MEZEI KITTI

A SZERVEZETT BŰNÖZÉS AZ INTERNETEN[1]

1. Bevezetés

Az internet vonzó környezetté vált a különböző profit-orientált bűnelkövetők számára, különösen mert a határokon átível, magasfokú anonimitást biztosít és nincs szükség arra, hogy jelen legyenek fizikailag a bűncselekmények elkövetésének a helyszínén, ezért a kockázat minimalizálása mellett jelentős profitra tudnak szert tenni.[2] Ez különösen kedvező, ha olyan országokból tudják működtetni a bűnözői infrastruktúrájukat, ahol nem biztosított a megfelelő jogszabályi háttér és technológiai kapacitás sem ahhoz, hogy hatékonyan feltudjanak lépni például az informatikai vagy másnéven kiberbűncselekményekkel[3] szemben.

A technológiai fejlődést kihasználó bűnelkövetők tevékenysége két csoportra osztható: egyrészt vannak az olyan büntetendő magatartások, amelyek korábban is léteztek, de az internetes kapcsolattartási és más lehetőségek jobban elősegítik azok terjedését, így akár nagyságrendileg is növelve a társadalmi veszélyességüket. Ide so-

[1] Az Emberi Erőforrások Minisztériuma ÚNKP-17-3-I kódszámú Új Nemzeti Kiválóság Programjának támogatásával készült.

[2] Gyaraki Réka: A számítógépes környezetben elkövetett gazdasági bűncselekmények – A PIN kód megadása sikeres vagy biztonságos az internet?! Pécsi Határőr Tudományos Közlemények XIII. Pécs, 2012. 235. o.

[3] A szakirodalom szerinti informatikai bűnözésre vagy kiberbűnözésre (cybercrime) mint egy gyűjtőfogalomként lehet tekinteni, amelynek két fő csoportja különböztethető meg: az egyik azon deliktumok csoportja, amelyek kizárólag információs rendszerekkel (számítógépekkel, azok hálózatával vagy egyéb ICT eszköz használatával) követhetők el. Jellemzően ezeknek a bűncselekményeknek a tárgya az információs rendszer, tehát amikor a támadás ez ellen irányul. Ezek a tisztán informatikai bűncselekmények vagy kiberbűncselekmények, az ún. „cyber-dependent crime" (pl. számítógépes vírusok használata, hacking stb.). A második tágabb kategóriába tartoznak azok a hagyományos bűncselekmények, amelyeket az információs rendszerek felhasználásával valósítanak meg mint például ilyen a csalás, zsarolás, gyermekpornográfia, szerzői jogi jogsértések, zaklatás stb., ez az ún. „cyber-enabled crime" esetköre, amikor az információs rendszer a bűncselekmény elkövetésének az eszköze. Lásd Clough, Jonathan: Principles of Cybercrime. Cambridge University Press, 2015. 10-11. o. https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assess-ment-iocta-2017 [2018.03.14.]

rolhatók mindenekelőtt a szervezett bűnözés hagyományos „üzletágai" (pl. kábítószer-kereskedés) és másrészről vannak azok, amelyek a már említett módon a technológiai vívmányok nélkül nem léteznének mint a kiberbűncselekmények köre.[4]

Kétségtelen tény, hogy a hagyományos szervezett bűnözői csoportok számára is kedvezővé vált a modern technológiák használata, azonban az kérdéses, hogy milyen mértékben terjed ki a tevékenységi körük például a kiberbűnözésre. Jellemző rájuk, hogy az ún. bűnözői feketegazdaságban[5] fejtik ki a különféle illegális tevékenységüket – melyet a kereslet-kínálat törvénye határoz meg –, és ezt is megkönnyíti számukra, hogy a valós téren kívül már a digitális platformokon keresztül is folytathatják ezt. Nem véletlen, hogy a szervezett bűnözés motorját napjainkban már az illegális online kereskedelem jelenti. A szervezett bűnözés és a kiberbűnözéssel kapcsolatban két kérdés merül fel:

– az internet egy új színteret jelent-e a tradicionális szervezett bűnözői csoportok számára a különböző illegális tevékenységük folytatásához és/vagy
– lehetőséget teremt az új típusú, „szervezett" kiberbűnözői csoportok működéséhez, amelyek kifejezetten a kiberbűncselekmények elkövetésére specializálódnak.

2. A szervezett bűnözés fogalma és a hazai szabályozás

A szervezett bűnözői csoportok működését és értékrendjét meghatározzák azok az országok, társadalmak, illetve kultúrák, amelyekben tevékenységüket kifejtik, így különösen hatással van a szerveződésükre az adott földrajzi és politikai helyzet, a kriminális tradíció – mint az illegális igények – és a bűnüldözés felépítése, valamint annak hatékonysága.[6] A társadalmak Európa-szerte egyre inkább egymással összekapcsoltabbá, illetve nemzetközi jellegűvé váltak, ami ugyanígy a szervezett bűnözés működésére is jellemző, hogy összekapcsoltabbá és nemzetközileg aktívabbá vált mint valaha.

A szervezett bűnözői csoportok tevékenységi és működési köre („üzleti portfoliója") egyre változatosabb, bár a kábítószer-kereskedelem továbbra is a legjöve-

[4] Korinek László: A technika fejlődése és a bűnözés. In: Borbíró Andrea – Inzelt Éva – Kerezsi Klára – Lévay Miklós – Podoletz Léna (szerk.): A büntető hatalom korlátainak megtartása: A büntetés mint végső eszköz – Tanulmányok Gönczöl Katalin tiszteletére. ELTE Eötvös Kiadó. Budapest, 2014. 290. o.

[5] Tóth Mihály: A gazdasági bűnözés és bűncselekmények néhány aktuális kérdése. MTA Law Working Papers 2015/4. 5. o.: „A feketegazdaság – szűkebb, vagy tágabb értelemben – elsősorban a legális gazdasági szférán kívüli tevékenységre, a követhetetlenségre, ellenőrizhetetlenségre, (vagy konkrétabban az adózatlanságra) utal, és a gondok alapvető forrásának a láthatatlan jövedelmek képződését tartja."

[6] Tóth Mihály – Kőhalmi László: A szervezett bűnözés. In: Borbíró Andrea – Gönczöl Katalin – Kerezsi Klára – Lévay Miklós: Kriminológia. Wolters Kluwer Kft. Budapest, 2016. 608. o.

delmezőbb tevékenységnek számít, azonban emellett jellemzően foglalkoznak még fegyverkereskedelemmel, embercsempészéssel, termékhamisításokkal és a kiberbűnözéssel is, és ezeket járulékosan a pénzmosás követi.[7]

A nagyobb „tradicionális", hierarchikus szervezett csoportok mellett a kisebb és lazább szerkezetű csoportok vannak jelen, amelyeket megbízott, speciális szaktudással rendelkező személyek erősítenek ad hoc jelleggel. Az is előfordul, hogy az egyes csoportok csak rövid időre alakulnak egy meghatározott illegális tevékenység elvégzéséig. Az Europol jelentése szerint jelenleg 5000 szervezett bűnözői csoport működik nemzetközi szinten, akikkel szemben folyamatban lévő nyomozás is van, míg 2013-ban csak 3600 ilyen csoportról számoltak be. A növekedés köszönhető a kisebb bűnözői csoportok megjelenésének, különösen az ún. bűnözői piacok (criminal market) népszerűségének, amelyeknek a működése és az alapjukat képező üzleti modell erősen függ az internettől. Ezen piacok fragmentáltsága különösen a kiberbűncselekményekkel kapcsolatban figyelhető meg, és ezeket növekvő számban önálló bűnelkövetők is mint egy vállalkozásként folytatnak, vagy akár többen együtt alkalmi jelleggel, hogy vállalkozásukat működtessék, ami általában illegális árucik-kekkel való kereskedést vagy különféle szolgáltatások nyújtását jelenti.[8]

Korinek László szerint – kriminológiai aspektusból vizsgálva – a szervezett bűnözést a következő ismérvek határozzák meg:

- a hatályos jogszabályok szerint tiltott szükségletek kielégítésére irányul,
- a lehető legkisebb kockázatvállalás mellett a leggyorsabb és lehető legnagyobb profitra törekvés jellemzi,
- a bűnözői csoportokon belül szakosodás, specializáció figyelhető meg,
- a szervezett bűnöző tevékenységét foglalkozásként űzi,
- jellemző az erőszak a bűnözőtársulás tevékenysége során,
- megfigyelhető a legális és illegális tevékenységek egyidejű jelenléte,
- a tevékenység nemzetközi, határokon átnyúló jellegű.[9]

2000 óta az Egyesült Nemzetek keretében létrejött nemzetközi szervezett bűnözés elleni Egyezmény határozza meg a nemzetközi fogalmát a szervezett bűnözői csoportnak, amely értelmében bizonyos ideig fennálló, három vagy több főből álló

[7] Abadinsky, Howard: Organized crime. Ninth Edition, Wadsworth Cengage Learning, 2010. 203. o.

