Nagy Zoltán András - Mezei Kitti

AZ INFORMATIKAI BŰNCSELEKMÉNYEK

egyetemi jegyzet

A jegyzet az Igazságügyi Minisztérium jogászképzés színvonalának emelését célzó programjai keretében valósult meg.

Pécs, 2017.

TARTALOMJEGYZÉK

Kriminológiai áttekintés

A számítógépek alkalmazásának fontossága, szükségessége ma már elvitathatatlan. Az elektronikus adatfeldolgozás- és adatátvitel nyújtotta előnyöket mindennapi életünkben szinte észre sem vesszük, természetesnek tartjuk. A számítógép egyszerre van jelen mindennapi munkánkban és teret hódít otthonainkban is. Elképzelhetetlen áldásos segítsége a közigazgatásban, az ipari tevékenység automatizálásában, a számvitelben, a közlekedésben, a távközlésben, a szállításban, a hadiiparban, az oktatásban, a tudományos kutatásban, az egészségügyben és másutt, életünk szinte valamennyi szférájában. Vásárlási, pénzkezelési szokásainkat is átformálja. A számítógépes „szupersztrádán", a különféle hálózatokon kedvünkre száguldozhatunk, igaz – idehaza - borsos áron. Hozzáférhetünk távoli országok adatállományaihoz, vásárolhatunk árut, szolgáltatást, részesei lehetünk nemzetközi konferenciáknak, küldhetünk szöveges, hang- és képüzenetet egy másik kontinensen élő ismerősnek vagy ismeretlennek, és végeláthatatlanul bolyonghatunk az egyelőre szabályozatlan cyber - térben, amelyre a „pénz" már kivetette hálóját. Az Internet gyorsabban terjed, mint bármely más médium eddig.

A komputerizáció elvitathatatlan jótéteményei mellett együtt kell élnünk valós *hátrányaival* is. Növekszik kiszolgáltatottságunk a kritikus infrastruktúrák felé, napjainkban szabadságunk illúzióvá válik, mivel minden pillanatban digitális nyomokat hagyunk magunk után, anyanyelvünk háttérbe szorul, az adatbázisok, tárak globalizálódnak, az angolszász kultúra feltartóztathatatlan, az írók, költők becses kézjegyei, kézírásai elvésznek, a felhasználókat compufóbia veszélyezteti.

A komputerizáció legszámottevőbb hátrányát azonban a számítógépes környezetben elkövetett informatikai bűncselekmények jelentik.

Az első számítógépes bűncselekmények egyike az egyesült államokbeli Walston end Co. alelnöke által elkövetett sikkasztás volt, aki hamis lyukkártyákat készítve 50.000.- dollárt sikkasztott még az ötvenes évek végén. Ez a bűncselekmény, a bűncselekmény alanyi oldalával ugyan egyezően, de módszerében másképp, elektronikus impulzusok begépelésével valósítható meg. A számítástechnika folyamatos fejlődése jelenti e bűncselekmények veszélyességét, újabb és újabb visszaélések látnak napvilágot.

A számítógépes bűncselekmények veszélyességét annak *tömegessége* jelzi. 390,000 malware naponta. A WannaCry zsarolóvírus egy nap alatt 200 millió gépet fertőzött meg. A tömegesség folyománya a kárérték.

A bűncselekmény *elkövetői* ma még zömmel a fiatalabb generáció tagjai között keresendők, ám a közel jövőben a számítógépek térhódításával és e mostani nemzedék idősebbé válásával a bűncselekmények eme kriminológiai jellemzője elenyészik. Az elkövetők rendkívül kreatívok, nem ritkán fehér-galléros bűnelkövetők dominálnak.

A valós térben elkövetett bűncselekményekben is tetten érhető a *sértett közrehatása* (victim blaming), ám számítógépes környezetben elkövetett bűncselekmények esetében ez még inkább jellemző. Az Interneten közzétett, spamekben, e-mailben írt csalás, vagy a piramiscsalás cselekményének áldozatává válhatnak könnyedén az óvatlan felhasználók. Míg a valós térben elkövetett bűncselekmények esetében látható, kézzel fogható nyomai, jelei vannak annak, hogy bűncselekményt követtek el (pl. az elkövetési tárgyat ellopták vagy megrongálták, a sértett bántalmazás során sérülést szenvedett stb.), addig a számítógépes környezetben a felhasználó sokszor nem is érzékeli, hogy bűncselekmény áldozata lett. Számítógépe a megszokott módon működik, dokumentumai („könyvtárak", a fájlok - akár hiánytalanul) a helyükön vannak. De e dokumentumokat akár „el is lophatták" (azaz átmásolhatták egy másik adathordozóra, megoszthatták az Interneten, feltölthették a támadó által ismert felhő-szerverre vagy adataival más módon visszaélhetnek, így felhasználhatják ellene, megzsarolhatják, lejárathatják, megszégyeníthetik, az e-kereskedelemben adatait jogellenesen használhatják stb.).

Az a körülmény, hogy a felhasználó nem érzékeli azt, hogy sértetté, áldozattá vált, megnöveli a bűncselekmények veszélyességét, látenciáját, a gyors és eredményes nyomozásnak komoly akadályt képeznek.

A következőkben tipizált *támadások* egyaránt fenyegethetnek egyes számítógépet és számítástechnikai rendszereket. Kivételként említhető a 9/89-es Európa Tanácsi Ajánlásban említett félvezetők (chipek) jogellenes másolása.

A számítógépes környezetben elkövetett bűncselekmények alapvető csoportosítása:

- a számítástechnikai rendszert érő fizikai támadások: a XIX. századi luddita géprongálások reinkarnációja,
- a számítástechnikai rendszert érő intellektuális támadások.

A számítógépes környezetben elkövethető cselekmények további *csoportosítási lehetősége*:
- olyan bűncselekmények, amelyek a valós térben is megvalósíthatok, valamint
- az új technikai környezet által teremtette feltételek hiányában nem követhetők el.
Az elsőként említett körbe sorolhatók, a csalás jellegű cselekmények, a gyűlöletkeltő, zaklató, becsületet sértő cselekmények, a gyermekpornográfia, a pénzmosás, a kábítószer népszerűsítése-, kereskedelme, a szerzői és szomszédos jogok megsértése és más jogsértések.
Míg a második csoportban említhetők a digitalizált szerzői alkotások megosztása, a kódfeltörő programok készítése,- terjesztése, a phishing különböző formái, a defacing, a hacking, a különböző malware-ekkel végrehajtott támadások, a DOS-, D(D)OS – támadások, az, e-mailek kifürkészés, nagyszámú spam-ek küldése és más tiltott tevékenységek.

Egyes *támadás-típusok* jellemzőek lehetnek meghatározott felhasználókkal szemben:
- a kritikus infrastruktúrákat,[1] és az ezeken kívül eső gazdasági – társadalmi – szervezetek fenyegető tipikus támadások: a hacking, a D(DoS) - támadás, a különböző malware-támadások, a defacing, jogosulatlan adatkifürkészés stb.
- az egyéni felhasználókat fenyegető támadások: a hacking, a különböző malware-támadások, a cyberbullying, a phishing, a személyiséglopás stb.
Ez utóbbi tipizálás gyakorlati előnye lehet az, hogy az egyes felhasználók, legyen az szervezett, vállalkozás, egyéni felhasználók felkészülhetnek a számítógépeiket, számítástechnikai rendszerüket érhető támadásokra.

Az intellektuális támadások csoportosíthatók:
Támadó jellegű intellektuális visszaélések:
- vagyoni kárt okozó támadások: csalás jellegű visszaélésekkel (man-in-the-browser támadás felhasználásával – a pénzintézet és az ügyfél közé ékelődő, a pénzintézetet hamisító támadás),

[1]„Kritikus infrastruktúrák alatt olyan, egymással összekapcsolódó, interaktív és egymástól kölcsönös függésben lévő infrastruktúra elemek, létesítmények, szolgáltatások, rendszerek és folyamatok hálózatát értjük, amelyek az ország (lakosság, gazdaság és kormányzat) működése szempontjából létfontosságúak és érdemi szerepük van egy társadalmilag elvárt minimális szintű jogbiztonság, közbiztonság, nemzetbiztonság, gazdasági működőképesség, közegészségügyi és környezeti állapot fenntartásában.
Kritikus infrastruktúrának minősülnek azon hálózatok, erőforrások, szolgáltatások, termékek, fizikai vagy információtechnológiai rendszerek, berendezések, eszközök és azok alkotó részei, melyek működésének meghibásodása, megzavarása, kiesése vagy megsemmisítése, közvetlenül vagy közvetetten, átmenetileg vagy hosszútávon súlyos hatást gyakorolhat az állampolgárok gazdasági, szociális jólétére, a közegészségre, közbiztonságra, a nemzetbiztonságra, a nemzetgazdaság és a kormányzat működésére."
[2080/2008. (VI. 30.) Korm. Határozat a Kritikus Infrastruktúra Védelem Nemzeti Programjáról 3.2 pont].

terheléses támadásokkal, számítógépes vírusokkal, „férgekkel”, logikai bombákkal, a web-tartalom felülírásával (defacing) stb.

- titoksértő támadások: kémprogramokkal (spyware-ekkel), titkos lehallgatásokkal (közbeékelődéses támadás - man-in-the-middle attack), jogellenes belépés valamely számítógépbe vagy számítástechnikai rendszerbe hacking), adathalászat (phishing), wifi-jel-lopás (war-driving) stb.

Didaktikai szempontokból tartalom-, és támadó visszaélések, bűncselekmények alapján elemezzük a bűncselekményeket.

Tartalom-bűncselekmények a számítógépes hálózatokon

A tartalomközlés a felhasználók zömének elérhető a Surface Weben történnek. Ez az Internet elérhető, kereshető része, - a különböző tematikájú weboldalak, a közösségi oldalak, videómegosztó oldalak, az elektronikus hirdetőtáblák (bulletin boards), a hírcsoportok (news-groupok) oldalai, blogok, a tárhelyszolgáltatók fórum oldalain, a chat-, twitter-, messenger-instagram és más kommunikációt biztosító nyilvános alkalmazás, a felhasználó által készített és mások számára is elérhető médiumok (pl. saját rádióállomás, saját televíziósműsor).

Továbbá tartalomközlések küldhetők különböző kommunikációt lehetővé tevő alkalmazással, így például elektronikus levélben, sms-ben, mms-ben, skype-on.

A jelszavakkal, belépési kódokkal védett, ún. Deep Weben az FTP-, a goopher-, a telnet-akadémiai stb. hálózatokon, az intra-, és az extraneten is megjelenhetnek jogellenes tartalmak, ám ezeknek elérése csak meghatározott hozzáférőknek lehetséges.

A közlések fájlformátuma közömbös, megjelenhetnek és elérhetők szöveg-, kép-, rajzábrázolásokban, a weboldalhoz csatolt audió- és videófájlokban.

Ezek a tartalmak lehetnek:

- *vagyoni viszonyokat sértő cselekményekre történő felhívások*, ezen belül:
- csalásnak minősülő cselekmények: nigériai levelek, iraki levelek, spanyol lottó, holland lottó és más megtévesztő hirdetések stb.
- piramisjáték szervezése, lebonyolítása stb.,
- *a közösséget és egyének becsületét sértő tartalmak*: becsületsértő, rágalmazó, rasszista, xenophob tartalmak megjelenítése, zaklatás (cyber-bullying),
- *pornográf, pedofil* tartalmak,
- *kábítószerek, doppingszerek* elérésére, - fogyasztására-, forgalmazására szolgáló tartalmak,
- bomba-, és más *fegyverek készítését* leíró tartalmak, az ezek elkészítéséhez szükséges információk publikálása számítógépes hálózatokon, weboldalakon.

