GYARAKI RÉKA

A KIBERBŰNCSELEKMÉNYEK MEGJELENÉSE ÉS HELYZETE NAPJAINKBAN

– Különös tekintettel a szervezett bűnözéssel kapcsolatos kérdésekre

Bevezetés

A szervezett bűnözés fejlődéséhez a kibertér és a különböző informatikai eszközök kiváló lehetőséget kínálnak, mert ezek segítségével a szervezett bűnözői csoportok nemcsak az egymás közötti kommunikációt képesek egyszerűbben megoldani, hanem a névtelenségük megőrzését is könnyebben tudják biztosítani. A következőkben a szervezett bűnözés és a kiberbűncselekmények közös kapcsolódási pontjait vizsgálom, kiemelt figyelmet fordítva a kibertérben elkövetett bűncselekményekre.

1. A szervezett bűnözés fogalma

A szervezett bűnözés általános fogalma alatt értjük többek között a következőket: a szervezett bűnözői csoport működésében résztvevő személyek profit elérésre törekednek, magas fokú szervezettség jellemzi, az elkövetők legtöbbször magasan képzett szakembereket vesznek igénybe az elkövetéskor, a szervezeten belül a munkavégzés tekintetében a centralizáltság jellemző és a szervezett tagjai sok esetben nem vagy csak a szükséges mértékben ismerik egymást. A szervezett bűnözők a céljaik elérése és a jogellenes cselekményeik elérése érdekében nem riadnak vissza a zsarolástól, a fenyegetéstől, a korrupciótól és a testi sértéstől vagy sok esetben az emberöléstől.

A szervezetten elkövetett bűncselekményeket a mély konspiráció, a tervezés, az időben elhúzódó végrehajtás jellemez. A szervezett bűnözés legfontosabb ismérvei a következők: monopolhelyzet létrehozása, extraprofit elérésére törekvés, a legális gazdasági struktúrák működtetése, valamint hierarchikus felépítés[1].

[1] Nyeste Péter: A nemzetbiztonsági célú stratégiai felderítés/elhárítás és a bűnügyi célú stratégiai hírszerzés összehasonlítása, kiemelten a szervezett bűnözés elleni fellépés területén. Felderítő szemle XII. évfolyam 1. szám 2013. 111. o.

A szervezett bűnözéssel szorosan összefüggnek a gazdasági és az egyéb gazdasági jellegű bűncselekmények, mivel az illegális tevékenységből származó jövedelmet valamilyen legális, pénzmozgást feltételező (például alapítványi vagy gazdasági társaságok) mögé rejtve, tisztára mosva, próbálják meg leplezni. Ezáltal biztosítva, hogy a hatóságok ne észleljék, vagy ne találják meg a bűnös eredetű bevételeket. A pénzmosás esetében szükséges, tehát egy „pénz mosoda" létrehozása, amelynek felderítése és illegális tevékenységének bizonyítása a hatóságokat kihívások elé állítja.

A fogalom szükséges és gyakori elemei mellett megjelennek esetleges jellemzők is, mint a paramilitaritás (katonai jellegű), erős függőségi rendszer, amelynél előfordulhat politikai vagy ideológiai indíttatás, az elkövetéshez kapcsolódó holdudvar megjelenése.

A szervezett bűnözést a 2012. évi C. törvény a Büntető Törvénykönyv (a továbbiakban: Btk.) bűnszervezetként határozza meg, és aszerint olyan, a három vagy több személyből álló, hosszabb időre szervezett, összehangoltan működő csoport, amelynek célja az öt évi vagy ezt meghaladó szabadságvesztessel bűntetendő szándékos bűncselekmények elkövetése.[2] Ugyanakkor a jogszabály nem áll meg ennél a fogalomnál, hiszen szabályozza még a bűnszövetséget és a csoportos elkövetést is mint többes elkövetési formát.

Érdemes megemlíteni még, hogy önálló deliktumként került értékelésre a bűnszervezetben részvétel (Btk. 321. §), mely szerint, aki bűncselekmény bűnszervezetben történő elkövetésére felhív, ajánlkozik, vállalkozik, a közös elkövetésben megállapodik, vagy az elkövetés elősegítése céljából az ehhez szükséges vagy ezt könnyít feltételeket biztosítja, illetve a bűnszervezet tevékenységét egyéb módon támogatja, bűntett miatt egy évtől öt évig terjedő szabadságvesztéssel bűntetendő.

Jelen írásban felvázolt fogalmak és a tényállás részletes elemzésétől eltekintek, mert ezekkel egy másik fejezet foglalkozik részletesen.[3]

A fentiek fényében azt gondolom, hogy nem túlzás azt állítani, hogy azokat a sztereotípiákat már átléphetjük, hogy a szervezett bűnözés tipikusan csak a fegyver- vagy kábítószerkereskedelemmel, prostitúcióval vagy a migrációval[4] összefüggő deliktumokkal azonosítható, hiszen a technika fejlődését és a virtuális tér előnyös

[2] 2012. évi C. törvény 459.§ (1) bekezdés

[3] Lásd bővebben: Tóth Mihály: Bűnszövetség, bűnszervezet. Complex Kiadó Kft. Budapest, 2009.; Nyitrai Endre: A szervezett bűnözés elleni küzdelem büntetőjogi és kriminalisztikai eszközei. PhD értekezés. Pécs, 2017. 23-41. o.; valamint Gellér Balázs – Ambrus István: A magyar büntetőjog általános tanai I. ELTE Eötvös Kiadó. Budapest, 2017. 410-425. o.; Tóth Mihály – Kőhalmi László: A szervezett bűnözés. In: Borbíró Andrea – Gönczöl Katalin – Kerezsi Klára – Lévay Miklós: Kriminológia. Wolters Kluwer Kft. Budapest, 2016. 603-626. o.

[4] Lásd bővebben: Hautzinger Zoltán: Idegen a büntetőjogban. AndAnn, Pécs, 2016.

oldalát a bűnelkövetők is maximálisan kihasználják, így már nemcsak mint elkövetési „eszközt", hanem az elkövetés helyeként és módszereként is a digitális világot választják.

Az informatikai rendszerek már lehetővé tették a XXI. században, hogy a különböző bűnszervezetek összekapcsolódjanak és kommunikáljanak úgy, hogy az anonimitásukat megőrizzék egymás előtt, az elkövetés gyorsabban és sok esetben precízebben történjen meg.

Jelen írásban a következőkre helyezem a hangsúlyt:

– Milyen bűncselekményeket követnek el meg a kibertérben a szervezett bűnözés körében?
– Milyen előnyeit használják ki az egyes szervezett bűnözői körök az információs rendszereknek és eszközöknek?
– Mire irányulhat a bűnszervezeteknek a figyelme a virtuális tér által kínált lehetőségeknél?
– Milyen kihívásokkal kell szembenéznie a hatóságoknak a fentiek fényében a bűncselekmények felderítésénél?

1.1. A modernkori szervezett bűnözés

A szervezett bűnözésről még mindig sok embernek az olasz maffia vagy éppen a dél-amerikai drogkereskedők jutnak az eszükben, így akár Al-Capone vagy Pablo Escobar.

A szervezett bűnözésnél jellemző a folyamatos megújulás, a kockázatvállalásnak a legminimálisabb szintre történő csökkentése, amelyek akár a szigorú életviteli, viselkedési szabályok megalkotását, betartását kívánják meg.

