SUB LEGE LIBERTAS

Kibervédelem a bűnügyi tudományokban

Szerkesztette:
KISS TIBOR

Dialóg Campus

Kibervédelem a bűnügyi tudományokban

Vákát oldal

KIBERVÉDELEM A BŰNÜGYI TUDOMÁNYOKBAN

Szerkesztette
Kiss Tibor

Dialóg Campus ❖ Budapest, 2020

A mű a KÖFOP-2.1.2-VEKOP-15-2016-00001
„A jó kormányzást megalapozó közszolgálat-fejlesztés”
című projekt keretében jelent meg.

Szerzők
Dornfeld László
(9. fejezet)
Gyaraki Réka
(7–8. fejezet, Simon Bélával közösen)
Kiss Tibor
(1–2. fejezet)
Kovács Zoltán
(5. fejezet)
Nagy Zoltán
(3–4. fejezet)
Simon Béla
(6. fejezet, 7–8. fejezet, Gyaraki Rékával közösen)

Szakmai lektor
Krasznay Csaba

Tartalom

Vákát oldal

1. A kibertér fogalma

Kiss Tibor

Az elmúlt évtizedekben napvilágot látott kibertér-definíciók közül az egyik legnépszerűbb William Gibson virtuális valósága, ami a *Neurománc* című világhírű regényében terjedt el világszerte. Gibson szerint a kibertér egy „akarattól független hallucináció, amelyet törvényes felhasználók milliárdjai tapasztalnak naponta, egészen a matematikai alapfogalmakat tanuló gyermekig. Az emberi civilizáció összes számítógépének adatbankjaiból származó adatok grafikus megjelenítése. Hihetetlen összetettség. Az elme nem-terébe nyújtózó fényvonalak, adatok nyalábjai és csoportjai. Mint a távolodó városi fények" (Gibson 1999, 65.). A kibertér gibsoni értelmezése csupán az agyinterfész révén „belakott" alternatív valóságot fejezi ki, nem egy olyan érintkezési és interakciós közeget, amelyben az emberi akarat lenyomatai tisztán kirajzolódnak – láthatóvá téve az emberi magatartásminták széles spektrumát. A kibertér-definíciók különböző formái az Európai Unió tagállamainak stratégiai dokumentumaiban is megtalálhatók. Magyarországon a Nemzeti Kiberbiztonsági Stratégia deklarálja eszerint: „A kibertér globálisan összekapcsolt, decentralizált, egyre növekvő elektronikus információs rendszerek, valamint ezen rendszereken keresztül adatok és információk formájában megjelenő társadalmi és gazdasági folyamatok együttesét jelenti."[1] A stratégiai fogalmak viszont jogi-bűnüldözési, közigazgatási nyelven szólalnak meg, nélkülözve a kibertérben zajló kölcsönhatásokat tudományosan is magyarázni képes fogalmi elemeket. Kötetünk témáját tekintve egyrészről célszerű a jogi-bűnüldözési megközelítést alapul venni, másrészről azokat a technodiskurzusokat, amelyekben a kiberteret technikai megközelítésből vizsgálják és építik fel. A kibertér meghatározásáról szóló részletes technikai megközelítések egyikét Fang Binxing kibertér-szuverenitást vizsgáló, átfogó tanulmánya tartalmazza. A szerző magyarázata szerint a szóösszetételből a *kiber* tag csomópontokból, kapcsoló csomópontokból, élekből és terhelésekből álló összekötő rendszerként értelmezhető, olyan, mint egy úthálózat, amelyben a végcsomópontok a végső állomásokat, a kapcsoló csomópontok a végcsomópontok közötti megállókat, az élek az állomásokat összekötő úthálózatot, a terhelés pedig a közlekedő járműveket jelöli. Abban az esetben, ha ezt egy információs hálózatra vonatkoztatjuk, akkor a *kiber* kifejezés információs és kommunikációs technológiai hálózatokat összekötő rendszerként értelmezhető, amelybe beletartoznak a távközlési, telefonos, nyilvános távíró, telex-, adatátviteli, faxkommunikációs, képkommunikációs, videotext-kommunikációs, mobil kommunikációs, műsorszóró televíziós, online szociális, érzékelő, ipari vezérlő és kvantumkommunikációs hálózatok, az internet, a mobilinternet és a tárgyak internete. Fang szerint a *kiber* és a *tér* együttes használata már komplex jelentésű szóösszetétel, és négy alapvető elem együttesét jelöli:

[1] Magyarország Nemzeti Kiberbiztonsági Stratégiájáról szóló 1139/2013. (III. 21.) Korm. határozat 3. pontja.

1. az információs és kommunikációs infrastruktúrát; 2. az adatok összességét; 3. a felhasználók és szerepkörök összességét; végül 4. a műveletek és tevékenységek összességét (FANG 2018). Az utóbbi kettőnek kiemelkedő szerepe van, ugyanis a kibertér akkor hiteles és valósághű, ha képes kivetíteni a fizikai társadalom működését, amelynek szerves része a felhasználó és az általa végzett művelet. Így például az online szociális hálózat a kibertér olyan hálózata, ahol fizikai szerepek működnek – azzal a különbséggel, hogy valós identitásukhoz képest lehetnek titkosak. Fang a *tér* fogalmát úgy összegezte, hogy a tér megértésének az emberi viselkedés és gyakorlat valóságán kell alapulnia. Jelentőségét a tér és ember kölcsönhatásában kell keresni, miközben a tárgyak vagy dolgok létezése és azok mozgása a tér jelentésének két fő tulajdonságát jelölik. Ezzel szemben utalt arra is, hogy miközben a kibertér szükségszerű kapcsolatban van a fizikai világgal, bizonyos szempontból mégis elválik attól. A kibertér abban mindenképp különbözik minden más tértől (például vízi, szárazföldi vagy légtér), hogy alapvetően senki sem képes teljes mértékben uralni és irányítani, ugyanakkor a technikai képességekkel rendelkező államok mégis felhasználhatják gazdasági, politikai, tudományos, kulturális és katonai céljaikra (FANG 2018). Ehhez képest a kibertér fogalmát egyes társadalmakban eltérő nézőpontból közelítik meg. A definíciós különbségek a négy alapvető elem kombinálásával ötféle formában tagolódnak. Eszerint a kibertér 1. információs és kommunikációs infrastruktúrák összessége; 2. információs és kommunikációs infrastruktúrák, illetve adatok összessége; 3. információs és kommunikációs infrastruktúrák és adatok, illetve a kibertérben lévő felhasználók összessége; 4. információs és kommunikációs infrastruktúrák, adatok és műveletek összessége; 5. információs és kommunikációs infrastruktúrák, adatok, felhasználók és műveletek összessége. Ez utóbbi képes a kiberteret valóságos és hiteles formájában kifejezni. Fang szerint az elmúlt években az infrastruktúrák, adatok, emberek és műveletek kombinációja mentén háromféle definíciós nézőpont került a figyelem középpontjába. Az első *a nyilvános* nézőpont, amely szerint a kibertér az ember által gyártott olyan elektromágneses tér terminálokkal, számítógépekkel, hálózati eszközökkel, amelyeken keresztül a felhasználók létrehozzák, tárolják, továbbítják, megjelenítik és használják az adatokat. A kibertérben az ember, a gép és az adat kapcsolódásával és kölcsönhatásával valósítható meg az információszolgáltatás, ami befolyásolja az emberek életét (FANG 2018). A másik az *akadémiai* nézőpont. Eszerint a kibertér olyan ember által alkotott hely, ahol a felhasználó információs és kommunikációs technológiák által általános jeleket (például optikai, elektromos, akusztikus, mágneses jeleket) generálhat, továbbíthat, tárolhat, dolgozhat fel és jeleníthet meg, és ezzel kifejezheti akaratát (FANG 2018). A harmadik nézőpont a *nemzetközi szervezetek* definícióiból ered. A kibertér olyan mesterséges tér, amely az információs és kommunikációs technológia infrastruktúrájára épülve támogatja az emberek információs tevékenységét, vagyis az adatok generálását, tárolását, átvitelét, megváltoztatását, használatát és megjelenítését megvalósító műveleteket (FANG 2018). Jason Whittaker megfogalmazása nem tér el Fang Binxing gondolatmenetétől. A kiberteret olyan technológiai ragasztóként jellemzi, amely a legtágabb értelemben is információs és kommunikációs technológiai hálózatok heterogén rendszerét alkotja, vagyis olyan különböző hálózatok összessége, amely egymástól eltérő digitális interakció vagy kommunikáció létrehozására képes. A kibertér hibrid tér, ami hatással van a társadalmakra és azok kultúrájára, amelybe az internet, a virtuális valóság és a hagyományos telekommunikációs hálózatok egyaránt beletartoznak (WHITTAKER 2004). Douglas Rushkoff elvont meghatározással a kiberteret olyan három-

dimenziós világként írja körül, amelyben az emberek időtől és helyszíntől függetlenül kerülhetnek egymással kölcsönhatásba. Ebben a világban a számítógépek hálózatokon keresztül kapcsolódva fedik le az egész világot. Rushkoff szerint a kibertérnek metaforikus értéke van azáltal, hogy az emberi kapcsolatokat hasonlóképp teremti meg, mint a rituálék, ahol az idő, a fizikai távolság és a test korlátjai értelmetlenek, sokkal inkább az emberi tudat számít. A felhasználók információs és kommunikációs csatornákat, számítógépes programokat és adatokat használva kerülnek egymással kölcsönhatásba, kilépve a fizikai valóság szabályai alól (RUSHKOFF 2002). Hasonlóképp vélekedik Thomas Ploug, aki a kiberteret olyan virtuális térnek nevezi, amelyben az egymással összekapcsolt hálózatokon a felhasználók kölcsönhatásba lépnek egymással. A kibertérbe való belépést és az interakciót az összekapcsolt információs és kommunikációs technológiai hálózatok, ezen belül az internet teszi lehetővé. A kibertér egyik legfőbb eleme a *virtuális természete,* ami azt jelenti, hogy független más tértől, és nem kívánja meg, hogy a virtuális térben kölcsönhatásba kerülő felhasználók meghatározott helyen legyenek adott pillanatban. Ezzel szemben a virtuális tér fogalma nem ellentétes a fizikai valósággal, és attól nem is független. A kibertér másik fontos eleme *az adat, a számítógépek összekapcsolt hálózata* és a hálózatokat összekapcsoló *internet.* Ploug kiemeli, hogy ez utóbbi nem egyezik meg a kibertér fogalmával, viszont nem igazán létezhet anélkül sem. A kibertér olyan helyként jellemezhető, amely az adat, a számítógépes hálózatok és az azokat összekapcsoló internet létezését és működését felügyeli (PLOUG 2009). A kibertér harmadik fontos eleme az *interakció.* Az interakcióval olyan szándékos cselekvések határozhatók meg, amelyek a fizikai világban az emberek által történnek, valamint az emberek között alakulnak ki. A kibertérben zajló kölcsönhatás minimuma egy válasz egy ingerre. A kibertérben zajló kölcsönhatásnak nagyon sok formája lehet, ezek közül kiemelhető az internetes pénzügyi tranzakció, az online vásárlás, az online játékok szereplőinek interakciói vagy épp a fájlok fel- és letöltése. Ilyen kölcsönhatásokon alapul a virtuális közösségi működés, a vitafórumok vagy a közösségi oldalak kommunikációja. A kölcsönhatás nem feltétlenül valós idejű, lehet egy weboldal tartalmára való reakció, amikor egy vásárló az online kereskedelmi oldalról választ, majd később vásárol. Ide tartozik az adatkeresés folyamata is, amelyben a felhasználó folyamatos kölcsönhatásban áll a keresőmotorokkal. Ploug szerint az interakciók tovább tipizálhatók aszerint, hogy kik között és milyen módon zajlanak. Eszerint különbséget kell tenni a valós idejű kapcsolatok és a nem valós idejű kapcsolatok között, részben az anonimitás, részben a felhasználók közötti közvetlenség miatt. A valós idejű kapcsolatokban olyan kommunikáció zajlik, ami az azonnali reakciót jelenti egy ember akciójára, míg más közvetett kapcsolatban ezen kívül más inger is éri a felhasználókat. Az első esetben olyan kölcsönhatásról van szó, ahol a két felhasználó közvetlen információja az inger, a másik esetében pedig egy közvetett tartalom vagy ingerkeltő hatás. Az anonimitás a közvetlen, valós idejű kommunikációban kevésbé, míg a nem közvetlen kapcsolatban fokozottabban érvényesülhet (PLOUG 2009). Martin Weik definíciója közvetlenül az összes definícióhoz kapcsolódik. Szerinte a kibertér az integrált számítógépes és kommunikációs rendszerek területe. Olyan információs világ, amely magában foglalja az információ előállítását, tárolását, cseréjét, elérését és használatát, illetve általában magában foglalja a kommunikációs rendszerekhez és a közös hordozóhálózatokhoz kapcsolódó számítógépek és adatbázisok használatát világszerte (WEIK 2001, 331–332.).

A definíciókból egyértelműen kirajzolódik, hogy a kibertér információs és kommunikációs technológiai infrastruktúrája nem szűkíthető le az internetes közegre. Az *internet* voltaképpen egy folyamatosan növekvő, nyílt elérésű, korlátlan és áttekinthetetlen mennyiségű információt tartalmazó, globális hálózat, amelynek gerinchálózatához nagy mennyiségű részhálózat kapcsolódik – az internetszolgáltatók közvetítésével. Az internetes hálózatban a számítógépek internetprotokollok (például a TCP/IP: *Transmission Control Protocol/Internet Protocol*) mentén kommunikálnak egymással (BÁRTFAI 2017). Ebbe a fogalomkörbe értendők a nem magáncélú, de nehezen elérhető internetes hálózatok is (például a *deep* vagy *dark web*). Bár a kibertér az internetnél sokkal szélesebb teret jelent, az interneten zajló műveletekkel generált kölcsönhatások jelentős része mégis vonatkoztatható a kibertér egészére. Pontosabban az internet globális hálózata egyes interakciók megfigyelése esetén a kibertér reprezentatív kutatási terepe.

1.1. Az ember és a kibertér kapcsolata

A technikai megközelítésű meghatározásokból egységesen kitűnik, hogy a kibertér alapvetően ember alkotta nóvum. Létezésének legfontosabb feltétele az információs és kommunikációs technológiák infrastruktúráinak megléte, illetve az adatok felhasználásával az infrastruktúrákon keresztül végzett emberi műveletek összessége. A felhasználó az adatok létrehozásával, tárolásával, továbbításával, megjelenítésével, felhasználásával vagy feldolgozásával hozza létre azt a virtuális valóságot, amelyben képes önmagát leképezni és ennek révén interakcióba lépni másokkal. A kibertérben történő műveletvégzésnek azonban két előfeltétele van. Az egyik a *hozzáférés,* a másik a *digitális kompetencia.*

Az általános kompetencia a személyiség olyan megismerési folyamat eredményeként kialakuló, képességalapú tulajdonsága, amely döntő szerepet játszik az autonóm magatartásban. Két alapvető alkotórésze a valóság absztrakt tükröződéséből származó ismeretjellegű, illetve cselekvéssel kialakuló, képeségjellegű tudás (FEHÉR–LAPPINTS 1999, 55., 109.). A digitális kompetencia az általánosan értelmezett kompetenciától abban tér el, hogy a hagyományos szocializációs tér és a kibertér összefonódott közegében formálódik, ahol az objektív valóság komplex tanulás útján alakul ismeret- és képességjellegűvé (RICHARDS 2000). A digitális készségek szintje az alapvető felhasználói tudástól a számítástechnikai szakértő ismeretszintjéig bezárólag széles skálán helyezkedhet el, és szoros összefüggésben áll az egyén cselekvési lehetőségeivel. Fogalmi körébe tartozik a számítástechnikai eszközök kezelésének technikai alaptudása (például billentyűzet, egér, okostelefon kezelése), a hálózatokhoz való kapcsolódás, a hálózatok és a szoftverek használata, valamint az adatkezelés (például az internet használata, operációs rendszerek használata, információgyűjtés, -feldolgozás, -tárolás, -megosztás). A digitális kompetencia a magabiztos műveletvégzéstől a virtuális kommunikációra való képességen és a kritikus tartalomértelmezésen át az online társadalmi szerepvállalással bezárólag átfogó tudást és képességhalmazt jelent. A digitális kompetencia a modern társadalmakban a tanulás, a munkavégzés és a szabadidő eltöltésének lehetőségét, valamint az önfejlesztésre való motivációt erősíti – mélyen összeforrva a hagyományos kompetenciákkal (FERRARI 2013, 7–32.). A digitális kompetencia pontosabb értelmezését adja Z. Karvalics Lászlónak az információs írástudásról és az információs műveltségről alkotott definíciója. „Az információs

írástudás az írás, olvasás és számolás mellé társuló új alapképességek együttese, amelyet a felnövekvő új generációk az iskolában és korai felhasználóként »szívnak magukba«, az idősebbek pedig élethosszig tartó tanulásuk részeként teszik magukat alkalmassá az információs ökoszisztémában való aktív jelenlétre" (Z. KARVALICS 2017, 239). A fogalom alkotója szerint a kifejezést először Paul G. Zurkowski használta, amikor a korai mikroszámítógépes közegben kialakult digitális szakadék két végletét megtestesítő digitális írástudók és a digitális analfabéták közötti különbségeket vizsgálta. Az információs írástudás még a mai eszköz- és programkörnyezetben is információs alapkészségek meglétét kívánja meg. Eszerint az információs írástudáshoz alapvető követelmény „az eligazodás, keresés, válogatás, megértés, feldolgozás-rendszerezés, értékelés, az információkezelés képessége az igény felismerésétől az alkalmazásig vagy új információ létrehozásáig" (Z. KARVALICS 2017, 240.). Az információs műveltség az előző fogalomtól eltérő, de attól nem független. „Az információs műveltség az információs írástudást megtestesítő készségek és jártasságok aktualizálásakor fokozatosan gyarapodó magasrendű érzékenység és tájékozottság az információs kultúra világában. A hagyományos műveltségágak kiegészülése a digitálisan született és digitálisan elérhető tartalmak fogyasztásával és teremtésével" (Z. KARVALICS 2017, 331). Az információs műveltség abban tér el az információs írástudás standardizáló és műveletvégző jellegétől, hogy sokkal inkább a tájékozottságot, az információs kultúra egyfajta autonóm rendjét, az ebből fakadó kritikai potenciált (digitális kultúrára való reflexiót) fejezi ki (Z. KARVALICS 2017, 331.). Az információs – más néven *digitális* – írástudás és műveltség tehát a digitális kompetencia két legnagyobb részét képezi.

A *hozzáférés* és annak különböző szintje olyan objektív tényező, amely a kompetencia technikai és hálózati infrastruktúrákkal történő érvényesülésének lehetőségét adja, pontosabban az egyén kibertérbe való belépését, bennmaradását és műveletvégzését biztosítja. A hozzáférés teszi lehetővé az *online állapotot,* ami a számítástechnikai eszközökkel és az internetszolgáltatók által az internet hálózatára csatlakozott, internetszolgáltatások felhasználására és online tevékenységek végzésére kész állapotot jelöli. A hozzáférés által válik lehetővé az *online tevékenység,* vagyis a csatlakozást követően az internet hálózatán az internetszolgáltatások felhasználásával végzett tevékenységek összessége. A hozzáférés gyengesége vagy hiánya a számítástechnikai eszközök és az internet elterjedésének korai szakaszában a digitális szakadék kialakulásának egyik jelentős oka volt. A digitális szakadék azt jelentette, hogy a társadalom tagjainak egy része a digitális kompetencia hiányán felül nem rendelkezett számítógéppel, internetelőfizetéssel, valamint a környezetében nem volt infrastrukturálisan kiépített szolgáltatás és lefedettség. A hozzáférési korlátozottság a modern társadalmakban jelentős mértékben oldódott, köszönhetően annak, hogy a megfizethetőbb internetet sok helyütt kiépítették, olcsóbb és könnyen kezelhető számítástechnikai eszközöket gyártottak, illetve a számítástechnikai eszközök kezelésének ismereteit az iskolák tananyagába illesztették.

1.2. A kibertér interaktív arénája

Don Tapscott és Anthony D. Williams szerint a kibertér ma már arra motiválja a társadalmi közösségek tagjait, hogy a kezük ügyébe kerülő számítástechnikai eszközökkel együttműködjenek, és az új környezet sajátosságait hasznosítva értéket teremtsenek, versenyezzenek,

az új technológiák mentén vegyék ki részüket az innovációból és a jólét megteremtéséből (TAPSCOTT–WILLIAM 2006, 21.). A kibertérben zajló kölcsönhatásoknak teret adó globális hálózatnak két meghatározó fejlődési mérföldköve hatott leginkább az emberi viselkedésre. Az egyik a virtuális jelenlétet megalapozó web 1.0, a másik a szimmetrikus információáramlást és az interaktív részvételt megteremtő web 2.0 korszaka volt. A web 1.0 Tim Berners-Lee nevéhez fűződik, aki 1994-ben a *Conseil Européen pour la Recherche Nucléaire* (CERN) mérnökeként a linkek potenciálját egyesítve olyan rendszert fejlesztett ki, ami a HTML *(Hypertext Markup Language)* szöveggel formázott weboldalaknak egy szabványos URL- *(Universal Resource Locator)* címet osztott ki, így az URL-címekkel ellátott oldalak a rendszerben alkalmazott HTTP *(Hypertext Transfer Protocol)* mentén a hálózat bármely pontjáról elérhetővé váltak. Abból a célból, hogy a weboldalak a távoli számítógépekről is megtalálhatók és megjeleníthetők legyenek, a mérnök egy böngészőprogramot készített, és ezzel megalkotta a *Word Wide Web* rendszerének alapját. Voltaképpen ezzel indult a statikus tartalmak egyirányú közzétételének korszakát jelentő web 1.0. A hiperhivatkozásokkal összekapcsolt, tájékoztató jellegű weboldalakon megjelenő tartalmak pusztán csak olvasásra voltak alkalmasak. A főként Netscape navigátorral működő web 1.0 szolgáltatások abból a szempontból nagy előrelépésnek számítottak, hogy a felhasználók az interneten szörfölve gyűjthették és felhasználhatták az információkat – megteremtve ezzel az online jelenlétet. Az interaktivitás abban merült ki, hogy a webhelyek látogatóinak megjegyzéseit egy vendégkönyvoldalhoz adták hozzá, ami egy erre a célra kifejlesztett levelezőszolgáltatáson keresztül egy űrlap kitöltésével valósulhatott meg. A világháló exponenciális terjedésével azonban egyre több potenciális szolgáltatási lehetőség kínálkozott egyre több felhasználó részvételével – különösképp az internetes kereskedelemben (LEINER et al. 1997, 12–14.). A 2000-es évek elején beindult a Dot.Com domain népszerűsége és az erre épülő üzleti tevékenységek köre. Felhasználók millióit vonzották a portálszolgáltatások (Yahoo), az online boltok (Amazon), aukciós oldalak (eBay), internetes banki szolgáltatások, hír- és reklámcsatornák, az internetes utazási szolgáltatást kínáló és toborzó oldalak (O'REGAN 2016, 173.). A Tim Berners-Lee nevéhez fűződő web 1.0 tehát az információmegosztás korszakát vezette be, ami önmagában alkalmas volt a tudásbázisok elérésére, a digitális írástudás és műveltség fejlődésére, valamint az információ és a bizalom felértékelődésére. A web 1.0 szerepét az internetes szolgáltatások generális átformálásával a Tim O'Reilly koncepcióján alapuló web 2.0 vette át 2004-ben. A szimmetrikus kommunikációval a szolgáltató által biztosított keretrendszerben a felhasználóknak lehetősége nyílt a tartalmak létrehozására és megosztására, sőt, néhol a tartalmi kereteket is a felhasználók alakíthatták. A web 2.0-val olyan interaktív közösségi jellegű terek nyíltak meg, ahol a szereplők értéket adhattak a folyamatosan bővülő tudásbázishoz (CSEPELI–PRAZSÁK 2010, 18.). Az internetre jellemzővé vált a részvétel kultúrája, amelynek szellemében szociális hálózatok különböző rétegei szerveződtek különböző kommunikációs lehetőségekkel (TAPSCOTT–WILLIAMS 2007, 23.).

1. táblázat

A virtuális közösségek szerveződését és az interaktivitást elősegítő web 2.0 szolgáltatások

Web 2.0 szolgáltatások	Interaktív közösségek
Közösségi oldalak Chatszolgáltatások és chatfórumok VoIP- (Voice over IP) alkalmazások	Az online társas oldalakon tartalommegosztás, -küldés és -fogadás funkciója, a beépülő valós idejű kommunikációs alkalmazások (VoIP és chat) működése megszámlálhatatlan kapcsolati kötelék létrejöttét támogatta. A *peer to peer* audio- és videokommunikációval az önkifejezés és önérvényesítés valamennyi fizikai érintkezést nélkülöző módjával élhettek a felhasználók. A közösségi weboldalakon teljesedett ki a digitális identitás, ami először regisztrációs adatok (például a személyes adatok, e-mail-cím), majd egyre részletesebb információk (például vágyak, gondolatok, érzelmek, titkok) összességeként jelent meg. Az interneten szerveződő egyéni és közösségi identitás a fizikai azonosságtudat virtuális adaptációjaként az internetes kapcsolatok legfontosabb alkotóeleme lett. Az egyénről és közösségről szóló információk a közösségi oldalakon profilokban összpontosultak, vagy más rendszerek regisztrációs adatbázisaiban.
Levelezőrendszerek	Az ingyenesen is elérhető elektronikus postai szolgáltatások nem valós idejű információcserét bonyolító felhasználókat tömörítettek. Az információcsere és a kommunikáció egyik legjelentősebb rendszereként egyre több chatszolgáltatást indítottak, csoportos csetelési lehetőségekkel.
Kép- és videómegosztó oldalak, podcastok, közösségi zeneajánló oldalak	A web 2.0 terjedésével a multimédia-megosztó és -ajánló oldalak köré szerveződő felhasználók zene- és videótartalmak fel-, illetve letöltésével, megosztásával és címkézésével (tegelés) kovácsolódtak közösséggé.
Blogok	A blogszolgáltatások a tartalmaikat látogatók sokaságából alakítottak (kritikai) véleményt formáló közösségeket.
Wikipédia és más tudásmegosztó wikik	A web 2.0 markáns sajátossága a wikik, avagy a tudásmegosztó weboldalak megjelenése. A Wikipédia jelenleg is egy olyan kollektív tudásbázis, amelynek tartalma folyamatosan gazdagodik azzal, hogy a felhasználók új és friss információkkal, ismeretanyagokkal töltik meg. A szabadon elérhető oldal tartalma a kollektív intelligencián alapul, alulról építkező tudásfejlesztő közösségi cselekvés produktuma (Csepeli–Prazsák 2010, 21.).
Online kereskedelemi oldalak és aukciós oldalak	A virtuális piacterek (például az eBay, Amazon) a weboldalak szimmetrikus működésének köszönhetően terjedtek, ahol aktív információcsere mellett felhasználók millióinak kereskedelmi tevékenysége zajlik.
Hírforrások, hírmegosztó oldalak	Egyre több online hírszolgáltató tette szabaddá tartalmai véleményezését, aktivizálva a látogatók részvételét. Hírcsatornák, hírfigyelő szolgáltatások segítik az interaktív híroldalak összegyűjtését, rendszerezését.
Onlinetárhely-szolgáltatók	Az internetes tárhelymegosztó szolgáltatások és a felhőszolgáltatások az adatok tárolását és nagyobb közösségekben való megosztását biztosították (O'Regan 2016, 182–186.).
Online játékok	Felhasználók tömege léphetett kapcsolatba egymással online szerep- és stratégiai játékok grafikus színterein virtuális karakterekkel, tartós vagy átmeneti csoportokban.

Forrás: O'Regan 2016

1.3. A digitális identitás és a kapcsolódás jelentősége

Az emberi magatartásminták legkülönfélébb formái a web 2.0 szolgáltatásai révén váltak igazán érzékelhetővé és megítélhetővé a kibertérben. Az emberi részvétellel járó virtuális kölcsönhatások iránya és kimenetele voltaképpen az emberi meghatározottságokon (személyiség, jellem, képesség, adottság, habitus) alapul. Ebből ered az elvárt normák betartására való képesség, a külső és belső viselkedési kontrollmechanizmusok érvényesítésére való hajlandóság, az egyén értékítélete, cselekvés- és gondolkodásmódja, akarati megnyilvánulásainak összessége. A kibertérben az emberi jellemzőkben gyökerező megnyilvánulások a hagyományos identitás virtuális térbe adaptált formájával, illetve ezek kapcsolati hálójában váltak láthatóvá. Katarzyna Musiał és Przemysław Kazienko hálózatkutatók szerint a felhasználó a kibertérbe való belépését követően digitális identitásával válik virtuálissá. A digitális identitás egyik alappillére technikai, vagyis olyan beállításokból és adattartalmakból áll, ami magában foglalja a felhasználó regisztrációs adatait, létrehozott profiljait, postafiókjait, az általa önmagáról tárolt, továbbított, megjelenített és feldolgozott információk összességét (MUSIAŁ–PRZEMYSŁAW 2009, 40.). A digitális identitás másik fontos elemét emberi meghatározottságok alkotják, amelyeket a felhasználó technikai beállításain keresztül az adatok kezelésével kifejez. A felhasználók ezzel a komplexummal *kötődnek* egymáshoz, és hoznak létre hálózatokat, majd hálózati rétegeket. A szerzők szerint ezekben a rétegekben a kapcsolatok lehetnek közvetlenek, majdnem közvetlenek és közvetettek. A *közvetlen* kapcsolódás olyan kötődést jelent, amelyben két felhasználó úgy lép kommunikációs kapcsolatba egymással, hogy abban más résztvevő nem szerepel. A kötődés ez esetben tudatos, tartós, szimmetrikus, gyakran rejtett és ritkábban nyilvános. A *majdnem közvetlen* kapcsolat két felhasználó között több résztvevő által képződik. Ebben a formában inkább véletlenszerű, gyakran ideiglenes, legtöbb esetben nyilvános és szimmetrikus kötődésekről beszélhetünk. A *közvetett* kapcsolatban a felek között nagy a távolság. Az információ több résztvevőn át áramlik, és a legtöbb esetben rétegek között alakul ki, véletlenszerű, ideiglenes, nyilvános és aszimmetrikus. A hálózatkutatók szerint az internetes identitások közötti *kötődések* taxonómiájával a felhasználók viszonyulásai, működési módjai és interakciói pontosabban értelmezhetők és strukturálhatók, voltaképpen körülírják az ember és az emberi kapcsolatok működését (MUSIAŁ–PRZEMYSŁAW 2009, 58–67.). Egyes kutatók szerint az online kötődések elemzése merőben más megközelítést igényel, mint az offline kapcsolatoké, ugyanis ebben a környezetben oldódik a formális kommunikációs kötöttségekhez való viszonyulás. Míg a hagyományos környezetben két ember kapcsolata magas elvárások és formális feltételek szerint alakul, addig az online térben kötöttségek nélkül formálódhat. Barry Wellman és Milena Gulia népszerű kutatásának eredménye azt támasztotta alá, hogy az online térben a kevésbé szabályozott *gyenge kapcsolatokban* az internetes közösségek támogatóbbak és heterogénebbek az offline csoportokhoz képest, amelyben az identitás elrejtésének lehetősége jelentős szerepet játszik. A gyenge kapcsolatok azért hangsúlyosak, mert lehetséges a hagyományos színtér formális elvárásainak mellőzése és ezáltal az eltérő társadalmi státuszú egyének találkozása. A gyenge kapcsolatok a bizalomra épülő támogatást, az őszinte megnyilatkozásokat és az önkifejezés szabadságát eredményezik – szemben azokkal az elképzelésekkel, hogy mindez csak erős kapcsolatokban alakulhat ki (WELLMAN–GULIA 1997, 4–10.). Manuel Castells ugyanakkor

kihangsúlyozta, hogy a hálózati társadalomban a gyenge kapcsolatok kockázatosak lehetnek, mert az internetes kommunikációban (CMC) alacsony kulturáltsági szintű felhasználók is részt vehetnek, ezért a gátlástalan kommunikáció lehetősége is adott (CASTELLS 2005, 473.). A digitális identitások és azok kapcsolati hálózata alkotja azt a felhasználói formációt, amelyben az érzelmek, gondolatok, vágyak és szükségletek által vezérelt virtuális magatartásminták keletkeznek (például a kritikai véleménynyilvánítás vagy a dominanciagyakorlás). Az ilyen megnyilvánulások viszont vegyesek: lehetnek a hagyományos társadalmi normákat követők és azzal szöges ellentétben állók.

Vákát oldal

2. Kiberdeviancia

Kiss Tibor

2.1. A normák változása a kibertérben

A norma alapja az érték, ami elsősorban valaminek azt a tulajdonságát jelöli, ami az egyén és a társadalom többsége számára kiemelkedő fontosságú. Az értékek nem függetlenek az adott társadalom kultúrájától, ugyanakkor közmegegyezésen alapuló, közös tudás eredményeként megjelenő, elvont manifesztációkként jellemezhetők. Az értékek kulturális alapelvekként kifejezik, hogy egy társadalomban mit tartanak jónak, rossznak, kívánatosnak vagy elítélendőnek mindamellett, hogy számos formában és módon válnak láthatóvá. Lehetnek elvek, eszmék, attitűdöket tükröző érzelmek, ideálok, trendek alapjai, állhatnak különböző magatartásminták, együttélési formák fókuszában, kifejeződhetnek kézzel fogható tárgyakban (Fehér–Lappints 1999, 29.; Andorka 2006, 569.). Az értékek akkor válnak társadalmivá, amikor a túlnyomó többség érdekéhez vagy szükségletéhez kötődve is értékként jelennek meg. Az ilyen módon közössé váló értékek felminősítése idővel a társadalom minden tagja részéről kötelezővé válik, vagyis normává emelkedik (Rosta 2007, 22.). A normák a társadalom többsége által jelentős értékekből eredeztethető magatartási szabályok, amelyek követése és betartása a társadalom minden tagja részéről kötelező, megszegésük formális vagy informális szankcióval jár. A normák összességeként kialakuló normarendszer kiépítése a társadalom stabil működésének alapvető feltétele, az együttélés biztosítéka, a közösség integritásának garanciája. Kijelöli a társadalom tagja számára a normális működési határokat, előírja azokat a cselekvésmódokat, amelyekhez az egyén viselkedési mintáit igazítani tudja, és a társadalom normakövető és normatartó tagjaként élhet. A legtöbb társadalomban a normák különböző szinteken pozícionáltak attól függően, hogy mennyire fontos és meghatározó értékeken alapulnak. Ebből az okból a normaképződést tárgyaló szociológiai irodalmakban a magatartási szabályokat jogi normák, erkölcsi normák és szokásnormák mentén tagolják. Míg a jogi normák megsértése jogszabályokban deklarált szankciókkal jár (például a bűncselekmények szankciói), az erkölcsi normák és a szokásnormák társadalmi rosszallást, informális elítélést, kiközösítést eredményezhetnek (például az illemszabályok megsértése). A szociálpszichológia képviselői a társas normák cselekvésmeghatározó erejének magyarázatában a leíró és az előíró normák funkcióját különösképp kihangsúlyozzák. A leíró társas normák a közösség tagjainak cselekvés-, érzés- és gondolkodásmódját prezentálják, vagyis azt, hogy a csoport tagjai valójában milyen értékek mentén működnek. Az előíró normák összessége pedig azt fejezi ki, hogy egy közösség tagjainak hogy kell gondolkodnia, éreznie és cselekednie, milyen normákat kell képviselnie. Mindkét társas norma közmegegyezésen alapul, gyakran a leíró normák előíró, társas normákká alakulnak át, vagyis amit a közösség többsége

tesz, azt később mindenkitől elvárt magatartásmintaként kell képviselnie. Akkor, amikor az egyén érzés-, cselekvés- és gondolkodásmódját csoportnormákhoz igazítja, valójában a leíró és előíró normák betartására törekszik, így a társadalom konform tagjaként viselkedik (SMITH–MACKIE–CLAYPOOL 2016, 497–498.). A kibertér és az annak esszenciális részét képező internetes hálózat számos emberi cselekvésforma megjelenésének terepe, ezért sokan úgy vélik, hogy az ember a kibertérben is a szocializációja során internalizált és interiorizált értékek és normák betartásával működik. Ezt a nézőpontot Peter N. Grabosky az *old wine in new bottles* kifejezéssel írta körül, amivel arra utalt, hogy a virtuális környezetben leképeződő, szokványostól eltérő magatartásmintázatok valójában hagyományos normasértések, csupán a környezet más. Szerinte az emberi motivációt az anonimitásra épülő interperszonális kapcsolatokat, a titkos működést, az ellenőrzésben felmerülő új kihívásokat, a földrajzi határok elmosódásával járó kiterjedt bűnözést sem lehet újnak tekinteni (GRABOSKY 2001, 243–249.). Grabosky gondolatmenete valójában a normasértésekre irányult, de a normákra éppúgy vonatkoztatható, vagyis a kibertérben megvalósított normasértés nem több, mint a hagyományos normahatárok átlépése. Ezzel szemben célszerű szem előtt tartani azokat a jelenségeket, amelyek a hagyományosan felfogott normákhoz és normasértésekhez képest eddig nem megszokott szerkezetben jelentek meg a kibertérben, ugyanakkor kezelésükre eszközbéli séma nem áll rendelkezésre (például a *cyberbullying*). A megváltozott magatartásformák mögött ma már olyan új tényezők állnak, amelyek könnyen láthatók, és a kibertér sajátosságaiban gyökereznek. Ezek a tényezők nem feltétlenül és közvetlenül vezetnek normasértő magatartásokhoz, de közvetett módon kapcsolódnak azokhoz:

- *Új javak.* Az informatikai rendszerek és a rendszereken belül tárolt adatok új értéket jelentenek, megszerzésük a hagyományostól eltérő technikai eszközöket, módszereket igényel, ami a *hacking* különböző formáiban és az automatizált eszközök, *malware-ek* használatában nyilvánul meg leginkább.
- *Szabályozatlanság.* A felhasználók köre napjainkra multikulturális közösséggé nőtte ki magát, sokféle érték- és normarendszert képviselve. Az egyre több területre kiterjedő társadalmi szabályozó erők ellenére koherens, univerzálisan is érvényes morális szabályrendszer még nem alakult ki, így a normák és ezzel együtt a deviáns magatartás értelmezése is bizonytalan.
- *A környezet jelentéktelenségének látszata.* A klasszikus normasértő megnyilvánulások némelyikét a virtuális környezetben enyhébb társadalmi elítélés övezi, mint a valós kontextusban (YAR 2006, 11.). Az ilyen normák megsértésének következményeivel szemben megszilárdulni látszik egyfajta immunitás, amely először az egyén, majd a közösség attitűdjeiben jelenik meg, ami később általánossá válhat.
- *Anonimitás.* A virtuális tér lehetővé tette anonim akciók felszabadítják az egyént belső és külső kontrolljaitól. Míg a valós életben a személyes identitás felvállalása visszatart a szabályszegéstől, és támogatja a konform viselkedést, addig a kibertérben a hagyományos normák különböző szintjei a rugalmas erkölcs (*flexible morality* – MICHELET 2003) szellemében könnyebben átléphetők.
- *Kontrollhiány.* Az online hálózatot ellenőrző intézmények által kevésbé ellenőrzött, privát böngészésre alkalmas *darkweb* működése növeli a kibertérben megvalósuló normasértések látenciáját (YAR 2006, 9.).
- *Az offline normák eróziója.* Az anonimitás által támogatott kettős lét a digitális bennszülöttek szocializációjának része (PRENSKY 2001, 1–6.). Az efféle szocializációs

folyamatban a hagyományos normák nem mindegyike internalizálódik és automatizálódik, ami a valós életviszonyokban az eligazodás és alkalmazkodás nehézségeit okozza és termeli újra.

- *Online-offline normakompatibilitás.* Egyre gyakoribb, hogy az egyén a virtuális szabályokhoz illeszti viselkedésének mércéjét, majd onnét kilépve ugyanezt a mércét a valós térbe is átviszi, és fordítva (Turkle 2000). Amennyiben a két mérce nem kompatibilis, a két színtér egymástól eltérő elvárási repertoárján alapuló normakompatibilitási feszültség keletkezhet, ami deviáns magatartásokhoz vezethet.
- *Destruktív e-trendek terjedése.* A fiatal felhasználók körében a kibertérben megjelenő trendek utánzása – ha hallgatólagosan is, de – részben a kortárs közösség nyomásgyakorlásának eredménye. A követendő trendek fókuszában álló tárgyak vagy cselekvések rövid idő alatt egy egész generáció szimbólumává emelkedhetnek, elérendő célként fogalmazódnak meg a generáció tagjaiban (például a veszélyes offline cselekvések teljesítése, vagyis a bátorságpróba). A világhálón megjelenő információbázisok gyártói és szerkesztői, a kortárscsoportok vélemény- és trendformálói, a tartalomszolgáltatók – ha nem is mindig közvetlen módon, de – cselekvést meghatározó hatalommal rendelkeznek, és képesek hozzájárulni a deviáns magatartásformák megvalósulásához.
- *A nyilvánosság megváltozása.* A nyilvánosság hagyományosan a közügyek intézésének a területe, élesen elhatárolva a magánszférától. Az internet megjelenésének egyik hatása éppen az, hogy a köz- és a magánszféra közötti határok (is) elmosódnak: gyakran magánügyek jelennek meg a nyilvánosságban. Sőt, a tabloidizáció következtében a közszereplők esetében kifejezetten reklámeszköz a magánélet közüggyé tétele. Azonban nemcsak a nyilvánosság előtt élők esetén merül fel a magán- és a nyilvános szféra közötti határ elmosódása. Minden olyan esetben, amikor magánügyek kerülnek nyilvánosságra, felmerül a személyes információkkal való visszaélés lehetősége. Például az egyén önbecsülését sértő, lejárató tartalmak destruktív erővel hatnak az egyén lelki integritására, ami további konfliktusokat generál (Smith–Mackie–Claypool 2016).
- *Digitális kompetencia.* A hagyományos deviáns viselkedések mintázataihoz képest a kibertérben leginkább az jöhet számításba normasértőként, aki alapvető digitális kompetenciával és az internet hálózatához elegendő hozzáféréssel rendelkezik. Ugyanez nem mondható el a kiberdevianciákat elszenvedőkről.
- *Az e-bizalom felértékelődése.* A bizalom az egyéni kötődések alapja és egyben a kereskedelmi tranzakciók (eBay) sikerének záloga (O'Regan 2016). Az ügylet vagy a személyes kapcsolat megbízhatóságáról való tájékozódás az outputperifériákon keresztül sokkal korlátozottabb, ezért a bizalom marad a legfőbb garancia. Az online bizalomra hagyatkozás nemes alapja az együttműködésnek, és bár közvetett módon, de kapcsolódik a devianciákhoz, voltaképpen azok folyamatában egyfajta kockázati tényezőként tartható számon.

Valójában az új társadalmi tényezők cselekvésmódosító hatásai a mai napig arra motiválják a kibertér kutatóit, hogy megalkossák azt a fogalmi keretet, ami felismerési, értelmezési és eligazodási lehetőséget nyújt a hagyományos színtéren, a kibertérben, illetve az ezek kombinációiban megjelenő normasértések között, és ezzel kijelölik a kibertér és a fizikai

színtér határait. Kötetünk következő fejezetében a normasértő magatartások besorolhatósága érdekében a kiberdeviancia fogalmi meghatározására teszünk kísérletet.

2.2. Deviancia a kibertérben

A *deviancia* legelterjedtebb meghatározása szerint egy adott közösségben uralkodó és a közösség többsége által egységesen elfogadott normáktól való eltérést, elhajlást jelent. A deviáns jelző sokféle magatartásformára utal: lehet funkcionális és diszfunkcionális, univerzális értékeket sértő, alkalmi vagy többször megismétlődő, egyéni jellemből kiinduló vagy informális és formális reakciókat kiváltó (ANDORKA et al. 1974; ROSTA 2007). A deviánsnak minősített egyén magatartásának veszélyességi fokát leginkább az fejezi ki, hogy a megsértett szabályokhoz milyen közösségi attitűdök kötődnek, vagyis mennyire fontos és meghatározó értékeken alapulnak. Mivel a deviancia köztudatban elterjedt fogalomköre magában foglal számos *eltérő,* de veszélytelen viselkedésformát vagy jelenséget, ezért célszerű kijelölni azokat a szempontokat, amelyek figyelembevételével kiemelhető és leszűkíthető a legnagyobb kockázatot jelentő deviációk csoportja. A deviánsnak tartott magatartások különböző definíciói között vannak olyan közös vonások, amelyek egységesen utalnak az univerzálisan károsnak ítélt magatartásformákra. Többek között

- a társadalom többsége negatív értékítéletét fejezi ki a deviánsnak minősített magatartásokkal szemben,
- az adott magatartás komplex reakciót vált ki mind a társadalom tagjaiból, mind a kontrollintézmények részéről,
- a deviáns viselkedésforma nem lehet túlsúlyban a konform magatartásformákhoz képest, és
- többnyire veszélyt jelent az egyénre és a közösségre, beleértve a deviáns személyt önmagát is (ön- és közveszélyesség) (GÖNCZÖL–KEREZSI 1993; ROSTA 2007; GIDDENS 2008).

A kriminológia képviselői a deviancia modern megfogalmazásában az ön- és közveszélyességet emelik ki fő szempontként, és a deviánsnak minősítést a kiváltott intézményes reakció meglétéhez kötik (GÖNCZÖL 2016, 115.). A deviáns jelenségek megítélése önmagában sem egyszerű, de az ön- és közveszélyes magatartásokkal szemben kialakuló különféle társadalmi viszonyulás ezt még bonyolultabbá teszi, például azzal, hogy „tűrt, még tolerált és már tiltott" magatartásokként – ha néha hallgatólagosan is, de – egymástól elkülöníti (GÖNCZÖL 2016, 115.). A meghatározást az is befolyásolja, hogy a társadalom mikor, milyen módon és eszközökkel reagál a negatív megnyilvánulásokra. Ennek hátterében markáns szerepet tölt be a már említett társadalmi toleranciaképesség, a tradíciók és a kultúra, valamint az adott társadalom kormányzatának törekvései és a deviancia kezelésére irányított valós erőfeszítései (például hogy milyen mértékű erőforrásokat fordít a társadalmi jelenség kezelésére) (GÖNCZÖL 2016, 116.). A deviancia kezelésében hozott kormányzati döntések jelentősen meghatározzák a devianciák alakulását pozitív és negatív irányban egyaránt. Voltaképpen ez azt jelenti, hogy a kormányzati intézkedések lehetnek a devianciákat mérséklők és a deviancia reprodukcióját vagy devianciaspirált generálók (GÖNCZÖL 2016, 116.). A modern megfogalmazás szerint tehát a deviancia „az átlagostól,

az uralkodó normáktól, az elvárt és még tolerált magatartási formáktól eltérő olyan ön- és/vagy közveszélyes magatartások halmaza, amely a többségi társadalom oly mértékű erkölcsi rosszallását váltja ki, hogy a féken tartásukra – a szaktudományok fejlettségének és az uralkodó felfogásoknak megfelelő – intézményes reakciókat rendszeresít" (Gönczöl 2016, 117.). Egyes jelenségeket a társadalom tagjai akkor is normálistól vagy megszokottól eltérőnek minősíthetnek, amikor egy olyan gyors lefolyású globális vagy társadalmi változás eredményei, amihez az adott közösség nem tud egyszerre alkalmazkodni. Az elmúlt évtizedekben az internet és a számítástechnikai eszközök globális forradalma pont ilyen jelenség volt. A technológia robbanásszerű fejlődése és a hálózatosodás kizökkentette a hagyományos kommunikációs környezetében élő egyént megszokott életmódjából, majd az innovációk társadalmi terjedésének következtében a digitális eszközökhöz való hozzáférés, valamint a digitális kompetenciákban mutatkozó különbségek mélyítették a társadalom egyes csoportjai között fennálló szakadékot. Ennek megfelelően még ma is megfigyelhető, hogy a korábbi predigitális generáció tagjai a technikai alapokra helyezkedő globális hálózatosodást gyakran erőn felülinek ítélik meg. Christopher Freeman a gyors lefolyású technológiai átalakulás társadalmi gazdasági folyamatokra gyakorolt hatását nem a normától való eltérésként, hanem technológiai paradigmaként fogalmazta meg, amelynek legfőbb jellegzetességét a technológia információra irányultságában, az új technológia mindent áthatóságában, a rendszerek és kapcsolatok hálózati logikát követő felépülésében, a rugalmas átalakulásban és a speciális technológiák integrációjában látta (Castells 2005, 117–119.). Freeman okfejtése tisztább képet fest, ugyanis az új környezet kínálta lehetőségeket felismerő és azokhoz alkalmazkodni tudó társadalmakban ma már megkérdőjelezhetetlen, hogy a technikai fejlődés és az internetes hálózatosodás sokkal inkább a gazdasági, társadalmi, politikai fejlődés kulcsa, mintsem egy olyan jelenség, amely a normálistól eltérő. A deviáns viselkedés inkább a kibertérhez kapcsolódó egyéni és közösségi érdekek és értékek szükségszerű következményeként alakult ki és vált megfogalmazhatóvá és súlyozhatóvá. Ez utóbbi a kiberdevianciák területén azt jelenti, hogy vannak olyan normasértő faktorok, amelyekkel szemben inkább a közömbösség erősödik (tűrt és tolerált), emellett léteznek olyanok is, amelyek időben és térben az állandó elítélés tárgyai. A durva, normaszegő magatartásmintákat és az enyhébb megítélésű elhajlásokat ennek okán egy szűkebb és egy tágabb fogalmi keretbe illesztve, a hagyományos deviancia fogalmi elemeinek figyelembevételével vázoltam fel. Eszerint az olyan cselekedet minősül kiberdevianciának,

- amely érinti a kiberteret;
- amely jogi normát sért vagy ön- és közveszélyes a kibertérben;
- amelyhez a társadalom többsége negatívan viszonyul;
- amely kiváltja a társadalmi többség és a kontrollintézmények negatív reakcióját;
- amely kisebbségben van az elfogadott magatartásmintákhoz képest;
- amelynek megvalósítója digitális kompetenciával rendelkezik;
- amelynek hátterében humán tényezők állnak (vagyis emberi célok, szándékok, motivációk, szükségletek).

A kiberdeviancia szűkebb értelemben a kibertérben megvalósított olyan közvetett vagy közvetlen, digitális kompetencián alapuló emberi magatartás, amelyhez az adott társadalom tagjainak többsége negatívan viszonyul, jogi normákat sért, formális reakció kiváltására

alkalmas, gyakoriságát tekintve kisebbségben van az adott társadalom többsége által elfogadott magatartásmintákhoz képest, vagy veszélyt jelent az egyénre és/vagy a közösségre.

A globális hálózat heterogén közösségeiben az értelmezés egy cseppet sem egyszerű. A legtöbb társadalomban a gyermekkorúakról készült pornográf felvételek terjesztése jogsértő, a rágalmazás vagy a becsületsértés azonban eltérő értelmezésű lehet. A fentiekben meghatározott szűkebb fogalom szerint a kibertérben elkövetett szabályszegő magatartás deviánsnak minősítése – bár nagyjából azonos feltételek szerint került megfogalmazásra – függ attól, hogy mely társadalom felhasználóinak körében került nyilvánosságra, és a deviáns magatartásokat megvalósító és elszenvedő mely társadalom tagja. A kiberdeviancia tágabb fogalomköre a szűkebb fogalomkört is magában foglalja, de annál jóval több megnyilvánulásra kiterjed, és nemcsak a súlyosabb normasértésekhez áll közel. Ennek alapján kiberdevianciának az olyan cselekedetet nevezem,

- amely érinti a kiberteret;
- amely valamely normát sért a kibertérben;
- amely kiváltja a társadalom többségének negatív értékítéletét;
- amely legalább a társadalom többségének negatív reakcióját váltja ki;
- amely kisebbségben van a társadalom többsége által elfogadott magatartásmintákhoz képest;
- amelynek megvalósítója digitális kompetenciával rendelkezik;
- amelynek hátterében humán tényezők állnak (vagyis emberi célok, szándékok, motivációk, szükségletek).

A kiberdeviancia tágabb értelemben tehát a kibertérben megvalósított olyan közvetett vagy közvetlen, digitális kompetencián alapuló emberi magatartás, amellyel szemben az adott társadalom tagjainak többsége negatív értékítéletét fejezi ki, legalább informális reakció kiváltására alkalmas, kisebbségben van az adott társadalom többsége által elfogadott magatartásmintákhoz képest, az adott társadalom valamely normáját sérti.

A kiberdeviancia mindkét fogalma két feltételben tér el a hagyományos devianciafogalomtól, mégpedig a kibertérben való megvalósulás szükségességében és a digitális kompetencia meglétében.

2.3. A kiberdeviancia színtérmódozatai

Bármilyen kiberdevianciáról is legyen szó, hátterében emberi motivációk és célok fogalmazódnak meg, végső soron emberi cselekvések eredményei, mint ahogyan azok megítélése és szankcionálása is, ezért az internet hálózatában a számítástechnikai rendszerek és eszközök együttese eszközként és lehetőségként is számításba vehető. Kétségtelen, hogy a legtöbb kutatás a humán meghatározottságokból és a hagyományos környezetből indul ki, vagyis a virtuális teret az alanyokhoz viszonyítva mutatja be, viszont kevésbé fókuszál a környezet katalizáló szerepére. A kibertér normasértő cselekvéseket generáló sajátosságai a belépő felhasználók magatartásváltozásai mentén figyelhetők meg, vagyis azokban az esetekben, amikor az új környezet hatásai révén a felhasználóban gyengülnek azok a visszatartó erők, amelyek a mindennapi feszültségek felszabadításában a hagyományos térben meggátolják (PARTI 2018). Az offline és az online tér közötti devianciaátjárásról szól

az *EU Kids Online* című kutatás is, amelyben Livingstone, Haddon és Görzig kockázatvándorlási hipotézisének *(risk migration hypothesis)* legfőbb mondanivalója, hogy az online kockázatvállalás nagyon szoros kapcsolatban áll a hagyományos környezetben tanúsított viselkedéssel és az életkorral (Barbovschi et al. 2012, hivatkozik rá Parti 2018). Az emberi cselekvések okai és megvalósulási színtereinek különböző kombinációi, röviden színtérmódozatai egyébként a korábban hivatkozott Grabosky diskurzusában használt hasonlat mentén is megragadhatók *(old wine in new bottles).* A térbeli mozgás (mobilizálódás) modellezése tehát időszerű és indokolt, ebben a normasértéseket logikus más-más színtéren zajló mozzanatokként és összefüggéseikben is vizsgálni. Az előbbi esetében a terekben külön-külön megvalósuló cselekvések eltérő súlya, különböző jogi és társadalmi megítélése, az utóbbi esetben a normasértő magatartás teljes hatása mérhető. A színterek között mobilizálódó deviancia akkor nevezhető kiberdevianciának, ha a normasértés folyamata valamilyen módon érinti a virtuális teret. A folyamatban a deviancia logikailag négy különböző módon jelenhet meg:

1. *Eredmény- és színtérmódozat.* Ebben a típusban a normasértés a kibertérben kezdődik, ott zajlik, és ott is végződik, vagyis tisztán a kibertérben. Ebben a módozatban felerősödik az anonimitás, a titkos információáramlás, a kevésbé szabályozott szürke foltok működése és a digitális identitás szerepe, ugyanakkor a normasértők köre leszűkül azokra, akik digitális kompetenciával rendelkeznek. Mivel az eredmény- és színtérmódozat minden elemében érinti a kiberteret – sőt, csak és kizárólag azt érinti –, ezért ebben a modellben helyezhetők el a kiberdeviancia új formái.
2. *Eredménymódozat.* A folyamat kiindulópontja a hagyományos tér, azonban a deviáns magatartások a virtuális „infrastruktúrákban" végződnek. Azaz olyan magatartásokról van szó, amelyek mind a rendszerintegritás elleni (például hagyományos színtéren való megtévesztéssel megszerzett adatokat követő rendszerfeltörés), mind a tartalommal vagy médiummal összefüggő deviáns magatartásformákat (például a párkapcsolati erőszak verbális, zaklató jellegű formája) magukban foglalják.
3. *Színtérmódozat.* A színtérmódozat az eredménymódozat fordítottjaként működik. Ebben az esetben is mind a valós, mind a virtuális teret érinti a normasértés, ezúttal viszont a kibertérben kezdődik a folyamat, ott is zajlik, de a valós térben fejeződik be. Ma már az sem újdonság, ha egy virtuális térben eszkalálódó konfliktus testi sértéssé fajul, vagy az internetes kábítószer-kereskedés megrendelője szemtől szemben veszi át a tiltott szereket. Ide köthető a prostitúciós szolgáltatások internetes reklámozása és még sok más folyamat, amely az offline térben zárul.
4. *Katalizáló módozat.* A hagyományos és a kibertér szoros kapcsolatát azok a normasértő magatartások fejezik ki igazán, amelyek történésük folyamatában átfogják a hagyományos és a virtuális teret. Ebben az esetben arról van szó, hogy a cselekvés egy szakasza kerül kapcsolatba az adott térrel – miközben nem ott kezdődik, és nem ott végződik. Ebből a szempontból mind az offline, mind az online térnek lehet katalizáló funkciója a normaszegő magatartás folyamatában. Azaz a katalizáló módozat két alcsoportra osztható a kibertér és az offline tér katalizáló funkciója szerint:
   – Az első esetben a kibertér gyakorol valamilyen hatást az eredményre, például amikor a hagyományos környezetben kialakuló féltékenység internetes konfliktussá formálódik, majd fizikai erőszakká fajul.

