No. 185; a továbbiakban Cybercrime Egyezmény) elfogadása óta megjelent új bűnelkövetési, ill. bűncselekményi formákat, és az azokra adott válaszokat legfőképpen a nemzetközi bűnügyi együttműködés szemszögéből megvizsgálni;
- eldönteni, szükség van-e a Cybercrime Egyezményt kiegészítő, egy, a kérdést az Egyesült Nemzetek Szervezete szintjén szabályozó egyezmény elfogadására;
- megfogalmazni azokat a szempontokat, amelyek a Bizottság által a számítástechnikai és internetes bűnözés nemzetközi felmérésére összeállítandó kérdőív tartalmazni fog.

II. A tanácskozás

A tanácskozáson az ENSZ 192 tagállamának 1-4 szakértője, az Európa Tanács Cybercrime Egyezménye kidolgozásában részt vevő szakemberek, valamint neves egyetemek és kutatóintézetek referensei vettek részt. A tanácskozás napirendi pontjai a következők voltak:

1. A számítástechnikai és internetes bűnözés jelensége

A XXI. század számítástechnikai bűnözése már csaknem teljes mértékben az internettel áll kapcsolatban. Az internetes bűnözés evolúcióját bemutató tanulmányok eleme a gépidőlopástól kezdve a phishing különböző alakzatai, amelyek már a fejlett „számítástechnikai csalások" kategóriájába tartoznak. (*Wall, 2010*) Ezekben a bűncselekményekben az elkövető a felhasználó hiszékenységét használja ki. Így pl. banki alkalmazottnak adva ki magát eléri, hogy adja meg felhasználónevét és jelszavát, egyéb személyes adatát.

Az evolúció másik eleme, hogy előtérbe kerülnek a kis összegre tömegesen elkövetett csalások (*many attacks targeting small amount*), az automatizált támadások (*automation of cybercrime*).

A harmadik jellegzetesség, hogy a virtuális közösségekben megjelennek a kis súlyú, de tömeges jogsértések, pl. virtuális alteregó feletti ellenőrzés átvétele, virtuális csalások, lopások.

Az új fejlemények következtében egyre nagyobb lesz a hatóságok által nem észlelt, rejtve maradó internetes bűncselekmények becsült száma, volumene. Ennek lehetséges okai egyebek között a reputációs veszteség elkerülésének igénye, a hatóságba vetett bizalom hiánya (főleg a fejlődő országokban, Európában pedig a posztszocialista régióban a rendőrség negatív megítélése, ld.: *Krémer, 2010*), a jogalkalmazók technikai képzetlensége (feljelentések elutasítása, lassú eljárások, elektronikus bizonyítási eszközök elfogadásának hiányos gyakorlata, inkompetens munkavégzés, ld. részletesen: *Parti, 2009b*; *Parti, 2010a*; *Parti, 2010b*).

Az utóbbi időben megfigyelhető a szakmák, szakterületek integrálódása, amely az IT szakértő nyomozásban kapott szerepében csúcsosodik ki. (ld. pl.: *Kármán et. al, 2010*; *Parti, 2004*) Megfigyelhető továbbá a legalitás-illegalitás határainak elmosódása, amelynek emblematikus példája a *legal hacking*, vagy a kiber hadviselés (*cyber warfare*). (ld. pl. Észtországban az országot ért orosz hackertámadásokat követően létrehozott, Nemzeti Cyber-Védelmi Központ működését.)[1]

Speciális kérdések

Az internetes bűnözés új trendjének témakörében érdemes vizsgálni a fájlcserélő rendszerek mibenlétét és nemzetközi megítélését (Pirate Bay ügy, ld.: *Szabó, 2010*). A mai napig vita tárgyát képezheti tagállamonként, hogy mely magatartással válik bűnsegéddé a közvetítő szolgáltató.

Megfontolandó ezen túl a kis értékre elkövetett online szerzői jogsértések dekriminalizálása a szabálysértési értékhatár egyidejű bevezetésével. (*Kármán et al., 2010*)

2. Statisztikai információk

A virtuális bűnözésre annak összetettsége, valamint országonként eltérő megítélése miatt nem létezik megbízható statisztika. Elérhetők ugyan nyilvántartások, de ezek elsősorban nem

[1] Cooperative Cyber Defence Centre of Excellence, Tallinn, Estonia: http://www.ccdcoe.org/

bűnügyi, hanem gazdasági szempontból gyűjtenek adatokat,[2] és nem egységes szempontok szerint, éppen ezért nem végezhető köztük összehasonlítás. (*Bocij, 2004*; *Wall, 2001*) Az online környezetben elszenvedett kár sokszor nem materializálódik, ha pedig keletkezik materiális kár, azt nehéz megbecsülni. (*Wall, 2008*; *Moitra, 2003*)

Elmaradhat a számítástechnikai rendszereket ért támadások bejelentése akkor, ha a sértettek nem észlelik a támadást, (*Murff, 2007*; *Moitra, 2003*), ha az adott ország nem készült fel a számítástechnikai rendszerben véghezvitt támadások regisztrálására: az adott cselekményt a jog nem bünteti, vagy nincs olyan fórum (adminisztrátor vagy közösségi választott bíróság), ahol az áldozat megtehetné bejelentését. Az is lehet, hogy az áldozat bejelentést tesz, de a panasz elbírálására jogosult szerint az eset nem igényel további intézkedést. Az internetes bűncselekmények egyes büntető törvénykönyvek szerinti meghatározása is eltérő, annak ellenére, hogy az Európa Tanács és az Európai Unió jelentős erőfeszítéseket tett a szabályozás egységesítéséért a nemzetközi bűnügyi együttműködés alapjainak megteremtése és a cselekmények hatékonyabb üldözése érdekében.[3] A technika fejlődése ugyanakkor több testhosszal vezet a jogalkotás előtt, így megjelenhetnek olyan cselekmények is, amelyeket a jog még nem „azonosított". Ilyen pl. a virtuális környezetben elkövetett zaklatás, amely a földrajzi jog szerint nem egyértelműen bűncselekmény. (Az online zaklatásnak gyakran csak zavarás a célja, és nem mindig eleme a megfélemlítés. A földrajzi jog azonban szinte mindig megköveteli az emocionális ráhatást. - *Bocij, 2004* -)

