7. Kiberbűnözés

Simon Béla – Gyaraki Réka

7.1. A szervezett bűnözés

A szervezett bűncselekmények fogalmát a Büntető Törvénykönyvről szóló 2012. évi C. törvény bűnszervezetként határozza meg, és eszerint olyan, a három vagy több személyből álló, hosszabb időre szervezett, összehangoltan működő csoport, amelynek célja az ötévi vagy ezt meghaladó szabadságvesztéssel büntetendő szándékos bűncselekmények elkövetése.[1] A bűnszervezetek jellemzője tehát, hogy több, egymással kapcsolatban álló személy összehangoltan működő (centralizált), a tagok között rendszeres kapcsolatot fenntartó, leginkább anyagi haszonszerzésre törekvő, jogellenes tevékenységüket a törvényesség látszata mögé rejtő bűnözők csoportja. Ugyanakkor a jogszabály nem áll meg ennél a fogalomnál, hiszen megemlíti még a bűnszövetséget és a csoportos elkövetést is. Ez utóbbi két szervezettségi forma esetében nemcsak az elkövetők száma, hanem az elkövetett cselekményben részt vevő személyek is – azaz hogy a kettő, három vagy annál több személy úgy követi el a deliktumot, hogy nem jön létre bűnszövetség – szerepet játszik a bűnszövetség megállapításánál.

A szervezett bűnözés általános jellemzői:

- a jól konspirált és szervezett elkövetés;
- legális tevékenységekkel leplezik magukat;
- a tanúk megfélemlítése, lefizetése (megsemmisítése);
- nagy anyagi, technikai és emberi erőforrásokkal rendelkeznek;
- a bűnszervezetek elfogott tagjai nem működnek együtt a büntetőeljárásban a hatóságokkal;
- a végrehajtók elkülönülnek a fő irányítóktól (több szint létezik);
- az egyes szintek nem feltétlenül ismerik egymást, vagy leplezett módon kommunikálnak.

A kiberbűncselekmény általános fogalma alatt az informatikai eszközök és/vagy rendszerek segítségével vagy az informatikai eszközök és hálózatok ellen elkövetett bűncselekmények értendők, amelyek célja lehet a rendszerben tárolt adatok megszerzése, a jogosultak számára hozzáférhetetlenné tétele, továbbá az elektronikus rendszerbe vetett bizalommal történő visszaélés. De e jellemzők mellett még a folyamatosan fejlődő kiberbűnözés miatt számtalan jellemzőt lehet majd még említeni.

[1] Btk. 459. § (1) bekezdés.

https://doi.org/10.36250/00782_07

A kiberbűncselekmények céljai:
- anyagi haszonszerzés,
- a tárolt elektronikus adatok illetéktelen felhasználása, az azzal történő visszaélés,
- politikai motiváció,
- üzleti vagy politikai ellenfelek egymás irányába történő erőfitogtatása,
- üzleti és/vagy politikai hírszerzés.

Az ilyen típusú bűncselekmény elkövetési helye maga a kibertér, vagy – bár a virtuális térhez kapcsolódik az elkövetés, de – leginkább az elektronikus információs rendszer felhasználásán van a hangsúly, mégis a fizikai térben történik maga a bűncselekmény. Amikor kizárólag a virtuális térben történik az elkövetés, mint az információs rendszerbe történő jogosulatlan behatolás vagy kifürkészés, 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, az anonimitásnak és a magas fokú látenciának köszönhetően a nyomozás és felderítés szinte lehetetlenné válik. Azokban az esetekben, amikor az elkövetők leginkább az információs rendszert, a kiberteret az elkövetés eszközeként használják, mint például a hirdetéses csalások, zaklatás, gyermekpornográfia esetében a szervezett bűnözői körök sokkal több nyomot hagynak maguk után, így a hatóságok megfelelő felkészülése, tudatossága esetén az elkövető megismerése és felderítése eredményesebb lesz.

A következő bűncselekmények tekintetében jellemző a szervezett elkövetés a kibertérben:
- pénzmosás (Btk. 399. §) megvalósulásának esetei online környezetben,
- tiltott szerek forgalmazása, azzal való kereskedés:
- kábítószer-kereskedelem (Btk. 176. §),
- kábítószer készítésének elősegítése (Btk. 182. §),
- kábítószer-prekurzorral való visszaélés (Btk. 183. §),
- új pszichoaktív anyaggal való visszaélés (Btk. 184. §),
- teljesítményfokozó szerrel való visszaélés (Btk. 185. §),
- egészségügyi termék hamisítása (Btk. 186. §),
- piramisjáték szervezése (Btk. 412. §),
- 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,
- (DoS, DDoS-támadások, ransomware-ek, APT-támadások, MITM-, WITM-támadások, booter/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. §).

7.1.1. A szervezett bűnözés megjelenése, ismérvei a kibertérben

A szervezett bűnözés, ahogy a 21. században szinte valamennyi bűncselekmény esetében elmondható, nagyobb részben áttevődött a hagyományos, fizikai térből, a fizikai eszközökről a virtuális térbe, és a bűnözők igyekeznek kihasználni az internet és az infokommunikációs eszközök nyújtotta lehetőségeket a jogellenes cselekményeik elrejtésére, eltitkolására és az egyre szélesebb körű terjesztésére. A szervezett bűncselekmények egyik piactere a darknet, amely egy Tor Browser nevű böngészővel használható. Ez nehezíti a felhasználók azonosítását, biztosítja nekik az anonimitást. A darkneten, azaz az internet sötét oldalán a bűnözők képesek rejtve maradni, ugyanakkor az illegális tevékenységüket, mint egy piacon, kínálni. Az őket igénybe venni kívánóknak lehetőségük van arra, hogy bérgyilkosokat, fegyvereket, kábítószert vagy egyéb illegális tevékenységet vegyenek igénybe. A SOCTA 2017-es jelentése alapján 2017. januárig több mint 1,7 millió közvetlen felhasználója volt a TOR-hálózatnak. Az anyagi javak kibertérbe történő eltolódása magával hozza a szervezett bűnözői csoportok fokozott aktivitását is a közeljövőben. Több esetben felvetődött már a legfőbb államhatalmi szervek és a szervezett bűnözői csoportok összefonódása is. Ezek egy részében az állami szervek – a bűnszervezetekhez hasonlóan – az illegális anyagi előnyök megszerzése céljából létesítettek meg nem engedhető kapcsolatot (Perl 2007), míg más esetekben titkos, operatív műveletek során kapcsolódik a kibertérben szervezetten elkövetett bűncselekményekhez állami megrendelés (iráni nukleáris dúsító, az orosz állam érdekeit szolgáló DDoS- és hacker támadások stb). A határok nagyon elmosódottak. Egy ország létfontosságú rendszerelemét vezérlő informatikai eszközök ellen intézett támadás eredményét tekintve lehet teljesen azonos akkor is, ha csak egy *cracker,* ha egy terrorista szándékú elkövető, és akkor is, ha egy állam kiberhadviselésre felkészített egysége hajtja azt végre. A valódi különbség csupán az elkövetők szándékában, céljában érhető tetten. Természetesen vannak olyan jelek egy adott támadás során, amiből lehet következtetni az elkövető személyére (használt programkódok, azok nyelvezete, fejlettsége, a felhasznált eszközök, a célpont megválasztása stb.), ami ugyanúgy igaz egy létfontosságú rendszerelem ellen intézett bombatámadás esetén is (használt robbanószer anyaga, eszközök fejlettsége stb.), de a leglényegesebb különbség, hogy a kibertérben sokkal nagyobb a végrehajtók lehetősége arra, hogy az elkövető kilétére vonatkozó következtetések alapját meghamisítsák. Mivel ezek a digitális bizonyítékok is a kettes számrendszer elemeiből állnak, így elméletben visszamaradó nyomok nélkül hamisíthatók. A számítógépes bűnözés típusainak és forrásainak sokfélesége miatt fontos elkerülni a számítógépes bűnözők sztereotipikus képét, vagy a valós veszélyhelyzetet messze meghaladó démonizálással egyfajta pánikot kelteni. A média híradásai alapján kialakultak már bizonyos képek: az anyagi érdekből fenyegető orosz hacker, a kínai *hacker patrióta* vagy az észak-koreai állam által foglalkoztatott hacker. Az ilyen elkövetői csoportokról kialakított képek sokszor félrevezetők lehetnek. A médiakép ellenére az elkövetők sok nemzetből származnak, és a motivációik sokszínűek, bár elvitathatatlan, hogy a korábbi szellemi kihívás helyébe a pénzügyi célok dominanciája került. Az ENSZ palermói egyezménye szerint[2] szervezett bűnözői csoportról akkor beszélhetünk, ha „bizonyos ideig fennálló, három vagy több főből álló strukturált csoport,

[2] 2006. évi CI. törvény az Egyesült Nemzetek keretében, Palermóban, 2000. december 14-én létrejött, a nemzetközi szervezett bűnözés elleni Egyezmény kihirdetéséről.

amely összehangoltan működik egy vagy több […] súlyos bűncselekmény elkövetése céljából, közvetlen vagy közvetett módon pénzügyi vagy más anyagi haszon megszerzésére törekedve." Ez az egységes fogalommeghatározás nem terjed ki olyan rendkívül kifinomult szervezési formákra, mint például akár több mint egymillió IT-eszközt magában foglaló zombigép-hálózatok – botnetek – működtetése, amit akár egyetlen személy is megvalósíthat. Egyes szakértői vélemények szerint az egyedüli elkövető által mozgósított botneteket a szervezett bűnözés formájának kell tekinteni (CHABINSKY 2018). Jól látható, hogy a szervezett bűnözés hagyományos definíciói mennyire elavultak, amikor a kibertér is a territórium egy része. Ha kétségbe vonjuk a szervezett bűnözői csoportok kiterjedtségét, szerepét a kibertérben, azzal akadályozzuk a megfelelő ellenintézkedések kialakulását. Miközben egyre több szakértő úgy véli, hogy a számítógépes bűnözés a szervezett csoportok tartományává vált, és az egyedülálló hacker napjai múlnak, még valójában kevéssé ismertek a csoportok által előnyben részesített struktúrák, és hogy miképpen biztosítják a bizalmat a szervezeten belül. Hiányzik a bizonyítékokon alapuló kutatás a támadó viselkedésről és a számítógépes térben való toborzásról, bár a tanulás és utánzás fontos szerepet játszik (BROADHURST 2005). Egy a kibertérhez köthető bűncselekményekre vonatkozó nemzetközi kutatásban 2012-ben (MCGUIRE 2012) azt találták, hogy a számítógépes bűnözés legfeljebb 80%-a lehet valamilyen szervezett tevékenység eredménye. Ez azonban nem jelenti azt, hogy ezek a csoportok hagyományos, hierarchikus szervezett bűnözői csoportok formáját öltik, vagy hogy ezek a csoportok kizárólag digitális bűnözést követnek el. A kutatás inkább azt sugallja, hogy a hagyományos szervezett bűnözői csoportok új, lazább bűnözői hálózatok mellett bővítik tevékenységüket a digitális világra. A bűnözői csoportok különböző szervezeti szinteket mutatnak be attól függően, hogy tevékenységük kizárólag az online célokat szolgálja-e, vagy olyan online eszközöket használnak, amelyek lehetővé teszik a „valós" világban elkövetett bűncselekményeket, vagy kombinálják az online és az offline célokat.