– A második esetben a hagyományos színtér katalizáló funkciója érvényesül. Ennek modellezésére a napjainkban ciklikusan változó irányú *cyberbullying* szolgál példaként, ahol az online lejáratást offline kiközösítés követ, majd ennek folytatásaként újabb internetes nyomásgyakorlás következik egy folyamatban (valójában a *cyberbullying* mindkét módozatra igaz lehet).

A négy módozat a kibertér átjárhatóságának olyan értelmezési struktúráját adja, amivel az egyes cselekvések mögött rejlő érzelmi és morális diszpozíció is felfedhető, mindazonáltal kiküszöbölhető a színtereket átfogó cselekvések leegyszerűsített megítélése.

2. táblázat

Az egyes magatartásformák színtérmódozatai

Magatartásmintázat	Eredmény- és színtér-módozat	Eredmény-módozat	Színtér-módozat	Katalizáló módozat	
				online	offline
Szexuális tartalmak szerepeltetése *(sexting)*	+	–	–	–	–
Heves párbeszéd *(flaming)*	+	–	–	–	–
Információs rendszerek megsértése	+	–	–	–	–
Behálózás *(grooming)*	+	–	+	+	–
Zaklatás	+	+	+	+	+
Zsarolás	+	+	+	+	+
Csalás	+	+	+	+	+
Kényszerítés	+	+	+	+	+
Extrémizmus, terrorizmus	+	+	+	+	+

Forrás: KISS 2018

2.4. A kiberdevianciák motivációi

A hagyományos, társadalmi együttélésre veszélyes devianciák szűk fogalomkörébe olyan stabil magatartásminták tartoznak, mint az alkoholizmus, a kábítószer-fogyasztás, az öngyilkosság, az antiszociális viselkedést megalapozó mentális betegségek és a bűnözés (ROSTA 2007). Fizikai megjelenésüktől eltekintve igen gyorsan integrálódtak a kiberkörnyezetbe (például a kábítószer-kereskedelemben való részvétel). Az interneten és az ahhoz kapcsolódó információs rendszerekben megvalósuló devianciák egyfelől az offline térből történő *egyszerű migrációval* kerülnek az online világba, és gyakran arra is korlátozódnak. Ezek többnyire a *szexuális* ösztönkésztetésekből, az *agresszív* érzelmekből és a *haszonszerzési* szükségletekből eredeztethetők, miközben a társadalom és kontrollintézményei jelentik megítélésük alapját.

2.4.1. Szexuális motiváció

A kibertérben a normasértő szexuális viselkedések valamennyi, az adott helyzetben részt vevő személy egységes akaratának hiányában, fizikai kapcsolat nélkülözésével vagy a fizikai érintkezés előkészítéseként, előzményeként zajlanak. A szexuális viselkedés hagyományos és virtuális alakzataiban meghatározó szerepe van a kommunikációnak, pontosabban a partner szexuális vágyát közvetíteni képes hanghatásoknak és a másodlagos nemi jegyek, erogén zónák látványát nyújtó vizuális ingereknek, illetve az agresszív feszültségeknek (Buda 2002, 56.). A kommunikáción alapuló, normasértő szexuális interakciók elsősorban a gyermek- és fiatalkorú felhasználókra, de az anonimitás miatt másokra nézve is különösen kockázatosak. Olyan fizikai védelmi bástyákat iktatnak ki, mint az elsődleges és a másodlagos szocializációs színtér, kortárs csoportokból álló baráti közösségek, a szemtől szemben történő észlelés és a személyi azonosítás lehetősége. Az anonimitás emellett a gátlások nélküli fantáziálásoknak és a parafíliák (például a pedofília) megjelenésének is melegágya lehet. A kibertérben megvalósuló szexuális motivációk által ösztönzött normasértő magatartások veszélyességük szerint három csoportba sorolhatók:

- a szexuális tartalmak a szexuális feszültség normasértő eredménnyel járó levezetését szolgálják (például a szexuális tartalmak küldése, fogadása, közzététele);
- a kibertérben zajló cselekvés bármely színtéren megvalósuló szexuális normasértés előzménye vagy előkészítő stádiuma (például a behálózás);
- a szexuális erőszak lenyomata vagy annak következményei a virtuális környezetben észlelhetők (például a zaklató jellegű magatartás vagy zsarolás).

A három viselkedésforma mindegyike valamilyen normasértést keletkeztet, és céljuk *a szexuális szükségletkielégítés vagy szexuális feszültséglevezetés.* Eltérés abban van, hogy más-más súlyú deviáns magatartásformák a részei a szexuális tartalmak küldésétől a behálózáson át az erőszak alkalmazásáig.

3. táblázat

A szexuális motivációkra épülő normasértések a kibertérben

Szexuális motivációk	• szexuális tartalmak szerepeltetésével való visszaélés (például *sexting,* szexuális témájú kommunikáció) • behálózás *(grooming)*
Szexuális motivációk agresszióval vagy erőszakkal összefonódva	• szexuális tartalmak szerepeltetésével történő visszaélés (például *sexting,* azaz a szexuális témájú kommunikáció bosszúból) • kibertérben történő szexuális zsarolás • kibertérben történő szexuális zaklatás

Forrás: Kiss–Parti–Prazsák 2019

2.4.2. Haszonszerzési motiváció

A haszonszerzési szükségletek – ahogy a hagyományos térben is – markáns motivációként szerepelnek a kiberdeviancák hátterében. Nagyon gyakran kapcsolódnak az agresszív vagy erőszakos motivációkhoz, és kimondottan anyagi vagy más haszon elérésére irányulnak. A magatartást megelőzheti a behálózás szakasza, és eszköze lehet a szexuális tartalmak szerepeltetése (például a szexuális tartalmak szerepeltetése az interneten), főként zsarolás esetében. A haszonszerzés szükséglete körül felépített műveletekre különösképp jellemző a terek közötti mozgás, pontosabban amikor az elkövetés a kibertérben, az anyagi kár a hagyományos színtéren történik, és fordítva. A kibertérben a haszonszerző normasértések három csoportja különíthető el megvalósításuk módja és terepe szerint:

- haszonszerzés információs rendszerek elleni támadásokkal, technikai módszerek segítségével (például a szolgáltatás megtagadásával járó kibertámadások);
- az illegális kereskedelmi tevékenységek útján történő jogtalan haszonszerzés (például a kábítószerekkel vagy fegyverekkel való kereskedelmi tevékenység);
- az információs csatornákon át történő információközléssel vagy kommunikációval megvalósított haszonszerzési folyamat (például egy megtévesztő tartalom elküldése a levelezőrendszerben).

4. táblázat

Haszonszerzési motivációkra épülő normasértések a kibertérben

Haszonszerzési motivációk	• engedély nélküli tevékenységgel illegális áruk és szolgáltatások kereskedelme (például kábítószer, fegyver, pornográf tartalmak kereskedelme) • engedély nélküli kereskedelmi tevékenység (például nem bejelentett, hatóságok által nem nyilvántartott vagy nem engedélyezett) • behálózás *(grooming)* • kibertérben megvalósuló csalás
Haszonszerzési motivációk agresszióval vagy erőszakkal összefonódva	• kibertérben történő zsarolás • kibertérben történő zaklatás

Forrás: KISS–PARTI–PRAZSÁK 2019

2.4.3. Agresszióra épülő motivációk

Az agresszió belső lelki tartományban rejtőző késztetésekhez, külső környezeti tényezők által alakított lelkiállapotokhoz köthető, támadó jellegű magatartás. Ellenséges belső rezdületek, élmények hatására keletkezik, és igen gyakran belső feszültséggel jár (HÁRDI 2010, 29.). Megjelenése szerint lehet *belső,* az egyén lelkivilágában, érzelmekben, lelki feszültségben, indulatok formájában, illetve *külső,* vagyis egyének és közösségek interakcióiban manifesztálódó jelenség. Irányulhat az egyéntől *önmaga felé* vagy *a külső környezet irányába,* előbukkanhat tudatos vagy tudattalan formában, közvetlenül vagy közvetve, de átalakult alakzatban is (agresszió szublimálása) (HÁRDI 2010, 30.). A kibertérben az agresszív megnyilvánulások széles palettájával találkozhatunk, ezek kifejeződhetnek

kép-, hang-, szöveg-, gif-, internetes mémes tartalmakban, kommunikációban zajló, heves párbeszédben. Az agresszív érzelmek – hasonlóan a hagyományos térhez – a kibertérben is a legsúlyosabb erőszakos normasértésekhez vezethetnek, azzal a különbséggel, hogy a hagyományos térhez képest az erőszak nem fizikai vetületeivel számolhatunk (például pszichikai erőszak). Az agresszió reaktív és instrumentális típusa – a legenyhébb sértegetésektől a rendszerintegritást sértő magatartásokon át – a kényszerítésig tartó magatartások ösztönzője, amiről az agresszióelméletek széles irodalma ad különböző magyarázatokat. A virtuális környezetben megjelenő agresszív megnyilvánulások nem mindegyike eredményez jogi normát sértő cselekvéseket és pszichés erőszakot sem, ugyanakkor a legenyhébb formája is negatív hatással van a résztvevőkre. A kibertérben megnyilvánuló agresszió társadalomra való veszélyességének mértéke szerint szükséges az *erőszak* és az *agresszió* megkülönböztetése. Ennek alapján *az agresszív cselekvésnek a virtuális térben* – hasonlóan a hagyományos környezethez – több jellemzője van:

- az egyén negatív érzelmeiből fakad;
- a kibertérben valamely normát sért, de minimálisan magára az agresszorra vagy más felhasználó(k)ra van negatív hatással (de nem minden esetben váltja ki a társadalom többségének rosszallását és a kontrollintézmények reakcióját);
- jellemzője a terek közti mobilizálódás.

Az agresszióból fakadó magatartás úgy értelmezhető, mint minden olyan, az egyén negatív érzelmeiből fakadó, kibertérben megnyilvánuló manifesztáció, amely magára az egyénre vagy másra negatív hatással van, vagy valamely normát sért, de még nem tartalmazza a fenyegetést, a kényszerítést és a megfélemlítést.

Az agresszió meghatározásához képest az erőszak szűkebb fogalom, a kriminológiai erőszakfogalom szerint „embertől eredő, másik személyre közvetlenül irányuló, a cél elérésére alkalmas fizikai vagy pszichikai erőt jelent" (Vigh et al. 1973, 42.). A WHO megfogalmazása szerint „az erőszak fizikai erő vagy hatalom szándékos alkalmazása – az ezzel való fenyegetés vagy tényleges alkalmazás –, amely önmaga, más személy, egy csoport vagy egy közösség ellen irányul, és amely fizikai sérülést, halált, pszichés ártalmat, fejlődési elakadást vagy deprivációt eredményez, vagy nagy a valószínűsége, hogy ilyen eredményre vezet" (Krug et al. 2002, 5., hivatkozik rá: Virág–Kulcsár–Rosta 2016, 554.). A kibertérben az erőszak nem fizikai formái illeszthetők, meghatározásához a fenti erőszakfogalmakban és az erőszakos bűncselekmények büntetőjogi tényállásaiban is megtalálható elemeket, *a kényszerítést és a fenyegetést* vesszük alapul, amelyek a virtuális környezetben is irányulhatnak személy ellen, manifesztálódhatnak szexuális magatartásokban és vagyon elleni normasértésekben. A kibererőszakra is érvényes az a megállapítás, hogy minden esetben agresszióból keletkezik, de az agresszió nem minden esetben válik erőszakos magatartássá (Virág–Kulcsár–Rosta 2016, 555.). Ha ebből indulunk ki, akkor a kibertérben megnyilvánuló erőszak az egyén vagy közösség irányába ható agressziónak a virtuális tér „infrastruktúrái" mentén megnyilvánuló tudatos, szándékos, károkozásra képes formája.

A kiberkörnyezetben az erőszakos magatartásmintázatok megvalósításuk szerint két csoportra oszthatók: amikor a *kényszerítés,* a *fenyegetés* alkalmazását követően a normasértés a *hagyományos térben végződik* (közvetett), és amikor a *kibertérben fejeződik be* (közvetlen). Az előbbire példaként a szexuális kényszerítés hozható fel, ahol maga a kényszerre irányuló cselekvés az internetes csatornákon történik, viszont az eredmény (szexuális aktus)

már fizikai kontaktussal végződhet. A másodikra a zsarolás bűncselekményét említjük példaként, ahol a fenyegetéssel, kényszerítéssel a cselekmény befejezése is a virtuális térben marad (Skype-os zsarolás, majd ennek következményeképpen az összeg banki átutalása). A kibererőszak fogalmába tartozhat a zsarolószoftver *(ransomware).* A szoftvert az elkövető eljuttatja a kiszemelt felhasználó rendszerébe, ahol rendszerbénulást okoz. Amíg a felhasználó nem fizet „váltságdíjat", a rendszere blokkolva marad (SYMANTEC 2015).

A kibererőszak két alapvető eleme valamelyik vagy mindegyik meglétéhez kötött, súlyosabb kiberdeviancákat eredményez, valamely normát sért, és a társadalom széles köre által elítélt. Az erőszak kiberkörnyezetben zajló mechanizmusa – hasonlóan az agresszióhoz – több jellemzővel bír:

- szándékos károkozásra vagy szükségletkielégítésre irányul, és agresszióból fakad (kényszerítéssel, fenyegetéssel megnyilvánuló agresszió);
- a kibertérben jogi normát sértő magatartás (legalább erkölcsi vagy szokásjogi normát sért);
- alapvető eleme a kényszerítés, a fenyegetés vagy a megfélemlítés;
- az egyénre vagy a közösségre káros hatással van;
- jellemzője a terek közötti mobilizálódás.

A kibertérben megnyilvánuló erőszak a fenti jellemzők szerint *minden olyan – nem fizikai formában megjelenő – kényszerítéssel, fenyegetéssel megvalósított agresszív cselekvés, ami pszichikai erőszak előidézésére alkalmas, másra mindenképp káros hatással van, társadalmi elítélés övezi, minden esetben normasértő, továbbá jogi normasértést idéz elő.*

Abban az esetben, ha az erőszakos magatartás hagyományos színtéren fejeződik be, csak akkor sorolható a kibererőszak fogalmi körébe, ha a kényszerítés, a fenyegetés valamelyike vagy mindegyike a kibertérben is megtörténik. A hagyományos térben erőszakos bűncselekményeknek minősített és a kibertérben megnyilvánuló erőszakos magatartások közt lehet különbség, ugyanis az offline térben a fenyegetés büntetőjogi értelmezés szerint nem feltétlenül tartozik az erőszakosnak tartott magatartások közé, attól függetlenül, hogy a kriminológiai értelmezés szerint pszichés nyomás előidézésére alkalmas. A kibererőszak megfogalmazását viszont a pszichés erőszak feltételei – vagyis a kriminológiai fogalom – mentén határoztuk meg. Míg tehát a kibertérben megjelenő zaklatás a büntetőjog értelmezése szerint nem tartozik az erőszakos bűncselekmények körébe, addig kriminológiai értelemben annak minősíthető.[1]

A virtuális térben az agresszió által motivált cselekvések oksági folyamatát és társadalomra való veszélyességét akkor lehet optimálisan feltérképezni, ha a magatartást több irányból vizsgáljuk, vagyis az *agresszort,* az agresszív magatartás *elszenvedőjét,* a magatartás *környezetét, időbeliségét* és más motivációkkal való összefüggéseit is górcső alá vesszük. Az agresszió és az erőszak különböző megközelítése tisztán rámutat a cselekvések veszélyességére, és lehetőséget biztosít a normasértések e szerinti besorolására. A kényszerítés és fenyegetés által előidézett és a kibertérben manifesztálódó magatartások körét a 7. fejezetben részletesen tárgyaljuk.

[1] Btk. 222. §.

5. táblázat

Agresszióra és erőszakra épülő normasértések a kibertérben

Agresszióra épülő	• negatív érzelmeken alapuló párbeszéd *(flaming)* vagy negatív érzelmek által motivált tartalommegjelenítés • negatív érzelmek által motivált, önbecsülést sértő vagy becsületcsorbító kifejezés, tényközlés kommunikációban vagy tartalommegjelenítéssel (például a becsületsértés, rágalmazás) • egyén vagy közösség elleni, szándékos károkozó magatartás a rendszerintegritás megsértésével (például információs rendszer befolyásolása bosszúból) • egyén és közösség elleni károkozó magatartás kommunikációs csatornákon vagy tartalommegjelenítéssel (például karaktergyilkosság, kollektív normasértés internetes mémek segítségével)
Erőszakra épülő (kényszerítés, fenyegetés, megfélemlítés vagy félelemkeltés alapvető eleme)	• kibertérben történő zsarolás • kibertérben történő zaklatás • extrém csoportok kibertérben történő erőszakos működése • terrorszervezetek kibertérben történő erőszakos működése

Forrás: Kiss–Parti–Prazsák 2019

2.5. A kiberbűnözés mint esszenciális kiberdeviancia

A kiberbűnözés létezése több mint húsz éve evidens jelenség, de a fogalmi meghatározására tett próbálkozások mégis csak az elmúlt tizenöt évben élénkültek fel, miután a web 2.0 által a normasértő magatartásmintázatok egyre szélesebb felhasználói réteget értek el, és egyre láthatóbbá váltak a globális hálózatokban. Ezt követően született meg néhány bűnözésfogalmat felvonultató tanulmány, amelyek közül az egyik a már korábban említett Peter N. Grabosky nevéhez fűződő *old wine in new bottles.* Grabosky fogalommeghatározását követte Rutger Leukfeldt kiberbűnözésről szóló tanulmánya. Ebben arról írt, hogy a kibertérben megvalósuló bűncselekmények azok a cselekvésformák, amelyek az információs térrel, információs technológiával jelentős kapcsolatban állnak, illetve azok, amelyek nem kifejezetten az információs technológiát célozzák, de kötődnek ahhoz. Eszerint a *cybercrime* átfogó kifejezése azokra a magatartásmintázatokra vonatkozik, amelyeknek feltétele az információs technológia igénybevétele. Leukfeldt ezen belül megkülönböztetett olyan devianciákat, amelyekben az információtechnológia egyben cél és eszköz, valamint olyanokat, amelyek megvalósításához az információtechnológia elengedhetetlen, de nem célpont (Leukfeldt 2016, 214–215.; Parti 2018). David S. Wall a kiberbűnözés kialakulásának folyamatát a számítógépes bűnözés evolúciójának nevezte, és olyan generációs korszakokra tagolta, amelyekben a globális internet generációról generációra egyre fontosabb szerepet töltött be (Wall 2008). A Wall által felvázolt modernkori harmadik generációs bűnözés olyan, a hálózat biztonsága elleni és a hálózatot mint médiumot az elkövetéshez felhasználó bűncselekmények összessége, amelyeknek elsődleges jellemzője az előre kifejlesztett számítástechnikai eszközök szervezett és elosztott formában, meghatározott munkavégzési rendben, automatizált módon való felhasználása valamely bűnözői csoportokkal vagy

bűnszervezetek hozzáadott tevékenysége nyomán, meghatározott cél elérésére (WALL 2008, 55–56.). Wall szerint a harmadik generációs bűnözés jellemzője a nemzetköziség, a gyorsaság, a magas látencia, valamint az intellektuális jelleg (PARTI–KISS 2016, 463–495.).

6. táblázat

A számítógépes bűnözés evolúciója

Első generációs bűnözés	A bűncselekményekhez a számítógépeket használták eszközként, az internetről csak információkat gyűjtöttek a bűncselekmények elkövetéséhez.
Második generációs bűnözés (hibridek korszaka)	Amikor az internetet már felhasználták egyes rendszerekbe való jogellenes bejutáshoz, de ennek nagyságrendje minimális volt.
Harmadik generációs bűnözés	A bűncselekmények elkövetésének folyamatában az internet globális hálózata nélkülözhetetlen (például automatizált eszközökkel történő bűnelkövetés).

Forrás: WALL 2008

Parti Katalin definíciója még ennél is logikusabb. Szerinte az informatikai bűnözés (kiberbűnözés) a számítástechnikai bűnözés *(computer crime)* és az internetes bűnözés *(internet crime, cyberspace crime)* kategóriájába tartozó magatartásokat kizárólagos módon magában foglaló kategória, amely egyben a kétfajta bűncselekmény közös halmazát is tartalmazza (PARTI–KISS 2016, 491.). Parti fogalomhasználatában a számítástechnikai bűnözés a számítástechnikai rendszerek és hálózat integritását sérti (például a rendszerekbe való illetéktelen behatolás), az internetes bűnözésnél az internet az elkövetés terepeként szolgál (például hamis weboldalak segítségével banki adatok kicsalása). Az informatikai bűnözés körébe tartozó magatartások kizárólagosan a számítástechnikai és/vagy az internetes bűnözés körébe tartoznak. Az e két kategórián kívül eső cselekmények, annak ellenére, hogy az elkövetéshez informatikai eszközöket is felhasználhatnak (például a számítógéppel vagy számítógépes hálózatban folytatott kettős könyvelés), nem tartoznak a modern informatikai bűncselekmények kategóriájába (PARTI–KISS 2016, 492.).

3. A kiberbűncselekmények fogalma és csoportosítása

Nagy Zoltán

Az információs rendszerek működésének alapvető követelményeit (például az elérhetőség, a zavarmentes funkcionalitás, az informatikai rendszer és a felhasználó relatív biztonsága) sokféle veszély fenyegeti. Eszerint lehetnek *vis major esetek* (például üzemszünetek, áramszünetek, természeti katasztrófák, háború), *vétlen emberi cselekvések,* valamint *szándékos és gondatlan emberi magatartások* összessége (az előbbi a civiljogban, az utóbbi a büntetőjogban szankcionálandó). A következő fejezetben főként azokra az emberi cselekvésformákra térünk ki, amelyek a szándékos károkozásra irányulnak, vagy gondatlanságból valósulnak meg a kibertérben, és bűncselekményként szankcionáltak.

3.1. A kiberbűncselekmények fogalma

A számítógépes bűncselekmények jogi környezetben való megjelenése az 1981. évhez köthető, amikor az Európa Tanács Miniszterek Bizottsága kiadta a 12. számú ajánlását a gazdasági bűncselekményekről.[1] Az ajánlás 4. pontjaként szerepelt a *számítógépes bűncselekmény (computer crime)* elnevezés. Az új cím alatt az ajánlás készítői példálózva említettek három bűncselekményt (például az adatlopást, a titoksértést és az adatmanipulációt). Az Európa Tanács Miniszterek Bizottsága később (1989-ben) bocsátott ki egy újabb ajánlást, amelyben már *számítógéppel összefüggő bűncselekmények (computer-related crime)* néven foglalta össze az új típusú jogsértéseket.[2] Ezt követte a mai napig meghatározó 2011-es budapesti egyezmény,[3] amelyben a jogalkotó szintén a *számítógépes bűncselekmény* elnevezést emelte ki. A 2000-es évektől az *informatikai* előtag használatával osztályozták az *informatikai bűnözést (IT crime, information technology crime),* ami a fogalomalkotók szerint magában foglalja a számítástechnikai bűnözést *(computer crime)* és a számítógépes hálózatokon megjelenő bűnözést *(internet crime, cyberspace crime)* egyaránt (Parti–Kiss 2016). Tankönyvünkben ezzel szemben a *kiber* előtagot használjuk az ebbe a körbe sorolható bűncselekmények megnevezésére és csoportosítására.

---

1 Council Of Europe Committee Of Ministers Recommendation No. R (81) 12 Of The Committee of Ministers to Member States On Economic Crime.

2 Council Of Europe Committee Of Ministers Recommendation No. R (89) 9. of The Committee of Ministers to Member States. On Computer-Related Crime.

3 The Council of Europe Convention on Cybercrime ETS No. 185.

3.2. A kiberbűncselekmények csoportosítása

3.2.1. Tradicionális visszaélések, bűncselekmények az új színtéren

Ebbe a kategóriába sorolhatók azok a jogellenes magatartások, amelyek voltaképpen különböző tartalmak küldésével, fogadásával, közzétételével és a kommunikáció különféle formájával megvalósított hagyományos cselekvések. A kibertér ebben pusztán egy új színtérként szerepel. Ebben a folyamatban a szöveg, kép, valamint a weboldalhoz csatolt audió- vagy videótartalmak az internet hálózatán jelennek meg, beleértve a *surface webet,* az elektronikus hirdetőtáblákat (például a *bulletin boards*), a hírcsoportokat (például a *news-group*), a különböző közösségi oldalakat (például a Facebook, LinkdIn, Badoo stb.), a chatszobákat, a felhasználó saját weboldalát, más weboldalak fórumrovatait, az FTP-, a Goopher, a Telnet hálózatokat, az intra- és az extranet hálózatokat. Emellett küldhetők efféle tartalmak célzott felhasználóknak és a nyilvánosságnak (e-mailben, MMS-ben vagy VoIP-alkalmazás bármelyikével). Jellemzően a *surface weben* különféle közlések között fellelhetők szélsőséges (tév-) eszmék, gyűlöletet szító, durva bejegyzések, gyermekről készült pornográf képek és videók, megtévesztő hirdetések, drog és doppingszer fogyasztását népszerűsítő, másokat zaklató, személyiségi jogokat sértő tartalmak, csalásra, piramisjátékban való részvételre, szerzői jogsértésre felhívó oldalak. Az internet egyes webhelyein betekintést nyerhetünk a fegyverek, robbanóanyagok elkészítésének titkaiba is. A *dark weben* rendelhetők fegyverek, kábítószerek, hamis útlevelek, más okmányok, bérgyilkosok és botnetek bérelhetők – mindez virtuális valutáért. E tartalomközlések és a kommunikáció egy része a hagyományos bűncselekmények virtuális megjelenését alapozza meg. Az informatikai hálózatokra való feltöltéssel a tartalmak elvileg megszámlálhatatlan felhasználóhoz juthatnak el, sok esetben még a tartalom nyelve sem akadály, valamint e tartalmak hosszabb ideig olvashatók, kommentelhetők, megoszthatók (posztolhatók). A kibertér eszerint az alábbi tradicionális és a hagyományos térben szabályozott bűncselekményeknek nyújt lehetőséget:

- rágalmazás, becsületsértés, kegyeletsértés,
- zaklatás (az informatikai rendszer közvetítésével *cyberbullying, cybermobbing*),
- háborús uszítás,
- nemzetiszocialista vagy kommunista rendszerek bűneinek nyilvános tagadása, nemzeti jelképek megsértése, önkényuralmi jelkép használata,
- gyermekpornográf felvétellel visszaélés,
- csalásra felhívás, valamint e körben is nagyszámmal az aukciós csalás elkövetése,
- piramisjátékra felhívás,
- kábítószer-kereskedelem, kábítószer készítésének elősegítése, kábítószer-prekurzorral visszaélés, új pszichoaktív anyaggal visszaélés,
- szerzői alkotások tiltott többszörözése, terjesztése,
- közveszéllyel fenyegetés,
- közérdekű üzem működésének megzavarása,
- tiltott szerencsejáték szervezése,
- pénzmosás,
- üzleti és más titoksértések,
- fogyasztók megtévesztése,

- rossz minőségű termék forgalomba hozatala,
- zsarolás,
- készpénz-helyettesítő fizetési eszközzel visszaélés stb.

3.2.2. Az informatikai rendszerhez és térhez kötött visszaélések, bűncselekmények

Az informatikai rendszereket több biztonságtechnikai megoldás védelmezi. A számítógépek fizikai védelmétől a beléptető rendszereken át a bonyolult és gyakran változtatott jelszavakig. A munkavállaló szakértelme, lojalitása is fontos biztonsági elem. Az informatikai rendszer védelmét a benne kezelt adatok minősége és értéke határozza meg. A költség-haszon elve itt is érvényesül, olyan szintű védelemre van szükség, hogy ne érje meg a rendszer elleni bűncselekmény mint „befektetés".

Hacking, social engineering, phishing. A hacker olyan mesterember, aki faipari munkát végez, fát farag stb. Az 1950-es évek végén az MIT-nagygépek programozói nevezték magukat így. Az akkori nagygépek szűk memóriakapacitásával küszködtek. A programokból törekedtek „kifaragni", hogy minél több hely maradjon a feldolgozni kívánt adatok számára. Az év, hónap, nap leírása mindössze 3×2 karakterre apadt. Ebben gyökerezett a 2000. év számítástechnikai problémája, az úgynevezett Y2K-probléma (a „millenniumi bomba"), tudniillik 2000-ben ez az évszám a számítógép számára értelmezhetetlen volt. A probléma megoldására nagyarányú hardver- és szoftvercserét kellett végrehajtani a világban, hiszen előre nem prognosztizálható veszélyt rejt egy-egy informatikai rendszer (például energia-, pénzügyi, igazgatási, honvédelmi) leállása. Az elektronikus adatfeldolgozó és -átviteli rendszerekbe történő jogtalan behatolást nevezzük angol szóval *hackingnek.* Magunk inkább az *elektronikus betörő* elnevezést használnánk.

A social engineering. Míg a hacking jellemzően a technikai eszközök elleni támadás, addig a social engineering teljes mértékben a humán erőforrás elleni támadás. E támadás célja – hasonlóan a hackinghez – az informatikai rendszerhez való hozzáférés. Ezt a támadást is általában alapos előkészület előzi meg. Az elkövető a nyílt forrású információszerzés módszerét alkalmazva igyekszik minél többet megtudni a célzott szervezetről, a felhasználóról. Az adatgyűjtés a helyszínen folytatódhat, ahol a technikai és az emberi feltételeket veheti szemügyre. A social engineering alapja az, hogy a biztonság leggyengébb láncszeme általában az ember, aki megtéveszthető, megvesztegethető, kényszeríthető, megfenyegethető, megzsarolható információk (személyes adatai, belépési azonosítók, jelszó) átadásáért. Az elkövető jellemzően kedves, behízelgő modorú, bizalmat ébresztő, gyors kapcsolatépítésre képes, külső megjelenésében a helyhez és alkalomhoz illően elegáns vagy sportos, sőt akár a munkavégzésre, karbantartásra szerződött cég munkatársainak munkaruhájához a megtévesztésig azonos öltözéket visel. Rendkívül sok és kifinomult módszere létezik ennek a támadásformának.

Az egyik példa lehet az, amikor az elkövető nyílt forrásból ismert telefonszámon bennfentes személyként vagy külsős – például IT-szakemberként – mutatkozik be, és célja a segítségnyújtás vagy annak felajánlása okán az informatikai rendszer hozzáféréséhez szükséges adatok megismerése *(Quid Pro Quo attack).* A telefonhívás vagy e-mailben

történő megkeresés után következhet a személyes találkozás kicsikarása, amely során az elkövető igyekszik személyes varázsát felhasználva a célszemély bizalmába férkőzni, lehetőség esetén a célszemélyt, érdeklődését, szokásait kiismerni, netán az asztalon, a naptáron, a monitoron hagyott jelszavát megismerni.

Az elkövető a helyszínen végezhet úgynevezett fordított social engineeringet, amikor például egy óvatlan pillanatban az ismerkedéskor beleavatkozik a célszemély számítógépének működésébe, ami után a célszemély kérhet majd segítséget az elkövetőtől, aki a segítségadás indokaként kéri a célszemély jelszavát vagy más azonosítót.

Vagy ilyen az, ha az elkövető ügynökként, más cég munkatársaként kiadva magát ajándékot visz a célszemélynek, amely ajándék része egy olyan pendrive, amelyen egy kém- vagy más program van telepítve. További példa: az elkövető kisebb szervezetek, magánfelhasználók számára programfrissítéseket, új programokat ajánl a felhasználó személyes adataiért cserébe. Vagy akár az elkövető munkahelyen kívüli kapcsolatot is kezdeményezhet a célszeméllyel.

A social engineering támadás sértettje bármely felhasználó lehet. Szervezetek, intézmények esetében ezek jellemzően az alacsonyabb beosztásban dolgozók, az ügyfélszolgálatnál dolgozók, a titkárnők.

A phishing. A social engineering egyik módszere a phishing (adathalászat). Az adathalászat célja szintén a felhasználók adatinak megismerése. Többféle módszer látott már napvilágot. Például olyan e-mail, sms, közösségi oldalon feltűnő hirdetés, banner csábítja a felhasználót, amely figyelmének felkeltésére szolgál, valamilyen vonzó, érdekes információval, hírrel kecsegtet. Üzeneteikben általában a legális webhelyen használt szövegek, logók, képek és stílusok másolatát használják fel leveleikben, hogy ezzel is valódinak tűnjön a felhasználók előtt. Ez a csalárd hirdetés azt sugallja, hogy az áldozatok, ha meglátogatják az adott weboldalt, akkor további információkat olvashatnak, szerezhetnek be. A támadók üzeneteikben egy URL-t vagy beágyazott hivatkozásokat mellékelnek, amelyek egy rosszindulatú weboldalra (amely lehet a törvényes weboldalnak a klónja is) irányítják a gyanútlan felhasználót. Ezeken az oldalakon a felhasználók további elérhetőségeit (címek, telefonszámok, bankszámlaadatok, személyazonosításra alkalmas okmányainak száma stb.) kérik kapcsolatfelvétel hamis céljával. De olyan is van, hogy az alacsonyabb beosztású dolgozók csalárd e-maileket kaphatnak saját általuk nem ismert magas beosztású vezetőjétől vagy szintén ismeretlen más szervezet, hivatal dolgozójától.

Az adathalász kísérletek szólhatnak magánfelhasználóknak és munkavállalóknak hamis információkról, hírekről *(pretexting),* például segítségkérés csalárd adománygyűjtéshez hamis indokkal, ígéretekkel, mondjuk hogy egy nem létező nyereményjátékban nyertes. Kérhetik a felhasználótól valamilyen politikai, közösségi kampányhoz való csatlakozását vagy annak támogatását. Kínálhatnak ingyenes zenét vagy filmletöltést a felhasználóknak, ha megadják bejelentkezési adataikat egy adott webhelynek *(baiting attack)* stb. Ide tartozhat bármely más csalárd tartalom, amelynek célja a felhasználó adatainak megszerzése.

Az adathalászat sajátos változata az úgynevezett bálnavadászat *(whaling attack),* amikor az adott szervezet, intézmény magasabb vezetője a célzott személy. A „kukázás" – különösen a lejárt naptárak, noteszek, jegyzetfüzetek kidobásakor – jó alkalom az odaírt és ott felejtett adatok megismerésére. Ez vonatkozik a magánszemélyek által otthonukban

kidobott naplókra, naptárakra is, de a napi munkavégzés során keletkezett és feleslegessé váló iratok is információk forrásául szolgálhatnak.

A malware-ek. Ha a magánfelhasználók és munkavállalók rákattintanak egy hamis e-mailre, könnyen válhatnak valamilyen malware-támadás áldozatává. A *malware* kifejezés az angol *malicious software* (rosszindulatú szoftver) összevonásából kialakított mozaikszó. A rosszindulatú számítógépes programok összefoglaló neve:

- vírusok (például boot-, alkalmazás-, makrovírusok), logikai bombák, férgek *(worm),*
- kémprogramok *(spyware),*
- agresszív reklámprogramok *(adware),*
- a rendszerben láthatatlanul megbúvó, egy támadónak különböző lehetőségeket biztosító program *(rootkit),*
- trójai programok,
- Stuxnet, DuQu.

Vírusok fajai:

- Bootvírus: a számítógép bootszektorába ágyazódik be, így még az operációs rendszer betöltése előtt aktiválódik. Ennek hatására a fertőzött merevlemez az összes meghajtóba helyezett lemezt megfertőzi.
- Alkalmazásvírusok (programvírusok): a megfertőzött állományokba beírják a saját kódjukat. Jellemzően két altípusát különböztetjük meg: kapcsolódó *(append)* és felülíró *(replace)* vírusok. Ez a vírus az alkalmazások végéhez kapcsolódik, a program elejére egy kódot fűz. Az alkalmazás indításakor a kód töltődik be, és csak utána a program. A felülíró vírusok az alkalmazások elejét írják felül saját kódjukkal, így a fertőzött állomány adatot veszít.

A zsarolóvírus a számítógépen tárolt fájlokat és könyvtárakat titkosítja le, és a feloldásukhoz szükséges kódért, programért cserébe pénzt (virtuális valutát) követelnek az elkövetők. Ismert a *police malware* zsarolóvírus, amely a felhasználó internetelérését zárolja a rendőrség nevében, azzal a hamis indokkal, hogy a felhasználó egy-egy tiltott tartalmat ért el, töltött le. Az internet újbóli elérését pénz fizetésétől teszik függővé. Ezek közül kiemelhetők az alábbiak:

- A *trójai program* egy másik programhoz kapcsolódik. Az eredeti program indításakor a felhasználó tudta és akarata nélkül aktiválódik (például egy letöltött játékprogrammal egy zombiprogramot is telepítünk).
- A *backdoor programok* a számítógép védelmi rendszerén nyitnak utat egy másik rosszindulatú program számára.
- A *spyware-ek* (általános elnevezéssel kémprogramok) a felhasználó aktivitását (a számítógép- és internethasználatunkat is) rögzíti, jelszavainkat, más ránk vonatkozó adatot fürkész ki, és továbbítja azokat egy másik számítógép számára a hálózaton.
- A *keylogger programok* speciális kémprogramok, amelyek billentyűleütéseinket rögzítik, naplózzák.
- A *dialer program* a telefonhoz modemen keresztül kapcsolódó számítógépeknél hatásos. A betárcsázó program a számítógép indításakor a felhasználó tudtán kívül egy emeltdíjas számot hív (akár folyamatosan). A hóvégi telefonszámla kifizetésekor szembesül a felhasználó a magas költséggel.

A számítógépes rosszindulatú programok mennyisége és veszélyessége folyamatosan növekszik, és időről időre új típusok terjednek el.

A Stuxnet-, DuQu-támadások. A Stuxnetet és DuQut azért kell külön kezelnünk, mert eltérnek az eddigi malware-ek tulajdonságaitól, és ez veszélyességüket rendkívül megnöveli. Egyfelől a malware-ek esetében már a nulladik napi támadást követően ismertté válik a hatásmechanizmusuk, így az ellenük kifejlesztett vírusirtó programok is hamarosan megjelennek és – legálisan vagy illegálisan – hozzáférhetők. Másfelől, míg a már megtapasztalt malware-ek hatása ismert, addig a Stuxnet csak egyetlen célba vett technikai, technológiai vagy más művelet megbénítására alkalmas. Veszélyessége tehát abban rejlik, hogy kiszámíthatatlan, hogy egy energetikai, honvédelmi, pénzügyi stb. rendszerben mely folyamatot vett célba, és annak milyen hatása lesz, hogyan mutálódik majd a malware, az elektronikus adatfeldolgozás és -átvitel mely pontján, mikor és ki fogja feltölteni az ilyen típusú malware-t.

Az adat- és programmanipuláció. A számítógépes adat szemmel nem látható, testetlen elektronikus impulzus, amely – információ hordozójaként – tények, fogalmak vagy utasítások formalizált ábrázolása, amely az emberek vagy automatikus eszközök számára közlésre, megjelenítésre vagy feldolgozásra alkalmas. A számítástechnikában adatnak számít a számítógépes állományok meghatározott része (minden, ami nem program), valamint mindaz, amivel a számítógépek működésük során foglalkoznak (ki- és bemeneti, tárolt, feldogozott, továbbított, megsemmisített adat). A program algoritmusok logikus sorozata, amely az adatokkal műveleteket képes végrehajtani.

Az informatikai rendszerben logikailag összetartozó, együtt kezelt adatokat nevezzük adatállománynak, amely tartalma szerint rendkívül sokrétű lehet, funkciója szerteágazó. A nemzeti adatállomány körébe tartoznak a Magyarországon kezelt adatok, amelyek megjeleníthetnek vagyoni (pénzügyi) értéket, az igazgatási szférák munkájához nélkülözhetetlen adatokat, személyhez kötött adatokat, audió- vagy videófelvételeket, szöveges vagy képi dokumentumokat. Az elektronikus adat csak meghatározott közegben, meghatározott időben bír jelentéssel az adatalany, az adat gyűjtője, más információbirtokos számára. Ezen adatokat lehet jogtalanul kifürkészni (megszerezni, „ellopni"), módosítani (felülírni: kiegészíteni, részlegesen törölni) vagy teljesen törölni, továbbá megosztani más belföldi vagy külföldi felhasználókkal. Az adatok manipulációja tartalmuktól függően okozhat vagyoni kárt és hátrányt, pénzben nem mérhető, jelentős érdeksérelmet, jelenthet szerzői, személyiségi jogsérelmet, titoksértést az adattal, vagy sértheti egy természetes személynek az adatállománnyal érintett jogát. Ugyanakkor egy-egy adatállomány vagy program manipulálása, továbbá más magatartások, például az elektronikus adatfeldolgozás akadályozása megbéníthat távközlési, kommunikációs rendszert, gyártási tevékenységet, pénzügyi folyamatokat. A programok kimunkálása, megalkotása szellemi tevékenység. Ez olyan érték, amely jogosulatlan használattal, másolással, kereskedéssel sérthető.

3.3. Veszélyek a közösségi hálózatokon

A közösségi hálók *(social networks)* története 1995-ben kezdődött. A *classmates.com* először az osztálytársak üzenőfalaként működött, majd megjelent a *SixDeegrees.com,* amelynek alapötlete az volt, hogy a Föld minden lakója megismerheti egymást hat lépés

(ismerős) megtételével. A magyar kísérlet az *iwiw.hu* oldallal kezdődött 2002-ben (a *who is who* rövidítésével), ezt a Facebook váltotta fel 2005-ben – ami a mai napig domináns világszerte a társas oldalak között. A közösségi hálók működésének anyagi alapját – leegyszerűsítve és a tőzsdei bevételeket nem tekintve – a reklámok teremtik meg. A vállalkozó fizet a Facebook reklámtevékenységéért, a Facebook pedig a felhasználó érdeklődési körének, életkorának, tartózkodási helyének és más paramétereinek megfelelően a reklámot kiosztja, azaz megjeleníti az idővonalakon. Minél több ismerőse van a hirdetőnek, annál több felhasználó idővonalán jelenik meg a reklám. Ezért kér a Facebook minél több adatot a felhasználótól/hirdetőtől, hogy azután a felhasználók által megadott adatokat összeillesztve, a közös találkozási pontok alapján jeleníthesse meg a reklámokat más felhasználó előtt. Sajnos a közösségi oldalak nemcsak ismerősök ismételt – virtuális, azután esetleg térbeli – találkozásához nyújtanak segítséget, hanem visszaélésekre is lehetőséget teremtenek.

Profillopás. A felhasználó fotójával egyetemben profilja „ellopható" (klónozható). Majd a valódi felhasználónak bosszúságot okozhat, lejárathatja, sőt jogellenes cselekménybe is sodorhatja, például a hamis profillal szélsőséges vallási, politikai csoportokhoz, nézetekhez csatlakozhat, tetszést nyilváníthat („lájkolhat") olyan bejegyzéseket, személyeket, amelyeket egyébként nem szeretne, valamint az áru- és szolgáltatásrendelés lehetőségét felkínáló reklámmal rendelhet tudtán kívül. A hamis felhasználó posztolhat olyan bejegyzéseket, képeket a valódi felhasználó nevében, amelyek személyiségi vagy más jogot, más felhasználókat sértenek.

Click-jagging. A klikk eltérítése, lopása egyben a felhasználók adatainak jogellenes gyűjtése. Olyan információ (hír vagy videó) megtekintésére invitál, amely a teljes terjedelmében nem jelenik meg, csak akkor látható teljességében, ha a felhasználó ráklikkel a *megosztás* vagy az *elfogadom* gombra, és akkor megjelenik a teljes információ. A felhasználó ezután továbblép, de a Facebookra feltöltött adatai ismertté válnak olyanok előtt, akik előtt nem is akarta volna, akikhez semmi kapcsolat nem fűzi. Illetőleg a clickjagger begyűjtött egy újabb kattintást is, ezáltal oldala *reklámértékét növelte.* Ugyanilyen clickjagging az az eset, amikor ingyenes vagy gyanúsan nagy árkedvezménnyel kínált termék vagy szolgáltatás elérhetőségével csábítják a felhasználót, de valójában csak a kattintására „vadásznak", mert szó sincs ajándékokról, kedvezményekről: vagy üres oldalra érkezik a felhasználó, vagy további adatait kérik el az immár a clickjagginget és a phishinget ötvöző elkövetők.

A közösségi oldalak remek terepet nyújtanak a hoaxnak. Ez a beugró információk, levelek, álhírek különféle változatait jelöli. Idetartoznak a lánclevelek is, amelyek információival továbbküldésre ösztönzik a felhasználót. A hoax küldői között a magányos elkövetőktől egy politikusig bárki lehet, akinek érdeke a megtévesztő hírközlés. A lánclevelek ugyanakkor Facebook-profilok, illetve sms-címek begyűjtésére is lehetőséget teremtenek.

3.4. A szerzői jog számítógépes környezetben

A könyvnyomtatás, a könyvterjesztés, a rádió- és televízióműsorok készítése, a terresztriális, majd műholdas, illetve (ezek kombinációjával is) kábelen történő műsorszórás a szerzői jog tradicionális rendelkezéseinek alapulvételével, illetőleg azok kiszélesítésével a szerzői jog – általában – alkalmazhatóvá vált. A szerzői jognak az új és újabb technikai eszközök és technológiák megjelenésére adott válasza és betartása (betartatása) a számítógép tömegessé

válásáig nem okozott eltúlzott nehézséget, mivel a szerzői művet készítők, továbbítók, forgalmazók és mások (például a rádió- és televíziós társaságok, a könyv- és lemezkiadással foglalkozó cégek, kábeltársaságok, színházak, filmforgalmazók, filmszínházak, könyvesboltok, kereskedelmi egységek) köre behatárolható volt. A szerzői művek az érdeklődők számára a valós térben érzékelhetők, ezáltal ellenőrizhetők voltak. De már a másológépek fejlődése, illetve hazánkban (is) a másolás állambiztonsági ellenőrzésének (stencilgépek kötelező elzárása, használatuk és használói naplózása, az intézményi és a vállalati írógépek ellenőrzése, azok betűmintáinak rögzítése stb.) megszűntével a másolás, majd a számítógépek háztartásokban történő megjelenésével a szerzői művek duplikálása, átalakítása, kiegészítése, engedély nélküli felhasználása, manipulálása és más, a szerzői jog által tiltott tevékenység tömegessé, ellenőrizhetetlenné vált. A számítógépek megjelenése magával hozta a digitális jelfeldolgozás (*Digital Signal Processing,* DSP) lehetőségét, azaz hogy a valóságos térben létező fizikai dolog (például szerzői mű) számítógéppel feldolgozhatóvá vált. A digitális jelfeldolgozás (a digitalizáció) lehetősége teremtette meg a szerzői művek másolását, készítését, kompilációját, tárolását, többszörözését, továbbítását, mégpedig a számítógépek és hálózatok fejlődésével egyre nagyobb mennyiségben. A digitális jelfeldolgozás vitte be az „övön aluli ütést", és megkérdőjelezte a szerzői jog tradicionális szabályait, intézményeit. A digitalizációval kiszabadult a szellem a palackból, amelyet már nem lehet visszatuszkolni. Ehhez már adott a technológia:

- a CD-k *(Compact Disc),* a VCD-k *(Video Compact Disc),* a DVD-k (*Digital Video* vagy *Versatile Disc*) készítésére, digitalizálásra, digitális formában történő tárolásra, többszörözésre, továbbításra;
- a DVD-k védőkódjainak feltörésére (dekódolásra);
- DVD, VCD konverziójára (rippelésére) valamely videofájl-formátummá;
- a szoftverek (számítógépes programok) védelmét kiiktató *crackek,* szériaszámok, *keygenerator-programok* (valamennyi alkalmas a kódfeltörésre) készítésére és a szoftverek védőkódjainak feltörésére (crackelésére);
- CD-lemezek rippelésére, tömörített MP3- vagy más tömörített fájl tömörítetlen audiofájllá alakítására;
- a régi mikrobarázdás (helytelenül: bakelit-) lemezek és a régi videókazetták digitalizálására;
- DVD kép- és hangfájljainak, feliratainak felhasználására, például idegen nyelvű DVD-felvételhez magyar szinkron vagy felirat illesztésére.

Mára megtört a szerzői művek másolásának, kiadásának, forgalmazásának monopóliuma. Mindez abban látható, hogy a fogyasztó nincs kiszolgáltatva a kínálati piacnak, választéknak, áraknak. Ha valamely filmhez nincs magyar szinkron, akkor régi videókazettáról (akár az eredeti filmről, akár a televízió műsoráról felvett filmről) a szinkron hozzáilleszthető a videófolyamhoz. Felirat készíthető olyan filmhez, amelyet hazánkban nem forgalmaznak, vagy lejárt a forgalmazás ideje. A digitalizált fényképekhez, videófilmekhez, a művészeti album képeihez önkényesen zenei aláfestés illeszthető, amely teljesebbé teszi az élményt diavetítéssel vagy videofájlformátumban való lejátszással. A számítógépes hálózatokon a felhasználó vagy más által rippelt, digitalizált szöveg-, audio-, video-, képfájlok, crackelt szoftverek megoszthatók (általában) ingyenesen a fájlcserélő hálózatokon

vagy (anyagi ellenszolgáltatás fejében) a surface weben vagy FTP-szervereken. A 2000-es évektől megjelent torrenthálózatok a szerzői művek illegális forgalmát megtöbbszörözték.

3.5. *Defacing* (webtartalom felülírása)

A fogalom felölel minden olyan jogosulatlan változtatást, amely egyetlen weboldal vagy egy teljes webhely megjelenésében változást eredményez, így a webtartalom módosul, a webhelyhez valamilyen veszélyes vagy fertőző kódot illesztenek, amely a webhelyet felkereső felhasználó számítógépére települ, ezzel a webhely működése leáll. A hackerek, miután hozzáfértek a kiszolgálóhoz, a képeket, szöveget a feltört weboldalra másolják. A cselekmény motívumai szerteágazók:

- külpolitikai vagy belpolitikai ok (a valós háborús cselekményeket gyakran kíséri az ellenség híroldalainak, kormányzati oldalainak felülírása, ezzel a lakosság félretájékoztatása),
- egyet nem értés, más jellegű tájékoztatás a belpolitikai helyzettel összefüggésben,
- terroristák félelemkeltés céljából üzennek ezzel a módszerrel,
- konkurens gazdasági vállalkozás weboldalának módosítása a vállalkozás vagy termékeinek lejáratása, rossz hírben történő feltüntetése céljából,
- hackerek, hackercsoportok erőfitogtatása,
- bosszú, unalom és más okok.

Mivel még viszonylag kevés számú felhasználó bír saját weblappal, így a *defacing-cselekményekben* sértettként elsősorban szervezetek, hivatalok, intézmények a veszélyeztetettek.

3.6. A terheléses vagy szolgáltatásmegtagadással járó támadások

Míg az előzőekben ismertetett támadásfajták bármely magánfelhasználót érinthetnek, addig a terheléses támadás jellemzően szervezetek, intézmények, hivatalok ellen irányulnak. A terheléses, avagy szolgáltatásmegtagadással járó támadás egy olyan támadási forma, amelynek a célja az információs rendszerek, szolgáltatások vagy hálózatok oly mértékben történő túlterhelése, hogy azok elérhetetlenné váljanak, ne tudják ellátni az alapfeladatukat. Az ilyen elektronikus támadást intézők a jogosult felhasználókat akadályozzák a szolgáltatás igénybevételében – innen a *szolgáltatásmegtagadással járó* elnevezés is –, ennek leggyakoribb formája a webszerver elérését és rendeltetésszerű használatát gátolja a mesterségesen generált és megnövekedett adatforgalommal. Az elnevezés a támadás angol megfelelőjének rövidítéséből ered, amely során az említett támadás egyetlen számítógéptől származik, több közbeiktatott gép nélkül: *Denial of Service (DoS).* Amennyiben a támadás összetettebb, mert összekapcsolt rendszerek csoportjától, egyszerre sok – lehetőleg minél több – helyről indul, akkor használatos a *Distributed Denial of Service (DDoS),* vagyis az *elosztott szolgáltatásmegtagadással járó támadás* elnevezés. Ebben az esetben a feladatot nem egyetlen eszköz végzi el, mint a DoS-támadásnál, hanem a rendszert alkotó – egymástól akár nagy távolságban lévő – eszközök (például asztali gépek, mobiltelefonok vagy routerek) párhuzamosan. A technikai alapja leegyszerűsítve a következőképpen néz ki:

amikor a felhasználó az internethez kapcsolódik, akkor egyben az úgynevezett hozzáférést biztosító szolgáltató szerveréhez is, amellyel adatcsomagokat váltanak egymással. Közben megtörténik mindkettőjük azonosítása (ügyfél személye, jogosultsága, a keresett weboldal azonosítása, a szerver azonosítása stb.), majd a szerver a keresett weboldal szerverére irányítja a felhasználót. A támadás esetében a célzott szerverre ezer- vagy tízezerszámra érkeznek adatcsomagok egy időben, amelyre a szervernek – időrendi sorrendben – válaszolni kellene. A DDoS-támadás során a támadó a hálózatot alkotó számítógépek adatcsomagjaival elárasztja a célzott szervert akkora forgalommal, hogy az képtelen lesz az adatcsomagok fogadására, azok megválaszolására, ezzel akár a rendszer teljes leállását is eredményezhetik, azonban a funkcionális működésképtelenséghez elegendő a nagymértékű lelassulás is, ami a válaszidő megnövekedett mértékéből adódik. Azokat a felhasználó tudta és akarata nélkül megfertőzött számítógépeket, amelyek távolról irányíthatók, *zombinak* nevezik. Másik elnevezésük a *robot* és *network* szavak összevonásából eredő *botnet,* amely a több bot összekapcsolásával keletkezett hálózatot jelenti. A botnet irányítóját, aki kiosztja a feladatot a fertőzött eszközöknek, *botmasternek,* illetve több irányító esetén *botherdernek* hívják. A botnet tagjait a fertőzött zombiszámítógépek alkotják. Azt a központi vezérlő eszközt, amely vezérli a botnetakciókat, *controllernek* hívjuk. A controller általában az úgynevezett *drop serverre* csatlakozik, amely a botnet által gyűjtött adatok tárolására szolgáló tárhelyet jelenti, ami hozzáférhető a botnet tagjai és a botmaster részére is. A botmaster és botnet közti kapcsolatot és az utasítások eljuttatását biztosító kommunikációs útvonal az úgynevezett *Command&Control (C&C-)* csatorna. A botnetek egyben alkalmasak spamküldésre, adathalászatra, hálózatfigyelésre, billentyűzetfigyelésre, illetve a klikkelések begyűjtésére is.

3.7. Az elektronikus adatok kifürkészése

Az internet kommunikációra született, és a kommunikációs lehetőségek is folyamatosan bővülnek. Többféle szöveges, audio- és videokommunikáció ad lehetőséget a felhasználóknak hírt adni magukról, beszélgetni. Az elektronikus adatok kifürkészése többféle esetkört ölel fel, és többféle technikai megvalósulása lehetséges már most is. Idesorolható

- az informatikai rendszeren belüli,
- az informatikai rendszerből származó vagy
- az informatikai rendszerre irányuló, nem a nyilvánosságnak szánt elektronikus adatok kifürkészése, a számítástechnikai rendszerből származó elektromágneses sugárzás rögzítése a technikai eszközök felhasználásával történő jogosulatlan, szándékos továbbítás során.

Az elektronikus adatok kinyerhetők az elektronikus adatot küldő személytől, az azt fogadó személytől és a kommunikáció útja során – az elektronikus kábel megcsapolásától, a különböző kémprogramoktól a közbeékelődéses támadáson át az informatikai eszközök meghackeléséig.

Ugyanígy, a bekapcsolva hagyott számítógépekbe, a nyitva hagyott e-mail-fiókokba történő jogosulatlan betekintés is jogosulatlan kifürkészés. Az elektronikus kifürkészés célja a kommunikáció tartalmának a megismerése, amelynek motívumai különbözőek lehetnek

a politikai kémkedéstől az üzleti titoksértésen át a magánszemélyek privát céljáig. A sértetté válás lehetősége a gondatlan, felkészületlen felhasználókat fenyegeti.