A szervezett bűnözői csoportok megváltoztak, sok esetben nem is ismerik már egymást személyesen, és egyre inkább az általuk elkövetett hagyományos, fizikai világhoz kapcsolható deliktumokat felváltja a kibertérben vagy az informatikai eszközök felhasználásával elkövetett bűncselekmények köre. A technika segítségével már az sem szükséges, hogy földrajzilag egy helyen legyenek, találkozzanak, egymásról a nick nevükön – esetleg e-mail címükön – kívül bármit is tudjanak. Sőt minél kevesebbet tudnak a bűnszervezet tagjai egymásról, annál nagyobb az esély, hogy a nyomozó hatóságok előtt nem lesznek mindannyian ismertek, ezáltal a felderítés ellehetetlenül vagy nehézkessé válik.

1.2. SOCTA

Először is szükséges beszélni az Európai Multidiszciplináris Platformról (European Multidisciplinary Platform against Criminal Threats – EMPACT), mely programot a bűnügyi fenyegetések elleni fellépések érdekében hoztak létre.

Az EMPACT Program az Európai Unió hatálya alatt, a nemzetközi szervezett bűnözés elleni hatékony fellépés sürgetése érdekében létrehozott olyan feladatrendszer, amelynek keretében számos eltérő prioritáshoz (így például a kiberbűncselekmények, az emberkereskedelem, a kábítószerkereskedelem és előállítás stb.) kapcsolódóan közös munkát végeznek az erre kijelölt EMPACT nemzeti szakértők az Europol-lal együtt.

A számítógépes bűnözés[5], valamint az internetes bűnözés elleni harc prioritást élvez, és ezeken belül kiemelten a bankkártya bűnözéssel, a kibertámadásokkal és gyermekek online szexuális kizsákmányolással szemben van szükség a közös fellépésre.

E szakterületet uniós szinten az Europol képviseli, melynek egyik fontos feladata, hogy elemezze és értékelje az Európai Uniót érő súlyos és szervezett bűnözési fenyegetettségét, melyről jelentést készít évente (Serious and Organized Threat Assessment – SOCTA).

A SOCTA jelentés készítésének célja a bűnelemzés (crime intelligence analysis), továbbá a bűnügyi és más, bűnügyileg érdemleges információk közötti összefüggés felismerése, azonosítása és azok értékelése, mely elősegítheti a rendszeres, célirányos és összehangolt tevékenységet.

A jelentés foglalkozik a tagállamonként azonosított bűnszervezetek számával, jellemző tevékenységi területeikkel, az általános bűnügyi helyzetre vonatkozó adatokkal, ami egyben a statisztikai szemlélet erősödésére utal. Világosan megfogalmazza a bűnszervezetek, illetve a súlyos és szervezett bűnözés képviselte fenyegetettség jellegét és a fellépés érdekében szükséges prioritásokat, melyek szakpolitikai elfogadása (legalizálása) is megtörtént.[6]

Az Európai Unió Tanácsa 2010-ben elfogadta az EU szakpolitikai ciklusát, amelyben a 2014-2017-es ciklus egy „árucikk" szerű megközelítést tartalmaz. Ebben a ciklusban 9 prioritási területre bővült a bűncselekmények kategória szerinti osztályozása a Tanács 8453/2/2013-es dokumentuma alapján:

[5] Bővebben erről: Parti Katalin – Kiss Anna: A számítástechnikai bűnözésről akkor és most. In: Bárd Petra – Hack Péter – Holé Katalin: Pusztai László emlékére. OKRI-ELTE ÁJK. Budapest, 2014. 297-310. o.

[6] A speciális felkészültséget igénylő elemzés kialakulása egy új rendvédelmi szakterületnek a létrejöttét eredményezte: a bűnelemzését. A taktikai és stratégiai bűnelemzés gyakorlata szakértői tevékenységként az 1970-es években jelent meg az Interpol révén. E szervezet közvetítésével az 1980-as években a magyar kriminalisztika részéve is vált a bűnelemzés. Lásd Urszán József: A szervezett bűnözés fenyegetettség értékelésének jelentősége az Európai Unióban. In: Gaál Gyula – Hautzinger Zoltán: Tanulmányok „A változó rendészet aktuális kihívásai" című tudományos konferenciáról. Pécsi Tudományos Határőr Közlemények. Pécs, 2013. 434-435. o.

1. Az illegális migráció elősegítésének a megakadályozása, különös tekintettel az uniós országok belépési pontjain, a főútvonalakon, valamint a forrás országokban,
2. a munkaerő szexuális célú emberkereskedelem visszaszorítása a legjelentősebb forrás országokból,
3. az egészségre, a biztonságra, az élelmiszerbiztonságra vonatkozó hamis termékek gyártásának és kereskedelmének megakadályozása,
4. jövedéki csalás és az MTIC281 („Eltűnő kereskedő a közösségen belül" jellegű csalás),
5. a kábítószerkereskedelem csökkentése,
6. a pénzügyi szolgáltatók elleni csalások csökkentése,
7. a számítógépes bűnözés visszaszorítása, elsősorban a bankkártya-csalás, a gyermekek online szexuális kereskedelme, valamint az infrastruktúrát és az informatikai hálózatot érő kibertámadások területén,
8. az illegális fegyverkereskedelem,
9. a bevándorló bűnözői csoportok által elkövetett tulajdon elleni bűncselekményekkel szembeni fellépés.

Az Európa Tanács Szervezett Bűnözés Büntetőjogi és Kriminológiai Kérdéseivel Foglalkozó Szakértői Csoportja (PC–S–CO) megfogalmazta azokat a követelményeket, amelyek fennállása esetén megállapítást nyerhet a bűnszervezet léte.

A Szakértői csoport által kötelező kritériumok szükségesek:

a) három vagy több személy együttműködése;
b) hosszú távú vagy határozatlan időre szóló együttműködés;
c) súlyos bűncselekmények gyanúja vagy azok elkövetése;
d) anyagi haszonszerzési és/vagy hatalmi pozícióba kerülési cél.

Az esetleges kritériumok:

a) minden egyes résztvevőnek meghatározott feladata vagy szerepe van;
b) valamely belső fegyelmi vagy ellenőrzési forma használata;
c) megfélemlítés céljából erőszak vagy egyéb eszközök alkalmazása;
d) befolyás kiterjesztése a politikusokra, a médiára, a közigazgatásra, a rendészeti szervekre, az igazságszolgáltatásra, illetve a gazdasági élet szereplőire a korrupció vagy bármely más üzleti módszer alkalmazásával;
e) kereskedelmi vagy üzleti jellegű struktúrák alkalmazása;
f) részvétel a pénzmosásban;
g) nemzetközi szintű működés.

Ahhoz, hogy a csoport bűnszervezetnek minősüljön a szakértői csoport szerint a kötelező kritériumoknak együttesen és legalább kettő esetlegesnek kell megvalósulnia.[7]

A szervezett bűnözői csoportok beazonosításához egyaránt nemzetbiztonsági és rendőrségi tevékenységre szükség van, azonban a bomlasztásuk és felszámolásuk már kizárólag rendőrségi feladat.[8]

A 2000-ben elfogadott Palermói egyezmény[9], amelyet az Egyesült Nemzetek Szervezete épp a szervezett bűnözésben, a szervezett bűnözői csoportok felszámolásában, az ilyen jellegű bűncselekmények észlelése kapcsán fogadott el az ahhoz csatlakozó államok feladatainak meghatározása céljából.