8. ábra

A szervezett bűnözés szerveződésének és felépítésének egy tipológiája

Forrás: MCGUIRE 2012

A *rajok* a hálózatok számos jellemzőjét mutatják, és közös célok nélküli, szervezetlen csoportokként írhatók le. Tagjaik közt tipikusan kevés kapcsolat van. Ilyen formákban működhetnek a korábbi *hacktivista* csoportok. Ez a típus leginkább az ideológiailag irányított online tevékenységekben (például a gyűlöletbűnözés és a politikai ellenállás) jelenik meg (8. ábra). Az Anonymous-csoport egy tipikus rajtípusú csoportot szemléltet. A *hubok* mint tömeg lényegében aktívak az interneten, de sokkal szervezettebbek, és világos parancsszerkezettel rendelkeznek. Ezek magukban foglalják a központi bűnözői középpontját (agyat), amely körül a perifériás társaik összegyűlnek. Online tevékenységeik sokszínűek, például a kalózkodás, az adathalász támadások, a botnetek és az online szexuális bűncselekmények, a bankkártyaadatok, kábítószerek, prekurzorok kereskedelme. Például a Silk Roadot működtető piacok szintén illeszkednek ehhez a modellhez. Központi parancsstruktúra, amely lehet hierarchikus. Erős kapcsolatok vagy folyamatos interakció az egyének között. Például a LulzSec rendelkezik a hub tulajdonságaival. A hub típusú csoportoknak felrajzolhatjuk különféle hibrid változatait: a *fürtözött hibridben* a bűncselekmény az egyének kis csoportja köré tagolódik, és konkrét tevékenységekre vagy módszerekre összpontosít. Némileg hasonlítanak a hubok struktúrájához, de zökkenőmentesen mozognak az online és az offline bűncselekmények között. E körben említhető, tipikus csoportok a bankkártyás visszaélésekre szakosodott szervezetek, amelyek a kártyaadatokat megszerző – majd azokat online vásárláshoz használó – vagy a megszerzett adatokat értékesítő személyekre tagolódnak. A *kiterjesztett hibrid hálózati formák* a fürtözött hibridekhez hasonlóan működnek, de sokkal kevésbé centralizáltak. Általában sok munkatársat és alcsoportot foglalnak magukban, és számos bűncselekményt végeznek, de még mindig elégséges szintű koordinációt tartanak fenn működésük sikerének biztosításához. A hierarchiában leginkább a hagyományos bűnözői csoportok (például a családi alapokon kialakított bűnöző csoportok) írják le, amelyek néhány tevékenységet exportálnak az online térbe. A szervezett bűnözői csoportok tevékenysége a profit elérését célozza, így minden olyan tevékenységet megpróbálnak beindítani az online térben, ami az offline térben is hasznot hajt. Például a prostitúcióban tevékeny bűnözői csoportok érdeklődése kiterjed a pornográf weboldalakra vagy a szolgáltatások online értékesítésére. Ide tartozik még az online szerencsejáték, a zsarolás az informatikai rendszerek leállításával összefüggésben vagy a különféle nyilvántartások adatainak megszerzésével vagy hozzáférhetetlenné tételével kapcsolatos zsarolások – függetlenül attól, hogy az értékes adatokat hackeléssel, malware-ek, ransomware-ek segítségével vagy más módon érték el (Broadhurst et al. 2014; McGuire 2012). A csoportok tipizálása nem öncélúan történik. Ennek azért van kiemelt jelentősége, mert az ellenük való fellépés erőforrásigényét alapvetően meghatározza. Ha erős a személyes kapcsolattartás az adott csoportban, akkor ott lehetőség nyílhat a bűnügyi hírszerzés hagyományos erőinek (informátor, bizalmi személy, fedett nyomozó stb.) alkalmazására, de ezek hiányában ezek alkalmazása csak a kibertérről magas szintű ismeretekkel rendelkező munkatársakkal, informatikai megoldásokkal lehetséges A legkifinomultabb számítógépes bűnözői szervezeteket jelentős funkcionális specializáció és munkamegosztás jellemzi. Az Egyesült Államok Szövetségi Nyomozóhivatal Cyber Divíziója egyik képviselőjének beszédében az alábbi szerepek mutatják be, milyen szerepet játszhatnak a nagy csalások összeesküvései (Chabinsky 2018):

- A kódolók vagy a programozók a rosszindulatú programokat, a kizsákmányolást és egyéb eszközöket írják le a bűncselekmény elkövetéséhez.
- A forgalmazók vagy a kereskedők eladják az ellopott adatokat, és garantálják a más szakterületek által kínált árukat.

- A technikusok fenntartják a bűnügyi infrastruktúrát és a támogató technológiákat, például a kiszolgálókat, az internetszolgáltatókat és a titkosítást.
- A hackerek az alkalmazások, rendszerek és hálózatok sebezhetőségét kutatják és kihasználják annak érdekében, hogy rendszergazdai hozzáférést szerezzenek.
- A csalási szakértők *social engineering* terveket fejlesztenek ki és alkalmaznak, beleértve az adathalászatot és a spameket.
- A szolgáltatók a *tiltott tartalomszerverek és helyek* biztonságos eszközeit nyújtják, gyakran bonyolult botnet- és proxyhálózatok révén.
- A pénztárosok ellenőrzik a folyószámlákat, és ezeket a neveket és számlákat más bűnözőknek adják díj ellenében – tipikusan egyéni készpénzes futárokat is kezelnek.
- A pénzmosással foglalkozó személyek átruházzák a csalásokból származó bevételt, amelyet továbbítanak egy harmadik félnek, hogy helyezzék azt biztonságos helyre.
- Az elszámolók nyilvántartják a tiltott bevételt a digitális pénznemben és a különböző nemzeti pénznemek között.
- A szervezet vezetői a bűncselekmény elosztásának irányításán kívül választják ki a célokat, és felveszik és tagokat rendelnek a fenti feladatokhoz.

Talán más potenciálisan hasznos paradigmákat is találhatunk a számítógépes bűnözéssel foglalkozó szervezetek leírásában. A gazdasági földrajzból kiindulva az olyan vállalkozások csoportosítása, amelyek hasonló termékeket kínálnak ugyanazon a környéken, általában az egész világon megtalálhatók. A Tor böngészőn keresztül például a Silk Road és a hozzá hasonló online webáruházak a tiltott piacok számára *hot pointokká* váltak az online kábítószer-kereskedelemmel foglalkozó vevők és eladók számára. Ugyanakkor itt is érzékelhető a kibertér határtalansága, hiszen akár egy tengerentúli üzemeltetők által izlandi szerveren üzemelő webáruházban európai vásárló szerezheti be a távol-keleti prekurzorokat. Vajon a működő szervezett bűnözői csoportok a jelentős profit reményében üzletágat indítanak a kiberbűncselekmények irányába, mint ahogy egy sikeresen működő élelmiszer-áruház vagy hipermarket a honlapján beindítja a webshopot, hogy még nagyobb piacot teremtsen magának? Vajon inkább előzmények nélkül alakulnak ki új szervezett bűnözői csoportok, akik kellő tudás birtokában rájönnek, hogy a kibertérben használható tudásukat illegális jövedelemszerzésre is használhatják? Minden bizonnyal mindkét irányváltásra találunk példákat. Míg a számítógépes bűnözés számos fajtája nagyfokú szervezést és szakosodást igényel, nincs elegendő empirikus bizonyíték annak megállapítására, hogy a számítógépes bűnözés most a szervezett bűnözői csoportok uralma alatt áll-e, és milyen formát vagy struktúrát igényel ez a csoport (LUSTHAUS 2013). A kormányok, a bűnüldöző szervek, az akadémiai kutatók és a kiberbiztonsági ipar azt feltételezi, hogy a „hagyományos" szervezett bűnözői csoportok egyre inkább részt vesznek a digitális bűnözésben. A rendelkezésre álló empirikus adatok azt sugallják, hogy az online vagy a tartózkodási helyükön tevékeny bűnöző személyek inkább a laza társulással működő tiltott hálózatokhoz csatlakoznak, mintsem formálisan is létező szervezetekhez (DÉCARY–HÉTU 2012). Ahogy az összetett feladatokat ellátó informatikai vállalkozásoknak is specialistákat kell alkalmaznia az egyes részfeladatok végrehajtásához, hasonló módon az összetett informatikai bűncselekmények elkövetéséhez is specialisták szükségesek. Ha összevetjük a kibertérben és a való világban tevékeny bűnözői csoportokat, akkor számos hasonlóságot fedezhetünk fel. A leglényegesebb, hogy mindkét működési formát szigorú konspiráció jellemzi,

és céljuk az illegális profit. A való világban a csoportok tagjai sok esetben antiszociális személyiségjegyeket mutatnak, és a fizikai erőszaktól sem tartózkodnak, a kibertérben a bűncselekményeket sorozatjelleggel elkövető személyek nem antiszociálisabbak, mint a legális tevékenységet folytató informatikusok. A hagyományos szervezett bűnözői csoportok jellemzően korábbi személyes kapcsolatokon alapulnak. A közvetlenül kapcsolódó tagok személyesen ismerik egymást, és ez adja a kölcsönös bizalom alapját. Egy kibertérre specializálódott szervezett bűnözői csoport tagjai sok esetben nem kell, hogy ismerjék egymást személyesen, mert csak az online megnyilvánulásaikon keresztül szerezhetnek információt egymásról. A hagyományos szervezett bűnözői csoportok erős csoportidentitással rendelkeznek, és sokszor territoriális háborúra is képesek. A kibertérben területi viták nehezebben jöhetnek létre annak határtalansága miatt, illetve a csoportidentitás sem olyan erős, mivel a *crime as a service* – azaz egy-egy részcselekmény elkövetése szolgáltatásszerűen és díjazással – azt teszi lehetővé, hogy az egy-egy területen jártas elkövető több csoportnak is tagjaként működhet. A digitális technológiák az elmúlt évtizedekben lehetőséget biztosítottak az egyéneknek, hogy külső segítség és agresszív magatartás nélkül is jelentős hatást gyakoroljanak kritikus infrastruktúrákra (Morgenson 2000). Ezek az akciók természetesen reakciót váltottak ki az információs rendszerek üzemeltetői körében, és egyre nehezebbé vált magányos elkövetőként jelentős eredményeket elérni. Tehát az elkövetői oldalon is szükségessé vált a szervezetekbe tömörülés. Nyilvánvaló, hogy sok, de nem minden típusú bűnszervezet alkalmas a számítógépes bűnözésre. Az internet és a kapcsolódó technológiák tökéletesen alkalmazkodnak az egyes tevékenységek közötti koordinációhoz.[3] Egy kibertérben működő szervezett bűnözői csoport működhet nagyon strukturált, hagyományos maffiaszerű csoportként, amely bűnöző informatikai szakembereket vonz. Elképzelhető, hogy egy meghatározott cél érdekében létrejön egy szigorúan konspirált bűnözői csoport, de az eddig megismert esetekben ezek egy-egy konkrét bűncselekmény, egy konkrét sértett ellen vagy cél érdekében szerveződnek, tehát nem tartós jellegű együttműködés, hanem sokkal inkább a projektszemlélet uralkodik (Simon 2017). A szervezett bűnözői csoportok végső célja a profit elérése, így abban az esetben, ha szervezetten, de politikai célzattal követnek el jogsértő cselekményeket, azt nem sorolhatjuk a szervezett bűnözői csoportok tevékenységéhez.[4] A kibertérrel kapcsolatban a hosszú távú bűnös együttműködés sokkal inkább jellemző különféle illegális adatokkal összefüggésben: például szellemi tulajdon sérelmével járó tartalmak, gyermekek szexuális abúzusaival összefüggő illegális tartalmak. Ezekben az esetekben a sértetteket érő vagyoni kár[5] jellemzően nem jár együtt az elkövetők vagyoni gyarapodásával. A számítógépes bűnözők laza hálózatokként működhetnek, de bizonyítékok arra utalnak, hogy a tagok még akkor is szoros földrajzi közelségben helyezkednek el, ha támadásaik átnyúlnak a határokon. Például a kis, helyi hálózatok, valamint a rokonokra és barátaikra koncentráló csoportok továbbra is jelentős szereplők maradnak. A szervezett bűnözői csoportokkal való lehetséges kapcsolatokkal rendelkező számítógépes bűnözés forró pontjait sok esetben Kelet-Európában és a volt Szovjetunióban találhatjuk

[3] Például: netmeating, webinarning, távmunka, home office.