Természetesen a tartalom jellegű bűncselekmények egyben „támadó jellegű” is, hiszen különféle, a büntetőjogban védett életviszonyokat sért.

Látható, hogy a tartalomközléssel elkövethető bűncselekmények jellemzően tradicionális deliktumok. A megtévesztő, szélsőséges véleményt megjelenítő tartalomközlések új helyszínre is áttevődnek. E modern környezetben a bűncselekmények veszélyesebbnek is értékelhetjük, mivel a felhasználók nagyon nagy száma ismerheti a jogsértő tartalmat, azokról megszámlálhatatlan másolat készíthető, kinyomtatható,

továbbítható, terjeszthető közösségi oldalakon, más weblapokra feltölthetők, a weboldalakon, gyorsítótárolókban (cache) hosszú ideig elérhetők.
Valós térben általában ezek a bűncselekmények kisebb közösségben és rövidebb ideig hatnak, megismerhetőségük is korlátozottabb.

Az Internet kimeríti a Büntető Törvénykönyvben definiált nagy nyilvánosság fogalmát. A Btk. 459.§ 22. pontja szerint „nagy nyilvánosságon a bűncselekménynek a sajtótermék, médiaszolgáltatás, sokszorosítás vagy elektronikus hírközlő hálózaton való közzététel útján történő elkövetését is érteni kell."
Függetlenül, hogy valójában hányan érik el, hányan olvassák a közlést, a maga teljességében vagy annak egyes részleteit. Amennyiben a nagy nyilvánosság értékelt az egyes tényállásokban, az vagy alapesetben vagy minősített esetben szerepel.

A hazai Büntető Törvénykönyvben a tartalomközléssel megvalósítható tényállások akkor alkalmazhatók, ha a weboldal magyarországi TCP/IP számról működik, illetőleg a nemzetközi bűnügyi jogsegély keretében az elkövetőket magyar haságok vonják felelősségre.

- *Egyes természetes személyek, személyközösségeket sértő cselekmények* minősítése:
Aki becsület csorbítása céljából hamis, hamisított vagy valótlan tartalmú hang- vagy képfelvételt feltölt számítógépes hálózatokra az *becsület csorbítására alkalmas hang- vagy képfelvétel nyilvánosságra hozatala* (Btk. 226/B.§) vétségének minősülhet.
A számítógépes programok alkalmasak a tényállásban írt falzifikálásra, képrészletek összevágására, egybemosására, részletek kiretusálására, a készítés dátumának meghamisítására, a hangok eltorzítására, különböző időben vagy helyen tett kijelentések összevágására és más hamisításokra.

Aki valakiről más előtt a becsület csorbítására alkalmas tényt állít, híresztel, vagy ilyen tényre közvetlenül utaló szöveget, képet, hang- vagy videófelvételt tesz közkinccsé az Interneten, az a *rágalmazás* (Btk. 226.§ 2 bekezdés b. pontja) vétségét valósíthatja meg.
Tényként vehető figyelembe minden múltban vagy a jelenben létező jelenség (emberi magatartás, viselkedés, elhangzott kijelentés, leírt tartalom stb.), amely a külvilág számára megismerhető, bizonyítható.
Tényközlés egy-egy múltbeli magatartás (pl. bűncselekmény elkövetése, múltban történő politikai szerepvállalás, privát életének intim részleteinek feltárása), esemény említése.

Aki viszont a becsület csorbítására alkalmas – nem tényt vagy tényre utaló – tartalmat tesz elérhetővé mások számára bármilyen fájlformátumban az Interneten, az a becsületsértés szabálysértését követheti el (Szabálysértési tv. 180.§).

Amennyiben a sértett munkakörének ellátásával, közmegbízatásának teljesítésével vagy közérdekű tevékenységével összefüggésben teszi a becsületsértés vétségét (Btk. 227.§) követheti el.

Becsületsértő a nyíltan szidalmazó, durva, megalázó, jellemzően jelzős szerkezettel kifejezett kijelentések.

Szintén szabálysértésként értékelhető annak tartalomközlése, aki mást félelemkeltés céljából a megfenyegetett személyre vagy annak hozzátartozójára vonatkozó, a becsület csorbítására alkalmas tény nagy nyilvánosság elé tárásával komolyan megfenyeget. (Szabálysértési tv. 178.§)

Büntetőjog szabályai szerint felel az, aki elhalt személyt vagy annak emlékét gyalázó tartalmat tesz közzé számítógépes hálózatokon, cselekménye kegyeletsértés vétségének (Btk. 228.§) értékelhető.

Valamennyi említett esetben, ha a közérdek vagy bárkinek a jogos érdeke indokolja valóság bizonyításának van helye (Btk. 229.§ (2) bekezdés).

- A különböző *közösségeket sértő tartalomközlések*

Az emberi becsületet védő büntetőjogi tényállások mellett, bizonyos feltételekkel helyett is a magánjog nyújt védelmet.

A Polgári Törvénykönyv biztosítja az a jogot, hogy a közösség bármely tagja jogosult a személyisége lényeges vonásaként értékelhető, jellemzően a magyar nemzethez, illetőleg az adott nemzeti, etnikai, faji vagy vallási közösséghez tartozásával összefüggésben a közösséget nagy nyilvánosság előtt súlyosan sértő vagy kifejezésmódjában indokolatlanul bántó jogsérelem esetén polgári bírósághoz fordulni.

A bírósághoz fordulás joga nemcsak a sportpályán szereplőt, hanem az érintett közösség más tagját is, aki a sportpályán, mint nézőt, továbbá a sportpályán történtekről a televízió-, rádió-internet stb. közvetítéssel egyidejűleg, akár később bármely forrásból értesült.

A jogsérelmet közvetlenül elszenvedett személy az elévülési időn belül fordulhat a bírósághoz és a Ptk. -ban meghatározott bármely szankció alkalmazható.

A közösség más tagjának a lehetőségei némileg korlátozottak, csak a jogsértést követő 30 napon belül fordulhat a bírósághoz és nem kérheti a jogsértéssel elért vagyoni előny átengedését.

A Ptk. személyiségi jogsértés esetén az alábbi szankciókat kínálja fel a bíróságnak:

Ptk. „2:51. § [Felróhatóságtól független szankciók]

(1) Akit személyiségi jogában megsértenek, a jogsértés ténye alapján - az elévülési időn belül - az eset körülményeihez képest követelheti

a) a jogsértés megtörténtének bírósági megállapítását;

b) a jogsértés abbahagyását és a jogsértő eltiltását a további jogsértéstől;

c) azt, hogy a jogsértő adjon megfelelő elégtételt, és ennek biztosítson saját költségén megfelelő nyilvánosságot;

d) a sérelmes helyzet megszüntetését, a jogsértést megelőző állapot helyreállítását és a jogsértéssel előállított dolog megsemmisítését vagy jogsértő mivoltától való megfosztását;

e) azt, hogy a jogsértő vagy jogutódja a jogsértéssel elért vagyoni előnyt engedje át javára a jogalap nélküli gazdagodás szabályai szerint."

A bíróság mérlegelésétől függ, hogy melyik szankciót alkalmazza, bármely szankció önálló jogvédelmei eszköz is lehet.

A Surface Weben gyakorta megtévesztő, *csalárd közlésekbe* ütközünk. Ezek célja az, hogy a gyanútlan, felkészületlen felhasználókat rávegye előnyökkel kecsegtető pénzügyi műveletekre, ami aztán valójában kárt okoz számukra. A csalásra irányuló közlések tárháza kimeríthetetlen, mindössze néhány ismertebb e körbe tartozó tipikus esetet említünk:

- Jogtalan vagyoni haszonszerzési célú megtévesztő információkat tartalmazó e-mailek és egyéb közlések is „keringenek" a számítógépes hálózatokon. Az ún. nigériai levelek, iraki levelek és ezek számtalan változata például segítséget kérnek későbbi busás haszon ígéretével. A nigériai levelekben vagyonok visszaszerzéséhez szükséges költségek fedezéséhez kérnek támogatást, amelyet majd a visszakapott vagyonból fizetnének vissza nagy haszonnal. Az iraki levelekben egy amerikai katona által Irakban talált mesés kincsek hazahozatalához kérnek hozzájárulást, amelyet a talált kincs értékesítését követően fognak visszafizetni nem csekély felárral.

Ugyanígy megtévesztő a holland vagy spanyol lottó nyereményéről történő tájékoztatás, amelyben nyereményátvételéhez szükséges költségeket kérnek, amelyek a nyereményátvételhez kellenének.

Közösségi oldalakhoz kapcsolódik a csalásnak azon formája, amelyben ismerősnek jelentkezik egy ismeretlen személy, aki a személyes kapcsolatfelvétel létrehozásához segítséget kér a legkülönfélébb valótlan indokokkal, például az állítólag ellopott vasúti-, repülőjegy pótlására, a közbejött betegsége költségeinek fedezésére.

A vagyoni haszonszerzés céljából történő tévedésbe ejtés, amely kárt okoz *csalásként* értékelhető (Btk. 373.§).
Amennyiben a megtévesztő közlés jótékony adománygyűjtés színlelése céljából kerül megosztásra, még ha 50.000.- forintot sem éri el, akkor e körülmény miatt bűncselekménynek minősül (Btk. 373.§ (2) bekezdés bd. pontja).

- A megtévesztő közlések sokféleségét jellemzi az, hogy piramisjáték szervezése folyik. A láncszerűen belépő könnyelmű felhasználók a láncban előttük álló felhasználók számára közvetlenül, vagy a játék szervezőjén keresztül jellemzően pénzfizetést vagy esetleg más szolgáltatás teljesítését vállalják a kilátásba helyezett, de valótlan nyereség fejébe.(Btk.412.§).

- Aki e-kereskedelmi oldalakon az áru értékesítése érdekében az áru lényeges tulajdonsága tekintetében valótlan tényt vagy valós tényt megtévesztésre alkalmas módon közöl, megtévesztésre alkalmas információkat oszt meg bámely fájlformátumban a *fogyasztók megtévesztése* (Btk. 417.§) vétségéért felelhet.
Az ilyen közlések jellemzően C2C (consumer to consumer relációban, a fogyasztó keresi a fogyasztót, pl. aukciós, secondhand web-oldalakon, elektronikus hirdetőtáblán) fordulnak elő, de – sajnos – nem zárható ki B2C (Business to Consumer, pl. webáruházak kapcsán) vagy B2B (Business to Business, üzleti partnerek keresnek üzleti partnereket) kapcsolatban sem.

A tartalomközlések között az egyik legnagyobb veszélyt a kábítószerekkel foglalkozó oldalak rejtik. Sok esetben mintegy polemikus oldalt látunk, ám a viták mögött kábítószertermesztéshez, az ahhoz szükséges eszközökhöz, magokhoz való hozzájutást teszik lehetővé.
A kábítószerek fogyasztását ösztönző tartalom feltöltése felhívásként, tehát a *kábítószer-kereskedelem* bűncselekményének előkészületi magatartásnak minősülhet (Btk. 177.§ (5) bekezdése).
A kábítószerek készítésének elősegítéséhez szükséges anyag, berendezés vagy felszerelés beszerzését kínálja fel, az is értékelhető *kábítószer készítésének elősegítésének* felhívásaként, tehát előkészületi magatartásként (Btk. 182.§ (4) bekezdése).

A számítógépes hálózatok jótéteménye, hasznossága, és azon zajló világméretű, gyors, szabad (és bizony, sokszor szabados) kommunikáció napjaink realitása.