Az Egyezményben a részes államok többek között vállalják a korrupcióval és a pénzmosással összefüggő cselekmények bűncselekménnyé nyilvánítását, valamint a részes államok hatóságai közötti – így a nyomozó hatóság, ügyészség, valamint a hatóságok és pénzintézetek közötti effajta bűncselekményekre vonatkozó együttműködést, egymás felé küldött jelzéseket, az elemző értékelő munka végrehajtásának és eredményeinek egymás közötti megosztását.

Amennyiben az Egyezmény elfogadásának időpontját megnézzük, úgy érthető, hogy a szervezett bűnözést és a kiberbűncselekményeket még összefüggésében nem említi, ugyanakkor a következőkben érthető lesz, hogy ez a hiányosság nem jelenti azt, hogy ez a két fogalom nincs összefüggésben egymással.

2. Szervezetten elkövetett bűncselekmények a kibertérben

A kiberbűncselekmény általános fogalma alatt az informatikai eszközök és/vagy rendszerek segítségével, vagy az informatikai eszközök és hálózatok ellen elkövetett bűncselekmények értendők, amelyek céljai lehetnek a rendszerben tárolt adatok megszerzése, a jogosultak számára hozzáférhetetlenné tétele, továbbá az elektronikus rendszerbe vetett bizalommal visszaélés.[10] A kiberbűncselekmények további

[7] KIRIPOVSZKY Csaba: Az emberkereskedelem és a szervezett bűnözés kapcsolata a prostitúció tükrében. Pécsi Határőr Tudományos Közlemények VIII. Különszám. Pécs, 2007. 79–80. o

[8] NYESTE: i.m. 111. o.

[9] Magyarországon az Egyesült Nemzetek keretében, Palermóban, 2000. december 14-én létrejött, a nemzetközi szervezett bűnözés elleni Egyezmény kihirdetéséről szóló 2006. évi CI. törvénnyel került bevezetésre.

[10] SZATHMÁRY Zoltán a következőképpen határozza meg a számítástechnikai bűncselekmény fogalmát: „az a bűncselekmény, mely a számítástechnikai rendszerek zavartalan működését, a bennük ke-

célja lehet az anyagi haszonszerzés[11], vagy az elektronikusan tárolt adatok illetéktelen felhasználása, vagy az azzal történő visszaélés.

Ezen típusú bűncselekmény elkövetési helye maga a kibertér[12] vagy, bár a virtuális térhez kapcsolódik az elkövetés – de leginkább az elektronikus információs rendszer felhasználásán van a hangsúly, de a fizikai térben történik maga a bűncselekmény.

Amikor kizárólag a virtuális térben történik az elkövetés, mint az információs rendszerbe történő jogosulatlan behatolás, kifürkészés esetén, az elkövető személyének megállapítása nehezebb vagy sokszor lehetetlen, hiszen a hatóságoknak és az érintett szervezeteknek elsődleges feladata – a tudomásra jutást követően – az okozott károk csökkentése és elhárítása, azonban a nyomozást és a felderítést nehezíti – sőt ellehetetlenítheti – az anonimitás és magasfokú látencia.

Azokban az esetekben, amikor az elkövetők leginkább az információs rendszert az elkövetés eszközeként használják – mint például a hirdetéses csalásoknál, zaklatásnál, gyermekpornográfiánál – akkor a szervezett bűnözői körök sokkal több nyomot hagynak maguk után, így a hatóságok megfelelő felkészülése, tudatossága esetén az elkövető megismerése és felderítése is eredményesebb lesz.

A következő bűncselekmények tekintetében jellemző a szervezett bűnelkövetés a kibertérben[13]:

- Pénzmosás (Btk. 399.§) megvalósulásának esetei online környezetben.
- Tiltott szerek forgalmazása, azzal való kereskedés:
- Kábítószer-kereskedelem (Btk. 176.§).
- Kábítószer készítésének elősegítése (Btk. 182.§).
- Kábítószer-prekurzorral visszaélés (Btk. 183.§).
- Új pszichoaktív anyaggal visszaélés (Btk. 184.§).
- Teljesítményfokozó szerrel visszaélés (Btk. 185.§).
- Egészségügyi termék hamisítása (Btk. 186.§).
- Piramisjáték szervezése (Btk. 412.§)

zelt adatok megbízhatóságához, hitelességéhez, titokban maradásához, illetőleg az ezekhez fűződő egyéb (nemzetbiztonsági, államigazgatási, gazdasági vagy személyes érdeket) sért, vagy veszélyeztet." Szathmáry Zoltán: A számítástechnikai bűncselekmények. Magyar Jog 2011/3. 162-163. o.

[11] Nagy Zoltán András: A számítógéppel megvalósítható vagyoni jogsértésekről. Bűnügyi Műhelytanulmányok 1992/1. 26. o.

[12] A kibertér szabályozásával kapcsolatos kérdéseket lásd bővebben Dornfeld László: A kibertér főbb nemzetközi és nemzeti szabályozásai. In: Pintér István (szerk.): Műhelymunkák: A virtuális tér geopolitikája. 43-88. o.

[13] Nagy Zoltán András NKE RTK Kiberbűnözés Elleni Tanszékének vezetője által felsorolt kibertérben elkövethető bűncselekmények

– Rossz minőségű termék forgalomba hozatala (Btk. 415.§)
– Fogyasztók megtévesztése (Btk. 417.§)
– Tiltott szerencsejáték szervezése (Btk. 360.§) és más bűncselekmények.
– Támadások kormányzati szerverek ellen.
– Támadások kritikus infrastruktúrák ellen.
– Támadások a pénzügyi szféra ellen (pl. DDoS-támadások, ransomwareek, APT támadások, MITM-, WITM-támadások, booster/streamer visszaélések stb.)
– Készpénz-helyettesítő fizetési eszközök elleni támadások:
– Készpénz-helyettesítő fizetési eszköz hamisítása (Btk. 392.§).
– Készpénz-helyettesítő fizetési eszközzel visszaélés (Btk. 393.§).
– Készpénz-helyettesítő fizetési eszköz hamisításának elősegítése (Btk. 394.§)

2.1. A szervezett bűnözés és a kiberbűncselekmények

A szervezett bűncselekmények és a kibertérben elkövetett bűncselekmények kapcsolódási pontjait a következő szempontok alapján csoportosítottam:

– Kibertérben elkövetett olyan bűncselekmények, amelyeknek a tárgya az információs rendszer;
– Az informatikai eszközök felhasználásával elkövetett bűncselekmények;
– Az informatikai eszközök mint kommunikációs eszközök.

A kibertér kifejezést szükségesnek éreztem kihangsúlyozni, hiszen, ahogy fentebb is említettem, amennyiben maga a számítógép mint tárgy ellen követnek el fizikai támadást, így lopást, rongálást, az még önmagában nem kiberbűncselekmény. Amennyiben maga az információs rendszer ellen, vagy az abban tárolt adattal összefüggésben követnek el bűncselekményt, akkor az már kiberbűncselekménynek (kibertámadásnak) minősül. Ilyen támadási formák az információs rendszer megsértése – vagyis meghekkelése, a rendszer ellen irányuló, zsarolóvírusok, malware-ek, a túlterheléses támadások (DDoS támadás)[14], vagy egy honlap megrongálása (defacement) is.

A felsorolt támadások hátterében a károkozás, a megfélemlítés, a zsarolás és mindennek előtt a pénzszerzés áll.

[14] Lásd erről: Mezei Kitti: A DDoS-támadások büntetőjogi szabályozása az Egyesült Államokban, Európában és Magyarországon. Pro Futuro 2018/1. 66-83. o.