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

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

(KSHETRI 2013, 39–65.). Az orosz és az ukrán hackereket ügyes újítóknak tartják. Például a romániai Râmnicu Vâlcea kisváros központja ilyen centrumnak számít Kelet-Európában (BHATTACHARJEE 2011). Az elmúlt évtizedben a kínai számítógépes bűnözésről is egyre aggasztóbb információk érkeznek (WANG 2010).

7.2. Kiberterrorizmus

A kiberbűncselekmények és a szervezett bűnözés egyik közös pontja a kibertérből érkező támadás. Kibertámadásnak vagy a kibertéren keresztül történő támadásnak azt nevezhetjük, amelynek célja egy információs környezet vagy infrastruktúra üzemelésének megszakítása, kikapcsolása, megsemmisítése, felügyeleti jogának megszerzése, a kezelt adat integritásának megsemmisítése vagy a felügyelet alatt álló adat megszerzése.

A kibertámadások fajtái:

- illetéktelen hozzáférés az információkhoz,
- illetéktelen adatbevitel,
- rosszindulatú szoftverek bevitele,
- információs környezetszennyezés (HAIG 2005, 230.).

7.2.1. Kiberterrorizmus és terrorizmus

A kiberterrorizmus a szakirodalmak szerint nem létezik, hiszen ha a 2001. szeptember 11-én New Yorkban a World Trade Center elleni támadásra gondolunk, akkor a sokszor emlegetett Stuxnet hatásai ezzel nem mérhetők össze. Míg a terrortámadás esetében véres, emberáldozatokról szóló támadásokról beszélhetünk, addig, ha létezne kiberterrorizmus, kisebb eséllyel valósulna meg egyszerre több ember élete, testi épsége ellen elkövethető erőszakos támadás. Azonban ha a terrortámadás olyan informatikai rendszereket támad, ahol lehetséges lenne, hogy egyszerre rövid idő alatt bekövetkezzen hasonló támadás, úgy már a kibertámadás fogalma a gyakorlatban is értelmezhető lenne, hiszen a Btk. 314. §-a szerinti tényállás alapján:

„Aki abból a célból, hogy

a) állami szervet, más államot vagy nemzetközi szervezetet arra kényszerítsen, hogy valamit tegyen, ne tegyen vagy eltűrjön,
b) a lakosságot megfélemlítse,
c) más állam alkotmányos, társadalmi vagy gazdasági rendjét megváltoztassa vagy megzavarja, illetve nemzetközi szervezet működését megzavarja, […]”.

Ahogy azt Horváth Attila megemlíti, célszerű megkülönböztetni a terrortámadásokat és a terrorfenyegetettségnek kitett terek jellemzői alapján:

- a rurális tereken végrehajtott terrortámadások,
- a városi tereken végrehajtott terrortámadások,
- a kibertérben elkövetett terrortámadások (HORVÁTH 2006, 1–19.).

A terrorizmus az egyik legnagyobb félelmet keltő támadási forma, amely – a kiberbűnözéssel ellentétben – nem a 21. században alakult ki. A hagyományos terrorizmus kinetikai eszközöket (például öngyilkos merénylőket vagy improvizált robbanóeszközöket) alkalmaz, és sokféleképpen működik. A halál, a sérülés és a tulajdon rombolásával együtt a terrorizmus félelmet és aggodalmat vált ki a célcsoportban. A terroristák azért használhatják a terrorizmust, hogy demoralizálják a polgári lakosságot, hogy nyomást gyakoroljanak egyes kormányokra vagy szervezetekre azért, hogy azok vállaljanak vagy tartózkodjanak egy meghatározott politikától. A terrorizmussal kapcsolatban legalább kétféle megközelítéssel élhetünk. Az egyik esetben célzott támadás történik, vagyis egy adott célpont ellen politikai célból követnek el kibertámadást, illetve a 2017-ben méltán nagy visszhangot kapó *Wannacry* zsarolóvírus-támadás esetén a kritikus infrastruktúrákat érte kibertámadás, amelynek következtében rendszerek álltak le, adatok váltak hozzáférhetetlenné vagy semmisültek meg. Az Amerikai Egyesült Államok Szövetségi Nyomozó Irodája szerint a kiberterrorizmus bármilyen „előre megfontolt, politikailag motivált támadás az információkkal, számítógépes rendszerekkel, számítógépes programokkal és adatokkal, amelyek szubnacionális csoportok vagy titkos ügynökök elleni erőszakot eredményeznek a nem harci célokat illetően. A terrorcselekmény jogi tárgya az állami szervek, más államok, a nemzetközi szervezetek zavartalan, kényszertől mentes működéséhez, a lakosság megfélemlítéstől mentes életviteléhez fűződő társadalmi érdek” (BLASKÓ 2015, 16.). Az elkövetési magatartás a tényállás alapján a tűrésre kötelezés, megfélemlítés, alkotmányos rend megváltoztatása, nemzetközi szervezet működésének megzavarása, anyagi javak hatalomba kerítése és azok sértetlenül hagyását vagy visszaadását állami szervhez vagy nemzetközi szervezethez intézett követelés teljesítésétől teszi függővé.[6] A szakirodalom ennél a bűncselekménynél meghatároz egy cél-, illetve eszközcselekményt is. Az eszközcselekménye a jelentős anyagi javak hatalomba kerítése, amely nem feltétlenül jelenti a jogellenes birtokbavételt és a rendelkezési jog gyakorlását. A kibertérből érkező fenyegetésekhez[7] tartozik például a zsarolóvírus kritikus információs infrastruktúrához történő eljuttatása, ami kimeríti a terrorcselekmény fogalmát. A Btk. már az előkészületet is bünteti, így már már azzal elköveti valaki a cselekményt, ha akár egy adott kritikus infrastruktúra információs rendszerének sérülékenységét ismerve, arra célzottan elkészíti a programvírust, de ugyanúgy az is elköveti a jogellenes cselekményt, aki – bár nem tudva a sérülékenységekről – egy rosszindulatú programot megír, ami egy adott, létfontosságú rendszerelem működését veszélyezteti vagy abban zavart okoz.

7.2.2. Közérdekű üzem működésének megzavarása

A Btk. 323. §-ának tényállása szerint: „Aki közérdekű üzem működését jelentős mértékben megzavarja, bűntett miatt egy évtől öt évig terjedő szabadságvesztéssel büntetendő.”

---

[6] Btk. 314. § (1)–(2) bekezdés.

[7] Az Ibtv 1. § 16. pontja meghatározza, hogy mit is jelent a fenyegetés: olyan lehetséges művelet vagy esemény, amely sértheti az elektronikus információs rendszer vagy az elektronikus információs rendszer elemi védettségét, biztonságát, továbbá olyan mulasztásos cselekmény, amely sértheti az elektronikus információs rendszer védettségét, biztonságát.

A közmű meghatározása: olyan termelő- vagy szolgáltató üzemek, amelyek a lakosság, továbbá az ipar, a mezőgazdaság, a szolgáltató tevékenység kiterjedt körét vízzel, elektromos, gáz-, gőz- vagy hőenergiával látják el (KERESZTY et al. 2004, 457.). Továbbá a közösségi közlekedési üzem, amely a tömeges közlekedés lebonyolítására alkalmas, a használók széles köre által igénybe vehető közlekedési eszközök üzeme. A tényállást kell alkalmazni az elektronikus hírközlő hálózatokra is, továbbá az egyetemes postai szolgáltató közérdekű feladatainak teljesítése érdekében üzemeltetett logisztikai, pénzforgalmi és informatikai központokra és üzemekre is. A bűncselekményt nyitott törvényi tényállásnak lehet nevezni, hiszen a törvényalkotó nem határozza meg benne az elkövetési magatartást, így elkövethető szándékosan, tevéssel vagy éppen mulasztással is. A deliktum eredménye a fent felsorolt közműhálózatban okozott bármilyen zavarral már bekövetkezik. A bűncselekmény elkövetője tettesként bárki lehet.

7.3. Vagyon elleni bűncselekmények a kibertérben

A kibertérben elkövetett vagyon elleni bűncselekményeknek egzakt meghatározása még nem alakult ki, a folyamatos információtechnológiai fejlődésnek és az azt követő jogi szabályozás változásának következtében nem is alakulhatott ki. Erre figyelemmel olyan taxatív felsorolás sem létezik, hogy konkrétan mely bűncselekmények tartoznak ebbe a kategóriába. A Btk. vagyon elleni bűncselekményeket tartalmazó fejezetéből tulajdonképpen a csalás és az információs rendszer felhasználásával elkövetett csalás sorolható szűkebb értelemben a kibertérben elkövetett vagyon elleni bűncselekmények körébe. Nem a Btk. vagyon elleni bűncselekményeket taglaló XXXVI. fejezetében található ugyan, azonban e kategóriába illeszthető további két bűncselekmény, egyrészt a Btk. 423. §-ában meghatározott információs rendszer vagy adat megsértése, illetve a Btk. 424. §-ában írt információs rendszer védelmét biztosító technikai intézkedés kijátszása, amelyeknek lehet akár vagyoni vonzatuk is. Az e-kereskedelem körében, az online térben elkövetett bűncselekmények elkövetési módszerei rendkívül változatos képet mutatnak, a technológiai fejlődésnek megfelelően szinte naponta jelennek meg újabb és újabb módszerek. Emiatt a nyomozó hatóságoknak rendkívül nehéz lépést tartaniuk a sokszor csúcstechnológiát is felhasználó elkövetőkkel és az általuk kidolgozott elkövetési technikákkal, továbbá azokra megfelelő felderítési módszereket alkalmazni. Valamennyi bűncselekmény felderítése során egyedileg kell meghatározni a nyomozás metodikáját, ezért univerzálisan és kötelezően végrehajtandó feladatok sem határozhatók meg egyértelműen. Kijelenthető, hogy az elkövetők ezen a területen is a lehető leggyengébb láncszemet keresik annak érdekében, hogy illegálisan jövedelemre tegyenek szert. Az internetes webáruházak működésének megindulásakor technológiai oldalról könnyebben támadható volt egy tranzakció: bankkártyaadatok megszerzése, tranzakciók eltérítése stb. A jelenkori és mindenki által elérhető ismeretek szintjén könnyen megvalósíthatók voltak a jogsértések, de azóta a különféle biztonsági elemek kialakítása, elterjedése a technológiai oldalról történő elkövetéshez szükséges ismeretek szintjét nagyon magasra emelte – azaz jellemzően sokkal magasabb szintű informatikai tudás szükséges egy illegális vagyonszerzésre irányuló, pusztán technológiai támadáshoz, mint ezelőtt 5 vagy 10 évvel. Így az elkövetők figyelme a gyengébb láncszem – az emberi tényező – felé irányult. A technológia oldaláról már olyan szintű ismeretekre van szükség,