[8] Europol: European Union Serious and Organised Crime Threat Assessment (SOCTA) – Crime in the age of technology. 2017. 14. o. https://www.europol.europa.eu/activities-services/main-reports/european-union-serious-and-organised-crime-threat-assessment-2017 [2018.03.21.]

[9] Korinek László: A szervezett bűnözés lényegi elemei. In: Harmadik Magyar Jogászgyűlés – Magyar Jogász Egylet. Budapest, 1996. 65-72. o.

strukturált csoportról[10] van szó, amely összehangoltan működik egy vagy több, az Egyezményben meghatározott súlyos bűncselekmény[11] elkövetése céljából, közvetlen vagy közvetett módon pénzügyi vagy más anyagi haszon megszerzésére törekedve.

Ezt a definíciót vette át az országok többsége, így Magyarország is. Ennek fényében a hatályos Büntető Törvénykönyvről szóló 2012. évi C. törvény (a továbbiakban: Btk.) 459.§ (1) bekezdés 1. pontja határozza meg a bűnszervezet fogalmát, amely három vagy több személyből álló, hosszabb időre szervezett, összehangoltan működő csoport, amelynek célja ötévi vagy ezt meghaladó szabadságvesztéssel büntetendő szándékos bűncselekmények elkövetése.

Az említett bekezdés 2. pontjában foglalt értelmező rendelkezés a bűnszövetséget is definiálja, amely akkor létesül, ha két vagy több személy bűncselekményeket szervezetten követ el, vagy ebben megállapodik, és legalább egy bűncselekmény elkövetését megkísérlik, de nem jön létre bűnszervezet. E fogalomnak a negatív eleme, hogy nem jöhet létre bűnszervezet.[12]

Áttérve azonban a bűnszervezet fogalmi ismérveinek részletes vizsgálatára: az „összehangolt működés" tartalmát tekintve nem más, mint a benne cselekvő személyek egymást erősítő hatása. Ugyanakkor az összehangoltság meglétének – természetéből adódóan – nem feltétele a bűnszervezetben cselekvők közvetlen kapcsolata, a más cselekvések, illetve a más cselekvők kilétének konkrét ismerete. A bűnszervezetben elkövetés azzal szemben is megállapítható, aki – eseti jelleggel – akár egyetlen cselekményt tettesként vagy részesként valósít meg, tehát nem az alanyi bűnösség, hanem a bűnszervezet fogalmi elemei megállapításának kérdése a «hosszabb időre szervezett" kitétel, amely a több bűncselekmény rendszeres jellegű elkövetését jelenti, de a bűnszervezet oldalán. Az elkövető tudatának továbbá nem arra kell kiterjednie, hogy egy bűnszervezet a törvényi előfeltételek szerint létrejött, hanem arra, hogy a bűnszervezet tárgyi sajátosságai ismeretében annak „működéséhez" csatlakozik, illetve annak keretében cselekszik. A Btk. hatályos rendelkezései nem tesznek különbséget a bűnszervezeten belüli cselekvés hiearchiája („posztjai"), aktivitása, intenzitása szempontjából, ezek a büntetéskiszabás körében értékelendő

[10] A strukturált csoport nem egyetlen bűncselekmény azonnali végrehajtására, valamint nem alkalomszerűen létrehozott csoport. Nem szükséges, hogy tagjai pontosan meghatározott szerepekkel rendelkezzenek vagy, hogy tagsága állandó legyen, illetve hogy fejlett hierarchiával rendelkezzen.

[11] Az Egyezmény definiálja továbbá a súlyos bűncselekményt is, melynek értelmében legalább négy év szabadságvesztéssel vagy súlyosabb büntetéssel büntethető bűncselekményt megvalósító magatartást jelenti.

[12] Lásd bővebben Gellér Balázs – Ambrus István: A magyar büntetőjog általános tanai I. ELTE Eötvös Kiadó. Budapest, 2017. 410-425. o.

körülmények.[13] A bűnszervezet megállapításához nem többletkövetelmény a bűnös profitszerzési célzat.[14]

A bűnszervezetben elkövetésre vont jogkövetkeztetésnek van helye – az egyéb törvényi feltételek megléte esetén –, ha az elkövetési magatartások egymást kiegészítő jellegűek, azok kapcsolódása a célzott és végrehajtott bűncselekményhez kölcsönös, az adott tényállásszerű elkövetési magatartás keretei közé illeszkedő cselekmény más személy előző cselekményéhez társul, avagy a célzott bűncselekmény megvalósulásához további láncolatos tevékenységet feltételez.[15] A bűnszervezet fogalmának utolsó objektív ismérve egy szervezeti célt határoz meg, amely szerint a bűnszervezet létének nem törvényi előfeltétele akár egyetlen bűncselekmény befejezett elkövetése vagy kísérlete sem. A Btk. nem sorolja fel, hogy milyen típusú bűncselekmények tartoznak ide csak annyit, hogy ötévi vagy ezt meghaladó szabadságvesztéssel büntetendő szándékos bűncselekményekről lehet szó. Ezzel kapcsolatban felmerül az a kérdés, hogy mindez azokra a bűnszervezetekre hogyan alkalmazható és miképpen minősíthető a szervezet működésébe becsatlakozó elkövetők magatartása, akik kihasználják az internet nyújtotta előnyöket és például az illegális tevékenységüket az online piacterekre kiterjesztve folytatják (pl. kábítószer-kereskedelem, gyermekpornográf tartalmak terjesztése stb.).

Mindezekre tekintettel azon az álláspontón vagyok, hogy amennyiben megvalósulnak a bűnszervezetnek a törvényi feltételei és az elkövető tudata át fogja azt, hogy bűnszervezethez kapcsolódva cselekszik – akár legyen szó csak egyszeri alkalomról –, akkor a bűnszervezetben történő elkövetés megállapítható, feltéve, ha az általa kapcsolódó bűncselekmény ötévi vagy súlyosabb szabadságvesztéssel büntetendő. Ugyanez vonatkozik a tetteseken kívül a részesekre is, tehát amennyiben a szükséges feltételek teljesülnek, akkor az esetükben is a bűnszervezetben elkövetésről van szó.[16] Ezt erősíti a Kúria friss eseti döntése is, amelyben kimondta, hogy a bűnszervezettel kapcsolatban elsődlegesen mindig a bűncselekmény elkövetését kell vizsgálni, majd az alanyi oldalt, az elkövető tudattartalmát, hogy felismerte-e, hogy az elkövetési magatartását a bűnszervezet keretén belül valósította meg. A törvény a bűnszervezet külső, tárgyi jellegű ismérveit határozza meg, ezért fontos, hogy ez a kívülálló számára is felismerhető legyen. A bűnszervezeten belüli személyes ismeretség valamennyi elkövetővel nem feltétele a megállapításának, és a bűnszervezet-

[13] 4/2005. számú BJE határozat; TÓTH Mihály: Bűnszövetség, bűnszervezet. Complex Kiadó Kft. Budapest, 2009. 148-151. o.
[14] BH 2008. 139.
[15] BH 2018.4.106.
[16] BH 2010.11.472.

nek nem törvényi kritériuma a hierarchikus kapcsolat sem.[17] Hiszen a bűnszervezet létrejöhet úgyis, hogy a keretében bűncselekményeket irányító vagy vezető személy hangolja össze azoknak az elkövetőknek a magatartását, akik egymás tevékenységéről nem is tudnak.[18] Amennyiben mégis hierarchikus szervezetről van szó, akkor a bűnszervezet vezetője felbujtóként tartozik felelősséggel a bűnszervezet tagjai által elkövetett bűncselekményekért.[19]

Mindezt figyelembe véve a tudattartalom vizsgálatának körültekintően kell történnie, és ezzel párhuzamosan vizsgálni kell a büntetőeljárás során feltárt bizonyítási eszközökből származó, és a bűnszervezet fennállásának megállapításához szükséges ismérvekre következtetést megalapozó bizonyítékokat, és erre nézve a tényállásban megállapítást kell tenni.[20]

Amennyiben nem éri el a meghatározott büntethetőséget az elkövető cselekménye, akkor súlyosító körülményként értékelhető és nem alkalmazhatók a bűnszervezeti elkövetéshez kapcsolódó jogkövetkezmények. Más kérdés, ha például az elkövető cselekményei több részcselekményből tevődnek össze, ugyanakkor a természetes egységbe vagy a folytatólagosság egységébe olvadnak, és amely a szervezetbe tartozó tag esetében eléri az ötévi fenyegetettséget, akkor a joggyakorlat ebben az esetben megfontolandónak tartja annak megállapítását, hogy a bűnszervezet törvényi feltételei fennállnak. Azonban a szakirodalombam eltérő álláspont is található, mely szerint a bűnszervezeti elkövetés célja bűncselekmények elkövetése, a többes szám pedig egység-többségtani szempontból bűncselekményi többségre, egy eljárásban történő elbírálás esetén pedig bűnhalmazat fennállására enged következtetni. A nyelvtani értelmezés alapján a bűnszervezet hatókörének kiterjesztése aggályos lehet. Hasonlóan alakul a törvényi egység más esetkörei vagy a látszólagos halmazat esetén.[21]

Összességében elmondható, hogy a bűnszervezet fogalmába a bűnöző célzatú tartós struktúrák számos formája beilleszthető, amely alkalmas lehet arra, hogy egyrészről kifejezze az alkalmi kisebb súlyú bűnszövetséghez viszonyított többletkriminalitást, másrészről magában foglalja a szervezettség súlyosabb formájában rejlő veszélyességet is. A bűnszervezet keretében történő elkövetéshez bármely szándé-

[17] BH 2016.9.234.