3.8. A *card not present* esetköre

E bűncselekményi formáról akkor beszélünk, amikor a tranzakciónál nincs jelen a kártya. Az online, a telefonon, mobiltelefon applikációján keresztül történő áru- vagy szolgáltatásrendelés kifizetésénél nincs jelen a bankkártya. A veszélye abban rejlik, hogy az eladó nem vizsgálhatja meg a bankkártya tulajdonosát, hogy a bankkártya valósnak tűnik-e, hiszen fizetéskor a bankkártya validitását ellenőrzi a befogadó bank rendszere. A bankkártya lehet klónozott is. A bankkártya ma már multifaktoros védelme (elektronikus és biometrikus azonosítók, a tranzakciók és az identitás összekapcsolása, figyelemmel kísérése és más megoldások) sem nyújtanak teljes körű biztonságot a *card not present csalások* ellen. A bankkártya azonosítóinak jogellenes megszerzése történhet:

- adathalászat által (hamis banki oldalon történő adatközléssel, hamis tartalomközlő e-mailben),
- korábbi tranzakciók esetében az adatok online kifürkészése által,
- a bankkártyával fizikai kapcsolatba került tisztességtelen személyek által.

A bankkártyahasználat bizalmasságát, titkosságát veszélyezteti a nyílt hozzáférésű wifi vagy a nem védett mobiltelefonok applikációinak a használata. Az alvilágban a bankkártyaadatok hatalmas értékkel bírnak. A bűnözők saját kényük-kedvük szerint költhetik a kártyabirtokos pénzét (megélhetésükre, kábítószerekre, hamis okmányokra, fegyverre, egy további bűncselekmény fizikai előkészületeire stb.), vagy továbbadják az adatokat.

3.9. A terrorjellegű támadások és más e körbe vonható jelenségek a kibertérben

A terroristák ugyanúgy élnek azokkal a lehetőségekkel, alkalmazásokkal, amelyeket bármely más felhasználó ismer. Amire fel kell figyelni, az a technikai adottságok szinte teljes körű és professzionális használata:

- a terrorista szervezetet népszerűsítő (hírközlő) tartalomközlések, weboldalhoz csatolt audió- és videófolyamok (például a lefejezések bemutatása félelemkeltés céljával),
- a terrorista szervezetet népszerűsítő weboldalak tartalmai tagtoborzás céljával (mélyen vallási vagy szerzői jogsértést segítő P2P-tartalmak segítenek a szimpátia elnyerésében),
- a terrorszervezet aktív tagjaival vagy *alvó ügynökeivel,* más segítőkkel (külföldre telepített támogatóival) való kapcsolattartás, információk (parancsok) közlése: például egy adatforgalmat nem mutató e-mail-fiókban a piszkozatmappában hagyott üzenetet elolvassák, majd törlik azokat, vagy újat írnak oda, vagy a weboldalon elrejtett üzenetek formájában (szteganográfia módszerével), illetőleg FTP-szervereken, a dark weben és másutt (gyakorlatilag bárhol),

- a tagok, a szimpatizánsok anyagi eszközökkel való ellátása (valós vagy virtuális térben történő pénzutalással),
- a szervezet anyagi eszközeinek realizálása pénzmosás útján,
- terheléses vagy malware-támadások, illetőleg ezekkel történő fenyegetések állami, társadalmi, politikai szervezetek szerverei, kritikus infrastruktúrák ellen,
- zsarolóvírussal történő támadások, illetőleg ezekkel történő fenyegetések ugyanezen célzott szerverek ellen,
- állami, társadalmi, politikai szervezetek weblapjainak felülírása hamis hírek közlése, propaganda céljával.

3.10. Az informatikai rendszer mint eszköz, cél és tárhely

Az informatikai rendszer bűncselekményeknek, jogsértésként (még) nem definiált visszaéléseknek, erkölcsbe ütköző cselekményeknek egyszerre *eszköze* (ennek is sajátos formája, ha kommunikációs eszköz), *célpontja* és *tárhelye.* Azokat a számítástechnikai instrumentumokat tekintjük eszköznek, amikkel a bűnelkövető felhasználó eléri vagy elérni kívánja célját. Céljai lehetnek: az informatikai rendszerben tárolt személyes, vagyoni értéket megtestesítő adatok jogellenes megszerzése, zaklatás, üzleti és más titkok kifürkészése, az informatikai rendszer működésének megzavarása malware- vagy terheléses támadással, vagy más módon.

Az *elektronikus adatok* lehetnek – a fenti bűncselekmények kapcsán említett – tartalomközlés megjelenítői is, így közvetett eszköznek is tekinthetők. Sajátos esetkör, ha az informatikai rendszer kommunikációs eszközként funkcionál. Ebben az esetben jellemzően a kommunikáció nem valósít meg bűncselekményt, kivéve, ha verbális bűncselekményekről vagy valamely verbális bűnrészesi (felbujtás, pszichikai bűnsegélyi) alakzatról van szó, esetleg olyan bűncselekményről, amelynek az előkészülete is büntetendő, és akkor a szóbeli előkészületi magatartások megvalósítása büntetni rendelt. *Célpont* lehet az informatikai rendszer azon adatok irányába, amelyeket a rendszer kezel (tárol, rendszerez, továbbít stb.). A személyes, pénzügyi, igazgatási és más adatok, titkok megszerzése céljából elkövetett adatszerzés bűncselekmény. Bár az informatikai bűncselekmények zöme intellektuális támadás, néhány fizikai támadásforma is előkerült, így a neoluddita eszmeiségű géprombolás vagy az ATM-t kitépése a falból, az ATM rendszerére történő technikai rácsatlakozás. Léteznek olyan esetek is, amelyekben az informatikai rendszer egyszerre *eszköz és célpont.* Például a készpénz-helyettesítő fizetési eszköz hamisítása inkább célcselekmények közé illeszthető, míg a készpénz-helyettesítő fizetőeszközzel történő visszaélés jellemzően olyan eszközcselekmény, amihez informatikai eszköz használható (*card present* esetek). Ugyanígy, a *card not present* esetek egy részénél a kártya adatainak kifürkészése egy célcselekmény, máskor pedig eszközcselekmény csalás végrehajtásához. A szerzői alkotások eléréséhez informatikai eszközök szükségesek, a cél pedig azokra szert tenni. Az informatikai rendszer *tárhelye* lehet a valós és a virtuális térben elkövetett bűncselekmények bizonyítékainak, egyéb nyomainak is.

4. A kiberbűncselekmények szabályozása

Nagy Zoltán

4.1. Kiberbűncselekmények a jelentősebb nemzetközi jogi dokumentumokban

A számítástechnika gyors fejlődése, a miniatürizálás, a gyártók számának dinamikus növekedése, ezzel a tömegtermelés lehetővé tette a számítógépek széles körű elterjedését, egyben magáncélú felhasználását az 1970-es évek második felétől. Ahogy a számítógépek a konvergencia térhódításával, valamint az 1990-es évektől az internetes alkalmazások egyre szélesebb lehetőséget nyújtottak, úgy a visszaélések fajtái is folyamatosan bővültek. Az új technika-technológia által teremtett új típusú visszaélésekre mint kihívásokra először az anyagi büntetőjogot értékelve kerestek választ. Az informatikai bűncselekmények első megjelenése az Európa Tanács által a tagállamok számára 1981-ben kibocsátott gazdasági bűncselekményekről szóló ajánlásában érhető tetten, ebben példálózva három informatikai bűncselekmény szerepelt csupán. Az OECD 1986-ban kiadott éves jelentésében négyféle e körbe tartozó bűncselekményt említ. Nagy előrelépést jelentett az Európa Tanács 1989-es ajánlása, mivel az ott felsorolt cselekmények lényegi ismérveit meghatározta. Az ajánlásban a kriminalizálni javasolt cselekmények közül nyolc az úgynevezett minimális listán, további négy cselekmény az úgynevezett fakultatív listán szerepel.[1] Ezek közül kiemelhető néhány:

- *Számítógépes csalás:* adatok, programok bevitele, megváltoztatása, törlése, elrejtése vagy más, az elektronikus adatfeldolgozási folyamat befolyásolását eredményező magatartás, amellyel az elkövető egy harmadik személynek gazdasági vagy vagyoni hátrányt okoz, illetve amelynek célja az, hogy az elkövető önmaga vagy más számára gazdasági, illetőleg vagyoni előnyhöz jusson. Az ajánlás alternatív tényállási eleme, hogy az elkövető más személyt vagyonától megfosszon.
- *Számítógépes hamisítás:* adatok, programok bevitele, megváltoztatása, törlése, mentése vagy más, az elektronikus adatfeldolgozási folyamat befolyásolását eredményező beavatkozás, amelynek révén megvalósul a hazai jogban meghatározott hagyományos hamisítás bűncselekménye.
- *A számítógépes adatokban és programokban történő károkozás:* az adatok és/vagy programok jogosulatlan törlése, rongálása, károsítása, mentése.

---

[1] Council of Europe (1989): *Computer-related crime, Recommendation No R (89) 9 on Computer-related Crime and final report of the European Committee on Crime Problems.* Elérhető: www.coe.int/t/dg3/healthbioethic/texts_and_documents/Rec(89)2E.pdf (A letöltés dátuma: 2019. 06. 01.)

- *Számítógépes szabotázs:* olyan adatok és/vagy programok bevitele, megváltoztatása, törlése vagy a számítógépes rendszerek más befolyásolása, amely célja, hogy annak telekommunikációs funkcióját akadályozza.
- *Jogellenes behatolás:* a számítógépes rendszerbe vagy hálózatba történő jogosulatlan bejutás a biztonsági intézkedések megsértése révén.
- *Jogellenes titokszerzés.*
- *Védett számítógépes programok jogellenes másolása.*
- *Félvezető topográfiák jogellenes másolása.*

Az ajánlás tartalmazott egy rövid fakultatív listát is, mint az adat- vagy programváltoztatás, kémkedés, számítógép jogellenes és kárt okozó használata, védett számítógépes programok jogellenes használata.

A büntetőjogot érintő kihívások nemcsak a büntető anyagi jogot, hanem a büntető eljárásjogot is szükségképpen érintette, és jelenleg is érinti. Az Európa Tanács 1995-ben adott ki egy újabb ajánlást, amely az információs technológiával kapcsolatos büntető eljárásjogi problémákat gyűjtötte egybe.[2] Az Európa Tanács ajánlása az alábbi kérdésekkel foglalkozott:

- A kutatás, lefoglalás jogszabályi feltételeinek megteremtése, ideértve a jogorvoslati lehetőséget is.
- A telekommunikációs vállalatok technikai őrizetre történő kötelezése jogi szabályainak kialakítása.
- Együttműködési kötelezettség a nyomozó hatóság és a nyomozással érintett szervek között.
- Az elektronikus bizonyítékok integritásának, eredetiségének biztosítása a nyomozás során és a nemzetközi együttműködés során. Az elektronikus bizonyítékok ugyanúgy kezelendők, mint a többi tárgyi bizonyíték.
- Titkosítás használata.
- Tudományos kutatás, képzés, statisztikák fontossága.

Hosszas előkészületek után 2001-ben írták alá a *Számítógépes bűnözés elleni nemzetközi egyezményt* Budapesten. Gyakran nevezik ezt a nemzetközi okmányt *budapesti egyezménynek* is. Az egyezményt Magyarország törvénnyel jogforrásai közé emelte.[3] Az Európa Tanács korábbi két ajánlása után – az ET 9. (89) sz. és ET 13. (95) sz. – a 2001-es *Számítástechnikai bűnözésről szóló egyezmény (Convention on Cyber-crime)* újabb mérföldkövet jelentett, mivel

- lépést tartott az elektronikus adatfeldolgozás és -átvitel technológiai fejlődésével folyamatosan megjelenő újabb visszaélések meghatározásával, így a hálózatokon megjelenő tartalomközlésekben megnyilvánuló cselekmények javasolt kriminalizálásával,

[2] Council of Europe, Recommendation No. R (95) 13 Concerning Problems of Criminal Procedural Law connected with Information Technology. Elérhető: https://rm.coe.int/16804f6e76 (A letöltés dátuma: 2019. 06. 01.)

[3] 2004. évi LXXIX. törvény az Európa Tanács Budapesten, 2001. november 23-án kelt Számítástechnikai Bűnözésről szóló Egyezményének kihirdetéséről.

- a számítógépes bűnözéssel összefüggő anyagi, eljárásjogi és nemzetközi büntetőjogi problémákat komplexen kezeli,
- a számítógépes környezetben felmerülő (jogi és technikai) fogalmakat definiálja, azaz egységes értelmezést nyújt azokról.

Az egyezmény a bűncselekményeket – az ET 9. (89) sz. ajánlását alapul véve – immár dogmatikailag letisztultan csoportosítja:

1. *A számítástechnikai rendszer és a számítástechnikai adat hozzáférhetősége, sértetlensége és titkossága elleni bűncselekmények:*
   - jogosulatlan belépés,
   - jogosulatlan kifürkészés,
   - számítástechnikai adat megsértése,
   - számítástechnikai rendszer megsértése,
   - eszközökkel való visszaélés.
2. *Számítógéppel kapcsolatos bűncselekmények:*
   - számítógéppel kapcsolatos hamisítás,
   - számítógéppel kapcsolatos csalás.
3. *Számítástechnikai adatok tartalmával kapcsolatos bűncselekmények:*
   - gyermekpornográfiával kapcsolatos bűncselekmények.
4. *Szerzői vagy szomszédos jogok megsértésével kapcsolatos bűncselekmények.*

Az 1. pontban említett cselekmények értelmezésére az Európai Tanács 2013/40-es direktíváját idézzük lentebb. A 3. pont később kiegészült egy 2002-ben született, de 2006. március 1-től hatályos jegyzőkönyvvel az informatikai környezetben elkövethető rasszista és idegengyűlölő cselekményekről.[4] Az egyezmény továbbá a büntetőeljárás során keletkezett jogi polémiák megoldására törekedett. Az egyezmény büntető eljárásjogra vonatkozó rendelkezései:

- tárolt számítástechnikai adat gyors megőrzése (tárolt számítástechnikai adat gyors megőrzése, forgalmi adat gyors megőrzése és részbeni átadása);
- közlésre kötelezés;
- tárolt számítástechnikai adat átvizsgálása és lefoglalása;
- számítástechnikai adatok valós idejű összegyűjtése (forgalmi adatok valós idejű összegyűjtése, tartalomra vonatkozó adatok kifürkészése).

Az egyezmény nemzetközi büntetőjogi tárgyú rendelkezései:

- jogsegélykérelemmel kapcsolatos eljárás hatályos nemzetközi megállapodás esetében, általános alapelvek,
- jogsegélykérelemmel kapcsolatos eljárás hatályos nemzetközi megállapodások hiányában, általános alapelvek,
- ideiglenes intézkedéssel kapcsolatos jogsegély,
- tárolt számítástechnikai adat gyors megőrzése,
- megőrzött forgalmi adat gyors átadása,

[4] Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems (ETS No. 189).

- nyomozati jogkörökkel kapcsolatos jogsegély,
- tárolt számítástechnikai adathoz való hozzáférésre vonatkozó jogsegély,
- tárolt számítástechnikai adathoz való hozzáférés határokra tekintet nélkül, hozzájárulás vagy nyilvános elérhetőség esetén,
- forgalmi adat valós idejű összegyűjtésével kapcsolatos jogsegély,
- tartalomra vonatkozó adat kifürkészésére vonatkozó jogsegély,
- a 24/7 hálózat (kapcsolattartás) megteremtése.

Az Európai Parlament és a Tanács 2001/29/EK irányelve egyetlen bűncselekménytípust érint: az információs társadalomban a szerzői és szomszédos jogok egyes vonatkozásainak összehangolására tett ösztönző lépéseket. Ugyanis a modern technológiák fejlődésével a szerzői jogot érő kihívásokra a tagállamok különböző módon reagáltak. A direktíva javaslatot tesz a tagállamok szerzői jogi rendelkezéseinek közelítésére. *In concreto* egyik fontos megállapítása kiemelést érdemel, ami szerint különbséget kell tenni az analóg és a digitális másolás között, és eltérő szabályokat lenne érdemes alkotni (38. pont).

Az *Európai Tanács 2001/413/IB kerethatározata* ugyancsak egy bűncselekményi körre vonatkozó rendelkezéseket tartalmazott. A nem készpénzes fizetőeszközökkel összefüggő csalás és hamisítás elleni küzdelem kapcsán arra hívja fel a figyelmet, hogy a készpénzhelyettesítő fizetőeszközök hamisítása számítástechnikai eszközökhöz kötött.

Az Európai Tanács 2004/97/EK határozatával[5] létrehozta az Európai Hálózat- és Információbiztonsági Ügynökséget (ENISA). A szervezet határozatban rögzített célja az, hogy az Európai Unió (EU), az EU-tagállamok és az üzleti szféra fokozottabb mértékben legyen képes a hálózat- és információbiztonsággal kapcsolatos problémák megelőzésére, kezelésére és az azokra történő reagálásra. Ennek érdekén a szervezet iránymutatásokat ad ki, tájékoztatókat, és gyakorlatokat tart. Éves jelentéseiben gyűjti össze az informatikai biztonságot érintő, az európai országokban felmerült problémákat és a megoldásukra tett javaslatot.

Az *Európai Tanács* 2009 decemberében fogadta el az úgynevezett *stockholmi programot,* amely a 2010–2014 közötti időszakra az Európai Unióban a jog, a szabadság, a biztonság szem előtt tartásával, annak érvényesülő követelményével összefüggő feladatokat határozta meg. A cselekvési program az alábbi határokat átlépő bűncselekmények, közöttük az informatikai bűncselekmények üldözésének fontosságát hangsúlyozza fő irányként:

- emberkereskedelem,
- szexuális zaklatás, gyermekek szexuális kizsákmányolása, gyermekpornográfia,
- *informatikai bűnözés,*
- gazdasági bűnözés, így a korrupció, hamisítás és kalózkodás, valamint
- a kábítószerrel összefüggő bűnözés.

A stockholmi program alapján került kibocsátásra a *2011/92/EU irányelv*, amely leszögezte, hogy a gyermekek szexuális bántalmazása, szexuális kizsákmányolása és a gyermekpornográfia elleni küzdelem egyaránt ki kell, hogy terjedjen a valós és a virtuális térre. A direktíva a tagországokat szigorú szankciók alkalmazására ösztönzi.

Ugyancsak a stockholmi program továbbvitelét jelenti a *2013/40/EU irányelv* az információs rendszerek elleni támadásokról. Az irányelv kibocsátásának célja az informa-

[5] Módosította: az 526/2013/EU rendelet.

tikai bűncselekmények tényállásaira és szankcióira vonatkozó minimumszabályokra tett javaslatok megtétele. A közös szabályrendszer ezáltal közelítse a tagállamok büntetőjogát; ezzel tegye hatékonyabbá a bűnügyi jogsegélyt, valamint a tagállamok nyomozó hatóságai, az Europol, az Eurojust[6] és az ENISA közötti együttműködés. A direktívában meghatározott minimum-bűncselekmények köre és azok tartalmi lényege a következő:

- *Információs rendszerekhez való jogellenes hozzáférés:* valamely információs rendszerhez vagy annak egy részéhez való, szándékosan és jogosulatlanul történő hozzáférés legalább a súlyosabb esetekben bűncselekménynek minősüljön akkor, ha a bűncselekményt valamely biztonsági intézkedés megsértésével követték el.
- *Rendszert érintő jogellenes beavatkozás esetében:* a számítógépes adatok szándékos és jogosulatlan bevitele, továbbítása, megrongálása, törlése, minőségi rontása, megváltoztatása vagy elrejtése, ilyen adatok szándékos és jogosulatlan hozzáférhetetlenné tétele révén történő súlyos akadályozása vagy megszakítása legalább a súlyosabb esetekben bűncselekménynek minősüljön.
- *Adatot érintő jogellenes beavatkozás esetében:* az információs rendszer számítógépes adatainak szándékos és jogosulatlan törlése, megrongálása, minőségi rontása, megváltoztatása vagy elrejtése, illetve az ilyen adatok szándékos és jogosulatlan hozzáférhetetlenné tétele legalább a súlyosabb esetekben bűncselekménynek minősüljön.
- *Jogellenes adatszerzés esetében:* az információs rendszeren belülre, kívülre vagy azon belül továbbított, nem nyilvános számítógépes adatok – többek között az információs rendszerekből érkező, ilyen adatokat hordozó elektromágneses sugárzás – technikai eszközökkel történő szándékos és jogosulatlan megszerzése legalább a súlyosabb esetekben bűncselekménynek minősüljön.
- *A bűncselekmények elkövetéséhez használt eszközök esetében:* meghatározott eszközök jogosulatlan és bármely fenti bűncselekmény elkövetéséhez való felhasználásának szándékával való előállítása, árusítása, használatra történő beszerzése, behozatala, forgalomba hozatala vagy egyéb módon történő hozzáférhetővé tétele legalább a súlyosabb esetekben bűncselekménynek minősüljön (olyan számítógépes programok, amelyek elsősorban a fentebb említett bármely bűncselekmény elkövetésére készültek vagy lettek átalakítva, olyan számítógépes jelszavak, belépési kódok vagy hasonló adatok, amelyekkel egy információs rendszerhez vagy annak egy részéhez hozzá lehet férni).
- Felbujtás, bűnsegély és kísérlet kérdésköre.
- Szankciók.

Mind a joggyakorlat, mind az oktatás-kutatás számára alapul szolgálnak – egyéb források mellett – az *Europol IOCTA-jelentései*[7] (magyarul: *Helyzetjelentés a számítógépes bűnözésről, a megismert fenyegetésekről, a várható tendenciákról*). A 2014 óta évente megjelenő kiadványok (megjelenésük alapján elnevezve *Fehér Könyvekben,* amelyek az interneten is szabadon elérhetők) összegezik az adott időszakban feltűnt fenyegetéseket, az újabb s újabb

[6] Az Eurojustot a Tanács 2002/187/IB határozata hozta létre.

[7] Internet Organised Crime Threat Assessment, avagy *az interneten zajló szervezett bűnözéssel kapcsolatos fenyegetésértékelés.*

visszaéléseket, a szakemberek, a tagállamok tapasztalatait, szakértőik és mások tudományosan megalapozott kutatásainak eredményeit.

4.2. A kiberbűncselekmények hazai szabályozása

Az első informatikai bűncselekmény 1994-ben tűnt fel a magyar Büntető Törvénykönyvben. A bűncselekmény elnevezése *számítógépes csalás* volt, de a tényállás alkalmazható volt valamennyi elektronikus adat vagy program elleni cselekményre, tehát például egy malware-támadás esetére is, így a tényállás tartalma túlnőtt a bűncselekmény elnevezésén. A tényállás 1996-ban a mobiltelefon és a közcélú mobiltelefon kártyája manipulálásának büntetendőségével bővült. A 2001-es módosítás megtartotta a bűncselekmény elnevezését. A tényállás struktúrája követte a „hagyományos" csalás szerkezetét azzal, hogy a megtévesztés az adat- vagy programmanipuláció volt, és a kár fogalmának a tényállásba épülésével a minősített esetek köre is a kár nagyságához igazodóan bővült. A 2012. évi C. törvény alapján három informatikai bűncselekmény tényállását tekintjük át.

4.2.1. Információs rendszer vagy adat megsértése

„423. § (1) Aki információs rendszerbe az információs rendszer védelmét biztosító technikai intézkedés megsértésével vagy kijátszásával jogosulatlanul belép, vagy a belépési jogosultsága kereteit túllépve vagy azt megsértve bent marad, vétség miatt két évig terjedő szabadságvesztéssel büntetendő.

(2) Aki

a) az információs rendszer működését jogosulatlanul vagy jogosultsága kereteit megsértve akadályozza, vagy

b) információs rendszerben lévő adatot jogosulatlanul vagy jogosultsága kereteit megsértve megváltoztat, töröl vagy hozzáférhetetlenné tesz,

bűntett miatt három évig terjedő szabadságvesztéssel büntetendő.

(3) A büntetés bűntett miatt egy évtől öt évig terjedő szabadságvesztés, ha a (2) bekezdésben meghatározott bűncselekmény jelentős számú információs rendszert érint.

(4) A büntetés két évtől nyolc évig terjedő szabadságvesztés, ha a bűncselekményt közérdekű üzem ellen követik el.

(5) E § alkalmazásában adat: információs rendszerben tárolt, kezelt, feldolgozott vagy továbbított tények, információk vagy fogalmak minden olyan formában való megjelenése, amely információs rendszer általi feldolgozásra alkalmas, ideértve azon programot is, amely valamely funkciónak az információs rendszer által való végrehajtását biztosítja."

A *bűncselekmény jogi tárgya* (a jog által védett érték) az informatikai rendszerek biztonságos működése, a *b)* pont esetében a jogi tárgy kiegészül az elektronikus adatok megbízhatóságához, hitelességéhez fűződő érdekkel.

4.2.1.1. A bűncselekmény elkövetési (tevékenységi) tárgyai

- Egyetlen számítógép vagy informatikai rendszer és
- számítógépes programok, elektronikus adatok mint elektronikus impulzusok.

Egyetlen számítógép esetében közömbös, hogy notebookról, laptopról, iPhone-ról, iPodról, iPadről, tabletről vagy okostelevízióról van-e szó. Az egyszerűség okán ezekre a továbbiakban csak a számítógép kifejezést használjuk. Az informatikai rendszer számítógépek összekapcsolódása révén létrejövő hálózat.

4.2.1.2. A bűncselekmény elkövetési (tevékenységi) magatartásai

Az (1) bekezdés *a)* pontjában szabályozott két eset:
- jogosulatlan belépés informatikai rendszerbe,
- a belépési jogosultság kereteit túllépve vagy azt megsértve a rendszerben maradás.

A jogosulatlan belépés történhet:
- egy más által jogszerűen használt számítógépbe, a jogosult használó színlelésével vagy
- számítógépen keresztül egy védett hálózatba.

A jogosulatlan belépés *akkor tényállásszerű,* ha
- a rendszer biztonsági megoldásokkal védett, és
- a védelem aktív, azaz szükséges legyen a belépéshez jelszavak, kódok, más azonosítók használata a hálózat eléréséhez. Ezek konjunktív feltételek.

Az elkövető aktív védelemmel ellátott számítógépbe vagy hálózatba *jogosulatlanul lép be,* ha
- a számítógép vagy hálózat biztonsági rendszerbeli hiányosságai kihasználásával lép be jogosulatlanul, vagy
- a jogosult felhasználó nevével (belépési kódjával), jelszavával vagy a belépést biztosító adat birtokában,
- kódfeltörő program segítségével vagy más módon teszi ezt.

Az itt olvasható (1) bekezdés esetében közömbös a kódok, jelszavak megszerzésének módja, azaz hogy megtévesztéssel, más csalárd módon, kifürkészéssel, a felhasználó hanyagsága folytán, a felhasználó ellen erőszak, fenyegetés alkalmazásával szerzi-e meg a jelszót. Az erőszakkal, fenyegetéssel történő belépési azonosító megszerzése, de fel nem használása kényszerítés bűncselekményének (Btk. 195. §) minősül. A kényszerítés útján szerzett belépési azonosítóval történő belépés esetén valódi, anyagi, heterogén halmazat jön létre. A megtévesztéssel történő belépési azonosító megszerzésének a módja az úgynevezett social engineering. A védett wifihálózatba történő jogosulatlan belépés – a kissé ijesztőnek tűnő – *war driving* elnevezéssel ismert a szakirodalomban. Büntethetőséget megszüntető ok, ha az informatikai rendszer nem védett, illetve a védelem nem aktivált. *A belépési jogosultsága kereteinek túllépésével, illetőleg annak megsértésével történő bennmaradás* esetében a belépés jogszerűen történt, az elkövető saját vagy rábízott felhasználói névvel,

jelszóval, a legális belépési ponton lép be az információs rendszerbe, ám a felhasználói jogosultságát meghaladó műveleteket kíván folytatni. Például a felhasználó jogszerűen veszi igénybe a kereskedelmi bankok telebanking szolgáltatását, de olyan műveleteket kíván végrehajtani, amelyre a bankkal kötött szerződés alapján nincs jogosultsága, például egy másik ügyfél bankszámláját, annak forgalmát kívánja megtekinteni. Továbbá, ha a rendszergazda, aki jogosult rendszerébe belépni, jogellenesen az intézmény, vállalkozás felhasználóinak adatait, forgalmát gyűjti ki, ha ez utóbbi nem valósít meg személyes adattal visszaélést (Btk. 219. §), kémkedést (Btk. 261. §), minősített adattal visszaélést (Btk. 265. §), esetleg más bűncselekményt. Megjegyezni kívánjuk, hogy a jogosulatlan belépést, „elektronikus betörést" *hackingnek* (hacker által végzett tevékenységnek) nevezik. A *hacker* és a *bűnöző* nem szinonim fogalmak. Ma már a rendőrségi nyomozáshoz, katonai műveletek folytatásához elengedhetetlenül szükség van egy szakmailag felkészült és elnevezésében „jó" hackerre, úgynevezett *white hat hackerre.* A *jó hackerek* tevékenysége nélkülözhetetlen, az ő tudásuk, ismereteik védhetik meg az állam, az intézmények, vállalkozások számítástechnikai rendszereit a *rossz hackerek* támadásaitól. Egyes országokban jó hackerekből álló önkéntes csoportokat is szerveztek. A *jó hacking* egyik legismertebb esete az űrben baleset szenvedett Apollo–13 űrhajósai életének megmentése volt 1970-ben, további példák a Hubble-teleszkóp, a Pioneer–10 működésének megmentése.

Az (1) bekezdés *b)* pontjában szabályozott esetben az elkövető az informatikai rendszer működését jogosulatlanul vagy jogosultsága kereteit túllépve *akadályozza.* Tipikus esete az úgynevezett malware-támadás indítása. A *malware* szó a *malicious software* szavak összevonásából keletkezett. Felöleli a legkülönbözőbb kártékony programokat: vírus, logikai bomba, féreg, trójai vírus, rootkit. A *spyware-ek* (kémprogamok) és *ransomware-ek* (zsarolóvírusok) ehelyütt nem vonhatók ide. A malware-ek hatása is sokféle lehet, az informatikai rendszer működését azzal akadályozhatják, hogy például lassítják, leállítják a számítógépet, felülírhatják a tárolt vagy továbbított adatainkat, módosíthatják a programokat. A malware-rel fertőzés különböző módjai sajátos bűnösségi eseteket vetnek fel: offline feltöltés esetében a malware számítógépre telepítése bármely adathordozóról történhet. A malware-program önállóan vagy más programba (például egy játékprogramba) rejtve is telepíthető.

A feltöltőnek közvetlen fizikai kontaktusba kell kerülni a célzott számítógéppel. Ez történhet:

i) a helyiségbe történő jogellenes behatolással,
ii) a számítógépet meghackelve (elektronikus betörés révén),
iii) jogszerűen hozzáférve a számítógéphez.

Az i) pont esetében a magánlaksértés (Btk. 221. §) is szóba jöhet. Hivatali helyiségbe történő jogosulatlan bemenetel esetében a bejutáshoz szükséges rongálás (Btk. 371. §) is szóba jöhet. Ezekben az esetekben a valódi, anyagi, heterogén halmazat állapítható meg. Az ii) pontban írt eset a bűncselekmény (1) bekezdés *a)* pontját is kimeríti. Az azonos jogi tárgy a halmazati értékelést kizárja. Az iii) pont esetében az (1) bekezdés *b)* pont alkalmazható, mivel az akadályozás a jogosultság kereteit túllépő tevékenység. Ezzel szemben a számítógépes hálózaton terjesztett (megosztott) malware-ek esetében, azaz online feltöltés esetében nem szükséges közvetlen fizikai hozzáférés a számítógéphez:

- a célzott szervert meghackelve történhet a malware telepítése,
- célzott számítógép hiányában is az informatikai hálózaton keresztül, például illegális warezoldalakra, *peer to peer (P2P-)* kapcsolat révén torrent- vagy más hálózatra telepítve, különböző alkalmazásokba rejtve, e-mailben, VOIP-hez csatolt fájlban.

A célzott számítógép hiányában történő feltöltés jellemzője, hogy a sértettek száma előre nem látható (attól függ, hogy hányan töltik le és telepítik azokat). Az informatikai rendszer akadályozásának másik tipikus esete a program manipulálása, megváltoztatása, valamely elemének egészben történő átírása vagy annak részleges vagy teljes törlése, továbbá ezek kombinációja. Valamint idetartozik minden olyan utasítás felvitele is, amelynek révén meg nem engedett műveletek végezhetők, amelyekkel az informatikai rendszert akadályozni lehet (szabotálni). A sértetti közrehatás sajnos ebben az esetben is valós problémát jelent, főként, ha

- a felhasználó kétes helyről (például warez-, szexoldalról, P2P-hálózatról) tölt le, telepít egy fertőzött programot,
- ellenben nem telepít számítógépére malware-t felismerő és azt törlő programokat,
- illetve nem frissíti a számítógépén dolgozó programokat.

Óvatosan ugyan, de felvethető a felhasználó felelőssége, hogy megtesz-e mindent számítógépe védelmében? A kérdés komolysága abban áll, hogy nem vagy nem megfelelően védett számítógépe nagyon súlyos bűncselekmények (terheléses támadás, spamek milliós megosztása stb.) „résztvevője" lehet. Felelőtlen magatartása kárt okoz intézményének, szervezetének, saját magának, esetleg szolgáltatójának stb.

4.2.1.3. A bűncselekmény minősített esetei

Súlyosabban büntetendő, ha a kárt okozó támadás jelentős számú információs rendszert érint – akár a felhasználók mint sértettek nagy számában, akár úgy, hogy a felhasználók tudtukon és akaratukon kívüli aktív részesei egy jogsértésnek (például DoS vagy DDoS). A számítógép erőforrásai meggyengülhetnek (például a weboldal lassabban töltődik be, az audio- és videostreamek megszakadhatnak, az e-mail-küldés akadozik stb.). Bár ennek valójában a hálózat- vagy a weboldal szolgáltatójánál keletkezett probléma is oka lehet. Az egyre nagyobb sávszélesség (az adatátvitel gyorsabbá válása) miatt egyre kevésbé érzékelhető az, ha terheléses támadás részese a felhasználó.

A terheléses támadás célpontjai jellemzően nem az egyéni felhasználók számítógépei, hanem azok az informatikai rendszerek, amelyek vagy különösen védett rendszerek (kritikus infrastruktúra, honvédelem, pénzügyi szféra stb.), vagy azok az informatikai rendszerek, amelyeknek 24 órás működése szükségszerű (például energetikai vagy online-szerencsejáték-szerverek). A terheléses támadással történő zsarolás (Btk. 367. §) mint modern „védelmipénz-behajtás" már ismert a szakirodalomban.

Még súlyosabban bünteti a törvény azt az esetet, ha a támadás közérdekű üzem ellen irányul. A közérdekű üzem fogalmát a Btk. 459. § 21. pontja tartalmazza, ami szerint:

a) a közmű,
b) a közösségi közlekedési üzem,

c) az elektronikus hírközlő hálózat,
d) az egyetemes postai szolgáltató közérdekű feladatainak teljesítése érdekében üzemeltetett logisztikai, pénzforgalmi és informatikai központok és üzemek,
e) a hadianyagot, haditechnikai eszközt, energiát vagy üzemi felhasználásra szánt alapanyagot termelő üzem.

4.2.1.4. Büntetéskiszabási szempontok

Büntetéskiszabási szempontok között súlyosbítóként jöhet szóba az információs rendszer működéséért felelős személyek és számítástechnikai szakemberek büntetni rendelt ténykedései, hiszen ők szakmai ismeretük felhasználásával követték el a bűncselekményt.

4.2.2. Az információs rendszer védelmét biztosító technikai intézkedés kijátszása

„424. § (1) Aki a 375. vagy a 423. §-ban meghatározott bűncselekmény elkövetése céljából az ehhez szükséges vagy ezt könnyítő

a) jelszót vagy számítástechnikai programot készít, átad, hozzáférhetővé tesz, megszerez vagy forgalomba hoz, illetve

b) jelszó vagy számítástechnikai program készítésére vonatkozó gazdasági, műszaki, szervezési ismereteit más rendelkezésére bocsátja, vétség miatt két évig terjedő szabadságvesztéssel büntetendő.

(2) Nem büntethető az (1) bekezdés *a)* pontjában meghatározott bűncselekmény elkövetője, ha – mielőtt a bűncselekmény elkövetéséhez szükséges vagy ezt megkönnyítő jelszó vagy számítástechnikai program készítése a büntetőügyekben eljáró hatóság tudomására jutott volna – tevékenységét a hatóság előtt felfedi, az elkészített dolgot a hatóságnak átadja, és lehetővé teszi a készítésben részt vevő más személy kilétének megállapítását.

(3) E § alkalmazásában jelszó: az információs rendszerbe vagy annak egy részébe való belépést lehetővé tevő, számokból, betűkből, jelekből, biometrikus adatokból vagy ezek kombinációjából álló bármely azonosító."

A törvényi szabályozás szerint a 375. és a 423. szakaszokban szabályozott bűncselekmények elkövetése céljából büntetni rendeltek a technikai megoldások kijátszásához szükséges vagy azt könnyítő cselekmények.

A bűncselekmény *jogi tárgya* – a fentebb említett jogi tárgyaknak megfelelően – az elektronikus adatfeldolgozás és -átvitel integritása, biztonsága, amely magában foglalja a számítástechnikai rendszert és annak működését, valamint a feldolgozásra rendelt adatok mint elektronikus impulzusok biztonságát.

1. A bűncselekmény *elkövetési (tevékenységi) tárgya* az elektronikus adatfeldolgozó és adatátviteli rendszer védelmi-biztonsági megoldásainak kijátszására alkalmas program, belépési kód, jelszó vagy egyéb adat, amely a védett rendszerbe történő jogszerű belépést biztosítja [424. § (1) bekezdés *a)* pont].

- *Belépési kód:* a felhasználónév, amely a hozzárendelt jelszóval együtt teszi lehetővé a jogosult számára a belépést valamely hálózatba, számítógépbe.

- *Jelszó:* hálózat (internet, intra- és extranet), valamint adatállomány hozzáféréséhez szükséges azonosító kulcsszó. Általában jelszavak védik a BIOS-t, különböző operációs rendszerekben például a megosztott erőforrásokat, a szövegszerkesztő programokban a dokumentumokat.

A különböző hálózatok használatához alkalmaznak jelszavakat. Az operációs rendszereket, a levelezőprogramokat vagy más programokat, a védett könyvtárakat és fájlokat is különböző azonosítók, jelszavak védik, védhetik.[8] A bűncselekmény elkövetési (tevékenységi) magatartásai közé tartozik az (1) bekezdés *a)* pontjában írott büntetni rendelt tevékenység: valamely védett informatikai rendszerbe jogosulatlan belépést biztosító program, jelszó, belépési kód vagy adat, illetve más számítógépes program, amely az informatikai csaláshoz vagy az informatikai rendszer, az abban kezelt adatok ellen irányul.

- *Készítés:* számítógépes program írása, az adott infromatikai rendszer védelmére szolgáló jelszó generálása, a jelszó felülírása stb. A szerzői jogi törvény 58. § (2) bekezdése miniszteri indokolását alapul véve, a szoftver bármely elemének (forráskód, tárgyi program, kísérő anyag) készítése e szakasz alá vonható. De az *interface* (hardver-szoftver közti összeköttetést létrehozó utasítássorozat) készítése már kívül esik e körön.
- *Átadás:* az adott számítástechnikai rendszer vonatkozásában a program készítőjétől stb. különböző személynek a birtokba adása. Közömbös, hogy ez ingyenesen, visszterhesen, megtévesztéssel vagy más módon történt.
- *Hozzáférhetővé tétel:* a program, jelszó, adat eljuttatása egyéb módon, akár aktív, akár passzív magatartással (például többek által használt helyiségben, irodában, gépteremben a belépési kód, jelszó stb. asztalon, képernyőre ragasztott papírdarabon történő otthagyása).

Tipikus lehet például a warezoldalon történő közzététel, a P2P-hálózaton, chatszobában, fórumrovatban, elektronikus hirdetőtáblán való megosztás stb. Közömbös, hogy ingyenesen vagy ellenszolgáltatás fejében történik. Ne feledjük, hogy az ingyenes sem ingyenes, igen nagy valószínűséggel ezekben a programokban egy másik kártékony program is rejtőzik.

- *Megszerzés:* a jelszó, program birtokbavétele a program írójától, más személytől, letöltése az internetről. Közömbös, hogy ellenszolgáltatás fejében, megtévesztéssel vagy más módon. A megszerzés módja legfeljebb büntetéskiszabási szempontként értékelhető.
- *Forgalomba hozatal:* több, akár meg nem határozható számú személy számára hozzáférhetővé teszi e programot akár úgy, hogy saját maga juttatja el a felhasználóknak, akár úgy, hogy egyetlen személynek adja át, ám abban a tudatban, hogy az a személy több személynek adja tovább. Irreleváns, hogy ez ellenszolgáltatás fejében történt-e, vagy sem.

2. A (1) bekezdés *b)* pontja szerint büntetendő cselekmény, egyfajta *delictum sui generis* bűnsegédi tevékenység büntetni rendelt. A tényállás megfogalmazásában mindkét

[8] A tényállás másik fordulatának elkövetési (tevékenységi) tárgyai a fentebb részletezett malware-vírusok, lásd 424. § (1) bekezdés *b)* pont.

bűnsegélyi alakzat (fizikai és pszichikai bűnsegély) szerepel: 1. a számítástechnikai program, jelszó, belépési kód vagy valamely számítástechnikai rendszerbe való belépést lehetővé tevő adat készítésére vonatkozó gazdasági, műszaki, szervezési ismeret átadása másnak; 2. kódfeltörő program írásához, jelszógeneráláshoz, ezek megszerzéshez, forgalomba hozásához szükséges elméleti vagy gyakorlati ismereteket, programrészleteket másnak továbbad, kapcsolatrendszert megoszt. Nem tartozik ide a programok megnevezése, a program működésének, hatásmechanizmusának leírása.

A bűncselekmény elkövetője mindkét esetben bárki lehet. Közömbös a szakismeret, a tudás szintje. Büntetéskiszabási szempont lehet, és súlyosító körülményként jöhet szóba az, ha a vádlott számítástechnikai képesítéssel bír, vagy ilyen munkakörben dolgozik, számítástechnikai cég, szerviz dolgozója stb. Az elkövetési (tevékenységi) magatartások célzatosak, azaz a Btk. 375. §-a, illetőleg a Btk. 423. §-a végrehajtása céljából történik, így a bűnösség az egyenes szándékra *(dolus directus)* korlátozódik.

3. A (2) bekezdés szerint nem büntethető az, aki program-, jelszó-, adatkészítő tevékenységét a hatóság előtt felfedi, és az elkészített dolgot a hatóságnak átadja, valamint lehetővé teszi a készítésben részt vevő más személy kilétének megállapítását. A büntethetőséget megszüntető ok akkor jöhet szóba, ha a bűncselekmény elkövetéséhez szükséges vagy ezt megkönnyítő számítástechnikai programot, jelszót, belépési kódot vagy valamely számítástechnikai rendszer egészébe vagy egy részébe való belépést lehetővé tevő adatot az elkövető azelőtt hozza a hatóság tudomására, vagy adja át a hatóságnak stb., mielőtt a hatóságnak erről ismerete lett volna.

Az (1) bekezdésben megfogalmazott bűncselekmény az elkövetési magatartás tanúsításával (program írása, belépési kód, jelszó generálása, ennek megszerzése, forgalomba hozatala, kereskedés, hozzáférhetővé tétel) befejezett, nem szükséges, hogy a 375. §, illetőleg a 423. § bármelyike is akár csak kísérleti szakaszba jusson. A (2) bekezdés esetében a gazdasági, műszaki, szervezési ismeretek másnak történő rendelkezésre bocsátásával a bűncselekmény befejezetté válik. Nem szükséges, hogy ez a személy ezeket programok írására, belépési kódok, jelszavak generálására felhasználja. A bűncselekmény rendbelisége a veszélyeztetett elektronikus adatfeldolgozó- és átviteli rendszerek számához igazodik. *De ege ferenda:* mivel az informatikai rendszerbe történő bejutást követően többféle bűncselekmény követhető el – a jogosulatlan adatszerzéstől a *defacingen* keresztül a tiltott tartalom feltöltésének lehetőségéig –, így nincs indoka annak, hogy a Btk. 424. §-a csupán a 375. § és a 423. § megvalósításához kapcsolódik. A harmadik tényállás *az információs rendszer felhasználásával elkövetett csalás.* A tényállás megalkotása azt a szakmai vitát zárta le, hogy a sértetti kontroll nélküli megtévesztő adatbevitel, adatmanipuláció – amely kárt okoz a sértettnek – lehet-e csalás. Ezt a vitát zárta le először a 89/9. európai tanácsi ajánlásban megfogalmazottakkal szinte azonos módon, ennek ellenére egy évtizeden át tévesen közelítette meg a kérdést a hazai törvénykezés. A mostani tényállás dogmatikailag már sokkal helyesebb.

4.2.3. Információs rendszer felhasználásával elkövetett csalás

„375. §. (1) Aki jogtalan haszonszerzés végett információs rendszerbe adatot bevisz, az abban kezelt adatot megváltoztatja, törli vagy hozzáférhetetlenné teszi, illetve egyéb művelet végzésével az információs rendszer működését befolyásolja, és ezzel kárt okoz, bűntett miatt három évig terjedő szabadságvesztéssel büntetendő.

(2) A büntetés egy évtől öt évig terjedő szabadságvesztés, ha

a) az információs rendszer felhasználásával elkövetett csalás jelentős kárt okoz, vagy

b) a nagyobb kárt okozó, információs rendszer felhasználásával elkövetett csalást bűnszövetségben vagy üzletszerűen követik el.

(3) A büntetés két évtől nyolc évig terjedő szabadságvesztés, ha

a) az információs rendszer felhasználásával elkövetett csalás különösen nagy kárt okoz, vagy

b) a jelentős kárt okozó, információs rendszer felhasználásával elkövetett csalást bűnszövetségben vagy üzletszerűen követik el.

(4) A büntetés öt évtől tíz évig terjedő szabadságvesztés, ha

a) az információs rendszer felhasználásával elkövetett csalás különösen jelentős kárt okoz, vagy

b) a különösen nagy kárt okozó, információs rendszer felhasználásával elkövetett csalást bűnszövetségben vagy üzletszerűen követik el.

(5) Az (1)–(4) bekezdés szerint büntetendő, aki hamis, hamisított vagy jogosulatlanul megszerzett elektronikus készpénz-helyettesítő fizetési eszköz felhasználásával vagy az ilyen eszközzel történő fizetés elfogadásával okoz kárt.

(6) Az (5) bekezdés alkalmazásában a külföldön kibocsátott elektronikus készpénz-helyettesítő fizetési eszköz a belföldön kibocsátott készpénz-helyettesítő fizetési eszközzel azonos védelemben részesül."

A bűncselekmény eklektikusságának megfelelően több *jogi tárgyat* véd: egyfelől az informatikai rendszer integritását, biztonságos működését, másfelől – a célcselekmény irányultsága folytán – a vagyoni viszonyokat. A bűncselekmény *elkövetési (tevékenységi) tárgya* a számítógépes adat, amely mint elektronikus impulzus ehelyütt vagyoni értéket jelöl. A bűncselekmény *elkövetési (tevékenységi) magatartása* a jogtalan haszonszerzés végett a számítástechnikai rendszerbe történő elektronikus adat bevitele, az informatikai rendszerben kezelt adat megváltoztatása, teljes törlése vagy hozzáférhetetlenné tétele. A tényállás e része a haszonszerzés végett végrehajtott, azaz célzatos cselekményeket foglal magában. Megtévesztő (csalárd) adatbevitel történhet:

- a számítógép billentyűzetét használva (offline vagy online módban),
- külső adathordozóról történő feltöltés,
- áru vagy szolgáltatás rendelésekor, illetve azok kifizetésekor,
- ATM-en keresztül hamis, hamisított, valódi más nevére szóló bankkártyával történő készpénzfelvétel,
- ATM-en keresztül mobiltelefonegyenleg-feltöltés, különféle szolgáltatók (telekommunikációs, közüzemi stb.) számláinak befizetése, szerencsejátékokra történő befizetés, utasbiztosítás kötése, autópálya-matrica vásárlása és más, a továbbiakban várhatóan bővülő fizetési lehetőségek.

A tényállás *materiális,* azaz a törvényhozó az eredményt, vagyis kár bekövetkeztét határozza meg befejezett bűncselekményként. Mivel az első minősített eset a jelentős kár fogalmát jelöli meg, így az alapesetben a cselekmény akkor büntetendő, ha a kisebb és a nagyobb kár is bekövetkezik, azaz a kárérték ötvenezertől ötmillió forintig terjed. A további minősített esetek a következő értékhatárokhoz igazodnak: ötmillió-egy és ötvenmillió forint között jelentős, ötvenmillió-egy és ötszázmillió forint között különösen nagy, ötszázmillió forint felett különösen jelentős (Btk. 459. § 6. pont).

A minősített esetekben az értékhatár mellett más körülmények is relevanciával bírnak. Bűnszövetség 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 (Btk. 459. § 2. pont). Üzletszerűen követi el a bűncselekményt, aki ugyanolyan vagy hasonló jellegű bűncselekmények elkövetése révén rendszeres haszonszerzésre törekszik (459. § 28. pont).

4.3. Joghatósági problémák az interneten

A *világháló* mint virtuális tér már elnevezésében is jelzi azt a nehézséget, hogy megállapítsuk, egy-egy bűncselekmény hol és mikor válik befejezetté, vagy lép kísérleti szakba, illetőleg, ha a Btk. az előkészületet is büntetni rendeli, mikor és hol tekinthető előkészületnek. Dogmatikailag és a törvényi szabályozásban (Btk. 2–3. §) is egyszerű a válasz: ahol a bűncselekmény tényállási elemei közül akár egyetlen is megvalósul (például a billentyűzet leütése magyar IP-címet jelző számítógépen vagy akár magyar IP-címről, de proxy-szerveren keresztül történik a tiltott tartalomközlés vagy más bűncselekmény elkövetése, vagy a tényállásban szereplő vagyoni kár, más sérelem Magyarországon következik be). De megalapozza a joghatóságot az, ha magyar állampolgár külföldön valósít meg a magyar Btk. szerint üldözendő bűncselekményt, (akár egyetlen) tényállási elemet, vagy egy nem magyar állampolgár által külföldön történő tényállási elem megvalósítása is idetartozik, ha az a cselekmény a magyar törvény szerint bűncselekmény, és az elkövetés helye szerint is büntetendő a cselekmény; de más eseteket is szabályoz a hatályos Btk. Az informatikai bűncselekmények esetében a joghatóság markáns megjelenése nem mindig egyértelműen rögzíthető, mert

- a cselekmény több országban valósul meg (a billentyű leütése az egyik országban történt, a pénzt egy másik ország pénzintézetéből szerezték, az így ellopott pénzt további más országban, országokban bújtatták, majd mindezektől is különböző országban, országokban mosták tisztára, majd egy ismeretlen országban, országokban helyezték el bankbetétként vagy költötték el),
- több ország felhasználóit érinti (például a botnet esetében),
- az elkövetők különböző országokból szerveződnek – akár egy akcióra is –, az internet sötét világában tűnnek fel és el,
- külön problémát jelent a határokon, földrészeken átívelő, a feltöltött adatokat folyamatosan áramoltató *felhőszolgáltatás.*

Az Európai Unió Tanácsának 2009/948/IB számú, a joghatóság gyakorlásával kapcsolatos, büntetőeljárások során felmerülő összeütközések megelőzéséről és rendezéséről szóló keret-

határozata (2009. november 30.) törekszik e problémát feloldani. A joghatósági viták során a tagállamok közötti konszenzusra hívja fel az EU tagállamait (3–113. pont), illetőleg ennek sikertelensége esetén az Eurojusthoz történő fordulást javasolja (14. pont). A joghatósági összeütközés vitájának megoldására, a konszenzus megteremtéséhez az Eurojust 2003-as éves jelentésében megadott szempontok együttes értékelését javasolja az EU Tanácsa. Eszerint a tagállamok vegyék figyelembe

- azt a helyet, ahol a bűncselekmény legnagyobb részét elkövették,
- azt a helyet, ahol a kár vagy veszteség jelentős része keletkezett,
- a gyanúsított vagy vádlott tartózkodási helyét, valamint
- más joghatóságok számára történő átadásának vagy kiadatásának lehetőségeit,
- a gyanúsított vagy vádlott állampolgárságát vagy lakóhelyét,
- a gyanúsított vagy vádlott jelentős érdekeit,
- a sértettek és tanúk jelentős érdekeit,
- a bizonyítékok elfogadhatóságát vagy
- az esetlegesen előforduló késedelmeket.

A felsorolt tényezők egyben sorrendet mutatnak az értékelésben. E körülmények elméletileg megalapozhatják Magyarország joghatóságát.[9] Azonban lehetőség van a büntető joghatóságról – célszerűségi okok miatt – való lemondásra. A büntetőeljárás *átadható,* ha

a) a Magyarországon tartózkodó terhelt annak az államnak az állampolgára, amelynek részére az eljárás átadása történik, vagy abban az államban van az állandó lakóhelye, illetve szokásos tartózkodási helye,
b) a terhelt az eljárás során külföldön tartózkodik, kiadatásának, illetve átadásának nincs helye, kiadatását, illetve átadását megtagadták, vagy kiadatási kérelem előterjesztésére nem kerül sor. A virtuális térben elkövetett bűncselekmények esetében gyakori, hogy a terhelt nem magyar állampolgár, akivel szemben a lefolytatandó büntetőeljárásról célszerű lemondani.

A büntetőeljárás átadására sor kerülhet – a jogerős határozat meghozataláig – az eljárás bármely szakaszában. A hazai jogi szabályozás szerint a büntetőeljárás átadásáról a vádemelésig a legfőbb ügyész, azt követően az igazságügyi és rendészeti miniszter dönt. Külföldi államban folyó büntetőeljárás e hatóság megkeresésére akkor vehető át, ha a terhelt magyar állampolgár vagy Magyarországra bevándorolt nem magyar állampolgár. A büntetőeljárás átvételéről a legfőbb ügyész dönt."[10]

4.4. A kiberbűncselekmények nyomozásának sajátosságai

A nyomozati teendők általában:

- A bűncselekmény alapjául szolgáló, inkriminált adatállomány felkutatása, megismerése, rögzítése.
- A naplózott és a regisztrációs adatok beszerzése a szolgáltatóktól.

[9] Btk. 2–3. §.
[10] 8002/2008 IRM tájékoztató.

- Az informatikai rendszerben fellelhető egyéb elektronikus nyomok, bizonyítékok kutatása, rögzítése.
- Valós térbeli nyomozati munka az ez idáig összegyűjtött bizonyítékok alapján gyanúsítható elkövetőkkel szemben.

A bizonyítékok összegyűjtése a bűncselekmény jellegétől függ. A bizonyítékoknak több lehetséges forrása is lehet.

Kézenfekvő a nyílt forrásból elérhető bizonyítékok felkutatása, rögzítése (OSINT), ezen túlmenően, ha szükséges, jogsegély alapján más nyomozati munkák eredményes elősegítéséhez is használható

- az 1996. évi XXXVIII. törvény a nemzetközi bűnügyi jogsegélyről,
- a 2000-ben aláírt uniós kölcsönös jogsegélyi egyezmény,
- az ez alapján született 2012. évi CLXXX. törvény az Európai Unió tagállamaival folytatott bűnügyi együttműködésről,
- olyan bilaterális vagy multilaterális szerződés, amelynek Magyarország részese,
- a budapesti egyezmény mint multilaterális egyezmény, amely szerint a nyomozáshoz szükséges segítségnyújtás nemzetközi szerződés hiányában (27. cikk) is történhet,
- továbbá előzetes megkeresés nélkül is segítség nyújtható egy másik államban zajló nyomozáshoz (26. cikk); a segítségnyújtásra rövid úton (e-mail, fax) is lehetőséget teremt az egyezmény (25. cikk 3. pont).

4.5. A közvetítő szolgáltatók típusai, felelőssége

A közvetítő szolgáltatók az információs társadalommal összefüggő szolgáltatást nyújtják:

- hozzáférést biztosító szolgáltatók,
- tárhelyszolgáltatók,
- keresőszolgáltatók,
- gyorsítótár-szolgáltatók,
- tartalomszolgáltatók,
- alkalmazásszolgáltatók.

Az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről szóló 2001. évi CVIII. törvény nem is mindegyiket nevesíti.[11]

1. *A hozzáférést biztosító szolgáltatók (accesss provider)* az internet elérését biztosítják a felhasználók számára. Ma már a legtöbb hozzáférést biztosító szolgáltató nemcsak hozzáférést biztosít, hanem további szolgáltatásokat is nyújt. E-mail fiókot működtet, tárhelyet biztosít, tartalomszolgáltatást nyújt: híreket és más tartalmakat közölnek, saját és mások szolgáltatásait hirdetik, üzletkötési, előfizetési és más lehetőségeket biztosítanak a weboldalukat felkeresőknek.

[11] 2001. évi CVIII. törvény az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről.

