Magyar Rendészet 2018/1. 161–168.

A kiberbűnözés aktuális trendjei[1]

SIMON Béla[2]

Az előadás és a kapcsolódó cikk tárgya A kiberbűnözés elleni fellépés egyes kérdései a rendészeti szerveknél *címmel indult kutatás egy szeletét mutatja be. Szükséges a bűncselekmények és a bűnüldözés jelenlegi helyzetének feltárása és a legjobb nemzetközi gyakorlatok felkutatása. Cél a magyar rendészeti szervek számára olyan javaslatok kialakítása, amelyek a belföldi és a nemzetközi együttműködés, az oktatás, a kutatás-fejlesztés, a jogalkotás, és a jogalkalmazás hatékonyságnövekedését eredményezhetik. A teljes vizsgálatból az előadás célja a kutatási részeredmények ismertetése.*

Kulcsszavak: *kiberbűnözés, kiberbűncselekmények, számítógépes bűnözés*

Mint általában egy kutatás megkezdésekor – úgy esetünkben is – fontos körülhatárolni a vizsgált területet. Egyrészt elkülöníteni más hasonló kutatásoktól, másrészt számba venni mindazon kérdésköröket, amelyekre a választ keressük. A cél, hogy az olvasó se kevesebbet, se többet ne kapjon, mint amire ígéretet adtunk a cím alapján. Így tehát első kérdésként felmerül, hogy mit is érthetünk a kiberbűnözés alatt?

Kiberbűnözés általános definíciója szerint – amit lehet a számítástechnikai bűnözés egyfajta szinonimájaként is értelmezni – a kibertérrel összefüggésben elkövetett bűncselekmények összessége. Ebben az értelemben viszont szinte minden bűncselekmény kapcsolódik a kibertérhez, mert alig van olyan büntető törvénykönyvi tényállás, amelyet ne lehetne infokommunikációs eszközzel elkövetni.

A bűnözés, kriminalitás nem jogi fogalom, hanem egy társadalmi tömegjelenség. Számos kriminológiai és más fogalommal leírható,[3] de esetünkben azon deviáns viselkedések összefoglaló megnevezése, amely egy adott helyen, meghatározott időn belül elkövetett összes bűncselekményt írja le. A bűncselekményi kategória már sokkal egyértelműbben körülírható, hiszen Büntető törvénykönyvünk[4] leglényegesebb feladata ennek meghatározása. Törvényünk értelmében bűncselekmény az a szándékosan vagy – ha e törvény a gondatlan elkövetést is büntetni rendeli – gondatlanságból elkövetett cselekmény, amely veszélyes a társadalomra, és amelyre e törvény büntetés kiszabását rendeli. Itt ismét elidőzhetünk egy gondolat erejéig, hiszen a kibertérhez

---

[1] A Nemzeti Közszolgálati Egyetem Doktorandusz Önkormányzatának A Magyar Tudomány Ünnepe rendezvénysorozat részeként 2017. november 22-én megrendezett, „A Haza Szolgálatában" című doktoranduszkonferenciáján elhangzott előadás szerkesztett változata.

[2] SIMON Béla dr., r. őrnagy, tanársegéd, NKE Rendészettudományi Kar, Bűnüldözési és Gazdaságvédelmi Tanszék
Béla SIMON dr., police major, 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

[3] Kiss–Parti (2016) 491–517.

[4] 2012. évi C. törvény 4.§ (1) bekezdés.

kapcsolódó bűncselekmények esetén, amelyek a szabályozási területüket illetően nagyon frissnek számítanak.[5] Ennek köszönhetően messze nem egyértelmű annak meghatározása sem, hogy e téren mit minősítünk társadalomra veszélyesnek. Egy emberi testet sértő magatartás egyértelműen skálázható. A könnyű testi sértést el nem érő sérelem például csak valamilyen többlet körülmény esetén válhat bűncselekménnyé (tettleges becsületsértés, garázdaság). A sérelem súlyosságával párhuzamosan pedig lehetőség van büntetések pontos meghatározására.

A kibertérben elkövetett jogsértések azonban nem ennyire egyértelműen skálázhatók és a jogalkotó szándékának pontos letükrözése sem egyértelmű a jogalkalmazók számára.