A kábítószer-probléma nem jogi probléma. A megoldatlan, feldolgozat(hatat)lan személyi-családi vagy (remélhetőleg nem „és") társadalmi–gazdasági – akár külön-külön, akár együttes - problémák mind-mind okai lehetnek a drogokhoz fordulásnak.
A büntetőjog teljes szigorával kell fellépni, erőt demonstrálni a kábítószer-kereskedőkkel szemben.
A szülők kötelessége az, hogy ne hagyják magukra a kiskorúakat problémáikkal, nehézségeikkel a valóságos térben!
Hívják fel figyelmüket a kábítószerek fogyasztásának veszélyére, a pótcselekvés hiábavalóságára, óvják gyermekeiket a kábítószerrel történő találkozástól nemcsak a valóságos, hanem a virtuális térben is!
Legyen ez a másik nyomós érv arra, hogy a szülők is belemélyedjenek a számítógép, az Internet világába. Ugyanígy a számítástechnikai ismereteket oktató, vagy más tanároknak is figyelmeztetniük kell a kiskorúakat!

- Tartalomközléssel megvalósulhatnak *köznyugalom elleni bűncselekmények* (Btk. XXXII. fejezet) is. Így a nemzetiszocialista vagy kommunista rendszerek bűneinek nyilvános tagadása, azok kétségbe vonása, jelentéktelen színben történő feltüntetése (Btk. 333.§), a nemzeti jelkép megsértése, meggyalázása, lealacsonyító ábrázolása bármely fájlformátumban, pl. zászlóégetés bemutatása videófelvételen, nemzeti jelképek sértő képi vagy szöveges ábrzáolása, a himnusz zenéjének sértő áthangszerelése, szövegének sértő átírása (Btk. 334.§), továbbá az önkényuralmi rendszerek áldozatainak emberi méltóságát, kegyeleti jogát sértve önkényuralmi jelképek használata pl. az áldozatok emlékét megjelenítő oldalak deface-elése (Btk. 335.§).

- Valótlan tényeken, illetőleg a valós tények elferdítésén alapuló közveszéllyel járó esemény (pl. hamis bombariadó) bekövetkeztével történő fenyegetés is elkövethető számítógépes hálózatokon. Ez esetben a közlés *közveszéllyel fenyegetésnek* (Btk. 338.§) minősülhet.

- Háborús hírverés is folytatható számítógépes hálózatokon és ez a magyar büntetőjog szerint *háborús uszításnak* minősülhet (Btk. 331.§).

- Nemcsak a Dark weben, hanem a Surface Weben is elérhetők hamis közokiratok (pl. nyelvvizsga bizonyítványok), amelyeket a bűnelkövetők kínálnak megvételre. Ha a közokirat kiállításra kerül a megrendelő számára, akkor a készítő a *közokirathamisítás* (Btk. 342.§)

tetteseként vonandó felelősségre, míg a hamis közokiratért fizető személy a hamis közokirat felhasználásának előkészületét valósíthatja meg.

Jogellenes belépés számítógépbe, elektronikus adatfeldolgozó- és átviteli rendszerbe (hacking)

A *hacker*-nek olyan mesterember, aki faipari munkát végez, fát farag stb. Az 50-es évek végén az MIT nagygépek programozói nevezik így magukat. Az akkori nagygépek szűk memóriakapacitásával küszködnek. A programokból törekszenek "faragni" minél karaktert, hogy minél több hely maradjon a memóriában. Ez a forrása az ún. Y2K-problémának (a "milleneumi bombának"). A 2000-et takarékossági megfontolásból 00-nak ábrázolták. Ezáltal az évszám a számítógép számára 1900-zal vagy más 00-ra végződő évszámmal összekeverhető.

Az angolszász országokban a hacking cselekményét a "házi béke" megsértéseként fogják fel.

Az "elektronikus betörés" a számítógépes rendszernek közvetlen, az adatállomány közvetett veszélyeztetésének legkorábbi stádiuma.

A hackerek a számítógép, e-mail, más program, alkalmazás jelszavát a következőképpen szerezhetik meg:

- erőszakkal, fenyegetéssel,
- social engineering (pszichikai manipuláció) módszerével,
- kódtörő program használatával,
- spyware (kémprogrammal) kitudakolva a jelszót, továbbá
- a felhasználó vétkes könnyelműsége miatt szerezheti meg.

Miután a hacker belépett a számítógépbe, bármit megtehet a számítógép memóriájában tárolt adatokkal, azokat lemásolhatja, kifotózhatja, törölheti, felülírhatja, az adatállományt átrendezheti, a programokat törölheti, malware-eket tölthet fel, leformázhatja a számítógépet stb.

Tisztázandó az a kérdés, hogy a hacker nem szinonim kifejezés a bűnözővel. Ma Magyarországon is létezik etikus hacker, (angol kifejezéssel „white hat hacker” képzés), akikre honvédelmi, rendőrségi feladatok teljesítése hárul. Létezik önkéntes kiberhadsereg, amely együttműködik a megfelelő szervezetekkel, segíti azok munkájukat, tapasztalataikat megosztja velük.

Léteznek gazdasági vállalkozások, amelyek üzleti alapon, szerződéssel számítástechnikai rendszerek biztonságát tesztelik, annak kiépítéséhez segítséget nyújtanak.

- a hacker a „legális betörések” etikai és jogi szabályrendszerét ismeri és betartja,
- az összes rosszindulatú „behatolási” módszertant ismeri,

- folyamatosan tanul, fejleszti szakmai tudását a legújabb technológiákból
- mindig egy lépéssel a rosszindulatú hacker előtt jár
- a megszerzett információkat nem haszonszerzésre, hanem a védelem érdekében használja fel.[2]

A „black hat hacker" azonban az informatikai rendszer védelmét biztosító technikai intézkedések megsértésével vagy kijátszásával jogosulatlanul belép, jogosultsága kereteit túllépve bennmarad, amiért büntetőjogi felelősséggel tartozik (Btk. 423.§ (1) bekezdése).
A hackerek kettőségének sajátos példája az ún. *Anonymus-jelenség*[3]. Számtalan hackingnél, defacingnél (weboldal engedély nélküli átalakítása), szerzői jogsértésnél, vagy káros tartalmak eltávolításánál olvasható, hogy „Anonymus" követte el. Kik ő? Egy bigott katolikus merénylő Guy Fawkes (1570-1606), - aki I. Jakab angol protestáns király életét akarta kioltani - maszkját viselik. Tulajdonképpen bárki lehet Anonymus, aki annak vallja magát. Az Anonymus vagy akár az Anonymus-csoport nem egyetlen személy, nem is szervezett csoport, nem tudni azt sem, hogy létezik-e ilyen csoport állandó tagokkal? Nyilván vannak olyan személyek, csoportok, akik annak vallják magukat, gyakorta vagy mindig használják an Anonymus álnevét akciójuknál, de akár egyetlen személy egyetlen akcióját is elkövetheti Anonymus álnévvel. Ténykedésük cyber-anarchizmusként is értékelhető. Az Anonymusok nem egyértelműen „black-hackerek", hiszen a káros vagy tiltott tartalmak törlése, azok deface-elése, terrorista személyének leleplezése (pl. az ISIS tagjainak adatait hozták nyilvánosságra) és más ténykedések hasznosnak ítélendők, bár ez ebben a formában jogellenes („grey-hacking").
Tegyük hozzá, némi éllel, hogy a nekik nem tetsző, tiltott tartalmak törlésével, deface-elésével - legitimnek egyáltalán nem nevezhető módon – „rövidre zárják", „kiiktatják" a különböző jogi akadályokat (joghatóság problémája, eltérő erkölcsi, és ezzel eltérő jogi megítélést von maga után), amelyek ezen inkriminált tartalmak levételének az útjában állnak.

[2] [2] http://www.kurt.hu/kurt_hirek_reszl.php?id=39 [2016.12.30.]
[3] Az Anonymus álarc nem más, mint Guy Fawkes arcát stilizálja, aki 1605. november5-én megpróbálta megölni a Stuart-házból származó I. Jakab angol királyt, aki a protestáns Angliában a katolikusoknak, katolicizmusnak tett egyoldalú engedményeket. A robbantásos merénylet sikertelen volt, ennek örömére Nagy-Britanniában a mai napig ez a tűzijátékokat rendeznek.

Wardriving és defacing

Ez a cselekmény annyiban hasonlít a hackinghez, hogy e körben is jogosulatlan belépés történik a számítógépbe, és egyben a számítógépes hálózatba. A jelenség nem olyan félelmetes, amint az az angol elnevezésből következnék. A wardriving lényege, talán elnevezése is lehetne a következő: védett WiFi-jel „lopás". A visszaélés nem képzelhető el vezeték nélküli adatátvitel technológiája nélkül. Az 1991-ben megalkotott vezeték nélküli kapcsolat több technológiát is felöl: az infravörös adatátvitelt, a vezeték nélküli hálózatot, például a WiFi-t (Wireless Fidelity-t). Mindegyik technológiában közös az, hogy az adatátvitel rádiófrekvenciás hullámokon keresztül zajlik.

A WiFi–kapcsolat elérhetősége a következő módokon történhet:

Publikus, nyílt hálózat: bármely WiFi routerrel kialakítható, az így létrehozott hálózathoz bárki csatlakozhat, mindenféle korlátozás nélkül (például a városok köztéri hálózatai). Privát hálózat saját felhasználásra hozható létre, például egy lakáson belül.

Publikus, zárt hálózat: egy speciális szoftver gondoskodik arról, hogy a hálózatot csak egy kód ismeretében, korlátozott ideig lehessen használni. Ezt a formát rendszerint vendéglátóhelyek használják. A kereskedelmi hotspot szolgáltatás csak díjfizetés ellenében vehető igénybe.

Ma számítógépeinkkel és mobiltelefonjainkkal és elektronikus eszközeinkkel „hotspot"-okon („elérési pontokon"), vagyis vezeték nélküli Internet elérési pontokon keresztül csatlakozhatunk a világhálóhoz. A mobilinternet használata azon alapszik, hogy egy hordozható eszköz (pl. ún. okostelefon, tablet) közvetlenül vagy notebook, asztali számítógép és más eszköz esetében egy pen-drive nagyságú modem segítségével kapcsolódik a vezeték nélküli hálózathoz. A WiFi hálózatot felhasználónév/jelszó biztosítja a felhasználónak az exkluzív használatot. A szolgáltatás ingyen vagy fizetés ellenében vehető igénybe. Általában havi díjban foglalt adatforgalomra lehet elfizetni, az ezen felül a letöltött adatmennyiséghez igazodóan kell további pénzösszeget fizetni.

Amennyiben a felhasználó felkészületlensége vagy gondatlansága miatt nem védi előfizetéses hálózatát azonosítókkal vagy a védelmi funkciót kikapcsolja vagy egyszerű, könnyen kiismerhető jelszót használ vagy azonosítóit megosztja másokkal, akkor előfordulhat a jogosulatlanul kapcsolódó felhasználó a szerződéses adatmennyiséget eléri vagy annál több adatmennyiséget tölt le vagy fel, amiért viszont az előfizetőnek fizetni kell.[4] A

[4] Blutmann László – Karsai Krisztina – Katona Tibor: Miért nem lehet a vezeték nélküli internet a lopás elkövetési tárgya? Bűnügyi Szemle, 2008/1. I. évf. 1. szám 42-49. o.

többletköltséget okozó WiFi lopás lopásnak minősülhet (Btk.370.§). Ha viszont kárt nem okoz a jogosulatlan belépés egy védett hálózatba, akkor hackingként értékelhető (Btk. 423.§ (1) bekezdése).
Az Internet szabad elérhetőségének bővülésével a wardrivingnak nem lesz lehetősége.

