Magyar Rendészet 2017/5. 83–103.

A bűnüldözés előtt álló digitális kihívások[1]

SIMON Béla[2]

Ez a tanulmány célul tűzte ki, hogy áttekintést adjon arról, hogy a bűnüldöző szervek számára milyen kihívásokat jelentenek az információs forradalom által generált új jogviszonyok és lehetséges visszaélések. A kutatás módja a nemzetközi irodalom átvizsgálása és annak összevetése a magyarországi gyakorlattal. A cikk következtetései szerint fontos többek között a feladatmegosztáson alapuló nemzetközi együttműködés fejlesztése, a legjobb gyakorlatok átvétele, az offenzív hírszerzési munka, a kiterjedt bűnmegelőzési tevékenység és az információs biztonság előtérbe helyezése a piaci szereplőknél.

Kulcsszavak: *rendészeti szervek, kiberbűnözés, jövőkép, kihívás*

E tanulmány címe némiképp félrevezető, hisz tartalmát illetően nemcsak a bűnüldözéssel, hanem a bűnmegelőzéssel, a bűnfelderítéssel, a büntető igazságszolgáltatással kapcsolatos kihívásokkal is foglalkozik, és természetesen nemcsak a digitális kérdéseknek kell megfelelni ezen rendszereknek, de a címválasztással arra is rá kívántam világítani, hogy bár a több évezredes múltra visszatekintő bűnüldözésünk az elmúlt évtizedek során robbanásszerű fejlődésen esett át, de még nagyon nagy fejlődésen kell keresztülmennie az eljövendő években, évtizedekben is. Ez a tanulmány próbál a következő évek fejlesztési horizontjának egyes szegmenseiből bemutatni néhányat, és tesz pár javaslatot a bűnüldözés hatókörén messze túlmutató kérdéskörben.

Számos olyan kérdés vetődik fel a – jelenleg is zajló – ötödik információs forradalommal összefüggésben, amelyre a jogalkotóknak és a jogalkalmazóknak választ kell találniuk vitás kérdések eldöntésekor. Ezek egy része kapcsolódhat bűncselekményekhez is. Például a kripto valuták vagy a szellemi tulajdon sérelmével járó tevékenységek számos civiljogi problémát vetnek fel, de szorosan kapcsolódhatnak bűncselekményekhez is. Ezek kontraktuális viszonyaival például csak annyiban indokolt foglalkoznunk jelen tanulmány keretein belül, amennyire az a deliktuális felelősség eldöntéséhez szükséges. A társadalmat sértő normaszegések közül tehát csak a legsúlyosabbakat vizsgáljuk, azokat, amelyek bűncselekmény megvalósulását eredményezik. A hatályos büntető

[1] A mű a KÖFOP-2.1.2-VEKOP- (tel:15201600001) azonosítószámú, „A jó kormányzást megalapozó közszolgálat-fejlesztés” elnevezésű kiemelt projekt keretében működtetett Ludovika Kiemelt Kutatóműhely keretében, a Nemzeti Közszolgálati Egyetem felkérésére készült.

[2] SIMON Béla tanársegéd Nemzeti Közszolgálati Egyetem Rendészettudományi Kar, Bűnüldözési és Gazdaságvédelmi Tanszék
Béla SIMON assitant lecturer, NUPS Faculty of Law Enforcement, Department of Law Enforcement and Economic Crime
orcid.org/0000-0002-1555-3690, simon.bela@uni-nke.hu

törvénykönyvünk alapján ez szándékos vagy – ha a törvény a gondatlan elkövetést is bünteti – gondatlanságból elkövetett cselekmény, amely veszélyes a társadalomra, és amelyre a törvény büntetés kiszabását rendeli. Kapcsolódóan a törvény rögzíti, hogy a társadalomra veszélyes cselekmény az a tevékenység vagy mulasztás, amely mások személyét vagy jogait, illetve Magyarország Alaptörvény szerinti társadalmi, gazdasági, állami rendjét sérti vagy veszélyezteti.

Az elmúlt évtizedekben az informatika fokozatos térnyerése az idézett fogalom két elemének is jelentős bővülését okozta. Egyrészt maga a védendő érdek – a személyek veszélyeztetett jogai – növekedett: tulajdonképpen rendkívüli módon megerősödött és a legfőbb értékké vált az információ. Kifejlődött és a modern társadalmak létezésének alapfeltételévé vált a jól működő IKT-szektor. Egy új veszélyeztetett érték jött létre, amely önmagához kötött minden, korábban nagy jelentőségűként számon tartott értéket. Például a nyersanyagok és az energia évszázadokkal korábban is értékek voltak, de a jelenlegi rendkívül összetett elosztásuk, hatékony felhasználásuk lehetetlen volna IT-infrastruktúrák nélkül. Egy termék gyártási folyamatai korábban is jelentős értéket képviseltek, de most már a folyamatokat vezérlő informatikai rendszerek és azok zavartalan működéséhez kapcsolódó érdek is jelentősen veszélyeztetett értékeknek minősülnek.

A másik – a fenti fogalomhoz kapcsolódó – bővülés a jogellenesség körének bővülése. Sokkal több olyan cselekmény vagy mulasztás van, ami a Magyarország Alaptörvénye szerinti társadalmi, gazdasági, állami rendjét sérti vagy veszélyezteti. Ezek nemcsak abból adódnak, hogy a jogalkotó pönalizált olyan cselekményeket, amelyek korábban nem voltak tiltva, hanem a régóta kodifikált tényállásokat is sokkal több módon lehet kimerítenie az elkövetőknek.

A különböző szektorszintű modernizációs törekvések: e-kormányzat, e-bankolás, e-egészségügy, e-tanulás, új generációs energiaellátás és -vezérlés, a közlekedés és a közszolgáltatások automatizálása, az intelligens városok és az okosinfrastruktúra kialakítása – szerepelnek az első helyen a legtöbb állam hosszú távú innovációs stratégiájában. Kína, India, Európa, Észak-Amerika mind-mind a „digitális alapokon nyugvó tudásközpontú gazdaság" irányába szeretnének haladni, támogatva az IT-szektor számára a munkaerőt biztosító képzési és átképzési tevékenységeket és minél több, a szektorhoz köthető munkahelyteremtő beruházást vonzani az adott országba a pénzügyi, az egészségügyi, a tudásmenedzsment területén és más határterületeken is.[3]

Az Európai Bizottság 2015. évi digitális egységes piaci stratégiájára vonatkozó előterjesztése szerint is az internet és a digitális technológiák átalakítják világunkat. Az online tranzakciók útjában álló akadályok miatt azonban a fogyasztók nem férnek hozzá bizonyos termékekhez és szolgáltatásokhoz, az internetes és az induló vállalkozások kilátásai korlátozottak, és sem a gazdasági szereplők, sem a kormányok nem tudják teljes mértékben kihasználni a digitális eszközök nyújtotta előnyöket. Az EU egységes piacát ezért hozzá kell igazítani a digitális korhoz: meg kell szüntetni azokat

[3] Horváth (2016)

a szabályozási akadályokat, amelyek az online szolgáltatások piacának széttagoltságát eredményezik. Ez évi 415 milliárd euróval gazdagítaná az uniós gazdaságot, és több százezer új munkahely létrejöttét eredményezné.[4] Az egységes digitális piac létrehozásával Európa évente mintegy 500 milliárd euróval növelhetné GDP-jét,[5] ami 1000 EUR/fő növekedési átlagot jelent. Az elmúlt években pedig ezt előmozdító intézkedések születtek:[6] roaming, adatroaming költségek megszűnése, csökkenése, több európai felhőszolgáltatás,[7] digitális hálózatok és szolgáltatások térnyerését elősegítő környezeti feltételek megteremtése.

Mindezek az innovációk nemcsak a piaci szereplők, a nyereséget termelő vállalkozások esetében kell hogy működjenek, hanem a rendvédelmi szerveken belül és azok között is hasonlóan nagy ívű tervek és erőforrások szükségesek. Az IT-szektorban a piaci szereplők egy őrült versenyfutásban vannak a fejlesztéseikkel a konkurencia megelőzésének érdekében.[8] Ez sok esetben a biztonság rovására megy. A rendvédelmi szervek is versenyben állnak a bűnelkövetőkkel szemben, de a biztonság itt sokkal fontosabb tényező. Mindezekkel együtt is a rendvédelmi szerveknek alkalmazniuk kell azokat a folyamatmenedzselési, -fejlesztési eljárásokat stb., amelyeket az IT-szektor multinacionális vállalatai kialakítottak, de természetesen a rendészeti szervek megvalósíthatósági keretein belül. A magyar – és jellemzően más – rendvédelmi szervek sem a brainstorming, a Pareto-elemzés,[9] az FMEA[10]-elemzés stb. eszközrendszerét használják a mindennapokban, de a hierarchikus működés egy félkatonai szervezetnél nagyon nehezen teszi lehetővé az egyébként működőképes eljárások alkalmazását is.