A magántulajdonban lévő PC-k elleni, valamint a kisebb vállalkozásokat ért támadásokról semmiféle statisztika nem áll rendelkezésre. Ennek oka, hogy a magánszemélyek nem rendelkeznek olyan szintű számítástechnikai ismeretekkel, hogy egyáltalán felismerjék a támadás tényét. Például a 2007 őszén, több magyarországi bank ellen megvalósított támadásokat magánfelhasználók otthoni számítógépeinek feltörésével és közbeiktatásával hajtották végre (adathalászat, un. zombi-gépek igénybevételével), ilyen módon a valódi támadó az adott személyre terelte a gyanút, ő maga azonban anonim maradt. A kisvállalkozások, ha észlelik is az ellenük foganatosított támadásokat, nem rendelkeznek olyan összegű mozgótőkével, hogy vállalni tudnák a büntetőeljárás megindításával járó terheket (eljárási költség, a számítástechnikai géppark büntetőeljárásban történő lefoglalása), valamint a kiesett munkaidő és az elvesztett ügyfelek miatti anyagi veszteség helyett inkább hallgatnak a támadásokról. A sok ügyfelet tömörítő bankok és pénzintézetek pedig a reputációs veszteségtől tartva tartják titokban az ellenük indított számítástechnikai támadásokat.

Szükség lenne sértetti empirikus kutatások elvégzésére a számítástechnikai rendszert ért támadások terén a támadások természetére, az elszenvedett kár mértékére és jellegére tekintettel, nemcsak a kockázatok felmérése érdekében, de a kockázattudatosság növelése miatt is. Az ilyen felméréseken alapulhatnának a jövő prevenciós stratégiái, amelyek a kis- és középvállalkozásokat, valamint a magánszemélyeket (ügyfeleket) céloznák meg.

---

[2] Például a Computer Emergency Response Team-ek (CERT) által fogadott bejelentések alapján gyűjtött statisztika, amely a cégeket ért támadások formáit, gyakoriságát és tendenciáit rögzíti. Magyarországon ld. a Hun-CERT weboldalát:
http://www.cert.hu/index.php?option=com_newsfeeds&task=view&feedid=11&Itemid=185

[3] Az első jelentősebb, globális egységesítési szerződésnek az Európa Tanács 2001. november 23-án, Budapesten elfogadott, a számítástechnikai bűnözésről szóló egyezménye tekinthető. Uniós szinten jelentős törekvés az egységes büntetőjogi szabályozásra a Tanács 2003. december 22-én elfogadott, a gyermekek szexuális kizsákmányolása és a gyermekpornográfia elleni küzdelemről szóló, 2004/68/IB kerethatározata. (HL L 13/44-8; 2004.01.20.)

Speciális kérdések

A tanácskozáson felmerült egy olyan központi adatbázis létrehozása, amilyen pl. az Europol nyilvántartása (TECS – The Europol Computer System). Ez az adatbázis nemcsak bűncselekményekre vonatkozó adatokat tarthatna nyilván (bűnügyi statisztika), hanem a közvetlen információcsere megkönnyítése érdekében a hatáskörrel és illetékességgel rendelkező hatóságok elérhetőségeit, valamint a nemzetközi együttműködésben részt vevő országok jó gyakorlatait.

3. A számítástechnikai és az internetes bűnözés kihívásai

A számítástechnikai és internetes bűnözés területén az utóbbi évtizedben jelentek meg olyan új megoldások, amelyek kezelésére nem ad választ a Cybercrime Egyezmény. Ilyen például a botnetek vagy a felhőalapú (*cloud computing*)[4] elkövetési forma.

A botnet az angol 'robot network' rövidítése, amelynek keretében sok egyéni számítógépet (PC-t) kapcsolnak össze az elkövetők, és a hálózat működését automatikussá teszik. Az automatizmus kiterjed kártékony szoftverek terjesztésére, kéretlen levelek (spam) küldésére, valamint DoS, DDoS támadások megvalósítására. Míg a botnetek létrehozása (mint egyéni számítógépek feletti uralom megszerzése a jogosult engedélye nélkül) önmagában büntetendő, addig a *cloud computing* lehet legális is. Utóbbi esetében *„a számítási erőforrások – alkalmazások, üzleti szolgáltatások – valós időben használhatók az interneten keresztül, a szolgáltatás díjazása pedig a felhasználás alapján történik."*[5]

A tanácskozás egyes részt vevői szerint a Cybercrime Egyezmény lehetővé teszi a botnetek kriminalizálását. (Számítástechnikai csalás, 8. Cikk), ám mások szerint a számítástechnikai csalás keretében csak a botnetek egyik feltétele, mégpedig a jogosult számítógépe feletti uralom megszerzése adott. Azonban a Cybercrime Egyezmény 8. Cikkének eleme az anyagi haszon megszerzésére törekvés is, amely nem okvetlen célja a botnet-hálózat kiépítésének. Ugyanígy vitás lehet, hogy a botnetek kriminalizálását magában foglalja-e az egyezmény 5. Cikke (A rendszer sértetlensége elleni cselekmény), hiszen a botnetek nem minden esetben akadályozzák valamely számítástechnikai rendszer működését, legfeljebb igénybe veszik azt. Minden esetben megvalósul azonban az egyezmény 2. Cikke (Jogtalan belépés) szubszidiárius bűncselekményként, amely cikkely egyben biztosítja a felhőalapú elkövetési formák kriminalizálását is. [6]

A felhő-technológián alapuló cselekmények inkább a nemzetközi együttműködésben okoznak gondot, hiszen nem lehet meghatározni az elkövetés helyét. A másik probléma az lehet, hogy nehézségekbe ütközik a forgalmi adatok beszerzése a külföldön található internet-szolgáltatótól (*transborder access*).

---

[4] A felhőalapú megoldásokkal bármilyen, internet-hozzáféréssel rendelkező eszközről azonnal elérhetők az adatok és az alkalmazások, ezért a felhőalapú számítástechnika segítségével a vállalatok azonnal, és akár ideiglenesen is hozzáférhetnek erőforrásaikhoz, amikor azokra igazán szükségük van. Ráadásul mindehhez nem kell új gépek beszerzésébe vagy új adatközpontok kiépítésébe pénzt befektetniük.