Az 2017-es év jelentős közérdeklődésre számot tartó ügyében egy 18 éves személy észlelte, hogy egy közlekedési vállalat online jegyértékesítési rendszerében jelentős biztonsági rés található. Ezt először a közlekedési vállalat irányába közölte, majd nem sokkal később nyilvánossá tette az interneten. A rendszert fejlesztő vállalkozás feljelentést tett, majd az ügyben a Készenléti Rendőrség Nemzeti Nyomozó Iroda információs rendszer vagy adat megsértése vétség elkövetésének megalapozott gyanúja miatt indított nyomozást. Utóbb az eljárást a társadalomra való veszélyesség hiánya miatt megszüntették.

Hasonlóan az etikus hackerek működésével összefüggő jogértelmezési problémát okozott a 2017-es év végén egy postaforgalmi vállalkozás online rendszerének sérülékenysége.

Ezek a folyamatok egyfajta precedens jellegű jogértelmezést adtak a jogalkalmazók számára, de nem nyugtatták meg az IT-biztonsággal, szoftverfejlesztéssel, üzemeltetéssel foglalkozó szakembereket, hiszen egyfajta üzenetként szólnak a társadalom széles rétegei irányába, hogy büntetlenül lehet biztonsági réseket keresni és tulajdonképpen szinte minden hacker nevezheti magát etikus hackernek, ha érdekei úgy kívánják.

A gondolat lezárásaként a tanulmány szerzője indokoltnak látja a büntetőjogi kérdés végleges rendezését vagy jogalkotói (törvényi, rendeleti úton), vagy jogalkalmazói (bírósági határozat, ügyészségi állásfoglalás stb.) oldalról.

Az élet azonban nem áll meg és a jogalkotás hosszadalmasabb megoldásaira várva a piaci szereplők is lépéseket tettek. Felgyorsultak a *„bug bounty"*[6] programok, illetve a *„responsible disclosure agreement"*[7] módszer bevezetésével kapcsolatos folyamatok.

Talán a leglényegesebb azonban, hogy a Kormányzati Eseménykezelő Központ (GovCERT) megnyitotta honlapján az „Anonim bejelentés etikus hekkereknek" felületet. A csak ide érkező bejelentések valóban kizárttá teszik, hogy sérülékenységet felismerő személy a sérülékenységre vonatkozó információk közreadásával bűnös ma-

[5] Összevetve a büntetőjog által érintett klasszikus területekkel: emberiesség elleni, háborús, élet, a testi épség és az egészség elleni bűncselekmények stb.

[6] Szoftverfejlesztők, üzemeltetők előre deklarált szerződéses szabályrendszer mellett engedik a sérülékenységek kontrollált feltárását, akár pénzbeli jutalmazásért cserébe is.

[7] Egy közzé tett felhívás/megállapodás alapján tipikusan nulladik napi sérülékenységet/hibát lehet a tulajdonos és üzemeltető felé kommunikálni privát, és lehetőleg titkosított csatornán. Csak abban az esetben lehet a hibát nyilvánossá tenni, ha a cég hosszú idő után sem reagál a megkeresésre.

gatartást kövessen el. Természetesen, ha ezzel párhuzamosan azt más módon is publikussá teszi, úgy a károkozási szándék valószínűsíthető. Úgyszintén büntetőjogi felelősséget vet fel, ha sérülékenység kutatását végző személy az információs rendszerbe az információs rendszer védelmét biztosító technikai intézkedés megsértésével vagy kijátszásával jogosulatlanul belép, az információs rendszer működését jogosulatlanul akadályozza, vagy az információs rendszerben lévő adatot jogosulatlanul megváltoztatja, törli vagy hozzáférhetetlenné teszi.[8]

Az eddig leírtakból látható, hogy a bűnözés pontos meghatározása e területen akadályokba ütközik, de ha elvonatkoztatunk attól a problémától, hogy a kibertérhez kapcsolódó bűncselekmények megállapíthatóságának kritériuma képlékeny, és csak azt vesszük figyelembe, hogy mi az, amit Magyarország statisztikai rendszere e bűncselekményi körhöz regisztrált, akkor azt gondolhatnánk, hogy könnyen tudunk trendvonalakat felmutatni az elmúlt időszakra.

A címben foglalt „kiberbűnözés" kifejezés egy másik oldalával is érdemes foglalkoznunk.

Bár a kibertérre vonatkozóan találunk jogszabályi körülírást,[9] de annak egységes fogalmi leírása nem megoldott. Mennyiben része e kibertér fizikai összetevőinek a hálózati eszközök, szoftverek összessége? Mit értünk a kibertér virtuális összetevői alatt? Részét képezik-e az internethez nem kapcsolódó hálózatok? Számos kérdés merül fel, amelynek kimunkálása nem e tanulmány célja.[10]

Esetünkben a kiberteret érintő bűncselekményeket a gyakorlati megfontolásokat alkalmazó szervezetek – különösen az Europol – gyakorlata alapján tarjuk célszerűen besorolhatónak.