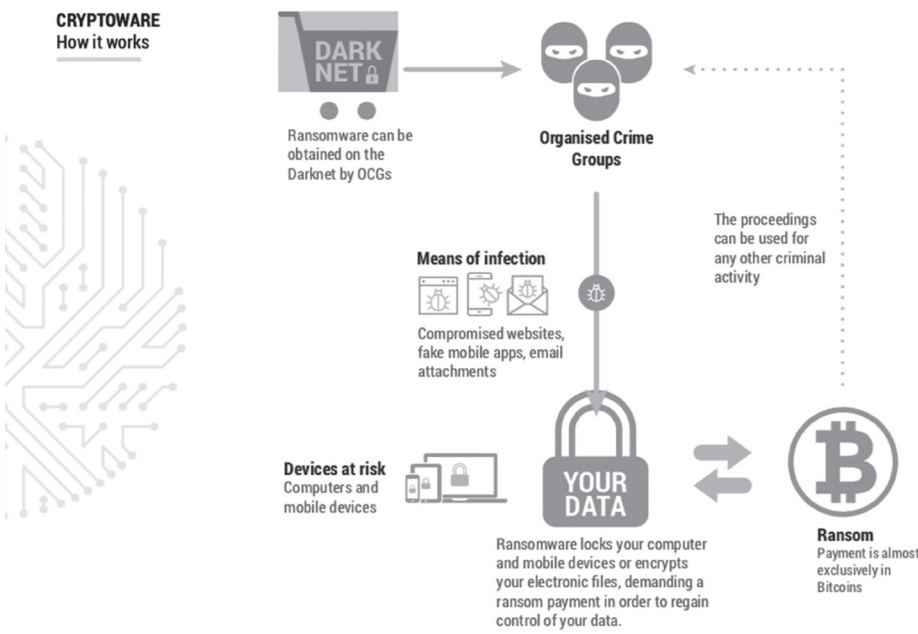
2.2. A szervezett bűnözés megjelenése és ismérvei a kibertérben

A bűnszervezetek egyre szélesebb körben használják ki az internet és az informatikai eszközök nyújtotta lehetőségeket a különféle jogellenes cselekményeik elrejtésére.

A szervezett bűnözői csoportok által elkövetett bűncselekményeknek az egyik piactereként szolgál az ún. Darknet, amely egy speciális Tor Browser nevű böngészővel használható, amelynek egyik előnye, hogy a magas fokú anonimitása révén megnehezíti a felhasználók azonosítását.

A Darkneten, azaz az internet sötét oldalán, a bűnözők képesek rejtve maradni, ugyanakkor az illegális termékeket vagy szolgáltatásokat, mint egy piacon kínálni (pl. bérgyilkos szolgáltatását vehetik igénybe, fegyvereket vagy kábítószert szerezhetnek be).

A SOCTA 2017-es jelentése alapján, a 2017. januárig több, mint 1,7 millió közvetlen felhasználója volt a Tor hálózatnak.



1. ábra: Az ún. cryptoware működése[15]

[15] Forrás: https://www.europol.europa.eu/activities-services/main-reports/european-union-serious-and-organised-crime-threat-assessment-2017 [2018.05.02.]

2.2.1. Gyermekpornográfia

Az egyik legnagyobb problémát jelentő és egyben a bűnszervezetek számára a legnagyobb bevételt generáló bűncselekmény a gyermekpornográfia[16] (Btk. 204.§), amelyet az online térben történő elkövetés mellett a fizikai térben is megvalósuló gyermekek szexuális kizsákmányolása, vagy abúzusa jelenti.[17] Az elkövetők az internet lehetőségeit maximálisan kihasználva, osztják meg egymás között a 18. életévüket be nem töltött személyekről készült szexuális tartalmú vagy a szexuális vágy felkeltésére alkalmas olyan felvételeket, amelyek elérése – az adott oldalról a letöltése, hozzáférhetővé tétele – vagy pénzért, vagy hasonló felvételekért cserébe valósul meg. Az elkövetők legtöbbször az érdeklődési területükből kifolyólag magányosak, ugyanakkor az internetnek köszönhetően egymással kommunikálnak könnyedén, valamint az általuk elkövetett bűncselekményekből származó felvételeket egymással megosztják (pl. a szexuális kényszerítés, szexuális visszaélés vagy vérfertőzés révén a saját közvetlen családtag segítségével járulnak ehhez hozzá). Például ezeket a képeket, videókat saját zárt csoportjukban online, vagy ritkább esetben adathordozón továbbítják egymásnak, azaz a Btk. 204. §-ban meghatározott elkövetési magatartásban meghatározottak alapján felvételre veszik és megosztják.

A gyermekpornográfia bűncselekményével kapcsolatban a szervezett bűnözői körök nemcsak az ilyen beállítottságú emberek személyét ismerik meg, hanem azok személyes adatait (bankkártya adatait) is, amely által zsarolhatóvá válnak, vagy az adataikkal visszaéléseket, esetleg egyéb bűncselekményt követnek el, ezáltal az elkövetők sértettek is lesznek, amelyet ritkán hoznak a hatóság tudomására, félve a rájuk váró szankcióktól.[18]

2.2.2. Tiltott szerek forgalmazása

A felsorolt bűncselekményekkel kapcsolatban a tiltott szerek forgalmazása és az ezekkel való kereskedés a kibertérben történhet az online fekete piactereken, ahol leggyakrabban a kábítószerek, illetve egyéb tiltott szerek adásvétele zajlik. A Darkneten megvalósuló illegális üzleti tevékenység kifejezetten azoknál a szolgáltatásoknak és termékek értékesítésének nyújt kiváló teret, amelyekhez a törvény által tilalmazott magatartások kapcsolódnak.

[16] Lásd bővebben Parti Katalin: Gyermekpornográfia az interneten. Bíbor Kiadó. Budapest, 2009.

[17] Dornfeld László – Mezei Kitti: Az online gyermekpornográfia elleni küzdelem aktuális kérdései. Infokommunikáció és jog 2017/68. 33. o.

[18] Mezei Kitti – Nagy Zoltán András: The organised criminal phenomenon on the Internet. Journal of Eastern-European Criminal Law 2016/2. 145. o.

Ugyanakkor nemcsak a rejtett piacterek használhatók e célból, hanem sok esetben akár a közösségi oldalakon vagy az egyszerű keresőmotor által elérhető weboldalakon is megtalálhatóak ezek a termékek – akár internetes hirdetésekben, ún. bannerekben elhelyezett reklámok révén –, és megvásárolhatóak (pl. azon gyógyszereket, amelyek hatóanyaguk révén akár kábítószernek, vagy illegális teljesítményfokozónak minősülnek és épp emiatt az adott országban legálisan nem kerülhet forgalomba).

Ugyanígy kedvez az internetes vásárlás a hamis vagy rossz minőségű gyógyászati termékek értékesítésének vagy a pszichoaktív anyagok készítésének (pl. az alkotóelemeinek, összetevőjének árusítása révén, az azzal történő kereskedéssel, valamint az elkészítéshez szükséges további instrukciók nyilvánossá tételének megosztásával).

2.2.3. Piramisjáték szervezése

A piramisjátékok szervezése virágkorát éli továbbra is napjainkban. A számítógépes technológia tömeges elterjedése előtt is már jelent volt e tradicionális deliktum[19], azonban új dimenzióba lépett az internet és a közösségi médiák térhódításával, mert a korábban ismerősök által történő beszervezés és hálózatépítés átalakult. Most már nem szükséges a bemutatókra és csapatépítésekre járni, de még az sem szükséges, hogy valaki a saját házába fogadja a látszólag MLM rendszert kínáló szervezőt. Elég, ha e-mailen vagy bármilyen más elektronikus eszközön – mobiltelefonon keresztül szóban megvalósuló egyetértő kifejezéssel – keresztül történő szerződéskötés, amely joghatás kiváltására alkalmas[20].