[5] Outsourcingcenter: http://outsourcingcenter.hu/2010/07/13/a-jovo-informatikaja-a-cloud-computing-es-ami-mogotte-van/

[6] ld. még: http://www.jogiforum.hu/publikaciok/50#ixzz1BJA6BAWA; valamint: http://www.jogiforum.hu/publikaciok/50#ixzz1BJAISUzD

4. A jogalkotás harmonizálása

Az alapvető gondot az jelenti, hogy az adott ország gazdasági fejlettségétől függ, mit tekint problémának, következésképpen mit szabályoz büntetőjogi vagy egyéb eszközökkel. Habár a fejlett országok „spam-értéke" is igen magas (sok spammel terhelt az internet), ez elsősorban nem itt okoz gondot, hanem a fejlődő régiókban (Ázsia, Afrika, Dél-Amerika), ahol az internet-sávszélesség kisebb, így annak jelentős hányadát lefoglalja az erős spamforgalom, ami pedig lassítja, illetve megbéníthatja az internet-elérést. Éppen ezért, a spam szabályozására a legnagyobb erőfeszítés nem a fejlett országokban, hanem a gazdaságilag elmaradottabb térségekben történik.

Ezzel szemben, a ritkán előforduló, ám nagy veszteséget okozó (*low possibility-high impact*), súlyos cyber-csalások kezelésére elsősorban a fejlett országokban (és ott nemzetközi szinten is) született szabályozás. Ezek a cselekmények a fejlődő országokban jórészt rejtve maradnak, illetve a felszínre kerülésük a fejlett régió által kezdeményezett nemzetközi együttműködésnek köszönhető, ám kizárólag azokban az esetekben, amelyekben a fejlett régió országai is érintettek. Az említett fejlődő régió a cyber-elkövetők számára un. „adatmenyország" (*data haven*), vagyis olyan szabályozatlan tér, ahonnan érdemes pl. egy hacker-támadást elkövetni, hiszen kevésbé valószínű, hogy ezekben az országokban az internet-szolgáltatók együttműködnének a (külföldi) nyomozó-hatósággal (jogsegély-kérelmek keretében adatbekérések, megkeresések teljesítése). (*Parti, 2009b; Szűts, 2008*)

5. Büntetőjogi válaszok a számítástechnikai és az internetes cselekményekre

Új elkövetési magatartások az online gyermek-kizsákmányolás kapcsán. A gyermekekkel szembeni online szexuális visszaélések a 2000-es évek elejétől fokozatosan az EU és az ET jogalkotásának középpontjába kerültek. A jogalkotás legutóbbi fejleményei, azaz az Európa Tanács 2007. október 25-én Lanzarotén elfogadott egyezménye,[7] valamint az Európai Parlament és a Tanács 2010. szeptember 6-án megfogalmazott javaslata a gyermekek szexuális kizsákmányolásának visszaszorítására[8] a következő lépéseket képzelik el:

- a gyermekkorúval való online kapcsolatfelvétel (*grooming*, azaz „becserkészés") sui generis büntetendővé tétele a tagállamokban, abban az esetben, ha a kapcsolatfelvétel bizonyíthatóan a gyermekkel szembeni szexuális visszaélés céljából történt;
- a gyermekek online szexuális abúzusát rögzítő felvételek letöltés (*download*) – azaz szándékos megszerzés – nélküli elérése (*access*) sui generis büntetendőségének biztosítása a tagállamok által;
- a gyermek pornográf tartalmakat hosztoló webes felületek üzemeltetői közvetlen büntetőjogi felelősségre vonhatóságának biztosítása a tagállamok által; (A közvetítő szolgáltatók felelősségét az Elektronikus kereskedelemről szóló Irányelv - 2000/31/EK - már tartalmazza. Az új javaslatok bevezetnék a tárhely-szolgáltatók közvetlen felelősségre vonhatóságát is, amennyiben tudomásukra jut illegális tartalom közlése.

[7] Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse CETS No.: 201 (2007.10.25. Lanzarote)

[8] Proposal for a Directive of the European Parliament and of the Council on combating the sexual abuse, sexual exploitation of children and child pornography, repealing Framework Decision 2004/68/JHA (2010/0064 (COD) Brussels, 6 September, 2010)

A viták tárgya az, hogy mi tekinthető „tudomásszerzésnek”, pl. egy állampolgár beadványa, levele elegendő, vagy szükség van a nyomozó hatóság eltávolítási felszólítására is.)

- a gyermekek és a felnőtt társadalom veszélytudatosságának elősegítése, valamint a digitális írástudatosság fejlesztése érdekében médiakampányok és edukációs programok támogatása a tagállamokban;
- az online visszaélés áldozatainak utólagos kezelésére civil szervezetek létrehozása és a szakmai párbeszéd megélénkítése az igazgatási, az igazságszolgáltatási szervek és civil szervezetek között;
- a 24/7 bejelentővonalak (hotline-hálózat) létrehozása az illegális és káros online tartalmak bejelentésére;
- intervenciós programok kidolgozása a szexuális elkövetők kezelésének biztosítására.

A digitális tudatosságnövelő kampányok és felvilágosító programok kidolgozását, a felhasználók tájékoztatását, valamint a hotline-ok létrehozatalát és nemzetközi hálózattá formálódását az Európai Parlament és a Tanács a Biztonságosabb Internet Akcióprogram keretében már 1999 óta hangsúlyozza,[9] összhangban az Európa Tanács Cybercrime Egyezményével.

A gyermekekkel szembeni online visszaélések kutatása terén nagy előrelépést jelentett a London School of Economics által koordinált, 25 ország részvételével folyó, *EU Kids Online* elnevezésű nemzetközi empirikus kutatás, amely 2009-ben indult. Az előzetes eredményeket 2010 novemberében publikálták, és a kutatás keretében 2011 nyarára várható a részletes nemzetközi összehasonlító elemzés.[10] (*Livingstone & Haddon, 2009*)

A kutatás vizsgálta a leggyakrabban internetező korosztály (9-16 éves gyerekek) és szüleik internetezési szokásait, az internet-használat kockázati fajtáit, a kockázatokkal való megbirkózás mikéntjét, valamint a szülők „kockázat-tudatosságát”, a gyerekeknek nyújtott segítség szintjét és mikéntjét.