Nemzetgazdasági szinten hét pillére van annak az ökoszisztémának, amelybe a biztonsági aspektusoknak szervesen be kell épülniük ahhoz, hogy az adott országot megfelelően felkészültnek tekinthessük informatikai biztonsági kérdésekben, ahogy Melissa Hathaway és kutatótársai ezt megfogalmazták:

1. Létezik-e az adott országban nemzeti kiberbiztonsági stratégia?
2. Meg van-e oldva e szervezett incidenskezelés?
3. Megfelelően kezeli-e a törvényhozás és a bűnüldözés a kiberbűncselekményeket?
4. Része-e az adott ország azoknak az információmegosztó hálózatoknak, amelyek segítenek megfelelően és gyorsan reagálni a fenyegetésekre?
5. Megfelelő-e az informatikai-biztonsági kutatásfejlesztésbe való befektetések aránya?

---

4 www.ec.europa.eu/commission/priorities/digital-single-market_hu (2017. 08. 11.)

5 European Policy Centre (2010)

6 ec.europa.eu/digital-single-market/ (2017. 08. 11.)

7 ec.europa.eu/digital-single-market/en/%20european-cloud-initiative (2017. 08. 11.)

8 A szoftverfejlesztés területén már rég túlhaladtunk azon az állapoton, amikor a néhány kilobájtnyi kódot az emberi elme képes volt átlátni és megtalálni benne a hibákat. A jelenlegi szoftverek többsége olyan összetett és átláthatatlan, hogy nyilvánvalóan magában hordozza a hibák lehetőségét.

9 Egy elemzési típus, amely segíthet abban, hogy azonosíthassuk a fő problémákat, illetve differenciált stratégiát alakíthassunk ki a különböző fontosságú területek esetében.

10 „Lehetséges hibák és összefüggéseinek elemzése"; „hibamód és -hatás elemzés". Az FMEA egy szisztematikus módszer a lehetséges hibák felismeréséhez, elemzéséhez, értékeléséhez, kezeléséhez és ezáltal a megelőzésükhöz.

6. Része-e az IT-biztonsági problémák kezelése a diplomáciai, a külpolitikai, illetve a kereskedelempolitikai tevékenységnek?
7. Megfelelő szintű-e a kibervédelem és az incidenskezelés a honvédelmi, külső elhárítási területen?[11]

Kijelenthetjük, hogy a fenti kritériumokkal Magyarország jó helyen áll, de ezek a pontok alkalmasak arra is, hogy az egyes területeken megvizsgáljuk, hogy a bűnüldöző szervek mindent megtesznek-e az informatikai biztonság érdekében. Magyarország Nemzeti Kiberbiztonsági Stratégiája[12] a bűnüldözés, a bűnmegelőzés feladatait és koncepcióját nem részletezi, de európai megfelelője[13] a jövőképet öt stratégiai prioritásban foglalta össze, amelyből a második a számítástechnikai bűnözés drasztikus csökkentése.

A bűnüldöző szervek részvétele az incidenskezelésben jelenleg nincs biztosítva intézményesítetten. Ezt igazolják azok a statisztikai adatok, amelyek a kormányzati, önkormányzati szektort ért támadások és az azok alapján indult büntetőeljárásokról adnak adatokat.[14]

A kibertérben elkövetett bűncselekmények ítélkezési gyakorlatának egységességére vonatkozóan további vizsgálatok szükségesek.

Bűnszervezetek a kibertérben

A jogrendet fenyegető egyik tényező a szervezett bűnözői csoportok megjelenése, amelyek számos kérdést adnak a bűnüldözésnek, de tulajdonképpen az egész jogrendszernek. Megítélésem szerint az anyagi javak kibertérbe történő eltolódása magával hozza a szervezett bűnözői csoportok fokozott aktivitását is a közeljövőben. A jelenlegi helyzet és a várható jövő prognosztizálása érdekében ezen alfejezetben áttekintem a lehetséges forgatókönyveket és az eddigi elméleteket.

Sok esetben felvetődött már a legfőbb államhatalmi szervek és a szervezett bűnözői csoportok összefonódása is. Ezek egy részében az állami szervek a bűnszervezetekhez hasonlóan az illegális anyagi előnyök megszerzése céljából létesítettek meg nem engedhető kapcsolatot,[15] míg más esetekben titkos, operatív műveletek során kapcsolódik a kibertérben szervezetten elkövetett bűncselekményekhez állami megrendelés (iráni nukleáris dúsító, az orosz állam érdekeit szolgáló DDOS- és hackertámadások stb.).

A határok nagyon elmosódottak. Egy ország létfontosságú rendszerelemét vezérlő informatikai eszközök ellen intézett támadás eredményét tekintve lehet teljesen azonos akkor is, ha csak egy cracker, ha egy terrorista szándékú elkövető, és akkor is,

---

11 Hathaway et al. (2015)
12 1139/2013. (III.21) Korm. határozat.
13 Az Európai Unió kiberbiztonsági stratégiája (2013)
14 Simon (2016a) 161–174.
15 Perl (2007). Az észak-koreai drogcsempészet esete: jellemzően elmondható, hogy a demokrácia alacsonyabb szintjén gyakoribb az összefonódás. A fejlettebb demokratikus berendezkedés során titkos, operatív műveletek során vetődhet fel az állami szervek és a szervezett bűnözői csoportok együttműködése.

ha egy állam kiberhadviselésre felkészített egysége hajtja azt végre. A valódi különbség csupán az elkövetők szándékában, céljában érhető tetten.

Természetesen vannak olyan jelek egy adott támadás során, amiből lehet következtetni az elkövető személyére (használt programkódok, azok nyelvezete, fejlettsége, a felhasznált eszközök, a célpont megválasztása stb.), ami ugyanúgy igaz egy létfontosságú rendszerelem ellen intézett bombatámadás esetén is (használt robbanószer anyaga, eszközök fejlettsége stb.), de a leglényegesebb különbség, hogy a kibertérben sokkal nagyobb a végrehajtók lehetősége arra, hogy az elkövető kilétére vonatkozó következtetések alapját meghamisítsák.

Mivel ezek a digitális bizonyítékok is a kettes számrendszer elemeiből állnak, elméletben visszamaradó nyomok nélkül hamisíthatók.

A számítógépes bűnözés típusainak és forrásainak sokfélesége miatt fontos elkerülni a számítógépes bűnözők sztereotipikus képét, vagy a valós veszélyhelyzetet messze meghaladó démonizálással egyfajta pánikot kelteni. A média híradásai alapján kialakultak már bizonyos képek: az anyagi érdekből fenyegető orosz hacker, a kínai „hackerpatrióta" vagy az észak-koreai államilag foglalkoztatott hacker. Az ilyen elkövetői csoportokról kialakított képek sokszor félrevezetőek lehetnek. A médiakép ellenére az elkövetők sok nemzetből származnak, és motivációik sokszínűek, bár vitathatatlan, hogy a korábbi szellemi kihívás helyébe a pénzügyi célok dominanciája került.[16]

Az ENSZ palermói egyezménye szerint[17] szervezett bűnözői csoport a „bizonyos ideig fennálló, három vagy több főből álló strukturált csoport, amely összehangoltan működik egy vagy több […] súlyos bűncselekmény elkövetése céljából, közvetlen vagy közvetett módon pénzügyi vagy más anyagi haszon megszerzésére törekedve". Ez az egységes fogalommeghatározás nem terjed ki olyan rendkívül kifinomult szervezési formákra, mint például akár több mint egymillió IT-eszközt magába foglaló zombigéphálózatok – botnetek – működtetése, amit akár egyetlen személy is megvalósíthat. Egyes szakértői vélemények szerint az egyedüli elkövető által mozgósított botneteket a szervezett bűnözés formájának kell tekinteni.[18]

Jól látható, hogy a szervezett bűnözés hagyományos definíciói mennyire elavultak, amikor a kibertér is a territórium egy része.

Ha kétségbe vonjuk a szervezett bűnözői csoportok kiterjedtségét, szerepét a kibertérben, azzal akadályozzuk a megfelelő ellenintézkedések kialakulását.[19] Miközben egyre több szakértő úgy véli, hogy a számítógépes bűnözés a szervezett csoportok tartományává vált, és az egyedül dolgozó hackerek napjai egyre múlnak, még valójában

---

[16] Néhány évtizeddel korábban a kártékony kódok alkotói sokkal inkább szellemi kihívásként tekintettek tevékenységükre, arra, hogy képesek-e egy program alkotóinak az eszén túljárni. Az idők folyamán ez a tevékenység sokkal magasabb képzettséget igényelt, és csak magasan kvalifikált személyek váltak képesek erre, akik ebből egyre inkább anyagi előnyt kívántak elérni.

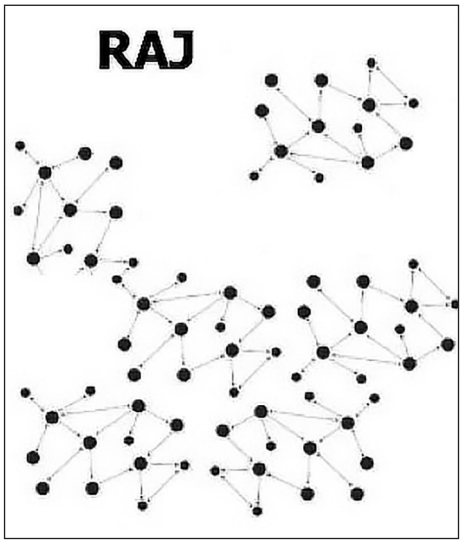
[17] 2006. évi CI. törvény: Az Egyesült Nemzetek keretében, Palermóban, 2000. december 14-én létrejött a nemzetközi szervezett bűnözés elleni Egyezmény kihirdetéséről.