2. *A tárhelyszolgáltatók* számítógépük, szervereik részleges vagy teljes területét bocsátják rendelkezésére ingyenesen vagy díj fizetése fejében olyan felhasználóknak, akik adataikat, tartalmaikat feltölthetik a tárhelyszolgáltató által biztosított területre. Ismert az osztott tárhelyszolgáltatás is, amikor egy fizikai szerveren, azonos IP-címen több weboldal is elérhető.
3. A *keresőszolgáltatók* (röviden: *search engines*) fő funkciója az internetre feltöltött óriási információtömeg tematikus elérésének biztosítása. A keresőszolgáltatók általában a *surface webet* érik el, a *deep webnek* saját szolgáltatója van. A keresőszolgáltatók további jellemző alkalmazásai a tartalomszolgáltatás, az e-mail-fiók biztosítása, nem ritkán a profilkövető reklámok szolgáltatása (számukra bevételként).
4. *A gyorsítótároló (cache-tároló)* elősegíti az elérni kívánt információ gyorsabb hozzáférését, átmeneti tárolását. Tipikus a böngészőprogramok korábbi eredményeinek tárolása.
5. *Internetes tartalmat nyújtó szolgáltatók (content providers).* A tartalomszolgáltatók információkat, azaz tartalmat töltenek fel az internetre (weboldalaikra), amelyeket az internetes szolgáltatást nyújtó szolgáltató kiszolgálóin (szerverein) helyezik el. A tartalomszolgáltatók szintén többféle lehetőséget nyújtanak, tárhelyet biztosítanak, üzletkötés, előfizetés lehetősége, e-mail-fiók biztosítása is gyakori eleme ezeknek a weboldalaknak.
6. *Az alkalmazásszolgáltatók (current providers)* lehetővé teszik a felhasználók számára, hogy az ahhoz szükséges eszközök megvásárlása nélkül, bérleti vagy eseti díj ellenében vegyenek igénybe információs és feldolgozási szolgáltatásokat (Facebook, Twitter, Yahoo stb.)

Az információs társadalommal összefüggő szolgáltatás megkezdéséhez, folytatásához általában előzetes engedély vagy hatósági határozat nem szükséges. Korlátozás csak a törvényben meghatározott okokból lehetséges:

- a közrend védelme, különösen a bűncselekmények megelőzése, nyomozása, felderítése és üldözése érdekében,
- ideértve a kiskorúak védelmét és a faji, nemi, vallási vagy nemzeti alapú bármilyen gyűlöletre uszítás és az egyének emberi méltóságának megsértése elleni fellépést,
- a közegészség védelme érdekében,
- a közbiztonság érdekében – ideértve a nemzetbiztonsági és honvédelmi érdekeket is,
- a fogyasztók vagy a befektetők érdekei védelmére; és ha a hatósági intézkedés
  a) a fentiekben említett érdekeket sértő vagy súlyosan veszélyeztető szolgáltatás ellen irányul; és
  b) az érdeksérelemmel, illetve a veszélyeztetéssel arányos (az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről szóló 2001. évi CVIII. törvény 3–3/A. § [Ekertv.]).

A törvény külön kiemeli a gyermekek védelme érdekében teendő intézkedéseket is. Olyan információ esetén, amely súlyosan károsíthatja a kiskorúak szellemi, lelki, erkölcsi vagy fizikai fejlődését, különösen azáltal, hogy meghatározó eleme az erőszak, illetve a szexualitás közvetlen, naturális ábrázolása, az adott aloldalt az információ megjelenítése előtt egy figyelmeztető jelzéssel kell ellátni, amely arról tájékoztat, hogy ez az információ

veszélyeztetheti a kiskorúakat. Továbbá az aloldal forráskódjában szereplő olyan azonosítókkal tehető csak közzé az ilyen információ, amelyek utalnak a tartalom kategóriájára, és amelyek szűrőszoftver által felismerhetők (Ekertv. 4/A. §). A *szolgáltatók felelősségéről* az Ekertv. az alábbiak szerint rendelkezik:

1. A *hozzáférést biztosító szolgáltató,* valamint az *alkalmazásszolgáltató* akkor nem felel a továbbított információért, ha
   a) nem a szolgáltató kezdeményezi az információ továbbítását;
   b) nem a szolgáltató választja meg a továbbítás címzettjét, és
   c) a továbbított információt nem a szolgáltató választja ki, illetve azt nem változtatja meg.
2. A *gyorsítótároló szolgáltatója* akkor nem felel az információ közbenső és átmeneti jellegű automatikus tárolásával okozott kárért, ha
   a) a szolgáltató nem változtatja meg az információt;
   b) a tárolt információhoz való hozzáférés megfelel az információ hozzáférésével kapcsolatban támasztott feltételeknek;
   c) a közbenső tárolóban az információ frissítése megfelel a széleskörűen elismert és alkalmazott információfrissítési gyakorlatnak;
   d) a közbenső tárolás nem zavarja meg az információ felhasználásával kapcsolatos adatok kinyerésére szolgáló, széleskörűen elismert és alkalmazott technológia jogszerű használatát; és
   e) a szolgáltató haladéktalanul eltávolítja az általa tárolt információt vagy nem biztosítja az ahhoz való hozzáférést, amint tudomást szerzett arról, hogy az információt az adatátvitel eredeti kiindulási pontján a hálózatról eltávolították, vagy az ahhoz való hozzáférés biztosítását megszüntették, illetve, hogy a bíróság vagy más hatóság az eltávolítást vagy a hozzáférés megtiltását elrendelte.
3. A *tárhely- és az alkalmazásszolgáltató* nem felel szolgáltatásáért, ha nincs tudomása az információval kapcsolatos jogellenes magatartásról vagy arról, hogy az információ bárkinek a jogát vagy jogos érdekét sérti. Amint a fentiekről tudomást szerzett, haladéktalanul intézkednie kell az információ eltávolításáról, vagy a hozzáférést meg kell tagadnia.
4. A *keresőszolgáltató* nem felel az információ hozzáférhetővé tételével okozott kárért, ha nincs tudomása az információval kapcsolatos jogellenes magatartásról vagy arról, hogy az információ bárkinek a jogát vagy jogos érdekét sérti.

Amint a 3–4. pontban írt szolgáltató tudomást szerzett a fenti tiltott cselekményekről, haladéktalanul intézkedik az információ eltávolításáról vagy a hozzáférés megtiltásáról. Ellenben a szolgáltató nem mentesül a felelősség alól, ha az igénybe vevő a szolgáltató megbízásából vagy utasításai alapján cselekszik (Ekertv. 7–12. §). Ha a bíróság az elektronikus adat ideiglenes hozzáférhetetlenné tételét rendelte el egy tárhelyszolgáltatónál, akkor a bíróság ítéletének egy napon belül eleget kell tenni. Ennek nem teljesítése rendbírság kiszabását vonja maga után (Ekertv. 12/A. §). Az EU e-kereskedelmi irányelve bevezette a *notice and take down (értesítés és levétel)* intézményét, amelyet az Ekertv. az alábbiak szerint emelt be a belső jogba: a felhasználó az őt sértő tartalomközlésről értesíti a közvetítő szolgáltatót, amely az értesítés kézhezvételét követő tizenkettő órán belül köteles az értesítésben megjelölt információt eltávolítani és feltüntetni, hogy az eltávolítás a jogosult

jogsértést állító értesítése alapján történt. Egyben három napon belül köteles értesíteni azt az igénybe vevő felhasználót, aki a tartalmat közzétette, hogy a feltételezett jogsértés miatti eltávolítás ellen kifogással élhet, tudniillik az általa közzétett tartalom mégsem volt jogsértő. Amennyiben az eltávolított tartalom közlője 8 napon belül teljes bizonyító erejű magánokiratba vagy közokiratba foglalt indokolt kifogással él az eltávolítás ellen, abban az esetben a közvetítő szolgáltató mérlegelés nélkül köteles az érintett információt újra hozzáférhetővé tenni, és erről a jogosultat a kifogás megküldésével értesíteni (Ekertv. 13. §). A jogosult egyébként a kifogás miatt újra közzétett információ vonatkozásában az igényét – többek között – a jogsértés abbahagyására és az eltiltás iránt ideiglenes intézkedés iránti kérelmet tartalmazó kereset vagy fizetési meghagyás útján érvényesítheti, vagy büntetőfeljelentést tehet. Ez utóbbi esetben a nyomozó hatóságnak felvilágosítási kötelezettsége van, ha magánindítványra büntetendő bűncselekményről van szó. Interneten történő tartalomközlés esetén jellemzően a magánindítványos személyiségi jogokat sértő bűncselekmények jöhetnek szóba (Btk. 211–228. §), kivéve, ha a becsületsértés sértettje rendvédelmi dolgozó. Ha egy szolgáltató – ahogy a fentiekben láttuk – többféle szolgáltatást nyújt, akár ugyanazon a szerveren/weboldalon (például tartalmat közöl és tárhelyként kívülállók kommentárjának is helyt ad), akkor felelőssége is eszerint alakul, azaz a tartalomközlésért felel (hiszen általa írt, szerkesztett tartalmat jelenített meg); míg a tárhelyszolgáltatás esetében (mivel a tartalmat közlő egy kívülálló személy, aki természetesen felelősséggel tartozik megnyilvánulásaiért) a *notice and take down* szabályai szerint kell eljárnia. A tartalommal érintett természetes vagy jogi személytől vagy jogi személyiséggel nem rendelkező személytől függ annak megítélése, hogy a róla közölt tartalom sértő-e vagy sem. Nyilvánvaló bűncselekmény elkövetése esetén a tartalomszolgáltató felelhet a tárhelyén egy kívülálló felhasználó által elhelyezett tartalomért, de a bejegyzés, vélemény jogi megítélését nem lehet a tartalomszolgáltatón számon kérni, különösen, ha az csupán véleménynyilvánítás.

4.6. A felhőszolgáltatás büntetőjogi problémája

A felhőszolgáltatás *(cloud computing)* napjaink olyan új technikai megoldása, amely tehermentesíti a felhasználót attól, hogy nagytömegű adatot tároljon, illetve különböző programokat kelljen telepítenie a számítógépére. A *cloud computing* első hulláma internetes levelezőszerverek (Gmail, Yahoo), közösségimédia-alkalmazások (Facebook, Twitter) és online alkalmazások (Wikinews, blogok, Google Docs) használatával kezdődött. A szerverek számos személyes adatot is tárolhatnak (például bankkártyaszámokat, egy e-mail-kliens címeit, kártyatársaságok adatait). De a felhasználó által előállított információk is (szövegek, képek) kerülhetnek ilyen tárhelyekre (például Dropbox, Evernote). E technikai megoldás következménye, hogy a bűnözés is átterjed a felhőre (2012, *Operation High Roller:* csalás olyan malware segítségével, amely kiiktatta a PIN-es és chipes azonosításokat).

A felhőszolgáltatások típusai:

- szoftverszolgáltatás: a webböngészőn keresztül érhetők el különböző szoftverek,
- platformszolgáltatás: az alkalmazás üzemeltetéséhez szükséges környezetet biztosítja terheléselosztással, frissítéssel,
- infrastruktúraszolgáltatás: virtuális hardver szolgáltatása, tárhely, számítási stb. kapacitás szolgáltatása.

A szolgáltatás számtalan előnnyel kecsegtet. Lehetővé teszi azt, hogy a felhasználók az adataikhoz, programokhoz, egyéb feladatok végrehajtásához a világ bármely pontjáról hozzáférhetnek. A felhasználó adatai nem vesznek el. Itt a jogtiszta programok legfrissebb verziói találhatók meg, amelyek garantáltan vírusmentesek, a szolgáltatás gyors és biztonságos. A felhasználó több platformot tud egyesíteni munkája végzéséhez (például a munkahelyén, utazása során és másutt a saját számítógépén, laptopján, mobiltelefonján keletkező, előállított adatokat együtt tárolja, dolgozik azokkal). A technikai részletek kíméletes említése nélkül nem érthetjük meg a jogi problémákat. A szolgáltatók több szerveren, más eszközön tárolják az adatokat, programokat. A szerverek lehetnek ugyanazon vagy különböző országokban, távoli szigeteken. Ez utóbbi a jellemző. Közöttük az adatkapcsolat élő, hiszen az adatok folyamatos biztonsági mentése a felhőszolgáltató feladata, kötelessége. Az adatokat a felhőszolgáltató titkosítja, a felhasználókon kívül más nem ismerheti meg. Kérdés, hogy a felhőben (egy ismeretlen helyen levő szerveren, illetve a szerverek között mozgásban) levő inkriminált adatállomány (például egy tiltott tartalom) és annak előállítója, közösségi oldalon közlője, blogoldalra feltöltője stb.) hogyan válhat egy büntető- vagy más eljárás alanyává, illetve bizonyítékká. A nyomozás nehézségei általában a felhőszolgáltatás vagy egy külföldön található szerver (tárhely) esetében a következők:

- különbözők a szolgáltatók, különböző a szerverek földrajzi elhelyezkedése, különböző joghatóságok alá tartoznak,
- sem a fizikai eszköz, sem az elektronikus adat nem alapozhatja meg a joghatóságot,
- a különböző országban (földrészen) levő szervereken az inkriminált adatállomány szétszórva is lehet, amit csak a *cloud service provider* képes összegyűjteni,
- a szolgáltató a székhelye szerinti jogi szabályokat alkalmazza (például közösségi oldalakon, *social networks* vonatkozásában; szigorúbb lehet az adatvédelem, tágabb lehet a véleménynyilvánítás szabadsága stb.),
- minél nagyobb földrajzi területen szolgáltat (a felhőszolgáltató, közösségi oldalak, kereskedelmi oldalak), annál több megkeresés érkezhet a szolgáltatóhoz, amely miatt a megkeresett szolgáltató szelektál.

A felhőszolgáltatók, a közösségi oldalak üzemeltetői, a kereskedelmi szolgáltatások együttműködési hajlandóságától függ, hogy az adott ügyben a magyar hatóságok megkeresésére válaszolnak-e vagy sem. Ugyanakkor, ha a szolgáltató nem adja át a kért információkat, akkor esetleg a koronabizonyítékokat vagy az azokat előállító személyek megismerését ez rendkívül megnehezíti. Mondhatnánk, hogy az eljáró hatóság keressen más bizonyítékot a cselekmény bizonyításához, de egy tartalomközlést a tartalom egészével, az azt feltöltő személyt annak adataival lehetséges bizonyítani. Manapság a terrorizmussal, emberöléssel, kábítószerrel kapcsolatos bűncselekményekkel, pénzmosással és más nagyon súlyos bűncselekménnyel összefüggésben történő megkeresés kecsegtet sikerrel. A polgárjogi felelősség kérdése is valós, például az elvesztett adatállományért vagy szolgáltatás igénybevételének elmaradásáért való civiljogi felelősség. Kívánatos volna a nemzetközi együttműködés megteremtése, a magánkézben levő szolgáltatók (és profitérdekeik), valamint az igazságszolgáltatás érdekei közötti egyensúlyt megtalálni.

5. Kibervédelem és biztonság

Kovács Zoltán

A kibervédelemmel foglalkozó szervezetek fontos feladatot látnak el a kibertérben vagy az annak segítségével elkövetett bűncselekmények elleni küzdelemben is. Egyrészt azért, mert azon támadók között, akik ellen küzdenek, megtalálható – a kevés tudással rendelkező személyektől a kiberbűnözőkön át egészen az államilag támogatott hackercsoportokig – a kibertérben illegális tevékenységet folytatók teljes palettája. A kibervédelmi szervek által végzett tevékenység azonban jelentősen akadályozza, adott esetben meg is akadályozza az említett támadókat céljaik elérésében. Másrészt pedig azért, mert ezek a szervezetek az általuk elérhető információk megosztásával és kapcsolatrendszerük segítségével hathatósan tudják támogatni akár a nyomozásokat, akár a szükséges intézkedések (például egy külföldi, káros tevékenységet folytató szerver lekapcsoltatása) végrehajtását.

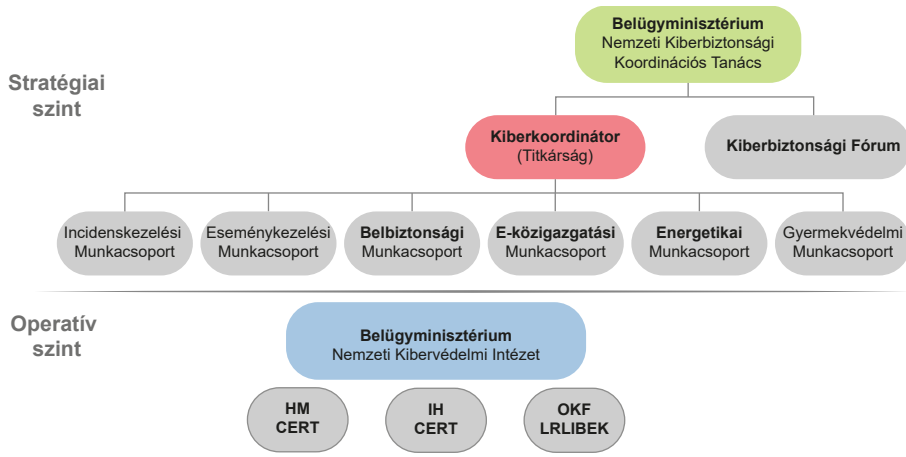
5.1. A hazai kibervédelemi szervezetek

Az elmúlt években kialakult a hazai kiberbiztonságért felelős szervezeti rendszer, amely alapvetően két szintre bontható: stratégiaira és operatívra. A stratégiai szinten a Kiberbiztonsági Fórum, a kiberkoordinátor, valamint az általa vezetett munkacsoportok találhatók, míg az operatív szintet – több esetben hatósági funkciókkal is kiegészülve – a Nemzetbiztonsági Szakszolgálat keretein belül működő Nemzeti Kibervédelmi Intézet (NKI), az Országos Katasztrófavédelmi Főigazgatóság szervezetében található Létfontosságú Rendszerek és Létesítmények Informatikai Biztonsági Eseménykezelő Központ (LRLIBEK), a Honvédelmi Minisztérium és az Információs Hivatal saját hálózatbiztonsági vészhelyzeteket elhárító csoportjai (*Computer Emergency Response Team,* a továbbiakban: CERT[1]) alkotják. Ezt mutatja be az 1. ábra.

Ezt a struktúrát egészítik ki azok a szintén operatív tevékenységet ellátó szervezetek (NISZ Zrt. kibervédelmi szervezeti egysége, Hun-CERT, KIFÜ CSIRT), amelyek vagy speciális kibervédelmi részfeladatokat látnak el az állami, önkormányzati rendszerekben, vagy nem az állami, önkormányzati rendszerek területén fejtik ki kibervédelmi tevékenységüket. Ezen szervezetekről a későbbiekben még esik szó.

---

[1] Az Amerikai Egyesült Államokban működő US-CERT feloldásaként a United States Computer Emergency Readiness Teamet használják.



1. ábra

A hazai kibervédelmi struktúra 2015. július 16. után

Forrás: saját szerkesztés TIKOS 2017 alapján

5.1.1. A hazai kibervédelem stratégiai szintje

A hazai kibervédelmi struktúra szervezeti, funkcionális és hatásmechanizmusait a 2. ábrán láthatjuk.

2. ábra

A magyarországi kibervédelmi struktúra szervezeti, funkcionális és hatásmechanizmusai

Forrás: saját szerkesztés RAJNAI 2016 alapján

5.1.1.1. Nemzeti Kiberbiztonsági Koordinációs Tanács

A Nemzeti Kiberbiztonsági Koordinációs Tanács (a továbbiakban: Tanács) feladatait a Nemzeti Kiberbiztonsági Koordinációs Tanács, valamint a Kiberbiztonsági Fórum és a kiberbiztonsági ágazati munkacsoportok létrehozásával, működtetésével kapcsolatos szabályokról, feladat- és hatáskörükről szóló 484/2013. (XII. 17.) Korm. rendelet[2] határozza meg. E szerint a Tanács feladata, hogy elősegítse a kormányzati tevékenységek koordinációját a Magyarország Nemzeti Kiberbiztonsági Stratégiájában meghatározott cselekvési területeken, valamint azokon figyelemmel kísérje az egyes feladatok végrehajtását. Ennek érdekében a meghatározott cselekvési területekhez társított kormányzati intézkedések alapján a Tanácsnak a kiberbiztonsági munkacsoportok, valamint a kiberkoordinátor irányításával és a Fórum javaslatainak figyelembevételével el kell készítenie és évente felül kell vizsgálnia az úgynevezett Nemzeti Kiberbiztonsági Akciótervet.

5.1.1.2. A kiberkoordinátor

A kiberkoordinátor feladatait szintén a 484/2013. (XII. 17.) Korm. rendelet tartalmazza. E szerint a kiberkoordinátor látja el

- a Kiberbiztonsági Fórum munkájának szakmai koordinálását;
- az állami szerveknek a kiberbiztonsági munkacsoportok munkájában való részvételre történő felkérését, ahol a delegált közszolgálati tisztviselő tagok mellett ő maga is részt vesz azok munkájában;
- a Tanács, a Fórum és a kiberbiztonsági munkacsoportok működtetésével kapcsolatos adminisztratív teendők irányítását;
- a kiberbiztonsági munkacsoportok és a kiberkoordinátor irányításával a Nemzeti Kiberbiztonsági Akcióterv elkészítését;
- a Tanács üléseinek összehívását;
- a Tanács elnökének irányításával a Tanáccsal kapcsolatos kommunikációs feladatok ellátását és felügyeletét.

A kiberkoordinátor szakértői támogatását az e-közigazgatásért felelős miniszter által vezetett minisztériumban működő titkárság látja el.

5.1.1.3. Kiberbiztonsági Fórum

A Kiberbiztonsági Fórum (a továbbiakban: Fórum) a stratégiából adódóan fontos szerepet tölt be a hazai kibervédelmi szervezetrendszerben. Fő feladata a Tanács munkájának segítése, elsősorban a nem kormányzati szervezetek (*non-governmental organization,* a továbbiakban: NGO) és más szakmai tömörülések, mint például a Szövetség a Digitális Gazdaságért Informatikai, Távközlési és Elektronikai Vállalkozások Szövetsége (a továbbiakban: IVSZ), Neumann János Számítógép-tudományi Társaság (a továbbiakban: NJSZT) és egyéb

[2] 484/2013. (XII. 17.) Korm. rendelet a Nemzeti Kiberbiztonsági Koordinációs Tanács, valamint a Kiberbiztonsági Fórum és a kiberbiztonsági ágazati munkacsoportok létrehozásával, működtetésével kapcsolatos szabályokról, feladat- és hatáskörükről.

mértékadó szolgáltatók (például a Magyar Telekom Csoport) alkotják. A Fórum elsősorban a jogszabályalkotás szakmai támogatását biztosítja, de képes elősegíteni, motiválni a Tanács által igényelt szolgáltatások megvalósulását is.

5.1.1.4. Kiberbiztonsági munkacsoportok

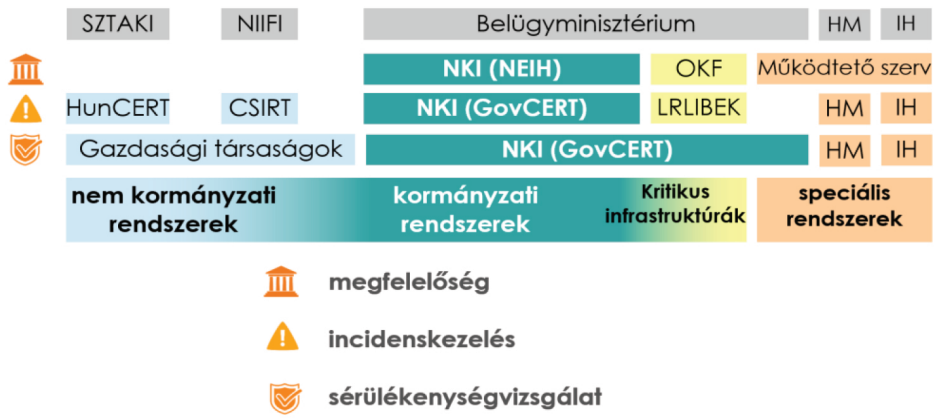
A 484/2013. (XII. 17.) Korm. rendeletben meghatározottak szerint ágazati és funkcionális kiberbiztonsági munkacsoportok segítik a Tanács koordinációs tevékenységét és döntéseinek végrehajtását. A jogszabály az alábbi olyan szakterületeket nevesíti, amelyeken kiberbiztonsági munkacsoportoknak kell működniük:

a) eseménykezelés,
b) belbiztonság,
c) e-közigazgatás,
d) energetika,
e) gyermekvédelem.

A Tanács felkérésére a fentieken kívül további munkacsoportok is létrehozhatók. Az 1. ábrán látható Incidenskezelési Munkacsoportot a 484/2013. (XII. 17.) Korm. rendelet nem nevesíti. Rajnai Zoltán kiberkoordinátorrá történő kinevezése után 2016-ban összesen hat munkacsoport alakult meg (vagy újjá). Ezek a Belbiztonsági Munkacsoport, az E-közigazgatási Munkacsoport, az Energiabiztonsági Munkacsoport, a Gyermekvédelmi Munkacsoport, az Egészségügyi Munkacsoport, valamint a Pénzügyi Munkacsoport (RAJNAI 2016). Jelenleg a 484/2013. (XII. 17.) Korm. rendeletben nevesített területekből a belbiztonsági és a gyermekvédelmi munkacsoportok működnek aktívan, ám a Belbiztonsági Munkacsoport ellátja az e-közigazgatási területen jelentkező feladatokat is. A Gyermekvédelmi Munkacsoport a Nemzetközi Gyermekmentő Szolgálat bázisán alakult meg, ez jelenleg a legintenzívebben működő munkacsoport. Tevékenységei között szerepel a szülőfelügyeleti programok támogatása, a gyermekbűnözés elleni fellépés elősegítése, de a munkacsoport aktívan részt vesz a digitális gyermekvédelmi stratégia megvalósításában is. A fent említettek mellett a bankbiztonsági, az egészségügyi munkacsoportokat sikerült aktívvá tenni. Ennek mozgatórugója elsősorban az volt, hogy ezt a két szektort érintették talán a legérzékenyebben az elmúlt időszak kibertámadásai (ilyen volt az egészségügyi szektort 2017-ben jelentősen érintő *WannaCry* zsarolóvírusos támadás (PALMER 2017) vagy a bankszektort megrázó, a SWIFT-rendszer sérülékenységét kihasználó támadássorozat (ANANTHALAKSHMI–BERGIN 2018; PAUL 2016). A Bankbiztonsági Munkacsoport a Bankszövetség információbiztonsági munkacsoportjának bázisán jött létre, fő feladata a bankszektor biztonságának erősítése, az állampolgárok e-banki tevékenysége biztonságának szavatolása. A 484/2013. (XII. 17.) Korm. rendeletben nevesített területek közül az energetika és az eseménykezelési szakterületen 2018. első félévének végéig még nem sikerült aktívan működő munkacsoportot kialakítani. Az e szektorokban felmerülő eseménykezelési problémákat, feladatokat az operatív szinten működő szervezetek kezelik.

5.1.2. A hazai kibervédelem operatív szintje

A hazai kibervédelem operatív szintjét mutatja be az alábbi 3. ábra. Az ábra jól szemlélteti, hogy megfelelőség, incidenskezelés és sérülékenységvizsgálat tekintetében mely szervezetnek milyen hatáskörrel milyen feladatai vannak, kiegészítve a civil szervezetek által működtetett CERT-ek feladataival.



3. ábra

Kibervédelmi feladatok a hazai struktúra operatív szintjén

Forrás: Bencsik 2017

5.1.2.1. Nemzeti Kibervédelmi Intézet

Az operatív szervezetek közül kiemelést érdemel a központi, vezető szerepet játszó Nemzeti Kibervédelmi Intézet. Az NKI 2015. október 1-jén alakult meg a Nemzetbiztonsági Szakszolgálat (a továbbiakban: NBSZ) bázisán, egységes szakmai keretbe foglalva a már ekkor az NBSZ alatt működő GovCERT-et, a 2015. január elsejétől már a Belügyminisztérium (a továbbiakban: BM) szervezeti keretében működő Nemzeti Elektronikus Információbiztonsági Hatóságot és az ezt megelőzően a Nemzeti Biztonsági Felügyelet (a továbbiakban: NBF) alatt tevékenykedő és szakhatósági, valamint sérülékenységvizsgálati feladatokat ellátó E-biztonsági Intelligencia Központot (NBF-CDMA).[3] Így egy egységes, koordináltabb, hatékonyabb feladat-végrehajtást és információáramlást lehetővé tevő kibervédelmi szervezetet sikerült létrehozni. Az NKI szervezetén belül három szakmai terület került kialakításra:

- a Kormányzati Eseménykezelő Központ (GovCERT-Hungary, a továbbiakban: GovCERT), amely a kibertérből érkező támadásokkal és fenyegetettségekkel foglalkozó incidenskezelési szakterület;
- a Nemzeti Elektronikus Információbiztonsági Hatóság (a továbbiakban: NEIH), amely a jogszabályi előírások ellenőrzésével és érvényesítésével foglalkozó hatósági szakterület;

[3] CDMA: Cyber Defence Management Authority.

- a Biztonságirányítási és Sérülékenységvizsgálati Osztály, amely az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény (a továbbiakban: Ibtv.) hatálya alá tartozó szervezetek esetében a kibervédelmi képességek fejlesztését és üzemeltetését támogatja, valamint ellátja az EMIR- és a FAIR-rendszerek elektronikus információbiztonsági feladatait is.[4]

Az NKI felépítését mutatja a 4. ábra. Az NKI szervezeti egységeinek fő feladatai viszont az 5. ábrán láthatók.

4. ábra

Az NKI szervezeti egységei

Forrás: Bencsik 2017

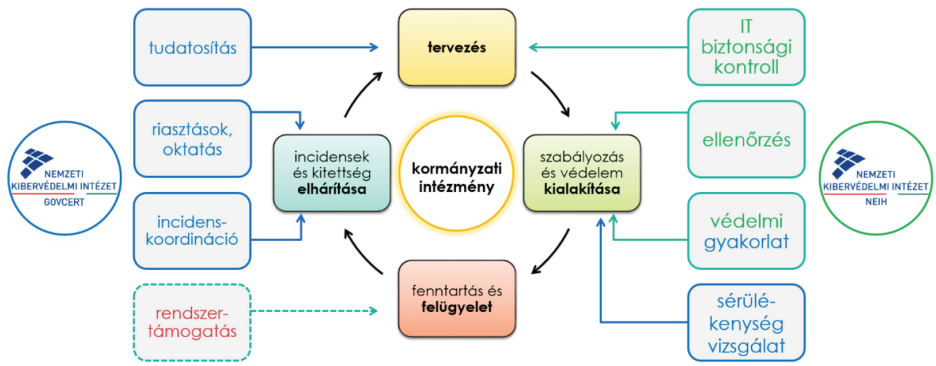
5. ábra

Az NKI szervezeti egységei és fő feladataik

Forrás: Tikos 2017

[4] Nemzetbiztonsági Szakszolgálat. Elérhető: http://nbsz.hu/?mid=42 (A letöltés dátuma: 2018. 06. 03.)

Az NKI így az egyes elektronikus információs rendszerek minden életciklusában rendelkezik valamilyen ellátandó információbiztonsági feladattal. Az egyes életciklusokban jelentkező feladatokat mutatja be a következő ábra.



6. ábra

A GovCERT- és NEIH-feladatok az elektronikus információs rendszerek életciklusában

Forrás: Bencsik 2017

Az NKI egyik kiemelendő feladata a nemzetközi kiberbiztonsági szervezetekkel való kapcsolattartás, az ezekkel való információmegosztás, az innen érkező információk eljuttatása az érintett hazai szervezetek számára, valamint a hazai szervezetek képviselete. Ennek érdekében az NKI (adott esetben a GovCERT) számos nemzetközi kiberbiztonsági tömörülésnek a tagja. Az NKI legfontosabb nemzetközi partnerei:

- ENISA: European Network and Information Security Agency,[5]
- FIRST: Forum of Incident Response and Security Teams,[6]
- TI: Trusted Introducer,[7]
- IWWN: International Watch and Warning Network,
- CECSP: Central European Cyber Security Platform (a visegrádi négyek és Ausztria kiberbiztonsági szervezeteit tömörítő platform).

Az NKI fent említett három szervezeti egységének a fő feladatai és hatáskörei az alábbiak.

5.1.2.2. Kormányzati Eseménykezelő Központ (GovCERT)

Az Ibtv. alapján 2013. július elsején létrejött a Kormányzati Eseménykezelő Központ (GovCERT-Hungary), amely a magyar kormányzat információmegosztó és incidenskezelő

[5] ENISA European Network and Information Security Agency. Elérhető: www.enisa.europa.eu (A letöltés dátuma: 2018. 06. 03.)

[6] FIRST Forum of Incident Response and Security Teams. Elérhető: www.first.org (A letöltés dátuma: 2018. 06. 03.)

[7] TI Trusted Introducer. Elérhető: www.trusted-introducer.org (A letöltés dátuma: 2018. 06. 03.)

szervezete. Alapvető rendeltetése az Ibtv. hatálya alá tartozó szervezetek informatikai biztonsági támogatása, amely két részből, megelőzési és reaktív tevékenységekből tevődik össze. Egyrészt megelőző jelleggel végzi a szoftversérülékenységek és információbiztonsági fenyegetések összegyűjtését, kezelését, valamint az információk megosztását, az érintettek tájékoztatását. Másrészt reaktív tevékenységként az Ibtv. hatálya alá tartozó szervezeteknél az elektronikus információbiztonsági incidensek kivizsgálásában, azok kezelésének koordinációjában működik közre.[8] A kormányzati eseménykezelő központ feladat- és hatáskörét a kormányzati eseménykezelő központ és az eseménykezelő központok feladat- és hatásköréről, valamint a biztonsági események kezelésének, a biztonsági események műszaki vizsgálatának és a sérülékenységvizsgálat lefolytatásának szabályairól szóló 185/2015. (VII. 13.) Korm. rendelet határozza meg. Eszerint a GovCERT főbb feladatai a következők:

1. a biztonsági események és fenyegetések kezelésével támogatja az állami és önkormányzati szerveket, ami kapcsán
   a) értesíti az érintetteket,
   b) az érintettek számára szakmai támogatás nyújt,
   c) a biztonsági eseményekről a megtett intézkedéseket és azok eredményét tartalmazó nyilvántartást vezet;
2. együttműködik
   a) az alábbi hatóságokkal:
      - a szintén az NKI keretein belül működő NEIH-hel,
      - a polgári hírszerzési szervezetrendszeren belül működő hatósággal,
      - a honvédelmi ágazaton belül működő hatósággal,
      - a hivatásos katasztrófavédelem szervezetrendszerén belül működő hatósággal;
   b) az alábbi eseménykezelő központokkal:
      - a kijelölt létfontosságú rendszerelem elektronikus információs rendszereit érintő eseményeket kezelő központtal,
      - a honvédelmi célú, elektronikus információs rendszereket érintő eseményeket kezelő központtal,
      - a polgári hírszerző tevékenységet végző nemzetbiztonsági szolgálat elektronikus információs rendszereit érintő eseményeket kezelő központtal,
   c) a rendvédelmi szervekkel és a Katonai Nemzetbiztonsági Szolgálattal (a továbbiakban: KNBSZ),
   d) a Nemzeti Média- és Hírközlési Hatósággal (a továbbiakban: NMHH) és az általa működtetett Országos Informatikai és Hírközlési Főügyelettel,
   e) az elektronikus hírközlési szolgáltatókkal,

[8] Nemzeti Kibervédelmi Intézet – Kormányzati Eseménykezelő Központ. Elérhető: www.cert-hungary.hu/node/1 (A letöltés dátuma: 2018. 06. 03.)

   f) a központosított informatikai és elektronikus hírközlési szolgáltatóval [a központosított informatikai és elektronikus hírközlési szolgáltatásokról szóló 309/2011. (XII. 23.) Korm. rendelet alapján ez a NISZ Nemzeti Infokommunikációs Szolgáltató Zártkörűen Működő Részvénytársaság, a továbbiakban: NISZ Zrt.],
   g) az elektronikus kereskedelmi szolgáltatókkal és a közvetítő szolgáltatókkal,
   h) az elektronikus információs rendszerek biztonságáért felelős személyekkel,
   i) a magyar és a nemzetközi hálózatbiztonsági szervekkel,
   j) az iparági szereplőkkel;
3. kivizsgálhatja a biztonsági eseményre vagy fenyegetésre utaló tevékenységeket;
4. figyelmeztetést ad ki konkrét biztonsági események kapcsán
   a) a NISZ Zrt.,
   b) a felhasználók,
   c) az eseménykezelő központok,
   d) a hatóságok felé;
5. sérülékenységekkel és fenyegető kockázatokkal, valamint a javasolt biztonsági intézkedésekkel összefüggésben tájékoztatást nyújt
   a) az elektronikus információs rendszerek biztonságáért felelős személyeknek,
   b) a hatóságoknak,
   c) az eseménykezelő központoknak,
   d) valamint az érdeklődőknek a saját honlapján keresztül;
6. elemzéseket, jelentéseket készít
   a) a magyar és nemzetközi információbiztonsági irányokról,
   b) a Tanács részére negyedévente,
   c) az irányító miniszter részére évente;
7. nem kötelező érvényű állásfoglalásokat, ajánlásokat ad ki;
8. mint országon belüli koordinációs szervezet kapcsolatot tart, információt cserél, tájékoztatást kérhet, valamint végzi az internetet támadási csatornaként felhasználó incidensek kezelését és elhárításának koordinálását, együttműködve
   a) az Európai Hálózat- és Információbiztonsági Ügynökséggel (European Union Agency for Network and Information Security, a továbbiakban: ENISA)
   b) a számítógép-biztonsági eseményekre reagáló csoportok (Computer Security and Incident Response Team, a továbbiakban: CSIRT) hálózatával,
   c) más országok CERT-jeivel,
   d) a magyar és nemzetközi kritikus információs infrastruktúra védelmi szervezeteivel,
   e) a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló Lrtv. szerint kijelölt, alapvető szolgáltatásokat nyújtó szereplőkkel,
   f) az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről szóló 2001. évi CVIII. törvény szerinti bejelentésköteles szolgáltatást nyújtókkal;
9. tájékoztatási, tudatosítási, szakértői-oktatói tevékenységet folytat (például szakmai anyagokat, útmutatókat készít, kiberbiztonsági konferenciákat, gyakorlatokat szervez, kiberbiztonsági témában megjelenik a médiában);
10. részt vesz az infokommunikációs biztonságra vonatkozó stratégiák és szabályozások előkészítésében.

Kiemelendő, hogy a GovCERT a kibertérben elkövetett bűncselekmények kapcsán hathatós segítséget tud nyújtani a nemzetbiztonsági szolgálatoknak és a rendvédelmi szerveknek. Fontos szerepe van ugyanis a határon átnyúló kibertérben vagy annak segítségével elkövetett bűncselekmények, káros tevékenységek esetében az információk megosztásában. Egyrészt a hazai nyomozások során feltárt információkat továbbítani tudja az illetékes ország(ok) CERT-je(i) felé, például kérve intézkedésüket egy káros tevékenységet folytató szerver lekapcsoltatásához, másrészt a külföldi CERT-ek hasonló jellegű megkereséseit továbbítani tudja a hazai bűnüldöző szervek irányába.

5.1.2.3. Nemzeti Elektronikus Információbiztonsági Hatóság (NEIH)

Alapvető rendeltetése az Ibtv. és más vonatkozó, az elektronikus információbiztonsággal kapcsolatos előírásokat tartalmazó jogszabályokban foglalt előírásoknak, követelményeknek való megfelelőség ellenőrzése az érintett szervezeteknél, de kiemelt szerepe van abban is, hogy e követelmények a központi költségvetésből és/vagy európai uniós forrásból megvalósuló infokommunikációs fejlesztések során elektronikus információs rendszerek teljes életciklusa alatt konzekvensen, teljes mértékben megvalósításra kerüljenek. A NEIH feladat- és hatáskörét az Ibtv. és az elektronikus információs rendszerek biztonsági felügyeletét ellátó hatóságok, valamint az információbiztonsági felügyelő feladat- és hatásköréről, továbbá a zárt célú elektronikus információs rendszerek meghatározásáról szóló 187/2015. (VII. 13.) Korm. rendelet határozza meg. Eszerint a NEIH főbb feladatai a következők:

1. az elektronikus információs rendszerek osztályba sorolása és a szervezetek biztonsági szintje kapcsán
   a) a bejelentett biztonsági osztályba sorolások nyilvántartása,
   b) az érintett szervezet által hozott döntés felülvizsgálata,
   c) hatósági eljárás keretében a jogszabályban meghatározott követelmények teljesülésének ellenőrzése,
   d) a biztonsági hiányosságok elhárításának elrendelése,
   e) utóellenőrzése,
   f) kockázatelemzés elvégzése;
2. elektronikus információs rendszer külföldön történő üzemeltetése esetén
   a) az Európai Gazdasági Térség (a továbbiakban: EGT) tagállamaiban történő üzemeltetésének engedélyezése,
   b) az EGT tagállamain kívül történő üzemeltetés ellenőrzése;
3. biztonsági eseményekkel kapcsolatos
   a) bejelentések fogadása,
   b) a kivizsgálásukra irányuló hatósági eljárás megindítása;
4. az európai uniós vagy központi költségvetési támogatásból információtechnológiai fejlesztési projektekben az információbiztonsági követelmények teljesülésének ellenőrzése;
5. éves ellenőrzési terv készítése;
6. nyilvántartások vezetése
   a) a szervezetek elektronikus információs rendszereiről (megnevezés, biztonsági osztályba sorolás, a szükséges védelmi intézkedések adatai stb.)
   b) a GovCERT-től kapott biztonsági eseményekkel kapcsolatos értesítésekről (amelyeket a honlapján közzé is tesz);

7. javaslattétel ágazati kijelölő hatóság részére a nemzeti létfontosságú rendszerelem kijelölésére;
8. együttműködés és kapcsolattartás
   a) az Elektronikus Ügyintézési Felügyelettel[9] (a továbbiakban: Felügyelet),
   b) a nemzetbiztonsági szolgálatokkal,
   c) az alábbi eseménykezelő központokkal:
      - a GovCERT-tel,
      - a kijelölt létfontosságú rendszerelem elektronikus információs rendszereit érintő eseményeket kezelő központtal,
      - a honvédelmi célú, elektronikus információs rendszereket érintő eseményeket kezelő központtal,
      - a polgári hírszerző tevékenységet végző nemzetbiztonsági szolgálat elektronikus információs rendszereit érintő eseményeket kezelő központtal,
      - a magyar és a nemzetközi hálózatbiztonsági szervekkel;
   d) a hálózati és információs rendszerek biztonságáért felelős nemzetközi szervezetekkel,
   e) az érintett EGT-tagállamok hatóságaival,
   f) a Nemzeti Adatvédelmi és Információszabadság Hatósággal (a továbbiakban: NAIH);
9. az Európai Bizottság részére tájékoztatás adása és adatok szolgáltatása (például az alapvető szolgáltatásokról, az azokat nyújtó szereplőkről, az információbiztonságra vonatkozó szabályokról).

5.1.2.4. Biztonságirányítási és Sérülékenységvizsgálati Osztály

A biztonságirányítás területén az NKI a biztonsági felügyeletére bízott, kiemelt kormányzati rendszerek esetében információbiztonsági irányítási rendszert (IBIR) működtet, emellett pedig egyrészt szakmai támogatást nyújt a NEIH, másrészt az állami és önkormányzati szervek számára. Sérülékenységvizsgálat kapcsán az NKI-nak több feladata is van. Az Ibtv. és a 185/2015. (VII. 13.) Korm. rendelet értelmében kizárólag a GovCERT jogosult a nemzetbiztonsági védelem alá eső állami és önkormányzati szervek, a zárt célú elektronikus információs rendszerek, valamint az állami és önkormányzati szervek létfontosságú rendszerelemeinek elektronikus információs rendszerei esetében sérülékenységvizsgálatot végezni. Az ebbe a körbe nem tartozó állami és önkormányzati rendszerek esetében az Ibtv. és a 185/2015. (VII. 13.) Korm. rendelet alapján megfelelő engedélyekkel rendelkező, az Alkotmányvédelmi Hivatal (a továbbiakban: AH) nyilvántartásában szereplő, a szakmai és biztonsági elvárásoknak megfelelő gazdálkodó szervezet végezhet sérülékenységvizsgálatot. Az AH a nyilvántartásába történő felvétel során a szakmai kompetenciák ellenőrzése érdekében kikéri a GovCERT állásfoglalását is. A vizsgálatok célja az adott elektronikus információs rendszer gyenge pontjainak feltárása, valamint javaslatok megfogalmazása azok javítására, kiküszöbölésére. Az IBIR és a sérülékenységvizsgálat is – megelőző intézkedésként – hathatósan elősegíti az elektronikus információbiztonsági incidensek megelőzését, bekövetkeztük megakadályozását.

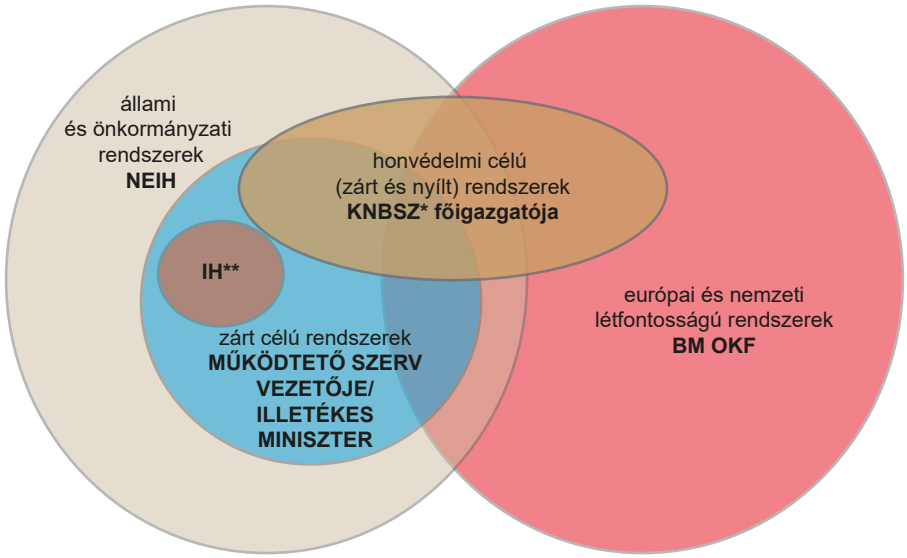
[9] 2015. évi CCXXII. törvény az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól.

5.1.2.5. OKF Létfontosságú Rendszerek és Létesítmények Informatikai Biztonsági Eseménykezelő Központ

A BM Országos Katasztrófavédelmi Főigazgatóság (a továbbiakban: OKF) szervezetén belül működő Létfontosságú Rendszerek és Létesítmények Informatikai Biztonsági Eseménykezelő Központ (a továbbiakban: LRLIBEK) látja el – az Ibtv. hatálya alá eső szervezetek által üzemeltetett létfontosságú rendszerek és létesítmények kivételével – a nemzeti létfontosságú rendszerek és létesítmények védelmével kapcsolatos hálózatbiztonsági tevékenységeket. Az LRLIBEK feladat- és hatáskörét az Ibtv., a 185/2015. (VII. 13.) Korm. rendelet, valamint az elektronikus információs rendszerek biztonsági felügyeletét ellátó hatóságok, valamint az információbiztonsági felügyelő feladat- és hatásköréről, továbbá a zárt célú elektronikus információs rendszerek meghatározásáról szóló 187/2015. (VII. 13.) Korm. rendelet határozza meg. Ezek alapján az LRLIBEK főbb feladatai:

1. eseménykezelés [a 185/2015. (VII. 13.) Korm. rendelet szerint];
2. biztonsági események kapcsán
   a) nyilvántartás vezetése,
   b) az érintettek haladéktalan értesítése,
   c) szakmai támogatás nyújtása,
   d) együttműködés a hatósággal, az érintett szervezetekkel,
   e) a kezelésükre irányuló tájékoztató tartása;
3. folyamatosan elérhető, 24 órás ügyelet működtetése;
4. sérülékenységekről és fenyegető kockázatokról tájékoztatás nyújtása;
5. a magyar kibertér rendszeres biztonsági helyzetértékelésének elvégzése;
6. hazai és nemzetközi információbiztonsági és kibervédelmi gyakorlatok tervezése, szervezése, gyakorlatokon történő részétel;
7. szakértői-oktatói, tudatosító tevékenység végzése;
8. információtechnológiai, hálózatbiztonsági és biztonságiesemény-kezelési együttműködési fórum működtetése.

2017 végén megjelent a hálózati és információs rendszerek biztonságának az egész unióban egységesen magas szintjét biztosító intézkedésekről szóló, 2016. július 6-ai (EU) 2016/1148 európai parlamenti és tanácsi irányelvet (a továbbiakban: NIS-irányelv) a hazai jogrendbe átültető, a bejelentésköteles szolgáltatást nyújtókról szóló 410/2017. (XII. 15.) Korm. rendelet, amely kibővítette a BM Országos Katasztrófavédelmi Főigazgatóság feladat- és hatáskörét. A NIS-irányelv az alapvető (az energia, a pénzügyi, az egészségügyi, a vízügyi és a közlekedési ágazatokban kijelölt kritikus) infrastruktúrák és bejelentésköteles szolgáltatást (online piacterek és keresőprogramok, felhőalapú számítástechnikai szolgáltatások) nyújtók esetében kívánja az általuk nyújtott szolgáltatások folyamatossága és az általuk kezelt adatok és információk védelme tekintetében emelni az információbiztonság szintjét. Az ehhez szükséges eseménykezelő központi és hatósági feladatokat utalta a 410/2017. (XII. 15.) Korm. rendelet az OKF feladat- és hatáskörébe. Az elektronikus információs rendszerek hatósági felügyeletének feladat- és hatáskörmegosztását a 7. ábra szemlélteti.



7. ábra

Az elektronikus információs rendszerek hatósági felügyelete

Megjegyzés:

* KNBSZ = Katonai Nemzetbiztonsági Szolgálat

**IH = Információs Hivatal, polgári hírszerző tevékenységet vezető nemzetbiztonsági szolgálat főigazgatója

Forrás: Országos Katasztrófavédelmi Főigazgatóság Létfontosságú Rendszerek és Létesítmények Informatikai Biztonsági Eseménykezelő Központ alapján saját szerkesztés

5.1.2.6. A HM CERT és az IH CERT

A Honvédelmi Minisztérium (a továbbiakban: HM) a KNBSZ keretein belül működteti saját, honvédelmi célú zárt és nyílt rendszerei kibervédelmét biztosító és mind az incidenskezelési feladatokat, mind pedig a hatósági funkciókat ellátó szervezetét, amely az 1. ábrán HM CERT néven szerepel. Ez a szervezet a szakfeladat szerint elkülönülő – a honvédelemért felelős miniszter irányítása, vezetése alatt álló szervnél, szervezetnél működő – eseménykezelő központokkal együtt látja el a biztonsági események és fenyegetések kezelését. A HM a honvédelmi szervezetek 2016. évi fő célkitűzéseinek és fő feladatainak, valamint a 2017–2018. évi tevékenysége fő irányainak meghatározásáról szóló 3/2016. (I. 22.) HM utasításban Military Computer Emergency Response Team, MilCERT megnevezéssel azonosította a szervezetet. Az Információs Hivatal (a továbbiakban: IH) szintén önálló, a szervezet keretein belül működő szervezetet működtet a saját zárt és nyílt célú elektronikus információs rendszereit érintő biztonsági események és fenyegetések kezelésére. Az IH CERT az eseménykezelő központot a 185/2015. (VII. 13.) Korm. rendelet alapján IntCERT megnevezéssel azonosítja.

5.1.3. A hazai kibervédelem rendvédelmi szervezete – Készenléti Rendőrség Nemzeti Nyomozó Iroda (KR NNI) Kiberbűnözés Elleni Főosztály

A rendőrség az Alaptörvényben, a Rendőrségről szóló 1994. évi XXXIV. törvényben, valamint ez utóbbi felhatalmazása alapján más jogszabályban meghatározott bűnmegelőzési, bűnüldözési feladatkörében általános bűnügyi nyomozó hatósági jogkört gyakorol, végzi a bűncselekmények megelőzését, megakadályozását és felderítését, valamint a bűncselekményből származó vagyon visszaszerzését. A rendőrség fellép a kiberbűnözés valamennyi szegmense, így különösen a számítógépes rendszerek elleni támadások, a rosszindulatú számítógépes szoftverek, az adathalászat, az internetes csalások, az elektronikus banki csalások, a bankkártyabűnözés, valamint a gyermekek online szexuális kizsákmányolása ellen. A rendőrség nyomozó hatóságainak hatásköréről és illetékességéről szóló 25/2013. (VI. 24.) BM rendelet, valamint az egyéb hatásköri és illetékességi szabályok alapján a rendőrség valamennyi területi és helyi bűnügyi szerve tevékenyen részt vesz a kiberbűnözés elleni harcban, így mind a megyei rendőrfőkapitányságok, mind a helyi rendőrkapitányságok folytatnak kiberbűnözéshez köthető büntetőeljárásokat. 2008. január elsején jött létre a Budapesti Rendőr-főkapitányság (a továbbiakban: BRFK) Korrupciós és Gazdasági Bűnözés Elleni Főosztály Pénzhamisítás és Csúcstechnológiai Bűnözés Elleni Osztály Csúcstechnológiai Bűnözés Elleni Alosztálya, amelynek többek között a bankkártyához köthető kiemelt jelentőségű visszaélések is a feladatkörébe kerültek. Szintén a BRFK-n került megalakításra a Bűnügyi Főosztály Gyermek- és Ifjúságvédelmi Osztálya, amely egyéb, fiatalkorúakkal kapcsolatos nyomozások mellett végzi a főváros területén a gyermekek online szexuális kizsákmányolásával kapcsolatos ügyek felderítését és nyomozását. A kiberbűnözés elleni fellépés prioritására tekintettel 2017. január elsején került felállításra a Készenléti Rendőrség Nemzeti Nyomozó Iroda Kiberbűnözés Elleni Főosztálya, a legnagyobb létszámú, kifejezetten kiberbűnözés elleni küzdelemre szakosodott rendvédelmi egység Magyarországon. A főosztály jelentős mértékű létszámbővítése és technikai fejlesztése jelenleg is folyamatban van. A KR NNI titkos információgyűjtést, titkos adatszerzést és nyomozási feladatokat ellátó, országos illetékességű szervezeti egység. A 25/2013. (VI. 24.) BM rendelet 2. mellékletének értelmében a főosztály kizárólagos hatáskörébe tartozik a Büntető Törvénykönyvről szóló 2012. évi C. törvény 375. §-ba ütköző, különösen jelentős kárt okozó, információs rendszer felhasználásával elkövetett csalás, ha annak elkövetője bűnszervezet vezetője vagy tagja, a 423. §-ba ütköző, közérdekű üzem ellen elkövetett információs rendszer vagy adat megsértése, valamint a 424. §-ba ütköző, közérdekű üzem ellen elkövetett információs rendszer védelmét biztosító technikai intézkedés kijátszása. A 2. mellékletben felsorolt bűncselekményeken kívül a KR NNI akkor rendelkezik hatáskörrel, ha a nyomozás alapjául szolgáló bűncselekménynek az Egyesült Nemzetek keretében, Palermóban, 2000. december 14-én létrejött, a nemzetközi szervezett bűnözés elleni Egyezmény kihirdetéséről szóló 2006. évi CI. törvény 3. cikk (2) bekezdésében meghatározottak alapján nemzetközi jellege van. Tekintettel a fentiekre, a főosztály bűnügyi nyomozó tevékenysége kiterjed a számítástechnikai eszközökkel, különösen az internet felhasználásával elkövetett kiemelt súlyú, speciális számítástechnikai ismereteket igénylő, gyakran nemzetközi vonatkozású bűncselekmények nyomozására és vizsgálatára (például információs rendszer elleni támadás, információs rendszer felhasználásával elkövetett csalás, gyermekek online szexuális kizsákmányolása, tiltott online szerencsejáték szervezése, személyes adattal való

visszaélés). A kiberbűnözés tágabb fogalmába tartozó készpénz-helyettesítő fizetési eszközökkel kapcsolatos szervezett és nemzetközi jellegű bűncselekmények nyomozása a szintén a KR NNI szervezetén belül működő Felderítő Főosztály Pénz- és Bankkártya Hamisítás Elleni Osztály hatáskörébe tartozik. A folyamatban lévő kiberbűncselekményekkel kapcsolatos nyomozások operatív támogatása mellett a Kiberbűnözés Elleni Főosztály egyéb feladatai:

1. bűnügyi hírszerző tevékenység folytatása a kiberbűnözéssel összefüggő legújabb jelenségekkel kapcsolatban (például: Bitcoin és egyéb elektronikus fizetőeszközök, darknet-jelenség, hackertevékenység, illegális online piacok, új típusú piramisjáték és csalás jellegű tevékenységek stb.);
2. forenzikus tevékenység végzése a KR NNI saját, valamint a területi és helyi rendőri szervek kiemelt jelentőségű ügyeiben (például a lefoglalt számítástechnikai adathordozók, így asztali számítógépek, laptopok, szerverek, pendrive-ok, külső merevlemezek, SD-kártyák, valamint mobiltelefonok és tabletek adatainak lementése, elemzése és értékelése);
3. közreműködés helyszíni intézkedésekben, házkutatásokon és lefoglalásokon;
4. együttműködik és kapcsolatot tart
   a) a helyi és területi rendvédelmi szervekkel,
   b) ügyészségekkel,
   c) az Alkotmányvédelmi Hivatallal,
   d) a Terrorelhárítási Központtal,
   e) a TIBEK-kel,
   f) a Nemzeti Kibervédelmi Intézettel,
   g) az Országos Katasztrófavédelmi Főigazgatósággal,
   h) a legjelentősebb hazai hírközlési szolgáltatókkal,
   i) a Nemzetközi Gyermekmentő Szolgálat Magyar Egyesülettel,
   j) a Nemzeti Média- és Hírközlési Hatósággal,
   k) a Nemzeti Infokommunikációs Szolgáltató Zrt.-vel,
   l) a Magyar Bankszövetséggel;
5. az ORFK és az NMHH, illetve az ORFK és a NISZ Zrt. között megkötött együttműködési megállapodások alapján a két magyar Internet Hotline-ra (internethotline.hu, biztonsagosinternet.hu) érkező állampolgári bejelentésekkel kapcsolatos elsődleges feladatok ellátása (bejelentés értékelése, nyomozás elrendelése, hatáskör és illetékesség megállapítása, adott esetben a nyomozás lefolytatása);
6. oktatási tevékenység végzése:
   a) az NKE Rendészettudományi Kar nappali és levelező tagozatos képzésén,
   b) a Magyar Igazságügyi Akadémia ügyészi és bírói továbbképzésein,
   c) regionális rendőri, ügyészi és bírói továbbképzéseken,
   d) a kormányzati szervek és a velük együttműködő civil szervezetek által szervezett képzéseken, továbbképzéseken és konferenciákon.