Az OKRI és az ESZTER Alapítvány kutatása 2009-2010-ben ugyancsak ezeket a kérdéseket vizsgálta, a budapesti 15-16 éves korosztály vonatkozásában.[11]

A kutatások lehetőséget kínálnak az online veszélyek és kockázatok országonkénti eltéréseinek mérésére is. Erre azért van szükség, mert a gyerekeket fenyegető online veszélyekkel kapcsolatos morális pánikreakciók helyett racionális és a lokális sajátosságokat figyelembevevő alapokra kell építeni a biztonságos internetezést célzó, digitális tudatformáló kampányokat, valamint a lakosság és a szakemberek képzését is. A digitális tudatosságnövelő programok kidolgozására hazánkban, és más, 2004-ben és 2007-ben csatlakozó EU-tagállamokban későn került sor (Magyarországon a Safer Internet Program keretében csak nem rég, 2010 őszén kezdődött el). Ezeknek a programoknak a fejlesztése, nemzeti, regionális igényekhez alakítása még idejében megtörténhetne – a kutatási adatok további elemzésével és az eredmények célzatos hasznosításával.

---

[9] Action Plan for a Safer Internet, 1999-2002: http://europa.eu/legislation_summaries/information_society/l24190_en.htm; valamint Safer Internet Plus Action Plan, 2005-2008: http://europa.eu/legislation_summaries/information_society/l24190b_en.htm; illetve a jelenleg hatályos Safer Internet Program (SIP), 2009-2013: http://ec.europa.eu/information_society/activities/sip/index_en.htm; magyar vonatkozásait és megvalósítását l.: http://www.saferinternet.hu/bemutatkozas

[10] A projekt weboldala: http://www2.lse.ac.uk/media@lse/research/EUKidsOnline/Home.aspx; a magyar együttműködő partner weboldala: http://www.ithaka.hu/Kutatas/EU_Kids_Online

[11] A kutatást a Szociális és Munkaügyi Minisztérium és a Mérei Ferenc Fővárosi Pedagógiai és Pályaválasztási Tanácsadó Intézet támogatásával végeztük.

6. Nyomozás és nemzetközi együttműködés

Nemzetközi befolyását és tagállamainak számát tekintve is kétségtelenül az ENSZ tehet a legtöbbet a globális bűncselekmények megelőzése és kezelése érdekében.

Az Európai Unió állásfoglalása szerint nincs szükség új konvencióra. A Cybercrime Egyezmény mind a büntető anyagi jogi tényállások körét (számítástechnikai rendszer- és adatok elleni bűncselekmény, gyermekpornográfia stb.), mind az együttműködés büntető-eljárási menetét (házkutatás, lefoglalás, számítástechnikai adatok megőrzésére kötelezés), mind pedig a támogató infrastruktúrát (internet-szolgáltatók együttműködési szabályai, tárolandó, rögzítendő adatok köre, adatszolgáltatás szabályai, rendőrségi egységek az internetes bűnözés kezelésére, 24/7 hotline-ok) kidolgozta. Az ENSZ-nek az a szerepe, hogy a fejlődő országokban is meghonosítsa azokat a megoldásokat, amelyek a fejlett ipari régiókban (Európa, USA) már jól működő gyakorlattal rendelkeznek. Ehhez szükséges a háttértanulmányok, kutatásokat lefolytatása.

Speciális kérdések

Néhány tagállam nem tesz eleget a Cybercrime Egyezmény forgalmi és tárolt adatok valós idejű összegyűjtésére vonatkozó rendelkezésnek (20-21. Cikkely: *Real time collection of computer data*). A legtöbb államban különbséget tesznek a valós idejű tartalomra vonatkozó, illetve a valós idejű forgalomra vonatkozó adatok gyűjtése között az adatok eltérő szenzitivitása miatt. A hazai szabályozásban nem mutatkozik eltérés a kétféle adatgyűjtés alkalmazhatóságának feltételrendszerében.

Néhány állam esetében a támadások melyek az egyezményben szerepelnek nem elég súlyosak ahhoz, hogy ezekkel kapcsolatban tartalmi adatok ellenőrzését lehessen elrendelni, néhány esetben pedig még a forgalomra vonatkozó adatok ellenőrzésére sincs lehetőség. Ezek a technikák pedig elengedhetetlenül szükségesek az egyezményben szereplő bűncselekmények nyomozásához. Néhány esetben például nem lehetséges a forgalomra vonatkozó valós adatok valós idejű összegyűjtése nélkül a terjesztési cselekmények (a hozzáférhetővé tétellel megvalósított szerzői vagy szerzői joghoz kapcsolódó jogokat megsértése bűncselekmények) forrását meghatározni.

Nem tisztázott az Adatmegőrzési irányelv[12] megítélése, ugyanakkor az abban megszabott határidőket a tagállamok eltérően alkalmazzák, s ez akadálya lehet a nemzetközi ügyekben az adatszolgáltatásnak, illetve átadásnak. Az Irányelv legalább hat hónap és legfeljebb kettő év időkorláttal állapítja meg az adatmegőrzés idejét, a tagállamok ezen belül úgy is dönthetnek, hogy a megőrzési idő szolgáltatásonként, illetőleg adatfajtánként akár különböző. A 2003. évi C. törvény az elektronikus hírközlésről (a továbbiakban Eht.) a hatályos szabályozás szerint is megőrzendő adatok vonatkozásában a korábbi három év helyett egy éves, a sikertelen hívások során keletkező adatok megőrzésére vonatkozó új kötelezettség esetében pedig az Irányelv szerinti minimális megőrzési idő alkalmazását rendeli el.

[12] Az Európai Parlament és a Tanács 2006. március 15-i 2006/24/EK irányelve a nyilvánosan elérhető elektronikus hírközlési szolgáltatások nyújtása, illetve a nyilvános hírközlő hálózatok szolgáltatása keretében előállított vagy feldolgozott adatok megőrzéséről és a 2002/58/EK irányelv módosításáról (a továbbiakban Adatmegőrzési irányelv)

Az aggályok a rögzítendő adatok körének túl széles meghatározásával, valamint a tárolás túl hosszú idejével kapcsolatosak.