[18] Csák Zsolt: Társas elkövetés, különös tekintettel a bűnszervezetre. In: Benisné Győrffy Ilona (szerk.): Negyvenegyedik Jogász Vándorgyűlés. Budapest, 2018. 328-329. o.

[19] EBH 2008.1849.

[20] BH 2014.131.

[21] ambrus István: Egység és halmazat – régi dogmatikai kérdés új megközelítésben. Szeged, SZTE ÁJK, 2014. 20. o.

kos bűncselekmény esetén súlyos általános részi jogkövetkezmények[22] társulnak – mivel a hatályos szabályok szerint általános jellegű minősítő körülmény –, míg a bűnszövetség esetében a bűncselekmény súlya közömbös, de csak akkor állapítható meg, ha a Különös Részben minősítő körülményként szerepel.[23]

A Btk. 321.§ (1) bekezdése szerint bűnszervezetben részvétel bűntette miatt büntetendő, aki bűncselekmény bűnszervezetben történő elkövetésére felhív, ajánlkozik, vállalkozik, a közös elkövetésben megállapodik, vagy az elkövetés elősegítése céljából az ehhez szükséges vagy ezt könnyítő feltételeket biztosítja, illetve a bűnszervezet tevékenységét egyéb módon támogatja. A tényállás kétfajta elkövetési magatartástípust rendel büntetni: egyrészt sui generis előkészületi bűncselekményt, azzal, hogy bár eltérő sorrendben, de az előkészület fogalmát alkotó magatartásokat jelöl meg; másrészt sui generis bűnsegélyt azzal, hogy azt, aki – mint a bűnszervezeten kívülálló személy – a bűnszervezet tevékenységét támogatja büntetni rendeli. Az elkövetési magatartások a bűncselekmény bűnszervezetben történő elkövetéséhez kapcsolódnak és amennyiben, aki az előkészületi jellegű magatartását tovább folytatva saját maga is bekapcsolódik a szervezet tevékenységébe, és azt a magatartást, amelyre felhívott stb. megkísérli vagy annak megvalósításában tettesként közreműködik, értelemszerűen a bűnszervezetben elkövetett bűncselekmény tetteseként fog felelni. A Btk. Kommentárja azt rögzíti, hogy a bűnszervezet tevékenységének „egyéb módon támogatása" csak a szervezeten kívülálló személy részéről valósítható meg, és feltételezi a bűnszervezet létezését. E fordulat elkövetőinek a cselekménye nem közvetlenül a bűnszervezetben elkövetett bűncselekményhez, hanem magához a bűnszervezet működéséhez kapcsolódik és tisztában kell lenniük azzal, hogy

[22] Azzal szemben, aki a szándékos bűncselekményt bűnszervezetben követte el, a bűncselekmény büntetési tételének felső határa a kétszeresére emelkedik, de a huszonöt évet nem haladhatja meg. Halmazati büntetés esetén a 81. § (3) bekezdése szerinti büntetési tételt, tárgyalásról lemondás esetén a 83. § (1)–(2) bekezdése szerinti büntetési tételt kell alapul venni. [91. § (1) bek.];

Azzal szemben, aki a bűncselekményt bűnszervezetben követte el, mellékbüntetésként kitiltásnak is helye van. [91. § (2) bek.];

A kétévi vagy ennél hosszabb tartamú szabadságvesztést fegyházban kell végrehajtani [37. § (2) bek. bb) pont];

A feltételes szabadságra bocsátás kizárt [38. § (4) bek. c) pont];

A végleges hatályú foglalkozástól eltiltás alól a bíróság az eltiltottat nem mentesítheti, ha az eltiltás méltatlanság okán, véglegesen történt [Btk. 53. § (4) bek.];

A bűncselekmény eszközének és tárgyának elkobzása méltányosságból nem mellőzhető [73. § b) pont.];

A bűnszervezet ideje alatt szerzett vagyont az ellenkező bizonyításáig elkobzás alá eső vagyonnak kell tekinteni [74. § (4) bek. a) pont];

A büntetés végrehajtásának felfüggesztése kizárt [86. § (1) bek. b) pont];

A tevékeny megbánás (közvetítői eljárás) kizárt [29. § (3) bek. b) pont].

[23] Tóth Mihály: A bűnszervezeti elkövetés szabályozásának kanyargós útja. Magyar Jog 2015/1. 5-6. o.

akár anyagi vagy más természetű támogatással a súlyos bűncselekmények elkövetésére létrejött csoportosulás tevékenységét előmozdítják anélkül, hogy a bűnszervezetben elkövetett bármely bűncselekményhez segítséget nyújtanának.[24] Tóth Mihály vitathatónak tartja a lehetséges alanyok szűkítését, mert indokolatlanul privilegizált helyzetet teremt azoknak a csoport-tagoknak, akik a tudatos csatlakozáson kívül akár rendszeres finanszírozással vagy öt évet meg nem haladó büntethetőségű bűncselekményekkel támogatják a bűnös tevékenység előkészítését. Nem világos, hogy miért kellene a lehetséges alanyok körét tekintve különbséget tennünk pl. a bűncselekmény elkövetéséhez szükséges eszközök beszerzésében, rendelkezésre bocsátásában testet öltő magatartás és az anyagi eszközök rendelkezésre bocsátása, esetleg a tekintélyen, befolyáson alapuló pszichikai támogatás között.[25]

Ezzel szoros összefügésben érdemes arra kitérni, hogyha egy adott, kívülálló személyt (pl. informatikus szakembert) megbíznak az online bűnözői infrastruktúra kezelésére, annak biztosítására vagy egyéb tevékenységre (pl. rosszindulatú programok készítésére), ami kapcsolódik a szervezet működéséhez – sőt elősegíti azt –, akkor ez hogyan értékelhető. Amennyiben fennállnak a bűnszervezetnek a feltételei és az elkövető a folyamatosan végzett, de ötévi szabadságvesztéssel fenyegetettséget el nem érő cselekményei valós bűnszervezethez kapcsolódnak és ezek a súlyos bűncselekmények megvalósulását biztosítják, akkor a bűnszervezetben részvétel bűntettét valósítja meg.

A kiberbűncselekmények vonatkozásában fontos kiemelni a 2013/40/EU irányelvet az információs rendszerek elleni támadásokról, mert kimondja, hogy helyénvaló súlyosabb szankciókat megállapítani, ha az információs rendszer elleni támadást bűnszervezetben követik el, valamint, ha jelentős számú információs rendszert érint.[26]

3. A kiberbűnözői csoportok tipológiája

A kiberbűnözői csoportok tipológiáját átfogóan Michael McGuire vizsgálta, aki a kutatása során az általa feltárt ügyek alapján arra a következtetésre jutott, hogy az informatikai bűnözéssel kapcsolatos esetek 80%-a valamilyen szervezett tevé-

[24] Belegi József: A közbiztonság elleni bűncselekmények – Btk. XXX. fejezet. In: Kónya István (szerk.): Magyar büntetőjog I-III. – új Btk. – Kommentár a gyakorlat számára. 5. kiadás, HVG Orac Lapkiadó Kft. 2016.

[25] Tóth (2015): i.m. 7. o.