Az Europol az általa lényegesnek tartott bűncselekményeket, nemzetközi bűnügyi együttműködést segítő eljárásokat elemző projektekben (*analysis project* – AP / korábban *analysis work file* – AWF) kezeli. Itt a vagyonvisszaszerzéstől az egyes kábítószer fajtákon át számos projekt él – jelenleg 28 darab. Egy ilyen elemző projektnek külön „kezelő személyzete" van, akik a beérkező adatokat elemzik, értékelik és az eredményeiket az érintett hatóságok támogatására megküldik.

Az Europol Kiberbűnözési Kompetencia Központja (EC3) három ilyen AP-t kezel:

- *AP Cyborg* – támogatja az EU-ban a kritikus számítógépes és hálózati infrastruktúrákat érintő számítógépes bűnözés elleni vizsgálatokat.
- *AP Terminal* – a nemzetközi elektronikus és online fizetési csalások felderítésén dolgoznak.

---

[8] Btk. 423. § – információs rendszer vagy adat megsértése.

[9] Magyarország Nemzeti Kiberbiztonsági Stratégiájáról szóló 1139/2013. (III. 21.) Korm. határozat 1.3. pontja: „A kibertér globálisan összekapcsolt, decentralizált, egyre növekvő elektronikus információs rendszerek, valamint ezen rendszereken keresztül adatok és információk formájában megjelenő társadalmi és gazdasági folyamatok együttesét jelenti."

[10] Bővebben: Munk (2017)

- *AP Twins* – elemzési projekt támogatja a gyermekek szexuális kizsákmányolásával és visszaélésekkel járó bűnözés minden formájának megelőzését és leküzdését.[11]

Az Europol más szervei által kiberbűnözéshez kapcsolódóan kezelt AP-i:

- *AP Copy* – amely támogatja a szellemi tulajdonjogokkal kapcsolatos bűncselekmények megelőzését és az azok elleni küzdelmet.
- *AP Check-the-Web*[12] – a nyílt internetforrások figyelemmel kísérése és értékelése az iszlamista terrorizmus ellen.
- *AP Apate* – különféle csalási cselekményekkel szembeni fellépés (jellemzően online csalások).[13]

Tehát azt jelenthetjük ki, hogy ezekhez a kiberbűncselekményi kategóriákhoz kapcsolódóan egyértelműen besorolhatók a magyar bűnügyi statisztika egyes tényállásai, amelyekből következtetéseket vonhatunk le. Sajnos azonban ez nem így van. A Bűnügyi Statisztikai Rendszer[14] adataiból nem különíthetők el a kérdéses kategóriák.

A vizsgált tényállások és azok statisztikai adatai 2013. évtől kezdődően:

Gyermekpornográfia

2013 – 5225 (4892 Nógrád megye)
2014 – 142
2015 – 334
2016 – 272
2017 (január–szeptember) – 1277 (1153 Heves megye)

Az esetszám nagy mozgásokat mutat, de a legnagyobb kiugrásokat 2013-ban és 2017-ben egy-egy ügycsoport eredményezte.

Bankkártyához kapcsolódó visszaélések

- *Készpénz-helyettesítő fizetési eszköz hamisításának elősegítése*

2013 – 3
2014 – 1
2015 – 3
2016 – 3
2017 (január–szeptember) – 1

Statisztikailag nem jelentős tényállás.

[11] Az elmúlt időszakban nagy számban valósítottak meg olyan módon gyermekbántalmazásokat, hogy annak végrehajtását élő videoközvetítést megtekintő személy utasításait követve hajtják végre. A végrehajtás helyszíne jellemzően a föld nagyon elmaradott régióira jellemző, míg a megrendelő tipikusan fejlett országok lakója.

[12] Bővebben lásd: register.consilium.europa.eu/doc/srv?l=EN&f=ST%208457%202007%20REV%202 (2017. 09. 07.)

[13] Simon (2018a)

[14] bsr.bm.hu/SitePages/Nyitolap.aspx (2017. 09. 07.)