A gyakorlatban számos olyan megoldás *nem* működik, amely lehetővé tenné a gyors kommunikációt. Ilyen pl. az eljárási jogsegélyek teljesítésének könnyítésére létrehozott, elektronikus eszközzel történő kommunikáció. Az eljárási jogsegélyek teljesítésének hatékonysága érdekében az Európai Unió tagállamaival folytatott bűnügyi együttműködésről szóló 2003. évi CXXX. törvény bevezette, hogy a megkeresést írásban, indokolt esetben a megkereső azonosítását lehetővé tevő más alkalmas módon vagy eszközzel – különösen telefax vagy számítástechnikai rendszer útján – is elő lehet terjeszteni, illetőleg az így előterjesztett megkeresést szabályszerűnek kell tekinteni. Ez a szabály lényegesen meggyorsítja az eljáró hatóságok közötti kommunikációt, mivel e szabály alapján akár e-mail-en keresztül is kommunikálhatnak egymással a tagállami igazságügyi hatóságok.

Ehelyütt kell megjegyezni, hogy az igazságszolgáltatás szerveinek folyamatos technikai továbbképzése és a technikai újításokkal lépést tartó utánkövetéses felkészítése mennyire fontos.

7. Elektronikus bizonyítékok

A probléma főként a gazdaságilag alulfejlett államokban (Európában a keleti régió) áll fenn: a technikai eszközök pénzhiány miatt nem állnak rendelkezésre, a jogalkalmazók azokat szakértelem hiánya miatt nem használják, a bíróságok idegenkednek a bevezetésüktől. A probléma másik része az, hogy az igazságügyi IT szakértők nem sztenderdizált eljárásokkal végzik az elektronikus adatokat tároló eszközök vizsgálatát (lefoglalás, tárolás, hiteles másolat-készítés, nyomozó hatóságnak átadás), így az egyes szakértők munkája eltérő minőségű, esetenként a hitelesség megkérdőjelezhető. A Magyar Szakértői Kamara Informatikai Szakértői albizottsága anyagi eszközök hiányában nem egységesíti a képzést. A minőségbiztosítás pénzbe kerül (felkészülés, képzésen részvétel, kiesett munkaidő, technikai felszerelés beszerzése, karbantartása). Ugyanakkor a minőségbiztosítás nélkül dolgozó szakértő munkája olcsóbb, így nagyobb rá a kereslet. Tehát a minőségbiztosítással nem rendelkező szakértő több megrendelést kap, annak ellenére, hogy az így lefoglalt, biztosított elektronikus adat bizonyítóereje megkérdőjelezhető.

Az UNODC szerepe ezen a téren a jó gyakorlatok összegyűjtésére, elemzésére, a LEA számára oktatási modulok összeállítására, valamint a követendő gyakorlatok egységesítésére irányulhat.

8. Az internet-szolgáltatók felelőssége

Az internet-szolgáltatók (Internet Service Provider, a továbbiakban ISP) szerepe alapvető az internetes bűncselekmények felderítésében és nyomozásában, hiszen ők tartják nyilván (log-file) a felhasználók adatait, így ők szolgáltatnak adatot is a nyomozó hatóság részére. Az adatokat kétféleképpen osztályozhatjuk:

1. adat-típusok szerint: forgalomra vonatkozó adatok (*traffic data*); tartalomra vonatkozó adatok (*content data*); és előfizetőre vonatkozó adatok (*subscriber data*).
2. dinamikájuk szerint: tárolt adatok és a kommunikációban részt vevő adatok. Míg az előbbi esetében már egy lezajlott kommunikációhoz kapcsolódó adatokat kell érteni,

Az internet-szolgáltatók között megkülönböztetünk tartalomszolgáltatót, tárhely-szolgáltatót, közvetítő szolgáltatót.

Közvetítő szolgáltató: azon elektronikus hírközlési szolgáltató, amely az előfizetői hozzáférést nyújtó szolgáltatóval kötött hálózati szerződése alapján biztosítja az előfizető választása szerinti esetekben a hívott előfizető vagy szolgáltatás elérését. (pl. T-Online) (A különböző szolgáltatókról ld. Eht.)

Tartalom szolgáltató: tipikusan ilyen a felhasználó, aki az általa bérelt/megvásárolt webes felületre bármilyen saját anyagot (tartalmat) feltölt. De ilyenek az online sajtó- vagy bármilyen információ-szolgáltatások is.

Tárhely szolgáltató: a tartalom elhelyezéséhez tárhelyet szolgáltat.

Az ISP-k felelősségét az európai régióban az Elektronikus kereskedelemről szóló Irányelv (2000/31/EK) tartalmazza. Az új javaslatok bevezetnék a tárhely-szolgáltatók közvetlen felelősségre vonhatóságát is, amennyiben tudomásukra jut illegális tartalom közlése. A viták tárgya az, hogy mi tekinthető „tudomásszerzésnek", pl. egy állampolgár beadványa, levele elegendő, vagy szükség van a nyomozó hatóság eltávolítási felszólítására is.

Az utóbbi időben a szolgáltatók körében egyre nagyobb népszerűségnek örvend az önszabályozás. Ennek jó példája a tartalom- és tárhely-szolgáltatók körében alkalmazott *notice-and-takedown* eljárás, amelyet törvény nem, csupán magatartás-kódexek rögzítenek. A kormányzati szintű internet-blokkolás ellentételezéseként pl. ennek az eljárásnak az előnyét hangsúlyozzák a szolgáltatók önszabályozó testületei (nemzetközi szinten az INHOPE, Internet Hotline Association). Erre figyelemmel az önszabályozás, a magatartási kódexek kifejlesztését kellene támogatni. (*Parti, 2010c; Parti, 2009a*)

Speciális kérdések

Nem tisztázott az „anonimizáló szolgáltató" felelőssége. Az un. anonimizáló szolgáltatók lényege az, hogy anonimmé, azaz felismerhetetlenné teszik a hálózati kommunikációban részt vevő számítógép IP címét, ezzel elvileg lehetetlenné teszik annak visszakövethetőségét. Azonban mind a Cybercrime Egyezmény (17. Cikkely) mind a 2006/24/EK (azaz az Adatmegőrzési) irányelv éppen arra kötelezi a közvetítő szolgáltatót, hogy bizonyos forgalmi adatokat azonosítható formában őrizzen meg.[13] Ezzel az anonimizáló szolgáltatók ideje leáldozott, illetve fogyasztóvédelmi előírásoknak nem megfelelő a hirdetésük, mivel ők is kötelesek megőrizni és azonosíthatóvá tenni a kommunikációban részt vevő számítógépek autentifikációját.