A piramisjáték szervezéséhez az internet és az általa kínált lehetőségek kifejezetten alkalmasak arra, hogy kevés szervezéssel, elegendő számítógép felhasználói ismerettel nagyobb tömeghez jusson el, mivel egy jól megtervezett honlap – ami lehet akár egy külföldi oldalnak a tükörmásolata – egy bankszámlaszám, egy létező vagy épp nem létező, de akár egy külföldön működő offshore cég létrehozásával tökéletesen kivitelezhető a piramisjáték. A szervezett bűnözői csoportok számára is kedvező a piramisjáték szervezése az online térben, hiszen az anonimitás biztosított – akár egymás előtt is –, az egymás közötti kapcsolattartásukat valamint a további tagok beszervezését egyszerűsíti, ráadásul egy jól megszerkesztett weboldalnak köszönhetően a bizalom elnyerése is egyszerűbbé vált minél több embernél. Mindez lehetővé teszi a számukra, hogy hosszabb időn keresztül folytassák a tevékenységüket, valamint, ha a nyomozóhatóságok eljárást indítanának, akkor azt követően

[19] Nagy Zoltán András: Kiberbűncselekmények, kiberháború, kiberterrorizmus – avagy ébresztő Magyarország! Magyar Jog 2016/1. 20-21. o.

[20] 2013. évi V. törvény a Polgári Törvénykönyv (Ptk.) 6:85.§ (1) bekezdés

más név alatt tovább folytathatják újabb áldozatokat gyűjtve. A játék szervezőjeként kizárólag a játék kitalálói, elindítói, fenntartói büntetendők. A beszervezett játékosok, akik a játék jellegéből fakadóan további játékosokat szerveznek be e bűncselekményben sem tettesnek, sem társtettesnek nem minősülnek.[21]

2.2.4. A rossz minőségű termék forgalomba hozatala

A rossz minőségű termék forgalomba hozatalának a fogyasztók érdekében végzett folyamatos ellenőrzések elkerülése miatt tökéletes színtere az internet. A Btk. értelmében rossz minőségű a termék, ha nem felel meg az EU ránk nézve közvetlenül kötelező jogi normában rögzített követelményeinek, valamint rendeltetésszerűen nem használható, vagy használhatósága jelentősen csökkent.[22]

A különböző aukciós és kirívóan olcsó termékeket árusító oldalakon, a közösségi oldalakon történő értékesítés esetén az eladó és a vevő közvetlenül lép úgy kapcsolatba – sokszor a külföldről történő rendelés esetén –, hogy azok a korábban Fogyasztóvédelmi Főfelügyelőségnek nevezett, mai elnevezése a Nemzeti Fogyasztóvédelmi Hatóság által végzett ellenőrzésekor – akár az elektronikus kereskedelmi tevékenység ellenőrzés során – sem juthat a rögtön a tudomására.

A leginkább az Európai Unión kívülről érkezett termékek esetében figyelhető meg – sokszor a jelentősen alacsonyabb árak miatt – hogy a magyar fogyasztók szívesebben rendelnek, még a hosszabb szállítási időbe is belenyugodva, a különböző kínai vagy ázsiai weboldalakról. Ezeken az oldalakon általában a következő – akár köztudottan hamis – termékeket rendelik: kozmetikai termékeket, ruhaneműket, ékszereket és játékokat, esetleg hamis csúcstechnológiai eszközöket. Ugyanez vonatkozik az adott országokon belül működő bűnszervezetekre, amelyek nemcsak, hogy rossz minőségű terméket „forgalmaznak", hanem a nagyobb bevétel érdekében még azokat silány minőségű anyagokkal keverik a nagyobb, de adózatlan bevételük érdekében.

2.2.5. Tiltott szerencsejáték szervezése

A virtuális hálózatokon is elterjedtek a különféle online szerencsejátékok.[23] Szerencsejátéknak minősül az 1991. évi XXXIV. törvény alapján[24] minden olyan játék,

[21] Molnár Gábor: Gazdasági bűncselekmények. HVG-ORAC Lap- és Könyvkiadó Kft. Budapest, 2009. 246. o.

[22] Tóth Mihály: XLII. fejezet – A fogyasztók érdekeit és a gazdasági verseny tisztaságát sértő bűncselekmények. In: Tóth Mihály – Nagy Zoltán: Magyar büntetőjog – Különös Rész. Osiris Kiadó. Budapest, 2014. 570. o.

[23] Nagy Zoltán András: A szervezett bűnözői jelenségek a számítógépes hálózatokon. Belügyi Szemle 2012/6. 114-115. o.

[24] 1991. évi XXXIV. törvény a szerencsejáték szervezéséről szóló törvény 1.§ (1) bekezdése

amelyben a játékos pénz fizetése, vagy vagyoni érték nyújtása fejében, meghatározott feltételek fennállása vagy bekövetkezése esetén pénznyereményre, vagy más vagyoni értékű nyereményre válik jogosulttá. A nyerés vagy a vesztés kizárólag, vagy túlnyomórészt a véletlentől függ.

Ahhoz, hogy legálisan lehessen szerencsejátékot szervezni a magyar törvények által előírt feltételeknek – így az adóhatóság felé történő bejelentési kötelezettség teljesítésével – meg kell felelniük, amelyeknek az ellenőrzése a hatóságok feladata. Ez az ellenőrzés – így a résztvevők életkora, a szervezők neve, a nyereményjátékban a nyeremény összegének kifizetése, egyáltalán a játék tisztasága a kibertérben nehezen vagy egyáltalán nem ellenőrizhető. A szervezett bűnöző csoportok felismerték és kihasználják ezt a lehetőséget, így a rendszerességet, a nagy nyilvánosságot megteremtve képesek a szerencsejáték lebonyolítására úgy, hogy abból adómentes bevételük származzon hosszabb időn keresztül. Amennyiben meg akarják teremteni a „tisztaság" látszatát, úgy a pénzmosást is megvalósítják tevékenységük során. Ennek egyik klasszikus formája lehet, amikor az internetes szerencsejáték során a szervezetthez tartozó személyek megvásárolják a játék részvétel jogát, majd attól elállva egy megadott – más személy – bankszámlaszámára utaltatják a pénzt, ahonnan aztán téves utalás címen visszakövetelik az összeget.

Arra is volt már példa, hogy az online pókerjáték során kártyázó hackereknek sikerült belenézni a játékosok lapjaiba. Ennek során a kiberbűnözőknek csak a trójai vírussal megfertőzött játékosokat kellett megtalálniuk[25], akiknek virtuális kártyalapjait módosították vagy épp a saját virtuális lapjaikat osztották, úgy hogy minél nagyobb összeget nyerjenek aztán a játékosoktól.