ami ez elkövetőket inkább abba az irányba indította, hogy támadásaikat az emberi hibák, tévedések és olykor kapzsiság kihasználásával vigyék sikerre. A kibertérben az egyik leghatékonyabb eszköz a *social engineering,* azaz a pszichológiai manipuláció. Hisz miért törje fel a vezérigazgató informatikai eszközeit összetett hackertechnikákkal az elkövető, ha egy ügyesen, telefonban előadott legenda alapján a titkárnő vagy a titkár a szükséges adatokat önként közli? Bár a példa abszurdnak tűnik, de a valósághoz közelít. Az emberek segítőkészségét, nagyravágyását, tudatlanságát, hiszékenységét precízen kihasználó elkövetők olyan hihető – és a valósággal több ponton összeilleszthető – történetet adnak elő, amely hatására a szükséges információt a célszemélytől megszerzik. Nemzetközi kitekintésben látható, hogy az Europol EC3 által publikált IOCTA-jelentésekben[8] is kiemelt jelentősége van a csalás jellegű visszaéléseknek. A nemzetközi bűnügyi együttműködésről szóló kurzusok során tárgyalásra kerültek az Europol által üzemeltetett Elemzői Projektek *(Analysis Project),* amelyek egy tagországok által megküldött adatbázist kezelnek. Ilyen az *AP Apate,* amelynek súlypontja a csalás jellegű cselekmények köre: ügyvezetői csalás *(CEO fraud, chief executive officer fraud),* üzleti e-mail-kompromittáláson alapuló csalás *(BEC fraud, business e-mail compromise fraud),* tömeges (*phishing* jellegű) levélküldés, szerelmi csalás, piramisjáték, befektetési csalás. A BEC- és CEO-csalások jellemzője, hogy sok esetben határon átnyúló elkövetői kör célzottan támad egy-egy személyt vagy szervezetet annak érdekében, hogy illegálisan anyagi javakra tegyenek szert. Ezekben az eljárásokban lehet hatalmas segítség, ha ez Europol adatbázisában szereplő információk is felhasználhatóvá válnak a magyar hatóságok számára egy itteni büntetőeljárásban. Ehhez azonban az szükséges, hogy ezek a tagállami hatóságok az adatbázisban elvégezzék az adatszolgáltatást. Ha egy Magyarországon folyó eljárásban beazonosításra kerül egy telefonszám, e-mail-cím, weboldal, számlaszám, az nagyon hatékonyan tudja segíteni a párhuzamosan más államokban folyó eljárásokat, hogy a bűncselekmények mozaikdarabjai összeilleszthetők legyenek, hogy a kriminalisztikai alapkérdésekre választ kapjunk, hogy a sorozatjellegű cselekményeket egymáshoz illesszük, hogy megakadályozzuk a további sorozatok kialakulását. Ehhez szintén hasznos eszköz lehet egy JIT *(Joint Investigation Team)* létrehozása is, amelynek első adatai sok esetben az Europol AP-jében felismert találatok, amelyek alapján a bűnüldöző szervek tájékoztatást kapnak arról, hogy például azonos elkövetői körrel szemben folytatnak eljárást párhuzamosan. A kibertér felől érkező csalás jellegű cselekmények kiváló lehetőséget biztosítanak az elkövetők számára, hogy valós identitásukat elrejtsék. Ehhez hozzájárul, hogy a felhasználók sok esetben rutinszerűen alkalmazzák az infokommunikációs eszközeiket, és nem vesznek észre gyanús jeleket, amelyek csalásra engednének következtetni. A csalás jellegű cselekmények esetén az oksági folyamatokat vizsgálva látható, hogy a sértett tudatát az elkövető olyan módon befolyásolja, hogy saját szándékos cselekményével okozzon kárt önmagának és illegális hasznot az elkövetőnek. Az emberi döntések jellemzően racionálisak,[9] de ez csak megfelelő informáltság esetén működik, így a csalás elkövetési magatartásának a döntési folyamatok bemeneti oldalát

[8] IOCTA-jelentés. Forrás: www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2018 (A letöltés dátuma: 2018. 09. 15.)

[9] Hagyományos közgazdaságtani értelmében a döntéshozói racionalitás esetén, konzisztens preferenciák mentén, megfelelő informáltság esetén a legkedvezőbb döntési lehetőséget választja.

kell manipulálni, kompromittálni. A kibertérhez kapcsolódó vagyon elleni cselekmények esetén ez az információs aszimmetria az alábbi formákban jelentkezhet:

1. *A sértett azt feltételezi, hogy számára az ügylet pozitív hatású, megéri. Ide sorolhatók a következő visszaélések:*
   - Internetes oldalakon, webáruházakban, aukciós oldalakon értéktelen vagy a feltüntetett értéknél jóval kevésbé értékes javakat értékesítenek. Ezekben az esetekben jellemzően a Btk. 415. § (1) bekezdésbe ütköző rossz minőségű termék forgalomba hozatala vagy a Btk. 417. § (2) bekezdésébe ütköző fogyasztók megtévesztése bűncselekmények valósulnak meg, azonban ezek vagy az adott kereskedési platform vitarendezési eljárásában vagy fogyasztóvédelmi eljárásban nyernek orvoslást. Büntetőeljárás e cselekményekkel összefüggésben nagyon kis számban indul.[10]
   - Az aukciós vagy apróhirdetési oldalakon meghirdetett javak értékesítése/megküldése nem is áll az elkövető szándékában, csupán bizonyos összegek kicsalását próbálja elérni (a csomagolási és postaköltség, előleg, foglaló, nagyon kedvező vételár előre utalása, postai csekken, kriptovalutában vagy bármilyen formában az elkövetőkhöz történő transzferálásával).
   - Gépjárművek, munkagépek színlelt eladási szándékával pénz kicsalása előlegre vagy a szállítási költségre. Ekkor az elkövetők létrehoznak egy megbízhatónak tűnő, tőlük látszólag független honlapot, ahol a megtévesztendő ügyfél nyomon tudja követni a neki szánt gépjárművet.
   - *Nigériai levelek* esetén az elkövetők valamilyen jelentős összeg ígéretével az ahhoz való hozzáférés biztosításához kérnek pénzt (például: a diktátor zárolt számlájához, távoli rokon hagyatékához, lottónyeremény utalásához stb.).
   - Kriptovalutákhoz kapcsolódóan az elkövetők egy új kriptovalutát fejlesztenek ki, és annak megvásárlására biztatják a sértetteket. Különféle megtévesztő információkkal azt a látszatot érik el, hogy a vásárlás jó üzlet lesz, de valójában az adott kriptovalutáról szóló információkat meghamisítják, az árfolyamot csalárd módon manipulálják, és így csalják ki az anyagi javakat a sértettektől (amelyek lehetnek akár értékkel bíró kriptovaluták is).
   - Különféle befektetési lehetőségekre vonatkozó felhívások, amelyek kihasználják az online térre vonatkozó információáramlás manipulálásának lehetőségét. Ezekben az esetekben a célzott közönséget e-mail-es címlisták, keresőoptimalizálás, mikrotargeting eszközeivel olyan internetes oldalakra irányítják az elkövetők, amelyeken az általuk kiválónak beállított befektetési lehetőségre gyűjtenek pénzt, kriptovalutát. Ezeknél az eseteknél jellemzően a sértett valamilyen kiváló ajánlatra kíván lecsapni, és fontos szerepet játszik a kapzsiság és a megszerezni kívánt dolog birtoklásának vágya, és sok esetben az azonnali döntés szükségessége miatt nem veszi észre a csalásra vonatkozó figyelmeztető jeleket.

[10] Rossz minőségű termék forgalomba hozatala miatt indult eljárások száma 2017. évben (online + offline együtt) 5 db, fogyasztók megtévesztése miatt: 12 esetben.

2. *A sértett azt feltételezi, hogy az általa hozott döntés helyes, azaz nem jogsértő, nem egyedi, hanem a rendelkezésre álló információk alapján logikus. Ide sorolhatók az alábbi visszaélések:*
   - Romantikus csalások, amikor az elkövető a sértett bizalmába férkőzve – benne sokszor szerelmet ébresztve – arra kéri több hónapnyi e-mailezés, chatelés után, hogy a személyes találkozóhoz szükséges repülőjegy megvásárlására, súlyos egészségügyi problémájára, váltságdíjra a sértett utaljon az elkövető által megadott számlaszámra jelentősebb összegű pénzt.
   - *Phishing,* azaz adathalász weboldalnak nevezünk egy olyan oldalt, amely egy ismert szervezet vagy vállalat hivatalos oldalának láttatja magát, és megpróbál személyes adatokat, jellemzően felhasználói azonosítókat, jelszavakat, bankkártyaadatokat megszerezni. A csalók gyakran kéretlen levelek, azonnali üzenetek küldésével, chatbeszélgetésekben igyekeznek rávenni a felhasználókat, hogy az üzenetben szereplő hivatkozásra rákattintsanak, amely az adathalász oldalra vezeti őket. Ha a felhasználók követik az ott szereplő utasításokat, akkor áldozattá válhatnak.
   - *CEO-fraud,* azaz ügyvezetői csalás. Ezekben az esetekben a károkozás abból következik be, hogy egy gazdálkodó szervezetbe olyan információkat juttatnak, mintha azokat egy vezető állású személy vagy az ügyvezető adta volna ki, és ezek hatására a tévedésbe ejtett munkavállaló átutalást indít az elkövetők által megjelölt számlára.

Ezekben az esetekben nem a sértettek nyereségvágya, kapzsisága okozza a téves döntést, hanem jellemzően az elkövetők hatékonyan összeállított meséje, legendája és a döntési helyzet azonnalisága, sürgőssége. A fenti két kategória közös tulajdonsága, hogy az infokommunikációs eszközökből érkező információ – bár nem valós, de – nem szükségszerűen jár információs rendszer vagy adat megsértése bűncselekmény elkövetésével. A célpontok kiválasztása, a lehetséges sértettek online jelenlétének megismerése járhat e bűncselekmény elkövetésével, de anélkül is elkövethető, így a felsorolt elkövetési magatartások helyes büntetőjogi értékelése a Btk. 373. § (1) bekezdésébe ütköző csalás. A Btk. 375. §-ba ütköző információs rendszer felhasználásával elkövetett csalás a jogalkotó szándéka szerint kiegészítő szerepet tölt be a csalás (Btk. 373. §) bűncselekménye mellett, mert olyan csalárd magatartásokat fog át, amelyek a vagyoni károsodást az információs rendszer közvetlen felhasználásával, befolyásolásával okozzák, így természetes személynek – a csalás megállapításához elengedhetetlen – megtévesztésével nem járnak. Az itt felsorolt elkövetési magatartások azonban szükségszerűen a természetes személyek tévedésbe ejtésével járnak.