5.1.4. A NISZ Zrt. kibervédelmi szervezete

A hazai állami, önkormányzati szektor kibervédelmére is erős befolyást gyakorol az a központosított informatikai és elektronikus hírközlési szolgáltató/szolgáltatások kialakítása érdekében zajló folyamat, amelyet azért indítottak el, hogy a korábbi széttagolt, drágán fenntartható, heterogén eszközrendszerű, sőt sok esetben elavult állami, önkormányzati infokommunikációs rendszert konszolidálja, és egységes, megfelelő szolgáltatási és biztonsági szintű szolgáltatást nyújtson minden érintettnek. A feladatra a NISZ Zrt.-t jelölte ki a kormány. A NISZ Zrt. működését meghatározó legfontosabb jogszabályok a már említett és hivatkozott 309/2011. (XII. 23.) Korm. rendelet mellett a kormányzati célú hálózatokról szóló 346/2010. (XII. 28.) Korm. rendelet, az egyes, az elektronikus ügyintézéshez kapcsolódó szervezetek kijelöléséről szóló 84/2012. (IV. 21.) Korm. rendelet, az elektronikus ügyintézés részletszabályairól szóló 451/2016. (XII. 19.) Korm. rendelet, valamint a központosított informatikai és elektronikus hírközlési szolgáltatásokat egyedi szolgáltatási megállapodás útján igénybe vevő szervezetekről, valamint a központi szolgáltató által üzemeltetett vagy fejlesztett informatikai rendszerekről szóló 7/2013. (II. 26.) NFM rendelet. A NISZ Zrt. működését meghatározó szabályozók mellett a téma szempontjából fontos megemlíteni az információbiztonság feladatait rögzítő, a központosított informatikai és elektronikus hírközlési szolgáltató információbiztonsággal kapcsolatos feladatköréről szóló 186/2015. (VII. 13.) Korm. rendeletet is. Az említett jogszabályok természetesen elsősorban a NISZ Zrt. által ellátandó feladatokról szólnak, ezáltal közvetetten az érintett szervezetek infokommunikációs rendszereinek konszolidálását irányozzák elő, e rendszerek egy részének, vagy adott esetben egészének központi szolgáltató által történő biztosításával – és adott esetben kiváltásával. Ez azonban az ezekben a rendszerekben tárolt, kezelt elektronikus információk biztonságát is érinti, hiszen az adott elektronikus információs rendszer azon részének, amelyet a NISZ Zrt. biztosít, neki kell megteremtenie az Ibtv. és a 41/2015. (VII. 15.) BM rendelet által előírt biztonsági kontrollok rá eső részét. Azaz akárcsak az elektronikus információs rendszer elemeinek tervezése, üzemeltetése, úgy a biztonság megteremtésének feladata, felelőssége is megoszlik a szolgáltató és a felhasználó között. A 186/2015. (VII. 13.) Korm. rendeletben foglaltak szerint a központi szolgáltató főbb kiberbiztonsági feladatai a következők:

1. informatikai biztonsági irányítási rendszer kialakítása és működtetése;
2. szolgáltatásokról, azok kritikusságáról, a szolgáltatásokban részt vevőkről (felhasználó, üzemeltető, fejlesztő stb.), a távoli hozzáférésekről, az igénybe vett egyéb külső szolgáltatásokról nyilvántartás vezetése;
3. kockázatértékelés végzése és ennek megfelelően a szükséges védelmi elemek kialakítása;
4. a szükséges és megfelelő azonosítási, hozzáférés-kezelési és jogosultságkiosztási feladatok biztosítása;
5. a szolgáltatások biztonsági állapotának folyamatos ellenőrzése, a biztonsági események azonosítása, a biztonsági információk gyűjtésének, elemzésének elvégzése;

6. a szolgáltatások biztonsági állapota megfelelőségének folyamatosan biztosítása, intézkedés a biztonsági események megelőzésére, a bekövetkezett biztonsági események által okozott kár csökkentésére;
7. biztonsági események kezelése során az illetékes eseménykezelő központok számára tájékoztatás nyújtása, a biztonsági események azonosításához, elemzéséhez és kezeléséhez szükséges bizonyítékok, adatszolgáltatás biztosítása, vizsgálatok elvégzése, valamint az elrendelt biztonságnövelő intézkedések végrehajtása.

A releváns jogszabályokban megfogalmazottak teljesítése érdekében a NISZ Zrt.-n belül kialakításra került az Elektronikus Információbiztonsági Igazgatóság. A fentiek mellett az igazgatóság látja el a jogosult szervezetek, így a rendvédelmi szervek számára a különböző nyílt és titkos információgyűjtés keretében kért, a NISZ Zrt. által üzemeltetett rendszerekből kinyerhető adatok tekintetében az adatszolgáltatási tevékenységet is.

5.1.5. Hun-CERT

A Hun-CERT egy, a Magyar Tudományos Akadémia Számítástechnikai és Automatizálási Kutatóintézetében (MTA SZTAKI) működő, az Internet Szolgáltatók Tanácsának (ISZT) támogatásával létrejött munkacsoport, amely éppen ezért a hazai internetszolgáltatók, különösképpen a Magyar Internet Szolgáltatók Tanácsának (ISZT) tagjai szolgálatában fejti ki tevékenységét. Mindezek mellett a Hun-CERT az egész hazai internetes közösség számára is szolgáltat a hálózati biztonságról szóló nyilvános információkat. A Hun-CERT fő célkitűzése, hogy segítse a magyar internetes társadalmat, ezen belül különösen a magyar internetszolgáltatókat abban, hogy megfelelő eljárásokat alkalmazzanak a kiberbiztonsági incidensek kockázatainak kezelésére és az ilyen incidensek előfordulásakor az azokra adandó válaszokra.

Főbb feladatai eszerint:

1. incidensek felderítése,
2. incidensek elemzése,
3. incidensek kezelése,
4. biztonsági tudatosság növelése.

Ennek megfelelően a Hun-CERT segítséget nyújt az ISZT tagszervezeteinél előforduló hálózati incidensek felderítésénél, elemzésénél és kezelésénél, valamint elsősorban az ISZT-tagok nagyszámú, nem hivatásszerűen számítástechnikával foglalkozó dolgozói számára szolgáltat olyan, a biztonsági tudatosság növeléséhez szükséges információkat, amelyek képessé teszik őket az internet használatával együtt járó kockázatok minél teljesebb megértésére és a sikeres védekezésre. A Hun-CERT kapcsolatot tart fenn más CSIRT-egységekkel Magyarországon belül és kívül.

5.1.6. KIFÜ CSIRT

Az Innovációs és Technológiai Minisztérium irányítása alatt működő Kormányzati Informatikai Fejlesztési Ügynökség (KIFÜ) az a Kormányzati Informatikai Fejlesztési Ügynökségről szóló 268/2010. (XII. 3.) Korm. rendeletben meghatározottak alapján végzi tevékenységét, amelynek két fő eleme van:

1. az uniós és hazai forrásból megvalósuló informatikai projektek vezetési, minőségbiztosítási feladatainak ellátása az előkészítéstől kezdve a megvalósításon keresztül egészen azok lezárásáig,
2. a hazai közoktatási, felsőoktatási, kutatási intézmények, közgyűjtemények számára informatikai infrastruktúra fejlesztése és üzemeltetése, valamint arra épülő szolgáltatások nyújtása.

Ez utóbbi tevékenységén belül a magyar köznevelés, felsőoktatás, kutatás és közgyűjtemények szolgáltatójaként a KIFÜ egy IT-biztonsági és incidenskezelő csoportot, CSIRT-et működtet. A KIFÜ CSIRT alapfeladata minden olyan kiberbiztonsági incidens kezelését és koordinációját segíteni, amelyben legalább egy KIFÜ által kiszolgált intézmény érintett. Ezek mellett tudatosító tevékenysége keretében a kiberbiztonsággal, az incidensek megelőzésével és elhárításával kapcsolatos rendszeres és eseti tájékoztatókat juttat el minden KIFÜ által kiszolgált intézmény számára. A KIFÜ a partnerei számára a CSIRT-szolgáltatást alapszolgáltatásként biztosítja.[10] A 3. számú ábrán a szervezet még a korábbi nevén, NIIFI (Nemzeti Információs Infrastruktúrafejlesztési Intézet) CSIRT-ként szerepel.

5.1.7. Tervezett kiberbiztonsági fejlesztések Magyarországon

2018-ban intenzív munka kezdődött a hazai kibervédelem továbbfejlesztése érdekében.

Megindult a nemzeti kibervédelmi stratégiája átalakítása, amely a tervek szerint a 2013-ban elfogadotthoz képest jelentősen ki fog bővülni. Várhatóan egy, a korábbinál részletesebb, a stratégiai célokat, az érintett területeket és az elérendő célokat pontosabban meghatározó stratégia kialakítása történik meg.

Változások várhatók az operatív szintű szervezetek feladatrendszerében és ezáltal azok felépítésében is. A 2018. év végi tervek szerint az NKI feladat- és hatásköre jelentősen kibővül, így többek között beolvad majd a Nemzeti Biztonsági Felügyelet szervezete és tevékenysége, valamint ide kerül a NIS-irányelv által Magyarországra rótt feladatok ellátása is, amely jelenleg az OKF feladat- és hatáskörébe tartozik. Ennek megfelelően várhatóan az NKI jelentősen kibővített feladat- és hatáskörrel, átalakított szervezeti struktúrával és felbővített létszámmal, talán egy új név alatt fogja folytatni tevékenységét, míg az LRLIBEK jelenlegi formájában várhatóan megszűnik.[11]

---

[10] KIFÜ. Elérhető: http://kifu.gov.hu (A letöltés dátuma: 2018. 06. 03.)

[11] T/2930. számú törvényjavaslat egyes belügyi tárgyú és más kapcsolódó törvények módosításáról http://www.parlament.hu/irom41/02930/02930.pdf (letöltés: 2018.12.09.)

Jelenleg az említett változásokról szóló jogszabálytervezetek kialakítása még folyamatban van, azok elfogadása még nem történt meg. A magyar kibervédelmi struktúra és feladatrendszer átalakulását ezek véglegesítése és közzététele után lehet és kell újra áttekinteni.

5.2. A fontosabb nemzetközi kibervédelemi szervezetek, együttműködések

5.2.1. ENISA (European Union Agency for Network and Information Security)

Az ENISA,[12] azaz az Európai Hálózat- és Információbiztonsági Ügynökség, a tagállamok és intézmények érdekében tevékenykedő, azokkal együttműködő szakértői központ, amely meghatározó szerepet tölt be az európai információbiztonság területén. Egyik legfontosabb feladata ezen a területen az ismeretek és a bevált gyakorlatok terjesztése, valamint az információcsere biztosítása. Az ENISA mint az EU által felállított, európai ügynökségként dolgozó szakértői testület specifikus technikai és tudományos feladatokat is ellát, valamint segíti az Európai Bizottság hálózat- és információbiztonsághoz kapcsolódó jogszabály-előkészítő és -fejlesztő munkáját. Az ENISA székhelye Görögországban, ezen belül Kréta legnagyobb városában, Irákliónban található, de Athénban is működtet egy irodát. Az ügynökség szorosan együttműködik a tagállamokkal és a magánszektorral, akik számára kiberbiztonsági kérdésekben tanácsokat és megoldásokat nyújt. Ennek keretében páneurópai kiberbiztonsági gyakorlatokat szervez, hozzájárul a nemzeti kiberbiztonsági stratégiák fejlesztéséhez, elősegíti a CSIRT-ek együttműködését és ilyen kapacitások kiépítését, valamint tanulmányokat készít és ad ki többek között a felhőalapú rendszerek biztonságos adaptálásáról és alkalmazásáról, az adatvédelmi kérdésekről és technológiákról, az e-igazolványokról és a bizalmi szolgáltatásokról, valamint a számítógépes fenyegetések aktuális helyzetéről. A hatáskörébe tartozó kérdésekben az ENISA támogatja az Európai Unió kiberbiztonsági politikájának és jogi eszközeinek kidolgozását és azok végrehajtását.

5.2.2. FIRST (Forum of Incident Response and Security Teams)

A FIRST a kiberbiztonsági eseménykezelés elismerten vezető szervezete a világon, amelynek tagjai a kormányzati, kereskedelmi és oktatási szervezetek eseménykezelő csapataiból tevődnek össze. Jelenleg Afrikából, Amerikából, Ázsiából, Európából és Óceániából több mint 400 szervezet tagja a FIRST-nek. A FIRST elsődleges célja az incidensek megelőzésében való együttműködés és koordináció elősegítése, az incidensekre való gyors reagálás ösztönzése, valamint a tagok és a nagyközönség közötti információcsere elősegítése. A FIRST azon kívül, hogy globális bizalmi hálózatot hozott létre és tart fenn

[12] European Union Agency for Network and Information Security (eredeti nevén European Network and Information Security Agency), Európai Hálózat- és Információbiztonsági Ügynökség.

a kiberbiztonsági incidensekre reagáló közösségben, egyéb hozzáadott értékű szolgáltatásokat is kínál. Ezek közül néhány:

1. a tagok számára hozzáférést biztosít a legfrissebb bevált gyakorlatokat leíró dokumentumokhoz;
2. lehetőséget biztosít a biztonsági szakértők számára technikai beszélgetésekre, vitákra;
3. gyakorlati oktatásokat szervez, tart;
4. éves konferenciát rendez a kiberbiztonsági eseménykezelés témakörében;
5. kiadványokat készít és webes szolgáltatásokat nyújt;
6. speciális érdeklődési körök mentén úgynevezett különleges érdekcsoportokat (*Special Interest Groups,* a továbbiakban: SIG) működtet.[13]

A különleges érdekcsoportokat azért hozták létre, hogy a FIRST-tagok közös érdeklődésre számot tartó témákról beszélhessenek. A SIG-ek a FIRST-tagokból és meghívott felekből állnak, akik rendszeresen találkoznak annak érdekében, hogy feltárják a speciális technológiai vagy az érdeklődési területükön felmerülő egyéb jellegű vizsgálandó kérdéseket, megosszák egymással tapasztalataikat, együttműködjenek a kihívások közös kezelésében.

A FIRST jelenleg az alábbi kategóriákban a következő SIG-eket működteti:

1. Munkacsoportok:
   a) egyetemi környezet biztonsági kérdései,
   b) Big Data,
   c) kiberbiztonsági fenyegetések figyelése és jelzése,
   d) etika,
   e) a kiberbiztonsági gyakorlatok támadó csapatainak (Red Team) kérdései,
   f) sérülékenységek jelentése és adatcseréje,
   g) információmegosztás;
2. szabványosítási csoportok:
   a) közös sérülékenységpontozási rendszer (*Common Vulnerability Scoring System,* CVSS) kialakítása,
   b) információmegosztási szabályok kidolgozása,
   c) érzékeny információk megosztásánál használt jelzések (*Traffic Light Protocol,* TLP) egységesítése,
   d) passzív DNS-csere;
3. vitafórumok:
   a) internetinfrastruktúra-szállítói,
   b) malware-elemzési,
   c) mérőszámokkal kapcsolatos,
   d) ipari vezérlőrendszerekkel foglalkozó (*Industrial Control Systems,* ICS);
4. konferenciákon tartandó találkozók előkészítését végzők.[14]

[13] FIRST Forum of Incident Response and Security Teams. Elérhető: www.first.org (A letöltés dátuma: 2018. 06. 03.)

[14] FIRST Special Interest Groups (SIGs). Elérhető: www.first.org/global/sigs (A letöltés dátuma: 2018. 06. 03.)

5.2.3. TI (Trusted Introducer)

A Trusted Introducer szolgáltatást 2000-ben az európai CERT-közösség hozta létre a közös igények kielégítésére és egy olyan szolgáltatási infrastruktúra kiépítésére, amely létfontosságú támogatást nyújt az összes kiberbiztonsági eseménykezelő csoport számára. A TI legfontosabb szolgáltatásai, hogy megbízható gerincinfrastruktúrát biztosítson az eseménykezelő szervezetek számára, valamint listázza az ismert incidenskezelő csapatokat, akkreditálja őket a kiírt feltételek szerint, valamint igazolja az általuk bemutatott és visszaellenőrzött érettségi szintjüket. A szolgáltatásai egy részét a nyilvánosság számára is hozzáférhetővé teszi annak érdekében, hogy tovább javítsák és megkönnyítsék az érintett felhasználók és szervezetek közötti együttműködés kialakulását. Így a TI honlapján elérhető egy lista az összes felsorolt, akkreditált és tanúsított incidenskezelő csapat adatairól és egyéb hasznos információkról.[15]

5.2.4. IWWN (International Watch and Warning Network)

Az IWWN-t 2004-ben hozták létre a számítógépes fenyegetések, támadások és sebezhetőségek kezelésére irányuló nemzetközi együttműködés előmozdítása érdekében. Az IWWN a globális kiberbiztonsági tudatosító és eseménykezelő képességek kiépítése érdekében a részt vevő országok számára információcserét biztosít.[16] Az IWWN világméretű hálózat, amely a szabályzás és az operatív végrehajtás területén fejt ki tevékenységet, és jelenleg tizenöt ország kormányzati képviselőit tömöríti. Az IWWN feladatai között az alábbiak találhatók:

1. a kiberbiztonsági eseménykezelő csapatok elérhetőségi adatainak folyamatos karbantartása a nemzeti képviselők közreműködésével;
2. a fenyegetések és válságok idején koordinátori tevékenység végzése;
3. gyakorlatok szervezése;
4. az együttműködések előmozdítása;
5. az információmegosztás ösztönzése.

5.2.5. EC3 (European Cybercrime Centre)

Az EC3, avagy magyar nevén a Számítástechnikai Bűnözés Elleni Európai Központ az EU számítástechnikai bűnözéssel szembeni kollektív fellépéseként jött létre annak érdekében, hogy megerősítse az EU-ban a számítógépes bűnözésre adott bűnüldözési válaszokat, és ezáltal segítse az európai polgárokat, vállalkozásokat és kormányokat az online bűnözés elleni védelemben. Ennek indoka az volt, hogy nincs még egy olyan bűncselekménytípus, amely annyira független lenne az országhatároktól, mint a bűnözés e fajtája. Az EC3-at 2013 januárjában az Europol keretein belül azzal a céllal hozták létre, hogy az EU számítástechnikai

---

15 TI Trusted Introducer. Elérhető: www.trusted-introducer.org (A letöltés dátuma: 2018. 06. 03.)

16 IT Law Wiki – International Watch and Warning Network. Elérhető: http://itlaw.wikia.com/wiki/International_Watch_and_Warning_Network (A letöltés dátuma: 2018. 06. 03.)

bűnözés elleni küzdelmének központi szervezeteként működjön. Feladata az EU tagállamainak és intézményeinek támogatása a kibertérben vagy annak segítségével elkövetett bűncselekmények nyomozásához szükséges operatív és elemzői kapacitás kiépítésében, valamint a nemzetközi partnerekkel való együttműködés az európai kiberbűnözés felszámolása érdekében. Tevékenységeinek köre magában foglalja a rosszindulatú szoftverek, rendszerfeltörések, adathalászat, rendszerekbe történő illetéktelen behatolások, manipuláció, személyazonosság-lopások és fizetőeszközökkel összefüggő csalások, valamint a gyermekek elcsábítása és online szexuális kizsákmányolása elleni küzdelmet is.[17] Az EC3 minden évben közzéteszi az interneten a szervezett bűnözéssel kapcsolatos fenyegetésértékelést (*Internet Organised Crime Threat Assessment,* a továbbiakban: IOCTA), amely stratégiai jelentés a legfontosabb eredményekről és a számítógépes bűnözésben felmerülő veszélyekről és fejleményekről. Az IOCTA bemutatja, hogy az internetes bűnözés menynyire széles és változatos, valamint azt is, hogy az EC3 milyen szerepet játszik az ezek elleni európai fellépésben. Az EC3 működése a számítógépes bűnözés elleni küzdelemben három alappilléren nyugszik:

1. Stratégiai tevékenység: Az EC3-nak két stratégiai csapata létezik. Az egyik a megelőzési és tudatosítási tevékenységeket koordináló, valamint a partneri együttműködésért felelős tájékoztató és támogató csapat. A másik pedig a stratégiai elemzésekért, a jogszabályalkotásért és a standardizált képzések kidolgozásáért felelős stratégiai és fejlesztő csapat.
2. Műveleti tevékenység (azaz a műveleti szinten az EC3 az alábbi kiberbűncselekményekre összpontosít):
   a) kibertéren alapuló high-tech bűnözés,
   b) gyermekek online, szexuális kizsákmányolása,
   c) fizetési csalás.
3. Forenzikus tevékenység: Az EC3-nak két forenzikus tevékenységet végző csoportja van: a digitális és a dokumentum-szakértőket magában foglaló, amelyek mindegyike operatív tevékenységek támogatására, kutatásra és fejlesztésre összpontosít.

A három kiemelt kiberbűncselekmény-fajta fajta kapcsán az EC3

1. a bűnügyi és hírszerzési információk központi elosztójaként működik;
2. operatív elemzésekkel, koordinációs tevékenységgel és jelentős szakértelem biztosításával támogatja a tagállamokat műveleti és nyomozati munkájuk során;
3. különböző stratégiai elemzéseket biztosít, amelyek segítik a taktikai és a stratégiai szintű, informált döntéshozatalt a kiberbűnözés elleni küzdelemben és megelőzésben;
4. átfogó tájékoztatási funkciót biztosít a bűnüldöző hatóságok számára, amelyek a számítógépes bűnözést a magánszektorral, az egyetemekkel és más nem bűnüldöző szervekkel együttműködve kezelik;
5. támogatja a képzést és a kapacitásépítést, különösen a tagállamok illetékes hatóságai számára;

[17] Az Europol profilja az Európai Bűnüldözési Hatóság. Elérhető: www.europol.europa.eu/publications-documents/europol-profile (A letöltés dátuma: 2018. 06. 03.)

6. magasan specializált technikai és digitális igazságügyi támogatási képességeket biztosít a műveleti és nyomozati munkához;
7. az EU bűnüldözési közösségét képviseli a közös érdekű területeken (kutatás-fejlesztési követelmények, internetes irányítási és szabályzófejlesztés).

A fenti tevékenységeket támogatja az úgynevezett Cyber Intelligence Team (CIT), akik az állami, magán- és nyílt forrásokból összegyűjtik és feldolgozzák a számítógépes bűnözéssel kapcsolatos információkat, és azonosítják a felmerülő fenyegetéseket és támadási mintákat. Az EC3 mellett dolgozik a kiberbűnözéssel foglalkozó közös munkacsoport (Joint Cybercrime Action Taskforce, a továbbiakban: J-CAT), amely azokkal a legfontosabb, nemzetközi kibertérben vagy annak segítségével elkövetett bűnügyekkel foglalkozik, amelyek hatással vannak az EU tagállamaira és állampolgáraira.[18]

5.2.6. CECSP (Central European Cyber Security Platform)

A CECSP a V4-országok (Csehország, Lengyelország, Magyarország, Szlovákia) és Ausztria együttműködési platformja a kiberbiztonság területén. A platform Ausztria és Csehország kezdeményezésére jött létre 2013 májusában, célkitűzésként pedig a kiberbiztonsági információk egymás közötti megosztását, a bevált gyakorlatok és különleges eljárásmódok cseréjét, a kibervédelmi kapacitás és képesség bővítését, közös képzések, oktatások és gyakorlatok megszervezését és megtartását, valamint koordinált kiberbiztonsági kutatási és fejlesztési programok elindítását fogalmazták meg. Hosszú távú célként egy nemzeteken átívelő, regionális kibervédelmi tudatosság és kockázatkezelés kialakítását tűzték ki.[19]

5.2.7. ENCS (European Network for Cyber Security)

Az ENCS egy 2012-ben alapított, nonprofit tagszervezet, amely a biztonságos európai létfontosságú energiahálózatok és infrastruktúrák kialakításának támogatása érdekében jött létre. Ennek megfelelően az ENCS megteremti a lehetőséget arra, hogy a létfontosságú infrastruktúrák tulajdonosai, üzemeltetői, valamint a biztonsági szakemberek között kialakulhasson a megfelelő kapcsolat. Az ENCS olyan kutatókkal és tesztelő szakemberekkel rendelkezik, akik képesek az ENCS-tagokat és partnereiket segíteni az alkalmazott kutatásban, a technikai biztonsági követelmények, rendszerelemek és tesztelési eljárások meghatározásában, valamint az oktatási és képzési programokban.[20]

---

[18] Europol: European Cybercrime Centre; EC3. Elérhető: www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3 (A letöltés dátuma: 2018. 06. 03.)

[19] Central European Cyber Security Platform held its third meeting in Vienna (2014). Elérhető: http://2010-2014.kormany.hu/en/ministry-of-public-administration-and-justice/news/central-european-cyber-security-platform-held-its-third-meeting-in-vienna (A letöltés dátuma: 2018. 06. 03.)

[20] European Network for Cyber Security. Elérhető: https://encs.eu (A letöltés dátuma: 2018. 06. 03.)

5.2.8. ECSO (European Cyber Security Organisation)

Az ECSO egy teljesen önfinanszírozású, nonprofit szervezet, amely a belga jog szerint 2016 júniusában jött létre. Az ECSO képviseli az ipari szereplőket az Európai Bizottságnál a kiberbiztonság szerződéses formában, a köz- és a magánszféra közötti partnerség (*Contractual Public Private Parntership,* cPPP) keretében történő kialakítása érdekében. Az ECSO tagjai között nagyvállalatok, kis- és középvállalatok (kkv), induló vállalkozások, kutatóközpontok, egyetemek, végfelhasználók, üzemeltetők, egyesületek mellett az európai tagállamok helyi, regionális és nemzeti közigazgatásának képviselői, valamint az Európai Gazdasági Térség (EGT) és az Európai Szabadkereskedelmi Társulás (EFTA) és a H2020 társult országok képviselői is megtalálhatók. Az ECSO fő célja az európai kiberbiztonsági fejlesztések, kezdeményezések vagy projektek támogatása, ösztönzése, különösen az alábbiak:

1. az európai digitális egységes piac növekedésének előmozdítása és védelme a számítógépes fenyegetések ellen;
2. az európai kiberbiztonsági piac fejlesztése, valamint a kiberbiztonsági és az infokommunikációs ágazat versenyképességének növelése;
3. a kiberbiztonsági megoldások kidolgozása és kialakítása a megbízható ellátási lánc azon kritikus összetevőihez, ahol Európa vezető szerepet tölt be.

Az ECSO különösen az alábbi területeken fejt ki aktivitást:

1. infokommunikációs infrastruktúrák (felhőalapú rendszerek, mobilhálózatok, hálózati megoldások stb.),
2. intelligens hálózatok (energiaszektor),
3. közlekedés (beleértve az autóipari és az elektromos járműveket),
4. okosépületek és okosvárosok,
5. ipari vezérlőrendszerek (ipar 4.0),
6. közigazgatás és nyitott kormányzás,
7. egészségügy,
8. pénzügy és biztosítás.

Az ECSO a kitűzött célok elérése érdekében jelenleg az alábbi munkacsoportokat működteti:

1. WG1: szabványosítás, tanúsítás, osztályozás és ellátásilánc-menedzsment;
2. WG2: piaci bevezetés, beruházások és nemzetközi együttműködés;
3. WG3: ágazati igények;
4. WG4: kkv-k támogatása, koordináció az országokkal (különösen Kelet- és Közép-Európa országaival) és régiókkal;
5. WG5: oktatás, biztonságtudatosság, képzés, kibergyakorlatok;
6. WG6: stratégiai kutatási és innovációs menetrend.[21]

[21] European Network for Cyber Security. Elérhető: https://encs.eu (A letöltés dátuma: 2018. 06. 03.)

5.2.9. Tervezett kiberbiztonsági fejlesztések az EU-ban

A fenti, már létező szervezetek mellett az EU komoly lépéseket tervez a kiberbiztonság megerősítése érdekében. A 2017-ben közzétett elképzelések szerint ennek fontosabb elemei a következők:

1. *Egy erős Európai Uniós Kiberbiztonsági Ügynökség létrehozása:* a már működő ENISA továbbfejlesztésével létrejövő szervezet feladata lesz a tagállamok segítése a kibertámadások megelőzésében, a bekövetkezett incidensekre történő reagálásban, évente páneurópai kiberbiztonsági gyakorlatok szervezése, a fenyegetettséggel összefüggő információk és tudás megosztása. A hálózati és információs rendszerek biztonságának az egész unióban egységesen magas szintjét biztosító intézkedésekről szóló, az Európai Parlament és a Tanács (EU) 2016/1148 irányelve (2016. július 6.)[22] végrehajtásának elősegítése, valamint az infokommunikációs termékek és szolgáltatások kiberbiztonságának garantálása érdekében uniós tanúsítási keretrendszer kialakításának és végrehajtásának elősegítése.
2. *Európai Kiberbiztonsági Kutatási és Kompetenciaközpont kialakítása:* a tervezett központ, együttműködve a tagállamokkal, segítséget nyújt a fejlett kibervédelmi eszközök és technológiák kifejlesztéséhez és alkalmazásához. Működésével kiegészíti az erre a területre irányuló uniós és nemzeti szintű kapacitásépítési erőfeszítéseket.
3. *Európa és a tagállamok gyors kibervédelmi reagálási képességének növelése:* a célkitűzés a nagyszabású kibertámadások miatti egységes operatív fellépés érdekében egy uniós kiberbiztonsági válságreagálási keretrendszer létrehozása, amelyhez a tagállamok és az uniós intézmények közreműködése elengedhetetlen. A keretrendszert a kiberbiztonsági és egyéb válságkezelési gyakorlatok során tervezik rendszeresen tesztelni és az eredmények alapján finomhangolni.
4. *Kiberbiztonsági Vészhelyzet-elhárítási Alap létrehozása:* az unió tervezi egy új Kiberbiztonsági Vészhelyzet-elhárítási Alap létrehozását azon tagállamok számára, amelyek az uniós jog által előírt összes kiberbiztonsági intézkedést felelős módon megvalósították. Az alap vészhelyzeti támogatást nyújt a tagállamok megsegítésére.
5. *A kibervédelmi kapacitások megerősítése:* a kibervédelem terén jelentkező készséghiány kezelésére az EU 2018-ban kibervédelmi képzési és oktatási platformot hoz létre, valamint elmélyíti a NATO-val való együttműködést, többek között párhuzamos és összehangolt gyakorlatok megtartásával.
6. *A nemzetközi együttműködés fokozása:* a rossz szándékú kibertevékenységekkel szembeni közös uniós diplomáciai intézkedések keretrendszerének végrehajtásával, a kibertérben kialakuló konfliktusok megelőzését és a stabilitást szolgáló stratégiai keretrendszer kialakításával, valamint új, harmadik országoknak a kiberfenyegetések elleni küzdelemhez segítséget nyújtó kapacitások kiépítésével kívánja az EU megerősíteni a kibertámadásokra való reagálási képességeket.
7. *Hatékony büntetőjogi válaszintézkedések kialakítása:* a kibertérben vagy annak segítségével elkövetett bűncselekményektől való hatékony visszatartás érdekében

[22] Az Európai Parlament és a Tanács (EU) 2016/1148 irányelve (2016. július 6.) a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről.

> az EU egy új, a csalással és a készpénz-helyettesítő fizetési eszközök hamisításával szembeni küzdelemről szóló irányelv kialakítását tervezi. Ebben az információs rendszerekkel kapcsolatos bűncselekmények körét kiterjesztenék minden fizetési tranzakcióra, beleértve a virtuális fizetőeszközökkel végrehajtott tranzakciókat is, így erősítve meg a bűnüldöző hatóságokat, kiterjesztve azok lehetőségeit. A tervek szerint a jogszabály a szankciók mértékére vonatkozó közös szabályokat is bevezetne, valamint tisztázná a tagállami illetékességet a csalással és a készpénz-helyettesítő fizetési eszközök hamisításával elkövetett bűncselekmények tekintetében.

A számítástechnikai eszközök felhasználásával elkövetett bűncselekményekre vonatkozó nyomozások és büntetőeljárások, így a felderítésre, nyomon követhetőségre és büntetőeljárás alá vonásra vonatkozó bűnüldözési válaszlépések hatékonyságának növelése céljából az Európai Bizottság javaslatokat fog előterjeszteni az elektronikus bizonyítékokhoz való határon átnyúló hozzáférés megkönnyítéséről, valamint a titkosítás bűnügyi nyomozásokban betöltött szerepéről.[23]

[23] Az unió helyzetéről szóló beszéd: *Kiberbiztonság: a Bizottság megerősíti a kibertámadásokkal szembeni uniós reagálási képességet* (2017). Elérhető: http://europa.eu/rapid/press-release_IP-17-3193_hu.htm (A letöltés dátuma: 2018. 06. 03.)

6. A kiberbűncselekmények statisztikai rögzítettsége

Simon Béla

Első kérdésként felmerül, hogy voltaképpen mit is érthetünk kriminálstatisztikai megközelítésből kiberbűncselekménynek. Ha a Büntető Törvénykönyvben található kategóriákat vesszük sorra, szinte minden bűncselekmény kapcsolható lehet a kibertérhez. Valójában alig van olyan tényállás, amelyet ne lehetne infokommunikációs eszközzel elkövethetőnek tekinteni. Esetünkben azon deviáns viselkedések sorolhatók a kiberbűncselekmények körébe, amelyek eredményüket és normasértő jellegüket tekintve nagyon gyakran érintik a kiberteret, vagy e tér nélkül kevésbé valósulhatnának meg (lásd: *A kiberdevianciák színtérmódozatai* 3. fejezet). A kiberbűncselekmények kriminálstatisztikai besorolása esetében is fontos a társadalomra való veszélyesség, amely például egy emberi testet ért támadás esetén viszonylag egyértelműen meghatározható súlyosságú, szemben a kibertérben elkövetett jogsértésekkel, ahol az effajta cselekvések nem ennyire egyértelműen skálázhatók. Az etikus hackerek tevékenysége és jogi megítélése erre kiváló példa. Lehetséges, hogy a rövid távú jogsértések hosszabb távon össztársadalmilag nagyobb közjót eredményeznek. Az eddig leírtakból látható, hogy a bűnözés pontos meghatározása e területen akadályokba ütközik, de ha elvonatkoztatunk attól a problémától, hogy a kibertérhez kapcsolódó bűncselekmények megállapíthatóságának kritériuma képlékeny, és csak azt vesszük figyelembe, hogy mi az, amit Magyarország statisztikai rendszere e bűncselekményi körhöz regisztrált, akkor azt gondolhatnánk, hogy könnyen tudunk trendvonalakat felmutatni az elmúlt időszakra. A *kiberbűnözés* kifejezés egy másik oldalával is érdemes foglalkoznunk. A kibertérre vonatkozóan találunk definíciós meghatározást, amit kötetünk elején részletesen is kifejtettünk.[1] Mennyiben része e kibertér fizikai összetevőinek a hálózati eszközök, szoftverek összessége? Mit értünk a kibertér virtuális összetevői alatt? Részét képezik-e az internethez nem kapcsolódó hálózatok? Számos kérdés merül fel, amelynek kimunkálása nem e fejezet célja (Munk 2018). Esetünkben a kiberteret érintő bűncselekményeket a gyakorlati megfontolásokat alkalmazó szervezetek – különösen az Europol – gyakorlata alapján tarjuk célszerűen besorolhatónak. Az Europol az általa lényegesnek tartott bűncselekményeket, a nemzetközi bűnügyi együttműködést segítő eljárásokat elemző projektekben (*analysis project,* AP; korábban *analysis work file,* AWF) kezeli. Itt a vagyonvisszaszerzéstől az egyes kábítószerfajtákon át számos projekt él – jelenleg 28 darab. Egy ilyen elemző projektnek külön „kezelőszemélyzete" van, akik a beérkező adatokat elemzik, értékelik, és az eredményeiket az érintett hatóságok támogatására megküldik. Az Europol Kiberbűnözési Kompetenciaközpontja (EC3) három ilyen AP-t kezel:

---

[1] Lásd: 1. fejezet.

- *AP Cyborg:* támogatja az EU-ban a kritikus számítógépes és hálózati infrastruktúrákat érintő számítógépes bűnözés elleni vizsgálatokat.
- *AP Terminal:* a nemzetközi elektronikus és online fizetési csalások felderítésén dolgoznak.
- *AP Twins:* elemzési projekt, támogatja a gyermekek szexuális kizsákmányolásával és visszaélésekkel járó bűnözés minden formájának megelőzését és leküzdését.

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

- *AP Copy:* támogatja a szellemi tulajdonjogokkal kapcsolatos bűncselekmények megelőzését és az azok elleni küzdelmet.
- *AP Check-the-Web:*[2] a nyílt internetforrások figyelemmel kísérése és értékelése az iszlamista terrorizmus ellen.
- *AP Apate:* különféle csalási cselekményekkel szembeni fellépés (jellemzően online csalások) (SIMON 2018).

Tehát azt jelenthetjük ki, hogy ezekhez a kiberbűncselekményi kategóriákhoz kapcsolódóan egyértelműen besorolhatók a magyar bűnügyi statisztika által jelölt tényállások, amelyekből következtetéseket vonhatunk le. Sajnos azonban ez nem így van. A Bűnügyi Statisztikai Rendszer[3] adataiból nem különíthetők el a kérdéses kategóriák.

7. táblázat

A kibertérhez köthető bűncselekmények alakulása a 2013–2018. év első féléve közötti időintervallumban

Büntetőjogi kategória	2013	2014	2015	2016	2017	2018. I–VI. hó
Gyermekpornográfia	5225♦	142	334	272	1439▪	146
Készpénz-helyettesítő fizetési eszköz hamisításának elősegítése	3	1	3	3	1	4
Készpénz-helyettesítő fizetési eszközzel való visszaélés	5804	1186	870	23 064•	434	218
Készpénz-helyettesítő fizetési eszköz hamisítása	65	202	130	425	739	1432
Információs rendszer felhasználásával elkövetett csalás, (5) bekezdés (nincs elkülönítés a statisztikában)	250	1398	2176	3409	4467	1876

Megjegyzések:
♦ Ebből Nógrád megye: 4892.
▪ Ebből Heves megye: 1153.
• Ebből Pest megye: 22 687.

Forrás: BSR 2018

[2] AP Check-the-Web. Forrás: www.register.consilium.europa.eu/doc/srv?l=EN&f=ST%208457%202007%20REV%202 (A letöltés dátuma: 2018. 10. 30.)

[3] Bűnügyi Statisztikai Rendszer. Forrás: www.bsr.bm.hu/SitePages/Nyitolap.aspx (a letöltés dátuma: 2018. 10. 30.), https://bsr.bm.hu/Document (A letöltés dátuma: 2018. 10. 30.)

A gyermekpornográfia bűncselekmény esetszáma nagy mozgásokat mutat. E bűncselekmény esetében a legnagyobb kiugrásokat 2013-ban és 2017-ben egy-egy ügycsoport eredményezte. Ezekben az esetekben nem a sértettek számához igazodott a rendbeliség, hanem az eljárás során biztosított felvételek számához, amely egy helytelen gyakorlat. A bankkártyához kapcsolódó visszaélések közül a *készpénz-helyettesítő fizetési eszközzel visszaélés folyamatosan csökkent az elmúlt öt évben, kivétel a 2016-os évet.* A BSR-rendszerben nincs lehetőség az információs rendszer felhasználásával elkövetett csalás (5) bekezdésében rögzített minősítést (elektronikus készpénz-helyettesítő fizetési eszköz felhasználásával) külön kezelni a többi tényállástól. Így összességében kijelenthetjük, hogy e tényállás erőteljes emelkedést mutat az elmúlt évekre – akár a bankkártyával, akár más módon történő elkövetésnél is (7. táblázat).

8. táblázat

A klasszikus kiberbűncselekmények alakulása a 2013–2018 első féléve közötti időintervallumban

Büntetőjogi kategória	2013	2014	2015	2016	2017	2018. I–VI. hó
Személyes adattal való visszaélés	2635	1059	975	487	722	530
Közérdekű üzem működésének megzavarása	73	66	34	40	38	31
Tiltott adatszerzés	20	31	23	20	16	6
Információs rendszer vagy adat megsértése	823	565	520	702	586	345
Információs rendszer védelmét biztosító technikai intézkedés kijátszása	580	31	15	44	8	5
Csalás	37 345	33 362	31 976	43 383	22 197	12 884

Forrás: BSR 2018

A kibertérben elkövethető bűncselekmények körében az elmúlt 5 évben jelentős csökkenés látható. A statisztikai adatok közé sorolható még a *nemzeti adatvagyon körébe tartozó állami nyilvántartás elleni bűncselekmény,* ami a hatálybalépése óta nem valósult meg, valamint a *jogosulatlan titkos információgyűjtés vagy adatszerzés,* ami 2 esetben valósult meg 2013 óta. Ezekben az esetekben nem beszélhetünk bűnelkövetői mintázatokról és trendekről sem. A kriminálstatisztikai adatok alapján 2013 óta 17 darab terrorcselekményt regisztráltak, de ezek közül nem állapítható meg, hogy mely esetekben volt érintett a kibertér. A csalás jellegű magatartások esetében a statisztika a 2017. év májusát megelőző időszakra vonatkozóan nem tartalmaz pontos információkat – azok együtt szerepelnek az összes csalással. Ezek az adatok azért különösen érdekesek, mivel az interneten elkövetett csalás jellegű cselekmények túlnyomó többsége helyes minősítés esetén e tényállásban jelenik meg (8. táblázat). Annak további vizsgálata indokolt, hogy a hatalmas statisztikai kiugrásokat okozó ügyekben mi okozta az éves országos összes esetszámot sokszorosan meghaladó bűncselekményszám előfordulását. Ezek nyilvánvalóan nem a társadalmi viszonyokat követő és bemutató statisztikai eredmények, sokkal inkább a statisztikai rendszer hibás működése valószínűsíthető mögötte. A bűnügyi statisztikai adatokból tehát nem látható egyértelműen

a kiberbűncselekmények hagyományos bűncselekményektől elválasztható struktúrája és dinamikája. E statisztikai probléma nemcsak Magyarországon jelentkezik, hanem azt Európa számos országában észlelte a GENVAL-jelentés (Simon 2018). Ennek orvoslására 2017 májusában a Bűnügyi Statisztikai Rendszerben bevezetésre került egy plusz kérdés: Az adott bűncselekményt online környezetben követték el? Ennek éves eredményeit még nem ismerjük, de az eddigi gyakorlat azt mutatja, hogy az összesítés sok fals-pozitív elemet is tartalmazni fog. A híradásokon túlmenően azonban más forrásból is az lehet a feltételezésünk, hogy a kiberbűncselekmények fenyegetése jelentős. Egyes szakértői vélemények szerint a kiberbűnözés globális és éves szinten 1200 milliárd USD kárt okozott 2017-ben (Frész 2017). E kijelentéseket jellemzően olyan személyek teszik, akiknek érdekében áll a problémák démonizálása. Azonban nyilvánvalóan egy információbiztonsággal foglalkozó vállalkozástól sem várható el, hogy megnyugtató nyilatkozatot tegyenek a várható trendekre vonatkozóan. Az elmúlt időszakban inkább az jellemző, hogy e nyilatkozatok gyakrabban jelennek meg a médiafigyelem homlokterében.

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.

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.

Vákát oldal

8. Kiberbűncselekmények felderítése és nyomozása

Simon Béla – Gyaraki Réka

8.1. A kiberbűncselekmények illetékességi és hatásköri felosztása

A kiberbűncselekmények nyomozása szempontjából – az illetékesség megállapításának kérdésében – az ügyek ok nélküli és értelmetlen áttételei, ezzel a nyomozás hátráltatása miatt szükséges tisztázni, hogy hogyan lehet megállapítani a kibertérben elkövetett bűncselekmények esetében az elkövetés helyét. Az illetékesség alatt a földrajzi, területi meghatározást értjük. A rendőrség nyomozó hatóságainak hatásköréről és illetékességről szóló 25/2013. (VI. 24.) BM rendelet 3. §-a alapján a nyomozás lefolytatására az a nyomozó hatóság illetékes, amelynek illetékességi területén a bűncselekményt – sorozatos bűncselekmények esetén a bűncselekmények többségét – elkövették. Amennyiben az elkövetés helye nem állapítható meg, vagy pedig a cselekmény jellegéből adódóan több hatóság lenne jogosult lefolytatni az eljárást, akkor a megelőzés elve érvényesül, vagyis ott fogják az ügyet kivizsgálni, ahol korábban intézkedtek. Az illetékesség tekintetében beszélhetünk *általános* és *kiemelt* illetékességről. Általános illetékességű nyomozó hatóságok a rendőrkapitányságok (így a kerületi és városi), kiemelt illetékességűek a megyei rendőrfőkapitányságok, a Budapesti Rendőr-főkapitányság, valamint a Készenléti Rendőrség Nemzeti Nyomozó Iroda és a Reptéri Rendészeti Igazgatóság. A kiberbűncselekmények esetében is első gondolatra sokakban az a válasz fogalmazódik meg, hogy ott követik el a kiberbűncselekményeket, ahol maga az eszköz található. Ugyanakkor a válasz ennyire nem egyszerű ennél a deliktumnál, hiszen ma, amikor már az asztali számítógépek helyett laptopokat, tableteket és okostelefonokat használunk, amelyek mozgatása, helyváltoztatása egyszerű, akkor már ennyire nem evidens a válasz. Amennyiben valaki útközben (két település között vagy éppen két ország között utazva) követi el egy vállalkozás ellen a jogellenes tevékenységét, akkor annak megállapítása, hogy ki jogosult megindítani a nyomozást, már ennyire nem egyszerű. Létezik az illetékesség megállapítására is olyan nézőpont, miszerint az elkövetés helye ott van, ahol maga a kibertérben elkövetett jogellenes cselekmény ténylegesen megvalósul (így fordulhatott elő az a probléma, amikor az elektronikus cégbejegyzés megjelent, hogy a cégbíróság székhelye szerinti kerületi kapitányságnál a közokirat-hamisítások miatt indított eljárások száma megsokszorozódott, mert valamennyi olyan ügyben, ahol cégbejegyzéssel vagy cégváltozással kapcsolatban történt feljelentés vagy jogellenes cselekmény, azokat a kerületi kapitányságra továbbították). A fentiek értelmezése alapján azt gondolom, hogy a kibertér esetében – bár az nem egy egységesen meghatározott terület, tér – is megállapítható, hogy melyik nyomozó szerv jogosult eljárni. A nyomozó hatóság a hatáskörét

és az illetékességét hivatalból vizsgálja,[1] amennyiben valamelyik hiányát észleli, akkor átteszi a hatáskörrel és illetékességgel rendelkező nyomozó hatósághoz vagy ügyészhez.[2] A feljelentés esetén a hatóságnak 3 nap áll rendelkezésre, hogy az abban foglaltakat megvizsgálja, és az alapján elrendelje a nyomozást, vagy elutasítsa, illetve feljelentéskiegészítést rendeljen el. A nyomozó hatóság tudomására kell hozni minden olyan tényt vagy információt, amely alapján a nyomozást le lehet folytatni. Amennyiben a rendőrség a rendelkezésre álló adatok alapján elrendeli a nyomozást, úgy a feljelentésben foglaltakat egy, de akár több alkalommal is kihallgatás formájában tisztázhatja, pontosíthatja, amely során érdemes valamennyi információt maradéktalanul a rendelkezésre bocsátani. A rendelkezésre bocsátott információk mellett a rendőrségnek lehetősége van a 2017. évi XC. törvény, a büntetőeljárásról szóló törvény 261. §-a alapján adatkéréssel élni a szolgáltató(k) felé, aki az abban foglaltaknak megfelelően köteles azt teljesíteni akár ügyészi engedéllyel vagy anélkül. Az egyik legfontosabb kiindulópont lehet az IP-cím *(Internet Protocol address)* beazonosítása. IP-címet használ valamennyi világhálóra feljelentkezett számítástechnikai eszköz, ugyanakkor amennyiben az elkövetők nyilvános számítógépet használtak, vagy technikai úton meg tudták változtatni az IP-címüket, úgy annak sikeres beazonosítása nem minden esetben vezet az elkövetőhöz.

A büntetőeljárás megindulásakor jelentősége van, hogy az adott bűncselekményt hol követték el, és az eljárás lefolytatására melyik hatóságnak van hatásköre. Ez utóbbi meghatározása a nyomozó hatóság hatáskörével és illetékességével foglalkozó rendeletben[3] van lefektetve, annyi kitétellel, hogy késedelmet nem tűrő esetben bármely nyomozó hatóság végezhet eljárási cselekményt, azonban erről a hatáskörrel és illetékességgel rendelkező nyomozó hatóságot köteles haladéktalanul tájékoztatni (BÁNÁTI et al. 2018, 473.). A nagyobb gondot sokszor az okozza a virtuális térben elkövetett cselekményeknél, hogy hol követték el a bűncselekményt, és így kinek kell a nyomozást lefolytatni (illetékesség). A 25/2013. (VI. 24.) BM rendelet szerint a nyomozás lefolytatására az a nyomozó hatóság illetékes, amelynek illetékességi területén a bűncselekményt elkövették.[4] Problémaként merül fel, hogy kiberbűncselekmény esetében az jogosult-e eljárni, akinek a területén észlelték a bűncselekményt, vagy az a hatóság jogosult eljárni, akinek az illetékességi területén a jogellenes cselekményt elkövették, esetleg, ahol az elkövető bejelentett lakcímmel rendelkezik, életvitelszerűen tartózkodik? Amennyiben elfogadjuk, hogy az elkövetés helye szerinti hatóság jogosult eljárni, akkor is egyes bűncselekménytípusoknál, például az online hirdetéses csalások esetében, kérdésként merül fel, hogy az elkövetés (tévedésbe ejtés) helye ott van, ahol az elkövető a szándékos megtévesztésre alkalmas dolgot vagy szolgáltatást feltöltötte és meghirdette, vagy ott van, ahol azt a sértett vagy sértettek megrendelték. A virtuális tér jellemzőit, az informatikai eszközök elterjedését, tulajdonságait figyelembe véve, ha annak megállapítása lehetetlen, hogy hol történt a tárgy hirdetésének feltöltése a hirdetési vagy közösségi oldalra, akkor annak a hatóságnak kell lefolytatni az eljárást, ahol az elkövető lakik, ismeretlen tettes ellen folytatott nyomozás során ott, ahol a sértett él, több sértett esetén pedig a megelőzés szabályát kell alkalmazni vitás kérdésekben, azaz, ahol először tettek

[1] A Rendőrség nyomozó hatóságainak hatásköréről és illetékességéről szóló 25/2013. (IV. 24.) BM rendelet.
[2] 25/2013. (IV. 24.) BM rendelet 4. § (2) bekezdés.
[3] A Rendőrség nyomozó hatóságainak hatásköréről és illetékességéről szóló 25/2013. (IV. 24.) BM rendelet.
[4] 25/2013. (VI. 24.) BM rendelet 3. § (1) bekezdés.

feljelentést egy adott bűncselekmény elkövetése miatt.[5] A kiberbűncselekmények jellemzői alapján el lehet mondani, hogy a virtuális térben elkövetett bűncselekmények esetében már problémát jelent az elkövetés helye, hiszen a világháló egy határok nélküli tér, amelyben az elkövetőnek és a sértettnek vagy áldozatnak még csak földrajzilag sem szükséges egy helyen tartózkodni, így annak megállapítása, hogy ki jogosult eljárni, a hatóságok között illetékességi vitát eredményez. Ibolya Tibor, a Fővárosi Főügyészség vezetője *A számítástechnikai jellegű bűncselekmények nyomozása* című jegyzetben (Ibolya 2012) az alábbiak szerint közelíti meg a nyomozó hatóság illetékességének problémáját: a gyanúsított egy ismert aukciós portálon egy műszaki terméket hirdetett meg a bolti árnál jóval alacsonyabb értéken. A vételárat előre, egy meghatározott bankszámlaszámra kellett fizetni. A termékre több vidéki városból is érkezett megrendelés és pénzátutalás, amelyeket a gyanúsított egy budapesti bankfiókban felvette. Ez alapján Ibolya Tibor megállapításai a következők voltak:

- a cselekmény elkövetésének helye a gyanúsított lakóhelye, mert onnan töltötte fel a csalárd hirdetést,
- a cselekmény elkövetésének helye a bank budapesti fiókja, mert a gyanúsított ott vette fel a pénzt, a kár ott következett be,
- a cselekmény elkövetésének helye a sértett számlavezető bankfiókjához igazodik, mert a sértett onnan utalta el a vételárat, a kár ott következett be,
- a cselekmény elkövetésének helye a sértett lakóhelye, mert ott olvasta el a hirdetést,
- a cselekmény elkövetésének helye az internetes honlap üzemeltetőjének székhelye, mert az elkövetési magatartást a gyanúsított az interneten tanúsította,
- a cselekmény elkövetésének helye az internet, ezért az iratokat megküldik az ügyésznek állásfoglalásra.

Az említett dilemmák és lehetőségek a csalás (Btk. 373. §) tényállásával kapcsolatban kerültek bemutatásra, mégis valamennyi kibertérben elkövetett bűncselekmény esetében a hatóság számára problémát jelenthet, hogy ki illetékes az ügyben az eljárás lefolytatására. Az ügyészség álláspontja ugyanakkor, hogy az ügyek értelmetlen áttétele helyett azok gyors és eredményes lefolytatása legyen a cél, és ne a kapitányságokon folyamatban lévő ügyek számának csökkentése. Az online csalásokkal kapcsolatban (nem az információs rendszer felhasználásával elkövetett csalás tényállása értendő ezalatt) a BH2011. 332. bírósági állásfoglalás szerint: 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." Ibolya ügyész úr továbbment az illetékesség fejtegetésekor, amikor azt írta, hogy fontos annak megállapítása, hogy a cselekményt a számítógép mint célpont ellen vagy a számítógép mint eszköz segítségével követték el. Az Egyesült Államokban ugyanakkor érdemes megfigyelni, hogy a joghatóság kérdése nem jelent ilyen problémát azon államokban, ahol van a kiberbűnözéssel, azaz számítógépes bűncselekményekkel kapcsolatban külön törvény, azokkal az országokkal szemben, ahol nincs külön kiberbűncselekményekkel kapcsolatos törvény. A külön kiberbűnözéssel kapcsolatos törvényekkel rendelkező államokban, amennyiben a deliktum elkövetési magatartása épp abba az államba irányul, vagy pedig a támadás vagy

[5] Ez a szabály természetesen csak a több sértett esetében érvényesül.

jogellenes magatartás onnan származik, akkor a joghatóság nem kérdéses,[6] hiszen annak az államnak a hatósága jogosult eljárni. Amennyiben a hazai szabályozást – beleértve, hogy a számítógépes bűnözésről szóló egyezmény sem rendelkezik ezzel kapcsolatban –, továbbá Ibolya Tibor ügyész úr álláspontját összehasonlítom az USA azon tagállamainak szabályozásával, ahol kifejezetten érvényesülnek a kiberbűnözéssel kapcsolatos törvények, akkor megállapítható, hogy melyik hatóság jogosult eljárni, egyszerűbben eldönthető. A hatáskör és illetékesség kérdésében az ügyek áttétele tekintetében elsősorban a szemléletmódbeli váltásra kellene koncentrálni, vagyis a megelőzés elve alapján az jogosult eljárni, amelyik hatóságnál hamarabb tették meg a feljelentést. Amennyiben az nem megállapítható, vagy az eljárás szempontjából a célszerűség szem előtt tartásával a gyanúsított tartózkodási helyének megfelelő hatóság illetékességi területén vagy több sértett esetén amennyiben azok egy helyhez köthetők, úgy azok tartózkodási helyén kellene lefolytatni az eljárást.