[26] Nagy Zoltán András: A 2013/40-es Uniós direktíva az informatikai rendszereket érő támadásokról. http://www.rendeszetelmelet.hu/Graphics/pdf/Nagy_Zoltan_Andras_A_2013_40_es_Unios_direktiva.pdf [2018.02.28.]

kenység eredménye. Ez azonban nem jelenti azt, hogy az elkövetők a tradicionális és hierarchikus szervezett bűnözői csoportokhoz tartoznának vagy kizárólag kiberbűncselekményeket követnének el. A tanulmányában arra hívja fel a figyelmet, hogy a hagyományos bűnszervezetek egyre inkább kiterjesztik a tevékenységüket az interneten, emellett újabb és kevésbé szoros kapcsolatú bűnözői csoportok jelennek meg. A bűnözői csoportok különböző szintű szervezettséget mutatnak, attól függően, hogy a tevékenységüket csak online fejtik ki, vagy online eszközöket használnak, hogy lehetővé tegyék a bűncselekmények elkövetését a „való" világban, vagy ezek kombinációja jelenik meg online és offline is.

McGuire egy tipológiát ajánl a kiberbűnözői csoportokkal kapcsolatban, amely hatféle csoport felépítését foglalja magában, kihangsúlyozva, hogy ezek az alapvető szervezeti minták gyakran keresztezik egymást és rendkívül rugalmasan alakulhatnak akár megtévesztő módon. Felhívja a figyelmet arra is, hogy mindez a folyamatos technológiai fejlődésnek köszönhetően változni fog a jövőben. Három főcsoportot különböztet meg, amelyeket további két alcsoportokra bont a tagok között fennálló kapcsolat erőssége alapján. Az első főcsoport online működik és további két alcsoportra osztható, amelyek a következők: a „swarm" és a „hub".

A „swarm" egy olyan csoport, amely valamely közös cél érdekében tevékenykedik, irányítás és szervezett működés nélkül. Általában az ideológiai vagy politikai indíttatású csoportok tartoznak ide, amelyek online fejtik ki a tevékenységüket mint például ilyen az Anonymous hacktivista csoport is.

A „hub" csoportok szintén online működnek, de a „swarm"-hoz képest szervezettebbek és hierarchikusabbaknak tekinthetők, mert meghatározott „irányító, létrehozó" kulcstagok köré csoportosulnak „az egyszerű" tagok. A tevékenységük széleskörű magában foglalhatja az ún. „crimeware"[27] terjesztést, az adathalász támadásokat (phishing) és a gyermekpornográfiát. McGuire szerint az online feketepiacok működése illeszkedik ebbe a modellbe.

A második főcsoportba tartoznak azok a hibrid csoportok, amelyek online és offline is jelen vannak.

A „clustered hybrid" esetében egy kisszámú csoportról van szó, amely meghatározott és speciális tevékenységgel foglalkozik. A „hub" felépítéséhez hasonló, de a különbség az, hogy az online elkövetés mellett az offline is megjelenik például bankkártyákat skimmelnek majd az interneten árulják a megszerzett bankkártya adatokat.

[27] A crimeware olyan rosszindulatú programokat foglal magában, amikkel az elkövetők célja, hogy haszonra tegyenek szert és egyúttal a felhasználók pénzügyi jólétét vagy értékes adatait veszélyeztessék (pl. a vírusok, a trójai vagy keylogger, amik a bűnözői csoportok számára lehetőséget teremtenek az adatok ellopásához, illetve azokkal való kereskedéshez).

Az „extended hybrid" csoportok kevésbé centralizáltak, általában többen társulnak és kisebb alcsoportokra osztható, de a különféle bűncselekmények elkövetéséhez megfelelő koordinációval rendelkeznek.

A harmadik főcsoport azokat a csoportokat foglalja magában, akik elsősorban offline fejtik ki a tevékenységüket, de egyúttal a modern technológiák és az internet nyújtotta előnyöket is kihasználják már.

A „hierarchies" azok a tradicionális bűnözői csoportok, akik illegális tevékenységüket az interneten is kifejtik, ilyenek lehetnek a tradicionális maffia családok, akik például a prostitúcióhoz kapcsolódó tevékenységüket kiterjesztik a pornográf, különösen a gyermekpornográf weboldalakra, illetve online szerencsejáték oldalakat üzemeltetnek vagy a zsarolást kibertámadások felhasználásával követik el.[28] A nemzetközi szindikátusok is érintettek a kiberbűnözésben mint például a Triádok vagy Yakuzák, akik szoftver kalózkodással, bankkártya hamisításokkal és csalásokkal is foglalkoznak.[29]

Az „aggregate" csoportok pedig lazán szervezettek, ad hoc jelleggel működnek. Például mobiltelefonokat használnak a csoport tevékenységének a koordinálásához vagy a nyilvános zavargás szervezéséhez.[30]

A téma szempontjából két csoportot érdemes kiemelni és részletesen ezek összehasonlításával foglalkozik a szerző: a „hierarchies", a tradicionális szervezett bűnözői csoportok és a „hub" mint az új típusú kiberbűnözői csoport.

4. A tradicionális szervezett bűnözői csoportok és a kiberbűnözői csoportok összehasonlítása

A tradicionális szervezett bűnözői csoportok általában etnikailag homogének, és hierarchikusan strukturáltak, valamint multifunkcionális és bürokratikus szervezeteknek tekinthetők. Az összehasonlítás alapját képező másik új típusú csoportosulás pedig az ún. „szervezett" kiberbűnözői csoport, amelynek meghatározására Marie-Helen Malas tett kísérletet: egy strukturált csoport, amely három vagy több tagból áll, amelynek célja egy vagy több súlyos kiberbűncselekmény anyagi haszonszerzési célú elkövetése az információs rendszerek, az internet felhasználásával.[31]

[28] McGuire, Michael: Organised Crime in the Digital Age. London: John Grieve Centre for Policing and Security. 2012.

[29] Kim-wang, Raymond – Choo-Grabosky, Peter: Cybercrime. In: Paoli, Letizia: The Oxford Handbook of Organized Crime. Oxford University Press, 2014. 485. o.

[30] Broadhurst – Grabosky – Alazab-Chon: i.m. 7. o.

[31] Malas, Marie-Helen: Cybercriminology. Oxford University Press. New York, 2017. 365 o.

A kiberbűnözői csoportok fejlődésük során soha nem mentek végbe olyan szintű szervezettségen mint a hagyományos bűnszervezetek. Az egyéni és fragmentált bűnözői tevékenységek felől mozdultak el a modern vállalati üzleti modellek alkalmazása felé és általában a hierarchikus felépítés hiányzik belőlük. A rugalmas kapcsolatrendszer jellemző rájuk, tagjaik magasan képzett szakemberek és általában a speciális szakismeretüknek, tudásuknak megfelelő feladatot látnak el, amivel hozzájárulnak a különféle crimeware és azokhoz kapcsolódó szolgáltatások fejlesztéséhez.

Míg a tradicionális bűnszervezetek ismérve, hogy erőszakos módon törekednek arra, hogy fenntartsák a monopol helyzetüket a saját területük, illetve érdekeltségük alá vont javak felett annak érdekében, hogy ellenőrzésük alatt tarthassák az általuk dominált piacot, addig a területi kontroll az interneten nyilván nem kivitelezhető a virtuális környezet sajátosságaiból adódóan, éppen ezért kedvező feltételeket biztosít azok számára is, akik amúgy az adott piacról kiszorulnának. Továbbá a kontroll mechanizmus még nehezebbé vált, mert a tagok között nincs szükség személyes kapcsolattartásra – sőt általában kizárólag elektronikus csatornákon keresztül kommunikálnak egymással – és a csoport működéséhez nem kellenek a formális szervezeti keretek (pl. a klasszikus hierarchikus szervezeti struktúra nem megfelelő a kiberbűnelkövetők számára). Az új típusú szervezett bűnözés működése a digitális környezetben hasonlóságot mutat a modern vállalati világhoz különösen, ami az alkalmazott árazási stratégiát, szolgáltatás-alapú versenyt, innovációt és az „ügyfélszolgálatot" illeti. A kiberbűnözői csoportok ereje a rendelkezésre álló szoftver fejlettségben rejlik és nem a csoport tagjainak a számában. Az alkalmazott automatizált műveletek nem csak a bűncselekmények elkövetéséhez és az online feketepiacok létrejöttéhez járultak hozzá, hanem a szervezeti struktúrára nézve is meghatározó tényezővé váltak, mert az emberek helyett a technológia került a középpontba.

A kiberbűnözőkre jellemző, hogy egyre nagyobb mértékben veszik át és másolják a legális vállalatok üzleti modelljeit, a 2000-es évek óta fejlesztenek ki olyan üzleti mintákat, amelyek az eBay, Yahoo, Google és az Amazon high-tech cégek által használtakhoz hasonló. A „kiberbűnözői iparágat" már a professzionalitás és kifinomultság határozza meg a különféle kibertámadások terén, illetve a specializáció vagyis munkamegosztás az elkövetők között, a kommercializáció és az integráció, ami azt jelenti, hogy az egyes jogsértéseket további jogsértés követi mint például az adatlopást követően eladható a megszerzett adat, majd azt csalásra használhatják fel.