2.2.6. Készpénz-helyettesítő fizetési eszközökkel való visszaélések[26]

Az e-kereskedelem elterjedése, a különböző interneten keresztül történő fizetési lehetőségek (pl. szolgáltatók felé a közüzemi számlák kiegyenlítése, banki átutalások netbankon keresztül, PayPal vásárlás, bankkártyás vásárlások stb.) lehetővé tették, hogy a szervezett bűnözői körök a felhasználók bankszámlaszámát, a bankkártya adatait – sok esetben kérik a háromjegyű biztonsági kód megadását – megismerjék. Ez történhet akár egy trójai vírus segítségével, az eredeti honlap lemásolásával vagy

[25] ESET WeLiveSecurity blog

[26] Lásd bővebben a szabályozást: Mezei Kitti – Tóth Dávid: A készpénz-helyettesítő fizetési eszközökkel kapcsolatos bűncselekmények. In: Hollán Miklós-Barabás A. Tünde (szerk.): A negyedik magyar büntetőkódex: régi és újabb vitakérdések. MTA Társadalomtudományi Kutatóközpont. Budapest, 2017. 297-308. o

akár csalással (pl. telefonos csalás[27] vagy hamis banki e-mail elküldésével), majd az adatok felhasználásával, leemelhetik a bankszámlán lévő pénzösszeget, hamis bankkártyát készíthetnek vagy csekket állíthatnak ki maguknak.

Ugyanígy említést érdemelnek a kelet-európai vagy afrikai bűnözők által elkövetett ATM-en (Automated Teller Machine) vagy POS (Point of Sale-Terminals) terminálon keresztül történő bankkártya hamisítások is, amelyek esetében az áldozatok bankkártya adatait megszerzik, a számlájukon lévő pénzt a saját vagy más bankszámlájára utalják és azt később leemelik, vagy esetleg a hatóságok munkájának megnehezítése érdekében kriptovalutát, bitcoint vásárolnak belőle, amellyel aztán az arra alkalmas helyen felhasználnak, fizetnek vele.

Gyakoriak még az ATM-ek vírussal történő megfertőzése, amelynek során közvetlenül is hozzájuthatnak a számlán lévő pénzhez és adatokhoz. Ilyen esetben az elkövetők – vagyis, akik a vírusokat megírják –, nem feltétlenül lépnek ki a fizikai térben, hanem a káros programot a Darkneten vagy egy sima online piacon értékesítik, esetleg épp felkérésre írják meg, majd azt követően arra alkalmas személynek azt egy adathordozón, jellemzően pendrive-on átadják, annak leírásával együtt, hogy hogyan kell az ATM-et szétszedni és azon belül hol található annak behelyezésére alkalmas USB port, és milyen módon lehet a vírust telepíteni. Ezek a leírások általában egy átlag felhasználó számára érthetőek, nem igényelnek különösebb informatikai tudást.

Ebben az esetben a hatóság számára nehézséget okoz már annak a megállapítása, hogy ki az elkövető (az lesz-e, aki megírta a káros programot vagy az, aki telepítette azt a bankautomatára?), illetve mivel személyes kontaktus nem vagy csak nagyon ellenőrzött keretek között történik, a program írójának személye sokszor rejtve marad.

Az informatika fejlődését szervezett bűnözői körök is igyekeznek kihasználni, hiszen a kibertérben tudják legjobban az anonimitásukat megőrizni. Az internet határok nélkülisége, sok esetben szabályozatlansága vagy épp az országok eltérő jogi szabályozása az, ami leginkább segíti őket a céljaik elérésében.

2.2.7. Pénzmosás

A pénzmosás az előbbi alpontokban említett valamennyi bűncselekményekkel összefüggő olyan illegális tevékenység, amelynek célja, hogy a bűncselekményből származó anyagi nyereséget törvényes bevételnek tüntesse fel, olyan módon hogy az a hatóságok előtt rejtve maradjon, illetve az elkövetők kiléte ne legyen megállapítható.

[27] Nagy Zoltán András: Bűncselekmények számítógépes környezetben. Ad librum, Budapest, 2009. 262. o.

A kiberbűncselekményekből származó bevételek elrejtésére az egyik legtökéltesebb eszköz, ha vagy egy legálisnak tűnő vállalkozást működtetnek, vagy pedig a megszerzett jövedelmet valamilyen kriptovalutába fektetik[28], amelynek ugyanakkor meg van a rizikója is, hiszen annak értéke folyamatosan változik és a felette való rendelkezés közel sem annyira egyszerű, mint a bankszámlán tartott pénzzé.

2.3. Támadások a kormányzati szerverek, a kritikus infrastruktúrák ellen

Érdemes azt is mérlegelni, hogy egy kibertámadás esetén mikor beszélünk a szervezett bűnözői körök által elkövetett bűncselekményről és milyen esetekben minősítjük a támadást terrorcselekménynek.

A kettő közötti különbség csekély. Talán az egyik legjellemzőbb eltérés a motiváció lehet, de ahogy Istanovszky László is rámutatott egy tanulmányában, az elkövetők célja a meghatározó.

Míg bűnszervezet esetében a cél az öt évi vagy azt meghaladó bűncselekmény elkövetése, addig a terrorista csoport[29] esetén a cél a terrorcselekmény elkövetése. A terrorcselekményekkel pedig a cél egy állam vagy szervezet kényszerítése, a társadalmi, gazdasági rend megzavarása, megrendítése, vagy a lakosság megfélemlítése[30].

Az Európa Tanács terrorizmus elleni küzdelméről szóló kerethatározatának[31] 2. cikk (1) bekezdése alapján: a „terrorista csoport" kettőnél több személyből álló, hosszabb idő alatt létrehozott, szervezett csoportot jelent, amely terrorista bűncselekmények elkövetése végett összehangoltan működik.

A „szervezett csoport" egy olyan csoportot jelent, amelyet nem egy deliktum azonnali elkövetésére hoztak létre alkalomszerű jelleggel, és amelyben a tagoknak nincs szükségképpen formálisan meghatározott szerepe, illetve nem szükséges a tagság folyamatossága vagy a fejlett struktúra.

A terrorista csoport és a bűnszervezet fogalmi elemei között több ismérv megegyezik, egyedül a célban mutatkozik különbség.[32] A szervezeti hasonlóság igazolható, amennyiben a Btk. bűnszervezetre és terrorszervezetre vonatkozó meghatározásait vetjük elemzés alá, az eltérés nem módszereikben, inkább céljaikban keresendő[33].

---

[28] Nagy Zoltán – Mezei Kitti: Pénzmosás a kibertérben. Infokommunikáció és jog. 2018/70. 27. o.

[29] Btk. 319. § értelmező rendelkezés szerint a terrorista csoport: a három vagy több személyből álló, hosszabb időre szervezett, összehangoltan működő csoport, amelynek célja terrorcselekmény elkövetése.

[30] Istvanovszki László: A szervezett bűnözés elleni harc új stratégiája és taktikája. Hadtudomány Szemle 2015/1-2. 140. o.

[31] 2002/475/IB kerethatározat

[32] Lásd bővebben: Neparáczki Anna Viktória: A terrorizmus elleni fellépés eszközei a magyar és német büntető anyagi jogban. PhD értekezés. Pécs, 2017. 60-66. o.

[33] Istvanovszki: i.m. 139–143. o.

2.4. A szervezett bűnözők és a csúcstechnológiai eszközök fejlődése kínált lehetőségek

A szervezett bűnözők nemcsak a kiberteret használják ki, hanem a csúcstechnológia kínálta lehetőségeket is, amelyek révén akár írásban (titkosítva), akár szóban, a rendvédelmi szervek munkáját megnehezítve, képesek egymással kommunikálni, utasítást adni vagy sok esetben a helyszínt és a személyt feltérképezve segíteni egymás munkáját.

A modern eszközöknek köszönhetően más hálózatokhoz csatlakozva képesek rejtve maradni, de akár tőlük független személyek mögé bújva ismeretlennek lenni a hatóságok előtt.