A kommunikáció folyamatában érintett minden közvetítő szolgáltató egy lényegi információt birtokol a kommunikációs lánc során keletkezett forgalomra vonatkozó adatból. Ilyenkor a kommunikáció forrásának és céljának meghatározásához el kell jutni mindig a soron következő közvetítő szolgáltatóhoz. A 17. Cikkelyt mindegyik, a kommunikációban érintett közvetítő szolgáltató vonatkozásában alkalmazni lehet. A Cybercrime Egyezmény két megoldási lehetőséget javasol a kommunikációs lánc feltérképezéséhez. Az egyik, hogy a kommunikációs lánc újabb elemének felderítését követően a hatóság ismételten határozatot

[13] A Cybercrime Egyezmény 17. cikkében foglaltak átadási kötelezettséget írnak elő a forgalomra vonatkozó adatok vonatkozásában annak érdekében, hogy azonosítani lehessen más közvetítő szolgáltató érintettségét a kommunikáció továbbításban. (L. még: Cybercrime Egyezmény Explanatory report 165. pont)

hoz a soron következő közvetítő szolgáltató vonatkozásában, míg a másik megoldás szerint a megőrzésre kötelezett közvetítő szolgáltató értesíti a megőrzésre kötelezésről a soron következő közvetítő szolgáltatót. Ez utóbbi módszer nem került alkalmazásra a magyar jogban.

9. Büntetőjogon kívüli válaszok a számítástechnikai és az internetes bűnözésre

Miközben hajlamosak vagyunk a jogszabályok abszolutizálására és a jogérvényesítésbe vetett hitre alapozni a cselekményeinket, csak a jó gyakorlatok segítenek. Hiába vannak cizellált jogszabályaink, ha a jogalkalmazók technikai eszközök vagy megfelelő tárgyi tudás hiányában ezeket nem tudják érvényesíteni, ha a felhasználók digitális ismeretei nem kellő mértékűek. Éppen ezért hangsúlyozzuk a nyomozás és a bűnüldözés felszereltségének és személyi állományának és szakértőinek képzése fontosságát. Ezen túl, a felhasználói szintű tudatosság is fontos. Ehhez a bizonyítottan működő legjobb gyakorlatokat és tréning-modulokat dolgoznánk ki, és ezek alkalmazását különböző pályázatok segíthetik (a forrásokra lehetne pályázni eszközbeszerzés, képzés, szemlélet formálás tárgyában, akár nemzetközi konzorcium keretében).

10. A nemzetközi szervezetek munkája

A tagállamok megfogalmazták, hogy mindenekelőtt szükséges a különböző együttműködési szinteken keletkezett jogszabályok és végrehajtási rendeleteik (*Commonwealth Model Law*) összevetése, beleértve az angolszász és a kontinentális jogi gyakorlatok összevetését is.

11. Technikai segítségnyújtás

Felmerül egy olyan önálló modul létrehozása az UNODC-n belül, amely az internetes elkövetésű bűncselekmények nyomozásához adna segítséget: adatcsere megkönnyítésével, saját adatbázissal, illetve technikai segítséggel és jó gyakorlatok kidolgozásával, és oktatásával. Hasonlóan az Europol adatbázisához, közös nyomozócsoportjaihoz, az Interpol adatcserében nyújtott segítségéhez és nyilvántartásaihoz, az Eurojust koordináló tevékenységéhez, vagy akár az EU elfogatóparancsot nemzeti szinten végrehajtó, kijelölt bírák tevékenységéhez.

A technikai segítséghez szervesen tartozik a szakmák együttműködésének ösztönzése.

12. A magánszektor együttműködése

A technikai fejlődéssel nemcsak, hogy egyre nagyobb teret nyer az igazságügyi informatikai szakértő az internetes bűncselekmények nyomozásában, de elmosódik a határ a jogalkalmazói és a szakértői feladatok között is.

A számítógépek és az internet térnyerésével számos olyan kérdés merül fel, amelyről nem lehet eldönteni, hogy szakkérdés-e (tehát informatikai szakértő különleges *szakértelmét* igényli), vagy csupán olyan jogkérdés, amelyet a nyomozó hatóság tagja kellő *szaktudás* birtokában megválaszolhat. Nem egységes a nyomozó hatóságok gyakorlata pl. az IP-cím vagy az IP-cím szolgáltatója, illetve a weboldalak IP-címének megállapításában. Ezekre a kérdésekre az alapvető informatikai, internet-felhasználói ismeretek birtokában ma már az

ügy előadója is válaszolhatna, ennek ellenére a szokás hatalmának engedelmeskedve azt a mai napig a szakértő feladatává teszik. Hasonló a helyzet azokkal a kérdésekkel, amelyek ugyan jogkérdések, ám a legtöbbször mégis a szakértő válaszolja meg azokat.

Ennek oka egyfelől az, hogy hazánkban nem egységes a bizonyítékok hiteles feltárására (házkutatás), hiteles rögzítésére (lefoglalás vagy adatok megőrzésére kötelezés) és hiteles tárolására (időbélyegző, elektronikus aláírás) felhasználható technikai eszközök és gyakorlatok rendje és köre. Másfelől pedig az, hogy a nyomozó hatóság nem rendelkezik az alapvető technikai eszközökkel, amelyek a jogalkalmazói – különleges szakértelmet nem igénylő – feladatok ellátására alkalmassá tennék. Harmadsorban nem megoldott a jogalkalmazók folyamatos képzése és megfelelőségi vizsgálata sem.[14]