Az vitatott, hogy az informatikai bűnözés által megteremtett üzleti modell és a legálisan működő vállalkozások között milyen eltérések mutatkoznak: míg utóbbi a vásárlók számára az értékteremtést célozza, addig a kiberbűnözés magában foglalja az áldozatok kijátszását a kreatív csalások révén és a kockázat minimalizálását arra vonatkozóan, hogy az illegális tevékenységüket elfedjék. Azonban, ha az informati-

kai bűnözést olyan modellnek tekintjük, ami kapcsolatot teremt az illegális eszközök, szolgáltatások „beszállítója" és a vásárlók között, akik ezeket bűncselekmények elkövetésére használják fel az áldozatokkal szemben, akkor ez a különbség nem jelentős, hiszen ez a rendszer is arra összpontosul, hogy értéket teremtsen a „fogyasztói" részére, akik azonban jelen esetben a kiberbűncselekmények elkövetői lesznek.

Az innováció eredményeképpen, a bűnözői ökoszisztémában új minták jelentek meg – amit mindkettő csoport ki is használ – mint például az áruk elhelyezésével, alvállalkozásokkal és kapcsolatépítéssel kapcsolatban. Olyan üzleti modellt alkalmaznak (Criminal-to-Criminal), amely hasonlóságot mutat a jogszerűen működő vállalkozásokéhoz (Business-to-Business), azonban ennek középpontjában az egymás közötti illegális áruk adásvétele és a tiltott szolgáltatások nyújtása áll az informatikai hálózatokon keresztül.[32]

Az automatizáció jelentős szerepet játszik a C2C modellek fejlődésében, mert idő- és költséghatékonyabbá teszi a működésüket. Az automatizált bűnözői tevékenységek alapját a botnet hálózatok képezik, amelyek a felhasználók tudta nélkül megfertőzött számítógépekből állnak és ezek az elkövetők által távolról irányíthatók mint egy „zombigépként". A használatuk révén akár nagyszabású támadásokat indíthatnak (pl. DDoS támadást[33]), különböző rosszindulatú programokat tudnak terjeszteni, vagy nagy mennyiségű személyes, illetve egyéb bizalmas adatokhoz is hozzájuthatnak a spamküldések és az adathalász technikák alkalmazásával.[34]

5. Specializáció és munkamegosztás

A kiberbűnözői iparág széleskörű tevékenységi kört ölelhet fel, amelyben az elkövetők funkcionálisan specializálódnak az egyes feladatokra, tehát jelen van munkamegosztás és ez a következőképpen alakulhat:

A programozók azok, akik a különböző rosszindulatú programokat (malware) írják meg és egyéb eszközöket rendelkezésre bocsátják, amelyek a bűncselekmények elkövetéséhez szükségesek.

[32] Tropina, Tatiana: The evolving structure of online criminality. eucrim 2012/4. 160-162. o.

[33] A DDoS támadás (Distributed Denial of Service) vagy másnéven szolgáltatásmegtagadással járó támadás egy olyan támadási forma, amelynek a célja az információs rendszerek, szolgáltatások vagy hálózatok erőforrásainak oly mértékben történő túlterhelése, hogy azok elérhetetlenné váljanak, vagy ne tudják ellátni az alapfeladatukat. Az ilyen elektronikus támadást intézők a jogosult felhasználókat akadályozzák a szolgáltatás igénybevételében. Nagy Zoltán András: Bűncselekmények számítógépes környezetben. Ad Librum, Budapest, 2009. 115.o. http://www.cert-hungary.hu/ddos [2018.03.05.]

[34] Tropina: i.m. 160. o.

A forgalmazók vagy eladók, akik kereskednek és eladják a lopott adatokat és szavatolják az árukat, amiket mások biztosítanak a számukra.

A technikusok, akik fenntartják a bűnözői infrastruktúrát, a technológiai támogatást biztosítják mint például a szerverek és a titkosítás zavartalan működését. A gazdagép (host), az a hálózatra csatlakoztatott számítógép, amely az illegális tartalmakat biztosító szervereket és hálózatokat kezeli sokszor botnetek és proxy hálózatok révén.

A hackerek, akik a sebezhetőségeket keresik a rendszerekben, programokban, illetve hálózatokban azzal a céllal, hogy rendszergazda szintű jogosultságot vagy ún. „root level access", illetve „god level access" szintű hozzáférést szerezzenek.

A csalás specialisták pedig különböző ún. social engineering[35] sémát dolgoznak ki és alkalmazzák azokat mint például a phishing és a spam küldés is ilyen.

A „pénztárosok" kezelik a bűnös eredetű pénzt és a hozzá tartozó fiókokat, és más bűnözők számára is biztosítják ezeket megfelelő díjazás fejében, továbbá általában ők felügyelik az önálló pénzfutárok, ún. „money mule"-ok tevékenységét is.

A pénzfutárok segítenek a bűncselekményekből befolyt bevételeknek az átutalásában harmadik félnek, hogy az további utalással biztonságosan elhelyezze a pénzt. Vannak olyan személyek, akik az átutalásokért és a pénz tisztára mosásáért felelnek digitális valuták és különböző országok pénznemei közötti átváltásokkal.

Végül a végrehajtók azok, akik kiválasztják a célpontokat, toboroznak és kijelölik a tagokat az említett feladatokra, ezen felül pedig a bűncselekményekből származó bevételek elosztásáért felelnek.[36]

6. Az online feketepiacok és fórumok

A kiberbűnözés egy profit-orientált, szolgáltatás-alapú üzleti modellé (Crime-as-a-Service) nőtte ki magát, amely által elérhetővé váltak olyan szolgáltatások a Surface Weben[37] vagy a Darkneten[38], melyekkel bármilyen kiberbűncselekmény elkövet-

[35] Mitnick, Kevin D.: A megtévesztés művészete című könyvnek a borítója: „A social engineering a befolyásolás és rábeszélés eszközével megtéveszti az embereket, manipulálja, vagy meggyőzi őket, hogy a social engineer tényleg az, akinek mondja magát. Ennek eredményeként a social engineer – technológia használatával vagy anélkül – képes az embereket információszerzés érdekében kihasználni."

[36] Chabinsky, Steven R. (2010): https://archives.fbi.gov/archives/news/speeches/the-cyber-threat-whos-doing-what-to-whom [2018.03.05.]

[37] A hagyományos böngészők használatával szabadon elérhető része az internetnek.

[38] A Darknet egy elosztott, anonimitást biztosító, titkosított hálózat a Deep Weben belül, ami kizárólag speciális szoftverek használatával érhető el mint például a The Onion Routerrel (TOR), I2P-vel vagy Freenettel, amelyek magasfokú titkosítással vannak ellátva. A bűnelkövetők kihasználják ezeket, mert a használatuk révén könnyedén eltudják rejteni a személyazonosságukat, az internetes forgalmukat és a szerverük helyét.

hető. Ahogy már korábban említésre került ezt az üzleti modellt az önálló kiberbűnözőktől kezdve – akik számára az internet lehetővé teszi a szervezeti kerethez kötöttség nélküli tevékenység végzését – a szervezett kiberbűnözői üzleti társulások vagy akár a tradicionális szervezett bűnözői csoportok is alkalmazhatják. Utóbbiak, amennyiben nem rendelkeznek a szükséges technikai ismeretekkel és eszközökkel, akkor ők is megtudják vásárolni a fórumokon keresztül, akár a kiberbűnözőktől.

A különböző illegális online tevékenységek egy egyre fejlettebb és önálló digitális feketegazdaságot hoztak létre, amelyen belül speciális weboldalakat üzemelnek, ún. online feketepiactereket és fórumokat, amelyeket arra használnak, hogy a tilalmazott árukkal kereskedjenek és szolgáltatásokat hirdessenek, amiket együttesen „hidden services"-nek, azaz rejtett szolgáltatásoknak hívnak.