- *Készpénz-helyettesítő fizetési eszközzel visszaélés*
  2013 – 5804
  2014 – 1186
  2015 – 870
  2016 – 23 064 (Pest megyében 22 687)
  2017 (január–szeptember) – 257

  Jelentős esetszám csökkenés figyelhető meg, amit csak egy 2016. évi kiugrás tör meg.

- *Készpénz-helyettesítő fizetési eszköz hamisítása*
  2013 – 65
  2014 – 202
  2015 – 130
  2016 – 425
  2017 (január–szeptember) – 32

- *Információs rendszer felhasználásával elkövetett csalás (5) bek. – nincs elkülönítés a statisztikában*
  2013 – 250
  2014 – 1398
  2015 – 2176
  2016 – 3409
  2017 – (január–szeptember) – 3149

A BSR-rendszerben nincs lehetőség az Információs rendszer felhasználásával elkövetett csalás (5) bekezdésében rögzített minősítést (elektronikus készpénz-helyettesítő fizetési eszköz felhasználásával) külön kezelni a többi tényállástól. Így összességében kijelenthetjük, hogy e tényállás erőteljes emelkedést mutat az elmúlt években – akár a bankkártyával, akár más módon történő elkövetésnél is.

Klasszikus kiberbűncselekmények

- *Személyes adattal visszaélés*
  2013 – 2635
  2014 – 1059
  2015 – 975
  2016 – 487
  2017 (január–szeptember) – 224

  Nagyon jelentős csökkenés látható, de a tényállást offline környezetben is meg lehet valósítani.

- *A nemzeti adatvagyon körébe tartozó állami nyilvántartás elleni bűncselekmény*
  Hatálybalépése óta nem valósult meg.

- *Jogosulatlan titkos információgyűjtés vagy adatszerzés*
  2 esetben valósult meg 2013. óta, így trendekről nem beszélhetünk.

- *Terrorcselekmény*
  2013 óta 17 darab terrorcselekmény regisztrálása történt, de ezekben a statisztikai rendszerből nem olvasható ki, hogy mely esetekben volt érintve a kibertér.

- *Közérdekű üzem működésének megzavarása*
  2013 – 73
  2014 – 66
  2015 – 34
  2016 – 40
  2017 (január–szeptember) – 24

Csökkenő tendenciát mutat, de az informatikai infrastruktúrák elkülönítése nem megoldható a statisztikai leválogatásban.

- *Tiltott adatszerzés*
  2013 – 20
  2014 – 31
  2015 – 23
  2016 – 20
  2017 (január–szeptember) – 11

Viszonylag alacsony esetszám, ami egy sávban mozog.

- *Információs rendszer vagy adat megsértése*
  2013 – 823
  2014 – 565
  2015 – 520
  2016 – 702
  2017 (január–szeptember) – 356

Itt sem látható dinamikus emelkedés.

- *Információs rendszer védelmét biztosító technikai intézkedés kijátszása*
  2013 – 580
  2014 – 31
  2015 – 15
  2016 – 44
  2017 (január–szeptember) – 4

A 2013-as évet követő időszakban egy alacsony sávban marad az esetszám.

A csalás jellegű magatartások esetében a statisztika 2017. év májusát megelőző időszakra vonatkozóan nem tartalmaz pontos információkat – azok együtt szerepelnek az összes csalással.

Annak további vizsgálata indokolt, hogy a hatalmas statisztikai kiugrásokat okozó ügyekben hogy volt lehetséges, hogy olykor az éves országos összes esetszámot sokszorosan meghaladó bűncselekményszám jelent meg. Ezek nyilvánvalóan nem a társadalmi viszonyokat követő és bemutató statisztikai eredmények, sokkal inkább a statisztikai rendszer hibás működése valószínűsíthető mögötte.

A bűnügyi statisztikai adatokból tehát alig láthatunk hatalmas dinamikát e bűncselekményi kategóriában, azonban az egyes globális esetek – még ha nem is érintik Magyarországot – alkalmasak arra, hogy az állampolgárok biztonságérzetét erodálják.