A kommunikáció mellett a közösségi oldalak és a felhasználók kínálta lehetőségeket használják ki, amelyek során adatainkkal vagy a nem védett informatikai eszközeink felhasználásával követik el a bűncselekményt.

3. Nyomozási kihívások

A rendvédelmi hatóságok feladata[34] a bűnszervezetek működésének a felderítése[35], amelyet a kibertér használata és az országok különböző szabályozása vagy szabályozatlansága miatt igazi kihívást jelent.

A szervezett bűnözéssel kapcsolatban használt titkos hang-, beszéd-, kép-, videófelvételek a modern bűnüldözés nélkülözhetetlen eszközei, egyre inkább „conditio sine qua non”-jai az egyes nyomozásoknak, bizonyos bűncselekmények metodikájának.

A bűnelkövetők első dimenzióból második dimenzióba való átlépését követte a bűnüldözés hasonló irányú lépése is, amelyben felértékelődtek a második dimenziós bizonyítékok szerepe mint például az elektronikus bizonyítékoké. A hagyományos fizikai nyomokkal ellentétben már az az elektronikus nyomokat kell vizsgálni az információs rendszerek adattáraiban, adatok és adatmaradványok után kutatva, amelyekhez általában speciális tudású igazságügyi informatikai szakemberekre van szükség.[36]

---

[34] Lásd Simon Béla: A rendészeti szervek együttműködése a kiberbűnözés ellen. Nemzetbiztonsági Szemle 2018/1. 36-58. o.

[35] Ehhez lásd bővebben: Boda József: A felderítés, hírszerzés, titkos információgyűjtés elvei és gyakorlata. Belügyi Szemle 2015/9. 5-29. o.

[36] Fenyvesi Csaba: Az új generációs bizonyítékok a kriminalisztika történeti mérföldköveinek tükrében. Magyar Jog 2014/7-8. 441-442. o.; valamint lásd Máté István Zsolt: Informatikai rendszerek elleni támadások szakértői vizsgálata – a digitális nyomok rögzítésének szerepe. Belügyi Szemle 2018/7-8.

Az Európai Unióban az Europol-on belül a Számítástechnikai Bűnözés Elleni Európai Központ (EC3) foglalkozik a kibertérben elkövetett bűncselekményekkel, így kiemelten a szervezett bűnözői csoportok által elkövetett nemzetközi, online fizetési csalásokkal (az Európai Központi Bankkal és nemzeti bankokkal szoros együttműködésben), valamint a gyermekeket érintő szexuális kizsákmányoló magatartásokkal és a kritikus infrastruktúrákat érintő támadásokkal.[37]

Magyarországon a szervezett bűnözéssel valamint a kiberbűncselekményekkel kapcsolatban a Rendőrség és a Nemzeti Adó- és Vámhivatal Bűnügyi Főigazgatósága, a Terrorelhárítási Központ és az ügyészség foglalkozik, míg a nemzetbiztonsági szervezetek közül az Alkotmányvédelmi Hivatal, Katonai Nemzetbiztonsági Szolgálat feladatai között szerepel a szervezett bűnözők és a kiberbűnözők feltérképezése.

Ezen szervezeteken kívül ugyanakkor még meg kell említeni a Nemzetbiztonsági Szolgálat – Kibervédelmi Intézetet, a BM Országos Katasztrófavédelmi Főfelügyelőség, a Nemzeti Adatvédelmi és Információszabadság Hatóságot és a Nemzeti Média- és Hírközlési Hatóságot, amelyeknek kiemelt szerepe van a kibertámadások során.

Az Európai Unió 2014. június 10 és 13. között elfogadta a határokon átnyúló szervezett bűnözésről szóló Fehér Könyvet (Európa Tanács Büntetőjogi Kérdésekkel Foglalkozó Európai Bizottsága CDPC), amelyben kiemelték az Európai Unió tagállamait fenyegető veszélyeket, így a szervezett bűnözést, a kiberbűnözést valamint az Unió nyomozó hatóságainak és nemzetbiztonsági szervezeteinek ezzel kapcsolatos kihívásait.

A Fehér Könyv a következő példákon keresztül utal a nyomozási eljárások szabályozásának problémáira és ezzel összefüggésben a jogharmonizáció szükségességére:

– A számítógépek átkutatása gyakran a felkutatás és lefoglalás általános szabályai szerint történik, ami nem mindig jelent kielégítő megoldást, különösképpen problémás a számítógépes hálózatokhoz való távoli hozzáférés esetén. Az ilyenkor alkalmazott trójai és más hacker szoftverek használata határon túl joghatósági és szuverenitási kérdéseket vethet fel.
– Az adathalászat (phising) kapcsán bizonyos jogrendszerek nagyobb szabadságot biztosítanak a bűnüldöző hatóságoknak, úgy tekintve azt, mint a közterület-felügyeletet, ha az adat nyilvános forrásból származik, máshol viszont

36-54. o.; továbbá Herke Csongor: A műszaki és könyvszakértői vélemény egyes sajátosságai. In: Elek Balázs – Háger Tamás – Tóth Andrea Noémi (szerk.): Igazság, ideál és valóság: Tanulmányok Kardos Sándor 65. születésnapja tiszteletére. Debrecen, 2014. 196-209. o.; Simon Béla: Az igazságügyi szakértés egyes kérdései a büntetőeljárásban, különös tekintettel az informatikai szakterületre. Belügyi Szemle 2016/7-8. 87-105. o.

[37] Mezei Kitti: Az informatikai bűnözés elleni nemzetközi fellépés – különös tekintettel az Európai Unió és az Egyesült Államok szabályozására. JURA 2018/1. 353. o.

úgy vélik, az ilyen eljárások sértik a magántitokhoz való jogot, ezért alkalmazásukhoz meghatározott bírói ellenőrzés szükséges.
– Hasonló eltérések mutatkoznak az egyes tagállamoknak a szolgáltatást nyújtó vállalatok adatkezelési kötelezettségeire, illetve a nyomozó hatóságok ezen adatokhoz való hozzáférésére vonatkozó szabályozásaiban. Van, ahol bírósági végzés nélkül kiadhatók a felhasználók IP-címei, vagy akár az összes rájuk vonatkozó adat, máshol viszont csak a bíró hatalmazhatja fel a szolgáltatót, hogy a kliensek adatait a bűnüldöző szervek számára elérhetővé tegye.
– A határon átlépő ellenőrzött szállítások és a fedett nyomozók hatékony alkalmazását sokszor jogi akadályok és az egyértelmű szabályozások hiánya hiúsítja meg.
– Problémákat okoz, hogy több tagállamban nem határolódnak el egyértelműen a szervezett bűnözés súlyos formáinak felderítését végző titkosszolgálatok, információszerző egységek az állam védelmét ellátó nemzetbiztonsági szolgálatoktól.
– Nem egységes és sok helyen nem tisztázott, hogy milyen kényszerintézkedéseket foganatosíthatnak a hatóságok az eljárás egyes szakaszaiban[38].

A fenti problémák megoldása érdekében a dokumentum javaslatot tesz a tagállamok hatályos szabályozásának átfogó összehasonlító vizsgálatára és ennek nyomán egy kézikönyv, illetve egy folyamatosan frissülő weboldal létrehozására, valamint a különleges nyomozási eljárások transznacionális szinten való alkalmazásával, a bizonyítékok felhasználhatóságával és a terheltek jogainak védelmével kapcsolatos problémák további tanulmányozására. A munkacsoport szerint az Európa Tanácsnak kulcsszerepet kell játszania a határokon átnyúló büntetőeljárások általános elveinek kidolgozásában is.