Hasonlóképpen nincs érvényben semmiféle szabvány Magyarországon az igazságügyi informatikai szakértők által alkalmazható technikai eszközök hitelességének biztosítására és a szakértő eljárásának auditjára sem, annak ellenére, hogy a világon számos infokommunikációs hitelesítési szabvány rendelkezésre állna (pl. ITSEC, COBIT stb.). (*Szádeczky, 2010*) Az igazságügyi informatikai szakértők eljárása nem egységes, tehát nem megbízható, így nem is lenne elfogadható a büntetőeljárásban a következő területeken:

- a szakértő által használható technikai eszközök;
- az eljárás sorrendje;
- a bizonyítékok hiteles rögzítésének (házkutatás, lefoglalás, adathordozó csomagolása) rendje;
- a hiteles másolat készítésének, és az eredeti adathordozó hitelessége megóvásának szabályai;
- a bizonyítékok nyomozó hatóság számára rendelkezésre bocsátásának rendje;
- valamint a szakértőnek feltehető és az általa megválaszolható kérdések köre. (részletesen ld. *Parti, 2010a*)

Az internetes bűnözés felderítésében és nyomozásában alkalmazott technikai eszközök és eljárások egységesítésére a határokon átnyúló bűnözés elleni nemzetközi fellépés egységesítése érdekében is szükség lenne.

Speciális kérdések

Jogszabályalkotás és prevenció az interdiszciplinaritás jegyében. A jogalkotóknak meg kell ismerniük az információs technológia (IT) fejlesztőinek adatgyűjtéshez, adatkezeléshez való hozzáállását, hiszen az adatvédelem területén gyakorlatilag ők „alkotják" a szabályokat. Lawrence Lessig szavaival élve, ha a kód a jog, akkor a kód alkotói egyben a jogalkotók *(„if the code is the law … then the coders are the legislators"*). Ha pedig a kódok fejlesztői a jogalkotók, akkor meg kell ismernünk a szemléletüket, a gondolkodásukat ahhoz, hogy megértessük velük, milyen szabályoknak szeretnénk, hogy megfeleljenek az adatbázisok és az adatkezelés.

A bűnüldözés egy helyben topogna a technikai szakemberek segítsége nélkül. Az IT-szféra bevonásával olyan jogi környezetet kell kialakítani, amely megteremti az internetes bűnözés elleni sikeres fellépés alapjait. A jogalkotók és a jogalkalmazók folyamatos, gyakorlatorientált képzése és továbbképzése mellett biztosítani kell a szakmák együttműködését a felmerülő új problémák megoldásában és a jó gyakorlatok kialakításában.

[14] 11/2003. (V. 8.) IM–BM–PM együttes rendelet és 23/2003. (VI. 24.) BM–IM együttes rendelet foglalkozik ezekhez kapcsolódó szabályokkal, ennek is lehetnének közös, jogszabályba foglalt feltételei

Emellett a társadalomtudományok együttműködésére is szükség van a gyakorlatban alkalmazható jogszabályok, valamint a hatékony prevenciós programok kidolgozásához. Így például az egyes internetes bűncselekmények megelőzéséhez ismernünk kell nemcsak a bűncselekmények kimeneti oldalát (eredmény, kár nagysága és jellege, sérülés mértéke), hanem a bemeneti oldalát is (elkövető motivációi, sértett közrehatása, megelőzés érdekében tett intézkedései). Ehhez elengedhetetlen a jelenlegi helyzet felmérésére szolgáló empirikus kutatások lefolytatása.

A különböző szakmák párbeszéde az internetes bűnözés elleni fellépés területén elengedhetetlen. Ennek megfelelően gondot kell fordítani a szakmák hálózatosodására és a jogszabályalkotásnál időt kell hagyni a szakmák közti egyeztetésekre. A nemzetközi együttműködés, a közös fellépés sikere érdekében át kell venni más országok jó gyakorlatait, de még inkább közösen kell kifejleszteni ilyeneket. Erre kell törekedni nemcsak a pályázatírásnál, hanem a projektek megvalósításánál is.

Eredmények

- Az ülésen a tagállamok megfogalmazták az egyes pontokhoz tartozó véleményüket.
- Az ülés végén elfogadtuk a számítástechnikai és internetes bűnözés felmérését szolgáló kérdőív főbb pontjait. A kérdőíves vizsgálatot az ENSZ Főtitkársága fogja elvégezni úgy, hogy a kérdőívet minden régiónak kiküldi. Ilyen „régiónak" számít pl. az Európai Unió.
- A vizsgálat elvégzéséhez minden régióban legfeljebb hat szakértőt jelölnek ki, akik igénybe vehetnek további szaktanácsadókat munkájukhoz. A vizsgálat célja az internetes bűnözés jelenségének és az arra adható válaszoknak a globális szintű felmérése, a nemzetközi együttműködés nehézségeinek és a helyi, valamint a régiós szintű jó gyakorlatoknak az összegyűjtése és összevetése. A vizsgálat elvégzésének ideje két év, végleges eredmények 2013 tavaszára születhetnek.

Bár a Munkacsoport (elnevezésében is) „szakértői" volt, az egy hetes munkát a témával kapcsolatos diplomáciai/politikai érdekek érvényesítése dominálta. Az eredményeket – amit a magyar küldöttség vezette EU koordináció jelentős sikerének tekinthetünk - *Dr. Csuday Balázs* nagykövet az alábbiak szerint értékelte.

"Az ülésszakon a bécsi EU Team a CATS 2010. december 13-i brüsszeli ülésén elfogadott mandátumot sikeresen képviselte, miszerint az EU a számítógépes bűnözés kapcsán az Európa Tanács (CoE) által létrehozott, ám globálisan hozzáférhető „Budapesti Egyezményt" tartja a legmegfelelőbb nemzetközi jogi instrumentumnak. Így elutasítja az ENSZ égisze alatt létrehozandó „Cybercrime Konvenciót".

Kifejtés:
A CATS mandátum alapján az EU Team felvette a kapcsolatot az Európa Tanács és a COM szakértőivel annak érdekében, hogy az ülésszakon koordinált álláspontot képviselve meg tudja akadályozni egyes államok azon törekvését, hogy az elkészítendő tanulmány egy új ENSZ Cybercrime konvenció előkészítését irányozza elő. Ennek érdekében az EU szorosan együttműködött - az Európa tanács mellett- az USA delegációjával is.