[18] Chabinsky (2010)

[19] A magyar szervezett bűnözés elleni harcra sem hatott pozitívan, amikor 2003-ban egy fővárosi rendőrfőkapitány kijelentette, hogy nincs szervezett bűnözés.

kevéssé ismertek a csoportok által előnyben részesített struktúrák és hogy miképpen biztosítják a bizalmat a szervezeten belül. Hiányzik a bizonyítékokon alapuló kutatás a támadó viselkedésről és a számítógépes térben való toborzásról, bár a tanulás és utánzás fontos szerepet játszik.[20]

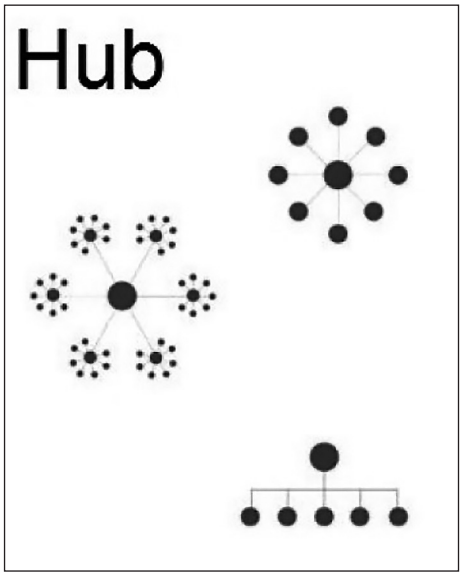
McGuire[21] kutatásában nagy számú ismert esetet vizsgált meg. Úgy találta, hogy a számítógépes bűnözés legfeljebb 80%-a lehet valamilyen szervezett tevékenység eredménye. Ez azonban nem jelenti azt, hogy ezek a csoportok hagyományos, hierarchikus szervezett bűnözői csoportok formáját öltik, vagy hogy ezek a csoportok kizárólag digitális bűnözést követnek el. A tanulmány inkább azt sugallja, hogy a hagyományos szervezett bűnözői csoportok új, lazább bűnözői hálózatok mellett bővítik tevékenységüket a digitális világra. A bűnözői csoportok különböző szervezeti szinteket mutatnak be attól függően, hogy tevékenysége kizárólag az online célokat szolgálja-e, vagy olyan online eszközöket használ, amelyek lehetővé teszik a „való" világban elkövetett bűncselekményeket, vagy kombinálják az online és az offline célokat.



1. ábra: A „raj" típusú hálózatok ábrázolása. Forrás: Broadhurst–Grabosky (2014)

A „rajok" a hálózatok számos jellemzőjét mutatják, és „közös célok nélküli szervezetlen csoportok"-ként írhatók le. Tagjaik közt tipikusan kevés kapcsolat van. Ilyen formákban működhetnek a korábbi „hacktivista" csoportok. Ez a típus leginkább az ideológiailag irányított online tevékenységekben (például a gyűlöletbűnözés és a politikai ellenállás) jelenik meg. Az Anonymous csoport egy tipikus raj típusú csoportot szemléltet.

[20] Broadhurst–Grabosky (2005) 347–360.
[21] McGuire (2012)



2. ábra: A „hub" típusú hálózatok ábrázolása. Forrás: Broadhurst–Grabosky (2014)

A hubok mint tömeg lényegében aktívak az interneten, de sokkal szervezettebbek, és világos parancsszerkezettel rendelkeznek. Ezek magukban foglalják a központi bűnözői középpontot (az agyat), amely körül a perifériás társaik összegyűlnek. Online tevékenységeik sokszínűek, például a kalózkodás, az adathalász-támadások, a botnetek, valamint az online szexuális bűncselekmények, a bankkártyaadatok, a kábítószerek és a prekurzorok kereskedelme. Például a Silk Roadot működtető piacok szintén illeszkednek ehhez a modellhez.

Központi parancsstruktúra, amely lehet hierarchikus. Erős kapcsolatok vagy folyamatos interakció az egyének között. Például a LulzSec rendelkezik a hub tulajdonságaival.

A hub típusú csoportoknak felrajzolhatjuk a különféle hibrid változatait: a fürtözött hibridben a bűncselekmény az egyének kis csoportja köré tagolódik, és konkrét tevékenységekre vagy módszerekre összpontosít. Némileg hasonlítanak a hubok struktúrájához, de zökkenőmentesen mozognak az online és az offline bűncselekmények között. E körben említhető tipikus csoportok a bankkártyás visszaélésekre szakosodott szervezetek, ahol a kártyaadatokat megszerző személyekre, majd azokat online vásárláshoz, vagy a megszerzett adatokat értékesítő személyekre tagolódnak.

A kiterjesztett hibrid hálózati formák a fürtözött hibridekhez hasonlóan működnek, de sokkal kevésbé centralizáltak. Általában sok munkatársat és alcsoportot foglalnak magukba, és számos bűncselekményt végeznek, de még mindig elégséges szintű koordinációt tartanak fenn működésük sikerének biztosításához.

A hierarchiában leginkább a hagyományos bűnözői csoportokat (például családi alapokon kialakított bűnöző csoportokat) írják le, amelyek néhány tevékenységet exportálnak az online térbe. A szervezett bűnözői csoportok tevékenysége a profit elérését célozza, így minden olyan tevékenységet megpróbálnak beindítani az online térben, ami az offline térben is hasznot hajt. Például a prostitúcióban tevékeny bűnözői csoportok érdeklődése kiterjed a pornográf weboldalakra vagy a szolgáltatások online értékesítésére. Ide tartoznak még az online szerencsejáték, a zsarolás az informatikai rendszerek leállításával összefüggésben, illetve a különféle nyilvántartások adatainak megszerzésével vagy hozzáférhetetlenné tételével kapcsolatos zsarolások – függetlenül attól, hogy az értékes adatokat hackeléssel, malware-ek segítségével vagy más módon érték el.

A csoportok tipizálása nem öncélúan történik. Ennek azért van kiemelt jelentősége, mert az ellenük való fellépés erőforrásigényét alapvetően meghatározza. Ha erős a személyes kapcsolattartás az adott csoportban, akkor ott lehetőség nyílhat a bűnügyi hírszerzés hagyományos erőinek (informátor, bizalmi személy, fedett nyomozó stb.) alkalmazására, de ezek hiányában az alkalmazásuk csak a kibertérről magas szintű ismeretekkel rendelkező munkatársakkal, informatikai megoldásokkal lehetséges.

A legkifinomultabb számítógépes bűnözői szervezeteket jelentős funkcionális specializáció és munkamegosztás jellemzi. Az Egyesült Államok Szövetségi Nyomozóhivatal Cyber Divíziójának egyik képviselőjének beszédében az alábbiak mutatják be, milyen szerepet játszhatnak a nagy csalások összeesküvései:[22]

- A kódolók vagy a programozók a rosszindulatú programokat, a kizsákmányolást és egyéb eszközöket írják le a bűncselekmény elkövetéséhez.
- A forgalmazók vagy a kereskedők eladják az ellopott adatokat, és garantálják a más szakterületek által kínált árukat.
- A technikusok fenntartják a bűnügyi infrastruktúrát és a támogató technológiákat, például a kiszolgálókat, az internetszolgáltatókat és a titkosítást.
- A hackerek az alkalmazások, a rendszerek és a hálózatok sebezhetőségét kutatják, és kihasználják annak érdekében, hogy rendszergazdai hozzáférést szerezzenek.
- A csalásszakértők „social engineering”-terveket fejlesztenek ki és alkalmaznak, beleértve az adathalászatot és a spameket.
- A szolgáltatók a „tiltott tartalomszerverek” és „helyek” biztonságos eszközeit nyújtják, gyakran bonyolult botnet- és proxyhálózatok révén.
- A pénztárosok ellenőrzik a folyószámlákat, majd ezeket a neveket és számlákat más bűnözőknek adják díj ellenében; tipikusan egyéni készpénzes futárokat is kezelnek.
- A pénzmosással foglalkozó személyek átruházzák a csalásokból származó bevételt, amelyet továbbítanak egy harmadik félnek, hogy helyezzék biztonságos helyre.

[22] Chabinsky (2010)

- Az elszámolók nyilvántartják a tiltott bevételt a digitális pénznemben és a különböző nemzeti pénznemek között.
- A szervezet vezetői a bűncselekmény elosztásának irányításán kívül választják ki a célokat, és tagokat rendelnek a fenti feladatokhoz.

Talán más, potenciálisan hasznos paradigmákat is találhatunk a számítógépes bűnözéssel foglalkozó szervezetek leírásában. A gazdasági földrajzból kiindulva az olyan vállalkozások csoportosítása, amelyek hasonló termékeket kínálnak ugyanazon a környéken, általában az egész világon megtalálhatók. A Tor böngészőn keresztül például a Silk Road, a tiltott piacok számára „hot point"-okká váltak az online kábítószer-kereskedelemmel foglalkozó vevők és eladók számára.