A weboldal tartalmának jogellenes megváltoztatása az ún. *defacing*, amely olyan cselekmény, ami a weboldal szöveges tartalmát, vizuális megjelenését módosítja, ahhoz egy másik audió- vagy videófájlt csatol. Lényegében egy elektromos graffiti. A hacker átveszi az oldal szerkesztését, egyszersmind az oldal feletti „uralmat". Politikai, vallási és véleményt közlő weboldalak a veszélyeztettek. A kiberháborút vívó felek és terroristák gyakran élnek a weboldal tartalmának felülírásával elsősorban dezinformálás céljával, a saját sikereiket felnagyítják, kudarcaikat elfedik, a valós tájékoztatást akadályozzák. A deface-elt weboldalak olvasóikat elveszíthetik, reklámértékük csökken, az üzemeltető goodwilljét rombolják.
A defacer azzal, hogy az információs rendszerben lévő adatot jogosulatlanul vagy jogosultsága kereteit megsértve megváltoztat, töröl vagy hozzáférhetetlenné tesz bűncselekményt követ el (Btk. 423.§ (2) bekezdése b) pontja).

A malware támadások

A számítógépes adatok és programok, a számítógépek és a számítástechnikai rendszerek elleni intellektuális támadás egyik rendkívül veszélyes és alattomos formája a *malware-támadások*. A malware gyűjtőfogalom, e körbe vonhatók a vírusok (rootkitek, trójai, zsarolóvírusok), „férgek”, logikai bombák és más kárt okozó programokat, illetőleg a spyware-eket, mint kémprogramokat, ezek azok a programok, amelyek a számítógépes munkafolyamatot, elektronikus adatot, a számítástechnikai eszközöket károsítja. A malware kifejezés valamilyen rosszindulatú programot jelent, amely a malicious software angol szavak összetételéből származik.

A hetvenes években csupán szakmai körökben "suttogtak" róla, de a nyolcvanas években már a szélesebb szakmai körökben tért hódít egy új fogalom, a vírusprogram. A fogalom eredete az orvostudomány hasonló kategóriájából származik. Ugyanis a komputervírus szintén egy gócpontból kiindulva "fertőzi meg" az adatállományokat, programokat. A sajtóban e vírusokról pusztító hatásuk miatt "számítógépes AIDS-nek" valamint "delírium digitalis-nak" vagy hasonló hangzatos elnevezésekkel találkozunk.
Az első vírusok egyikét, az Elk Clonert egy 15 éves fiatal felhasználó alkotta meg. Azóta a vírusok, és más malware-programok százezrei keringenek a számítógépes hálózatokon.
Néhány ismert program típusú malware:
- A számítógépvírusok és programférgek különböző károsító programok, amelyek adatállományok, programok, hardver ellen irányulnak. Hatásuk sokféle, a programok az elektronikus adatforgalmi- és átviteli rendszerek működését akadályozhatják, lassíthatják, leállíthatják, törölhetik, titkosíthatják a számítógépen található a fájlokat, könyvtárakat, a programok eredeti működését befolyásolhatják, telíthetik a számítógép memóriáját.
- A *trójai - program* egy másik programhoz kapcsolódik. Az eredeti program indításakor a felhasználó tudta és akarata nélkül aktiválódik (pl. egy letöltött játék-programmal egy másik malware-t is telepítünk gépünkre).
- A *backdoor* - programok pedig a számítógép védelmi rendszerén nyitnak utat egy másik rosszindulatú program számára.
- A *dialer* program a telefonhoz modemen keresztül kapcsolódó számítógépeknél hatásos. A betárcsázó-program a számítógép indításakor a felhasználó tudtán kívül egy emelt-díjas számot hív akár folyamatosan. A hóvégi telefonszámla kifizetésekor szembesül a felhasználó a magas költséggel. Ma már egyre ritkább.

- A *spyware-ek* (kémprogram általános elnevezéssel) a felhasználó aktivitását (a számítógép-, és Internethasználatunkat is) rögzíti, jelszavainkat, más ránk vonatkozó adatot fürkész ki és továbbítja egy másik számítógép számára a hálózaton. Részben hírszerzési célokat, részben marketing-célokat szolgálnak. Ez utóbbi esetben (természetesen) nem a nagy vagy hivatalos marketing-cégek terjesztik, de a mások által gyűjtött „információkat elfogadják" (megvásárolják).
- A *keylogger-programok* speciális kémprogramok, ami billentyű-leütéseinket rögzítő, naplózó kémprogram. Tipikusan a begépelt szöveg kifürkészése a cél.
- *Flame* és *Gauss* – ma ismert kémprogramok. Tulajdonképpen egy multi-kémprogram, mindenre kíváncsi.

Az ad-ware-ek, és spyware-ek elleni *védekezésnek* többféle formája van:
Ne töltsünk le (feleslegesen) mindenféle programot, különösen nem azonosítható oldalról.
Próbáljunk a program kibontásának, aktiválásának minden egyes fázisára alaposabban odafigyelni. (Pl. milyen más programokat jelez a letölteni kívánt program.)
Használjunk tűzfalat, amely meggátolja a számítógépünkről kimenő adatáramlást.
Használjunk ad-ware, spyware elleni programokat (pl. az Ad-Aware program).

Néhány ismert szöveg típusú malware:
- A *spam*[5] kéretlen kereskedelemi küldeményeket jelent (hirdetések, semmire sem jó felmérések stb.). Sajnos, milliószámra terjednek számítógépes hálózatokon, foglalva az e-mailek memóriáját, használva a rendszergazdák drága munkaidejét, idegesítve felhasználókat a spam-ek törlésével.
- A *hoax-levelek* általános, gyerekes szövege, a felhasználó babonás félelmére apellál, hogy „küldd tovább xy.. példányban, mert … balszerencse ér."

Veszélyességük miatt ki kell emelni néhány malware-fajtát. A *Stuxnetet* és *DuQut* azért kell külön kezelnünk, mert eltér az eddigi malware-ek tulajdonságaitól, és ez veszélyességüket rendkívül megnöveli.
Egyfelől, míg az ún. nulladik napi támadást követően a malware-ek hatásmechanizmusa ismert lesz, így az ellenük kifejlesztett vírusirtó programok is hamarosan megjelennek - és legálisan vagy illegálisan – hozzáférhetők. Egy „macska - egér harc" folyik, ismertté válik

[5] Sütő János: SPAMtelenül. Budapest, SZAK Kiadó, 2008. 3-9. o.

egy általános jellemzőkkel bíró (valamennyi fertőzött számítógépen ugyanazon károkat okozó) malware, majd megjelenik ennek az ellenszere.
A Stuxnet és a DuQu egyedi, célzott hatása miatt nem valószínű, hogy lesz általános ellenszere (felismerés, irtás).
Másfelől, míg a kommersz malware-ek hatása ismert, addig ennek a két új malware csak egyetlen célba vett technikai - technológiai vagy más művelet megbénítására alkalmas.
A Stuxnet nevű malware az iráni natanzi atomerőmű urándúsítását vezérlő számítógép működésének akadályozására készült és sikerrel használták. Ezeknek az újtípusú malware-eknek az alkalmazása azért veszélyes, mert túl azon, hogy ismeretlenek, egyetlen művelet, egyetlen cél végrehajtására íródnak. Kiszámíthatatlan, hogy a kritikus infrastruktúra mely elemét, folyamatát veszik, vehetik célba és annak milyen hatása lesz. Hogyan mutálódik majd a malware, az elektronikus adatfeldolgozás- és átvitel mely pontján, mikor és ki fogja feltölteni a rosszindulatú programot.

A malware-t zsarolási célzattal már az 1990-es években használták. A zsarolóvírusok megjelenése az otthoni számítógépek elterjedésével egyidős: 1989-ben floppy lemezen érkezett az első hasonló kártevő. Joseph Popp biológus programot írt, amely címében az AIDS-re vonatkozó információkat tartalmazta. Ez azonban valójában egy "trójai faló" program volt. Az "AIDS Information Disk" számítógépbe történő betöltése után arra szólította fel a felhasználót, hogy küldjön pénzt egy privát panamai postafiók címére. Ennek fejében Popp küldött (volna) egy újabb szoftvercsomagot. Ellenkező esetben a lemezen rögzített program 90. hozzáférést (újraindítást) követően tönkreteszi, pontosabban a felhasználó számítógépében rögzített adatállományát titkosítja. Az inkriminált lemezeket Popp angliai és panamai címekről 20 ezer (!) címzettnek küldte el, amelyekből Magyarországra is érkezett két (?) lemez.[6]
A *zsarolóvírus* (ransomware)[7] modern változata már online terjed, az elővigyázatlan felhasználók telepítik számítógépeikre. A program a számítógépen levő adatállományt

[6] http://www.origo.hu/techbazis/20170421-floppyn-erkezett-a-vilag-elso-zsarolovirusa.html [2017.05.21.]
[7] https://ransomware.hu/ [2017.05.21.] Zsarolóvírusok típusai:
- Fájltitkosító ransomware-ek: rendszerbe jutva gyors sebességgel megkeresi és titkosítja a személyes fájlokat. A titkosítást követően a zsarolóvírus egy figyelmeztető ablakot jelenít meg, amely azt állítja, hogy az adatok visszaállításának egyetlen módja a váltságdíj kifizetése. Az új típusú zsarolóvírusok már képesek a teljes merevlemezt is titkosítani. (Petya)
- Nem titkosító ransomware: A fertőzést követően a vírus lezárja a rendszert és látszólag valamilyen bűnüldöző hatóságtól származó figyelmeztetést jelenít meg (FBI, CIA, Nemzeti Nyomozó Iroda, Rendőrség). A rendszer átvizsgálása során megtalált fájlokat mind bizonyítékként sorolja fel. Továbbá tájékoztatja az áldozatot arról, hogy ha nem fizeti ki a követelt büntetést, akár börtönbe is kerülhet.

letitkosítja, így a felhasználó nem fér adataihoz, könyvtáraihoz. A titkosítás feloldását pénzösszeg megfizetésétől teszi függővé. Az elkövető kilétének megismerése szinte lehetetlen, hiszen a „váltságdíjat" virtuális valutában, Bitcoinban vagy valamely altcoinban kéri. A pénz kifizetése sem garancia arra, hogy a zsaroló a titkosítást feloldja. De előfordulhat, hogy a váltságdíj fejében titkosított adatállomány egyrészét teszi ismét elérhetővé, majd további követelésekkel áll elő. Az elkövetők célja az anyagi haszonszerzés, ezért általában ezek nem célzott támadások, de 2016-ban megfigyelhető volt egy tendencia, amely során sorozatos támadások a kórházakat érintette. Például a Hollywood Presbyterian Hospital Medical Center 17 000 $ értékű Bitcoint fizettet ki, mert a vírus napokig megbénította a kórhát működését. Részben ennek a támadásnak köszönhető, hogy Kalifornia állam Büntető törvénykönyvébe önálló bűncselekményként jelent meg a ransomware felhasználása.[8] A magánvállalkozások, amelyek nagyobb összeget is képesek fizetni, könnyedén válhatnak szintén a zsarolóvírusok célpontjaivá.

Az egyéni felhasználók inkább a *police malware* potenciális áldozataivá válhatnak. A malware, amelyre egy rendőri jelvényt másoltak egy üzenetet küld, amely szerint a felhasználó valamely jogilag tiltott tevékenységet folytatott az Interneten, így a program ideiglenesen működésképtelenné teszi a számítógépet. A malware ugyanis letilt minden programot, ennek feloldása „pénzbírság" megfizetésével történhet. A „váltságdíj" természetesen nem a rendőrséghez, illetve az állami költségvetésbe kerül, hanem bűnelkövetőkhöz, akik korántsem biztos, hogy feloldják a tiltást.