A piactereken és fórumokon belül gyakran jelen van egy merev és egyedülálló struktúra, ami a kijelölt szerepekkel, feladatmegosztással és az eltérő felelősséggel lehetővé teszi, hogy a tagok hatékonyan biztosítsák a fórum működésének a rendjét. Ezeket a fórumokat az adminisztrátorok irányítják, akik meghatározzák az adott fórum célját és a működéshez szükséges szabályokat. Az alfórumokat pedig moderátorok ellenőrzik, akik megbízható személyek, gyakran az alfórum témájában jártas szakemberek és ezért annak a tartalmát kezelik. A fórumokon találhatók nagyszámú eladók is, akik különféle szolgáltatásokat nyújtanak és a termékekkel kereskednek a fórum tagjaival. Az eladói státusz eléréséhez általában próbamintát kell a moderátorok számára nyújtani, akik értékelik azt, majd később a szolgáltatás vagy termék további folyamatos értékelést és pontozást kap a vásárlóktól. Az értékelést és visszajelzést biztosító rendszer hasonló a legális kereskedelmi oldalakéhoz azzal a kivétellel, hogy a bűnözők számára a magas értékelés, vagyis „a jó hírnév" elérése nem olyan egyszerű. Lényegében ezek az online fórumok biztosítják a szükséges logisztikát a felhasználók számára, hogy különféle kiberbűncselekmény elkövetésében részt vehessenek a megszerzett ismeretek és eszközök révén.[39]

Az illegális árukkal való kereskedésnek a Darkneten keresztül számos előnye van mind az eladók és mind a vásárlók részéről is. A Peer-to-Peer (P2P) technológiára épülő platformoknak köszönhetően az eladók és a vásárlók is közvetlenül kapcsolatba tudnak lépni egymással és közvetítő nélkül tranzakciókat folytathatnak le. Ezeket magasfokú anonimitás jellemez, amely során egyik félnek sem kell személyes adatot megadnia, bár a vásárló számára a fizikai áruk vásárlásakor nyilván meg kell adni egy szállítási címet, azonban manapság a kézbesítés különböző anonim he-

[39] Europol: The Internet Organised Crime Assessment (IOCTA) 2014. 19-21. o. https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2014 [2018.03.25.]

lyekre is történhet (pl. csomag automatákba), így az áruk átvételekor is biztosítható az áruért érkező személy anonimitása. A tranzakciók lebonyolításához nehezen lenyomozható ún. virtuális fizetőeszközöket használnak mint például ilyen a Bitcoin és az egyéb altcoinok (pl. Etherum, Zcash, Monero). Használatuk népszerű, mert pszeudoanonimitást biztosítanak, ami azt jelenti, hogy az utalások végrehajtásához nincs szükség azonosításra, illetve hitelesítésre, ezáltal azok nem köthetők konkrét személyekhez. További előnyként említhető, hogy decentralizáltak, vagyis központi felügyeleti szerv nélkül működnek, tehát nem tartoznak egy jegybankhoz vagy országhoz sem, ami a nyomozást tovább nehezíti, mert a nyomozó hatóságok nem tudnak kihez fordulni mint mondjuk egy pénzintézet esetén. A kriptovaluták kihívást jelentenek, mert nincs egységes jogi szabályázásuk és országonként eltérő a megítélésük: kérdéses, hogy pénznek, árunak vagy vagyoni értékű jognak tekinthetők-e. Általában fizetőeszközként funkcionálnak, amikor használatuk az illegális tevékenységekhez kapcsolódik, valamint pénzmosási és terrorizmusfinanszírozási kockázatot jelentenek.[40] Külön érdekesség, hogy a büntetőeljárásról szóló új 2017. évi XC. törvény már külön nevesíti az elektronikus adatot a bizonyítási eszközök között.[41] A 315. §-ban pedig kialakította az ún. virtuális vagyontárgyak biztosításának a keretszabályait, amely alapján a virtuális fizetőeszközök mint a Bitcoin, valamint az elektronikus pénz egyes típusai is a jövőben lefoglalás tárgyát képezhetik.[42]

Az online feketepiacokon, illetve fórumokon jellemzően az alábbi áruk adásvétele zajlik: kábítószer, gyermekpornográf tartalmak, hamis és hamisított áruk, fegyverek és crimeware.

6.1. Kábítószer-kereskedelem

A kábítószer-kereskedelem továbbra is a legnagyobb illegális piacnak számít és egyre több hagyományos szervezett bűnözői csoport vesz részt a különféle kábítószer előállításban, forgalmazásban és terjesztésben, amely során az internet nyújtotta előnyöket is kihasználják. A különböző feketepiacok fő profilját is a kábítószer adja mint például ilyen híres online „bazár" volt a Silk Road és az Alphabay is. Az egyes tanulmányok szerint a havi bevétele az első nyolc Darknet piactérnek 10,6 millió és 18,7 millió euró között mozog, amely kizárólag a kábítószer-kereskedelemből szár-

[40] Szathmáry Zoltán: Az elektronikus pénz és a bitcoin biztosítása a büntetőeljárásban. Magyar Jog 2015/11. 639-647. o. https://fintechzone.hu/rendvedelmi-szervek-latokoreben-a-kriptovalutak/ [2018.04.30.]

[41] Lásd a digitális adatokról Fenyvesi Csaba: Az új generációs bizonyítékok a kriminalisztika történeti mérföldköveinek tükrében. Magyar Jog 2014/7-8. 441-442. o.

[42] Dornfeld László: A kibertérben elkövetett bűncselekményekkel összefüggésben alkalmazható kényszerintézkedések. Belügyi Szemle 2018/2. 126. o.

mazik.[43] A kábítószer-kereskedelmet a Btk. 176.§-ban szabályozza, mely szerint, aki kábítószert kínál, átad, forgalomba hoz, vagy azzal kereskedik, bűntett miatt két évtől nyolc évig terjedő szabadságvesztéssel büntetendő.

A kábítószer-kereskedelmen (Btk. 176.§) kívül szóba jöhetnek még a hazai szabályozás értelmében a következő bűncselekmények, amelyek a tiltott szerekhez kapcsolódnak: a kábítószer készítésének elősegítése (Btk. 182.§), kábítószer-prekurzorral visszaélés (Btk. 183.§), új pszichoaktív anyaggal visszaélés (Btk. 184.§), teljesítményfokozó szerrel visszaélés (Btk. 185.§), valamint a gyógyszerhamisítás (Btk. 185/A.§).

6.2. Gyermekpornográfia

A gyermekpornográf tartalmak készítése, illetve azzal való kereskedés jövedelmező üzletté vált, amit a szervezett bűnözői csoportok is felismertek és kihasználnak. A Darkneten keresztül hirdetik és terjesztik a tiltott pornográf tartalmakat vagy külön weboldalakat hoznak létre haszonszerzési céllal. Új trendként jelent meg, hogy a gyermekmolesztálást az interneten keresztül élőben közvetítik, vagyis „streamelik". Az online tevékenység célja egyben lehet az offline szexturizmus iránti igény felkeltése is. A Btk. 204.§ (1) bekezdés a)-c) pontja értelmében, aki tizennyolcadik életévét be nem töltött személyről vagy személyekről pornográf felvételt megszerez vagy tart, készít, kínál, átad vagy hozzáférhetővé tesz, forgalomba hoz, azzal kereskedik, illetve ilyen felvételt a nagy nyilvánosság számára hozzáférhetővé tesz az gyermekpornográfia bűntette miatt két évtől nyolc évig terjedő szabadságvesztéssel büntetendő.

6.3. Hamis és hamisított termékekkel kereskedés

Az Europol szerint a hamis és hamisított termékek is népszerűek, amelyek széles skálája elérhető mind a Surface Weben és a Darkneten is: ruházati termékek, ékszerek, „kalóz" szoftverek, gyógyszerkészítmények, előfizetések különböző TV és zenei platformokhoz, online játék fiókokhoz, valamint a legkeresettebb termékek közé tartoznak a hamis pénzek és személyazonosító okmányok.

6.4. Crime-as-a-Service üzleti modell

A Crime-as-a-Service üzleti modellt követve az online feketepiacokon különböző szolgáltatások érhetők el, így a következők:

[43] Europol (2017): i.m. 49-50. o.

Infrastruktúra mint szolgáltatás (Infrastructure-as-a-Service): az informatikai támadások végrehajtásához szükség van egy védett infrastruktúrára, ami biztosítja a biztonságot, anonimitást és ellenállást a bűnüldöző hatóságok beavatkozásai elől. A tárhelyszolgáltatók (hosting providers), különösen az ún. „bulletproof hosting" szolgáltatások népszerűek, mert lehetőséget biztosítanak arra, hogy a felhasználók szabadon feltöltsék a kívánt tartalmat anélkül, hogy azokat eltávolítanák, még akkor is, ha illegálisnak minősülnek. Éppen ezért kulcsfontosságú szerepük van az online feketepiacok esetében, mert biztonságos tárhelyet biztosítanak a crimeware-nak, az ellopott adatoknak és egyéb illegális tartalmaknak. A VPN, vagyis a virtuális magánhálózat és a proxy szolgáltatások pedig fontos szerepet játszanak az anonimitás biztosításában, ezáltal segítenek a bűnüldöző szervek kijátszásában.