3. *A sértett azt feltételezi, hogy az információs rendszerből származó adatok validak, és azokra tekintettel cselekszik és válik sértetté.*
   - BEC-csalások: a szükséges adatok beszerzését követően az elkövető az általa kiválasztott pénzügyi partner arculatát (logó, elnevezés, karakterek, szimbólumok stb.) és e-mail-címét felhasználva létrehoz egy hamis e-mail-fiókot, majd fizetési kötelezettségről szóló, célzott értesítést küld a sértett munkavállalójának vagy tisztviselőjének. A célzott e-mailek a legtöbb esetben formailag és tartalmilag is azt a látszatot keltik, hogy a küldőként megjelölt személytől vagy szolgáltatótól származnak és – a felek között fennálló jogviszony

alapján – valós követelésre vagy pénzügyi teljesítésre hívják fel a figyelmet. Ezzel összefüggésben gyanúra adhat okot a kedvezményezett számlaadataiban történőt változásról szóló értesítés.
– Informatikai eszközök, alkalmazások kompromittálása révén az elkövetők olyan kártékony kódot juttatnak a célszemélyekhez, ami például a vágólapra helyezéskor felismeri, hogy az egy számlaszám vagy egy kriptovaluta publikus tárcacíme, és azt beillesztéskor az elkövetők számlaszámára, tárcacímére módosítják.

Ezekben az esetekben jellemzően nincs szó a döntések azonnaliságáról, sem a sértettek kapzsiságáról, sokkal inkább arról, hogy az elkövetők a normális ügymenetet jól ismerve megkeresik azt a pontot, amikor az információk manipulálásával anyagi javakra tehetnek szert. Ezen elkövetési magatartások megvalósításához szükségszerű az információs rendszerek kompromittálása, hiszen ha például a BEC- vagy CEO-csalások nem a sértett vállalkozások jelenlegi vagy korábbi munkatársainak segítségével valósulnak meg, akkor az elkövetőknek szükséges ismerniük a támadott vállalkozások belső ügymenetét, a jellemző pénzügyi tranzakciókat, döntési folyamatokat. Ezeknél az elkövetési magatartásoknál már valószínűsíthető a Btk. 375. §-ába ütköző információs rendszer felhasználásával elkövetett csalás elkövetése.

7.3.1. A BEC-csalásokról bővebben

Az ilyen típusú csalások hazai viszonylatban is egyre jellemzőbbek, de az ezzel kapcsolatos ismeretek kidolgozására még nem került sor. Az elkövetési magatartás tömegesen először az Amerikai Egyesült Államokban jelent meg, de azóta az egész világon elterjedt. A cselekményt az időbeliség alapján négy fontos állomásra oszthatjuk.[11]

1. A célpont kiválasztása, profilalkotás:
Az elkövetői csoport kiválasztja a lehetséges célpontot, vagyis azt a vállalkozást vagy személyt, akinek a pénzügyi portfóliója, illetve alkalmazotti (vagy vezetői) köre könnyen feltérképezhető online forrásból elérhető adatokat felhasználva. A célponthoz kapcsolódó profil megalkotása során jelentős szerepet kap a nyílt forrású információgyűjtésre (OSINT) épülő adatszerzés, ezzel ugyanis nagyobb mennyiségű – közvetve vagy közvetlenül is felhasználható – adat szerezhető be (például kapcsolati háló, munkarend, munkahelyi szokások stb.).

2. Célzott támadások:
A korábban beszerzett információk birtokában az elkövető célzott támadásokat indít vezető beosztású vagy a pénzügyi területen tevékenykedő és a kifizetésekre jogosult személyek ellen. Az elkövetők az e személyekhez kapcsolódó tevékenységük során a manipuláció és nyomásgyakorlás különböző eszközeire építenek. Az ehhez szorosan kapcsolódó fiktív e-mailek vagy telefonhívások mellett (amely az emberi tényezőt célozza – *social engineering*) megjelennek azok az eszközök is, amelyek például az informatikai rendszereket támadják.

[11] Federal Bureau of Investigation (Szövetségi Nyomozó Iroda) tájékoztató anyaga szerint. Elérhető: www.fbi.gov/news/stories/business-e-mail-compromise-on-the-rise (A letöltés dátuma: 2018. 09. 15.)

Ennek megfelelő eszközei például a trójai vírusok vagy kémprogramok, amelyek elsődleges célja a belső rendszer sebezhetőségének felmérése. A külön bűncselekményt megvalósító (Btk. 422–423. §) kibertámadások célja tehát nem a zavarkeltés, hanem a rendszer felhasználói adatainak – különösen az egyes profilokhoz kapcsolódó felhasználónevek, jelszavak és kódok – megszerzése, mivel ezek birtokában fizikai jelenlét nélkül is lehetséges a belső rendszerek közvetlen befolyásolása. Nem zárható ki ebben az esetben sem az elkövetőkkel együttműködő belső személy sem a malware-ek telepítésében, sem az információ közvetlen megszerzésében.

3. A pénzügyi ügylethez kapcsolódó információk kicserélése:
Miután az elkövető kiválasztotta a manipulálni kívánt személyt, célzott levelet küld az érintettnek. A korábban beszerzett adatokat felhasználva az e-mail származhat valamely pénzügyi, vállalati vezető vagy külső partner hozzáférését megszerezve valós e-mail címről, illetve valamilyen megtévesztő címzést felhasználva (formailag és tartalmilag is hivatalosként feltüntetve), kifejezetten a csalás megvalósítására létrehozott e-mail-fiókból is. Az e-mail kötelező eleme az esedékes vagy elmaradt pénzügyi tranzakcióhoz kapcsolódó tájékoztatás, értesítés vagy felszólítás. A célzott üzenet fontos vonása, hogy azzal kapcsolatban hiányzik a tényleges teljesítés vagy a teljesítés szándéka, mivel a kedvezményezetti számlaszám felett a sértettel üzleti kapcsolatban nem álló (az elkövető vagy az elkövetővel együttműködő) személy rendelkezik. Az ügylet rögzítésére jogosult személy az e-mail tartalma alapján abban a tudatban indítja meg az utalást, hogy annak kedvezményezettje – valós kötelezettség alapján – a tényleges jogosult.

4. Átutalás, továbbutalás:
A csalással érintett ügyletekből származó jóváírások pénz- vagy hitelintézet által vezetett folyószámlára érkeznek. Az e számla felett rendelkező személyek jellemzően olyan strómanok, akik anyagi ellenszolgáltatásért cserébe létrehozzák és fenntartják a számlát, illetve az arra beérkező összegeket továbbutalva, illetve készpénzt felvéve azt a csalást elkövetők rendelkezésére bocsátják. Fontos megjegyezni, hogy a számla fenntartása, kezelése, illetve az annak egyenlegét érintő pénzügyi műveletek alkalmasak lehetnek a Btk. 399–400. §-aiban meghatározott pénzmosás bűntettének megállapítására. Tipikus magyarországi jelenség a külföldi BEC-csalásokból, illetve CEO-csalásokból származó összegek megjelenése a honi számlákon. Mivel a nyugat-európai gazdasági szereplők közti tranzakciók jellemzően nagyobb összegeket érintenek, így a csalások elsődlegesen ott, de az illegálisan eltérített tranzakciókból származó összegek feletti uralom megszerzése (tipikusan készpénzben történő felvétele) a kelet-európai országokban jellemző, ahol a pénzmosásgyanús bejelentések, illetve a pénzmosás miatt indított eljárások alacsonyabb száma azt valószínűsiti, hogy nagyobb arányban sikeresek a bűncselekmények ezen mozzanatai (Nagy 2010). Az adatgyűjtés során az elkövetők akár heteken, hónapokon keresztül is megfigyelhetik a célpontot, ez megvalósulhat nyílt adatgyűjtéssel, illetve jogtalan formában: tipikusan az információs rendszereket támadva vagy a célzott gazdálkodó, vagy annak partnere ellen. A csalás esetén nagyon fontos az információs aszimmetria az elkövetők és az áldozatok között. Minél nagyobb a különbség, annál inkább könnyű dolga van az elkövetőknek, akik az áldozataik kiválasztása során erre tekintettel vetik ki hálójukat. Mivel egy létező folyamat, hogy az idősebb korú személyek is a világhálóra kapcsolódnak,

ezért az ő áldozattá válásuk megelőzésére szükséges intézkedéseket tenni. A magyar nyelv *unikális* jellege és az állampolgárok idegennyelv-tudásának alacsony szintje miatt számos csalás jellegű visszaéléskampány alacsonyabb hatásfokkal működik. Az elektronikus eszközökön keresztül történő, csalás jellegű cselekmények azonban jelentős emberierőforrás-igénnyel is járnak, így az ipar földrajzi fejlődésének irányához hasonlóan itt is az olcsó munkaerő felé történő elmozdulás figyelhető meg. Az indiai médiában szereplő jelentések szerint egy csaló bűnszervezetnek kilenc call centerje volt, amely 770 embert foglalkoztatott. Magukat az Egyesült Államok adóügyi tisztviselőinek kiadva, minden alkalmazott naponta több mint 100 amerikai embert hívott fel telefonon károkozási szándékkal és sokszor eredménnyel (Lim 2016).

További jellemző elkövetési magatartások:

- Külföldi (külföldön tartózkodó) személy vásárol e-boltból, a megrendelt terméket nem kapja kézhez, a vételárat készpénzküldő szolgáltatás útján küldi meg Magyarországra, mert az eladó a vételár teljesítését ilyen formában kéri. Amennyiben bankszámlára történik a vételár átutalása, gyakori, hogy csekély ellenérték fejében adják át egyes – esetleg hajléktalan – személyek az adataikat, vagy úgynevezett alvó vagy kevés forgalmat bonyolító számlák adatait használják fel az elkövetők, majd a bűncselekmény útján megszerzett pénzt bankautomatából (ATM) felveszik.
- Az elkövető jogosulatlanul szerzi meg a bankkártyaadatokat, majd azzal a tulajdonos jelenléte, tudta és beleegyezése nélkül hajt végre vásárlásokat, jellemzően külföldön, de esetenként Magyarországról történő vásárlásindítással.
- Az elkövetők gyakran használják a Facebook közösségi oldalait, vásárlói csoportjait nem létező termékek eladására vonatkozó hirdetések feladásához, amelynek révén elkerülik a szabályosan működő online piactereken megkövetelt személyazonosítási folyamatot, ezáltal beazonosításukat jelentősen megnehezítik.
- Különféle távközlési szolgáltató cégek webshopjain keresztül fiktív adatokkal vagy valós személy adataival visszaélve előfizetési szerződést köt az elkövető, és ehhez kapcsolódóan jelentős kedvezménnyel értékes telefonkészüléket vagy egyéb műszaki cikket is vásárol. A megrendelt terméket átveszi, és használtként továbbértékesíti, valamint a távközlési szolgáltatás igénybevételével jelentős összegű tartozást halmoz fel, amit azonban nem fizet meg (Nagy 2018).