A folyamatos adatmentés minden felhasználónál rendkívül fontos, hogy zsarolóvírusok ne okozzanak a felhasználónak hátrányt.

2017-ben a WannaCry zsarolóvírus söpört végig a világon, amely a Windows sebezhetőségét használta ki. A vírus e-mailek mellékleteiben és fertőzött linkek megnyitásával terjedt, s azért tudott ilyen léptékben rendszereket megfertőzni, mert féregként viselkedve egy lokális hálózatban elég volt, ha egyetlen felhasználó óvatlanul rákattintott a fertőzött fájlra, és máris átterjedt a rendszer többi gépére. A legrosszabb helyzet Nagy-Brittanában volt, ahol National Health Service gépeit teljes egészében blokkolta a vírus. Oroszországban a Belügyminisztérium, és a Sperbank volt érintett, míg Németországban a

---

- Böngészőlezáró ransomware: Ez a ransomware típus nem fertőzi meg a teljes rendszert. Egy Javascript segítségével egyszerűen blokkolja a böngészőket, és figyelmeztető üzenetet jelenít meg.

[8] https://www.barkly.com/hospital-ransomware-healthcare [2017.05.21.]
https://blog.barkly.com/hospital-ransomware-attacks [2017.05.21.]
https://www.bleepingcomputer.com/news/government/new-california-law-makes-ransomware-a-standalone-crime/ [2017.05.21.]

Deutsche Bahn vasútvállalat gépeit támadták, a kijelzőkön megjelent a vírus üzenete. Az Egyesült Államokban a FedEx csomagküldő cég gépei váltak a vírus áldozataivá.[9]

A malware támadások az Információs rendszer vagy adat megsértésének minősülnek (423.§): aki az információs rendszer működését jogosulatlanul vagy jogosultsága kereteit megsértve akadályozza, vagy információs rendszerben lévő adatot jogosulatlanul vagy jogosultsága kereteit megsértve megváltoztat, töröl vagy hozzáférhetetlenné tesz, bűntett miatt három évig terjedő szabadságvesztéssel büntetendő.

A malware-ek feltöltése a számítógépre történhet off-line és online módon:

Az offline feltöltése esetén a számítógéphez fizikailag szükséges hozzáférni. Ha a számítógép jelszóval védett, akkor a jelszó megszerzése (megtévesztéssel, kényszerrel, fenyegetéssel, jelszófejtő programmal, social engineering [pszichológiai manipuláció] módszerével elengedhetetlen.

A malware off-line feltöltése esetén fizikailag nélkülözhetetlen a számítógéphez a hozzáférés. Ha a számítógép jelszóval védett, akkor szükséges a jelszó kifürkészése, megszerzése. Majd a számítógépbe „belépve" valamilyen adattárolóról megtörtént vagy megtörténhetett a feltöltés. A feltöltést maga a számítógép használója is megvalósíthatta, vélhetően tudtán kívül, amikor egy adattárolót a számítógépébe helyezve azt elindította, elindítja vagy a rajta levő fájlokat átmásolta, átmásolja.

Az off-line feltöltésre példák voltak a Stuxnet, illetőleg a Tyupkin-malware. Mindkettő malware feltöltése a munkahelyen „belülről" történt. Ezek az esetek a személyi és technikai biztonsági rendszer hiányosságaira figyelmeztetnek.

On-line feltöltés esetén a számítógép használója az, aki az általa használt számítógépre telepíti a malware-t. A malware-t a felhasználó a számítógépes hálózaton keresztül pl. warez- (wares és software, program és áruk) oldalakról, P2P (peer-to-peer) közvetlen kapcsolatból vagy különböző web-helyekről letöltött tömörített fájlokban, továbbá .exe (esetleg .com) alkalmazásokban, vagy valamely weboldalra lépve indul a letöltés számítógépére. Malware telepíthető e-mailhez csatolt fájl megnyitásával, letöltésével, vagy e-mailben küldött vagy ahhoz csatolt linkre kattintással is.

A malware készítői zömmel az ismeretlenség homályába vesznek. Így felelősségre vonásuk szinte lehetetlen.

[9] http://www.hirado.hu/2017/05/15/vilagszerte-terjed-a-virusfertozes/ [2017.05.21.]

A túlterheléses támadások vagy botnet-támadások

A túlterheléses, 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 igénybevételére – innen a szolgáltatásmegtagadással járó elnevezés is -, amelynek a leggyakoribb formája a webszerver elérését és rendeltetésszerű használatát gátolja a mesterségesen generált és megnövekedett adatforgalommal.[10] Kezdetben 100 Gbps támadások voltak megfigyelhetők, napjainkra ez már a 300 Gbps-ot is meghaladhatja, sőt állítólag 600 Gbps támadásra is sor került és ezek 24 óránál tovább is tarthatnak.[11]

Az elnevezés a támadás angol megfelelőjének rövidítéséből ered, amely során az említett támadás egyetlen számítógéptől származik, több közbeiktatott gép nélkül: Denial of Service (rövidítve: DoS). Amennyiben a támadás összetettebb, mert összekapcsolt rendszerek csoportjától, egyszerre sok – lehetőleg minél több - helyről indul, akkor használatos a Distributed Denial of Service (rövidítve: DDoS), vagyis az elosztott szolgáltatásmegtagadással járó támadás elnevezés. Ebben az esetben feladatot nem egyetlen eszköz végzi el, mint a DoS-támadásnál, hanem a rendszert alkotó – egymástól akár nagy távolságban lévő - eszközök (pl. asztali gépek, mobiltelefonok, vagy routerek stb.) párhuzamosan.[12]

A technikai alapja leegyszerűsítve a következőképpen néz ki: amikor a felhasználó az Internethez kapcsolódik, akkor egyben az ún. 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 ez a szerver a keresett weboldal szerverére irányítja a felhasználót. A támadás esetében pedig a célzott szerverre – egyszerre – ezer-, vagy tízezer számra érkeznek adatcsomagok, amelyekre a szervernek – időrendi sorrendben – válaszolni kellene. A DDoS-támadás során a támadó egy hálózatot alkotó számítógépek adatcsomagjaival elárasztja a célzott szervert akkora forgalommal, hogy az képtelen lesz az adatcsomagok fogadására, azoknak válaszolására, ezzel akár a rendszer teljes leállását is eredményezhetik, azonban a funkcionális

[10] http://www.cert-hungary.hu/ddos [2017.01.06.]
[11] Europol: The Internet Organised Crime Assessment. 2016. 35. o. https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2016 [2017.01.11.]
[12] Gyányi Sándor: Az információs terrorizmus által alkalmazott támadási módszerek és a velük szemben alkalmazható védelem. PhD értekezés. Budapest, 2011. 88. o.

működésképtelenséghez elegendő a nagymértékű lelassulás is, ami a válaszidő megnövekedett mértékéből adódik. Egy mindennapi példán szemléltetve ez úgy néz ki, mintha egy ajtón szépen sorban kopogtatnak és egyesével, szépen sorban beengedjük őket az azonosítást követően, azonban rövid időn belül fennakadást okoz, amennyiben egyszerre több ember dörömböl az ajtón és szeretne bejutni, anélkül, hogy megvárnák, hogy sorra kerüljenek.[13]

A felhasználó tudta nélkül megfertőzött számítógépeket, amelyek távolról irányíthatók „zombi"-nak 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, „botmaster"-nek, illetve több irányító esetén „botherder"-nek hívják. A botnet tagjait a fertőzött zombi számítógépek alkotják. Azt a központi vezérlő eszközt, amely vezérli a botnet-akciókat „controller"-nek hívjuk. A controller általában az ún. „drop server"-re 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 ún. Command&Control (C&C) csatorna.[14] A botnetek alkalmasak a DDoS támadások indításán kívül spamküldésre, adathalászatra,[15] hálózat-figyelésre,[16] billentyűzet-figyelésre,[17] illetve az internetes reklámokhoz a klikkelések begyűjtésére.

A botnetek terjeszkedési fázisa, amely a rosszindulatú program, (malware) - amellyel átveszik a gép feletti irányítást - eljuttatását célozza, általát két féle módon történhet: valamilyen sebezhetőség (pl. a fertőzött tag a saját alhálózatban keres operációs rendszer hibát vagy futatott program rést, a tűzfal nem megfelelő konfigurációját és ezt kihasználva fertőzi meg) vagy a felhasználó hiszékenységének a kihasználásával (pl. a botok vírust tartalmazó mellékletet vagy fertőzött weblapra mutató linket tartalmazó kéretlen e-mailt, üzenetet küldenek, illegálisan letöltött programokkal).[18] Bármely felhasználó számítógépe bármikor

[13] Nagy Zoltán András: A sértett szerepe néhány kibertérben elkövetett bűncselekményben – alkalmazott viktimológia. In: Finszter Géza – Kőhalmi László – Végh Zsuzsanna (szerk.): Egy jobb világot hátrahagyni… Tanulmányok Korinek László professzor tiszteletére. 2016. 487. o.
[14] Gyányi: i.m. 89. o.
[15] A botnetek képesek nagy mennyiségű személyes vagy egyéb titkos adat megszerzésére. Általában jól ismert cégek – főleg bankok, pénzintézetek – nevében e-mail üzeneteket küldenek, melyekben azt kérik a felhasználótól, hogy lépjen be elektronikus úton fiókjába. A levél általában egy linket is tartalmaz, hogy az áldozat könnyebben eljuthasson a honlapra. A link azonban nem a cég weblapjára mutat, hanem egy ahhoz kísértetiesen hasonlító – esetleg kívülről nem is megkülönböztethető – ál-honlapra, mely többnyire a botnet valamely tagján fut.
[16] A botok felruházhatóak a hálózaton áthaladó adatcsomagok megfigyelésére.
[17] A keylogging nem más, mint a felhasználó által lenyomott billentyűk rögzítése és továbbítása a botmasternek.
[18] Faragó Márton – Mészáros Tamás: Anonim rendszer botnet forgalom felismerésére és szűrésére. 2009. 10. o. math.bme.hu/~slovi/farago_meszaros_TDK.pdf [2017.01.05.]

válhat könnyedén „zombigéppé”. A számítógépek a számítógépes hálózatra történő csatlakozással már ki vannak téve a veszélynek, a kockázat pedig különösen megnövekedett az új mobilinformatikai és Internet of Things (IoT)[19] eszközök elterjedésével, főleg azért, mert utóbbinak még nincs megfelelően biztosított informatikai védelme és a többségük magánszemélyek használatban van, akik a biztonsági frissítésekkel hajlamosak nem foglalkozni.[20]

Az első bot, 1999-ben PrettyPart féreg néven jelent meg, ami egy IRC (Internet Relay Chat) szerverhez csatlakozva távolról vezérelte a fertőzött számítógépeket. Napjainkban a botnetek a technológiai fejlődésnek köszönhetően már megosztott hálózatokon, fájlmegosztó rendszereken, peer-to-peer (P2P) hálózatokon, HTTP weblapokon, illetve akár közösségi oldalakon mint a Facebook, Twitter, Reddit-en keresztül is terjedhetnek.