Az adat a legkeresettebb áru manapság. Nagy mennyiségű személyes és pénzügyi adatok adásvétele zajlik a digitális feketegazdaságban.[44] Az adat befolyásolja az illegális piacok fejlődését: meghatározott bűnözői tevékenységeket fejlesztettek ki, illetve folyamatosan dolgoznak azon, hogy javítsák, jobbá tegyék ezeket, annak érdekében, hogy hatékonyan szerezzék, „lopják el" ezeket az érzékeny adatokat (pl. phishing, malware és egyéb eszközök használatával a kereskedelmi, pénzügyi adatbázisokkal szembeni támadásokhoz).[45] A bankkártya és bankfiók adatokon kívül elérhetőek lakcímek, telefonszámok, e-mail címek, e-pénztárcák, társadalombiztosítási azonosítók és egyéb online felhasználó fiókokhoz kapcsolható adatok, különösen, amelyekhez pénzmozgás köthető.

Pay-per-install szolgáltatások népszerű módszerei a malware terjesztésnek, ami úgy működik, hogy akik a szolgáltatást nyújtják, azok terjesztik a rosszindulatú fájlokat, amiket pedig a szolgáltatást igénybe vevők biztosítanak a számukra és a letöltések száma utána fizetnek nekik. Az ilyen szolgáltatások országspecifikus forgalmat biztosíthatnak. További népszerű szolgáltatás, hogy a DDoS támadások indítására szolgáló botneteket, illetve a létrehozásukra szolgáló eszközöket, programokat lehet igénybe venni (DDoS-for-hire vagy DDoS-as-a-Service) – napi vagy havi díjjal átlagosan 5$ és 1000$ közötti áron.[46] Hasonlóképpen a különböző rosszindulatú programokhoz (pl. vírusokhoz) is hozzá lehet jutni szolgáltatásként mint például a legkönnyebb pénzszerzési módhoz: a zsarolóvírushoz (Ransomware-as-a-Service). A legnagyobb veszélyt pedig az egyedi hatású és célzott támadásokra kifejlesztett kártékony programok jelentik különösen, amelyek a kritikus infrastruktúrákat célozzák és ezek is már elérhetőek a feketepiacokon (pl. a Stuxnet ismertté válásával

[44] Europol (2014): i.m. 19-21. o.
[45] Tropina: i.m. 162. o.
[46] Europol: (2014): i.m. 19-21. o.

„közkinccsé vált", ezután annak elemei kikerültek a „szabadpiacra" és tovább fejlesztve már hasonló mechanizmusokat tartalmazó malware-ek is elérhetővé váltak mint a DuQu).[47]

Azért különösen veszélyes a Criminal-as-a-Service üzleti modell, mert könnyen hozzá lehet jutni a kiberbűncselekmények elkövetéséhez szükséges ismeretekhez, programokhoz, akár kész bűnözői infrastruktúrához, és ezért is fontos, hogy már az előkészületi cselekmények sui generis bűncselekményként kerüljenek meghatározásra. Hiszen a szolgáltatás igénybevételével a hozzá nem értő felhasználók is olcsón, egyszerűen és gyorsan tudnak támadást indítani, sokszor csak egy egérkattintás az egész, sőt a végrehajtáshoz még technikai segítséget is kapnak. Ennek megfelelően a Btk. 424.§-ban szabályozza az információs rendszer védelmét biztosító technikai intézkedés kijátszásának vétségét, melynek értelmében büntetendő, aki a Btk. 375.§ szerinti információs rendszer felhasználásával elkövetett csalás, a 422.§ (1) bekezdés d) pontjában szabályozott tiltott adatszerzés vagy a 423.§-ban meghatározott bűncselekmény elkövetése céljából az ehhez szükséges vagy ezt könnyítő jelszót vagy számítástechnikai programot készít, átad, hozzáférhetővé tesz, megszerez vagy forgalomba hoz; valamint aki, a jelszó vagy számítástechnikai program készítésére vonatkozó szervezési ismeretet más részére rendelkezésére bocsát. A megszerzett ismeretekkel kiberbűncselekményeket tudnak elkövetni, amit a Btk. a 423.§-ban az információs rendszer vagy adat megsértése bűncselekmény körében szabályozza a jogosulatlan vagy jogosultság keretének túllépésével elkövetett módozatokat, így az (1) bekezdés a jogosulatlan belépést (ún. hacking), (2) bekezdés a) pontjában az információs rendszer akadályozását (pl. DDoS támadás), valamint a b) pontjában az adat megváltoztatását, törlését vagy hozzáférhetetlenné tételét, végül a (3) és (4) bekezdés szerinti minősített esetek valósulnak meg, ha jelentős számú információs rendszert (pl. botnet alkalmazása), illetve közérdekű üzemet érint a bűncselekmény.

Hacking mint szolgáltatás (Hacking-as-a-Service): Alap szinten ez magában foglalhatja az e-mail vagy közösségi oldalak fiókjainak a feltörését vagy összetettebb támadásokat mint a gazdasági kémkedés vagy személyes adatok gyűjtését a meghatározott célponttól.

Fordításokhoz kapcsolódó szolgáltatások: A támadások sokszor országspecifikusak és előfordulhat, hogy az elkövető nem feltétlenül beszéli a célország nyelvét, ezért igénybe vehet szolgáltatást fordítóktól, akik helyesen megfogalmazott szöve-

[47] Nagy Zoltán András: A kiber-háború új dimenzió – a veszélyeztett állambiztonság (Stuxnet, DuQu, Flame – a Police malware). In: Gaál Gyula-Hautzinger Zoltán (szerk.): Pécsi Határőr Tudományos Közlemények XIII. 2012. 227-228. o.

geket nyújtanak nekik, ezzel maximalizálva a támadás sikerét, mert sok esetben éppen a nyelvtani pontatlanságok lehetnek árulkodó jelei a csalásnak.

Pénzmosás mint szolgáltatás (Money laundering-as-a-Service): A bűnözők nem csak saját maguk javára végeznek pénzmosást, hanem szolgáltatásként is elérhető általuk az meghatározott díj ellenében.[48] Azért, hogy „tiszta" profitra tegyenek szert az illegális tevékenységükből a „piszkos pénzek" tisztára mosásához különféle szolgáltatásokat vehetnek igénybe annak érdekében, hogy ezeket a legális gazdaságba vissza tudják forgatni.[49] Ezek a szolgáltatások magukban foglalják az online és offline megoldások kombinációit, amelyeknek a középpontjában általában a pénzfutárok hálózatok állnak. A „money mule" elnevezéssel ismert új pénzmosási technika a pénzintézetekkel történő kapcsolatfelvételt iktatja ki és egy harmadik személy – azaz a pénzhordó személy – közreműködésével terítik, bújtatják a bűncselekményből eredő „piszkos pénzt". Az elkövetők munkaszerződést ajánlanak a pénzfutárnak, amelynek keretében a megkeresett fél „munkája" annyi lenne, hogy saját bankszámláján jelentősebb összegeket kell fogadnia, majd azt készpénzben felvenni, vagy a „munkáltató" által megadott számlákra továbbutalni magas jutalékért cserébe. Indokolt tehát a fokozott óvatosság, hiszen aki akár az igen vonzónak tűnő ajánlatot elfogadja, maga is érintetté válik a pénzmosás bűncselekmény elkövetésében.[50] A pénzmosásnak (Btk. 399.§) a három fázisa, így az elhelyezés, rétegzés és az integráció ezekben az esetekben is megvalósul. Ezzel szoros összefügésben új trendként jelent meg, hogy a nagyobb összegek tisztára mosása úgy történik, hogy azt kisebb összegű tranzakciókra bontják (micro money laundering), melynek előnye, hogy kevésbé feltűnő, mert a sok kicsi sokra megy elvet követi.[51]

7. Egyéb illegális tevékenységek

7.1. Online szerencsejáték

A hagyományos szervezett bűnözői csoportok számára népszerű bevételi forrást jelentenek az általuk üzemeltetett különböző online szerencsejáték oldalak is, amelyek alkalmasak az illegális bevételek tisztára mosására. A virtuális hálózatokon is,

[48] Europol (2014): i.m. 19-21. o.

[49] Tóth Mihály: Gazdasági bűnözés és bűncselekmények. KJK-KERSZÖV Jogi és Üzleti Kiadó Kft. Budapest, 2002. 375. o.

[50] Europol (2014): i.m. 19-21. o.; Kármán Gabriella – Mészáros Ádám – Tilki Katalin: Pénzmosás a gyakorlatban. Ügyészségi Szemle 2016/3. 88. o.