E statisztikai probléma nemcsak Magyarországon jelentkezik, azt Európa számos országában észlelte a GENVAL jelentés.[15]

Ennek orvoslására 2017. év májusában az ENYÜBS-ben[16] bevezetésre került egy plusz kérdés: az adott bűncselekményt online környezetben követték el? Ennek éves eredményeit még nem ismerjük, de az eddigi gyakorlat azt mutatja, hogy az összesítés sok fals pozitív elemet is tartalmazni fog.[17]

A híradásokon túlmenően azonban más forrásból is az lehet a feltételezésünk, hogy a kiberbűncselekmények fenyegetése jelentős. Egyes szakértői vélemények szerint a kiberbűnözés globális és éves szinten 1200 milliárd USD kárt okozott 2017-ben.[18] E kijelentéseket jellemzően olyan személyek teszik, akiknek érdekében áll a problémák démonizálása. Azonban nyilvánvalóan egy információbiztonsággal foglalkozó vállalkozástól sem várható el, hogy megnyugtató nyilatkozatot tegyenek a várható trendekre vonatkozóan.

Az elmúlt időszakban inkább az jellemző, hogy e nyilatkozatok gyakrabban jelennek meg a médiafigyelem homlokterében.

Természetesen számos szakértői elemzést sorolhatnánk fel arra vonatkozóan, hogy milyen kártékony kódok, elkövetési magatartások várhatóak a 2018. évben, de ezek közép- és hosszú távú stratégiák, operatív programok megalkotására nem alkalmasak.

Összegzés

Kijelenthető, hogy nincsen olyan objektív forrás, amely az elmúlt évek magyarországi kiberbűnözési folyamatait leírná. A honi bűnüldöző szervek vezetőinek hosszú távú stratégiáiban vizionálniuk kell, hogy a kiberbűnözés miként fog alakulni 4-5 év múlva, mivel a szükséges szakképzett munkatársak felvételéhez meghatározott keretszámok kialakítása, a felvételi eljárás, majd a képzés időtartama ezt teszi szükségessé.

---

15 Simon, (2018b)

16 Egységes Nyomozóhatósági és Ügyészségi Bűnügyi Statisztika

17 A kitöltők olyan esetben is online környezetben elkövetést jelölnek, amikor például csak az elkövetéshez gyűjtött információt az elkövető az internetről szerezte.

18 Frész (2017)

Ilyen megbízható prognózisokat felállítani nem lehetséges, az azonban evidens, hogy nemcsak a kiberbűncselekmények nyomozásánál jutnak egyre nagyobb jelentőséghez a digitális és IT forenzikus ismeretek, hanem majd minden bűncselekményi körnél.

IRODALOMJEGYZÉK

Bányász Péter (2017): Kiberbűnözés és közösségi média. *Nemzetbiztonsági Szemle*, 5. évf. 4. sz. 55–74.
Frész Ferenc (2017): Kiberháborús játékok. ITBN 2017. konferenciaelőadás. Forrás: www.youtube.com/watch?v=M2Nakh-Emqo&list=PLSOYQEF9YFBIsO8SqRZOEuQsi_MBhSRHC&index=22 (2017. 09. 07.)
Munk Sándor (2017): A kibertér fogalmának egyes, az egységes értelmezést biztosító kérdései. Kézirat.
Simon Béla, dr. (2018a): Rendészeti szervek együttműködése a kiberbűnözés ellen. *Nemzetbiztonsági Szemle,* megjelenés alatt.
Simon, Béla, dr. (2018b): Az EU rendészeti szerveinek együttműködése a kiberbűnözés ellen. *Nemzetbiztonsági Szemle,* megjelenés alatt.
Kiss Tibor – Parti Katalin (2016): Informatikai bűnözés In Borbíró Andrea – Gönczöl Katalin – Kerezsi Klára – Lévay Miklós szerk.: *Kriminológia.* Budapest, Wolters Kluwer. 491–517.
Kiss Tibor (2014): Gyűlölet-bűncselekmények és szélsőséges csoportok az információs társadalomban. In Prazsák Gergő szerk.: *Nemzeti szempont.* Budapest, Apeiron Kiadó. 71–92.

Internetes források

register.consilium.europa.eu/doc/srv?l=EN&f=ST%208457%202007%20REV%202 (2017. 09. 07.)
https://bsr.bm.hu/SitePages/Nyitolap.aspx (2017. 09. 07.)

ABSTRACT

Current Trends in Cybercrime

SIMON Béla

The presentation and the relating article present a section of research called "Issues of Anti-cyber Crime at Law Enforcement Agencies". In order to reach this aim, it is necessary to assess the current status of crimes and relating law enforcement activities. At the same time, an investigation is being conducted to identify the best international practices. Considering these sources, proposals are expected from the Hungarian law enforcement agencies that may result to be efficient in domestic and international cooperation, education, research and development, legislation and law enforcement. The purpose of the lecture is to describe the partial results of the research.

Keywords: *law enforcement, cybercrime*