7.3.2. A phishingről, azaz adathalászatról bővebben

Az átverős üzenetek célja, hogy minél több banki felhasználói hitelesítő adathoz jussanak hozzá, és ezek segítségével elérjék az online tranzakciókhoz szükséges felhasználói fiókokat, majd egyszerűen ellopják az áldozatok pénzét. Jól mutatja elterjedtségét, hogy a Kaspersky nevű kiberbiztonsági cég megállapítása szerint 2017-ben minden második kibertámadás az áldozatok pénzének ellopására törekedett. 2017-ben a Kaspersky Lab antiadathalász technológiái több mint 246 millió alkalommal észleltek olyan oldallátogatást, amelyen különböző adathalász módszereket kíséreltek meg. Ebből 53% kifejezetten pénzügyekkel kapcsolatos honlapokra próbálta átirányítani a felhasználókat, amely 6%-os emelkedés 2016-hoz képest. 2017-ben a pénzügyi adathalász támadások összesítése – bankok, online

fizetési rendszerek, valamint webshopok elleni támadások – alapján kiderült, hogy ez a kategória első alkalommal került a TOP 3 kibercsapdák közé. A kiberbűnözők érdeklődése az általános fiókadatok ellopásától a pénzügyi fiókok irányába tolódott. Az adatok azt is mutatják, hogy a Mac-felhasználók egyre nagyobb veszélyben vannak. A közhiedelemmel ellentétben a Mac-eszközök biztonsága is sérülékeny: 2016-ban még az adathalász támadások 31,38%-a irányult pénzügyi adatok ellopására, majd ez a szám 2017-ben rekordméretűre duzzadt 55,6%-kal.

7.3.3. A vagyoni jogokat sértő kiberbűncselekmények nyomozása

Az online térben elkövetett bűncselekmények csak azok észlelése után, a cselekmény rendkívül gyors elkövetéséhez viszonyítottan hosszabb idő elteltével jutnak a nyomozó hatóságok tudomására (Parti 2004). A feljelentések megtételének módja nem tipizálható, azokat személyesen és elektronikus úton egyaránt eljuttatják a nyomozó hatósághoz, a postai úton küldött feljelentések e körben értelemszerűen nem jellemzők. Az ORFK tapasztalatai szerint az említett deliktumok miatt indított nyomozások tárgyát jelentős részben a Btk. 375. § (5) bekezdésébe ütköző információs rendszer felhasználásával elkövetett csalás alkotja, azonban nem elhanyagolható az internetes hirdetések feladásához köthető csalás gyanújának megállapíthatósága sem. Az internet útján elkövetett csalás jellemzően – eltérően a „klaszszikus" csalástól – hirdetés feladása útján realizálódik, amikor is az egymással kapcsolatba kerülő sértett és elkövető nem feltétlenül találkozik személyesen, sok esetben csupán elektronikus levelezést vagy telefonos egyeztetést folytatnak egymással, így állapodnak meg az ügylet részleteiben. Az információs rendszer felhasználásával elkövetett, kárt okozó magatartások elsősorban vagyoni érdekeket sértő, csalásszerű magatartások, mindazonáltal ezeket a csalástól elkülönítetten indokolt szabályozni, hiszen hiányzik a klasszikus értelemben vett tévedésbe ejtés vagy tévedésben tartás. A kárt az információs rendszer jogtalan befolyásolása okozza. A törvény ennek megfelelően a vagyon elleni bűncselekmények fejezetében önálló tényállásként szabályozza az információs rendszer felhasználásával elkövetett csalást. Az információs rendszer felhasználásával elkövetett csalás egyik leggyakoribb elkövetési magatartása a jogosulatlanul megszerzett elektronikus készpénz-helyettesítő fizetési eszköz (tipikusan bankkártyaadatok) felhasználása, ami elsősorban különböző online oldalakon történő vásárlásban manifesztálódik. E magatartás a külföldi szakirodalomban a *card not present fraud* (CNP) néven ismert, azaz a kártya jelenléte, annak fizikai birtoklása nélkül követik el a bűncselekményt. A bankkártyák és egyéb készpénz-helyettesítő fizetési eszközök biztonsági adatain túlmenően egyéb adatok (például PayPal-azonosító) jogosulatlan megszerzésére is irányulhat az elkövetők magatartása haszonszerzési célzattal, bár indokolt megemlíteni, hogy a PayPal e tekintetben fokozta az ügyfélbiztonságot a tranzakciók telefonon történő megerősítése lehetőségének megadásával. Az adatok felhasználásának végső célja mindig az, hogy az elkövető pénzhez (elsősorban készpénzhez vagy kriptovalutához) vagy egyéb értékhez jusson, így a felhasználás módozatai is ehhez igazodnak. Jellemzően internetes piactereken vásárlással, különböző telekommunikációs cégek honlapján való mobilegyenleg-feltöltéssel vagy szolgáltatásmegrendeléssel próbálnak haszonra szert tenni. Az információs rendszer felhasználásával elkövetett csalás – egyebek mellett – a jogosulatlanul megszerzett készpénz-helyettesítő fizetési eszköz felhasználásával

valósulhat meg, ezáltal a készpénz-helyettesítő fizetési eszközzel visszaélés az előbbi bűncselekménynek rendszerinti eszközcselekménye. A Btk. 375. § (5) bekezdésében a törvény összetett bűncselekményként törvényi egységet hozott létre, a két bűncselekmény halmazata tehát kizárt. Ennek következtében csak az előbbi bűncselekmény megállapításának van helye.[12] Ha tehát csupán az adatszerzés történt meg, de az adatok felhasználására még nem került sor, akkor a Btk. 393. § (1) bekezdésének valamelyik fordulata szerinti készpénz-helyettesítő fizetési eszközzel visszaélés gyanúja vetődhet fel (GÁL 2013), míg az adatok felhasználásával a Btk. 375. §-ában meghatározott információs rendszer felhasználásával elkövetett csalás valósul meg. A pénzintézet internetes felületén végrehajtott olyan pénzügyi műveletek azonban, amelyek a pénzintézettel megkötött netszámlaszerződésben, illetve az internetbanki szerződésben foglaltaknak megfelelnek, a számítógépes rendszer rendeltetésszerű igénybevételét jelentik, ezért az információs rendszer felhasználásával elkövetett csalás különös részi tényállását nem valósítják meg.[13] Meg kell jegyezni, hogy ezeknek a cselekményeknek a felderítése és bizonyítása a gyakorlatban nehéz, a kártyák leolvasásának utólagos bizonyítása, a vásárlók azonosítása rendkívül problematikus, ráadásul ezekre gyakran a bűncselekmény megvalósítása után több hónappal, néha évekkel később kerül sor (SINKU 2006). A vagyon elleni bűncselekmények közül ki kell emelni a napjainkban rendkívül elterjedt, úgynevezett pszichológiai manipulációs csalást (*social engineering fraud,* SEF). A SEF lényege, hogy a bűnelkövetők, manipulálva az embereket, bizalmas információkhoz jutnak hozzá (például jelszavak, banki adatok). A jelenség és az ahhoz kapcsolódó pénzmosás 2014-ben Magyarországon is megjelent. 2015 második felétől jelentősen megnőtt azoknak a pénzmosási bejelentéseknek a száma, amelyek alapcselekménye a külföldön elkövetett SEF típusú csalás (nemzetközi szinten általában a BEC-, CEO-fraud elnevezés használatos). A jelenség azt a jellemzően gazdálkodó szervezetek (ritkábban: állami szerv, ügyvédi iroda, magánszemély) ellen elkövetett csalási módszert jelenti, amely során az elkövetők általában a célpont üzleti partnere informatikai rendszerének feltörését követően pszichológiai manipulációval ráveszik a sértett gazdálkodó szervezet pénzügyi műveletek teljesítéséért felelős alkalmazottját, hogy teljesítse részükre az üzleti partner nevében, de valójában az általuk megküldött hamis vagy hamisított fizetési utasításban foglaltak szerinti átutalást. Az informatikai rendszer feltörésével az elkövetői csoport hozzájut a két cég közötti gazdasági kapcsolatra vonatkozó minden információhoz: korábbi és aktuális szerződésekhez, szállítási levelekhez, valamint a teljes kommunikációs anyaghoz, ideértve a kapcsolattartó személyek azonosítási, elérhetőségi adatait is. Az összegyűjtött információk alapján – a legtöbb esetben – az üzleti partnernek az ügyletek lebonyolítására használt e-mail-címével szinte teljesen megegyező, az elkövetők által készített e-mail-címről küldenek a partner nevében olyan fizetési utasítást, amelyben a cégek között ténylegesen létrejött szerződéshez kapcsolódó fizetési kötelezettség teljesítését kérik a cég megváltozott fizetési számlaszámára, amely már az elkövetők ellenőrzése alatt áll. Közvetlenül nem tartozik ugyan a vagyon elleni bűncselekmények körébe, azonban közvetve számolni kell, illetve lehet kárral, illetve vagyoni hátránnyal a Btk. 423. § (1) bekezdésében szankcionált információs rendszer vagy adat megsértése bűncselekmény elkövetése esetén. E tényállás tekintetében nem szükséges a célzat vizsgálata, hiszen az nem tényállási

[12] BH2015. 244.
[13] BH2017. 252.

elem, így mindegy, hogy az elkövető milyen célzattal követte el cselekményét. Leggyakoribb elkövetési magatartásként jellemzően *érzékeny adatokat* kísérelnek meg megszerezni az elkövetők, amelyeket a későbbiekben egyéb céljaik elérésére használhatnak fel. Az információs rendszer felhasználásával elkövetett csalás megvalósítható adatbevitellel, adat módosításával, törlésével, hozzáférhetetlenné tételével, továbbá minden más olyan művelet elvégzésével, amely az információs rendszert befolyásolja, és ezzel kárt okoz. A Btk. 424. §-ában büntetni rendelt információs rendszer védelmét biztosító technikai intézkedés kijátszása *sui generis* tényállás, mivel annak keretében a jogalkotó a Btk. 375. §., 422. §. és 423. §-ának előkészületi magatartásait pönalizálta. Elhatárolási kérdésekkel összefüggésben a BEC-csalásokhoz kapcsolódóan felmerülhet a Btk. 374. §-ába ütköző gazdasági csalás elkövetése, de az elhatárolás alapja az, hogy a hamis vagy megtévesztő elektronikus üzenet – hiába utal gazdasági tevékenység alapján fennálló követelésre – nem értékelhető színlelt gazdasági tevékenységként. Információs rendszer felhasználásával elkövetett csalás (Btk. 375. §) a BEC-csalásokkal összefüggésben akkor valósulhat meg, ha az elkövető az információs rendszert is kompromittálta. Ennek hiányában csak csalás valósul meg. Fontos kiemelni azonban, hogy a Btk. 375. §-ában rögzített tényállásnak nincsen szabálysértési alakzata, így akár 5 forintos elkövetési érték esetén is megvalósul. A tiltott adatszerzés kapcsán megfogalmazott törvényi tényállás számos esetben lefedi azt a tevékenységet, amely a BEC-csalás kapcsán az elkövető előkészületi tevékenységeként is értékelhető (személyes adatot, illetve – a sértett gazdasági tevékenységével összefüggésben – gazdasági vagy üzleti titkokat derítenek fel). A tiltott adatszerzés a csalással, illetve más – az információs rendszereket sértő – bűncselekményekkel halmazatban is megállapítható. A Btk. 422. § (1) bekezdés szerinti bűncselekmény rendbeliségének száma nem a titok sértettjeinek száma, hanem a konkrétan támadott személyiségi jogok sértettjeinek száma alapján állapítható meg. Annyi rendbeli bűncselekmény valósul meg, ahány magánlakást-információs rendszert az elkövető átkutat stb., függetlenül attól, hogy hány személy titkának megismerésére törekszik. Ellenben a (2) bekezdés szerinti bűncselekmény – a megismert személyes adat, magántitok, gazdasági titok vagy üzleti titok továbbítása vagy felhasználása esetén – a sértettek száma határozza meg a rendbeliséget (Hegedűs et al. 2018).