[51] Maras: i.m. 336. o.

akár a valós térben elterjedtek a különféle szerencsejátékok és fogadási oldalak. Általában az ismeretlen felhasználókkal korrektnek nevezhető módon játszanak, de a „bennfentes" felhasználók csak vesztenek, azaz csak befizetnek oda.[52]

7.2. A zsarolás új formái

A DDoS támadásokat zsarolási céllal is felhasználják, amely során olyan cégek oldalait választják ki, amelyek folyamatos és zavartalan működést követelnek meg (pl. webshopok, online szerencsejáték és fogadó cégek, energia- és pénzügyi szféra) és ezekkel szemben kisebb támadást indítanak, és a további erőteljesebb – akár teljes rendszer leállást eredményező – támadások elkerülése érdekében Bitcoint kérnek fizetségért. 2016-ban az Europol sikeres akciót hajtott végre és letartóztatta a zsarolásokban élen járó DD4BC (Distributed Denial of Service for Bitcoin) Team hacker csoportnak a kulcsfontosságú tagjait, akik számos DDoS támadást indítottak szervezetten európai cégekkel szemben.[53] Ezen kívül a túlterheléses támadással történő zsarolás a terroristák fegyvertárába is tartozik.[54]

Europol továbbá figyelmeztet a zsarolás új formájára, amikor a kiszemelt sértettektől kompromittáló képfelvételeket szereznek meg például a közösségi médián keresztül a bizalmukba férkőzve majd a felvételek megosztásával fenyegetnek, amennyiben meghatározott összeget Bitcoinban nem fizetnek. Ezek az esetek egyre növekvő számban bűnszervezetekhez köthetők, akik mint egy „call center"-t működtetnek haszonszerzési céllal.[55]

8. Összefoglalás

A bűnelkövetők gyorsan átveszik és integrálják az új technológiákat a különböző bűncselekmények elkövetésekor és új üzleti modellt alkalmaznak, amelyeknek az alapját egyre inkább az internet használata jelenti. A hagyományos szervezett bűnözői csoportok esetében is megfigyelhető a modern technológiák kihasználása, amely magában foglalja az interneten történő terjeszkedést mint például az illegális online kereskedelmet és a széles körben hozzáférhető, titkosított kommunikációs csator-

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

[53] Conneller, Philip (2016): https://www.cardschat.com/news/pokerstars-ddos-attackers-arrested-by-Europol-extortion-group-also-alleged-to-have-targeted-betfair-neteller-18629 [2018.04.18.]

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

[55] Europol (2017): i.m. 35. o.

nák használatát és egyéb informatikai újításokat. Megállapítható, hogy az új technológiai vívmányok lényeges és maradandó hatással vannak a bűnözés természetére.

Az is kétségtelen tény, hogy az informatikai bűnözés egy hatalmas profit-orientált és szolgáltatás-alapú üzletté nőtte ki magát, azonban az még mindig nem világos, hogy ez a piac milyen mértékben van az egyes tradicionális szervezett bűnözői csoportok kezében, illetve mennyiben tekinthető az új típusú kiberbűnözői csoportok tevékenysége szervezett bűnözésnek egyáltalán. Ugyanis a szervezett bűnözés és az informatikai bűnözés kapcsolatára vonatkozóan még mindig nincs egy világos koncepció, különösen azért, mert nehéz a szervezett bűnözés hierarchikus, homogén struktúrájába az informatikai bűnözést beilleszteni. A „kiberbűnözői ipar" rendkívül erőssé és fejletté vált, azonban még mindig a fejlődésének korai szakaszában van, éppen ezért kevés a rendelkezésre álló adat, különösképpen a szervezettségi szintjére vonatkozóan.

Összességében elmondható, hogy az internet helyszínül szolgál mind a régi és mind az új típusú „szervezett" bűnözésnek, illetve mindkettő egymás mellett tud működni anélkül, hogy egymást zavarnák és ez köszönhető a virtuális tér speciális jellegének.

A jogalkotók, jogalkalmazók és a nyomozó hatóságok számára egyaránt kihívást jelent a titkosítást és anonimitást biztosító eszközök bűnelkövetési célú felhasználása, így különösen a kriptovatulák, az online feketepiacok és fórumok, melyek szabályozására szükség lenne, illetve a bűnüldöző szervek részéről kiemelten fontos, hogy biztosítsák az egymás közötti[56] és a magánszektorral való szoros együttműködést a hatékony fellépés érdekében.

Felhasznált Irodalom

Abadinsky, Howard: Organized crime. Ninth Edition, Wadsworth Cengage Learning, 2010.

Ambrus István: Egység és halmazat – régi dogmatikai kérdés új megközelítésben. Szeged, SZTE ÁJK, 2014.

Belegi József: A közbiztonság elleni bűncselekmények – Btk. XXX. fejezet. In: Kónya István (szerk.): Magyar büntetőjog I-III. – új Btk. – Kommentár a gyakorlat számára. 5. kiadás, HVG Orac Lapkiadó Kft. 2016.

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

Clough, Jonathan: Principles of Cybercrime. Cambridge University Press, 2015.
Csák Zsolt: Társas elkövetés, különös tekintettel a bűnszervezetre. In: Benisné Győrffy Ilona (szerk.): Negyvenegyedik Jogász Vándorgyűlés. Budapest, 2018.
Dornfeld László: A kibertérben elkövetett bűncselekményekkel összefüggésben alkalmazható kényszerintézkedések. Belügyi Szemle 2018/2.
Europol: European Union Serious and Organised Crime Threat Assessment (SOCTA) – Crime in the age of technology. 2017.
Europol: Internet Organised Crime Threat Assessment (IOCTA) 2017.
Europol: The Internet Organised Crime Assessment (IOCTA) 2014.
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.
Gyaraki Réka: A számítógépes környezetben elkövetett gazdasági bűncselekmények – A PIN kód megadása sikeres vagy biztonságos az internet?! Pécsi Határőr Tudományos Közlemények XIII. Pécs, 2012.
Kármán Gabriella – Mészáros Ádám – Tilki Katalin: Pénzmosás a gyakorlatban. Ügyészségi Szemle 2016/3.
Kim-wang, Raymond – Choo-Grabosky, Peter: Cybercrime. In: Paoli, Letizia: The Oxford Handbook of Organized Crime. Oxford University Press, 2014.
Korinek László: A szervezett bűnözés lényegi elemei. In: Harmadik Magyar Jogászgyűlés – Magyar Jogász Egylet. Budapest, 1996.
Korinek László: A technika fejlődése és a bűnözés. In: Borbíró Andrea – Inzelt Éva – Kerezsi Klára – Lévay Miklós – Podoletz Léna (szerk.): A büntető hatalom korlátainak megtartása: A büntetés mint végső eszköz – Tanulmányok Gönczöl Katalin tiszteletére. ELTE Eötvös Kiadó. Budapest, 2014.
Malas, Marie-Helen: Cybercriminology. Oxford University Press. New York, 2017.
McGuire, Michael: Organised Crime in the Digital Age. London: John Grieve Centre for Policing and Security. 2012.
Nagy Zoltán András: A 2013/40-es Uniós direktíva az informatikai rendszereket érő támadásokról.
Nagy Zoltán András: A kiber-háború új dimenzió – a veszélyeztett állambiztonság (Stuxnet, DuQu, Flame – a Police malware). In: Gaál Gyula-Hautzinger Zoltán (szerk.): Pécsi Határőr Tudományos Közlemények XIII. 2012.
Nagy Zoltán András: A szervezett bűnözői jelenségek a számítógépes hálózatokon. Belügyi Szemle 2012/6.
Nagy Zoltán András: Bűncselekmények számítógépes környezetben. Ad Librum, Budapest, 2009.

NAGY Zoltán András: A számítógéppel megvalósítható vagyoni jogsértésekről. Bűnügyi Műhelytanulmányok 1992/1.

SIMON Béla: A rendészeti szervek együttműködése a kiberbűnözés ellen. Nemzetbiztonsági Szemle 2018/1.

SZATHMÁRY Zoltán: Az elektronikus pénz és a bitcoin biztosítása a büntetőeljárásban. Magyar Jog 2015/11.

TÓTH Mihály – KŐHALMI László: A szervezett bűnözés. In: Borbíró Andrea – Gönczöl Katalin – Kerezsi Klára -Lévay Miklós: Kriminológia. Wolters Kluwer Kft. Budapest, 2016..

TÓTH Mihály: A bűnszervezeti elkövetés szabályozásának kanyargós útja. Magyar Jog 2015/1.

TÓTH Mihály: A gazdasági bűnözés és bűncselekmények néhány aktuális kérdése. MTA Law Working Papers 2015/4.

TÓTH Mihály: Bűnszövetség, bűnszervezet. Complex Kiadó Kft. Budapest, 2009.

TÓTH Mihály: Gazdasági bűnözés és bűncselekmények. KJK-KERSZÖV Jogi és Üzleti Kiadó Kft. Budapest, 2002.

TROPINA, Tatiana: The evolving structure of online criminality. eucrim 2012/4.