Vajon a működő szervezett bűnözői csoportok a jelentős profit reményében üzletágat indítanak a kiberbűncselekmények terén, mint ahogy egy sikeresen működő élelmiszer-áruház vagy hipermarket a honlapján beindítja a webshopot, hogy még nagyobb piacot teremtsen magának? Vajon inkább előzmények nélkül alakulnak ki új szervezett bűnözői csoportok, amelyek kellő tudás birtokában rájönnek, hogy a kibertérben használható tudásukat illegális jövedelemszerzésre is használhatják? Minden bizonnyal mindkét irányváltásra találunk példákat. Míg a számítógépes bűnözés számos fajtája nagyfokú szervezést és szakosodást igényel, nincs elegendő empirikus bizonyíték annak megállapítására, hogy a számítógépes bűnözés most a szervezett bűnözői csoportok uralma alatt áll-e, és milyen formát vagy struktúrát igényel ez a csoport.[23]

A kormányok, a bűnüldöző szervek, az akadémiai kutatók és a kiberbiztonsági ipar azt feltételezi, hogy a „hagyományos" szervezett bűnözői csoportok egyre inkább részt vesznek a digitális bűnözésben. A rendelkezésre álló empirikus adatok azt sugallják, hogy az online vagy a tartózkodási helyükön tevékeny, bűnöző személyek inkább a laza társulással működő tiltott hálózatokhoz csatlakoznak, mintsem formálisan is létező szervezetekhez.[24]

Az elmúlt években arra is volt példa, hogy politikai céljaik eléréséhez anyagi erőforrások érdekében valósítottak meg informatikai bűncselekményeket. Erre példaként említhető Imam Samudra, a 2002-es Bali robbantások helyszíni koordinátora, aki követőit arra szólította fel emlékirataiban, hogy például bankkártyacsalásokkal teremtsék elő a szükséges anyagi forrásokat a szent háborúhoz.[25]

Ez a megkülönböztetés idővel erodálódni fog, mivel a digitális technológia egyre átterjedtebbé válik.

Ahogy az összetett feladatokat ellátó informatikai vállalkozásoknak is specialistákat kell alkalmazniuk az egyes részfeladatok végrehajtásához, hasonló módon az összetett informatikai bűncselekmények elkövetéséhez is specialisták szükségesek.

Ha összevetjük a kibertérben és a való világban tevékeny bűnözői csoportokat, akkor számos hasonlóságot fedezhetünk fel. A leglényegesebb, hogy mindkét működési

[23] Lusthaus (2013) 52–60.
[24] Décary–Hétu (2012)
[25] Sipress (2004) A19.

formában szigorú konspiráció jellemzi, és céljuk az illegális profit. A való világban a csoportok tagjai sok esetben antiszociális személyiségjegyeket mutatnak, és a fizikai erőszaktól sem tartózkodnak, a kibertérben bűncselekményeket sorozatjelleggel elkövető személyek nem antiszociálisabbak, mint a legális tevékenységet folytató informatikusok.

A digitális technológiák az elmúlt évtizedekben lehetőséget biztosítottak az egyéneknek, hogy külső segítség és agresszív magatartás nélkül is jelentős hatást gyakoroljanak a kritikus infrastruktúrákra.[26]

Ezek az akciók természetesen reakciót váltottak ki az információs rendszerek üzemeltetői körében, és egyre nehezebbé vált magányos elkövetőként jelentős eredményeket elérni.

Tehát az elkövetői oldalon is szükségessé vált a szervezetekbe tömörülés. Nyilvánvaló, hogy sok, de nem minden típusú bűnszervezet alkalmas a számítógépes bűnözésre. Az internet és a kapcsolódó technológiák tökéletesen alkalmazkodnak az egyes tevékenységek közötti koordinációhoz.[27]

Egy, a kibertérben működő szervezett bűnözői csoport működhet nagyon strukturált, hagyományos maffiaszerű csoportként, amely bűnöző informatikai szakembereket vonz.

Elképzelhető, hogy egy meghatározott cél érdekében létrejön egy szigorúan konspirált bűnözői csoport, de az eddigi megismert esetekben ezek egy-egy konkrét bűncselekmény vagy egy konkrét sértett ellen, illetve cél érdekében szerveződnek, tehát nem tartós jellegű együttműködés, hanem sokkal inkább a projektszemlélet uralkodik.

A szervezett bűnözői csoportok végső célja a profit elérése, így abban az esetben, ha szervezetten, de politikai célzattal követnek el jogsértő cselekményeket, azt nem sorolhatjuk a szervezett bűnözői csoportok tevékenységéhez.[28]

A kibertérrel kapcsolatban hosszú távú bűnös együttműködés sokkal inkább jellemző különféle illegális adatokkal összefüggésben: például szellemi tulajdon sérelmével járó tartalmak, gyermekek szexuális abúzusaival összefüggő illegális tartalmak. Ezekben az esetekben a sértetteket érő vagyoni kár[29] jellemzően nem jár együtt az elkövetők vagyoni gyarapodásával.

A számítógépes bűnözők laza hálózatokként működhetnek, de a bizonyítékok arra utalnak, hogy a tagok szoros földrajzi közelségben helyezkednek el, még akkor is, ha támadásaik a határokon átnyúlnak. Például a kis helyi hálózatok, valamint a rokonok és barátaikra koncentráló csoportok továbbra is jelentős szereplők maradnak. A szervezett bűnözői csoportokkal való lehetséges kapcsolatokkal rendelkező számítógépes

[26] Morgenson (2000). Több esetben magányos tinédzserek légiforgalmiirányító-rendszereket kompromittáltak, leállítottak nagyobb e-kiskereskedőket, vagy akár manipulálták a kereskedelmet a NASDAQ tőzsdén.

[27] Netmeeting, weblearning, távmunka, home office stb.

[28] Azokat az eseteket, amikor a szervezett bűnözői csoportok politikai befolyást kívánnak szerezni bűnös úton – szintén a hatalom, és azon keresztül a vagyoni javak megszerzése motiválja.

[29] A szoftverkalózkodás, az illegális filmletöltés stb. esetében nem beszélhetünk vagyoni kárról, csak elmaradt vagyoni előnyről.

bűnözés forrópontjait Kelet-Európában és a volt Szovjetunióban találják.[30] Az orosz és az ukrán hackereket ügyes újítóknak tartják. Például a romániai Ramnicu Valcea kisváros központja ilyen centrumnak számít Kelet-Európában.[31] Az elmúlt évtizedben a kínai számítógépes bűnözésről is egyre aggasztóbb információk érkeznek.[32]

Nemzetközi egyezmények, nemzetközi együttműködés

A több mint 15 éves budapesti cybercrime egyezmény *(Convention on Cybercrime)* továbbra is a számítástechnikai bűnözésről és az elektronikus bizonyítékokról szóló legfontosabb nemzetközi megállapodás marad, nemcsak a belföldi jogszabályok iránymutatásaként és a nemzetközi együttműködés alapjaként, hanem az együttműködési kapacitásépítés katalizátoraként is.[33]

Az Európai Unió a joghatósági korlátok ledöntése terén számos előremutató intézkedést tett. Például a korábbi irányelvek egyik közös jellemzője volt, hogy különleges szabályokat állapítottak meg az Európai Unió tagállamain kívül elkövetett extraterritoriumi bűncselekményekkel kapcsolatos joghatóság érvényesítésére, amennyiben az elkövető az érintett tagállami állampolgárok egyike. A 2011. december 13-i 2011/92/EU irányelv[34] azonban továbblép, és kifejezetten magába foglalja a joghatóság alárendeltségét és az elkövetők büntetőeljárás alá vételének követelményét.

A számítógépes rendszerekkel és az internetet használó támadásokkal kapcsolatos bűncselekmények tekintetében a joghatóság érvényesítésére vonatkozó európai jogi keret valószínűleg az egyik legátfogóbb. Annak ellenére, hogy a világ ezen régiójában a számítógépes bűnözés elleni bűnüldözésre vonatkozó joghatóság érvényesítésére törekszik, a valóság az, hogy az egyes uniós tagállamok által elfogadott megközelítések között még nincs teljes egységesség. Az Európai Unió tagállamainak nemzeti bíróságai továbbra is diszkrecionális jogköröket alkalmaznak a nemzeti eljárási büntetőjogi törvények alapján annak érdekében, hogy saját módszertanuk és jogi hagyományaik szerint járjanak el az internetes bűncselekményekkel vagy az információs technológiák támogatásával elkövetett bűncselekményekkel kapcsolatos ügyekben.

A bűnüldözés nemzetközi hatóképessége érdekében szükséges, hogy a budapesti cybercrime egyezmény minél szélesebb körben elfogadottá váljon, vagy hogy szellemiségének megfelelő más egyezményeket írjanak alá az államok. Például Afrikában és az UNODC országokban az elmúlt években számos ország megreformálta a belföldi jogszabályokat, gyakran iránymutatásként a budapesti egyezményt alkalmazva. Ugyanakkor például az afrikai országok több mint fele még nem rendelkezik jelenleg a szükséges jogszabályokkal, de az Afrikai Unió Malabo Egyezménye tükrözi az afrikai

[30] Kshetri Nir (2013) 39–65.
[31] Bhattacharjee (2011)
[32] Wang Jingqiong (2010)
[33] Octopus Conference (2016)
[34] Az Európai Parlament és a Tanács 2011/92/EU irányelve (2011. december 13.) a gyermekek szexuális bántalmazása, szexuális kizsákmányolása és a gyermekpornográfia elleni küzdelemről, valamint a 2004/68/IB tanácsi kerethatározat felváltásáról.

vezetők világos politikai elkötelezettségét a kiberbiztonság, az adatvédelem és az internetes bűnözés vonatkozásában.