Új trendként jelent meg, hogy a DDoS támadások könnyű indítására szolgáló botneteket, illetve a létrehozásukra szolgáló eszközöket, szoftvereket mint egy szolgáltatásként bérelni (DDoS-for-hire vagy DDoS-as-a-Service) – napi vagy havi díjjal átlagosan 5 $ és 1000 $ közötti áron -, vagy akár vásárolni lehet manapság a fekete online piacokon és fórumokon keresztül (pl. Alphabay és Exploit), amik az ún. Deep Weben keresztül érhetőek el és közös jellemzőjük, hogy nehezen lenyomozhatók. A hackerek gyakran nem egyértelműen hirdetik a szolgáltatásukat, hanem a „stressers” vagy „booters” elnevezést használják. A szolgáltatás igénybevételével a hozzá nem értő felhasználók is olcsón, egyszerűen és gyorsan tudnak támadást indítani, mert csak a célpontot kell kiválasztaniuk, egy egérkattintás az egész, sőt sokszor a végrehajtáshoz technikai segítséget is kapnak. Ezek a szolgáltatások és eszközök kiberfegyvernek minősülnek, ezért velük szemben szigorú és azonnali fellépés szükséges, különösen figyelembe véve az egyre növekvő népszerűségüket és széleskörű elérhetőségüket.[21]

Érdemes felhívni a figyelmet a hazai helyzetre. A magyarországi botnet fertőzöttségre figyelmeztető 2015-ös Symantec tanulmány szerint Magyarország a bot fertőzött

---

[19] http://www.digitalhungary.hu/e-volution/Mi-is-az-az-IoT/2202/ [2017.01.05.]: „Az ’Internet of Things’, vagy rövidítve ’IoT’ magyarul a ’dolgok (tárgyak) internete’, mellyel a mindennapjainkban használt eszközök (például háztartási gépek, autók, mérőórák, pénztárgépek, stb.), az interneten keresztül is elérhetőek, és képesek egymással akár önállóan is kommunikálni. Ennek a kommunikációnak a motorja az ún. M2M (machine-to-machine) technológia, ami olyan adatáramlást jelent, mely emberi közreműködés nélkül, gépek között zajlik. A kommunikáció minden olyan gép között létrejöhet, amely a megfelelő technológiával (érzékelőkkel, chipekkel) van ellátva ahhoz, hogy bekapcsolható legyen a rendszerbe.”

[20] https://www.symantec.com/content/dam/symantec/docs/reports/istr-22-2017-en.pdf [2017.01.05.]: Például a Mirai botnet folyamatosan keres olyan IoT eszközöket, amelyek még a gyári beállításokkal vagy megváltoztathatatlanul hagyott felhasználónévvel és jelszóval rendelkeznek. Amennyiben talál ilyen készüléket, akkor megfertőzi malware-rel, ami arra kényszeríti, hogy jelentsen a központi szervernek, és bottá alakul, amely alkalmazható DDoS támadásra.

[21] James Scott–Drew Spaniel: Rise of the machines: The DYN attack was just a practice run. 2016. 7-12. o.

számítógépek számát tekintve a 6. legfertőzöttebb ország a világon – Kína, USA, Tajvan, Törökország és Olaszország előz meg minket - és 2. helyet foglalja el az európai országok között.[22]

A túlterheléses támadásokat sokszor anyagi haszonszerzés céljából indítják. Ezeket a támadásokat egyre többször zsarolás vagy ún. „védelmi pénz" követelése során használják fel, amit az áldozatoktól online fizetés - általában Bitcoin - formájában követelnek. Az elkövetők gyakran olyan cégek weblapjait választják ki, amelyek folyamatos és zavartalan működést követelnek meg (pl. online casinok, energia-, pénzügyi szféra).
2016-ban az Europol sikeres akciót hajtott végre és letartóztatta a zsarolásokban élen járó DD4BC Team hacker csoportnak a kulcsfontosságú tagjait, akik számos DDoS támadást indítottak európai cégekkel szemben (pl. a PokerStars online szerencsejáték cég is célpont volt). Az általuk alkalmazott zsaroló séma a következőképpen néz ki: felmérik a célpont hálózati sérülékenységét, majd kisebb DDoS-támadásokat indítanak a céggel szemben, ezt követően a további támadások indításának elkerülése érdekében Bitcoin formájában fizetséget kérnek a cégtől. Abban az esetben, ha az áldozat ennek a követelésnek nem tesz eleget, akkor további, erőteljesebb támadásokat indítanak a cég weblapjával szemben, amely annak a teljes elérhetetlenségéhez is vezethet. Azonban nem javasolt, hogy fizessenek a zsarolóknak, mert a támadók célja a haszonszerzés, valamint nincs garancia fizetség esetén sem a támadás elkerülésére. DD4BC csapatnak a módszere egyre elterjedtebbé vált és már „copycat" hacker csoportok is megjelentek, akik másolják őket.[23]

Az anyagi haszonszerzésen kívül gyakori a gazdasági célzat, ami az üzleti versenytársak technológiai folyamatai ellen intézett támadásokban nyilvánul meg. A támadók általában tudatosan, jól időzítve olyan időpontokat választanak a támadásokhoz, amikor az adott cég nagyobb bevételre számíthat - így nagyobb kárt is tudnak okozni - pl. ilyen a Cyber Monday, Black Friday vagy karácsony. A weboldalak működésének a megszakítása költséges terhet jelent bármely weboldal üzembentartójának legyen szó kis- és középvállalkozásról vagy nagyobb cégről. A támadással járó pénzügyi veszteség esetenként különbözhet és nem

[22] https://www.symantec.com/content/en/us/enterprise/other_resources/21347933_GA_RPT-internet-security-threat-report-volume-20-2015.pdf [2017.01.05.]
[23] https://www.cardschat.com/news/pokerstars-ddos-attackers-arrested-by-Europol-extortion-group-also-alleged-to-have-targeted-betfair-neteller-18629 [2017.01.18.]
http://news.softpedia.com/news/members-of-dd4bc-the-group-that-blackmailed-companies-with-ddos-attacks-arrested-by-Europol-498797.shtml [2017.01.18.]
http://neih.gov.hu/zsarolo-ddos [2017.01.21.]

kizárt, hogy az adott vállalkozás működésére hosszútávon is hatással lehet. Ez megnyilvánulhat a kieső és pótolhatatlan bevételben, illetve akár presztízsveszteséget is okozhat, mivel az ügyfelek nem tudják elérni a támadással célzott cég honlapját, sem igénybe venni a cég által kínált szolgáltatást, ezért inkább a konkurens vállalkozásokat választják és lemorzsolódnak az adott cégtől (pl. a pénzügyi ágazaton belül, különösen az értéktőzsde, értékpapír kereskedés piacán ez pillanatok alatt súlyos és hatalmas kárt okozhat).[24]

A túlterheléses támadások hátterében politikai vagy ideológiai indíttatás is állhat, amit az ún. hacktivizmus elnevezéssel illetek. A hactivista nem egy csalárd hacker, aki személyes információkat szeretne megszerezni vagy egyéb kárt okozna, hanem bomlasztó tevékenységével az a célja, hogy felhívja a figyelmet valamely politikai vagy társadalmi ügyre. Számára a hacktivizmus egy Internet által biztosított stratégia, amely lehetővé teszi a polgári engedetlenség gyakorlását (pl. DDoS támadások indításával, a weboldal felülírásával azaz „defacement"-tel, adatlopással, illetve azok későbbi nyilvánosságra hozatalával, vagy egyéb virtuális szabotázs akciókkal).[25]

Az egyik legismertebb hacktivista csoport, az Anonymous[26], akiknek a támadásai rendszerint valamilyen közös ügyet szolgálnak. A csoport nevében intéztek már támadást amerikai, izraeli, tunéziai és ugandai kormányszervezetek weblapjai, gyerekpornográf tartalmú oldalak, szélsőségesen rasszista szervezetekkel ellen (mint például a Westboro Baptist Church), de nagyvállalatok is váltak már célpontjukká. A legutóbbi áldozataik között szerepelnek a brazil kormányzati oldalak a Rió-i olimpia miatt. A másik ismert csoport a LulzSec, akiknek hasonló támadásaik voltak ugyanúgy kormányzati (pl. CIA webszervere ellen intézett túlterheléses támadás) és nagyvállalati rendszerek ellen (pl. a Sony Playstation online szolgáltatásait tették elérhetetlenné, illetve több százezer regisztrált felhasználó adatait, fontosabb rendszerleírásokat tették nyilvánossá).[27] További példa a politikai célzatú támadásokra az USA elnök választásának kampány időszaka, amikor Trump és Clinton oldalait sorozatos támadások érték. Magyarországi érintettségű ügy is volt, amikor a

[24] Urcuyo: i.m. 302-303. o.
http://hirek.prim.hu/cikk/125744/ [2017.06.23.]
[25] https://www.techopedia.com/definition/2410/hacktivism [2017.01.21.]
[26] Török Szilárd: Anonymous a világban és Magyarországon. Felderítő Szemle. 2014. március XIII. évfolyam I. szám. 192. o.: Az Anonymous egy nemzetközi hacker csoport, amely formálisan 2003-tól létezik és 2008 óta indít támadásokat. Több, egymástól független sejtből áll, a világ számos országában vannak aktivistái. A csoport megalakulását a „4chan" internetes oldalhoz kötik.
[27] Török: i.m. 196. o.

Belügyminisztérium kormányzati rendszereinek az egyes nyilvánosanan elérhető szolgáltatásait jelentős mértékű túlterheléses támadás tette időszakosan elérhetetlenné.[28]

Itt fontos megjegyezni, hogy a DDoS támadás végrehajtása történhet önkéntesen vagy a felhasználó tudta nélkül is. Az önkéntes esetben az irányított számítógépeket átadják a controller-nek vagy közvetlenül a felhasználók maguk csatlakoznak a koordinált támadáshoz.

A hazai Btk. értelmében egy DDoS támadás végrehajtása a 423. § szerint az információs rendszer vagy adat megsértésének minősül és a 2) bekezdés szerint büntetendő, aki a) az információs rendszer működését jogosulatlanul vagy jogosultsága kereteit megsértve akadályozza, vagy az információs rendszerben lévő adatot jogosulatlanul vagy jogosultsága kereteit megsértve, megváltoztat, töröl vagy hozzáférhetetlenné tesz. A minősített eset valósul meg, ha a (2) bekezdésben meghatározott bűncselekmény jelentős számú információs rendszert érint. A DDoS támadás során a támadó sok száz vagy több ezer felhasználó gépei felhasználásával kísérel meg kapcsolatot létesíteni a megtámadott számítógéppel. E sok száz vagy ezer zombigép egy botnet hálózatot alkot, amelyet a támadó vezérel. Az egyszerre küldött nagy mennyiségű adatkérés és továbbítás bénítja a támadott számítógépet és rajta keresztül az információs rendszert.[29] A büntetés két évtől nyolc évig terjedő szabadságvesztés, ha a bűncselekményt közérdekű üzem ellen követik el.

[28] www.kormany.hu/hu/belugyminiszterium/hirek/senki-nem-vallalta-magara-a-kormanyzati-informatikai-rendszerek-elleni-tamadast [2017.01.21.]
[29] Nagy Zoltán András: XLIII. fejezet tiltott adatszerzés és az információs rendszer elleni bűncselekmények. Magyar Büntetőjog: Különös rész. Osiris Kiadó, Budapest 2014. 598. o.

Social engineering, phishing (adathalászat)

„A social engineering a befolyásolás és rábeszélés eszközével megtéveszti az embereket, manipulálja, vagy meggyőzi őket, hogy a social engineer tényleg az, akinek mondja magát. Ennek eredményeként a social engineer – technológia használatával vagy anélkül – képes az embereket információszerzés érdekében kihasználni."[30]

Az ember a leggyengébb láncszem a kiberbiztonságban, mindig egyszerűbb a hackerek számára az emberek hiszékenységének a kihasználása, ami azt eredményezi, hogy az áldozat a saját vagy cége érdeke ellen cselekeszik és lényegében hozzájárul egy sikeres támadáshoz.