7.4. Az elsődleges nyomozási cselekmények

Az elkövetett deliktum jellegéhez képest kell minden esetben dönteni a konkrét, elvégzendő nyomozási cselekmények meghatározását illetően. Indokolt esetben nyomozási tervet kell készíteni, felsorolva ebben az elvégzendő elsődleges feladatokat, amit azok végrehajtását követően a beérkezett adatok, információk elemzése alapján bővíteni kell. A kibertérben elkövetett bűncselekmények nyomozási tapasztalatai szerint az ilyen ügyekben jellemzően jelentősen elhúzódnak a nyomozások, elsősorban a szolgáltatókkal való nehézkes kapcsolattartás, illetve felvetődő szakkérdések miatt. Pedig az interneten megjelenő adatok, képek, fájlok stb. a „kézzelfogható" bizonyítékoknál (kinyomtatott papíralapú szöveg, ujjnyom, egyéb biometrikus jelek stb.) sokkal egyszerűbben és gyorsabban változtathatók, átalakíthatók vagy akár hozzáférhetetlenné tehetők, ez pedig csökkenti a bizonyítékok összegyűjtésére nyitva álló időt (Parti 2004), így a nyomozások hatékonysága kerülhet veszélybe. Mindenképpen kerülni kell a nyomozás indokolatlan elhúzódását. Az említett

bűncselekmények gyanújával indított büntetőeljárások nyomozása során az időszerűség, ezzel párhuzamosan az eljárások hatékonyságának és eredményességének az elősegítése érdekében a következő eljárási cselekmények soron kívüli végrehajtása lehet indokolt.

- A feljelentő (sértett) mielőbbi mindenre kiterjedő, részletes kihallgatása.
- Kapcsolatfelvétel azzal a személlyel, aki az informatikai jellegű kérdésekre egzakt választ tud adni (milyen a hálózat felépítése, ki férhet hozzá a rendszer egyes elemeihez, milyen adattartalmú logfájlt készít a rendszer, azt meddig őrzi).
- Az internetszolgáltató megkeresése (az adott felhasználónevet ki, milyen adatokkal, mikor, milyen IP-címről regisztrálta).
- Amennyiben egy hálózatot ért támadás, a hálózatot üzemeltető informatikustól be kell szerezni a nyomozás során elengedhetetlenül szükséges adatokat (például a logadatokat).
- Meg kell keresni a hírközlési, illetve közösségi portált üzemeltető szolgáltatókat a releváns adatok beszerzése érdekében (híváslista, előfizetői adatok, IP-címek).
- Telefonszámok esetében a számhordozás ellenőrzése is indokolt annak érdekében, hogy a megkeresést a megfelelő szolgáltató részére meg lehessen küldeni.
- Az internet mint nyílt forrású hírszerzés (*Open Source Intelligence,* OSINT) kiaknázása elengedhetetlen. A közösségi portálok (például a Facebook) külön felületet hoztak létre a hatósági megkeresések teljesítése érdekében.
- Pénzintézeti megkeresések soron kívüli megküldése különös tekintettel az ATM biztonságikamera-felvételeinek beszerzésére (amennyiben rendelkezésre állnak a térfigyelőrendszer felvételei, azokat is be kell szerezni).
- Előzménykutatás elvégzése, tekintettel arra, hogy az internet felhasználásával elkövetett bűncselekmények esetében megalapozottan feltehető, hogy potenciálisan több személy sérelmére is megvalósul a bűncselekmény, akik feljelentése alapján több, különböző nyomozó hatóság előtt is indul büntetőeljárás.
- A későbbiekben tervezett kényszerintézkedésekre (kutatások, lefoglalások) való megfelelő felkészüléshez szintén elengedhetetlen tudni, milyen módon, hol, milyen eszközzel valósult meg a konkrét bűncselekmény elkövetése (GORICSAN 2006).
- Kutatás, lefoglalás foganatosítása, indokolt esetben igazságügyi szakértő bevonása az eljárásba. A kutatás során a bizonyítási eszközök felkutatásán kívül célszerű a fellelt számítógépeken, egyéb informatikai eszközökön vizsgálatokat, adatmentést végezni (DORNFELD 2018).
- Ha az elkövetett bűncselekménynek nemzetközi vonatkozása van, indokolt a Nemzetközi Bűnügyi Együttműködési Központ (NEBEK) megkeresése, és ha szükséges, jogsegélykérelem előterjesztése.

7.4.1. Nyomozás a BEC-csalásokkal összefüggésben

A hasonló jellegű bűncselekmények felderítése során – különös tekintettel a tényállás teljes körű tisztázására – elengedhetetlen a cselekmény alapvető feltételeinek ismerete, illetve ezzel összefüggésben azon technikai jellegű bizonyítékok beszerzése, amelyek rendelkezésre állnak. A nyomozás sikeressége kapcsán kritikus szerepe van az idő múlásának, vagyis a hatóság tudomásszerzését követően haladéktalanul meg kell tenni azokat

az intézkedéseket, amelyek elsősorban az elektronikus rendszerben tárolt adatok megőrzését szolgálják. E körben gondoskodni kell:

- a felhasználói rendszerekhez kapcsolódó belépési és műveleti adatok lementéséről,
- az egyes felhasználók adatainak (különösen a felhasználónevek, jelszavak és jogosultságok tekintetében) beszerzéséről,
- a sértett korábbi számlaforgalmi adatainak teljes körű beszerzéséről (mivel a cselekményt sok esetben több hónapos előkészítés előzi meg, illetve a folytatólagos elkövetés sem kizárt, ezért indokolt a nagyobb időtartamra vonatkozó adatgyűjtés),
- a belső informatikai rendszerről, az azt kiszolgáló eszközök, illetve az egyes munkaállomásokon (vagy a munkaállomások többségén) használt programokkal kapcsolatos állapotfelmérésről,
- az elektronikus/informatikai rendszert érintő korábbi támadások, illetve az ezekkel kapcsolatban tapasztalt következmények feljegyzéséről,
- annak megállapításáról, hogy milyen adat- és vírusvédelmi megoldásokat alkalmaztak a számítógépes hálózattal összefüggésben,
- annak megállapításáról, hogy milyen könyvelési, elszámolási vagy fizetési rendszert használnak,
- a levelezési rendszert kiszolgáló (SMTP-) szerver adatainak lementéséről (indokolt azon vállalkozás szerverére kiterjeszteni, amely az e-mail alapján az utalás kedvezményezettje).

Az informatikai rendszerekben fellelhető adatok lefoglalásával és elemzésével párhuzamosan az alábbi nyomozati cselekmények végrehajtása indokolt:

- a kedvezményezetti számlaszámhoz kapcsolódó adatok beszerzése (számla felett rendelkező személy adatainak, az általa kezelt más számlák adatainak, a számlavezető pénzintézet, a számlanyitás időpontja, valamint a kapcsolódó szolgáltatások és a teljes számlatörténet beszerzése);
- előzménykutatást kell végezni az azonos vagy hasonló módon elkövetett bűncselekmények kapcsán;
- azonosítani kell, hogy milyen forrásból és partnerektől érkezik egyéb jóváírás a számlára;
- a vagyonelkobzás biztosítása érdekében a bűncselekménnyel összefüggésben fel kell mérni, hogy a számlatulajdonos milyen nagyobb értékű ingó- vagy ingatlantulajdonnal vagy tartozással rendelkezik (a közhiteles nyilvántartások, például gépjármű- és ingatlan-nyilvántartás, illetve a KHR-adatainak beszerzése útján);
- az azonosított számlán vagy számlákon kezelt – a bűncselekménnyel összefüggően beérkező – összegre indokolt a vagyoni kényszerintézkedés elrendelése;
- a számlaforgalmi adatok alapján (beérkező és kimenő utalások) azonosítani kell a számlatulajdonos pénzügyi partnereit;
- listázni kell a készpénzfelvételek helyét, összegét, továbbá be kell szerezni az ezzel kapcsolatban elérhető ATM- vagy egyéb kamerafelvételeket (ha voltak ilyenek) a közreműködő személyek azonosítása érdekében;
- netbankos hozzáférés esetén a használt eszközre, IP-címre, másodlagos azonosításhoz használt forrásra vonatkozó adatokat, illetve az azonos alkalommal azonos hozzáférési pontról elért más számlákra vonatkozó adatokat,
- a telefonos banki ügyintézésre vonatkozó adatokat.