A föld minden országára kiterjedő egységes fellépés kialakítása természetesen utópisztikus vágyálom, ami sohasem fog megvalósulni. A kiberbűnözéshez hasonló és nagy számú sértettet érintő nemzetközi szintű jelenség a pénzmosás vagy az offshore paradicsomok működése.

Mindegyiknél megfigyelhetők párhuzamok:

- összességében káros folyamatok;
- az egyes szereplők hasznot realizálnak;[35]
- nemzetközi jogi eszközökkel nehezen kényszeríthető ki az együttműködés;
- azon államokon belül, amelyek kárvallottjai a jelenségnek, szintén vannak előnyt élvezők;
- évtizedek óta megoldatlan probléma.

Voltak az elmúlt évtizedekben olyan folyamatok, amelyek a nemzetközi közös fellépést egy-egy jelenség kapcsán előmozdították. Példaként említhető, hogy a 9.11. után minden olyan nyomozásban, amely pénzmosással volt kapcsolatba hozható – a megkeresések szerte a világban, de különösen az Egyesült Államok részéről –, addig soha nem látott gyorsasággal és alapossággal kaptak választ.

A számítógépes bűnözés joghatóságának jövője nem könnyű feladat,[36] de a bűnügyi nyomozások sikere nagyrészt nemcsak a meglévő joghatósági elvek és a számítógépes bűnözők elleni törvények megfelelő érvényesítésének biztosításától fog függeni, hanem az igazságszolgáltatási szervek technológiai tudásszintjén, az internetszolgáltatók bűnüldözési hatóságokkal való segítségnyújtási hajlandóságán, a nemzeti és nemzetközi szintű nyomozások összehangolásán, valamint azon, hogy a nemzeti bíróságok mennyire alkalmasak és elkötelezettek az elkövetők felderítésére a földrajzi helyzettől függetlenül.[37]

A határokon átnyúló bűnüldözési hozzáférés az adatokhoz és az elektronikus bizonyítékokhoz nagy kérdés, különösen a felhőalapú számítástechnika területén. Számos ország engedélyezi a határon átnyúló hozzáférést az adatokhoz közvetlenül vagy korlátozott körülmények között a szolgáltatókon keresztül.[38] Közös szabályokra és biztosítékokra van szükség.[39]

Megítélésünk szerint az adatok fizikai hollétének figyelembe vétele nélkül, az eljárás ökonómiai szempontjai szerint a nyomozást folytató hatóság onnan jogosult

---

[35] Az offshore területeknek jelentős bevételük származik az offshore tevékenységből, de példaként említhető az is, hogy a banktitok jelentősen elősegítette/elősegíti például a svájci bankrendszer működését is, amiből 10%-ot messze meghaladó GDP származik (természetesen a svájci bankrendszer nyeresége nem pénzmosásból származik/származott, de az erős banktitok a bűnelkövetőket is segíti/segítheti).

[36] Council of Europe (2010)

[37] Velasco (2017)

[38] Sok esetben azonban problémát okoz, hogy az 'A' országban folyó nyomozásban a 'B' országban bejegyzett cég által 'C' országban tárolt információ esetén a jogsegélykérelem teljesítése kinek a feladata, vagy joga.

[39] Council of Europe – Octopus Conference (2012)

az adatokat kérni, ahonnan azokat a leggyorsabban beszerezheti.[40] Egy tengerentúli szolgáltató tárhelyén tárolt és a magyar jogot sértő tartalommal összefüggésben kért adatokat a magyar hatóságok magyarországi telephely/leányvállalat/megbízott esetén magyar nyelven helyben kérhetik, de a képviselettel nem rendelkező tengerentúli vállalkozásokkal vagy ismeretlen üzemeltetőkkel összefüggésben problémát okoz, ha a válaszadást vagy az intézkedést elmulasztja, vagy megítélése szerint a Magyarországon vizsgált cselekmény saját joguk szerint nem bűncselekmény.[41] Ezekben az esetekben indokolt volna a rendbírsághoz és az elektronikus hírközlő hálózat útján közzétett[42] adatok ideiglenes hozzáférhetetlenné tételéhez hasonló eljárásban a megkeresett szerveket rábírni a kérések teljesítésére. Természetesen ez a kérdéskör az internetszolgáltatók, a tartalomszolgáltatók, a tartalomelőállítók felelősségi kérdéseinek minden vetületét nem hivatott megvilágítani – ehelyütt csak arra kívánjuk felhívni a figyelmet, hogy a nemzetközi egyezmények önmagukban nem elégségesek arra, hogy egyes szolgáltatók a saját elveik vagy üzleti érdekük ellenében segítsék a hazai nyomozásokat. Szükségesek olyan eljárások kidolgozása, amelyekkel az érintett feleket az államok büntetőjogi igényének elismerésére lehet kényszeríteni – jellemzően anyagi érdekeiken keresztül.

A igazságügyi hatóságok között egyfajta paradigmaváltás szükséges,[43] ami megköveteli, hogy új ötleteket, utakat és mechanizmusokat[44] fedezzenek fel a büntetőjogi jogszabályok érvényesítésére, és hogy a létező kölcsönös segítségnyújtási jogi mechanizmusok dinamikusabban és rugalmasabban működjenek. Azonban e tevékenység során is meg kell szüntetni a párhuzamosságokat. Az Európai Unió bűnüldöző hatóságai önállóan csak alacsony hatékonysággal tudnak kidolgozni jogi megoldásokat a nagy multinacionális cégekkel való együttműködésre, és szintén meg kell szüntetni a párhuzamosságokat a forenzikus eljárások fejlesztése területén.

Azt mondhatnánk, hogy a föld állami vezetőinek egységes és szigorú fellépéséhez – bármelyik előbb említett nemzetközi jogsértés esetében – „át kellene esnie a tű fokán", hogy erre vonatkozóan radikális lépéseket tegyenek. Ha azonban sem a terrorcselekmények, de még a gyermekpornográfia sem képes a nemzeti territoriális korlátokat ledönteni,[45] akkor tulajdonképpen bízzunk benne, hogy erre nem is fog sor kerülni.[46]

---

[40] Lehetséges területiségre vonatkozó további elvek: elkövető állampolgársága, sérelem bekövetkezésének állama, adatok fizikai létének állama.

[41] Az Egyesült Államoknak küldött megkeresések egy részében a szólásszabadság körébe esnek egyes cselekmények, például önkényuralmi jelképek.

[42] Például ha egy adott tárhelyszolgáltató nem szolgáltat információt egy megkeresésre, vagy nem törli a tárhelyről a jogsértő tartalmat, akkor a Magyarországról való elérhetőség korlátozása indokolt lehet még akkor is, ha ez más, jogszerűen működő vállalkozásokat is érint.

[43] Mint a hírszerző szervek között: korábban a „need to know" szemléletet felváltotta a „need to share" szemlélet.

[44] Példaként említhető az európai bűnügyi jogsegély működésének módosulása, az EUROPOL, az EUROJUST segítségével továbbított adatok, az egységes európai körözési rendszer, a nemzetközi közös nyomozócsoportok, a JIT-ek.

[45] Azaz az államok vagy nem adnak, vagy csak hosszadalmas folyamatokon (nemzetközi jogsegély) keresztül adnak nyomozást segítő információkat más államok nyomozó hatóságainak.

[46] A második világháború például alapot szolgáltatott arra, hogy a föld országai belássák, hogy saját hatalmukat csak addig gyakorolhatják, amíg az mások hatalmát nem sérti. Ez volt az egyik ok, amiért az ENSZ létrejött.

Felkészülés a jövőre

A bűnüldöző szerveknek a jövőre való felkészülés keretében számos intézkedést kell foganatosítaniuk jelenleg is, amelyeknek eredménye csak később fog realizálódni. Az egyik ilyen a készletező adatgyűjtés. A jövő fekete kalapos hackerei ma még scriptkiddiként bontogatják szárnyaikat. Minden elkövetőnek megvannak a rá jellemző jegyei, a modus operandik, amelyekből egy elkövetett bűncselekmény esetén a feltételezett elkövetőkre szűkíteni lehet. Ahogyan egy páncélszekrények feltörésére szakosodott elkövető az általa ismert és jól bevált eszközöket és metodikát használja visszatérően, úgy nyúl az eszközeihez a kibertérben működő elkövető is. Természetesen ezek a személyek is fejlődnek, de az információk jó irányvonalat adhatnak egy későbbi nyomozás során. A létrehozott adatbázisok pedig nem csak az elkövetett bűncselekményekre kell hogy vonatkozzanak. Az elkövetők előszeretettel térnek vissza korábban már használt nickneveikhez, e-mail-címükhöz,[47] és az ezekből létrehozott adatbázisok nagy segítséget nyújthatnak a bűnüldöző és a hírszerző szerveknek[48] is.