A védett WiFi-jel „lopásnál" veszélyesebb az ún. *phishing* (adathalászat), amely lényegesebb nagyobb vagyoni kár okozására teremt lehetőséget. Az elkövetők egy vagy több szervert bérelnek, akár több országban. Kiválasztják egy másik ország bankját, e-kereskedelmet folytató vállalkozásait, Internet-szolgáltatóit vagy más céget. Ezek honlapjait „lemásolják" – weboldal szerkesztő, karakter felismerő stb. programokkal. E-mailekben keresik meg ezen bankok, vállalkozások ügyfeleit. Az ügyfelek e-mail címeit a legkülönfélébb adatbázisokból szerzik meg legálisan, vagy illegálisan. Rögtön felmerül a kérdés, hogy banki ügyfelek adatai hogyan kerülnek az adathalászokhoz? Csalárd szándékú mobilhívások révén vagy netán „házon belülről"?[31]

A következő lépésben az ügyfelektől e-mailben, mint az Internet szolgáltatójuk, számlavezető bankjuk, vagy más vállalkozás, számlaszámukat, kódjaikat, személyi adatait stb. általában ezek ellenőrzésének színlelésével, azaz csalárd szándékkal kérnek információkat. Pl. az intézmény szerverének szervizelése miatt megkérik az ügyfelet, hogy lépjenek be a bank, más vállalkozás rendszerébe és ellenőrizzék adataikat, számláikat stb.

Az e-mailben szereplő linkre klikkelve a felhasználók bankjuk, szolgáltatójuk weboldalához kísértetiesen hasonlító, de hamis weboldalra lépnek be, ahol az ügyfél felhasználó nevét, jelszavát, vagy más azonosítóját kérik. A gyanútlan ügyfél, ha ezeket begépelik, kapnak egy hiba-üzenetet, amely szerint a rendszer nem érhető el, például karbantartása még folyik és térjenek vissza később. Ám az előzőleg begépelt azonosítókkal az adathalászok már hozzáférnek az ügyfelek számláihoz, más adataihoz.

Napjainkban leggyakrabban a fertőzések már az ún. *spear-phishing*, vagyis célzott adathalász támadások révén történnek: ezek során viszonylag kisszámú, kiszemelt

[30] Kevin D. Mitnick: A megtévesztés művészete című könyv borító

[31] Az ún. Tyupkin-malwaret, amely „végteleníti"' a pénzkiadást az ATM-ból, szintén „házon belülről" kell off-line feltölteni, majd azonnal használni a bankkártyát és tartani a zsákot.

felhasználók (pl. banki alkalmazottak vagy kormányzati személyek) személyre szabott e-maileket kapnak egy csatolmánnyal (általában Microsoft Word vagy PDF dokumentumot), amelynek a megnyitásával általában a rendszer valamilyen sebezhetőségégének a kihasználása révén juttatják be a kártevőket vagy a megnyitással a felhasználó tudta nélkül kártékony program fut, amely hátsó kaput nyit a támadónak. A cél, hogy az áldozat a csatolmányt megnyissa, ezért az üzenet célzott, ami azt jelenti, hogy tartalma valamilyen valós élethelyzetre, eseményre, tevékenységre utal, ami miatt a célpont azt hiszi, hogy az üzenet valós.[32]

Az egyik formája az ún. *CEO fraud* (vezérigazgatói csalás), amely során a támadó e-mailben megkeresi a célszemélyt (pl. könyvelőt) a szervezet vezetőjének kiadva magát, hogy egy sürgős tranzakciót intézzen el az áldozat. Gyakori, hogy a munkaidő vége fele küldik az üzenetet, hogy nehezen lehessen utána járni és igazolni a megkeresést. Az ún. *whaling* esetében pedig a célpontok pont a szervezet vezetői.[33]

Az adathalászat másik módszere az ún. *VoIP-csalás* (más elnevezéssel vishing-csalás), azaz telefonos csalás. Az elkövetők ebben az esetben az ügyfél telefonszámát tárcsázzák (pl. mert letiltották bank-, illetve hitelkártyáját), és arra kérik az ügyfelet, hogy hívjon fel egy adott számot, amelyen pl. ellenőrzés céljából akadja meg nevét, kártyaszámát, vagy reaktíválja a „letiltott" bank-, vagy hitelkártyáját stb.

További módszer az ún. *sms-csalás* (más elnevezéssel: smishing-csalás), amely során az adatkérés sms-ben történik és sms-számra kérnek válaszokat az elkövetők.

Az e-mailben történő adathalászattal kicsalt adatokkal 240 millió realt (kb. 45 millió dollárt) szerzett banki ügyletek révén 53 brazil elkövető.[34]

Magyarországon is a különböző bankok így a Raiffeisen Bank, a Szigetvári Takarékszövetkezet és a Budapest Bank után az Erste Bank és az OTP ügyfeleinek is küldenek adatkérő e-maileket ismeretlenek.[35] Az adathalászattal, azaz megtévesztéssel történő pénzszerzésnek 3 fázisa különíthető el:

---

[32] http://netk.uni-nke.hu/uploads/media_items/svkk-elemzesek-2017-9-az-internet-politikat-is-befolyasolo-hatasa-a-2016-os-amerikai-elnokvalasztas-soran-kovacs-l-krasznay-cs.original.pdf [2017.05.28.]
https://www.hwsw.hu/hirek/49634/kaspersky-lab-rec-october-biztonsag-kartevo-sebezhetoseg.html [2017.05.28.]

[33] https://www.vadesecure.com/en/ceo-fraud [2017.05.28.]

[34] http://software.silicon.com/malware/0,3800003100,39125173,00.htm [2016.10.25.]

[35] http://abiweb.obh.hu/abi/index.php?menu=81&ddate=2006-12-07 [2016.10.25.]

- Az ügyfél személyes adatok (felhasználó név, belépési kód vagy jelszó, valamint, ha szükséges telefonszám) megtévesztéssel történő megszerzése.
- A megtévesztéssel megszerzett adatokkal történő belépés a bank számítástechnikai (e-banking) rendszerébe.
- Ezen adatokkal történő pénzszerzés (pl. átutalás, valutavásárlás, esetleg értékpapír-vásárlás), azaz a jogosult ügyfélnek ezzel kár okozása. Eredményes védekezés lehet a mobiltelefonra történő visszajelzés, jelszóval való engedélyeztetése a műveletnek, feltéve, ha azt az elkövetők nem kerültek birtokába.

Összességében a legtöbb támadás az emberi faktorra vezethető vissza mint például a különböző online „bankrablások" és az Egyesült Államok elnök választásának befolyásolása is.[36]

Az adathalászat kapcsán fel kell hívni figyelmet a felhasználók könnyelműségére, gondatlanságára. Sőt gondatlansága, könnyelműsége kétszintű, egyfelől lehetővé teszi a visszaélések elkövetését, másfelől maga válik sértetté. Bármekkora is a sértetti önhiba, a cselekmény jogellenessége elvitathatatlan, és büntetőjog szempontjából is fontos értékelni.

[36] http://netk.uni-nke.hu/uploads/media_items/svkk-elemzesek-2017-9-az-internet-politikat-is-befolyasolo-hatasa-a-2016-os-amerikai-elnokvalasztas-soran-kovacs-l-krasznay-cs.original.pdf [2017.05.28.]

Pénzmosás a kibertérben

A virtuális térben végrehajtott pénzmosásnak is ugyanaz a célja, mint a valós térben, azaz jellemzően gazdasági tevékenységek alatt folytatott illegális pénzügyi művelet, amelynek célja az, hogy a bűncselekménnyel szerzett vagyon eredete igazolhatóvá váljon, jogellenes voltától megszabaduljon.[37]

- „Money mule" ügyletek,[38]
- Bitcoin és egyéb altcoins műveletek,
- valódi vagy hamis alapítványok támogatásának színlelése,
- illegális szerencsejátékok,
- online fizetős játékok,
- bármely C2C üzletkötés felveti a pénzmosás gyanúját.

A *„money mule"* elnevezéssel ismert új pénzmosási technika a pénzintézetekkel történő közvetlen kapcsolatfelvételt iktatja ki és egy harmadik személy (mint „teherhordó öszvér", azaz a pénzhordó személy) közreműködésével, ténykedésével, terítik, bújtatják a bűnözők a bűncselekményből eredő „piszkos pénzt".

A kiszemelt személyeknek egy a számukra is kedvező ajánlatot tesznek, hogy meghatározott jutalék, fiktív munka fejében, reklám- vagy más marketing ígéretével fogadjanak nem túljelentős összeget bankszámláikra. A kapott pénzt majd egy másik bankszámlára kell, hogy utalják. Tehát a pénzmosók magánszemélyek bankszámláira aprózzák fel a pénzt, amelyet majd a bankszámla tulajdonos személyek átutalnak az elkövetők számlájára, így legalizálják a „piszkos pénzt". Mivel nem nagy összegek mozognak a bankszámlák között, így a tranzakciók általában nem feltűnők és nem akadnak fenn a pénzmosási ellenőrzéseken. Újabban a pénzt hordó személyeket legkülönfélébb áruk-, illetőleg szolgáltatás megrendelésére veszik rá. Miután ma az áruszállítás, a kézbesítés különböző anonim helyekre is történhet (pl. postahivatalok csomag automatáiba stb.), így az áruk átvételekor is biztosítható az áruért érkező személy anonimitása. A pénzt hordó személy nem vesz részt az alapbűncselekmény elkövetésében, de cselekménye a magyar törvények alapján pénzmosásnak minősül.

---

[37] Gál István László: A pénzmosás. In: Új Btk. Kommentár 8. kötet (főszerkesztő: dr. Polt Péter). Nemzeti Közszolgálati és Tankönyv kiadó. Budapest, 2013. 45.o.

[38] https://www.europol.europa.eu/newsroom/news/europe-wide-action-targets-money-mule-schemes [2017.01.25.]

A *virtuális valuták* létre jötte összefügg a mindig új megoldás utáni kutatás igényével és a pénzügyi szféra iránti bizalom megrendülésével.

Ezek a valuták a nemzeti bankoktól függetlenek, jellemzően decentralizáltak, konverziós költségeik nincsenek, továbbá a digitális valuták hamisíthatatlanok, valódi valutára vagy más virtuális valutára konvertálhatók. A pénzügyi műveletek nyilvánosak, valamennyi a rendszerbe kapcsolódó felhasználó láthatja valamennyi tranzakciót.[39] Emellett a felhasználók anonimok maradhatnak, nincs személyiséglopás.

A hálózatban tranzakciókat lehet lebonyolítani anélkül, hogy azok bármelyik résztvevőjében - eladóban, vevőben vagy a bankban - meg kellene bízni. A bizalmat a rendszer matematikai alapjai helyettesítik: minden egyes Bitcoin egyedi, tehát nem lehet őket hamisítani. A tranzakció gyorsan végrehajtható, illetve nem visszavonható.

A virtuális valuta működését, használatát a Bitcoinon, mint a legnépszerűbb elektronikus fizetőeszközön keresztül mutatjuk be, ami egy virtuális valuta és fizetési rendszer is egyben, amelyet 2009-ben egy Satoshi Nakamoto[40] felhasználó talált ki.

A Bitcoin nyílt forráskódú digitális valuta. A kliens program letöltését követően, annak egyidejű telepítésével, automatikusan létrehoz egy, az ügyfél azonosítására alkalmas fogadó címet és a hozzá tartozó jelszót. A rendszert használók ezt az azonosító számsort láthatják, - ismételjük - anélkül, hogy a mögöttük álló felhasználó beazonosítható lenne.