A joghatóság, hatáskör, illetékesség kérdését a rendőrség vonatkozásában a 25/2013. (VI. 24.) BM rendelet szabályozza: elsődleges az elkövetés helye. Az Országos Rendőr-főkapitányság már több alkalommal kifejtette, hogy a feljelentett cselekmény pontos jogi minősítésének, valamint a bűncselekmény elkövetési helyének a megállapítása a feljelentést fogadó nyomozó hatóság feladata. Mindaddig nem kerülhet sor az ügy áttételére, ameddig a hatáskör és az illetékesség kérdésében megalapozott döntés nem hozható. Ezzel az indokolatlan illetékességi viták is elkerülhetők. Az internetes hirdetéssel megvalósított csalás esetén az elkövetési magatartás – a megtévesztés – akkor (és ott) valósul meg, amikor (és ahol) a sértett megnyitja a honlapon megtévesztési szándékkal közzétett eladási ajánlatot.[14] Az idézett bírósági határozat alapján általánosságban elmondható, hogy internet útján elkövetett bűncselekmények esetén a megtévesztő hirdetés sértett általi megnyitásának helye az irányadó. Nem elégséges csupán egy valótlan hirdetés megjelenítése, majd annak valaki általi elolvasása, hanem az is szükséges, hogy a hirdetés alapján kialakuljon a sértettben a valóságtól eltérő téves tudattartam, amelynek következtében a sértett vagyoni joghatással járó cselekményt végez. Ez különösen az aukciós oldalakhoz kapcsolódó csalárd magatartások esetében nem elhanyagolandó szempont. Indokolatlan azonban az, hogy ingatlan vagy egyéb nagy értékű dolog (például személygépkocsi) értékesítésére vonatkozó hirdetés kapcsán a hirdetés megnyitásának helye szerint illetékes nyomozó hatóság folytassa le a nyomozást, mivel az ingatlan megtekintése (vagy autó megtekintése és kipróbálása, az eladó által közölt információk személyes meghallgatása, valamint áralku) nélkül ritkán születik döntés annak adásvétele vonatkozásában. A Legfőbb Ügyészség rámutatott arra, hogy amikor nem konkrétan meghatározható helyen történik a sértett bankkártyájának felhasználása (ATM-készülékből készpénzfelvétel, közvetlen vásárlás üzletben), hanem ismeretlen helyről, elektronikus úton indítják a vásárlást, és csak a célállomás helye, az online fizetési rendszer azonosítható, nem zárható ki a magyar joghatóság, illetve hogy Magyarországon (is) valósult meg tényállási elem. Ilyen feljelentések esetén a kár bekövetkezésének helye szerinti nyomozó hatóság az általános szabályokat alkalmazva rendelkezik a feljelentés kapcsán. Az említett esetben a nyomozás során a joghatóságot körültekintően vizsgálni kell, és a Btk. 3. § (3) bekezdésében foglaltak fennállása esetén a nyomozás felügyeletét ellátó ügyészségre előterjesztést kell tenni, mivel a Btk. 3. § (2) bekezdés *b)* pont alapján a magyar állampolgár, a magyar jog alapján létrejött jogi személy és jogi személyiséggel nem rendelkező egyéb jogalany sérelmére nem magyar állampolgár által külföldön elkövetett, a magyar törvény szerint büntetendő cselekményre is kiterjedhet a törvény személyi hatálya. A jogsegélyek szükségessége vonatkozásában a nyomozás felügyeletét ellátó ügyészség utasítását kell követni és annak megfelelően eljárni. Mérlegelés tárgya a jogsegély kérdése a bűncselekmény bizonyításának kérdésében azokban az esetekben, amikor arra áll rendelkezésre adat, hogy a külföldi hatóság az elkövetői kör kapcsán nyomozást folytat, illetve megalapozottan feltehető, hogy az elkövetők beazonosíthatók. Annak megállapítására, hogy külföldi társhatóság indított-e büntetőeljárást, indokolt lehet az ORFK Nemzetközi Bűnügyi Együttműködési Központ megkeresése. A Btk. 423. §-ába ütköző információs rendszer vagy adat megsértése bűncselekmények nyomozása vonatkozásában felvetődött, az illetékesség kérdéskörét

[14] BH2011. 332.

érintő gyakorlati problémák kapcsán a következő megállapítások tehetők. A jogsértő magatartás nem csupán levelezőrendszerekbe, hanem Facebook-profilokba történő jogosulatlan belépéssel, adatok törlésével is megvalósulhat. Alapvetően magyar információs rendszer tekintetében a szolgáltató megkeresésével tisztázható, hogy földrajzi értelemben hol üzemel az a szerver, amely a megváltoz(tat)ott adatokat tárolja, így az minősülhet a bűncselekmény joghatóságot és illetékességet megalapozó elkövetési helyének. Ha az inkriminált szerver külföldön található (például Facebook, Yahoo stb.), a szolgáltató megkeresésével tisztázható, hogy mely IP-címekhez kapcsolódik a bűncselekmény elkövetése, aminek alapján esély nyílik az elkövető és a lakhelye beazonosítására – amennyiben nem, úgy feltehetően TOR-hálózat használatára került sor. Ebben az esetben ez alapozhatja meg a joghatóságot, valamint az eljáró hatóság illetékességét, ugyanis a rendelet 3. § (3) bekezdése értelmében, mivel az elkövető a bűncselekményt Magyarország határain kívül követte el, a nyomozás lefolytatására – fogva tartás hiányában – az a nyomozó hatóság illetékes, amelynek illetékességi területén az elkövető utolsó ismert belföldi lakó- vagy tartózkodási helye van (Nagy 2018).

Mindegyik csalás jellegű cselekménycsoport esetében érdemes vizsgálni a bűncselekmény bekövetkezéséhez vezető folyamatot. Ennek szakaszai:

1. Az elkövető információt gyűjt a lehetséges áldozatokról.
2. A megtévesztő információt az elkövető elküldi a potenciális sértetteknek.
3. A sértetthez/képviselőjéhez/ügyintézőjéhez megérkezik a megtévesztő információ.
4. A sértett/ügyintézője a megtévesztő információk hatására károkozó cselekményt hajt végre.
5. Az anyagi javak kikerülnek a sértett birtokából.
6. A megtévesztés hatására kicsalt javak az elkövető birtokába kerülnek.

Ennek azért van jelentősége, mert egy sorozat jellegű vagy gyakran megvalósuló elkövetési módozat visszaszorítása érdekében a bűncselekmény elkövetését lehetővé tevő körülmények megszüntetése érdekében szükséges intézkedéseket tenni a hatóság részéről (szignalizáció). Az egyes területeken párhuzamosan alkalmazhatóak a bűnmegelőzés, felvilágosítás, a piaci szereplőkkel való együttműködés és a bűnüldözés eszközei.

7.5. A kapcsolódó jogértelemzés a pénzmosással összefüggésben

Fontos iránymutatást ad a helyes jogértelmezésben a Legfőbb Ügyészség Kiemelt és Katonai Ügyek Főosztályának KF.9725/2004/379-II. számú körlevele, amely anyagi jogi vonatkozásban a pénzmosás bűncselekményével összefüggésben meghatározza: „A pénzmosásért való büntetőjogi felelősségre vonás szempontjából az alapcselekmény elkövetésének helye, az elkövető kiléte vagy éppen kilétének ismeretlen volta közömbös, és annak sincs jelentősége, hogy az alapcselekmény miatt indult-e büntetőeljárás.” Tehát a vélhetően más országban elkövetett CEO-csalásokból származó és magyar számlán megjelenő összegekkel összefüggésben – ha annak valószínűsíthető a bűnös eredete – a vagyoni kényszerintézkedés (jellemzően lefoglalás) foganatosítható. A kibertérben elkövetett csalás jellegű bűncselekmények esetében fontos kiemelni, hogy a jogtalanul megszerzett javak felhasználása

büntetlen utócselekmény, de itt sem feledkezhetünk meg a saját pénz mosásáról.[15] A jelenlegi bűnüldözői gyakorlat a felhalmozott illegális javak esetében sok esetben csak azok visszaszármaztatásával foglalkozik, pedig a pénzmosás bűncselekmény megállapításának is sok esetben helye volna. A Legfőbb Ügyészség 1/2017. számú körlevele rögzíti, hogy „a Btk. 399. §-ának (3) bekezdésébe ütköző pénzmosás büntetendővé nyilvánításának elvi alapja az, hogy a bűncselekményből származó dolognak a pénzügyi-gazdasági szférában végrehajtott műveletek révén, legális forrásból származó vagyonként való feltüntetése az alapcselekmény körében már értékelten felüli, önálló társadalomra veszélyességet hordoz. Ez, az alapcselekmény által előidézett jogtárgysérelmen túlmutató veszély szűk körben ugyan, de az alapcselekmény elkövetője általi, eredetleplezési célú utócselekmények szankcionálását indokolja. E tényállás keretében ugyanakkor – a kétszeres értékelés tilalmából következően – csak azok az eredetleplezési célú magatartások nyerhetnek önálló büntetőjogi értékelést, amelyek nem szükségszerű velejárói az alapcselekmény elkövetésének." A saját bűncselekményt követő pénzmosás elkövetési magatartásai: a gazdasági tevékenység során történő felhasználás, illetve a pénzügyi tevékenység végzése (vagy igénybevétele) a tényállásszerű. A gazdasági tevékenység során történő felhasználás bármilyen tevékenység lehet, amely a gazdálkodás körében valósul meg. Ez lehet befektetés, üzleti vállalkozás létesítése, bővítése stb., és megvalósítható saját cég körében és idegen, más céghez való bekapcsolódással is. A pénzügyi tevékenység végzése vagy ennek igénybevétele akár legálisan (például részvények vásárlása), akár illegálisan (például uzsorakölcsön adása) is történhet. A készpénzes felvétel sem pénzügyi műveletnek, sem gazdasági tevékenységben való felhasználásnak nem tekinthető, ahogyan egy egyszerű pénzátutalás sem (például a hozzátartozó számlájára). A pénzügyi tevékenység fogalmát a Btk. 402. § (2) bekezdése adja meg.[16] Eszerint például üzletszerű pénzkölcsön vagy hitel nyújtása forintban vagy valutában, a követelésvásárlási tevékenység is pénzügyi szolgáltatási tevékenység. A saját pénz tisztára mosása is célzatos cselekmény. Itt egyébként az elkövető tudata a dolog eredetére szükségképpen kiterjed, hiszen az elkövető saját cselekményéből származik a dolog. Fontos említeni a Legfőbb Ügyészség 2/2017. számú körlevelét, amely eljárásjogi vonatkozású: a más joghatóság alá tartozó alapcselekmény felderítése érdekében minden lehetséges és törvényes eszközt fel kell használni. A bizonyítási eszközök összegyűjtésében és megszerzésében segítséget nyújthatnak a pénzmosás és terrorizmus finanszírozása elleni információs irodák, a vagyonvisszaszerzési hivatalok és a bűnüldöző szervek nemzetközi együttműködés keretében igénybe vehető eszközei, valamint az igazságügyi hatóságok formális és informális együttműködési hálózatai. A vagyongeneráló alapcselekmény (tipikusan csalás vagy információs rendszer felhasználásával elkövetett csalás) és a pénzmosás elkövetői körének tisztázása azért is releváns, mert azonos elkövetői kör esetében indokolatlan az alapcselekmény és a pénz-

[15] Btk. 399. § (3) bekezdés: büntetendő, aki büntetendő cselekményének elkövetéséből származó dolgot ezen eredetének leplezése, titkolása céljából
a) gazdasági tevékenység gyakorlása során felhasználja,
b) a dologgal összefüggésben bármilyen pénzügyi tevékenységet végez, vagy pénzügyi szolgáltatást vesz igénybe.

[16] Kommentár a Büntető Törvénykönyvről szóló 2012. évi C. törvényhez.

mosás nyomozásának elkülönítése, de még bizonyíthatóan eltérő elkövetői kör esetében is csak akkor lehet indokolt az elkülönítés, ha annak a büntetőeljárási törvényben írt valamely feltétele egyébként fennáll. Mindaddig tehát, amíg akár a terheltek nagy száma, akár más olyan ok nem merül fel, amely a büntetőjogi felelősség egy eljárásban történő elbírálását jelentősen nehezítené, a bűnügyek elkülönítése és az elkülönített ügy áttétele indokolatlan. Az ORFK egységes gyakorlata értelmében egyébként – a nyomozás hatékonyságának, eredményességének és időszerűségének szem előtt tartásával – egy éven túli nyomozások esetében csak különösen indokolt esetben lehet helye a bűnügy áttételének.[17]

[17] Az ORFK BF Bűnügyi Főosztály által 29000/3631/2017. ált. számon kiadott *Módszertani segédlet* a Büntető Törvénykönyvről szóló 2012. évi C. törvény 399–401. §-ai szerinti pénzmosás gyanúja miatt indult nyomozások egységes gyakorlatának kialakítása céljából.