A következő előregondolást a bűnmegelőzés jelenti. Első körben itt azonnal a kibertérrel kapcsolatban álló szereplők széles körének tájékoztatására gondolunk – mindig a célcsoportra optimalizált üzenetekkel: a fiatalkorúakra vonatkozó szexuális kizsákmányolás az általuk használt csatornákon,[49] míg például az átutalásos csalások[50] esetében a vállalati szektort az általuk inkább használt felületeken[51] célszerű az információkkal ellátni. Itt a legköltséghatékonyabb megoldásokat a máshol kipróbált és haszonnal működtetett kampányok átvételével lehet megvalósítani. Fontos azonban, hogy ne csak az áldozattá válás megelőzését szolgálja a bűnmegelőzés. Sokkal nehezebben célba juttatható üzenet, de szintén nagyon fontos, hogy az elkövetővé válás megelőzésére is jelentős erőforrásokat dedikáljunk. Az elkövetővé válás egyszerű megvalósulását jól mutatja a szervezett bűnözéssel kapcsolatban már tárgyalt jelenség, amelyben az elkövetők a kiberbűncselekményt mint szolgáltatást nyújtják. Az egyes részcselekmények végrehajtása esetenként semmilyen kriminális magatartást nem igényel, mivel azok teljesen azonosak lehetnek a legális működéssel, például web-, adatbázis-, webshop-, programfejlesztés stb. Emellett komoly elvi kérdéseket vet fel, hogy a rosszindulatú céllal is használható informatikai ismeretek korlátlan hozzáférhetővé tétele mennyiben pozitív hatású össztársadalmi szinten.[52] Meg lehet-e valósítani, hogy az információk átadását csak bizonyos erkölcsi, etikai normák elplántálása után kapják meg az érdeklődők, ahogyan ezt jellemzően a hagyományos felsőoktatásban is teszik. Indokolt a feltárt hibák, a sérülékenységek közzétételét megelőzően az érintett szerep-

---

47 Ezek az adatbázisok hatalmas segítséget tudnak jelenteni például egy gyermekek online szexuális abúzusára szakosodott és felszámolt bűnözői csoport adataiból feltöltött Europol AWF-ekben, focal pointokban.

48 Természetesen amennyiben a hírszerző szervezetek számára készletező adatgyűjtéssel ezek az információk rendelkezésre állnak, úgy megfontolás tárgyává kell tenni a bűnüldöző szervek számára a hozzáférhetővé tételt.

49 ORFK Kommunikációs Szolgálat Nemzetközi kampány a gyermekek online szexuális kizsákmányolása ellen.

50 Europol (2016a)

51 Europol (2016b)

52 Bratus (2007) 2-2 – a hackerek jelentős része iskolai forrásból szerzi ismereteit.

lők tájékoztatása annak érdekében, hogy a sérelmeket elkerülhessék.[53] Az illegális célra történő információmegosztás korlátozása úgyis lehetetlen küldetés.[54]

Kijelenthető, hogy a kiberbiztonsági kockázatok és a költségek egyfajta adóként rakódnak a digitális növekedés hozadékaira. Az államoknak látniuk kell azt, hogy a biztonságos IT-infrastruktúra sokkal fontosabb annál, minthogy az egyes vállalkozások a kibertérben állami befolyásoktól és korlátoktól mentesen és ezáltal hatékonyabban tudjanak működni.[55] Az IT-vállalkozások számára a biztonsággal kapcsolatos kiadások a gépjármű kötelező felelősségbiztosításhoz hasonlók. Annak is meg kell fizetnie a biztosítási díjat, aki csak hétvégén és nagy vezetői rutinnal ül a kormány mögé. Ennél a biztosítási területnél az államok úgy döntöttek, hogy az ilyen jellegű feladatokat kiszervezik biztosítási társaságoknak – magánvállalkozásoknak –, mivel a piaci szabályok mellett hatékonyabb a működés ezen a területen is. Természetesen a biztosítási vállalkozásokat komoly állami kontroll alatt tartják, de a biztosítási szerződések megkötését és a díjak megfizetését akár az állam legitim erőszak szervezetei is kikényszerítik.

A kibertér szereplőinek a tevékenységük megkezdését megelőzően a tervezési fázisban szükséges a biztonsági elemekkel mint feladattal és költségtétellel számolniuk. Az állami szerepvállalás szükségessége itt is fontos szerepet játszik. E téren az építkezéssel húzhatunk párhuzamot: ha valaki egy házilag összeszerelhető kerti fészert vásárol, akkor ott nem követelik meg a jogszabályok, hogy minősített mérnök készítse el az engedélyezési tervet, amit aztán hatóságok hagynak jóvá. Egy többszintes lakóépület vagy híd esetén mindezek komoly követelményként szerepelnek. A kibertérben hasonlónak kell lennie a helyzetnek: ha valaki a kézműves termékeihez készít honlapot, amihez instant webáruházat telepít, ahhoz nem kell sem magas szintű szakértelem, sem hatósági engedélyeztetés. Egy nagyszámú vásárló személyes és fizetési adatait tartalmazó weboldal elindításához azonban szükséges volna előzetes engedélyezés.[56] A szabályozási igényt természetesen felismerték a döntéshozók olyan döntéseikkel, mint a GDPR.[57] Az adatvédelem azonban csak az egyik aspektusa a kibertérből származó fenyegetésnek. Kicsit olyan ez, mintha engednénk, hogy mindenki továbbra is olyan és akkora épületet építsen, amilyet csak akar – azzal a megkötéssel, hogy az értékeiket egy tűz- és vízálló stb. szekrényben kell tartaniuk. Ez a szabályozás viszont nem foglalkozik azzal, ha az „épület" összeomlik, vagy más javakban, más módon tesz kárt.

---

[53] Ez a „white hat hacker"-mentalitás az elmúlt időszakban teret hódít, hiszen a tudományos elismerést nem csorbítja az a tény, hogy a sérülékenységet időközben megszüntették.

[54] Például a Btk. 386. § (1) bekezdésébe ütköző: védelmet biztosító műszaki intézkedés kijátszása, a 424. § (1) bekezdésébe ütköző információs rendszer védelmét biztosító műszaki intézkedés kijátszása, bűncselekmények elkövetése nagyon nagy számban megvalósul az interneten.

[55] A vasút kialakulásakor is komoly problémát jelentettek a mozdonyok szikrája által felgyújtott mezőgazdasági területek, de az államoknak be kellett látniuk, hogy a vasút fejlesztéséhez nagyobb érdekek fűződnek, így a károkat szétterítették.

[56] A helyzet eddig olyan volt, mint az új világ meghódításakor. Mindenki olyan épületet rakott a kitűzött területére, amilyet tudott vagy akart. Az épületek azonban a kibertérben már egymást és másokat is veszélyeztetnek (persze a kibertérben korlátlan mennyiségben áll rendelkezésre a „terület").

[57] General Data Protection Regulation – Egységes Adatvédelmi Irányelv: www.eugdpr.org.

A túlszabályozás természetesen az internet egyik lényegét – a korlátlan szabadságot – ölné meg. Ha a tartalom létrehozását és az információ közzétételét anyagi javak és különféle erőforrások meglététől tennénk függővé, az rendkívül káros volna. A leglényegesebb választóvonal a terhek viselésére kötelezés eldöntéséhez az anyagi érdekeltség. A kibertérben anyagi előnyökre szert tevő, vagy az arra törekvő aktoroknak viselniük kellene a biztonsággal kapcsolatos költségeket, hiszen az internet ma már nem az adatok és információk elérésének hatékony útja, hanem „bombaüzlet".

Annak eldöntése összetett kérdés, hogy a különféle kötelezően bevezetendő biztonsági auditok és engedélyek a rendészeti szervek, az államigazgatási szervek, a köztestületek vagy a koncesszióban működő magánvállalkozások feladataivá vállnak.

A magyar rendészeti szervek – mint jellemzően más rendészeti szervek is – szenvednek a saját kötöttségeiktől, hagyományaiktól. A magyar rendőrség egyik nagy béklyója a tettes alapú bűnüldözési szemlélet.[58] A kibertérrel kapcsolatos jogsértésekkel összefüggésben is szükséges azt vizsgálni, hogy egy ügyféli bejelentés, feljelentés milyen célból született. Ezeknek az inputoknak sok esetben az a céljuk, hogy a jogsértő állapot szűnjön meg: a jogsértő (személyiségi, szellemi alkotáshoz fűződő) tartalom kerüljön le az internetről, a DDOS-támadás szűnjön meg, a zárolt/titkosított adatok váljanak elérhetővé, a csalás útján elvont javak kerüljenek vissza stb. A feljelentő – mint ügyfél – elégedettségét az szolgálja, ha az általa elérni kívánt cél minél gyorsabban és minél nagyobb arányban teljesül. Egy sorozatos aukciós csalás elkövetőjével szemben a nyomozó hatóságok elsődleges feladata a bűnösséget igazoló információk összegyűjtése mellett: a vagyoni reparáció érdekében a gyanúsítottól (vagy a tőle ingyenesen, vagy rosszhiszeműen szerző harmadik személyektől) a vagyon elvonása. Ha a bűnösség megállapításához (üzletszerűség, sorozatjelleg) szükséges bizonyítékokat összegyűjtik, és kiderül, hogy a gyanúsítottnak nincsen végrehajtás alá vonható vagyona, akkor azt követően minden további nyomozati cselekmény improduktív. A sértettek beidézése, tanúkénti kihallgatása, a további adatgyűjtések, megkeresések nem változtatnak érdemben a kiszabandó büntetés mértékén, mindössze azt eredményezik, hogy ez idő alatt a nyomozó hatóság erőforrásait elvonják más ügyek nyomozásától, az ügyben improduktív tevékenységre kényszerítik a beidézett tanúkat a nyomozati szakban és később a bírósági szakban is.