Az Európai Parlament és Tanács 2013/40. számú irányelvének 12. cikke a joghatóság kérdésében a tagállamokra bízza a döntést, így a direktívában említett bűncselekményeket

a) egészben vagy részben a területükön követték el; vagy
b) egy állampolgáruk követte el, legalább azokban az esetekben, ha a cselekmény az elkövetés helyén bűncselekménynek minősül.

A tagállamok biztosítják, hogy joghatósággal rendelkezzenek abban az esetben, ha

a) az elkövető a bűncselekmény elkövetésekor fizikailag jelen van a területükön, függetlenül attól, hogy a bűncselekmény a területükön található információs rendszer ellen irányul-e; vagy
b) a bűncselekmény a területükön található információs rendszer ellen irányul, függetlenül attól, hogy az elkövető a bűncselekmény elkövetésekor fizikailag jelen van-e a területükön.

8.2. A kiberbűncselekmények nyomozása

8.2.1. A bűncselekmények eljárási szabályai

A kibertérben elkövetett vagy bármilyen, informatikai eszközökkel vagy eszköz/rendszer ellen elkövetett jogellenes cselekmény esetében is a büntetőeljárásról szóló törvény rendelkezéseit kell alkalmazni. Hazánkban – az Egyesült Államok egyes tagállamaival ellentétben – még nincs számítógépes bűncselekményekkel kapcsolatos külön anyagi és eljárásjogi szabályozás, azokra az általánosan érvényben lévő szabályokat kell alkalmazni, azzal, hogy az eljáró hatóságoknak a kényszerintézkedések és egyéb eljárási cselekmények törvényi ismerete mellett a kreativitásukat is igénybe kell venni, úgy, hogy a törvényesség, az egyenlőség és az arányosság követelményeit is be tudják tartani.

---

[6] Arkansas Code of 1987, A.C.A §5-27-606 Jurisdiction. Elérhető: http://lexisnexis.com/hottopics/arcode/Default.asp (A letöltés dátuma: 2018. 05. 10.) Például Észak-Karolinának is van külön számítógépes bűnözéssel kapcsolatos törvénye: 2010 North Carolina Code, Chapter 14 Criminal Law. Article 60: Computer Related Crime.14-453.2.Jurisdiction.

8.2.2. A felderítés

A bizonyítás mint büntető eljárásjogi fogalom nem más, mint a büntetőjogilag (anyagi jogilag és eljárásjogilag) releváns, múltbéli tények megismerése a törvényes bizonyítási eszközök és módszerek útján, illetve ezeknek a tényeknek az igazolása és rögzítése bizonyítási eszközökkel (Fantoly–Gácsi 2013, 202.). A bizonyítás célja a büntetőjogi felelősség eldöntéséhez szükséges releváns tények, ismeretek megszerzése, feladata pedig a bűncselekmény vonatozásában a tényállás tisztázása (Fantoly–Budaházi 2015, 144.). A bizonyítékok tekintetében megkülönböztetünk szabad és kötött bizonyítási rendszert. Magyarországon a büntetőeljárási törvény alapján a szabad bizonyítás elve érvényesül, azaz minden, a büntetőeljárási alapján meghatározott bizonyíték felhasználható, ugyanakkor a törvény elrendelheti egyes bizonyítási eszközök igénybevételét.[7]

8.2.3. A bizonyítékok összegyűjtése

Az internetes környezetben elkövetett bűncselekmények esetében a bizonyítékok összegyűjtése okozhatja az egyik legnagyobb problémát. A hagyományosnak mondható deliktumokkal szemben a számítástechnikai környezetben elkövetett jogsértő cselekmények vonatkozásában nemcsak fizikai, megfogható bizonyítékok lefoglalása (például: desktop, laptop, tablet, CD/DVD, pendrive) válhat szükségessé, hanem az azokon lévő adatok, információk, valamint a kibertérben lévő elektronikus (elektronikus információs rendszerben tárolt) adat megszerzése, megismerése és evidenciaként történő felhasználása is szükséges lehet. A bizonyítékok megszerzése tekintetében a hatóság rendelkezésére álló lehetőségeket a 2017. évi XC. törvény a büntetőeljárásról, valamint az 1994. évi XXXIV. törvény, a rendőrségről szóló jogszabály sorolja fel, amelyek alapján két típusú adatszerzés lehetséges: 1. a nyomozás elrendelése és a kényszerintézkedés elrendelése során szükséges az esetlegesen felmerülő akadályok miatt a különböző forrásokból – így nyílt vagy nem nyílt forrásokból – származó információk beszerzése és mérlegelése. Az elektronikus bizonyíték – mint a digitális eszközökből vagy a kibertérből nyerhető bizonyíték – magán viseli annak változékonyságát, manipulálhatóságát. Emiatt egyes tagállamokban az e-bizonyítékok összegyűjtésével és értékelésével szemben különleges követelményeket támasztanak annak érdekében, hogy a bíróságok számára elfogadható legyen. Nem mindegy ugyanakkor, hogy a bizonyítékként felhasználható adat hol található. Így az fizikai adathordozón – amelynek nyomai fellelhetők telefonon, számítógépen, nyomtatón vagy netalán gépjárműben, okoseszközön (hűtőgép, hűtő-fűtő berendezés stb.) – vagy a felhőben *(cloud)* tárolódik-e? Sok esetben, eltérően a fizikai térben található bizonyítékoktól, nem elég megtalálni a kérdéses „dolgot”, hanem annak útját mint egy bizonyítékláncolatot szükséges felderíteni és rögzíteni, ily módon

[7] 1998. évi XIX. törvény a (régi) büntetőeljárásról.

alkalmas lehet a teljes bizonyításra. A bizonyítási eljárás lefolytatásához az alábbi elektronikus vagy digitális bizonyítékok, bizonyítási eszközök begyűjtése szükséges:[8]

- a telekommunikációs eszközök, illetve azok adattartalma,
- számítástechnikai eszközök, illetve azok adattartalma,
- egyéb adathordozók (például pendrive, merevlemez, memóriakártya), illetve azok adattartalma,
- elektronikus formában tárolt könyvelési iratok,
- elektronikus levelezés,
- hangfelvétel,
- elektronikusan tárolt távközlési előfizetői és forgalmi adatok, illetve egyéb mobilkommunikációs adatok,
- elektronikusan tárolt pénzintézeti, előfizetői és forgalmi adatok,
- ATM-felvételek,
- mobilkommunikációs adatok,
- biztonsági kamerák és térfigyelő kamerák felvételei.

A bizonyítékok összegyűjtésére vonatozóan az alábbi megállapítás tehető. A bizonyítékok leggyakoribb beszerzésének lehetősége – például: ATM-felvételek, biztonsági és térfigyelő kamerák felvételei tekintetében – elsődlegesen a nyílt típusú adatszerzés módszerének alkalmazása a célravezető. Ezek: adatkérés kényszerintézkedéssel, mint lefoglalás, információs rendszerben tárolt adatok; megőrzésre kötelezés az ügy megítélésétől vagy attól függően, hogy ismeretlen vagy nem ismeretlen tettes ellen folyt az eljárás; OSINT (*Open Source Intelligent,* azaz nyílt forrású/típusú információgyűjtés) alkalmazásával.

A nem nyílt adatszerzés tekintetében a nyomozó hatóság a nyílt eljárásban nem beszerezhető módon és lehetőségekkel szerezheti meg az ügy eldöntéséhez szükséges adatokat:

- bírói és ügyészi engedélyhez nem kötött leplezett eszközök alkalmazása,
- ügyészi engedélyhez kötött leplezett eszközök,
- bírói engedélyhez kötött leplezett eszközök alkalmazása,
- titkos információgyűjtés.

8.2.4. Az elektronikus bizonyítékok

A nyomozás során a múltban történt események megállapításához szükséges a bizonyítékok összegyűjtése, a tanúvallomások értékelése. A digitális bizonyítékok koncepcionálisan ugyanazok, mint bármely más bizonyíték, vagyis az információ felhasználásával az azt vizsgáló hatóságok igyekeznek az embereket és az eseményeket időben és térben elhelyezni annak érdekében, hogy a bűncselekmények okait, módszereit a lehető legpontosabban, legprecízebben feltárják. A büntetőeljárási törvény külön nem rendelkezik a digitális bizonyítékokról *(digital evidence),* hanem az elektronikus adatot, valamint az információs eszközt nevesíti, nem határozza meg azok fogalmát, hanem felsorolásszerűen, a hagyományos bizonyítékok körébe vonva tárgyalja azokat. A büntetőeljárásról szóló 2017. évi

[8] A felsorolás nem teljes, azok köre folyamatosan változik, bűncselekménytípusonként eltérő lehet a bizonyítékként felhasználható elektronikus bizonyítékok köre.

XC. törvény és a Büntető Törvénykönyv is az *elektronikus* kifejezést használja, de emellett a hazai és a külföldi szakirodalomban használt *digitális* kifejezés is szerepel, ezért mindkettő érvényes jelenleg. A *digitális adat* olyan adat, amely egy kódolási eljárással jön létre, és amely alkalmas az elektronikus dokumentum előállítójának és egyúttal a dokumentum tartalmának azonosítására. Digitalizálás alatt azt a folyamatot értjük, amelynek során a korábban más (analóg) hordozón rögzített tartalmakat valamilyen digitalizáló eszköz segítségével a számítógép által értelmezhető formában kódoljuk, illetve rögzítjük a gép által olvasható adattároló eszközre. A digitális bizonyítékok egyik nagy területe a hagyományos keresőoldalak kutatása és azok elemzése. A bűncselekményekkel, például a gyermekpornográfiával és a szexkereskedelemmel kapcsolatos nyomozások a digitális bizonyítékokkal foglalkoznak; azonban új utak nyíltak meg az internet egyre növekvő kihasználásával globális értelemben vett kommunikációs eszközként. Ilyen digitális bizonyíték lehet a közösségi oldalak (Facebook, Twitter, Instagram) vagy a különböző kommunikációra használt applikációk, oldalak (Messenger, Viber, Skype, e-mail) tartalma. A digitális bizonyítékok sokszor több információt hordoznak a hatóság számára, mint az elektronikus bizonyítékok, hiszen az azok tartalmához történő hozzáférés nagyobb segítséget nyújthat a hatóság számára, mint a kizárólag elektronikus úton keletkezett evidenciák. Ugyanakkor nem lenne szakszerű, ha a két típusú bizonyítékot megkülönböztetnénk egymástól, hiszen azok több ponton összefüggnek, sokszor együtt említik őket.

8.2.5. A bizonyítékok és az elektronikus adatok

A kiberbűncselekményekkel kapcsolatban a bizonyítékok, azok beszerzése, rögzítése rendhagyónak is tekinthető. A nyomozás során nem feltétlenül a fizikai térben behatárolható evidenciák észlelése nehéz, hanem az azokból összegyűjthető digitális bizonyítékok, amikre eltérő végrehajtási szabályok vonatkozhatnak. A további részletezés előtt szükséges tisztázni, hogy mit is ért a jog az *adat* és az *elektronikus adat* fogalma alatt.

8.2.6. Az adat és az elektronikus adat fogalma

A 2011. évi CXII. törvény az információs önrendelkezési jogról és az információs szabadságról (a továbbiakban: Infotv.) nem határozza meg az adat fogalmát, csak a személyes adat és a különleges adat meghatározását tartalmazza. A 2013. évi L. törvény, az állami és önkormányzati szervek elektronikus információbiztonságát szabályozó jogszabály (a továbbiakban: Ibtv.) értelmező rendelkezéseiben található meg az adat jogi fogalma. Az Ibtv. 1. § (1) bekezdés 1. pontja alapján adatnak tekinthető az információ hordozója, a tények, fogalmak vagy utasítások formalizált ábrázolása, amely az emberek vagy automatikus eszközök számára közlésre, megjelenítésre vagy feldolgozásra alkalmas. A régi Be. nem határozta meg az elektronikus adat fogalmát, sőt, sok esetben nem is használja ezt a kifejezést, így a hatóság a más jogszabályban található fogalomra támaszkodott. A 2018. július elsejétől életbe lépett új büntetőeljárási törvény már külön nevesíti azt: „Elektronikus adat a tények, információk vagy fogalmak minden olyan formában való megjelenése, amely információs

rendszer általi feldolgozásra alkalmas, ideértve azon programot is, amely valamely funkciónak az információs rendszer által való végrehajtását biztosítja."[9]

8.2.7. Az adatkérés

A 2017. évi XC. törvény, az új Be. megszüntette a megkeresés jogintézményét, és helyette bevezette a 261. §-sal az *adatkérést,* amelynek „keretében a büntetőeljárással összefüggésbe hozható,

a) a szervezet birtokában lévő adat továbbítása,
b) a szervezet birtokában lévő elektronikus adat vagy irat továbbítása vagy
c) a szervezet által teljesíthető tájékoztatás adása

kérhető."[10]

8.2.8. Az adatkérés jelentősége a bizonyítás során

A nyomozó hatóság, az ügyészség és a bíróság adatkéréssel élhet jogi személy, jogi személyiséggel nem rendelkező gazdasági szervezet, állami vagy helyi önkormányzati szervezet felé is. Az eljárási törvény tételesen felsorolja az érintett szervezeteket. Az adatkérésnek fontos szerepe van a bűncselekmény felderítésében és további szakaszokban is, ugyanakkor számtalan esetben volt arra példa, hogy a gyanúsított épp egy adatkérés során szerzett tudomást az őt érintő eljárásról. A bizonyítás során a különféle adatok, információk (így például metaadatok) ismerete, hozzáférése a nyomozás alkalmával sok esetben szükséges, azok beszerzése a Be. 261. §-a alapján lehetséges a szolgáltatótól az előkészítő eljárás során, például az elektronikus hírközlési szolgáltatótól, banktitkokat, fizetési titoknak, értékpapírtitoknak vagy biztosítási titoknak minősülő adatot kezelő szervezettől, az egészségügyi és a hozzájuk kapcsolódó személyes adatot kezelő szervezettől. Meghatározott feltétel bekövetkezése esetére a rendőrség vagy a terrorizmus kezelésével foglalkozó szervezet ügyészségi engedéllyel, három hónapra (amely egyszer még meghosszabbítható) állami, helyi önkormányzati stb. szervezettől a Be. 266. §-a alapján adatszolgáltatást kérhet (feltételes adatkérés). De az adatkéréssel beszerezhető és felhasználható adatok a nyomozás szempontjából sokszor nélkülözhetetlenek; a hírközlési szolgáltatóktól beszerezhető a hívószám előfizetőjének a neve és adatai, a telefon IMEI-száma, a SIM-kártya IMSI-száma, valamint ennek alapján a híváslista, a hívások időtartama, valamint az úgynevezett kelő-fekvő pozíciók, a telefonpartner neve. Az adatkérés során a hatóság a harmadik félről az alkalmazásszolgáltatótól szerzi be az információt. A szolgáltató az elektronikus kereskedelmi szolgáltatásokról, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről szóló 2001. évi CVIII. törvény alapján titkosított kommunikációt biztosító szolgáltatást nyújt, köteles az ilyen alkalmazás igénybevételével továbbított küldeményekkel, közlésekkel kap-

[9] Be. 205. § (1) bekezdés.
[10] Be. 261. § (3)–(4) bekezdés.

csolatosan keletkező vagy kezelt[11] adatokat, beleértve a metaadatokat, azok keletkezésétől számított egy évig megőrizni.[12] Így az alkalmazásszolgáltatók tekintetében a kért adatok vonatkozásában a hatóság megkereséssel kell, hogy éljen. A külső engedélyhez kötött titkos információgyűjtésre jogosult szerv megkeresése esetén a titkosított kommunikációt biztosító szolgáltatást nyújtó alkalmazásszolgáltató a szolgáltatás típusát, a szolgáltatás előfizetőjének vagy felhasználójának a szolgáltatás igénybevételéhez szükséges azonosító adatait, a szolgáltatás igénybevételének dátumát, kezdő és záró időpontját, a regisztrációhoz használt IP-címét és portszámát, az igénybevételnél használt IP-címét és portszámát, a felhasználói azonosítót köteles átadni.[13]

8.2.9. Az elektronikus bizonyítékokhoz történő hozzáférés

A legtöbb problémát a nyomozó hatóság számára az jelenti, amikor a számítástechnikai rendszerben tárolt adathoz hozzá kell férni, vagy amikor az ügy szempontjából olyan lényeges adatra van szükség, amely valamelyik közösségi oldalon a felhasználó fiókjában vagy felhőben kerül elhelyezésre. Ezt a két esetet, illetve szabályozást tekintve az alábbiak szerint történik az eljárás. Van olyan, hogy akár a levelezési rendszer, akár pedig valamelyik közösségi háló fiókjába a belépéshez nem kell sem a felhasználónevet, sem a jelszót megadni, mivel az adott informatikai eszközön a kényszerintézkedést elszenvedő be van jelentkezve, vagy a beállítások úgy vannak megadva, hogy a felhasználónevet és a jelszót az adott számítógépen vagy IP-címen megjegyzik, és az automatikus belépési funkció be van rajta állítva. A nyomozó hatóság számára az eljárás lefolytatása szempontjából a büntetőeljárásról szóló törvény alapján a következő eljárási cselekmény lefolytatása válhat szükségessé: bár a belépés akadályok nélkül végrehajtható, főleg abban az esetben, amikor a kényszerintézkedést elszenvedő fél együttműködik, mégis a Be. 302. §-a szerint lehetséges a lakás, az egyéb helyiség vagy jármű átkutatása, valamint az információs rendszer, illetve adathordozó átkutatása a büntetőeljárás eredményességének érdekében. Ebből az eljárásjogi szabályból következik, hogy az informatikai rendszerben tárolt elektronikus adat – függetlenül attól, hogy a kutatást elszenvedő fél abba beleegyezik-e vagy sem, illetve az adott rendszert (*ergo* számítógépet, adattároló eszközt) védik-e jelszóval vagy nem, az lefoglalható, átvizsgálható, az azon tárolt adat rögzíthető, megismerhető, az bizonyítékként felhasználható. A Be. alapján a kutatást (annak részletes szabályait lásd *A kutatás* című alfejezetben) az érintett – tehát nem feltétlenül a gyanúsított – jelenlétében kell lefolytatni. A kutatás megkezdése előtt az érintettet fel kell szólítani, hogy a keresett dolgot adja elő, vagy pedig az információs rendszeren tárolt adatokat tegye a hatóság számára hozzáférhetővé. Amennyiben a kért bizonyítékot a hatóság részére átadja, vagy az adatot önszántából hozzáférhetővé teszi – azaz a belépéshez szükséges jelszót megmondja, átadja –, úgy a kutatás nem folytatható (az erre vonatkozó részletes eljárás menete a későbbiekben kerül kifejtésre). Ugyanakkor amennyiben a hatósággal nem működik

[11] 2001. évi CVIII. törvény az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről.

[12] 2001. évi CVIII. törvény 13/B. § (1) bekezdés.

[13] 2001. évi CVIII. törvény 13/B. § (1) bekezdés.

együtt az eljárással érintett, úgy a nyomozó hatóságnak más módon kell az információs rendszerben tárolt adatot megszerezni, megismerni, olyan formában, hogy az bizonyításra alkalmas legyen. Ugyanez a szabály vonatkozik arra az esetre is, ha a gyanúsított eleve be van jelentkezve a levelezési rendszerébe vagy pedig a közösségi fiókjába, és a hatóságnak „csak" a belépés gombra kell kattintania, vagy az automatikus belépés van a böngészőjébe beállítva. Ezekben az esetekben is érvényben van a számítástechnikai bűnözésről szóló egyezmény (az Európa Tanács Budapesten, 2001. november 23-án kelt Számítástechnikai Bűnözésről szóló Egyezménye) 32. cikke, a *Tárolt számítástechnikai adathoz való hozzáférés határokra tekintet nélkül, hozzájárulás vagy nyilvános elérhetőség esetén* kimondja, hogy „a Szerződő Fél a másik Szerződő Fél engedélye nélkül:

a) a nyilvánosság számára elérhető módon (nyílt forrású) tárolt számítástechnikai adathoz hozzáférhet, függetlenül az adat földrajzi elhelyezkedésétől; vagy
b) a másik Szerződő Fél területén tárolt számítástechnikai adathoz hozzáférhet vagy a területén levő számítástechnikai rendszer útján azt megszerezheti, amennyiben a Fél beszerzi az adat számítástechnikai rendszer útján történő átadására jogszabályban feljogosított személy önkéntes és jogszerű hozzájárulását."

A helyzet bonyolultságát adja, hogy nem minden állam írta ezt alá, így az eljárást csak az aláíró országok/felek területén kell végrehajtani. Kérdésként merül fel, hogy az egyezmény implementálása megtörtént-e a saját büntetőeljárási törvényükben.

A kiberbűncselekmények nyomozása során a legnagyobb jelentősége egyrészt magának a felhasználó által megadott adatoknak van, másrészt a felhasználó által hagyott úgynevezett *internetes lábnyomnak,* avagy digitális nyomnak van, amely a webes böngészési előzményeket, a készített és a tárolt, feltöltött dokumentumainkat jelenti. A felhasználók nyomokat hagynak az interneten, a különböző informatikai eszközökön, akár levelezésekkel, (családi) fényképek, videók megosztásával, internetes rendeléssel, vásárlással, a különböző online piaci műveletekkel vagy pedig az elektronikus közigazgatási rendszerek (ügyfélkapu) igénybevételével. A régi Be. szerint a nyomozó hatóság feladata az, hogy a bizonyítási eljárás során a Be. rendelkezéseit betartva bizonyítsa a jogellenes cselekmény elkövetését, felderítse és értékelje az eljárás során összegyűjtött bizonyítási eszközöket,[14] a törvényesség betartása mellett a szükséges nyomozati cselekményeket elvégezze. Az új büntetőeljárási törvény a nyomozó hatóság feladatát már másképp határozta meg: a bűncselekmények felderítése érdekében előkészítő eljárást és nyomozást végez.[15] Az informatikai eszközök és rendszerek terjedése, azok széles körű használata során új kihívásokkal szembesülnek a rendészeti és nemzetbiztonsági szervek, amelyek sok esetben megkönnyíthetik a cselekmény, illetve az elkövető megállapítását, ugyanakkor – a jogi szabályozásra figyelemmel – sokszor indokolatlanul van megkötve a kezük a bizonyítékok beszerzése és értékelése tekintetében. Érdekes módon, a jogalkotók szándékainak ismeretében a hatóságokat sokkal szigorúbb szabályok kötik az internetes környezetben elkövetett eljárási cselekmények szabályozása

[14] A régi büntetőeljárásról szóló 1998. évi XIX. törvény 77. § (1)–(2) bekezdés.
[15] Be. 31. § (1) bekezdés.

tekintetében, és a figyelem nagyobb eséllyel irányul rájuk, mint a felhasználók által hanyagul kezelt jelszavak, adatvédelmi beállítások esetére. A digitális bizonyítékok keletkezésével kapcsolatban a legfontosabb annak megértése, hogy valamennyi nyom egyedi, annak keletkezésével, értékelésével kapcsolatban nem szabad egy sémát felállítani, hiszen a bűncselekmények jellegétől, az elkövetők számától, informatikai tudásától és jellemzőitől függően változhatnak.

8.2.10. Bizonyítékok a fizikai térben

A kibertérrel összefüggésbe hozható deliktumokkal kapcsolatban a kutatás során a fizikai térben is keletkezhetnek bizonyítékok, az azokkal kapcsolatos cselekmények a kényszerintézkedés foganatosítása során dilemmát jelenthetnek.

1. Számítógép: az egyik legfontosabb nyomhordozó eszköz lehet a számítógép, amely fajtáját tekintve vagy PC *(personal computer),* vagy laptop. A számítógép a kutatás során általában a legkézenfekvőbb tárgy, ami szinte valamennyi bűncselekmény esetében hordozhat olyan nyomokat, amelyek bizonyítékként használhatók.
2. Mobiltelefon: a mobiltelefont ma már a legtöbb felhasználó miniszámítógépként, személyi asszisztensként használja. Sokszor több adatot és információt tartalmaz, és több mindent lehet megtudni a tulajdonosáról, mint a rendelkezésre álló rendszerből, a személyről elvégzett információgyűjtésből. A mobiltelefonok egyrészt telekommunikációs eszközök, másrészt dokumentumok, fényképek, egyéb adatok tárolására alkalmasak. Ugyanannyi vagy talán több információt hordozhatnak, ezért a bizonyítás során kiemelkedő szerepük van.
3. Perifériák: a perifériák azok a számítógéphez csatlakoztatható eszközök, amik egy további eszköz illesztését oldják meg. A perifériát általában – de nem feltétlenül – a külvilággal történő kapcsolattartásra használja a számítógép. Tipikus periféria a nyomtató, a billentyűzet, az egér és a monitor.[16] A perifériák már nemcsak egyszerűen kiegészítik a számítógépet, hanem sok esetben olyan információt is hordoznak, amelyek digitális bizonyítékok nyomait hordozzák, így kényszerintézkedések során lefoglalásuk és vizsgálatuk nélkülözhetetlen.
4. Tartós adathordozók: Az Európai Parlament és a Tanács 2011/83/EU irányelve (2011. október 25.) a fogyasztók jogairól (23) bekezdése – a fenti határozatnak megfelelően – kimondja, hogy „[a] tartós adathordozóknak lehetővé kell tenniük a fogyasztó számára az adattárolást mindaddig, amíg […] érdekei védelmének érdekében szükségesnek tartja", továbbá, hogy „[a]z ilyen adathordozók közé sorolandók különösen a papír, az USB-kulcsok, a CD-ROM-ok, a DVD-k, a memóriakártyák vagy a számítógépek merevlemezei, illetve az elektronikus levelek."

[16] *Periféria* címszó. Elérhető: https://pcforum.hu/szotar/perif%C3%A9ria (A letöltés dátuma: 2018. 07. 30.)

8.2.11. Bizonyíték a virtuális térben

A nyomozás sikeres lezárásának érdekében a hatóságnak mérlegelnie kell, hogy mit lehet bizonyítéknak tekinteni, valamint azokat hogyan, milyen eszközökkel és milyen taktika keretében lehet beszerezni. A bizonyítékok megszerzése még a hagyományosnak nevezhető bűncselekmények (így a lopás, csalás vagy akár emberölés) esetében is gondos mérlegelést igényel. Mérlegelni kell, hogy mit kell bizonyítéknak tekinteni, valamint annak átgondolása is nélkülözhetetlen, hogy az evidenciákat milyen módszerrel szerzik meg és tárolják annak érdekében, hogy azok minden kétséget kizáróan az eljárás végéig alkalmasak legyenek a bíróság előtti bizonyításra. A *hagyományosnak* nevezhető bűncselekmények esetében – emberölés, közokirathamisítás, csalás, lopás stb. – a bizonyítás az elkövetés eszközének maradéktalan megszerzése, a helyszínen rögzíthető nyomok biztosítása, rögzítése (fénykép-, videó- vagy akár hangfelvétel formájában) esetlegesen oly módon, hogy azok alkalmasak legyenek arra, hogy szakértő vagy szaktanácsadó a hatóság által feltett kérdéseket minden kétséget kizáróan meg tudjanak válaszolni.

8.2.12. A kutatás és a lefoglalás

A kényszerintézkedések közül a kutatás és a lefoglalás szabályai kerülnek részletesen bemutatásra mint a bizonyítékok megszerzésének egyik, hatóság által történő kikényszerítése.

8.2.12.1. Kutatás

Nem új eljárási cselekményként, hanem a *házkutatás* kifejezés helyett alkalmazza a jogalkotó a *kutatást* mint kényszerintézkedést. Annak végrehajtásakor a hatóság beleavatkozik az Alaptörvényben meghatározott kutatást elszenvedő személy(ek) alapvető jogaiba azáltal, hogy a bűncselekmény gyanúja esetén annak bizonyítására, a bizonyítékok felkutatására, az elkövető kilétének megállapítására, valamint az információs rendszer, illetve adathordozó átvizsgálása érdekében hajtja végre. A kutatás a büntetőeljárás eredményes lefolytatása érdekében a lakás, az egyéb helyiség, a bekerített hely vagy a jármű átkutatása. A kutatás információs rendszer, illetve adathordozó átvizsgálására is kiterjedhet. A kutatásra vonatkozó eljárási szabálynál nincs lényegi változás annak elrendelése tekintetében. Így akkor kerül az elrendelésére, ha

- bűncselekmény elkövetőjének elfogására,
- bűncselekmény nyomainak felderítésére,
- bizonyítási eszköz megtalálására,
- elkobozható, illetve vagyonelkobzás alá eső dolog megtalálására vagy
- információs rendszer, illetve adathordozó átvizsgálására vezet.[17]

A kutatást a bíróság, az ügyészség vagy a nyomozó hatóság saját hatáskörében eljárva rendelheti el az új eljárási törvény életbelépése után. A védett helyiségekben, így a közjegyzői vagy ügyvédi irodában végrehajtandó kutatás esetében, amikor a közjegyzői vagy

[17] 2017. évi XC. törvény 302. § (1) bekezdés.

ügyvédi tevékenységgel összefüggő védett adat megismerésére irányul az intézkedés, a kutatást a bíróság rendeli el, ahol az ügyész részvétele kötelező. Ugyanakkor azokra a helyiségekben, ahol szenzitív, illetve személyes adatokat kezelnek, például az egészségügyi intézményekben történő kutatás esetén sem a bíróság általi elrendelés, sem az ügyész részvétele nem szükséges a jogalkotó szándéka szerint. Ha a kutatás elrendeléséhez szükséges bírósági határozat meghozatala olyan késedelemmel járna, amely a kutatással elérni kívánt célt jelentősen veszélyeztetné, a kutatás a bíróság határozata nélkül is végrehajtható. Ilyen esetben a bíróság határozatát utólag haladéktalanul be kell szerezni. Ha a kutatást a bíróság nem rendeli el, annak eredménye bizonyítékként nem használható fel.[18] A kutatást elrendelő határozatnak tartalmaznia kell a kutatás célját és az elrendelését megalapozó tényeket. Ha ez lehetséges, a kutatást elrendelő határozatban meg kell jelölni azt a személyt, bizonyítási eszközt, elkobozható vagy vagyonelkobzás alá eső dolgot, információs rendszert vagy adathordozót, aki vagy amely megtalálására a kutatás irányul. A kutatást az érintett ingatlan vagy jármű tulajdonosának, birtokosának vagy használójának a jelenlétében kell végrehajtani. A kutatásra vonatkozó lényeges változások nem történtek, így annak megkezdése előtt ismertetni kell a kutatást elrendelő határozat tartalmát, és a határozatot a helyszínen kézbesíteni kell.[19] Ha a kutatás meghatározott személy, bizonyítási eszköz, dolog, információs rendszer vagy adathordozó megtalálására irányul, akkor fel kell szólítani az érintett ingatlan, illetve jármű tulajdonosát, birtokosát vagy használóját, illetve az általa megbízott személyt, hogy a keresett tárgyi bizonyítási eszköz vagy személy hollétét fedje fel, illetve a keresett elektronikus adatot tegye hozzáférhetővé. A felszólítás teljesítése esetén a kutatás csak akkor folytatható, ha megalapozottan feltehető, hogy a kutatás során más bizonyítási eszköz, dolog, információs rendszer vagy adathordozó is fellelhető. A Be. 305. § (4) bekezdése szerint tehát a hatóság felszólítására az elektronikus információs rendszer vagy adat önkéntes hozzáférhetővé tétele esetén a kutatás kizárólag abban az esetben folytatható, ha megalapozottan feltehető, hogy a további kutatás eredményeként újabb bizonyítékok is fellelhetők. A kutatás végrehajtását egy tervezésnek kell megelőznie, amely során a nyomozók adatkéréssel és információgyűjtéssel megszerzik azokat az adatokat, hogy milyen eszközöket kell keresni. Ennek tudatában lehetne előre megtervezni, hogy hogyan hajtsák végre a kényszerintézkedést. De nem minden információ szerezhető meg az eljárási törvényben meghatározott lehetőségekkel. Így tervezés során nem deríthetők fel azok az eszközök (például pendrive, SSD-kártya), amelyek a kereskedelmi forgalomban bármikor és bárhol beszerezhetők, és amelyek mérete alkalmassá teszi ezeket a könnyű elrejtésre. Fontosnak tartom annak hangsúlyozását, hogy ma már bármilyen bűncselekményről legyen szó – akár kiberbűncselekmény, testi sértés, vagyon elleni bűncselekmény, akár katonai bűncselekmény –, a gyanúsított vagy sértett birtokában lévő informatikai eszközöknek szerepük van a bizonyítás tárgya vagy eszköze tekintetében, így azok rejtekhelyét, az azzal kapcsolatos teendőket szükséges megtervezni, az adathordozókra történő esetleges rögzítésre felkészülni. A számítástechnikai és telekommunikációs eszközök vonatkozásában a 100/2018. (VI. 8.) Korm. rendelet[20] alapján, valamint a lefoglalt eszköz tekintetében az arra vonatkozó BM-PM rendeletnek (a lefoglalás alpontban részle-

[18] 2017. évi XC. törvény 303. § (3) bekezdés.

[19] 2017. évi XC. törvény 305. § (3) bekezdés.

[20] A nyomozás és az előkészítő eljárás részletes szabályairól szóló 100/2018. (VI. 8.) Korm. rendelet.

tezetteknek) megfelelően járnak el a hatóságok. Amennyiben felmerül annak lehetősége, hogy számítástechnikai eszköz átvizsgálása válhat szükségessé, úgy informatikai szakértők/szaktanácsadók kirendelésének szükségességét meg kell fontolni, akik esetleg már a kutatás alkalmával is megjelennek, elvégzik az adatok és eszközök szakszerű átvizsgálását, szükség esetén az adatok mentését. A Készenléti Rendőrség Nemzeti Nyomozóiroda Kiberbűnözés Elleni Főosztálytól (röviden: KR NNI KBEFO) vagy a Budapesti Rendőr-főkapitányság Korrupciós és Gazdasági Bűnözés Elleni Főosztály Pénzhamisítás és Csúcstechnológiai Bűnözés Elleni Osztály Csúcstechnológiai Bűnözés Elleni Alosztálytól (a továbbiakban: BRFK KGBEFO) szakirányítás kérhető. Mivel nem minden kapitányság rendelkezik a kényszerintézkedések végrehajtásához szükséges megfelelő eszközökkel, továbbá bizonyos szakkérdésekben a rendőrség állománya nincs a megfelelő tudás birtokában, emiatt sokszor vesznek igénybe külső segítséget. A külső segítség, a szakértő vagy szaktanácsadó az, aki a helyszínen elvégzi azokat a teendőket és rendelkezik azokkal az eszközökkel, amelyek a sikeresen végrehajtott eljárási cselekményhez elengedhetetlenek. Az informatikai eszköz tulajdonosát vagy kezelőjét az eljárás megkezdésekor fel kell szólítani, hogy a keresett adatot tegye hozzáférhetővé. Amennyiben az eszköze vagy csak egyes dokumentumok jelszóval vagy biometrikus azonosítóval védettek, akkor annak a hatóság rendelkezésére bocsátása a rendszerbe történő belépéséhez szükséges. Az információs rendszerben létrejönnek olyan információk, amelyek a különböző alkalmazások, szoftverek segítségével keletkeznek – dokumentumok, táblázatok, az internetről letöltött képek stb. (digitális lábnyom) –, amelyek háttérinformációval szolgálhatnak a hatóság számára, és amelyek egyébként nem beszerezhetők, csak az informatikai eszköz és a rajtalévő adat átvizsgálásakor. Ha csak egy bizonyos információra van szükség, amelynek szolgáltatására az állami, önkormányzati szerv egyébként is köteles, és az információ kinyeréséhez nem szükséges speciális ismeret, akkor a nyomozó hatóságok a megkeresés eszközéhez nyúlnak, azaz küldenek egy átiratot. Erre példa lehet annak lekérdezése, hogy adott időszakban mely munkatársak végeztek munkát az állami, önkormányzati szerv adott épületében. Ha a beszerzendő információ az eljárás szempontjából kiemelten fontos, vagy annak kinyeréséhez speciális információ szükséges, esetlegesen tartani lehet attól, hogy az adatokat törlik vagy felülírják, akkor egy erőforrás-igényesebb és gyorsabb eljárási cselekmény következhet: a lefoglalás.

8.2.12.2. Lefoglalás

Erre példa lehet, amikor a nyomozó hatóság akár az állami, önkormányzati szerv épületében önálló cselekményként, akár egy nyilatkozattételre jogosult személy tanúkénti kihallgatása alkalmával lefoglalja a munkatársak rendszerhasználatáról szóló logfájlokat tartalmazó adatokat és az azokat rögzítő adathordozót. A kutatás az eljárás alá vont személy jogaiba történő egyik legerősebb beavatkozás a fentebb említettek közül. Tipikusan akkor alkalmazható, ha más intézkedés nem biztos, hogy eredményre vezetne, vagy a nyomozás érdekében ez tűnik a legcélszerűbbnek. Jellemzően akkor kerül foganatosításra, ha az eljárás alá vont személy nem együttműködő, vagy a beszerzendő adat, információ nem egyszerűen körülírható, annak kigyűjtéséhez speciális ismeret szükséges. Példaként említhető, amikor az állami, önkormányzati foglalkoztatott a hivatali informatikai eszközöket használja fel illegális tevékenységre, például zsaroló, fenyegető e-mailek küldésére, gyermekeket ábrá-

zoló pornográf felvételek tárolására (Simon–Gyaraki 2017). Az eljárásjog szerint tárgyi bizonyítási eszköz alatt értendő minden olyan tárgy – ideértve az iratot és az okiratot is –, amely a bizonyítandó tény bizonyítására alkalmas, többek között:

- amely a bűncselekmény elkövetésének vagy a bűncselekmény elkövetésével összefüggésben az elkövető nyomait hordozza,
- amely a bűncselekmény elkövetése útján jött létre,
- amelyet a bűncselekmény elkövetéséhez eszközül használtak, vagy
- amelyre a bűncselekményt elkövették.

Irat minden olyan tárgyi bizonyítási eszköz, amely műszaki, vegyi vagy más eljárással adatokat rögzít, így különösen a papíralapú vagy elektronikus adatként létező szöveg, rajz, ábra. Okirat az az irat, amely valamilyen tény, adat valóságának, esemény megtörténtének vagy nyilatkozat megtételének bizonyítására készül, és arra alkalmas. Az okiratra vonatkozó rendelkezések irányadók az okiratból készült kivonatra is. A 100/2018. (VI. 8.) Korm. rendelet a nyomozás és az előkészítő eljárás részletes szabályairól a kutatásról és a lefoglalásról felvett jegyzőkönyvvel összefüggésben a 86. § (1) bekezdésében az alábbi rendelkezéseket tartalmazza: „Az információs rendszer átvizsgálása során biztosítani kell az információs rendszer útján – védelmi eszköz vagy informatikai megoldás megkerülése vagy kijátszása nélkül – hozzáférhető adatok megismerését és rögzítését."

Amennyiben tehát a nyomozás során számítógép lefoglalására kerül sor, fontos kiemelni, hogy egy kutatás alkalmával nem vizsgálhatjuk át a számítógépen tárolt adatokat. Sőt, ha az adott eszköz kikapcsolt állapotban van, akkor azt tilos a helyszínen bekapcsolni. Ennek az az oka, hogy minden bekapcsoláskor a korábban mentett adatok az adathordozón módosulnak. Olyan adatok is, amelyek a nyomozás során relevanciával bírhatnak (például, hogy mikor volt az utolsó rendszerindítás). Ez alól képeznek az esetlegesen a nemzetbiztonságot vagy a közbiztonságot súlyosan sértő bűncselekmények körébe tartozó esetek, vagy ahol a várható bizonyítékok késedelmes beszerzése rendkívüli érdeksérelemmel vagy kár okozásával járna. A bíróság előtt hitelt érdemlően bizonyítani kell tudni a rögzített digitális adatok, bizonyítékok eredetiségét. Az eljárás minden pontján – az intézkedés megkezdésétől egészen a bírósági tárgyalásig – igazolni kell tudni az eszközök változatlanságát, vagy ha azokon változtatás történt, akkor arra csak dokumentálás mellett, szakmai előírások betartásával van lehetőség.

1. A lefoglalásra aprólékosan fel kell készülni. Ha okunk van feltételezni, hogy az elkövető konspirál és adatait rejti, vagy biztonsági intézkedéseket vethet be az adatok hozzáférhetetlensége érdekében, akkor mindig vonjunk be szaktanácsadót (KR NNI KBEFO, NBSZ, BRFK KGBEFO vagy belső rendszergazda), esetleg szakértőt a szakértői névjegyzékből.
2. A kutatás, lefoglalás megkezdésekor az intézkedés alá vont személyeket el kell távolítani az adott eszköz közeléből, és meg kell akadályozni a fizikai hozzáférést (szükség esetén kényszerintézkedések alkalmazásával). Az intézkedés alá vont személyeket célszerű akár ekkor kihallgatni arra vonatkozóan, hogy ki használja a számítógépet. Az elkövetők ezen a területen általában nem tapasztalt kriminális személyiségek – így az első kényszerintézkedés okozta „sokkot" még hatékonyabban ki lehet használni.

3. Az inkriminált IT-eszközről fénykép- és videófelvételt indokolt készíteni, majd a külső fizikai adatkapcsolatot megszakítani (a hálózatról leválasztani). Wifi-kapcsolatot a bejövő internet kapcsolatának megszakításával – például külső antenna lecsavarásával, laptopon repülőgépmód-kapcsolóval –, jegyzőkönyvi rögzítés mellett kell megszüntetni.
4. Alapvető szabály, hogy az eljárási cselekménnyel érintett személyt sosem hagyjuk magára, mindig felügyelet alatt kell állnia, és meg kell fosztani minden lehetséges kommunikációs eszköz alkalmazásának lehetőségétől. Indokolt a ruházat átvizsgálása is, amely során felszólítjuk a zsebében található tárgyak átadására.
5. Az adatkapcsolat megszüntetését követően rögzítjük a jegyzőkönyvben, fénykép-, esetleg videófelvételen, hogy milyen alkalmazások futnak, milyen környezetben helyezkedik el a számítógép, amiből esetlegesen a használóját is lehet azonosítani (például csak ő cigarettázik, és csikkek vannak a gépnél).
6. Amennyiben szükségessé válhat, úgy minden, az eljáráshoz kapcsolódó adathordozót lefoglalunk, majd a számítógépet lehetőség szerint rendes, szabályos leállítással kikapcsoljuk.
7. Amennyiben destruktív folyamatok zajlanak az eszközön – azaz törlés vagy enkriptálás zajlik –, akkor minden más intézkedést megelőzően indokolt lehet a folyamatok megszakítása, amit leghatékonyabban az áramellátás (az elektromos áram vagy az akku lecsatolása) megszüntetésével valósítható meg.
8. Amennyiben az elkövető személye vagy az aktuálisan futó alkalmazások (BitLocker, Truecrypt, DiskCryptor, FileVault) arra engednek következtetni, hogy az eszköz titkosítva van, de az eljárási cselekmény foganatosításánál a titkosítás fel van oldva, akkor semmiképpen nem kapcsolható ki az eszköz a jelszó ismerete nélkül. Ilyen esetben például a laptoppal szakértőhöz kell menni, vagy azt kihívni, amennyiben ez semmiképpen nem oldható meg, akkor az egyébként titkosított, de aktuálisan elérhető adatokról nem titkosított másolatot kell készíteni folyamatos jegyzőkönyvi, esetleg videófelvételes rögzítés mellett.
9. A gép kikapcsolás nélküli – jellemzően szakértőt igénylő – vizsgálata abban az esetben is szükséges lehet, ha valamilyen hálózati szolgáltatás (Facebook, Gmail stb.) vagy felhőalapú tárolás valósul meg. Ezek a kapcsolatok az eszközök kikapcsolásával, elszállításával jellemzően megszűnnek, így az eljárás adataira tekintettel mérlegelni kell, hogy mi szolgálja jobban annak érdekeit.
10. A csomagolásra legalkalmasabb a nagyméretű plasztikzsák bekötve, bűnjelcímkézve. (Nem megfelelő eljárás, hogy a készüléket és annak csatlakozási felületeit a lefoglalást elszenvedő által is aláírt öntapadós vagy leragasztott papírokkal biztosítjuk, hiszen ezek sérülése, leválása esetén nem bizonyítható az eszközök lefoglaláskori állapota.)
11. Ezt követően nyílik majd lehetősége a szakértőnek vagy a szaktanácsadónak, hogy a bitazonos másolat készítését követően a másolaton szakértői munkát, keresést hajtson végre. A bűnjelzsák kibontása az érintettek előzetes kiértesítését követően jegyzőkönyvi rögzítés mellett lehetséges, ha arra a szakértőnek történő megküldés előtt szükség van.

Bontható digitális eszközök esetén lehetőség van rá, hogy egyenként rögzítsük az eszközben található adathordozók gyártmányát, típusát, egyedi sorozatszámát – természetesen minden esetben fényképek készítése mellett az eszközről és a szerelési folyamatról. Ennek akkor lehet jelentősége, ha a szakértő kirendelését megelőző ajánlatkéréshez pontos információkat szeretnénk megadni. Itt tehát három lehetőség van:

- a helyszínen rögzítjük az eszközök tulajdonságait,
- későbbi bűnjelzsák bontásakor vesszük fel az adatokat,
- a szakértő az ajánlatát hiányos adatok alapján adja meg, ami később az ajánlat kibővítéséhez vezethet.

Nem bontható vagy lezárt burkolatú digitális eszközök esetén rögzíteni kell az eszköz gyártmányát, típusát, egyedi sorozatszámát. Fontos, hogy hiteles igazságügyi másolatot készíteni megfelelő hardver (írásvédő) és/vagy szoftver segítségével lehetséges. A másolási folyamat nem változtathatja meg az eredeti adatot. Az igazságügyi másolás eredménye lehet hiteles másolat *(forensic clone)* vagy hiteles lemezkép *(forensic image).* Előbbinél egy 4GB-os pendrive-on lévő 3MB-os kép másolata kb. 4GB-os lesz, míg az utóbbinál csak kb. 3MB-os. Ezek az eszközök (például írásvédő) csak kiemelt rendőri egységeknél állnak rendelkezésre. Az általános bűnügyi munkában szükséges szoftverek (FTK Imager)[21] alkalmazásának szabályai gyakorlati foglalkozásokon kerülnek ismertetésre. Az azonos bittartalmat egy kódolással generált ellenőrzőösszeg (hash-kulcs) igazolja. Ha az eredeti adatot akár egy bittel is módosítják, akkor az újragenerált kód nem lesz azonos. Ezzel biztosítható az adatok integritása.

8.2.13. Általános eljárás a mobilkommunikációs eszközök lefoglalása esetén

Az eszközt működésben tartani kizárólag akkor szükséges, ha az ügy során észszerűen feltételezhető, hogy az észlelt biztonsági elemek vagy titkosítás akadályoznák a *post mortem* – azaz kikapcsolt állapotú – szakértés hatékonyságát. Ebben az esetben a mobil kommunikációs eszközt bekapcsolva kell tartani, de a távközlési hálózattól el kell szigetelni (például Faraday-kalitka segítségével), valamint biztosítani kell az eszköz folyamatos tápellátását. Bekapcsolva lefoglalt eszköz hálózattól való elszigetelése azért indokolt, mert a felhasználó távolról megsemmisítheti az eszközön tárolt digitális bizonyítékokat, illetve a normális hálózati működés során is megváltozhatnak a készülékben tárolt digitális bizonyítékok.

8.2.14. A szemle

A bűncselekmény elkövetésével érintett rendszer alaposabb vizsgálata lehet szükséges a bűncselekmény elkövetője által hátrahagyott nyomok összegyűjtése és rögzítése érdekében. A vizsgálat a szemle szabályai szerint hajtható végre. A régi Be. alapján szemlét

[21] FTK Imager. Elérhető: https://accessdata.com/product-download/ftk-imager-version-3.2.0 (A letöltés dátuma: 2018. 09. 19.)

a bíróság, illetőleg az ügyész rendel el és tart, ha a bizonyítandó tény felderítéséhez vagy megállapításához személy, tárgy vagy helyszín megtekintése, illetőleg tárgy vagy helyszín megfigyelése szükséges.[22] A szemle mint bizonyítási cselekmény lehetőséget biztosít a nyomozó hatóságnak, az ügyészségnek, illetve a bíróságnak arra, hogy a bizonyítandó tény megállapítása érdekében, vagy amennyiben a bizonyítás szempontjából indokolt, tárgyat, személyt vagy helyszínt megfigyeljen. A szemlénél, ha a hatóság úgy ítéli meg, vagy valamilyen körülmény indokolja, szakértőt is lehet alkalmazni, vagy amennyiben az információs rendszer vagy adathordozó átvizsgálása valami miatt különleges szakértelmet igényel, az elektronikus bizonyítékok összegyűjtésére szaktanácsadó vehető igénybe, aki a későbbiekben már nem rendelhető ki szakértőként. A szemle alkalmával a bizonyítás szempontjából jelentős körülményeket részletesen rögzíteni kell. A szemlén fel kell kutatni és össze kell gyűjteni a tárgyi bizonyítási eszközöket, és gondoskodni kell a megfelelő módon történő megőrzésükről. A szemle tárgyáról, ha lehetséges és szükséges, kép- vagy hangfelvételt, illetve képet és hangot egyidejűleg rögzítő felvételt, rajzot vagy vázlatot kell készíteni, és azt a jegyzőkönyvhöz kell csatolni. Az interneten található bizonyítékok mentése általában *online szemle* keretében történik. Az adatmentésben az eljáró nyomozók végzik az ügyben releváns adatok keresését és rögzítését, így az internetes kereséseket, a letöltött fájlokat. Az adatmentés folyamatáról jegyzőkönyv vagy jelentés készül, amelynek részletesnek kell lennie, a folyamatokat, megállapításokat rögzíteni kell. Az adatokról érdemes úgynevezett *image-fájlt* készíteni, amit *hash-kulccsal* kell azonosítani, amelyet egy adathordozón rögzítenek (ez utóbbi lehet CD-/DVD-/BR-disc vagy winchester). E mozzanat részleteit is jegyzőkönyvben kell rögzíteni. Amennyiben az információs rendszer vagy adathordozó részletes átvizsgálása a nyomozó hatóság részéről nem szükséges, bizonyos esetekben az elektronikus bizonyíték adatkérés útján is beszerezhető.

8.2.15. Leplezett eszközök a kiberbűncselekmények felderítésében

A fent nevesített kényszerintézkedések mellett a másik legcélravezetőbb megoldás a nyomozó hatóság kezében a leplezett eszközök alkalmazása, amelyek különösen alkalmasak lehetnek a szervezett bűnözés, a terrorcselekmény megállapítására, a korrupcióval összefüggő bűncselekmények és a kiberbűnözés felderítésére, megelőzésére. A büntetőeljárási törvényben, a Rendőrségről szóló 1994. évi XXXIV. törvényben, továbbá a Nemzeti Adó- és Vámhivatalról szóló 2010. évi CXXII. törvényben, a 100/2018. (VI. 8.) Korm. rendeletben meghatározzák a leplezett eszközök alkalmazásának lehetőségeit, az ügyészi és bírói engedélyhez kötött, valamint ahhoz nem kötött lehetőségeket. A szabályozás említését azért tartom fontosnak, mivel ez az egyik olyan lehetőség a nyomozó hatóság kezében, amellyel a kibertérben elkövetett jogellenes cselekményeket és az azt elkövetőket jóval nagyobb eséllyel lehet tetten érni, mint a nyílt eljárásban meghatározott módszerekkel.

[22] Be. 119. § (1) bekezdés.

8.2.16. A leplezett eszközök igénybevételének általános szabályai

A számítógépes bűncselekmények olyan atipikusnak nevezhető, a társadalmat, gazdaságot és nemzetállamokat veszélyeztető cselekmények, amelyek az elkövetés jellege, annak hatása miatt nemcsak a nyomozó szervekre, hanem a nemzetbiztonsági szervezetekre is feladatokat rónak. „A leplezett eszközök alkalmazása olyan a magánlakás sérthetetlenségéhez, valamint a magántitok, a levéltitok és a személyes adatok védelméhez fűződő alapvető jogok korlátozásával járó, a büntetőeljárásban végzett különleges tevékenység, amelyet az erre feljogosított szervek az érintett tudta nélkül végeznek."[23]

A leplezett eszközök alkalmazása során az azt igénybe vevő szervezetnek be kell tartania:

- a szükségesség,
- az arányosság,
- a célszerűség elvét.

Azaz a leplezett eszközök akkor alkalmazhatók, ha

- megalapozottan feltehető, hogy az eljárás során bizonyítékként felhasználható adatok, információk a leplezett eszköz alkalmazása nélkül nem lennének megismerhetők;
- a leplezett eszköz alkalmazása nem jár az érintett(ek) alapvető jogainak aránytalan sérelmével.

A leplezett eszközök és módszerek alkalmazása a számítógépes bűncselekmények felderítésének talán egyik legfontosabb lehetősége, ugyanakkor nem minden esetben olyan egyszerű, mint a hagyományos bűncselekmények esetében.

8.2.17. Az információs rendszer titkos megfigyelése

A bírói engedélyhez kötött leplezett eszközök egyike – ahogyan az előzőekben is említettem – az információs rendszer titkos megfigyelése. Az eszköz alkalmazása során az arra feljogosított szerv bírói engedéllyel az információs rendszerben kezelt adatokat titokban megismerheti, az észlelteket technikai eszközzel rögzítheti. A rögzítés módját a Be. nem határozza meg, így az a megfigyelt személytől, a bűncselekmény jellegétől és a helyszín adott tulajdonságaitól kiterjedhet:

- a rendszerben tárolt adatok tartalmára, esetleg a metaadatokra,
- a rendszerhez történő hozzáféréshez szükséges jelszavakra, felhasználó azonosítókra,
- a rendszeren keresztül történő kommunikáció megfigyelésére, megismerésére,
- a rendszert használók megismerésére (hang- és képrögzítésre).

Az információs rendszer titkos megfigyelése történhet közvetlenül és közvetetten; a számítástechnikai eszközön egy kívülről feltelepített program segítségével, valamint

[23] Be. 214. § (1) bekezdés.

a számítógépet megfigyelő kép-, illetve hangrögzítésre alkalmas eszköz elhelyezésével [Be. 232. § (3) bekezdés, a hely titkos megfigyelése], illetve ennek a két rendszernek a kombinációjával együttesen.

8.2.18. Az előkészítő eljárás

Az új büntetőeljárásról szóló törvény a nyomozásokban nagyobb szerepet szán az ügyészségnek mint közvádlónak mind a vizsgálati, mind pedig a felderítési szakban. A törvény szerint az ügyészség nyomoz, felügyeli a felderítés törvényességét, valamint irányítja a vizsgálatot. Az ügyészség előkészítő eljárást végez, és a más szerv által végzett előkészítő eljárásban ellátja az e törvényben meghatározott feladatait.[24] A kibertérben elkövetett deliktumok során az előkészítő eljárásnak kiemelt jelentősége van, hiszen a hagyományos bűncselekményekkel ellentétben magasabb a látencia, valamint a bizonyítást is sokban nehezíti a nemzetközi és technikai jellege is. Előkészítő eljárást a nyomozó hatóság vagy az ügyészség folytathat le annak érdekében, hogy megállapítsák, hogy a bűncselekmény gyanúja fennáll-e.[25] Maga az előkészítő eljárás nem más, mint a leplezett eszközök alkalmazására feljogosított szerv által folytatható eljárás, valamint nyílt eszközökkel is folytatható adatszerzés, amit a törvényben meghatározott szervezetek és azok megsegítésére a rendőrség belső bűnmegelőzési és bűnfelderítési feladatokat ellátó szerve, illetve a rendőrség terrorizmust elhárító szerve is végezhet. Az előkészítő eljárás az egyik legalkalmasabb jogintézménye lehet annak, hogy a hatóság egyszerű gyanú esetén saját monitorozó tevékenységet végezve a törvényben meghatározott eljárás lehetőségével éljen, és a rendelkezésre álló idő – hat hónap, egyes esetekben kilenc hónap – alatt bűncselekmény elkövetésének fennállását bebizonyítsa, vagy épp elvesse. Bármely bűncselekmény miatt folytatható (így nincs megkötés sem a büntetési tétel, sem pedig a bűncselekmény típusa tekintetében), így a kibertérben elkövethető valamennyi deliktum miatt, saját hatáskörben eljárva a nyomozó hatóságok vagy az ügyészség megkezdheti az eljárást. Az előkészítő eljárás esetében elvégezhető adatszerző tevékenység a rendelkezésre álló és a törvényben meghatározott szervezetek nyilvántartásaiból és a törvényben még nem szabályozott OSINT-tal (*Open Source Intelligence* – nyílt forrású információgyűjtés) is elvégezhető. Az OSINT-tevékenység törvényben történő szabályozásával kapcsolatban nem vagyok meggyőződve annak szükségességéről, ugyanakkor az azáltal szerzett bizonyítékok hitelessége, felhasználhatósága kérdéseinek tisztázása viszont időszerű lenne már. A leplezett eszköz is igénybe vehető az előkészítő eljárás során, de csak azzal a gyanúsítottal szemben, aki a bűncselekmény elkövetőjeként szóba jöhet, és az ő tartózkodási helyének megállapítása, elérhetőségének megismerése céljából. A kiberbűncselekmények esetében az elkövetők megismerése, felderítése mindig nehézséget okoz az internetes felhasználók anonimitása miatt. A bűnözők számára egyre népszerűbb a kibertér, mivel az azon keresztül folyó kommunikáció ténye a hatóságok számára sokszor nehézségekbe ütközött. Amennyiben az unió kívánságát figyelembe vesszük, miszerint a kibertér ne a bűnözők menedéke legyen, úgy további szabályozásokra még szükség lenne, anélkül, hogy a szólás- és véleménynyilvánításhoz fűződő jogok sérülnének.