Az ülésszakon elfogadott, az elkészítendő tanulmány témaköreit meghatározni hivatott dokumentumban az EU számára legfontosabb kérdések megfelelő módon szerepelnek.

1., A számítógépes bűnözésre adott jogi válaszok fejezetben az emberi jogokra és az adatvédelemre vonatkozó biztosítékok kerültek be az EU javaslatára: *„Safeguards and conditions including protection of fundamental human rights and personal data.* Ezzel párhuzamosan (*package deal*) elfogadtuk Kína Oroszország által is erőteljesen támogatott javaslatát, amely önmagában nem tartalmazott az EU érdekeivel szemben álló elemeket és korábbi ENSZ dokumentumokban is szerepel: "*Respect for the principle of state sovereignty and equality of States, non-interference into the affairs of other States".*

2. A nemzetközi instrumentumokra vonatkozóan, az elkészítendő tanulmány céljaira történő utalás kapcsán - intenzív informális egyeztetéseket követően – az EU által javasolt kompromisszumos megfogalmazásban egyeztek meg a felek. *„Examining options with regard to effective legal bases, including universal international bases, and other options for combating cybercrime."*

3. A tanulmány témakörei között helyet kapott a technikai segítségnyújtás, valamint a büntető igazságszolgáltatási képességek fejlesztése a jobb nemzetközi együttműködés elősegítése érdekében. Az EU-ban kiemelkedően működő 24/7 hálózat legjobb gyakorlatára való utalás szintén szerepel a szövegben. *„Inventory of best practice examples from bilateral and multilateral treaties and arrangements, inter alia, lessons learned from the functioning of the 24/7 network of focal points; Identification of ongoing and ideas for future training programmes, exchanges of experiences, capacity-building and technical assistance activities to strengthen criminal justice capabilities and enable countries to cooperate internationally."*

A tanulmány elkészítése kapcsán alkalmazandó metodológia meghatározása során is sikerült az EU álláspontját eredményesen érvényre juttatni, eszerint a tanulmányt az **UNODC Titkárság készíti majd el. A regionális csoportok szakértőket javasolhatnak (maximálisan 6 főt)**, akikkel a Titkárság szükség esetén konzultál. Az **EU és partnerei sikeresen akadályozták meg, hogy egy formális (al)csoport jöjjön létre, amely felügyelné a Titkárság tevékenységét a tanulmány elkészítése kapcsán.**

Megjegyzés:

A munkacsoport ülései során az EU tagállamok kitűnőnek minősítették az EU Team koordinációs tevékenységét, az információk folyamatos megosztását, valamint üdvözölték az USA és az Európa Tanács delegációival való zökkenőmentes, eredményes együttműködést. **Mindez annak tükrében is jelentősnek mondható eredmény, hogy az EU Team e témakört illetően a gyakorlatban a magyar elnökség, vagyis Képviseletünk irányításával, illetve hazai szakértőink támogatásával végezte munkáját."**

Irodalomjegyzék

Bocij, P. (2004) *Cyberstaling: Harassment in the Internet age and how to protect your family.* Praeger: Westport, Connecticut, London

Kármán G., Mészáros Á., Nagy L.T. & Szabó I. (2010) *A szellemi tulajdonjogokat sértő bűncselekmények vizsgálata. Empirikus elemzés.* OKRI Zárójelentés

Krémer F. (2010) *Rossz döntések kora*. Napvilág Kiadó

Livingstone, S. & Haddon, L. (Eds.) (2009) *Kids Online. Opportunities and Risks for Children*, Policy Press, Bristol

Moitra, S.D. (2003) *Analysis and Modelling of Cybercrime: Prospects and Potential,* Research in Brief, Max Planck Institute for Foreign and International Criminal Law Freiburg

Murff, K. N. (2007) *Digital Crime Investigation Trends in State and Local Law Enforcement,* UMI Dissertation Services, UMI Number: 3294390 Ann Arbor, Michigan, USA

Parti K. (2010a) *Beszámoló az INFOLABOR – Az elektronikus bizonyítékszerzés helye és szerepe a büntetőeljárásban c. konferenciáról* In: Ügyészek Lapja 2010/2, pp. 75-82

Parti K. (2010b) *Újratervezés, avagy miért fontos az elektronikus bizonyítékszerzés?* In: Rendészeti Szemle 2010 (58. évf.) 3. sz. pp. 99-107

Parti K. (2010c) *„10 dolog, amit utálok benned", avagy a kormányzati szintű internet-blokkolás kritikája a német törvény kapcsán* In: Infokommunikáció és Jog, 38. szám (2010. június) pp. 97-104

Parti K. (2009a) *The importance and future of alternative reporting hotlines* In: e-Newsletter on the Fight Against Cybercrime, September 2009 Online: http://www.cybex.es/e-newsletter/2009/indice_nl0909_en.html

Parti K. (2009b) *Gyermekpornográfia az Interneten*. Bíbor Kiadó

Parti K. (2004) *Az internetes bűncselekmények nyomozásának egyes kérdései* In. Kriminológiai Tanulmányok 41. Budapest, 2004. Szerk.: Irk Ferenc pp. 249-75

Peszleg T. (2010) *A digitális bizonyítási eszközök megszerzésének elvei és gyakorlati érvényesülésük* In: Ügyészek Lapja 2010/2 pp. 23-32

Szabó I. (2010) *„The Pirate Bay" case in the mirror of Hungarian criminal law.* In: Ügyészek Lapja 2010/2 pp. 83-106

Szűts M. (2008) *Számítógépes bűncselekmények* In: Kondorosi F. & Ligeti K. (Szerk.) Az európai büntetőjog kézikönyve, Magyar Közlöny- és Lapkiadó 2008, pp. 601-611

Wall, D.S. (2001) *Maintaining order and law on the Internet*, In: Wall, D.S. (Ed.): *Crime and the Internet,* 167-83 Routledge: London

Wall, D.S. (2008) Cybercrime, media and insecurity: The shaping of public perceptions of cybercrime, *International Review of Law Computers & Technology* Vol. 22 Nos. 1–2: 45–63

Wall, D. (2010) *Criminalising cyberspace: the rise of the Internet as a 'crime problem'* In: Yar, M. & Jewkes, Y. (Eds.) Handbook of Internet Crime, Willan, pp. 88-103