4. Összegzés

Az említett bűncselekményekkel kapcsolatban felvetődik egy kérdés. Ezeket bűnszervezetek követik el, vagy pedig maga az elkövetés módja igényel szervezettséget? Nem technikai oldalról közelítve meg a felvetést, levezethetőek az alábbi megállapítások:

– A támadásokat rosszindulatú programok/szoftverek megírásával kezdik meg, aminek megírásához sok esetben nem elég egy személy, hanem több, egymást személyesen nem ismerő emberek követik el.

[38] http://www.juris.u-szeged.hu/kutatas-tudomany/tornyai-gergely/feher-konyv [2018.05.28.]

– Sokszor nem egy adott információs rendszer ellen hajtják végre, hanem eshetőlegesen, azok ellen, amelyek nem megfelelően (vagy egyáltalán nem) vannak védve, vagy esetleg egy úgynevezett backdoor-ral (hátsó kapuval) rendelkeznek és kihasználják annak gyengeségét
– A cselekmény végrehajtása a social engineering-gel vagy emberi manipulációval történik (ami szintén kérdéses kimenetelű és meg van a lehetősége, hogy egyáltalán nem vagy csak részben lehet kivitelezni).

Ezen a hármas tagolódást figyelembe véve, kiemelhető az elkövetők között a szerepek megosztása, ugyanakkor nem feltétlenül érvényesül a centralizáltság, hiszen a cél kivitelezéséhez technikailag legalább ugyanúgy kell érteni. A kivitelezés módjának informatikai, pszichológiai lehetőségeit és megoldásait sokkal egyszerűbb alakítani az elkövetők tudásához és habitusához, mint a hagyományosnak nevezhető szervezett bűnözőknél.

Felhasznált Irodalom

Boda József: A felderítés, hírszerzés, titkos információgyűjtés elvei és gyakorlata. Belügyi Szemle 2015/9.

Dornfeld László – Mezei Kitti: Az online gyermekpornográfia elleni küzdelem aktuális kérdései. Infokommunikáció és jog 2017/68.

Dornfeld László: A kibertér főbb nemzetközi és nemzeti szabályozásai. In: Pintér István (szerk.): Műhelymunkák: A virtuális tér geopolitikája.

Fenyvesi Csaba: Az új generációs bizonyítékok a kriminalisztika történeti mérföldköveinek tükrében. Magyar Jog 2014/7-8.

Gellér Balázs – Ambrus István: A magyar büntetőjog általános tanai I. ELTE Eötvös Kiadó. Budapest, 2017.

Hautzinger Zoltán: Idegen a büntetőjogban. AndAnn, Pécs, 2016.

Herke Csongor: A műszaki és könyvszakértői vélemény egyes sajátosságai. In: Elek Balázs – Háger Tamás – Tóth Andrea Noémi (szerk.): Igazság, ideál és valóság: Tanulmányok Kardos Sándor 65. születésnapja tiszteletére. Debrecen, 2014. .

Istvanovszki László: A szervezett bűnözés elleni harc új stratégiája és taktikája. Hadtudomány Szemle 2015/1-2.

Kiripovszky Csaba: Az emberkereskedelem és a szervezett bűnözés kapcsolata a prostitúció tükrében. Pécsi Határőr Tudományos Közlemények VIII. Különszám. Pécs, 2007.

MÁTÉ István Zsolt: Informatikai rendszerek elleni támadások szakértői vizsgálata – a digitális nyomok rögzítésének szerepe. Belügyi Szemle 2018/7-8.
MEZEI Kitti – NAGY Zoltán András: The organised criminal phenomenon on the Internet. Journal of Eastern-European Criminal Law 2016/2.
MEZEI Kitti – TÓTH Dávid: A készpénz-helyettesítő fizetési eszközökkel kapcsolatos bűncselekmények. In: Hollán Miklós-Barabás A. Tünde (szerk.): A negyedik magyar büntetőkódex: régi és újabb vitakérdések. MTA Társadalomtudományi Kutatóközpont. Budapest, 2017.
MEZEI Kitti: A DDoS-támadások büntetőjogi szabályozása az Egyesült Államokban, Európában és Magyarországon. Pro Futuro 2018/1.
MEZEI Kitti: Az informatikai bűnözés elleni nemzetközi fellépés – különös tekintettel az Európai Unió és az Egyesült Államok szabályozására. JURA 2018/1.
MOLNÁR Gábor: Gazdasági bűncselekmények. HVG-ORAC Lap- és Könyvkiadó Kft. Budapest, 2009.
NAGY Zoltán – MEZEI Kitti: Pénzmosás a kibertérben. Infokommunikáció és jog. 2018/70.
NAGY Zoltán András: A szervezett bűnözői jelenségek a számítógépes hálózatokon. Belügyi Szemle 2012/6.
NAGY Zoltán András: Bűncselekmények a kibertérben. Ad librum, Budapest, 2009.
NAGY Zoltán András: Kiberbűncselekmények, kiberháború, kiberterrorizmus – avagy ébresztő Magyarország! Magyar Jog 2016/1.
NAGY Zoltán András: A számítógéppel megvalósítható vagyoni jogsértésekről. Bűnügyi Műhelytanulmányok 1992/1.
NEPARÁCZKI Anna Viktória: A terrorizmus elleni fellépés eszközei a magyar és német büntető anyagi jogban. PhD értekezés. Pécs, 2017.
NYESTE Péter: A nemzetbiztonsági célú stratégiai felderítés/elhárítás és a bűnügyi célú stratégiai hírszerzés összehasonlítása, kiemelten a szervezett bűnözés elleni fellépés területén. Felderítő szemle XII. évfolyam 1. szám 2013.
NYITRAI Endre: A szervezett bűnözés elleni küzdelem büntetőjogi és kriminalisztikai eszközei. PhD értekezés. Pécs, 2017.
PARTI Katalin – KISS Anna: A számítástechnikai bűnözésről akkor és most. In: Bárd Petra – Hack Péter – Holé Katalin: Pusztai László emlékére. OKRI-ELTE ÁJK. Budapest, 2014.
PARTI Katalin: Gyermekpornográfia az interneten. Bíbor Kiadó. Budapest, 2009.
SIMON Béla: A rendészeti szervek együttműködése a kiberbűnözés ellen. Nemzetbiztonsági Szemle 2018/1.
SIMON Béla: Az igazságügyi szakértés egyes kérdései a büntetőeljárásban, különös tekintettel az informatikai szakterületre. Belügyi Szemle 2016/7-8.

Szathmáry Zoltán: A számítástechnikai bűncselekmények. Magyar Jog 2011/3.
Tóth Mihály – Kőhalmi László: A szervezett bűnözés. In: Borbíró Andrea – Gönczöl Katalin – Kerezsi Klára – Lévay Miklós: Kriminológia. Wolters Kluwer Kft. Budapest, 2016.
tóth Mihály: Bűnszövetség, bűnszervezet. Complex Kiadó Kft. Budapest, 2009.
Tóth Mihály: XLII. fejezet – A fogyasztók érdekeit és a gazdasági verseny tisztaságát sértő bűncselekmények. In: Tóth Mihály – Nagy Zoltán: Magyar büntetőjog – Különös Rész. Osiris Kiadó. Budapest, 2014.
Urszán József: A szervezett bűnözés fenyegetettség értékelésének jelentősége az Európai Unióban. In: Gaál Gyula – Hautzinger Zoltán: Tanulmányok „A változó rendészet aktuális kihívásai" című tudományos konferenciáról. Pécsi Tudományos Határőr Közlemények. Pécs, 2013.