Ha egy elkövető az azonos sérülékenységet kihasználva, azonos eljárással számos weboldalt deface-el, és az okozott kár megtérítésére a nyomozás adatai szerint nincs reális lehetőség, akkor szintén felesleges költséges szakértői vizsgálatok folytatása, ha néhány eset bizonyításával a büntetőjogi felelősség tisztázható.

Természetesen ez a típusú szemlélet nemcsak a kibertérhez kapcsolódóan elkövetett bűncselekmények esetében jelent problémát, de az igazságszolgáltatás szereplőinek – különösen a nyomozó hatóságoknak és az ügyészségnek – fel kell készülniük

[58] Számos nagyon jól működő jogintézmény és eljárás működik, ami a sértetti reparációt, a felek megegyezését stb. célozzák, de ezek az eredmények nem elégségesek.

arra, hogy a számítástechnikai rendszerekhez kapcsolódóan a jövőben sokkal gyakoribbak lesznek a sorozatjellegű elkövetések.

A digitális forenzikus tudomány jövője

További, a bűnüldöző, az igazságszolgáltatási és a hírszerző szerveket érintő korlátként jelentkezik az e célra költhető anyagi javak mennyisége. Pedig az egy nyomozásban lefoglalt adatmennyiség már jelenleg is megközelíti a három terrabájt méretet,[59] ami még fokozódni fog. Ezen túlmenően a titkosítások használata, a felhő alapú tárolás további elterjedése, az IT-eszközök diverzifikálódása (például IoT-eszközök), a rohamos fejlesztések a mobileszközök piacán, a big data stb. egyre összetettebb és drágább adatelemző, nyomozást segítő szoftverek igénybevételét teszik szükségessé. A speciális célszoftverek egyik fontos célja, hogy a bizonyítékok hitelesített láncolatának megőrzése mellett lehetővé tegyék a nyomozó hatóságok számára, hogy az adatokból kigyűjtsék a bizonyítékokat olyan módon, hogy nagyon magas szintű informatikai ismeretekkel rendelkező munkatársakat és szakértőket kelljen foglalkoztatniuk. Ez azonban csak az ügyek kevésbé bonyolult szintjéig működik. A célszoftverek egyre bonyolultabbak, és képzett üzemeltető személyzetet igényelnek. A nyomozó hatóságoknak el kell dönteniük, hogy külső szakértőket vonnak be piaci alapon, vagy saját kapacitásokat fejlesztenek.[60] Ez utóbbi hosszú távon kifizetődőbb, de szintén jelentős erőforrásokat igényel.

A digitális forenzikus tudomány vitathatatlanul egyre több kérdéssel néz szembe. A Charlie Hebdo elleni terrortámadást követően az akkori angol miniszterelnök, David Cameron, majd az MI5 vezetője, Andrew Parker is olyan tartalmú kijelentéseket tett, hogy az egyéneknek egyre inkább rendelkezésére állnak olyan eszközök, amelyekkel kivonják magukat az állami ellenőrzések alól, ezáltal a digitális forenzikus vizsgálatok eredménytelenekké válnak, és a bűnüldöző szervek nem tudnak eredményesen működni.

A digitális forenzikus tudománynak fel kell készülnie többek között az elkövetők ellenlépéseire is. Edward Snowden szivárogtatását követően a hírszerző szervek komoly kihívásokkal szembesültek, amikor a korábbi eszközeik[61] eredményessége jelentősen visszaesett. A bűnüldöző szervek esetében ezt a hatást gyakorolja a *CSI-effektus,* ami a filmekből, sorozatokból ismereteket szerző bűnelkövetőknél jelentkezik.[62] Azok, akik tisztában vannak a cselekvéseik által elhagyott bizonyítékokkal, és rendelkeznek azzal a tudással, hogy hatékonyan elpusztítsák azokat, egy lépéssel közelebb kerülnek a „tökéletes bűncselekmény" típusú forgatókönyv elkövetéséhez.[63]

---

59 iSOCTA 2016 által vizsgált ügyek.
60 Simon (2016b) 87–105.
61 SIGINT, CYBINT, DNINT, MASINT eszközök.
62 Overill (2013) 81–89.
63 Graeme Horsman (2017)

Az adathordozó, adattároló eszközök árának csökkenése szintén megnehezíti a nyomozó hatóságok tevékenységét, mivel ezek fizikai megsemmisítése a bizonyítékok elenyészésével jár.

Hagyományos forenzikus vizsgálatok közé tartozik a vérvizsgálat, amelyben hatalmas lépést jelentett a szerológiai vizsgálathoz képest a DNS-vizsgálat. A digitális forenzikus vizsgálatokkal kapcsolatban az a gond, hogy ahány informatikai eszközt kell vizsgálni, az tulajdonképpen annyiféle élőlény vére. Ha pedig sok vizsgálat segítségével megismertük ennek az „élőlénynek a vérét", akkor azzal kell szembenéznünk, hogy egy szoftver update, vagy firmware-frissítés elavulttá tette ismereteinket, miközben az emberi vér vizsgálata ugyanazon elveken nyugszik hosszú ideje.

A kibertérhez kapcsolódó nyomozásoknak két fő iránya van. Az egyik az elkövetőhöz kapcsolódó informatikai eszközök, míg a másik a különféle szolgáltatóktól beszerezhető digitális bizonyítékok. Mindkét frontvonal folyamatosan változik. Az elkövetőnél található eszközök titkosítása esetén TOR net használatakor, vagy ha a szolgáltatóknál az adatvédelmi elvek[64] előtérbe kerülnek, akkor a bűnüldöző szervek nyilvánvalóan vesztésre állnak, de a különféle operatív intézkedések a hátrány ledolgozását nagyban segítik. A titkosszolgálati eszközök alkalmazása csak akkor tud hatékony lenni, ha sorozatjellegű bűncselekményeknél alkalmazzák, illetve tervezett vagy folyamatban lévő bűncselekmények nyomozását segítik. Ehhez azonban elengedhetetlenül szükséges az operatív pozíciók kiépítése a kibertérben, azaz proaktív rendészeti fellépés és stratégia szükséges.

A fejlődés irányai: az online és az offline titkosítások egyszerűvé, felhasználóbaráttá válása, az elkövetők tudatosságának emelkedése, az elkövetési módszerek diverzifikálódása, a gyártók támogatásának hiánya[65] mind a digitális forenzikus vizsgálatok eredményességének csökkenését fogják eredményezni. Egyre kevesebb bizonyíték beszerzésére nyílik lehetőség az eszközökből, ezért azokat máshol lesznek kénytelenek keresni a nyomozó hatóságok tagjai.

További tényezők

A bűnüldöző szervekkel szemben felmerülhetnek olyan új jelenségek is, amiket egyelőre nem is lehet prognosztizálni. Lehetséges, hogy teljesen új viselkedési szokások alakulnak ki, amelyek a fejlett társadalmak működését is erőteljesen befolyásolják.

2004 februárjában[66] aligha gondolta volna bárki, hogy a közösségi kapcsolattartásnak ennyire meghatározó eleme lesz a Facebook. Az emberek és a tudósok számára is komoly fejtörést okoz, hogy valójában mi is a sikerének titka? Az vitathatatlan, hogy a közösségi oldalaknak jelentős szerepük van a fiatalkorú felhasználók személyiségfej-

[64] Például a német alkotmánybírósági döntés alapján az ISP-nek tulajdonképpen nincs is előzményadat-tárolási kötelezettségük, így például a nagy szolgáltatók is csak hét napig tárolnak adatokat a kiosztott IP-címekről.

[65] Az Apple Inc. ügyvezetője, Tim Cook 2016. februári nyilatkozata a készülékeik titkosítási rendszeréről.

[66] 2004. február 4-én kezdte meg működését a Facebook.

lődésében.[67] Az emberben szunnyadó igény önmaga megmutatására, a nárcisztikus jellem és a fokozott exhibicionizmus a közösségi oldalak hatására fokozódik a felnövekvő nemzedék tagjainak személyiségében. Az ilyen közösségi oldalak megjelenésével szintén megnövekedett a védendő jogi tárgyak száma és tovább variálódtak a lehetséges elkövetési magatartások is. Nem zárható ki, hogy a Facebook sikeréhez vezető rejtett emberi tulajdonságokon kívül további, eddig ismeretlen dolgok törnek elő, és hoznak létre új jelenségeket a kibertérben.

Konklúzió

A bűnüldöző szervek önállóan nem képesek fellépni a kibertérből érkező kihívásokra, ezért együttműködés szükséges:

- más államok rendészeti szerveivel;
- nemzetközi szervezetekkel;
- piaci szereplőkkel, vállalkozásokkal;
- NGO-kkal.