---

[24] Be. 25. § (1)–(3) bekezdés.

[25] Be. 340. § (1) bekezdés.

8.2.19. Az előkészítő eljárás során alkalmazható ügyészi engedélyes leplezett eszközök

A leplezett eszközök alkalmazásának előnye, hogy a bűncselekményt elkövetővel szemben az annak végrehajtására feljogosított szerv – azért, hogy az eljárás célját titokban tartsa – a bűncselekményre vonatkozóan információkat, adatokat gyűjthet anélkül, hogy arról az adott személy értesülne. A számítógépes környezetben elkövetett gazdasági, illetve tartalombűncselekmények, valamint a terrorcselekmények bizonyítása esetében a rendelkezésre álló leplezett eszközök alkalmazása nagyobb sikerrel kecsegtethet, mint a korábbi Be.-ben szabályozott lehetőségek.

8.2.20. A fizetési műveletek megfigyelése

A fizetési műveletekre vonatkozó új eljárásjogi szabályozás különösen alkalmas lesz az információs rendszer felhasználásával elkövetett gazdasági bűncselekmények felderítésére és vizsgálatára. Bármelyik bűncselekmény elkövetésének legfontosabb bizonyítása lehet a pénz útjának nyomon követése, az illegális forrásból származó jövedelmek felderítése, de a kibertérben elkövetett bűnözésnél – ahol sokszor csak egy bankszámlaszám ismert, és esetleg egy fiktív vagy hajléktalan személy, ahol a számlák közötti átvezetések a netbankolásnak köszönhetően bárhonnan és bármikor intézhetők – a fizetési műveletek határozott időtartamra történő megfigyelésének köszönhetően a pénz mozgása, a számlák birtokosainak tevékenysége valós időben válik nyomon követhetővé, és nem napokkal vagy esetleg jóval később beszerezhető adatokból ismerhető meg. Fizetési művelet megfigyelésének számít például a pénzforgalmi számlával kapcsolatos valamennyi fizetési művelet vagy a fizetési műveletekre vonatkozó adatok rögzítése, továbbítása.

A fizetési műveletek megfigyelése legfeljebb három hónapra rendelhető el, amelyet az ügyészség egy alkalommal legfeljebb további három hónappal hosszabbíthat meg. A megfigyelés alatt a fizetési műveletek felfüggeszthetők legfeljebb két napig, de ennek tényéről a pénzintézet – a szolgáltató – sem az érintettnek, sem harmadik félnek nem adhat tájékoztatást.

A kriptovalutákkal kapcsolatos műveletek mint fizetési műveletek megfigyelésének szabályai jelenleg még nem kivitelezhetők. A probléma egyik oka, hogy a fizetési művelet nem függeszthető fel, hiszen nincs számlavezető bank a digitális pénz mögött, valamint a 100/2018. (VI. 8.) Korm. rendeletben meghatározott szabályok szerint a szolgáltatót tájékoztatni kell az eljárásról, ami a kriptovaluták esetében nem lehetséges.

8.2.21. Álvásárlás

Az ügyészség engedélyével a bűncselekménnyel feltehetően összefüggésbe hozható dolog vagy annak mintája megszerzésére vagy szolgáltatás igénybevételére, az eladó bizalmának erősítése céljából a bűncselekményre vonatkozó tárgyi bizonyítási eszközt eredményező dolog megszerzésére vagy szolgáltatás igénybevételére, az elkövető elfogásának

elősegítésére irányuló színlelt megállapodás köthető és teljesíthető.[26] Az álvásárlás tehát nemcsak kézzel fogható dolog, hanem bármilyen szolgáltatás igénybevételére alkalmazható (feltételezhetően a dark net esetében bitcoinért, vagyis kriptovalutáért megszerezhető illegális szolgáltatás vagy dolog is érthető alatta). Az álvásárláshoz fedett nyomozó vehető igénybe.

8.2.22. Fedett nyomozó alkalmazása[27]

A fedett nyomozó feladata a kibertérben elkövetett bűncselekmények esetén speciálisabb lehet, mint a fizikai térben végzett munkájuk, hiszen amellett, hogy a technikai eszközök sokszor a segítségükre lehetnek egy-egy feladat elvégzése során, ugyanakkor hátráltató tényező is az, hogy ismerniük kell a kibertérben alkalmazott nyelvezetet, a szakzsargont, és nem utolsósorban nehezítésként előfordulhat, hogy a bűnözővel nem kerülnek kapcsolatba személyesen. A Be.-ben a fedett nyomozó alkalmazására legfeljebb hat hónapra van lehetőség az ügyészség engedélyével, amely alkalmanként hat hónappal meghosszabbítható. A büntetőeljárás céljának végrehajtása érdekében „[…]

a) bűnszervezetbe történő beépülés,
b) terrorista csoportba vagy terrorcselekmény feltételeinek biztosításához anyagi eszközt szolgáltató vagy gyűjtő, továbbá terrorcselekmény elkövetését vagy terrorista csoport tevékenységét anyagi eszközök nyújtásával vagy egyéb módon támogató szervezetbe történő beépülés,
c) álvásárlás,
d) rejtett figyelés végrehajtása,
e) […] az információ továbbítása vagy
f) a bűncselekménnyel összefüggő információk és bizonyítékok megszerzése

érdekében alkalmazható.”[28]

Fedett nyomozó alkalmazása különösen alkalmas lehet olyan bűncselekmények elkövetésének bizonyításában az előkészítő eljárás vagy a felderítés[29] során, amikor az ügy bonyolultsága, az abban részt vevő személyek összetartása miatt egyébként lehetetlen lenne a bizonyítékok megszerzése vagy azok biztosítása.

Ilyen bűncselekmény lehet különösen a kritikus infrastruktúrák elleni támadások malware-rel vagy a gyermekpornográfia bűncselekmény bizonyítása, amikor is az elkövetők zárt csoportokban kommunikálnak egymással titkosított csatornákon, így a szervezetbe történő beépülés, a tagok megismerése, a bűncselekmény helyének lokalizálása során lehet kiemelkedő jelentősége a munkájuknak.

---

[26] Be. 221. §.
[27] Be. 222. §.
[28] Be. 222. § (2) bekezdés.
[29] A nyomozás és az előkészítő eljárás részletes szabályairól szóló 100/2018. (VI. 8.) Kormányrendelet 133. §.

„Nem büntethető a fedett nyomozó az alkalmazása során elkövetett bűncselekmény, szabálysértés vagy közigazgatási bírsággal sújtandó szabályszegés miatt, ha annak elkövetése

a) a fedett nyomozó alkalmazásának eredményességéhez, az alkalmazással elérni kívánt bűnüldözési célhoz szükséges, és az alkalmazással elérni kívánt bűnüldözési érdek jelentősebb, mint a fedett nyomozó felelősségre vonásához fűződő érdek,
b) a fedett nyomozó biztonságának biztosítása, lelepleződésének megakadályozása érdekében szükséges, és a fedett nyomozó biztonságával, lelepleződésének megakadályozásával kapcsolatos érdek jelentősebb, mint a fedett nyomozó felelősségre vonásához fűződő érdek, illetve
c) más bűncselekmény elkövetésének megelőzése vagy megszakítása érdekében szükséges, és a bűncselekmény megelőzéséhez vagy megszakításához fűződő érdek jelentősebb, mint a fedett nyomozó felelősségre vonásához fűződő érdek."[30]

8.2.23. A szakértő

A szakértő bevonásának, szerepének fontossága, a szakértő igénybevétele egy büntetőeljárás során mindig is kérdéses. A szakvéleménynek egyre nagyobb szerepe van a bizonyítási eszközök között, hiszen a technika, technológia fejlődésének köszönhetően a korábban még sikertelenül befejezett ügyekben szerzett bizonyítékok értékelhetővé váltak, és a bizonyítás és az elkövető felderítése is egyre sikeresebb lett. A büntetőeljárási törvény alapján, ha a bizonyítandó tény megállapításához vagy megítéléséhez különleges szakértelem szükséges, szakértőt kell alkalmazni.[31] Szakértelmet igénylő kérdésnek, vagyis szakkérdésnek minősíthető minden olyan releváns kérdés, ami nem minősül jogkérdésnek, és a bizonyításhoz szükséges felhasználhatósága szakértelmet kíván. Az új büntető eljárásjogi törvény ismét nem határozta meg a különleges szakértelem fogalmát (ahogy más jogszabályok sem), ennek ellenére a szakértő kirendelése szükségességének mérlegelésekor az alábbi meghatározást kell szem előtt tartani: a jogi szakmától különböző, valamely más tudományos, technikai szakterületre, esetleg művészeti ágra vonatkozó ismereteket takarja. A szakértő a bíróság különleges szakértelmét pótolja, feladata a releváns szakkérdések megvilágítása és értékelése. Ebből következik, hogy a szakértő jogkérdésekben nem nyilváníthat véleményt. Ebből következhetne, hogy a szakértő csak olyan különleges szakkérdésekben adhat véleményt, amellyel kapcsolatban a bíróságnak nincs relevanciája (szubjektív tényező), ami nem zárja ki tehát azt, hogy egyes esetekben a nyomozó hatóság eljáró tagja, aki viszont képességeinél vagy tudásánál fogva bizonyos véleményt adhatna, megtehetné azokat a cselekményeket, amelyekre képes. A szakértő és szaktanácsadó jogszabályi környezete mellett az egyes bűncselekménytípusok vizsgálata során a kirendelésükre ténylegesen a törvényben meghatározott különleges szakértelem miatt kerül sor, vagy pedig a nyomozó hatóság tagjának a „kényelmét", esetleg a tehetetlenségét vagy még rosszabb esetben „mert így szoktuk" hozzáállását tükrözi. A bizonyítás tárgya közé tartozik a szakvélemény, amelynek elkészítése csak az igazságügyi szakértői tevékenységről szóló törvényben meghatározott feltételek

[30] Be. 224. § (1) bekezdés.
[31] Be. 188. § (1) bekezdés.

alapján végezhető.[32] Az igazságügyi szakértő feladata – a hatóság kirendelése vagy megbízása alapján –, hogy a tudomány és a műszaki fejlődés eredményeinek felhasználásával készített szakvéleménnyel döntse el a szakkérdést.[33] Szakkérdésnek minősülnek azok a vizsgálatok, amelyek elvégzéséhez különleges szakértelem szükséges (például halott személy esetében DNS-vizsgálat, mérgezéssel összefüggő toxikológiai vizsgálat stb.) A szakértő feladata, hogy az adott ügyben a hatóság által történt kirendelés alapján, a legjobb tudása szerint, pártatlanul, a szakértői kirendelő határozatban feltett kérdésekre a törvényben meghatározott határidő alatt befejezze a vizsgálatot. De a szakértőnek nem feladata, hogy jogkérdésben döntsön. Vagyis az, hogy a hatóság egy cselekményt bűncselekménnyé minősítsen, vagy a pontos tényállás meghatározását a szakértőtől várja, már nem tartozik a különleges szakértelem alá. Ugyanúgy igaz ez a kiberbűncselekmények esetében is, még ha az eljáró nyomozó a legkevesebb informatikai ismerettel is rendelkezik, akkor sem várhatja el az általa kirendelt informatikai szakértőtől, hogy minősítse az adott cselekményt.

8.2.24. Szakértő, szaktanácsadó és eseti szakértő

Szakértő alkalmazására akkor van tehát szükség, ha a bizonyítandó tény megállapításához vagy megítéléséhez különleges szakértelem szükséges.[34] A meghatározás nem is feltétlenül szükséges, hiszen a különleges szakértelem szubjektív fogalom, ráadásul azt sem fejti ki a jogalkotó, hogy az adott szakértelem valamilyen különleges eszköz felhasználásával vagy pedig a szakember különleges tudásával függ össze. Az informatikával kapcsolatos ismeretek igen széles körben mozognak. Kezdve azzal, hogy a jogalkalmazók körében annak ismerete, hogy melyik mobileszköz, számítógép milyen típusú operációs rendszerrel működik, vagy melyik futtatható rajta, egészen a komoly informatikai tudást igénylő programozási kérdésekig, eltérést mutat, amely összefügg az életkorral, a tanulással és a nyitottsággal az új tudás felé. A rendőrségen dolgozó nyomozók tudása tekintetében is erős eltérések mutatkoznak, amit még nehezít az is, hogy az informatikai eszközök szinte valamennyi bűncselekmény vagy szabálysértés esetében megtalálhatók mint bizonyítékot hordozó eszközök, így az sem teljesen egységes, hogy milyen esetekben elég egy egyszerű megállapítás. Ehhez még hozzátartozik, hogy semmilyen iránymutatás, állásfoglalás nem született arra vonatkozóan, hogy mely típusú vizsgálatok esetében szükséges a szakértő kirendelése, és mely esetekben elég, ha azt rendőri jelentés formájában (amely teljes bizonyító erejű okirat) az ügy gazdája végzi el. A szakértő szerepe a büntetőeljárás során a rendelkezésre bocsátott adatok, eszközök vizsgálata a feltett kérdésekre, ezáltal a bizonyítékok szolgáltatása. Az eseti szakértő olyan – az eljárásban megállapítandó vagy megítélendő jelentős tény vagy egyéb körülmény megállapításához vagy megítéléséhez – megfelelő szakértelemmel rendelkező természetes vagy jogi személy, aki nem igazságügyi szakértő; valamint olyan igazságügyi szakértő, aki az igazságügyi szakértői szakterületekről, valamint az azokhoz

[32] 2016. évi XXIX. törvény az igazságügyi szakértőkről, 5–10. §.
[33] Az igazságügyi szakértőkről szóló 2016. évi XXIX. törvény 3. § (1) bekezdés.
[34] Be. 188. § (1) bekezdés.

kapcsolódó képesítési és egyéb szakmai feltételekről szóló rendeletben meg nem határozott szakterületen ad szakvéleményt.[35]

A szakértői törvény szerint eseti szakértő is igénybe vehető, ha

- az adott szakterületen nincs bejegyzett igazságügyi szakértő,
- az adott szakterületen – időszakos hiány vagy egyéb szakmai ok miatti hiány okán – a bejegyzett igazságügyi szakértők egyike sem tud eleget tenni a kirendelésnek, vagy
- az adott szakterület nem szerepel a miniszter rendeletében felsorolt szakterületek között.

A jogalkotó a 9/2006. (II. 27.) IM rendelet mellékleteiben határozza meg azokat a szakterületeket és az azokhoz tartozó felsőfokú végzettségeket, amelyek igazságügyi szakértői tevékenység végzésére jogosítanak:

- a tűzvédelmi, valamint személy- és vagyonvédelmi területeken,
- orvosi, továbbá egyes pszichológiai és biológiai területeken,
- munkabiztonsági területen,
- mező- és erdőgazdálkodási, valamint az élelmiszeripari területeken,
- közlekedési és az ipari területeken,
- informatikai és hírközlési területeken,
- környezetvédelmi, a természetvédelmi és a vízügyi területeken,
- kulturális területen,
- gyógypedagógiai és egyes pszichológiai területeken,
- közgazdasági, vámügyi és egyes pénzügyi területeken,
- lakás- és építésügyi, településrendezési, valamint az idegenforgalmi területeken,
- kriminalisztikai területeken,
- audiovizuális média területén,
- titokvédelmi területen.

Abban az ügyben, amelyben számítástechnikai eszköz vagy az azon tárolt adat került lefoglalásra, és szükséges annak vizsgálata, mindenképpen fel kell tenni a kérdést: biztos, hogy ki kell rendelni szakértőt az adott ügyben? A kérdés megválaszolásakor mérlegelni kell, hogy a szakértő, még ha a legcsekélyebb vizsgálatot is végzi, mindig időt vesz el, és növeli a bűnügyi költséget, amely a végén nem feltétlenül terül meg az államnak. Jogszabály meghatározhatja azokat a szakkérdéseket, amelyekben meghatározott szakértő jogosult véleményt adni.[36] Milyen vizsgálatok végezhetők el a szakértő igénybevétele nélkül?

- Egy adott informatikai vagy mobileszköz típusának, IMEI-, IMSI-számának megállapítását a nyomozó hatóság bármely tagja el tudja végezni, még abban az esetben is, ha a készüléken nem látható ez az információ.
- Amennyiben a mobiltelefonon lévő információk hozzáférhetők, úgy az abban tárolt fényképek, telefonkönyv, kimenő, bejövő, nem fogadott hívások mind a telefon menüjéből, mind pedig a szolgáltatótól beszerezhetők, az ügy előadója önállóan képes megnézni. Ugyanez vonatkozik az üzenetekre is.

[35] Az igazságügyi szakértőkről szóló 2016. évi XXIX. törvény 2. § (2) bekezdés.

[36] Be. 188. § (3) bekezdés.

- Amennyiben a számítástechnikai rendszer hozzáféréséhez szükséges jelszó rendelkezésre áll, arról természetesen feljegyzést kell készíteni, az abban tárolt adatok tulajdonságaihoz, kiterjesztésükhöz, típusának megállapításához szintén nem kell szakértő kirendelése.

8.2.25. Az igazságügyi szakértő kirendelésének szükségessége

Jelenleg általánosan elmondható, hogy a kibertérrel összefüggő bűncselekmények esetében a nyomozó hatóság azért rendel ki szakértőt, mert vagy félnek attól, hogy a digitális bizonyítékot nem ismerik fel, eljárási hibát követnek el a kényszerintézkedés végrehajtásakor, az ügy fajtája ténylegesen indokolja, vagy az ügyben eljáró ügyészség csak a „pecsétes" papírt fogadja el, és a hatóság tagja által készített jelentést, amely egyébként közokiratnak minősül, nem fogadja el, hanem szakértő kirendelését írja elő. A szakértőtől várják el azt a szaktudást, amivel nem rendelkeznek. De ne várjuk el, hogy a szakértő minden esetben az ügy kellő ismerete nélkül képes elvégezni az ügygazda munkáját, és a vonatkozó törvény értelmében ez nem is az ő feladata.

Annak meghatározását, hogy az adott ügyben milyen tárgyi bizonyítékra van szükség, és azt milyen kényszerintézkedéssel kell beszerezni, ne a kirendelt szakértőtől várjuk el. A kirendelő határozatban a pontosan meghatározott tényállás, az adatkérés és a nyílt információgyűjtés során beszerzett adatok szükséges mértékű tájékoztatása hozzájárul a fölösleges szakértői vizsgálatok elvégzéséhez és a kiegészítő szakvélemény készítéséhez, továbbá a bűnügyi költség fölösleges növeléséhez.

8.2.26. Igazságügyi informatikai szakértő kirendelése, az igazságügyi szakértő jogai és kötelezettségei

A kirendelésre vonatkozóan általában a szokásjog játszhat szerepet, pedig egyes esetekben az adott kérdés megválaszolása saját hatáskörben is megoldható lenne. Az igazságügyi szakértővel kapcsolatban elvárható magatartás, hogy úgy kell eljárnia, mint ahogyan azt kirendelője (az ügy előadója) tenné, ha rendelkezne olyan különleges szakértelemmel, amelyre vonatkozóan szakértő bevonását látta szükségesnek. A szakértőtől elvárható tehát az az ismeret és jártasság, amely biztosítja számára, hogy a kirendelésekor birtokába került informatikai eszközök vagy elektronikus adatok vizsgálata úgy történjen, hogy egyrészt a kirendelő határozatban megadott tényállásnak megfelelően a feltett kérdésekre teljes mértékben válaszoljon, kétség se férjen hozzá, hogy azok megőrizték eredetiségüket, változatlanságukat. Az elkészített szakértői véleménynek érthetőnek, világosnak kell lenni, hogy az alkalmas legyen a büntetőeljárásban a további felhasználásra. Nem utolsósorban pedig a szakértő kötelessége a számára átadott tárgyak, eszközök, adatok eredetiségének a megőrzése és a szakértői vélemény elkészítésével együtt a hatóság számára történő visszaadása.

A kirendelt szakértő köteles és jogosult mindazokat az adatokat megismerni, amelyek a feladatának teljesítéséhez szükségesek, e célból

a) az eljárás ügyiratait – a törvényben meghatározott kivételekkel – megismerheti,
b) az eljárási cselekményeknél jelen lehet,

c) a terhelttől, a sértettől, a tanútól, a vagyoni érdekelttől, az egyéb érdekelttől és az eljárásban kirendelt szakértőtől felvilágosítást kérhet,
d) a kirendelőtől újabb adatokat, ügyiratokat és felvilágosítást kérhet,
e) a kirendelő felhatalmazása alapján a neki át nem adott tárgyi bizonyítási eszközt, elektronikus adatot megtekintheti, megvizsgálhatja, mintavételt végezhet.

A szakértő a vizsgálat során személyt és tárgyi bizonyítási eszközt, elektronikus adatot tekinthet és vizsgálhat meg, a személyhez kérdéseket intézhet.[37] Ha a szakértő olyan tárgyi bizonyítási eszközt vagy elektronikus adatot vizsgál meg, amely a vizsgálat folytán megváltozik vagy megsemmisül, annak egy részét lehetőleg az eredeti állapotban úgy kell megőriznie, hogy az azonosság, illetve a származás megállapítható legyen. A kirendelő meghatározhatja azokat a vizsgálatokat, amelyeket a szakértőnek a kirendelő jelenlétében kell elvégezni, ezáltal biztosítva van annak lehetősége, hogy a nyomozó hatóság a a vizsgálatokban aktívan részt vegyen, ezáltal folyamatosan figyelemmel kísérje a szakvélemény elkészítésének menetét. Az új szakértői törvény a szakértői vélemények tartalma vonatkozásában az alábbi kötelezettségeket fogalmazza meg.[38]

„A szakvéleménynek tartalmaznia kell
a) a leletet,
b) a vizsgálat módszerének rövid ismertetését,
c) a szakmai ténymegállapításokat,
d) a szakértő véleményét,
e) ha az ügyben korábban vizsgálat lefolytatására került sor, és a kirendelés erre kiterjed, a korábbi vizsgálatra vonatkozó adatok és megállapítások értékelését,
f) a módszertani levélre történő utalást, illetve a módszertani levélben foglaltaktól történő eltérés esetén ennek indokait."

A szakértő – valamennyi típusú igazságügyi szakértőt értve alatta[39] – részvételének szükségessége a kiberbűncselekmények nyomozása vagy bármelyik eljárási cselekménye során vita tárgyát képezheti. Nincs egységes álláspont sem a hatóságok, sem a büntetőeljárás egyéb résztvevői – így az ügyészség, bíróság – között annak tekintetében, hogy van-e szükség szakértő kirendelésére, és ha igen, mikor, vagy pedig fölösleges pénzkidobás a legtöbb esetben, hiszen azokat a vizsgálatokat, amelyeket elvégez, azt akár a helyi informatikus vagy rendszergazda is el tudja végezni.

[37] Be. 192. §.
[38] Az igazságügyi szakértőkről szóló 2016. évi XXIX. törvény 47. § (1) bekezdés.
[39] Az igazságügyi szakértők típusát, ahol szükséges, pontosan meg fogom határozni. Amikor a szakértő kifejezést használom, akkor mint gyűjtőfogalmat értem alatta.

8.2.27. A szakértő vagy szaktanácsadó igénybevételével kapcsolatban felmerülő elvárások, feltételek

A régi büntetőeljárásról szóló törvény alapján csak abban az esetben szükséges a szakértő kirendelése, ha a bizonyítandó tény megállapításához vagy megítéléséhez különleges szakértelem szükséges,[40] ennek szabályozása a 2017. évi XC. törvényben sem változott.

Az eljárásjogunk sajnos nem határozza meg a *különleges szakértelem* fogalmát, így előfordulhat, hogy még abban az esetben is ki kellett rendelni a szakértőt, amennyiben a nyomozó hatóság tagja rendelkezik a szakkérdés megválaszolásához szükséges képességgel, tudással (esetleg a megfelelő végzettsége is megvan hozzá, de mégsem szakértő), pusztán azért, hogy ezáltal bizonyítási eszközt szolgáltasson a nyomozás során. Ugyanakkor a nyomozás során a szakértő által készített szakvélemény részbizonyítéknak minősül, hiszen az ő feladata a rendelkezésre bocsátott bizonyítékok, valamint az őt kirendelő határozatban feltett kérdésekből levonható következtetések megállapítása, azok alapján a vélemény elkészítése.

A szakértő alkalmazása kötelező, ha

a) a bizonyítandó tény, illetőleg az eldöntendő kérdés személy kóros elmeállapota, illetőleg kábítószerfüggősége,
b) a bizonyítandó tény, illetőleg az eldöntendő kérdés kényszergyógykezelés szükségessége,
c) a személyazonosítást biológiai vizsgálattal végzik,
d) elhalt személy kihantolására kerül sor.

A kiberbűncselekmények esetében a szakértő kirendelése más, mint az eddig ismertetett eljárási szabályok során, mert a kényszerintézkedésnél történő igénybevétele az ügytípusok és a nyomozók felkészültségének függvénye. Az igazságügyi szakértőkről szóló törvény alapján tehát „Az igazságügyi szakértő feladata, hogy a hatóság által kirendeléssel vagy megbízás alapján, a tudomány és a műszaki fejlődés eredményének felhasználásával készített szakvéleménnyel, a függetlenség és pártatlanság követelményének megtartásával döntse el a szakkérdést, és segítse a tényállás megállapítását.”[41] A szakterületek elkülönítése az igazságügyi szakértőkről szóló, korábban hatályos 2005. évi XLVII. tv. 3. § (1) bekezdésében, majd a jelenleg hatályos 2016. évi XXIX. tv. 5. § (5) bekezdésében foglalt felhatalmazás alapján a 9/2006. (II. 27.) IM rendeletben történt meg.

A rendelet az informatika vonatkozásában az alábbi (szak)területeket határozza meg:

- informatikai berendezések, számítógépek, perifériák és helyi hálózatok (hardver),
- informatikai biztonság,
- informatikai rendszerek tervezése, szervezése,
- stúdiótechnika, multimédia területtel összefüggő informatikai tevékenység,
- számítástechnikai adatbázis, adatstruktúrák,
- szoftverek [9/2006. (II. 27.) IM rendelet 6. számú melléklet *A)* pont, MÁTÉ 2017].

Az informatikai szakértő kirendelésével kapcsolatban fontos, hogy ne azért történjen meg annak igénybevétele, mert a hatóság a jogszabályok és/vagy alapvető informatikai tudás birtokában nem képes az ügyben dönteni, hiszen magának a szakvéleménynek az elkészítése időigényes, és esetleg fölösleges bűnügyi költséget generálhat.

---

40 A régi büntetőeljárásról szóló 1998. évi XIX. törvény 99. § (1) bekezdés.

41 Az igazságügyi szakértőkről szóló 2016. évi XXIX. törvény 3. § (1) bekezdés.

A szakértő kirendelése mellett szóló érvek:

- mivel a digitális nyomok változó környezetben keletkeznek, így azok változatlanságának biztosításához az átlagosnál magasabb szakértelemre is szüksége lehet,
- a kutatás és lefoglalás során a szakértő igénybevétele a nyomok rögzítésénél hasznos lehet,
- a tiszta, világos megfogalmazás,
- a bíróság előtt sokszor nagyobb érvényt lehet szerezni a vádnak.

A szakértő kirendelése ellen szóló érvek:

- a nem alapos vagy nem érthető szakértői vélemény nehezítheti a nyomozást, vagy nem megfelelő bizonyítékot eredményezhet,
- esetlegesen a szakértő elfogulatlansága megkérdőjelezhető,
- a szakértés elvégzésére nyitva álló határidő – a 60 + 30 nap – egyes esetekben hosszú, indokolatlanul késlekedhet annak befejezésével,
- sokszor indokolatlanul magas a szakértő díjazása,
- a hatóság nem mindig szakkérdésben veszi igénybe, sokkal inkább az általános ismeretek hiánya miatt.

A szakértő alkalmazása kirendeléssel – határozattal – történik, amelyben többek között meg kell jelölni

a) a szakértői vizsgálat tárgyát és azokat a kérdéseket, amelyekre a szakértőnek választ kell adnia,
b) a szakértő részére átadandó iratokat és tárgyakat, ha az átadás nem lehetséges, az iratok és a tárgyak megtekintésének helyét és idejét,
c) a szakvélemény előterjesztésének határidejét (2016. évi XXIX. tv. 45. §).

Ha a szakvélemény elkészítéséhez sürgős részvizsgálatra van szükség, e vizsgálat kirendelő határozat nélkül, az ügyész vagy a nyomozó hatóság szóbeli rendelkezése alapján is elvégezhető.[42] A szakértő a szakvéleményét két hónapon belül kell, hogy előterjessze. Ez a határidő a szakértő kérelmére egyszer, legfeljebb egy hónappal hosszabbítható. Az eljárási törvény szerint általában egy szakértőt kell alkalmazni egy eljárásban az adott szakkérdésben. Ha a vizsgálat jellege szükségessé teszi, több szakértő is kirendelhető. Ez úgy is történhet, hogy a kirendelés csak a szakértői csoport vezetőjét jelöli ki, és feljogosítja őt arra, hogy a többi szakértőt bevonja. A köztudomású tények meghatározása egyébként szubjektív jellegű a kiberbűncselekmények nyomozása során, hiszen az informatika sok esetben speciális szakértelmet igényelhet, illetve a nyelvezete (általában angol) miatt, az informatikai eszközök gyors változása és sajnos sokszor az életkori sajátosságokból kifolyólag előfordulhat, hogy az ügyészség vagy a bíróság rendel majd ki szakértőt, amennyiben ezek miatt a nyomozás irataiban, a jelentésben, a jegyzőkönyvben foglaltak nem érthetők vagy értelmezhetők.

8.2.28. A szakértő kirendelésének lehetősége

A bíróság, az ügyész, illetőleg a nyomozó hatóság a szakértői névjegyzékben szereplő igazságügyi szakértőt, illetőleg szakvélemény adására feljogosított gazdasági társaságot

[42] Be. 189. § (1)–(2) bekezdés.

(a továbbiakban: gazdasági társaság), szakértői intézményt vagy külön jogszabályban meghatározott állami szervet, intézményt, szervezetet (a továbbiakban: szervezet), ha ez nem lehetséges, kellő szakértelemmel rendelkező személyt vagy intézményt (a továbbiakban: eseti szakértő) rendelhet ki szakértőként. A témában végzett vizsgálataim során feltett kérdésekre adott válaszok alapján a rendőrségnél a következő általános gyakorlatokról szereztem tudomást: a bűnügyi állomány tekintetében a házkutatás és lefoglalás eljárása a bűncselekmények típusától függ. Amennyiben feltehetőleg elektronikus adat kerül lefoglalásra, úgy egy CD-t, DVD-t, esetleg külső merevlemezt visznek magukkal, amelyre a vizsgálni kívánt adatokat kimentik. A saját maguk által vitt eszközöket lefoglalják a büntetőeljárási törvényben előírtaknak megfelelően, majd ezt követően szakértőt rendelnek ki, akinek feladata az adathordozó átvizsgálása, a kirendelő határozatban feltett kérdések megválaszolása. Ugyanakkor, amennyiben nagyobb adat lefoglalása és vizsgálata válik szükségessé, úgy az egész számítógép, illetve informatikai eszköz lefoglalása mellett szoktak dönteni. Arra a kérdésre, hogy milyen módon hozzák el a számítógépeket, informatikai eszközöket, meglepő válasz született: az áramforrásból és a hálózatból eltávolítják, majd ezt követően valamennyi ki- és bemeneti egységet leragasztják, és a rendeletnek megfelelően bűnjelezik, majd szállítják be a kapitányságra vagy közvetlenül az igazságügyi informatikai szakértőhöz. A lefoglalás tekintetében nincs protokoll, hanem az ügy előadója sokszor saját elgondolása szerint dönt arról, hogy kell-e, mikor, és milyen módon történjen meg annak végrehajtása. Az egyenruhás – azaz közrendvédelmi állomány – tekintetében sem sokkal jobb a helyzet. Általában nem fordítanak gondot az oktatásukra, képzésükre. A legmeglepőbb dolog, hogy régi megszokott módszerrel „vizsgálnak" meg egy talált vagy igazoltatás során gyanússá vált mobiltelefont: a *#06# kombinációk leütésével a telekommunikációs eszköz IMEI-számát ismerik meg. Arra a kérdésre, hogy mi a helyzet azokkal az eszközökkel, amelyek jelszóval vagy ujjlenyomattal védettek, nem tudtak válaszolni. A mérlegelés, illetve annak lehetősége, hogy a fent említett kombinációval esetleg bizonyítékokat semmisíthetnek meg, fel sem merült.

8.2.29. A szakértő és a szaktanácsadó

Az elmúlt időszakban nem volt jellemző, hogy a kirendelt szakértő túlterjeszkedett volna a kompetenciáján. Ugyanakkor az ügyészségek általában megengedhetőnek tartják, ha a nyomozó hatóság tagja a kirendelő határozatban arra kéri a szakértőt, hogy a bűncselekménnyel kapcsolatban keressen adatokat, ugyanis ez már a saját kompetenciáján, feladatán történő túlterjeszkedés. Az ügyészségen elfogadhatónak ítélik meg, ha bizonyos esetekben az ügyben eljáró hatóság végzi el az adatállomány elemzését, értékelését, de ők sem tudták meghatározni, hogy pontosan milyen kérdésnél húzható meg a határ. A helyszínen igénybe vett szakértő vagy szaktanácsadó feladata, a számítógép átvizsgálása a hatóság irányítása alatt nélkülözhetetlen lehet. Ugyanakkor, ahogy a táblázatban is megtekinthető, az informatikai szakértők is specializálódnak, így amennyiben nem a szakterületének megfelelő területről ad ki szakvéleményt, úgy az a bizonyítékok értékelésénél nem vehető figyelembe. Ugyanúgy aggályos, ha a szakértő nemcsak az adatok átvizsgálását végzi el, hanem egyes esetekben kijelenti, hogy annak tartalma alapján milyen bűncselekmény elkövetése állapítható meg.

9. Bűnmegelőzés a kiberbűncselekmények területén

Dornfeld László

Az ENSZ meghatározása szerint a bűnmegelőzés „azon stratégiák és intézkedések összessége, amelyek a bűnelkövetés veszélyének, és az egyénekre, valamint a társadalomra potenciálisan káros következményeinek visszaszorítását célozzák a kiváltó okokra irányuló beavatkozásukkal", ugyanakkor a büntető igazságszolgáltatás szerepét is elismeri.[1] A bűnmegelőzés irodalma az elmúlt évszázadban jelentősen kibővült, és a kriminológia egyik legtöbbet kutatott területévé vált. A hagyományos bűnmegelőzés terén számos különböző irányzat alakult ki, a büntetőpolitikán belüli és azon kívüli eszközök igénybevételét irányzó beavatkozással (Borbíró 2011). Ugyan nem lehet elvitatni a büntetések szerepét az elrettentésben, ám az elkövetőn túlmutató, társadalmi mértékű elrettentő erejének (az úgynevezett generális prevenció) mértéke a mai napig vitatott. A bűnmegelőzésben kiemelkedő szerepet töltenek be a kormányok, a minisztériumi és hatósági együttműködések és partnerségek, a közösségi és civil szervezetek, a piaci szereplők és az egyének.[2] A bűnmegelőzési politika nélkülözhetetlen részei az alapelvek, a struktúra (bűnmegelőzési tervek), az implementáció eszközei (tudásbázis kialakítása) meghatározása és ezek átültetése a gyakorlatba (UNODC 2013, 225.). A kiberbűnözés újszerűsége és sajátosságai a kialakult bűnmegelőzési struktúrák számára is kihívást jelentenek. Ezek között említhetjük az online kapcsolódásra képes eszközök (számítógépek, laptopok, táblagépek, mobiltelefonok stb.) egyre növekvő számát és csökkenő árát, amelyek jelentősen növelik a potenciális elkövetők és áldozatok számát; az online teret igénybe vevő emberek nagyobb hajlandóságát arra, hogy deviáns módon cselekedjenek; az anonimitás és a nyomok elrejtésének lehetőségét az elkövetői oldalon; a transznacionális bűnözésből eredő bűnüldözési problémákat és az elkövetési technikák gyors fejlődését (UNODC 2013, 226.). A kiberbűncselekmények prevenciója esetén egyrészt fontos a megfelelő, specializált stratégia kialakítása, a minden érdekelt féllel történő együttműködés, valamint a hagyományos módszerek mellett a technológiai megoldások szerepét is fontos hangsúlyozni.

9.1. Stratégiák

2013-ban az ENSZ által vizsgált 53 állam mintegy egyharmada rendelkezett saját nemzeti kiberbiztonsági stratégiával (UNODC 2013, 227.), amely arány azóta bizonyosan magasabb. Ugyan erős kapcsolat áll fent a kiberbiztonsági és kiberbűnözés elleni stratégiák

[1] ENSZ Gazdasági és Szociális Tanács 2002/13. sz. határozata 3. §.

[2] ENSZ Gazdasági és Szociális Tanács 2002/13. sz. határozata 7–9. §.

között, mégis fontos a kettőt megkülönböztetni egymástól. A fő különbség, hogy míg a kibervédelem egy reaktív tevékenység, addig a kiberbűnözés üldözése aktív magatartást igényel az érintett felektől (9. ábra). A további különbségeket a mellékelt ábra szemlélteti. A jelentősebb hatalmak közül az Amerikai Egyesült Államok, Ausztrália és az Európai Unió az előbbit, míg az Egyesült Királyság, Oroszország és Kína az utóbbit preferálja (LEVIN–ILKINA 2013).

9. ábra

Kiberbűnözés elleni kiberbiztonsági stratégiák

Forrás: SEGER 2011

A nemzeti stratégia megalkotása alapvető lépés a kiberbűncselekmények megelőzésében, hiszen ebben történik meg a működési és stratégiai prioritások meghatározása, amely alapján aztán normatív erejű jogszabály születhet. A stratégia ezen kívül alapdokumentumként szolgálhat a bűnüldöző és igazságszolgáltatási szervek számára saját belső eljárásrendjük kialakításában. A vizsgált stratégiák fele jelölte meg a megelőzést, a magánszektorral való együttműködést és a jogszabályalkotást prioritásként, míg kétharmaduk a nemzetközi együttműködés és a tudatosságnövelés fontosságát hangsúlyozta (UNODC 2013, 228.). A vezető szerep terén nincs általánosan elfogadott szerv: a vizsgált stratégiák mintegy harmada rendőri szervet jelölt meg, hasonló arányban került kijelölésre a feladatra az ügyészség és az igazságügyi minisztérium. Tíz százalék jelölt meg hatóságközi koordinációt, és hasonló arány kommunikációs vagy belügyminisztériumot, kiberbűnözés elleni szervet vagy CERT-et (UNODC 2013, 229–230.). Ez jól mutatja, hogy a legtöbb állam számára a kiberbűnözés elsősorban bűnügyi és nem technológiai kihívás. Kiberbiztonsági vonalon a hazánkban is jelentőséggel bíró nemzetközi dokumentumok közül ki kell emelni az Európai Unió kiberbiztonsági (JOIN/2013/01) és biztonsági [COM (2015) 185] stratégiáját, amelyek megszövegezése az eszközrendszer kialakítása terén egyenrangú prioritást biztosít a kiberbűncselekmények megelőzésének és felderítésének. Különösen fontos megemlíteni, hogy a Magyarország Nemzeti Kiberbiztonsági Stratégiájának [1139/2013. (III. 21.) Korm. rendelet] integráns része a megelőzésre törekvés. Már a dokumentum 1. szakaszában, a célok meghatározása között szerepel a „megelőzésre épülő hatékony védelmi intézkedések" megfogalmazása, a 9. szakasz *a)* és *d–e)* pontja pedig az ország számára követelményként rögzíti a hatékony megelőzést, a megfelelő oktatást, valamint a gyermekek számára biztonságos kibertér kialakítását. A 10. szakaszban megtalálható tényleges feladatok között helyt kapott a kormányzati koordináció, az együttműködés a civil, a gazdasági és a tudományos területek képviselőivel, a felhasználók

és vállalkozások körében tudatosság kialakítása, a megfelelő oktatás és kutatás-fejlesztés és a gyermekvédelem. A kiberbűnözés elleni stratégiák közül példaként hozható az Egyesült Királyság kiberbűnözési stratégiája, amelyet 2010-ben fogadtak el. A dokumentum első fele a kiberbűnözés különböző megjelenési formáira fókuszál, és azokat csoportosítja aszerint, hogy kire jelentenek veszélyt (a felhasználókra, a vállalkozásokra és a kormányzatra). A motiváció terén megkülönbözteti a pénzügyi előnyt eredményező, illetve nem eredményező bűncselekményeket. Ezután a dokumentum második fele a kormányzat, illetve a Belügyminisztérium fenyegetésekre adott válaszait mutatja be. A 39. pont a kiberbűnözés megelőzéséhez szükséges megfelelő védelmi intézkedések szükségességét tartalmazza, azzal az analógiával élve, hogy miként a gépjárművek és az otthonok védelméhez szükséges eszközök fontosak a bűncselekmények megelőzéséhez, úgy ugyanez igaz a kibertérben is. A prevenció számos bűncselekményi formánál és a különböző kormányzati szerveknél is kimondott prioritásként jelenik meg a dokumentumban.

Az átfogó stratégiák mellett szót kell ejteni az egy területre fókuszáló stratégiákról is. Ilyen például a gyermekvédelem területe, amely önmagában is elég jelentős ahhoz, hogy külön stratégia foglalkozzon vele. Az EU 2012-ben fogadta el az *A gyermekbarát internet európai stratégiája* (COM/2012/0196) dokumentumot, amely az Európai Unió, a tagállamok és az ágazati szereplők számára is határoz meg feladatokat. Hazánkban erre a területre fókuszál Magyarország Digitális Gyermekvédelmi stratégiája, amelyet a Digitális Jólét Programról szóló 2012/2015. (XII. 29.) Korm. határozat végrehajtásának részeként, a gyermekek és a személyiségi jogok védelmét szolgáló szabályok és intézkedések hangsúlyosabb érvényesítése érdekében alkottak meg. A dokumentum először meghatározza a digitális gyermekvédelem alapvető fontosságú tételeit, így a káros tartalmak és magatartások felismerését, az oktatás helyzetét, az érintettek szerepét és tapasztalatait. A második fejezet a védelmi megoldásokat (például a szűrőszoftvereket), illetve a gyermekek jogait tekinti át. A harmadik fejezetben a szankcióalkalmazás és segítségnyújtás eszközei kerülnek bemutatásra. A stratégia utolsó nagy része a cél- és eszközrendszert mutatja be.

Ez utóbbin belül a stratégia három pillért különböztet meg: tudatosság és médiaműveltség, védelem és biztonság, végül pedig szankcióalkalmazás és segítségnyújtás. A pilléreken belül meghatározott eszközök igen változatosak, némelyek a gyermekvédelem már meglévő eszközrendszerére támaszkodnak, vagy azt erősítik, mások a digitális kor vívmányainak tesznek eleget. Fontos kiemelni a tudatosítás és médiaműveltség fejlesztésének előtérbe helyezését az első pillérnél, a szűrőszoftverek fejlesztését és elérhetővé tételét, a veszélyes tartalmak korlátozását a másodiknál, a jogsértések monitorozását és adatbázis építését a harmadikban.

9.2. Programok, koordináció, ajánlások

A bűnmegelőzési programok a bűnelkövetés kockázati tényezőit veszik célba, és konkrét akcióterveket tartalmaznak ezek kezelésére, így csökkentve a bűnelkövetést. Ezek száma minden bűncselekmény esetén nő, és igaz ez a kiberbűnözésre is. Számos program kiindulópontja nemzetközi vagy szupranacionális szervezet, így az ENSZ, az EU vagy az Európa Tanács. Az ENSZ Közgyűlésének 65/230. sz. határozata, valamint a Bűnmegelőzési és Bűnügyi Igazságszolgáltatási Bizottság 22/7. és 22/8. sz. határozata kezdeményezte

2010-ben a Kiberbűnözés Elleni Általános Programot, aminek a végrehajtásával az ENSZ Kábítószer-ellenőrzési és Bűnmegelőzési Hivatalát (UNODC) bízták meg (UNODC 2013). Ez korántsem volt előzmény nélküli, ugyanis az ENSZ már ezt megelőzően számos kiberbűnözéssel kapcsolatos határozatot fogadott el, amiben a hatékonyabb globális fellépést, valamint a potenciális veszélyek korlátozását, megelőzését hangsúlyozza. Az Európai Bizottság *A gyermekbarát internet* európai stratégiájának részeként finanszírozza a tagállamokban működő *Safer Internet programokat*.[3] Ezek célja a tudatosság növelése és a digitális írástudás terjesztése a fiatalok, a szülők és a tanárok körében. Hazánkban 2010 óta zajlik a program keretében az iskolások biztonságos internethasználatra való oktatása. A program ezenkívül segélyvonalat és hotline-t is biztosít.

A 2015-ös Európai Bűnmegelőzési Díjra *(European Crime Prevention Award)* 19 tagállam nyújtott be valamilyen tervet. Ennek elsődleges témája volt a gyermekek és az internet problematikája.[4] Ezek közül az egyik a *TABBY (Threat Assessment of Bullying Behavior among Youth) in Internet* kutatás volt, ami az iskolai és online bántalmazás gyakoriságát vizsgálta öt országban (Bulgária, Ciprus, Görögország, Magyarország és Olaszország) 2011–2012-ben. A hazai program négy egymásra épülő modulból állt: a pedagógusok és diákok felkészítése az online bántalmazási esetek felismerésére és kezelésére, első panelfelvétel, érzékenyítő foglalkozások, végül a második panelfelvétel.[5] A kutatás eredményei önmagukban is sokat árulnak el a vizsgált jelenségről, valamint a későbbi iskolai bűnmegelőzési és devianciakezelési programok kidolgozása során a gyakorlatban is hasznosíthatók. Bár a program maga nem gyakorolt hatást az elkövetőkre, az áldozatok bántalmazásnak kitettsége jelentősen csökkent (PARTI et al. 2011). A luxemburgi *Bibi és barátai* program a 3–6 évesek első online tapasztalatait próbálta meg pozitív irányba befolyásolni. Ezeken kívül lengyel és litván online bántalmazás elleni program is volt a megvalósítottak között.

Az Európa Tanács és az Európai Unió 2013 és 2016 között futó közös programja, a Globális Akció a Kiberbűnözés Ellen (*Global Action on Cybercrime,* GLACY) hét ázsiai és afrikai országot érintett, akiket a Számítástechnikai Bűnözés Elleni Egyezmény iránti elkötelezettségük miatt választottak ki. Ennek részeként 135 eseményre került sor, amik a jogalkotástól és a bűnüldöző egységek felállításától kezdve az együttműködésen át a magánszektorral való együttműködésig széles spektrumon igyekeztek a kiberbűnözés elleni fellépést és a megelőzést előmozdítani.[6] A program tapasztalatai alapján indult el 2014-ben a *Cybercrime@Octopus* program.

Az Európai Unió a kiberbűnözés elleni küzdelem részeként, szervezeti alapként létrehozta a Számítástechnikai Bűnözés Elleni Európai Központot (*European Cybercrime Centre,* a továbbiakban: EC3) az Europol keretein belül, a szervezet meglévő infrastruktúrájának a felhasználásával. Ennek stratégiai központja foglalkozik a megelőzéssel és a tudatosság növelésével (DORNFELD 2016). Az EC3 az összegyűjtött adatok alapján elemzi

---

3 Safer Internet Program. Elérhető: https://ec.europa.eu/digital-single-market/en/content/creating-better-internet-kids-0 (A letöltés dátuma: 2018. 06. 01.)

4 EUCPN. Elérhető: https://eucpn.org/sites/default/files/content/download/files/toolbox_8.pdf (A letöltés dátuma: 2018. 06. 01.)

5 Eszter Alapítvány. Elérhető: www.eszteralapitvany.hu/wp-content/uploads/2013/03/Iskolaknak-TABBY-2013.03.12..pdf (A letöltés dátuma: 2018. 06. 01.)

6 Capacity building on cybercrime & e-evidence. Elérhető: https://rm.coe.int/16807069d8 (A letöltés dátuma: 2018. 06. 01.)

a kiberbűnözés kialakult trendjeit, és az ez alapján kiadott ajánlások segítik a hatékonyabb bűnmegelőzést.[7] A szervezet a főszervezője a Kiberbűnözés Megelőzési és Tudatossági Fórumnak, amelyen a tagállamokon kívül uniós szervek is képviseltetik magukat. A rendezvény célja a tevékenységek és kampányok összehangolása, a témába vágó tudásanyag megosztása, új megoldások kidolgozása és a jó gyakorlatok cseréje.[8]

Már 2004 óta működik az Európai Hálózat- és Információbiztonsági Ügynökség (ENISA), amely az Európai Unió, a tagállamok, a magánszektor és az európai polgárok szolgálatában álló hálózat- és információbiztonsági szakértői központ. A szervezet feladatkörét 2013-ban jelentősen kibővítették. Feladata alapvetően a kapcsolódó uniós politikák kidolgozásában és alkalmazásában való részvétel, de segítséget nyújt a tagállamoknak is a felkészültségük fejlesztésében, az együttműködések elősegítésében, a figyelemfelkeltésben és a kutatás-fejlesztésben (Dornfeld 2016). A hazánkban működő Nemzeti Kibervédelmi Intézet részeként operáló Kormányzati Eseménykezelő Központ, valamint a Nemzeti Elektronikus Információbiztonsági Hatóság honlapján riasztásokat ad ki az új fenyegetések és sérülékenységek kapcsán, valamint szabadon elérhető ajánlásokkal és tanácsokkal, tudatosító anyagokkal vesz részt a bűnmegelőzésben.

9.3. Együttműködés a magánszektorral

Az együttműködésnek és koordinációnak a kormányzati szerveken kívül a magánszektorral is nagy jelentősége van. Hiszen a biztonság kialakításában, a jogellenes cselekmények felderítésében az IT-iparág és az internetszolgáltatók is fontos szerepet játszanak. Különösen igaz ez a nyugati világban, amely partnerként kezeli ezeket a szereplőket a kiberbiztonságban. Ennek a szabályozási modellnek az elnevezése a *minden érdekelt fél bevonása,* ahol nagy tér jut a kölcsönös előnyökkel járó együttműködésnek (Dornfeld 2016). Ezen együttműködés kialakításának alapja az, hogy az állam működésének biztosításához elengedhetetlen a kritikus infrastruktúra védelmének biztosítása, ám ezek nagy része magántulajdonban van (Carr 2016). Az ENSZ-felmérésben vizsgált 35 ország mintegy fele rendelkezett már kialakított együttműködési programmal, míg harmadukban nem létezett ilyen és előkészítés alatt sem állt (UNODC 2013, 231.).

A magánszektorral történő együttműködésnek öt elsődleges modellje alakult ki: 1. non-profit globális információmegosztás, 2. osztott közösségi szintű információmegosztás, 3. központi közösségi szintű információmegosztás, 4. zárt kormányzat, 5. informális együttműködés (UNODC 2013, 232.). Más szerzők aszerint tesznek különbséget, hogy van-e az együttműködésben olyan fél, amely hierarchikusan a többiek felett áll. Ezek alapján különbséget tesznek horizontális és hierarchikus együttműködések között (Carr 2016, 54.). A horizontális vagy informális együttműködés elsősorban az angolszász országokra jellemző megoldás, ahol a felek egyenrangú partnerekként vesznek részt, nem jogszabályi kötelezettség, hanem felismert közös érdekek alapján. Az Egyesült Királyság

[7] Europol EC3. Elérhető: www.anacom.pt/streaming/Benoit_Godart.pdf?contentId=1176117&field=ATTACHED_FILE (A letöltés dátuma: 2018. 06. 01.)

[8] Europol. Elérhető: www.europol.europa.eu/newsroom/news/cybercrime-prevention-%E2%80%93-unified-message-towards-online-criminals (A letöltés dátuma: 2018. 06. 01.)

kiberbiztonsági stratégiája például „közös kihívás"-t fogalmaz meg, ahol szükséges „a magánszektor, az egyének és a kormányzat" együttműködése (CARR 2016, 55.). Linder ezzel szemben hat különböző modellt határoz meg, és a neoliberális, illetve neokonzervatív ideológiákhoz köti ezeket. Így például az egyik által felállított modell az „együttműködés mint menedzsmentreform", amely szerint a kormányzati tisztviselők utánozni kezdik partnereiket, és a szigorú bürokratikus szabályalkotás helyett vállalkozói és rugalmas módon kezdenek el működni (CARR 2016, 55–56.). Ennek érdekessége az, hogy jelen esetben a kormányzati szervek idomulnak a magánszektor működéséhez, és nem fordítva. Ennek jelentősége, hogy informális együttműködés – hiába alapul az közös érdeken (DAHABIYEH 2015, 2–4.) – kialakításában nehézséget jelent az, hogy az üzleti élet szereplői gyakran bizalmatlanok az állammal szemben, az állami szervek eljárását túl merevnek tartják. Jól összefoglalja ezt az a vélekedés, hogy „ha az egyetlen eszközöd a kalapács, az egész világ szögnek tűnik" (WOLF 2001). Az együttműködések túlnyomó többsége informális, általában csak a kritikus infrastruktúrát szolgáltatók esetén léteznek kormányzati döntésen vagy jogszabályon alapuló együttműködések (UNODC 2013, 232.). Az együttműködés legtipikusabban információcserére és segítségnyújtásra terjed ki, de hasonlóan gyakori a tudatosság növelése és a jó gyakorlatok cseréje. Jóval kevésbé jellemző a technikai megoldások kidolgozásába, illetve a nemzetközi együttműködésbe történő bevonás, és szinte elenyésző a politikák kialakításában van részvétel (UNODC 2013, 233.).

A Világgazdasági Fórum 2016-os ajánlása öt pontban tartalmaz javaslatokat az együttműködésre.[9] Az első ezek közül az állandó és biztonságos *információs csatornák kialakítása,* valós idejű információmegosztás a CERT-ekkel, valamint a technikai megelőzés eszközeinek és a tapasztalatoknak, illetve a jó gyakorlatoknak a megosztása. Az ilyen szintű információcsere szükségessége összefügg azzal a problémával, hogy nem mindig egyértelmű egy-egy esetben eldönteni, hogy valamilyen technikai hiba vagy pedig kibertámadás történt-e (CARR 2016, 58.). Ráadásul a látencia is igen jelentős a kiberbűnözés esetén, ami vagy abból ered, hogy nem ismerik fel a támadásokat az áldozatok, vagy abból, hogy a közvélemény szemében való bizalomvesztéstől, illetve az üzleti titkaik kitudódásától való félelmükben nem jelentik be azokat (DORNFELD 2015, 29.). Mivel a magánszektor szereplőitől begyűjtött adatok potenciálisan piaci versenytársaikhoz is eljuthatnak, ezért kellő körültekintéssel kell eljárni, és csak olyan információkat megosztani, amelyek nem sértenek üzleti titkot. Ilyen módon csökkenthető a bizalmatlanság a hatóságokkal szemben (BRENNER–CLARKE 2005, 684.). A második javaslat a globális, illetve *regionális szintű együttműködési platformok* felállítását szorgalmazza, ami összefügg a kiberbűnözés mint probléma globális, határokon átnyúló jellegével. Ilyen például az INTERPOL égisze alatt működő Globális Innovációs Komplexum (*Global Complex for Innovation,* IGCI).[10] Hasonló együttműködés létezik az Interpol és a bankkártya-szolgáltatók között, ami a csalás visszaszorítását szolgálja (LI 2007). A negyedik javaslat a korábban már említett bizalmatlansággal összefüggésben a *bizalomépítést,* a *párbeszédet* és a *kapacitásépítést* emeli ki.

[9] World Economic Forum Recommendations for Public-Private Partnership against Cybercrime. January 2016. 6–10.

[10] Interpol. Elérhető: www.interpol.int/About-INTERPOL/The-INTERPOL-Global-Complex-for-Innovation/Implementation (A letöltés dátuma: 2019. 06. 10.)