A hatékony rendészeti működéshez szükséges a kapacitásfejlesztés az erők és az eszközök területén is, valamint az innovatív eljárások alkalmazása a rendészetben. A fejlesztések érinthetik az ügyfélkapcsolatokat, a belső folyamatok célszerűsítését, a legjobb gyakorlatok átvételét más rendészeti szervektől, vagy akár vállalkozásoktól is.

A hatékony bűnüldözés érdekében vizsgálni kell az inputokat és azokra a leghatékonyabb outputokat kell megkeresni, azaz törekedni kell az ügyfélelégedettségre.

Kapacitásfejlesztés szükséges a titkosszolgálatok és a rendészeti szervek elemző-értékelő egységeinél a szervezett bűnözői csoportok felderítése és a büntetőeljárás alá vonása érdekében.

A várható veszélyekre történő felkészülés (például készletező adatgyűjtés, bűnmegelőzés, IT-szektor vállalkozásainak bevonása stb.) nem fogja megszüntetni a bűnözést a kibertérben, de ez egy hosszú sakkjátszma, ahol a nyitó lépések nagyban meghatározzák a végeredményt.

IRODALOMJEGYZÉK

Broadhurst, Roderic – Grabosky, Peter (2005): *Cyber-crime: The Challenge in Asia.* Hong Kong, Hong Kong University Press, 347–360.

Broadhurst, Roderic – Grabosky, Peter (2014): Organizations and Cyber Crime: An analysis of the nature of group engaged in cybercrime. *International Juornal of Cyber Criminology,* Vol. 8.

Chabinsky, Steven R.: *The Cyber Threat: Who's Doing What to Whom?* Forrás: https://archives.fbi.gov/archives/news/speeches/the-cyber-threat-whos-doing-what-to-whom (2017. 07. 21.)

[67] Zella–Moeller (2017) 70–73.

Hathaway, Melissa – Demchak, Chris – Kerben, Jason – McArdle, Jennifer – Spidalieri, Francesca (2015): *Cyber readiness index 2.0*. Potomac Institute for Policy Studies. Forrás: www.potomacinstitute.org/images/CyberReadinessIndex2.0.pdf (2017. 07. 21.)
Horsman, Graeme (2017): Can we continue to effectively police digital crime? *Science & Justice.* Forrás: https://doi.org/10.1016/j.scijus.2017.06.001 (2017. 07. 21.)
Kshetri, Nir (2013): "Cybercrimes in the Former Soviet Union and Central and Eastern Europe: Current Status and Key Drivers". *Crime, Law and Social Change,* Vol. 60. No. 1. 39–65. Forrás: https://libres.uncg.edu/ir/uncg/listing.aspx?id=15333 (2017. 08. 03.)
Lusthaus, J. (2013): How organised is organised cyber crime? *Global Crime,* Vol. 14. No. 1. 52–60. Forrás: https://doi.org/10.1080/17440572.2012.759508 (2017. 07. 31.)
McGuire, M. (2012): *Organised Crime in the Digital Age.* John Grieve Centre for Policing and Security and BAE Systems Detica. London.
Morgenson, Gretchen (2000): S.E.C. Says Teenager Had After-School Hobby: Online Stock Fraud. *The New York Times.* Forrás: www.nytimes.com/2000/09/21/business/sec-says-teenager-had-after-school-hobby-online-stock-fraud.html (2017. 08. 03.)
Octopus Conference (2016): *Cooperation against Cybercrime – Key messages.* Forrás: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806-be360 (2017. 07. 31.)
ORFK Kommunikációs Szolgálat (2017): *Nemzetközi kampány a gyermekek online szexuális kizsákmányolása ellen.* Forrás: www.police.hu/hirek-es-informaciok/bunmegelozes/aktualis/nem-vagy-egyedul-0 (2017. 07. 31.)
Overill, Richard E. (2013): "The'inverse CSI effect': further evidence from e-crime data." *International Journal of Electronic Security and Digital Forensics,* Vol. 5. No. 2. 81–89.
Perl Raphael F. (2007): *Drug Trafficking and North Korea.* Forrás: www.fas.org/sgp/crs/row/RL32167.pdf (2017. 07. 13.)
Simon Béla (2016a): Hacktivism and its status in Hungary. *Magyar Rendészet,* 16. évf. 2. sz. 161–174.
Simon Béla (2016b): Az igazságügyi szakértés egyes kérdései a büntetőeljárásban, különös tekintettel az informatikai szakterületre. *Belügyi Szemle,* 64. évf. 7–8. sz. 87–105.
Sipress, Alan (2004): An Indonesian's Prison Memoir Takes Holy War Into Cyberspace. In: *Sign of New Threat, Militant Offers Tips on Credit Card Fraud*. Washington Post Foreign Service, A-19. Forrás: www.washingtonpost.com/wp-dyn/articles/A62095-2004Dec13.html (2017. 08. 03.)
Velasco, Cristos (2017): Cybercrime jurisdiction: past, present and future. *Science & Justice,* Vol. 57. Issue 6. 448–454. Forrás: www.scienceandjusticejournal.com/article/S1355-0306(17)30080-1/fulltext (2017. 07. 31.)
Wang Jingqiong (2010): *Internet policing hinges on transnational cyber crime.* Forrás: www.chinadaily.com.cn/china/2010-11/10/content_11525646.htm (2017. 08. 02.)
Zell, Anne L. – Moeller, Lisa (2017): Narcissism and "likes": Entitlement/Exploitativeness predicts both desire for and dissatisfaction with responses on Facebook. *Personality and Individual Differences,* Vol, 110. No. 1. 70–73.

Internetes források

Az Európai Parlament 2013. szeptember 12-i állásfoglalása az Európai Unió kiberbiztonsági stratégiájáról: nyílt, megbízható és biztonságos kibertér (2013/2606(RSP) Forrás: http://www.europarl.europa.eu/sides/getDoc.do?type=MOTION&reference=B7-2013-0386&language=EN (2017. 08. 03.)
Bhattacharjee, Yudhijit (2011): *How a Remote Town in Romania Has Become Cybercrime Central.* Forrás: www.wired.com/2011/01/ff_hackerville_romania/ (2017. 08. 02.)

Bratus, S. (2007): Hacker curriculum: How hackers learn networking. *IEEE Distributed Systems Online*, Vol. 8. No. 10. 2.
Conference Washington, D.C. Forrás: www.archives.fbi.gov/archives/news/speeches/the-cyber-threat-whos-doing-what-to-whom (2017. 05. 10.)
Council of Europe: *Cloud Computing and cybercrime investigations: Territoriality vs. the power of disposal? – Project on Cybercrime.* Forrás: https://rm.coe.int/16802fa3df (2017. 07. 31.)
Council of Europe: Octopus Conference: *Cooperation against Cybercrime – Key messages.* 2012. Forrás: www.coe.int/en/web/cybercrime/octopus-interface-2012 és www.rm.coe.int/16802f23ae (2017. 07. 31.)
Décary-Hétu, David (2012): *The social network of hackers.* Forrás: www.tandfonline.com/doi/abs/10.1080/17440572.2012.702523 (2017. 08. 10.)
Digitális egységes piac. Forrás: https://ec.europa.eu/commission/priorities/digital-single-market_hu (2017. 08. 12.)
European Policy Centre: *The economic impact of a European Digital Single Market.* Forrás: www.epc.eu/dsm/2/Study_by_Copenhagen.pdf (2017. 08. 12.)
Europol (2016a). Forrás: www.europol.europa.eu/activities-services/public-awareness-and-prevention-guides/infographic-fraud-scams-targeting-employees (2017. 08. 03.)
Europol (2016b). Forrás:www.twitter.com/europol/status/748855809141010433 (2017. 08. 03.)
ec.europa.eu/digital-single-market/ (2017. 08. 11.)
ec.europa.eu/digital-single-market/en/%20european-cloud-initiative (2017. 08. 11.)
Horváth Attila – Erdősi Péter Máté – Kiss Ferenc (2016): *Az informatikai sérülékenységek gazdasági összefüggései – A kiberbiztonság megjelenése a makro- és mikroelemzésekben.* Forrás: http://infota.org/wp-content/uploads/2016/11/dr.horvath_attila_%E2%80%93_erdosi_peter_mate_%E2%80%93_dr.kiss_ferenc_az_informatikai_serulekenysegek_gazdasagi_osszefuggesei_%E2%80%93__a_kiberbiztonsag_megjelenese_a_makro%E2%80%93_es_mikroelemzesekben.pdf (2017. 08. 10.)

Jogforrás

1139/2013. (III.21.) Korm. határozat

ABSTRACT

Digital Challenges in Law Enforcement

SIMON Béla

This study aims to give an overview of the challenges that the law enforcement organisations are facing due to the new legislations and possible misuse generated by the informational revolution. The study is based on comparing the international literature review and Hungarian practices. According to the findings of the article, among others, it is crucial to improve the international cooperation based on task sharing approach; integrate best practices; the offensive intelligence work; the extensive crime prevention activity and promoting information security for affected parties.

Keywords: *law enforcement, cybercrime, vision, challenge*