9.4. Oktatás, tudatosság kialakítása

Az ENSZ Bűnmegelőzési Iránymutatásai kiemeli a közoktatás és a tudatosságnövelés fontosságát. A viktimizációs veszélyek ismerete és a védelmi intézkedések szélesebb körű ismertetése alapvető fontosságú a sikeres bűnmegelőzéshez (UNODC 2013, 234.). A kiberbűnözés viktimizációja erősebben jelentkezik a fejletlenebb országokban, ami azt mutatja, hogy itt még nagyobb szükség van a megfelelő megelőzésre, elsősorban a tudatosság növelésén keresztül.[11] Ennek eszközrendszere meglehetősen széles lehet, internetes figyelemfelhívó kampányoktól kezdve, kiberbiztonsági napok szervezésén keresztül egészen az akadémiai szféra és az oktatás bevonásáig. A kampányokat tipikusan állami szervek készítik nemzeti szinten, de léteznek regionális szintű és techcégek, illetve nonprofit civil csoportok által kezdeményezett események is. Erre lehet példa a Google tevékenysége (UNODC 2013, 236.).

A megfelelő figyelemfelhívó kampány kialakítása meglehetősen nehéz lehet. Egy 2011-es felmérés szerint sok ilyenhez egyáltalán nem kapcsolódik utólagos értékelés, és azt is nehéz eldönteni, hogyan lehet minél költséghatékonyabb módon a megfelelő hatást elérni. Hasonlóan komoly probléma a technikai oldalon, hogy további tréningek és képzések nélkül csak korlátozott hatást képesek elérni. A felmérés szerint a leghatékonyabbak az egyszerű, egy adott csoportot célzó kampányok (UNODC 2013, 236.). A felmérések szerint mára a legtöbb internetfelhasználó az alapvető óvintézkedéseket megteszi internetezés közben.[12] A figyelemfelhívásnak és tudatosításnak így inkább valamely kifejezett veszélyre kell vonatkoznia, például a zsarolóvírusokra vagy a botnetekre, nem kizárólag általánosságokra. Továbbá fontos azt is észben tartani, hogy a javasolt biztonsági megoldások ne legyenek túl bonyolultak, mert ez csökkentheti a felhasználók hajlandóságát, hogy alkalmazzák azokat.[13] Például a gyakorlati javaslatok ellenére meglehetősen valószínűtlen, hogy egy átlagos felhasználó minden szolgáltatáshoz külön jelszót fog használni, ezeket rendszeresen cseréli, és anélkül emlékszik rájuk, hogy bárhová felírná őket. A veszélyekkel kapcsolatos oktatást minél hamarabb szükséges elkezdeni, ugyanis a fiatalok hatványozottan kitettek az interneten található veszélyeknek. Ennek első lépése a köznevelés, ahol szükséges a tanárok továbbképzése is, hogy ők maguk is tisztában legyenek a veszélyekkel, illetve a rájuk adható jó válaszokkal. Ennek céljait jelentősen segítheti az is, ha állandó kapcsolat alakul ki a helyi rendőrség és az iskolák között, így egy gyakorlati tapasztalatokkal is rendelkező előadó tud az oktatási tevékenységen részt venni.

Az akadémiai szféra szerepe változó lehet a megelőzés terén, így például részt vehetnek az oktatásban és a szakemberek képzésében, a jogszabályok és vonatkozó politikák, illetve a technikai standardok és megoldások kidolgozásában. Az egyetemeken gyakran találhatók specializált kutatóintézmények és kiberbűnözési szakemberek is. A kiberbűnözés elleni küzdelemhez felhasználható tudásanyag számos tudományos diszciplínában megtalálható,

---

[11] Comprehensive study of the problem of cybercrime and responses to it by Member States, the international community and the private sector. UNODC/CCPCJ/EG.4/2013/2. 3.

[12] Comprehensive study of the problem of cybercrime and responses to it by Member States, the international community and the private sector. UNODC/CCPCJ/EG.4/2013/2. 12.

[13] Comprehensive study of the problem of cybercrime and responses to it by Member States, the international community and the private sector. UNODC/CCPCJ/EG.4/2013/2. 12.

így többek között a számítástechnikában, a jogban, a kriminológiában és a szociológiában. Az elmúlt évtizedekben egyre nőtt az ezen témákkal foglalkozó folyóiratok és kutatások száma, és az elméleti tudást a gyakorlatban is fel lehet használni (UNODC 2013, 236–237.).

Brenner javaslata a jelenlegi rendszer helyett egy *osztott rendészeti stratégia* létrehozása, ahol nem a rendőrség, hanem az állampolgárok elsődleges feladata a kibertér biztonságának őrzése. Az ő elképzelése szerint a rendőrség feladata ebben a rendszerben az elrettentés és megelőzés lenne, míg a felhasználókat jogszabályok köteleznék bizonyos magatartásokra, így például az illegális tartalmak jelentésére vagy bizonyos szoftverek telepítésére (CHANG 2017). Chang is a lakosság növekvő szerepét emeli ki, felhívva arra a figyelmet, hogy mivel a legtöbb rendszer ugyanolyan zárt forráskódú szoftvereket használ, egy sebezhetőség felfedezése láncreakciót indíthat el (WALL 2008). Jól mutatja ennek potenciális veszélyét a *WannaCry* zsarolóvírus futótűzszerű elterjedése is (NAGY–MEZEI 2017).

9.5. Technológiai eszközök a bűnmegelőzés szolgálatában

A technológia bűnmegelőzési célú felhasználása nem új keletű gondolat, így a kiberbűncselekmények prevenciója terén is hamar felmerült alkalmazása. Ennek elméleti alapja szorosan kapcsolódik a szituációs bűnmegelőzéshez, amelynek lényege szerint a bűnözés azáltal csökkenthető, ha nehezebbé tesszük a bűncselekmények elkövetését, csökkentjük a várható előnyöket vagy növeljük az elkövető kockázatát. Ez a fajta hozzáállás népszerű állami szinten is, így például Nagy-Britannia kibertérrel kapcsolatos politikájában is, ahol az állami kezdeményezések a fejlesztőket a bűnözésre való lehetőségek csökkentésére ösztönzik. Az elmúlt évtizedben két egymástól elkülöníthető modell alakult ki a szakirodalomban: a rendszerek bűnmentessé tétele, illetve a bűnmegelőzés beépítése a rendszerbe.

9.5.1. Modellek

A rendszerek bűnmentessé tétele azon az elképzelésen alapszik, hogy a lehetőségét is meg kell szüntetni a rendszer jogellenes használatának. Ilyen megoldás lehet például, ha egy vállalkozás kizárja a közvetlen bankkártyás fizetés lehetőségét, és csak letéti fizetési rendszerek (például PayPal) közbeiktatásával enged fizetni, ami jelentősen csökkenti a bankkártyás csalások lehetőségét. Hasonló megoldás, ha egy információs rendszer tervezésekor a biztonsági beállítások alapállapotban bekapcsoltak. Ennek a megközelítésnek ugyanakkor sok buktatója van, így például az, hogy a tervezési szakaszban nem határozható meg előre, mennyire sikerült a bűnözési lehetőségeket kizárni, valamint, hogy a mindennapi használatot túlságosan nehezítő védelem esetén az átlagfelhasználók hajlamosak kikapcsolni a védelmi funkciókat, mivel a funkcionalitás fontosabb számukra (WALL 2008, 188.).

A másik megoldás a bűnmegelőzés rendszerbe építése, amelyek közül a legismertebb a felhasználónév-jelszó kombináció, ami szükséges a védett rendszerekbe történő belépéshez. A használható eszközök között kap helyet az adatbányászás is, ami az összegyűjtött és tárolt forgalmi adatok elemzését jelenti, mivel ezek tartalmazzák az összes internetes tranzakciót. Ezzel a technikával számos fontos információ kinyerhető, és a *kockázati társadalom* rendfenntartásának egyik alapköve lehet, ahogy a rendvédelmi szervek közötti

kapcsolatoknak is egyre fontosabb részét képezi az információmegosztás. Az információközvetítés bűnmegelőzésben betöltött szerepét az Egyesült Államokban is felismerték, ahol a 9/11-es terrortámadást követően javasolták az összes fontos nemzeti adatbázis egyesítését (Wall 2008, 189.). Ez nemcsak a kibertérben, de azon kívül is igen hasznos lehet, így például a 2016-os nizzai kamionos terrortámadást is meg lehetett volna előzni, ha megfelelően használják és összevetik a francia listákkal a Schengeni Információs Rendszert.[14] A bűnözéskontroll másik módja lehet a szoftveres bűnmegelőzés beépítése, anélkül, hogy az a hardware-t érintené, ezáltal automatizált, aktív rendfenntartó eszközöket létrehozni. Ilyen lehet például egy olyan honlap létrehozása, ami külsőre valósnak tűnik, és látszólag illegális tartalmakkal van feltöltve, ám ehelyett egy rendőrségi figyelmeztetés fogadja a látogatókat (Wall 2008, 190.). Gyakorlati példaként hozható az Europol *Police2Peer* programja, amelynek részeként a *peer2peer* fájlcserélő rendszereken folyó gyermekpornográfiaterjesztés ellen léptek fel. A rendőrök látszólag gyermekpornográf tartalmú fájlokat tettek közzé, ám ezek a valóságban egy rendőrségi figyelmeztetést tartalmaztak az azt letöltők számára.[15] Ezek a fajta tartalmak azonban ellenkező hatást is elérhetnek: vicces kedvű felhasználók látszólag ártalmatlan címek mögé rejthetik a rendőrségi figyelmeztetésre mutató linket, ami az egyszerű felhasználókban pánikot okozhat. Rosszabb esetben a bűnelkövetők dolga egyszerűsödhet, ha például egy fiatalkorúnak, akitől meztelen képet csaltak ki, megmutatnak egy olyan figyelmeztetést, hogy az ilyen képek készítése bűncselekmény, így további szexuális szolgáltatásokat zsarolhatnak ki belőle. Katyal is azon az állásponton van, hogy a kód megfelelő felhasználása a bűnmegelőzés céljait segítheti elő. Véleménye szerint ehhez az offline bűnmegelőzési eszközökből merítve négy alapelv betartására van szükség: 1. természetes megfigyelés lehetőségének megteremtése; 2. területiség érzésének keltése; 3. közösségépítés; 4. a bűncselekmények célpontjainak védelme. Az első pont alapján például amellett érvel, hogy a zárt forráskódú szoftverek biztonságosabbak, mint a nyíltak. A területiségnél az *ellenőrzött pszeudoanonimitás* mellett foglal állást, vagyis az IP-címek logolását javasolja megoldásként, ahol megmarad az anonimitás, de könnyebbé válik a hatóságok dolga (Chang–Grabosky 2008, 537.).

9.5.2. Tartalomszűrés

A megelőzés technikai megoldásai közé sorolható a tartalomszűrés is. Ez nem más, mint a különböző jogsértő tartalmak kiszűrése, majd eltávolítása vagy más módon történő elérhetetlenné tétele. A szűrésnek három szintje különböztethető meg: az elsődleges szint a felhasználói, ahol a számítógépet használó vagy az azt üzemeltető intézmény állítja be a szűrés mértékét; a második szint az internetszolgáltató által alkalmazott szűrés; míg a harmadik szint pedig az állam által előírt tartalom blokkolása (Parti–Marin 2012, 58.).

Az első szinten történő szűrés egyik fontos eszköze a szűrőszoftverek, ahol a felhasználó maga állíthatja be a szűrni kíván tartalmakat. Az elektronikus hírközlésről szóló 2003. évi C. törvény 149/A. § előírja az internet-hozzáférési szolgáltatást nyújtó

[14] EPP. Elérhető: www.eppgroup.eu/news/Five-lessons-learned-from-the-terror-attacks-in-France (A letöltés dátuma: 2018. 11. 12.)

[15] Europol. Elérhető: www.europol.europa.eu/partners-agreements/police2peer (A letöltés dátuma: 2018. 11. 12.)

szolgáltatónak, hogy a kiskorúak védelmét lehetővé tevő, magyar nyelvű, könnyen telepíthető és használható szoftver letöltését ingyenesen elérhetővé kell tenni. A Gyermekvédelmi Internet-kerekasztal kapcsolódó 5/2014. (IV. 23.) sz. ajánlása javaslatokat fogalmaz meg e szoftverek elérhetősége, telepítése és beállítása, a korlátozása módja és a tevékenységek monitorozása, illetve a riasztások kapcsán; továbbá előírja az oktatási intézmények számára a szoftverek alkalmazását.

A harmadik szinten történő tartalomszűrés egyik alapját az Európai Unió a gyermekek szexuális bántalmazása, szexuális kizsákmányolása és a gyermekpornográfia elleni küzdelemről szóló 2011/93/EU irányelve teremti meg, amelynek *A gyermekpornográfiát tartalmazó vagy azt terjesztő weboldalak elleni intézkedések* címet viselő 25. cikke kötelességként írja elő az ilyen weboldalak eltávolítását, illetve az ezekhez való hozzáférés meggátolását. Ennek hazai jogszabályokba történő átültetése a Büntető Törvénykönyv 77. §-ba foglalt elektronikus adat végleges hozzáférhetetlenné tétele intézkedésként, illetve a büntetőeljárási törvény 335. § szerinti elektronikus adat ideiglenes hozzáférhetetlenné tétele kényszerintézkedésként történt meg. A 23/2003. (VI. 24.) BM–IM együttes rendelet alapján a kényszerintézkedés elrendelésére a nyomozó szerv vezetője tesz előterjesztést az ügyészhez, az előterjesztésnek az egyéb releváns adatok mellett tartalmaznia kell az IP-címet IPv4- vagy IPv6-szabvány szerint és az alhálózati maszkot, a domainnevet, az URL-címet, valamint a portszámot. Ugyan a jogintézmény elsődleges célja a már folyamatban lévő bűncselekmények megszakítása, a megelőzés célját is szolgálja az, hogy ezek a tartalmak elérhetetlenné válnak, így más már nem férhet hozzájuk.

9.5.3. Sweetie-projekt

A holland Terre des Hommes gyermekjogi civil szervezet 2013-ban digitális képalkotási technikával létrehozott egy virtuális filippínó kislányt, és négy kutató 10 héten keresztül megszemélyesítette őt. Ezalatt az idő alatt 20 ezren léptek velük kapcsolatba nyílt chatszobákban, és mintegy 1000 elkövetőt tudtak azonosítani 71 különböző országból.[16] Ugyan ezeket az adatokat átadták a joghatósággal rendelkező hatóságoknak, nagyon kevés esetben indult eljárás, elsősorban a kutatók potenciális ráhatása miatt, amit az elkövetők védekezésként felhozhattak volna. A büntetést nehezíti az, hogy Sweetie csak egy „virtuális áldozata" egy bűncselekménynek, valamint, hogy semmiféle szexuálisan explicit dolgot nem tesz (SCHERMER et al. 2016). Mindezen tényezők megnehezítik azt, hogy a begyűjtött adatok alapján ténylegesen eljárás indulhasson. Az első projekt ezek ellenére sikeresnek volt tekinthető, hiszen világméretű médiafigyelmet kapott, és így sikerült a problémát a figyelem középpontjába állítani. Ennek sikerén felbuzdulva a szervezet elindította a Sweetie 2.0 projektjét, ahol már egy kenyai kisfiút és egy másik filippínó lányt személyesítenek meg. A Terre des Hommes dokumentumaiban maga is proaktív eszközként jellemzi Sweetie-t, aminek segítségével még azelőtt avatkozhatnak be, hogy tényleges bűncselekmény történne. Sweetie ugyan nehezen alkalmazható a bűnözők elítéléséhez, a megelőzésben igen fontos szerepet tölt be, ugyanis elbizonytalaníthatja az elkövetőket, akik sosem tudhatják,

[16] Webcam Child Sex Tourism. Elérhető: www.terredeshommes.org/wp-content/uploads/2013/11/Webcam-child-sex-tourism-terre-des-hommes-NL-nov-2013.pdf (A letöltés dátuma: 2018. 11. 12.)

nem egy virtuális kislánnyal folytatnak-e épp beszélgetést, aki mögött kutatók figyelik tevékenységüket.

9.6. Egyes bűncselekménytípusok megelőzésének kérdései

9.6.1. Agresszió és online megfélemlítés

Az online megfélemlítés *(cyberbullying)* a kutatások fókuszába kerülő egyik új jelenség, aminek sokrétűsége nehézzé teszi a megelőzést. Így például a szándékos, célzott bántalmazást célzó eszközök nem feltétlenül járnak sikerrel olyan esetben, ha valaki hirtelen felindulásból válaszol így egy provokációra. Ugyanígy a bosszúból történő elkövetést célzó eszközök hatástalanok lehetnek azzal szemben, aki csak szórakozásból, trollkodásból végzi a tevékenységét. A különböző motivációkkal és megjelenési formákkal foglalkozik az agressziókutatás, amelynek a kibertérben történő agressziónál nagy jelentősége van. A kutatások tanulsága szerint az online zaklatás elkövetőit legtöbbször a kikapcsolódás igénye, az unaloműzés, a bosszú, illetve a mások feletti hatalom érzete vezérli. A motivációk tanulmányozása és feltárása hasznos tapasztalatokat jelent a jelenség megelőzéséhez, illetve a beavatkozáshoz (Runions et al. 2016, 75.).

A *cyberbullying* ellen nem jelenthet megoldást, ha kikapcsoljuk az áldozat elektronikus eszközeit, és megfosztjuk az internethozzáféréstől, hiszen ezzel tulajdonképpen őt büntetjük meg. A bántalmazás során jelentősége van a családon belüli érzelmi kapcsolatoknak is, a felmérések szerint ugyanis az érzelmi támogatás mérsékelte az online zaklatás negatív következményeit, és csökkentette az ismétlődés veszélyét is. Rajtuk kívül azonban fontos az egészségügyi, iskolai dolgozók bevonása a megelőzésbe, illetve a kortársak, akik egymást támogatva védőhálót nyújthatnak az ilyen próbálkozások ellen. Az érintetteken túl a szemlélőknek is fel kell ismerniük, hogy a bántalmazás sikeréhez az is elegendő, ha passzívak maradnak, és nem sietnek a bántalmazott segítségére (Zsila–Ujhelyi–Demetrovics 2015, 57–58.). Magyarország Digitális Gyermekvédelmi Stratégiája a büntetőeljárás helyett az alternatív vitarendezési mechanizmusokat helyezi előtérbe, és előbbit kizárólag utolsó megoldásként kívánja alkalmazni. Az online megfélemlítésre adott válaszok közül a legnépszerűbbek azok, amelyek valamilyen módon megbirkóznak vele (úgynevezett megküzdési stratégiák). Ilyen például a bántalmazó tiltólistára helyezése/blokkolása, az online név vagy telefonszám megváltoztatása. Léteznek azonban rossz megoldások is a helyzet kezelésére, így például, ha valaki maga is megfélemlítéssel válaszol. Arra azonban már ritkábban, utolsó lehetőségként kerül sor, hogy ezeket az incidenseket szülőkkel, tanárokkal közöljék, ami az életkori sajátosságokon túl abból is ered, hogy úgy érzik, ők nincsenek tisztában a probléma mértékével (Slonje–Smith–Frisén 2012, 5.).

Az online megfélemlítés kezelésének legjobb módja az iskolai megelőzés, illetve beavatkozás. Ilyen például, ha ráébresztjük az elkövetőt, hogy milyen következményekkel járnak tettei az áldozatra nézve. Ennél a bűncselekménynél különösen nagy jelentősége van a tudatosításnak és a felelősségteljes internethasználat oktatásának (Slonje–Smith–Frisén 2012, 6.). A megfelelő szemléletmódot nemcsak az érintettekkel, de a szülőkkel, tanárokkal és a szélesebb társadalommal is meg kell ismertetni. Hazánkban 2015-ben került megrendezésre a Magyar Országos Cyberbullying Konferencia (MOCK), ahol a tudományos

élet képviselői mellett a Nemzeti Média- és Hírközlési Hatóság és a Nemzeti Adatvédelmi és Információszabadság Hatóság tagjai is részt vettek.

9.6.2. Szexuális devianciák

A szexuális vágyak kiélése a kibertérben elkövetett bűnözés másik jelentős csoportja. Az új információs technológiák fundamentálisan eltérő módokon teszik lehetővé a gyermekek és nők kizsákmányolását. A kulturális befolyásuk révén ezek a technológiák jelentősen kiterjesztik az erőszak elfogadásának a mértékét, és normalizálnak olyan tevékenységeket, amelyek korábban elfogadhatatlanok voltak (MALTZAHN 2006, 7.).

A *groominghoz* és a gyermekkel történő *sextinghez* hasonló tevékenységeket nagyon nehéz kiszűrni, és fellépni ellenük. Ugyanígy problémás a gyermekpornográfia terjesztésének megakadályozása, amely szinte robbanásszerű növekedésnek indult az új technológiák nyújtotta lehetőségeknek köszönhetően (DORNFELD–MEZEI 2017, 32.). Számos szegényebb országban, így például a már említett Fülöp-szigeteken elterjedt az a gyakorlat, hogy a szülők maguk kényszerítik a gyermekeket, hogy élőben streameljenek szexuális tevékenységeket. A helyi hatóságok sokáig nem léptek ez ellen fel, míg végül 2012-ben megszületett a kiberbűncselekmények megelőzéséről szóló törvény, ami fellép a *kiberszex* és a gyermekpornográfia ellen is. A fellépés nemcsak a gyermekeket kényszerítő felnőttek, de a szexkamera-turisták ellen is megtörtént, ami alapvető fontosságú. Ha a keresleti oldalt nem érik behatások, a jelenség sem szűnik meg, csak más, a problémára kevésbé érzékeny országokba kerül át. Mindemellett jelentős tudatosítási erőfeszítésekre is sor került az iskolákban, ahol a kiberszex veszélyeire hívták fel a fiatalok figyelmét.[17]

A Fülöp-szigeteken történt változás egyfajta modellprogramnak is tekinthető, amely a hasonló helyzetű országokban alkalmazható. Az Európai Bűnmegelőzési Hálózat által Romániában folytatott kutatás európai környezetben is a tudatosítás fontosságát jelzi.[18] A tapasztalatok szerint egyrészt meg kell ismertetni a fiatalokkal a jelenséget, és lehetővé tenni azt, hogy jelentsék, másrészt fel kell hívni a figyelmüket, hogy a szexuális tartalmú képek maradandó károkat képesek okozni. Fontos azonban figyelembe venni, hogy az elkövetők egy kisebb köre az, aki a gyakorlatban is részt vesz a gyermekpornográf anyagok elkészítésében, a többiek csak a fogyasztásukkal generálják az igényt rá. A fogyasztás első időszakában még csak érdeklődőkről, később letöltőkről, gyűjtőkről, majd legvégül előállítókról beszélhetünk. A sikeres fellépéshez elengedhetetlen az, hogy ez a folyamat ne érje el az utolsó fázisát, és pontosan e beavatkozás miatt volt fontos például a korábban már említett holland Sweetie-projekt.

---

17 Terre des Hommes: *Children of the Webcam. Updated Report on Webcam Child Sex Tourism.* Elérhető: www.savesweetienow.org/sites/default/files/2017-03/HR%2017021%20TdH%20Report%20Webcam%20-Manilla.pdf (A letöltés dátuma: 2018. 06. 10.)

18 EUCPN. Elérhető: https://eucpn.org/document/prevention-and-investigation-child-pornography-cases-internet-partnership-romanian-police (A letöltés dátuma: 2018. 11. 12.)

Felhasznált irodalom

Szakkönyvek, tanulmányok

Ananthalakshmi, A. – Bergin, Tom (2018): Malaysian Central Bank Says Foiled Attempted Cyber-Heist. *Reuters.com,* 2018. 03. 29. Elérhető: www.reuters.com/article/us-malaysia-cenbank-cybersecurity-incide/malaysian-central-bank-says-foiled-attempted-cyber-heist-idUSKBN1H50YF (A letöltés dátuma: 2018. 06. 03.)

Andorka Rudolf (2006): *Bevezetés a szociológiába.* Budapest, Osiris.

Andorka Rudolf – Buda Béla – Cseh-Szombathy László szerk. (1974): *A deviáns viselkedés szociológiája.* Budapest, Gondolat.

Bánáti János – Belegi József – Belovics Ervin – Erdei Árpád – Farkas Ákos – Kónya István (2018): *A büntetőeljárási törvény magyarázata.* Budapest, HVG-Orac.

Bártfai Barnabás (2017): *Számítógéphasználat mindenkinek.* Budapest, BBS-Info.

Bencsik Balázs (2017): *Nemzeti Kibervédelmi Intézet* (előadásanyag). Elérhető: https://njszt.hu/sites/default/files/BencsikBalazs.pptx (A letöltés dátuma: 2018. 06. 03.)

Bezsenyi Tamás – Csányi Gergely – Kiss Tibor (2018): Szervezett bűnözői csoportokról alkotott szervezeti reprezentáció és információáramlás a szervezett bűnözéshez kapcsolódóan. Kvantitatív elemzés az NNI-ről és az ORFK-ról. In Nyitrai Endre – Inzelt Éva – Kiss Tibor – Bezsenyi Tamás – Zsigmond Csaba – Frigyer László szerk.: *Nemzetközi jellegű szervezett bűnözés nyomozásának kutatása információ*áramlási szempontból. Tanulmánykötet II. Budapest, NKE. 69–83.

Bhattacharjee, Yudhijit (2011): How a Remote Town in Romania Has Become Cybercrime Central. *Wired.com,* 2011. 01. 31. Elérhető: www.wired.com/2011/01/ff_hackerville_romania (A letöltés dátuma: 2018. 08. 02.)

Blaskó Béla szerk. (2015): *Büntetőjog különös rész II.* Budapest, Rejtjel.

Borbíró Andrea (2011): *Kriminálpolitika és bűnmegelőzés a késő-modernitásban.* PhD-értekezés. Budapest, ELTE ÁJK.

Brenner, Susan W. – Clarke, Leo L. (2005): Distributed Security. Preventing Cybercrime. *The John Marshall Journal of Information Technology & Privacy Law,* Vol. 23, No. 4. 659–709.

Broadhurst, R. – Grabosky, P. (2005): *Cyber-Crime. The Challenge in Asia.* Hong Kong, Hong Kong University Press.

Buda Béla (2002): *Szexuális viselkedés.* Budapest, Animula.

Carr, Madeline (2016): Public-Private Partnerships in National Cyber-Crime Strategies. *International Affairs,* Vol. 92, No. 1. 43–62. DOI: https://doi.org/10.1111/1468-2346.12504

Castells, Manuel (2005): *A hálózati társadalom kialakulása.* Budapest, Gondolat.

Chabinsky, Steven R. (2010): *The Cyber Threat. Who's Doing What to Whom?* Elérhető: https://archives.fbi.gov/archives/news/speeches/the-cyber-threat-whos-doing-what-to-whom (A letöltés dátuma: 2018. 08. 02.)

CHANG, Lennon YC – GRABOSKY, Peter (2017): The Governance of Cyberspace. In DRAHOS, Peter ed.: *Regulatory Theory. Foundations and Applications.* Acton, ANU Press. 533–551. DOI: https://doi.org/10.22459/RT.02.2017.31

CSEPELI György – PRAZSÁK Gergely (2010): *Örök visszatérés. Társadalom az információs korban.* Budapest, Jószöveg.

DAHABIYEH, Laila (2015): *Networks of Cybercrime Prevention. A Process Study of the Credit Card.* Conference Paper. Elérhető: www.researchgate.net/publication/316275759_Networks_of_Cybercrime_Prevention_A_Process_Study_of_the_Credit_Card (A letöltés dátuma: 2018. 08. 02.)

DÉCARY-HÉTU, David – DUPONT, Benoit (2012): The Social Network of Hackers. *Global Crime,* Vol. 13, No. 3. 160–175. DOI: https://doi.org/10.1080/17440572.2012.702523

DORNFELD László (2015): A kiberbűnözés elleni küzdelem kihívásai. *Diskurzus,* 5. évf. klsz. 27–35.

DORNFELD László (2016): A kiberbűncselekmények nyomozásával kapcsolatban folytatott uniós bűnügyi együttműködés fejlődése. *Külügyi Szemle,* 15. évf. 4. sz. 96–97.

DORNFELD László (2018): A kibertérben elkövetett bűncselekményekkel összefüggésben alkalmazható kényszerintézkedések. *Belügyi Szemle,* 66. évf. 2. sz. 115–135.

DORNFELD László – MEZEI Kitti (2017): Az online gyermekpornográfia elleni küzdelem aktuális kérdései. *Infokommunikáció és Jog,* 14. évf. 68. sz. 25–31.

FANG, Binxing (2018): *Cyberspace Sovereignty. Reflections on Building a Community of Common Future in Cyberspace.* Beijing, Springer. DOI: https://doi.org/10.1007/978-981-13-0320-3

FANTOLY Zsanett – BUDAHÁZI Árpád (2015): *Büntető eljárásjog I. Statikus rész.* Budapest, NKE Szolgáltató.

FANTOLY Zsanett – GÁCSI Anett (2013): *Eljárási büntetőjog. Statikus rész.* Szeged, Iurisperitus.

FEHÉR Irén – LAPPINTS Árpád (1999): *Pedagógiai fogalomtár.* Pécs, Comenius.

FERRARI, Anusca (2013): *DIGCOMP. A Framework for Developing and Understanding Digital Competence in Europe.* Luxembourg, Publications Office of the European Union.

FRÉSZ Ferenc (2017): *Kiberháborús* játékok. ITBN 2017. Konferenciaelőadás. Elérhető: www.youtube.com/watch?v=M2Nakh-Emqo&list=PLSOYQEF9YFBIsO8SqRZOEuQsi_MBhSRHC&index=22 (A letöltés dátuma: 2018. 08. 02.)

GÁL István László (2013): A pénz- és bélyegforgalom biztonsága elleni bűncselekmények. In POLT Péter szerk.: *Új Btk. kommentár.* 7. kötet. *Különös Rész.* Budapest, Nemzeti Közszolgálati és Tankönyv Kiadó.

GIBSON, William (1999): *Neurománc.* Budapest, Valhalla Páholy.

GIDDENS, Anthony (2008): *Szociológia.* Második kiadás. Budapest, Osiris.

GORICSAN Tamás Károly (2006): *A kényszerintézkedések végrehajtásának sajátosságai a számítástechnikai eszközök felhasználásával megvalósított bűncselekmények nyomozása körében.* Pécs, PTE ÁJK.

GÖNCZÖL Katalin – KEREZSI Klára szerk. (1993): *A deviancia szociológiája.* Budapest, T-Twins.

GRABOSKY, Peter N. (2001): Virtual Criminality. Old Wine in New Bottles? *Social and Legal Studies,* Vol. 10, No. 2. 243–249. DOI: https://doi.org/10.1177/a017405

HAIG Zsolt – VÁRHEGYI István (2005): *Hadviselés az információs hadszíntéren.* Budapest, Zrínyi.

HÁRDI István (2010): *Az agresszió világa.* Budapest, Medicina.

HEGEDŰS István et al. (2018): *Kommentár a Büntető Törvénykönyvről szóló 2012. évi C. törvényhez.* Budapest, Wolters Kluwer.

HORVÁTH Attila (2006): Terrorfenyegetettség. Célpontok, nagyvárosok közlekedés. *Nemzetvédelmi Egyetemi Közlemények,* 10. évf. 3. sz. 136–152.

Ibolya Tibor (2012): *Számítástechnikai jellegű bűncselekmények nyomozása.* Budapest, Patrocinium.

Kereszty Béla – Maráz Vilmosné – Nagy Ferenc – Vida Mihály (2004): *A magyar büntetőjog. Különös rész.* Budapest, Korona.

Kiss Tibor (2013): Az internet és a társadalmi egyenlőtlenségek. *Információs Társadalom,* 13. évf. 3–4. sz. 97–99.

Kiss Tibor (2014): Áldozattá válás dimenziói az online színtéren. In Fazekas Marianna szerk.: *Jogi tanulmányok 2014.* Budapest, ELTE ÁJK. 382–393.

Kiss Tibor (2014): Gyűlölet-bűncselekmények és szélsőséges csoportok az információs társadalomban. In Prazsák Gergő szerk.: *Nemzeti szempont.* Budapest, Aperion. 71–92.

Kiss Tibor (2016): Internetes mémek mint káros információs egységek a tartalom-bűncselekmények körében. In Fazekas Marianna szerk.: *Jogi tanulmányok 2016.* Budapest, ELTE ÁJK. 350–360.

Kiss Tibor (2017: Agresszió szerepe az internetes tartalom-bűncselekmények oksági mechanizmusában. In Zséger Barbara szerk.: *Kriminológiai közlemények 77.* Budapest, Magyar Kriminológiai Társaság. 257–270.

Kiss Tibor (2018): Cyberbűnözés. In Nyitrai Endre – Inzelt Éva – Kiss Tibor – Bezsenyi Tamás – Zsigmond Csaba – Frigyer László szerk.: *Nemzetközi jellegű szervezett bűnözés nyomozásának kutatása információáramlási szempontból. Tanulmánykötet II.* Budapest, NKE. 30–69.

Kiss Tibor (é. n. a): Cyberbűnözés. In Barabás Andrea Tünde szerk.: *Alkalmazott kriminológia.* Budapest, Dialóg Campus. (Megjelenés folyamatban.)

Kiss Tibor (é. n. b): Devianciák. In Barabás Andrea Tünde szerk.: *Alkalmazott kriminológia.* Budapest, Dialóg Campus. (Megjelenés folyamatban.)

Kiss Tibor (é. n. c): Kriminológia tudománytörténete. In Barabás Andrea Tünde szerk.: *Alkalmazott kriminológia.* Budapest, Dialóg Campus. (Megjelenés folyamatban.)

Kiss Tibor (é. n. d): *Agresszió a cybertérben.* Budapest, NKE (Megjelenés folyamatban.)

Kiss Tibor – Parti Katalin (2016): A mém vajon mi? A mémekért való felelősség megállapíthatóságának kérdései és lehetőségei. *Infokommunikáció és Jog,* 13. évf. 66–67. sz. 39–47.

Kiss Tibor – Parti Katalin – Prazsák Gergely (2019): *Cyberdeviancia.* Budapest, Dialóg Campus.

Kshetri, Nir (2013): Cybercrimes in the Former Soviet Union and Central and Eastern Europe. Current Status and Key Drivers. *Crime, Law and Social Change,* Vol. 60, No. 1. 39–65. DOI: https://doi.org/10.1007/s10611-013-9431-4

Leiner, Barry M. – Cerf, Vinton G. – Clark, David D. – Kahn, Robert E. – Kleinrock, Leonard – Lynch, Daniel C. – Postel, Jon – Roberts, Larry G. – Wolff, Stephen (1997): *A Brief History of the Internet.* Elérhető: www.researchgate.net/publication/2413637_Barry_M_Leiner_Vinton_G_Cerf_David_D_Clark_Robert_E_Kahn_Leonard_Kleinrock_Daniel_C_Lynch_Jon_Postel_Lawrence_G_Roberts_Stephen_S_Wolff (A letöltés dátuma: 2018. 08. 03.)

Leukfeldt, Rutger E. (2016): *Cybercriminal Networks. Origin, Growth and Criminal Capabilities.* Portland (OR), Eleven.

Levin, Avner – Ilkina, Daria (2013): *International Comparison of Cyber Crime.* Elérhető: www.ryerson.ca/tedrogersschool/privacy/documents/Ryerson_International_Comparison_ofCyber_Crime_-March2013.pdf (A letöltés dátuma: 2018. 08. 03.)

Li, Xingan (2007): International Actions against Cybercrime: Networking Legal Systems in the Networked Crime Scene. *Webology,* Vol. 4, No. 3. Elérhető: www.webology.org/2007/v4n3/a45.html (A letöltés dátuma: 2018. 08. 03.)

LIM, Linette (2016): Why Scams Succeed. Human Behaviour Experts Explain. *CNA,* 2016. 11. 02. Elérhető: www.channelnewsasia.com/news/singapore/why-scams-succeed-human-behaviour-experts-explain-7696934 (A letöltés dátuma: 2018. 08. 03.)

MALTZAHN, Kathleen (2006): *Digital Dangers. Information & Communication Technologies and Trafficking in Women.* (APC Issue Papers.) Elérhető: http://lastradainternational.org/lsi-docs/386%20digital_dangers_EN_1.pdf (A letöltés dátuma: 2018. 08. 03.)

MÁTÉ István Zsolt (2017): *Az igazságügyi informatikai szakértő a büntetőeljárásban.* PhD-értekezés. Pécs, PTE ÁJK Doktori Iskola. Elérhető: http://pea.lib.pte.hu/handle/pea/16947 (A letöltés dátuma: 2018. 06. 03.)

MCGUIRE, Michael (2012): *Organised Crime in the Digital Age.* London, John Grieve Centre for Policing and Security.

MORGENSON, Gretchen (2000): S.E.C. Says Teenager Had After-School Hobby. Online Stock Fraud. *The New York Times,* 2000. 09. 21. Elérhető: www.nytimes.com/2000/09/21/business/sec-says-teenager-had-after-school-hobby-online-stock-fraud.html (A letöltés dátuma: 2018. 08. 03.)

MUNK Sándor (2018): A kibertér fogalmának egyes, az egységes értelmezést biztosító kérdései. *Hadtudomány,* 28. évf. 1. sz. 113–131.

MUSIAŁ, Katarzyna – KAZIENKO, Przemysław (2013): Social Networks on the Internet. *World Wide Web,* Vol. 16, No. 1. 31–72. DOI: https://doi.org/10.1007/s11280-011-0155-z

NAGY Richárd (2018): A kibertérben elkövetett vagyon elleni bűncselekmények nyomozásának egyes kérdései. *Belügyi Szemle,* 66. évf. 7–8. sz. 83–95.

NAGY Tamás (2018): *Business E-mail Compromise. Az átutaláshoz kapcsolódó vagy e-mailes csalások* című tájékoztató, amit a KR NNI által tartott oktatáshoz kapcsolódóan adtak ki. Budapest, 2018. 09. 10–14.

NAGY Zoltán András – MEZEI Kitti (2017): A zsarolóvírus és a botnet vírus mint napjaink két legveszélyesebb számítógépes vírusa. In GAÁL Gyula – HAUTZINGER Zoltán szerk.: *Szent Lászlótól a modernkori magyar rendészettudományig.* Pécs, Magyar Hadtudományi Társaság Határőr Szakosztály Pécsi Szakcsoport. 163–168.

O'REGAN, Gerard (2016): *Introduction to the History of Computing. A Computing History Primer.* Cham, Springer. DOI: https://doi.org/10.1007/978-3-319-33138-6

PALMER, Danny (2017): Hospitals Across the UK Hit by WannaCrypt Ransomware Cyberattack, Systems Knocked Offline. *ZDNet.com,* 2017. 05. 12. Elérhető: www.zdnet.com/article/hospitals-across-england-hit-by-cyber-attack-systems-knocked-offline (A letöltés dátuma: 2018. 06. 03.)

PARTI Katalin – KISS Tibor (2016): Informatikai bűnözés. In BORBÍRÓ Andrea – GÖNCZÖL Katalin – KEREZSI Klára – LÉVAY Miklós szerk.: *Kriminológia.* Budapest, Wolters Kluwer. 491–517.

PARTI Katalin – MARIN, Luisa (2012): Foltvarrással az on-line illegális tartalom ellen. A tartalomblokkolás, a közvetítő szolgáltató felelőssége és az értesítési-levételi eljárás. *Infokommunikáció és Jog,* 9. évf. 49. sz. 58–65.

PARTI Katalin – SCHMIDT Andrea – NÉRAY Bálint – VIRÁG György (2014): TABBY in Internet. Az online bántalmazás volumenének iskolai felmérése és mentorképzés Magyarországon. *Ügyészek Lapja,* 21. évf. 3–4. sz. 47–58.

PARTI Katalin (2004): Az internetes bűncselekmények nyomozásának egyes kérdései. In IRK Ferenc szerk.: *Kriminológiai Tanulmányok* 41. Budapest, Országos Kriminológiai Intézet. 251–263.

PARTI Katalin – KISS Tibor – KOPLÁNYI Gergely (2018): Architecture of Aggression in Cyberspace. Testing Cyber Aggression in Young Adults in Hungary. *International Journal of Cybersecurity,* Vol. 1, No. 1. 56–68. Elérhető: www.researchgate.net/publication/327069329_Architec-

ture_of_aggression_in_cyberspace_Testing_cyber_aggression_in_young_adults_in_Hungary (A letöltés dátuma: 2018. 06. 03.)

Perl, Raphael F. (2007): *Drug Trafficking and North Korea.* Elérhető: www.fas.org/sgp/crs/row/RL32167.pdf (A letöltés dátuma: 2017. 07. 13.)

Ploug, Thomas (2009): *Ethics in Cyberspace. How Cyberspace May Influence Interpersonal Interaction.* Copenhagen, Springer. DOI: https://doi.org/10.1007/978-90-481-2370-4

Prensky, Marc (2001): *Digitális bennszülöttek, digitális bevándorlók.* Kovács Emese ford. Elérhető: http://goliat.eik.bme.hu/~emese/gtk-mo/didaktika/digital_kids.pdf (A letöltés dátuma: 2017. 07. 13.) Eredeti megjelenés: Digital Natives, Digital Immigrants. *On the Horizon,* Vol. 9, No. 5. 1–6.

Rajnai Zoltán (2016): *Kibervédelem és kiberkoordináció, vállalati aspektusok, vízió* (előadásanyag). Elérhető: https://njszt.hu/sites/default/files/rajnai.pptx (A letöltés dátuma: 2018. 06. 03.)

Richards, Cameron (2000): Hypermedia, Internet Communication, and the Challenge of Redefining Literacy in the Electronic Age. *Language Learning – Technology,* Vol. 4, No. 2. 54–71.

Rosta Andrea (2007): *A deviáns viselkedés szociológiája.* Budapest, Loisir.

Ruma, Paul (2016): Exclusive: Some Bangladesh Bank Officials Involved in Heist. *Reuters.com,* 2016. 12. 12. Elérhető: www.reuters.com/article/us-cyber-heist-bangladesh-exclusive/exclusive-some-bangladesh-bank-officials-involved-in-heist-investigator-idUSKBN1411ST?utm_campaign=trueAnthem:+Trending+Content&utm_content=584f82a904d30107e6eeb727&utm_medium=trueAnthem&utm_source=twitter (A letöltés dátuma: 2018. 06. 03.)

Runions, Kevin C. – Bak, Michal – Shaw, Therese (2016): Disentangling Functions of Online Aggression. The Cyber-Aggression Typology Questionnaire (CATQ). *Aggressive Behavior,* Vol. 43, No. 1. 74–84. DOI: https://doi.org/10.1002/ab.21663

Rushkoff, Douglas (2002): *Cyberia. Life in the Trenches of Cyberspace.* Manchester, Clinamen.

Schermer, Bart W. – Georgieva, Ilina – Van der Hof, Simone – Koops, Bert-Jaap (2016): *Legal Aspects of Sweetie 2.0.* Leiden–Tilburg, Leiden University Faculty of Law – Tilburg University, Faculty of Law. Elérhető: www.savesweetienow.org/sites/default/files/2016-10/20161003Sweetie20_1_0.pdf (A letöltés dátuma: 2018. 08. 03.)

Simon Béla (2017): A bűnüldözés előtt álló digitális kihívások. *Magyar Rendészet,* 17. évf. 5. sz. 83–105.

Simon Béla (2018a): Rendészeti szervek együttműködése a kiberbűnözés ellen. *Nemzetbiztonsági Szemle,* 6. évf. 1. sz. 36–58.

Simon Béla (2018b): Az EU rendészeti szerveinek együttműködése a kiberbűnözés ellen. *Nemzetbiztonsági Szemle,* 6. évf. 4. sz. 21–47.

Simon Béla – Gyaraki Réka (2017): *Biztonsági események rendészeti szempontból. A kiberbűncselekmények kezelése.* (Megjelenés folyamatban.)

Sinku Pál (2006): A bankkártya mint elkövetési tárgy büntetőjogi és eljárásjogi problémái. In Gál István – Nagy Zoltán András szerk.: *Informatika és büntetőjog.* Pécs, PTE ÁJK. 161–180.

Slonje, Robert – Smith, Peter K. – Frisén, Ann (2012): The Nature of Cyberbullying, and Strategies for Prevention. *Computers in Human Behavior,* Vol. 29, No. 5. 26–32. DOI: https://doi.org/10.1016/j.chb.2012.05.024

Smith, Eliot R. – Mackie, Diane M. – Claypool, Heather M. (2016): *Szociálpszichológia.* Budapest, ELTE Eötvös.

Tapscott, Don – Williams, Anthony D. (2006): *Wikinómia.* Budapest, HVG-Orac.

Tikos Anita (2017): *Az NKI bemutatása* (előadásanyag). Elérhető: www.eoq.hu/szakb/11/inf170227.pdf (A letöltés dátuma: 2018. 06. 03.)

TURKLE, Sherry (2005): *The Second Self: Computers and the Human Spirit.* Cambridge (MA), MIT Press. DOI: https://doi.org/10.7551/mitpress/6115.001.0001

VIGH József – GÖNCZÖL Katalin – KISS György – SZABÓ Árpád szerk. (1973): *Erőszakos bűncselekmények és elkövetőik.* Budapest, Közgazdasági és Jogi Könyvkiadó.

VIRÁG György – KULCSÁR Gabriella – ROSTA Andrea (2016): Erőszakos bűnözés. In BORBÍRÓ Andrea – GÖNCZÖL Katalin – KEREZSI Klára – LÉVAY Miklós szerk.: *Kriminológia.* Budapest, Wolters Kluwer. 553–598.

WALL, David S. (2008): Cybercrime, Media and Insecurity. The Shaping of Public Perceptions of Cybercrime. *International Review of Law, Computers and Technology,* Vol. 22, No. 1–2. 45–63. DOI: https://doi.org/10.1080/13600860801924907

WANG, Jingqiong (2010): Internet Policing Hinges on Transnational Cyber Crime. *Chinadaily.com,* 2010. 11. 10. Elérhető: www.chinadaily.com.cn/china/2010-11/10/content_11525646.htm (A letöltés dátuma: 2018. 08. 02.)

WEIK, Martin H. (2001): Cyberspace. In *Computer Science and Communications Dictionary.* Boston (MA), Springer. 331–332. DOI: https://doi.org/10.1007/1-4020-0613-6_4119

WELLMAN, Barry – GULIA, Milena (1997): *Net Surfers Don't Ride Alone. Virtual Communities as Communitites.* Toronto, University of Toronto Department of Sociology an Centre for Urban and Community Studies.

WHITTAKER, Jason (2004)*:* Cyberspace, Digital Media and the Internet. In WHITTAKER, Jason: *The Cyberspace Handbook.* London – New York, Routledge. 3–21. DOI: https://doi.org/10.4324/9780203486023

WOLF, Jonathan B. (2001): War Games Meets the Internet. Chasing 21st Century Cybercriminals With Old Laws and Little Money. *American Journal of Criminal Law,* Vol. 28. 95–117.

YAR, Majid (2006): *Cybercrime and Society.* London, SAGE.

Z. KARVALICS László (2017): *Informatórium Szó-kalauz a kortárs információs kultúrához.* Budapest, Tinta.

ZSILA Ágnes – UJHELYI Adrienn – DEMETROVICS Zsolt (2015): *Online zaklatás a legújabb kutatások tükrében.* Budapest, Imágó.

További internetes források

Additional Protocol to the Convention on Cybercrime, Concerning the Criminalisation of Acts of a Racist and Xenophobic Nature Committed through Computer Systems (ETS No. 189). Elérhető: www.coe.int/en/web/conventions/full-list/-/conventions/treaty/189 (A letöltés dátuma: 2018. 06. 03.)

Az Europol profilja: Európai Bűnüldözési Hatóság. Elérhető: www.europol.europa.eu/publications-documents/europol-profile (A letöltés dátuma: 2018. 06. 03.)

Central European Cyber Security Platform held its third meeting in Vienna (2014). Elérhető: http://2010-2014.kormany.hu/en/ministry-of-public-administration-and-justice/news/central-european-cyber-security-platform-held-its-third-meeting-in-vienna (A letöltés dátuma: 2018. 06. 03.)

Council of Europe (1989): *Computer-related crime, Recommendation No R (89) 9 on Computer-related Crime and final report of the European Committee on Crime Problems.* Elérhető: www.coe.int/t/dg3/healthbioethic/texts_and_documents/Rec(89)2E.pdf (A letöltés dátuma: 2018. 06. 03.)

Council Of Europe (2012): *Recommendation No. R (81) 12 Of The Committee of Ministers to Member States On Economic Crime.* Elérhető: https://rm.coe.int/16806cb4f0 (A letöltés dátuma: 2018. 06. 03.)

ENISA European Network and Information Security Agency. Elérhető: https://www.enisa.europa.eu/ (A letöltés dátuma: 2018. 06. 03.)

European Commission (2017): *Az Európai Unió helyzetéről szóló 2017. évi beszéd. Kiberbiztonság: a Bizottság megerősíti a kibertámadásokkal szembeni uniós reagálási* képességet. Elérhető: http://europa.eu/rapid/press-release_IP-17-3193_hu.htm (A letöltés dátuma: 2018. 06. 03.)

European Cyber Security Organisation. Elérhető: www.ecs-org.eu/about (A letöltés dátuma: 2018. 06. 03.)

European Network for Cyber Security. Elérhető: https://encs.eu (A letöltés dátuma: 2018. 06. 03.)

Europol European Cybercrime Centre (EC3). Elérhető: www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3 (A letöltés dátuma: 2018. 06. 03.)

FIRST Forum of Incident Response and Security Teams. Elérhető: www.first.org (A letöltés dátuma: 2018. 06. 03.)

FIRST Special Interest Groups (SIGs). Elérhető: www.first.org/global/sigs (A letöltés dátuma: 2018. 06. 03.)

FTK Imager. Elérhető: https://accessdata.com/product-download/ftk-imager-version-3.2.0 (A letöltés dátuma: 2018. 06. 03.)

IT Law Wiki – International Watch and Warning Network. Elérhető: http://itlaw.wikia.com/wiki/International_Watch_and_Warning_Network (A letöltés dátuma: 2018. 06. 03.)

KIFÜ. Elérhető: http://kifu.gov.hu (A letöltés dátuma: 2018. 06. 03.)

Létfontosságú Rendszerek és Létesítmények Informatikai Biztonsági Eseménykezelő Központ (Belügyminisztérium, Országos Katasztrófavédelmi Főigazgatóság). Elérhető: www.katasztrofavedelem.hu/index2.php?pageid=lrl_ibek (A letöltés dátuma: 2018. 06. 03.)

National Cyber Security Centrum Ministerie van Justitie en Veiligheid – International Collaboration, International Watch and Warning Network. Elérhető: www.ncsc.nl/english/Cooperation/international-collaboration.html (A letöltés dátuma: 2018. 06. 03.)

Nemzetbiztonsági Szakszolgálat. Elérhető: http://nbsz.hu/?mid=42 (A letöltés dátuma: 2018. 06. 03.)

Nemzeti Kibervédelmi Intézet – Kormányzati Eseménykezelő Központ. Elérhető: www.cert-hungary.hu/node/1 (A letöltés dátuma: 2018. 06. 03.)

Országos Katasztrófavédelmi Főigazgatóság BM OKF (Belügyminisztérium). Elérhető: www.katasztrofavedelem.hu/index2.php?pageid=lrl_iht (A letöltés dátuma: 2018. 06. 03.)

Safer Internet Program. Elérhető: https://ec.europa.eu/digital-single-market/en/content/creating-better-internet-kids-0 (A letöltés dátuma: 2018. 06. 03.)

TI Trusted Introducer. Elérhető: www.trusted-introducer.org (A letöltés dátuma: 2018. 06. 03.)

UNODC (2013): Comprehensive Study on Cybercrime. Elérhető: www.unodc.org/documents/organized-crime/cybercrime/CYBERCRIME_STUDY_210213.pdf (A letöltés dátuma: 2018. 06. 03.)

Jogszabályi hivatkozások

100/2018. (VI. 8.) Korm. rendelet a nyomozás és az előkészítő eljárás részletes szabályairól

185/2015. (VII. 13.) Korm. rendelet a kormányzati eseménykezelő központ és az eseménykezelő központok feladat- és hatásköréről, valamint a biztonsági események kezelésének, a biztonsági események műszaki vizsgálatának és a sérülékenységvizsgálat lefolytatásának szabályairól

186/2015. (VII. 13.) Korm. rendelet a központosított informatikai és elektronikus hírközlési szolgáltató információbiztonsággal kapcsolatos feladatköréről
187/2015. (VII. 13.) Korm. rendelet az elektronikus információs rendszerek biztonsági felügyeletét ellátó hatóságok, valamint az információbiztonsági felügyelő feladat- és hatásköréről, továbbá a zárt célú elektronikus információs rendszerek meghatározásáról
1994. évi XXXIV. törvény a Rendőrségről
1998. évi XIX. törvény a büntetőeljárásról (régi Be.)
2001. évi CVIII. törvény az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről
2006. évi CI. törvény az Egyesült Nemzetek keretében, Palermóban, 2000. december 14-én létrejött, a nemzetközi szervezett bűnözés elleni Egyezmény kihirdetéséről
2012. évi C. törvény a Büntető Törvénykönyvről
2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról
2015. évi CCXXII. törvény az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól
2016. évi XXIX. törvény az igazságügyi szakértőkről
2017. évi XC. törvény a büntetőeljárásról
25/2013. (VI. 24.) BM rendelet a Rendőrség nyomozó hatóságainak hatásköréről és illetékességéről
268/2010. (XII. 3.) Korm. rendelet a Kormányzati Informatikai Fejlesztési Ügynökségről
309/2011. (XII. 23.) Korm. rendelet a központosított informatikai és elektronikus hírközlési szolgáltatásokról
346/2010. (XII. 28.) Korm. rendelet a kormányzati célú hálózatokról
41/2015. (VII. 15.) BM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről
451/2016. (XII. 19.) Korm. rendelet az elektronikus ügyintézés részletszabályairól
484/2013. (XII. 17.) Korm. rendelet a Nemzeti Kiberbiztonsági Koordinációs Tanács, valamint a Kiberbiztonsági Fórum és a kiberbiztonsági ágazati munkacsoportok létrehozásával, működtetésével kapcsolatos szabályokról, feladat- és hatáskörükről
Az Európai Parlament és a Tanács 526/2013/ EU rendelete (2013. május 21.) az Európai Uniós Hálózat- és Információbiztonsági Ügynökségről (ENISA) és a 460/2004/EK rendelet hatályon kívül helyezéséről
7/2013. (II. 26.) NFM rendelet a központosított informatikai és elektronikus hírközlési szolgáltatásokat egyedi szolgáltatási megállapodás útján igénybe vevő szervezetekről, valamint a központi szolgáltató által üzemeltetett vagy fejlesztett informatikai rendszerekről
8002/2008. IRM tájékoztató a nemzetközi vonatkozású büntetőügyek intézéséről
84/2012. (IV. 21.) Korm. rendelet egyes, az elektronikus ügyintézéshez kapcsolódó szervezetek kijelöléséről
Az Európai Parlament és a Tanács (EU) 2016/1148 Irányelve (2016. július 6.) a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről
ENSZ Gazdasági és Szociális Tanács 2002/13. sz. határozata
Az Európai Tanács 2002/187/IB határozata az Eurojust létrehozásáról
A Hun-CERT alapokmánya. Elérhető: www.cert.hu/a-hun-cert-alapokmanya (A letöltés dátuma: 2018. 06. 03.)

Vákát oldal

Ludovika Egyetemi Kiadó Nonprofit Kft.
Székhely: 1089 Budapest, Orczy út 1.
Kapcsolat: info@ludovika.hu

A kiadásért felel: Koltányi Gergely ügyvezető igazgató
Felelős szerkesztő: Kilián Zsolt
Olvasószerkesztő: Sós Dóra
Korrektor: Pokorádi Zsófia
Tördelőszerkesztő: Kőrösi László
Nyomdai kivitelezés: Pátria Nyomda Zrt.
Felelős vezető: Orgován Katalin vezérigazgató

ISBN 978-963-531-029-6 (nyomtatott)
ISBN 978-963-531-030-2 (elektronikus)

A kiberbiztonsági szakterületen egy dolog miatt biztosan ismerik Magyarországot: az Európa Tanács Budapesten, 2001. november 23-án kelt számítástechnikai bűnözésről szóló egyezményéről. Viszont annak ellenére, hogy a kiberbűnözés elleni küzdelem lassan 20 éve része a rendvédelmi gyakorlatnak, nem igazán készült olyan összefoglaló mű, amelyet a leendő rendőrtisztek oktatásában fel lehetett volna használni. A Kibervédelem a bűnügyi tudományokban című kötet ezt a hiátust pótolja, a Nemzeti Közszolgálati Egyetem témával foglalkozó oktatóinak közös munkája eredményeképpen. Az olvasó megismerheti az általános fogalmi és jogi alapok mellett a kriminológia, a felderítés és a bűnmegelőzés területén rendelkezésre álló legújabb eredményeket is. Mindez lehetőséget biztosít arra, hogy az egyre növekvő számú kiberbűncselekmények kezelését és ezek áldozatainak segítését a közeljövőben a megelőzésben, a felderítésben és a nemzetközi együttműködésben egyaránt sikeres rendvédelmi dolgozók hajthassák végre.

Krasznay Csaba

A mű a KÖFOP-2.1.2-VEKOP-15-2016-00001 „A jó kormányzást megalapozó közszolgálat-fejlesztés” című projekt keretében jelent meg.