Többféle módon tehet szert a felhasználó Bitcoinra:[41]

- „Bányászattal”. A rendszert – természetesen nem véletlenül – úgy alakították ki, hogy a rendszerbe lépők érdekeltek legyenek a Bitcoin gyűjtésében, illetőleg a felhasználóknak kiosztott „ajándék” Bitcoinok keresletet teremtsenek és ezzel a kínálati oldal (kereskedők, szolgáltatók) érdeklődését felkeltsék.

A felhasználó egy program telepítésével számítógépének kapacitását a Bitcoin - hálózatban folyó tranzakciók, a közös kriptográfiai feladatok megoldása - szolgálatába állítja.

Minden elvégzett művelet után kap a felhasználó egy "lottószelvényt", amellyel a körülbelül tíz percenkénti sorsolásban részt vesz és ezzel meghatározott mennyiségű virtuális valuta nyerhető. A nyerési esély a minimálisnál is kevesebb, hiszen a világban felhasználók milliói közül kerülnek ki a nyertesek. „Bányász farmok” próbálnak pénzt nyerni ilyen módon pénzre szert tenni.

---

[39] https://blockchain.info/ [2017.01.31.] Folyamatosan „pörög” a tracker, így figyelemmel kísérhető, hogy milyen Bitcoin tranzakció zajlik a piacon.

[40] Valóságos név vagy sem? Valószínűleg egy álnév. Hogy ki találta ki egyelőre rejtély? http://itmozaik.hu/hirek/2016/05/04/craig-wright-allitja-hogy-o-satoshi-nakamoto-a-Bitcoin-letrehozoja.html [2016.12.18.]

[41] Eszteri Dániel: Bitcoin: Az anarchisták pénze vagy a jövő fizetőeszköze? Jura, 2012. 2. szám 86 – 90.o.

- Bitcoin adásvétel zajlik a Surface- éppúgy, mint a Dark- és ezen belül a Deep Weben. Az adásvétel ellenőrizetlen és ellenőrizhetetlen (pl. bár két karibi ország bankszámlája érintett az ügyletben, de a pénz „körbejárja" a Földet, amíg megérkezik a vevő vagy eladó bankszámlájára). Vagy P2P kapcsolaton keresztül zajlik, bár maga a művelet látható (azonosítószámok látszanak), ám az, hogy kit takarnak az azonosítószámok az nem tudható. Az eladó meghirdeti, hogy milyen árfolyamon kíván vásárolni vagy eladni, ha megfelel az árfolyam és a valutaneme is, akkor létrejön az üzlet.
- Bitcoinnal lehet legálisan fizetni árukért és szolgáltatásokért. A Bitcoin népszerűsítésével, a kereslet növelésével az ilyen üzleti tranzakciók bővítése céljából „oszt ki" a rendszer „ajándék" Bitcoinokat. A Bitcoint nemcsak az e-kereskedelem körén belül, hanem a valós térben is elfogadják mint fizetőeszközt (pl. vendéglátóhelyeken, koncertjegyek értékesítésekor stb.).
- Utcán, vendéglátóhelyen felállított automatán keresztül szintén vásárolható Bitcoin.

Valamennyi ország azonos álláspontot foglal el abban a tekintetben, hogy bizonyos potenciális veszélyforrást jelent a Bitcoin megjelenése és egyre szélesebb körű használatának az elterjedése. A Bitcoin-rendszer használatából eredő biztonsági kockázatok szembeötlőek.[42]

A Bitcoin azért alkalmas pénzmosásra, mert ellenőrizetlen, ellenőrizhetetlen és követhetetlen. Nagy összegek cserélhetnek gazdát a felhasználók közötti közvetlen kapcsolat segítségével, egyes felhasználók több Bitcoinos „pénztárcával" rendelkezhetnek, nincs központja a hálózatnak, szerverek működnek valahol a „felhőben", bár a tranzakciók ismertté válhatnak (nagy tömegű, folyamatos adatáramlás figyelemmel kísérése igencsak aggályos), a felhasználók nem válnak ismertté. Ezek a tulajdonságai persze felkeltették az illegális üzletet folytatók figyelmét is. Például az Internet egyik legsötétebb - emiatt népszerű - piaca volt a Silk Road,[43] amely elfogadta a Bitcoint. Ne legyenek illúzióink, a Tor hálózatokon további jogellenes ügyletek - fegyver-, kábítószer-, hamis okirat vásárlása, készíttetése, terheléses támadás indítására alkalmas botnet hálózat bérlése,[44] „bérgyilkos" keresése és megbízása, illegális valutaügyeletek, szerzői jogsértések, pornográf, pedofil kép- és videófájlok

[42] Katona László: A hagyományos pénztovábbítási rendszerek és a modern technológiai alkalmazása a pénzmosás és a terrorizmusfinanszírozás területén. Hadtudományi Szemle. 7. évfolyam 2. szám Budapest, 2014. 191.o.

[43] https://silkroaddrugs.org/ [2016.12.18.]

[44] Magyarországi IP címen futó számítógépek a második legfertőzöttebbek botnet vírusokkal Európában és hatodik a Föld országai között. https://resource.elq.symantec.com/LP=2899 [2016.12.18.] Ugyanezt erősíti meg a Microsoft elemzése is. https://www.microsoft.com/security/sir/
Sajnos, nem beszélünk erről és más a fertőzött számítógépek használatával összefüggő veszélyekről és így nem teszünk ellen semmit, nem tanítjuk az Internet veszélyeit. A zaklatás, a pedofília emlegetése mellett más veszélyekre is fel kellene hívni a figyelmet. A valóság elhallgatása sosem vezet jóra …. e körben sem.

csereberéje, vásárlása Bitcoinnal és egyén virtuális valutával, majd ezek konverziója valós valutára és vica versa - zajlanak a nap minden másodpercében titkosítva, ellenőrizetlenül és nagy tételben.

Külön érdekesség, hogy az új Büntetőeljárásjogi kódex, a 2017. évi XC. törvény a büntetőeljárásról, kialakította az úgynevezett virtuális vagyontárgyak biztosításának keretszabályait, amely alapján a decentralizált virtuális fizetőeszközök (mint pl. a Bitcoin és az azonos technológiára épülő más virtuális valuták), valamint az elektronikus pénz egyes típusai a jövőben lefoglalás tárgyát képezhetik. A gyakorlatban azonban ez nem lesz egyszerű, hiszen a Bitcoin pénztárca használatához szükség van a privát kulcsra, amit előbb a hatóságoknak meg kellene szerezniük a tárca tulajdonosától.[45]

A rejtélyes, ismeretlen *alapítványok támogatása* tálcán kínálja a virtuális térbeli pénzmosás lehetőségét, leplezhetőségét és üldözésének nehézségét. Az Interneten számtalan, különféle alapítvány weboldala, számlaszáma, felhívása fellelhető. Ezek egyenkénti vizsgálata alapján lehetne eldönteni, hogy melyek követik az általuk hirdetett célt és melyek más célra szerveződtek. A nehézséget fokozza, hogy az adott weboldalak, rövid időre vagy időközönként érhetők el az Interneten. Különösen, ha ezek a site-ok az Internet nem Surface Web felületén vannak jelen. Egy-egy külföldi alapítvány számára, amelynek számláját szintén külföldön vezetik, szinte minden nehézség nélkül érkezhet bűncselekményből származó pénz és felderítésük sem egyszerű.

További nagy összegű pénz tisztára mosására alkalmas az Interneten fellelhető *legális vagy illegális szerencsejátékok* is. A kommunikációs lehetőségek világméretűvé bővülése, a sport, a játék iránti szurkolói érdeklődés, a szerencsejáték iránti vonzalom, nem utolsó sorban a versenyek, mérkőzések eredményért való izgalom fokozása, a „könnyűnek tűnő" pénzkereseti lehetőség, a fogadási eseményen történő részvétel illúziója és más okok folytán a sporthoz vagy bármely eseményhez kapcsolódó különböző szerencsejátékok népszerűségét hozta magával. Ezt a növekvő érdeklődést, ezzel együtt a szerencsejátékokba a pénz beáramlást, ezek nyereségességét használják ki azok, akik legális vagy illegális játékokat szerveznek akár valós térben, akár virtuális térben. Sőt, valós térben a szervezett bűnözői csoportok megpróbálják a szerencsejátékból a „szerencse" elemet kiiktatva, a számukra

[45] http://www.parlament.hu/irom40/13972/13972.pdf [2017.06.20.]

kedvező és egyben anyagi hasznot hozó eredménynek a kialakítását vesztegetéssel (játékosok, bírók megkeresésével, azok „lefizetésével” – fordítva ritkább), netán megzsarolásával elérni.[46]

Az illegális szerencsejáték szervezése tipikusan hosszabb távra szervezett tevékenység. A szervezett csoportok adómentes bevételhez jutnak. Az illegális szerencsejáték mindig is vonzotta azokat, akik az adózási és egyéb kötelezettségeket el kívánják kerülni.[47]

A probléma a következő: az Interneten fellelhető fogadási oldalak lehetnek legálisak vagy illegálisak. Mivel ezen oldalak tartalma általában megegyező, kivitelezése profi, sokszor megtévesztésig hasonlítanak egymásra, ezáltal alkalmasak a tájékozatlan felhasználók tévedésbe ejtésére. Ugyanakkor akár legális, akár illegális a weboldal, alkalmas a pénzmosásra is. Egy távoli, tételezzük fel karibi-szigetvilágban bejegyzett legális gambling oldalon is a játékos, mint befizető - úgy tűnik - folyamatosan veszít, pedig nem, hanem befizet és befizet. A másik játékos a szerencse forgásának megfelelően, hol veszít, hol nyer (vélhetően inkább veszít). A pénz a legális szerencsejátékot üzemeltető vállalkozás számlájára kerül és ezzel az „tiszta” lesz. A tipikusan karibi-, délkelet ázsiai országokban, a ciprusi, máltai, sőt svájci nyitott bankszámlák a bankok megkeresésével nem, legfeljebb a bankszámla-tulajdonoson keresztül érhető el.

Az eddig bemutatott pénzmosási praktikák nagyobb összegű „piszkos” pénzek tisztára mosására nyújtanak lehetőségét. Emellett léteznek mikro-pénzmosási technikák, amelyek bár sokszor jelentéktelen összeg mozgását rejtik, de „sok kicsi sokra megy” alapon működnek.

Az Internet teremtette távmunka nem csupán egyetlen vállalkozás keretében működhet, hanem akár országhatárokat átívelve, arra is opciót nyújt, hogy egy - egy munka elvégzésére alkalmazzon, alkalmazhasson egy személyt. Az ún. *szabadúszó oldalak* (freelancer.com, freelancer.hu, fiverr.com stb.) egyszerre keresnek és kínálnak munkát az arra vállalkozóknak. Minden olyan jellegű munkavégzés szóba jöhet, amely távmunkában teljesíthető (szoftverírás, tervezés, fordítás, zeneszerzés, szövegírás, beadványkészítés, bérszámfejtés, könyvelés, utókalkuláció, egyéb gépelési feladatok stb.).

Szabadúszó oldalakon mind a munkát ajánló, mind a munkát vállaló számára elegendő egy regisztráció pl. egy külföldi oldalon történő, így - gyakorlatilag – akár anonimok is maradnak egymás előtt és bárki más előtt. Az anonimitás lehetőség arra, hogy a felhasználó egy személyben legyen „munkáltató” és „munkavállaló” szerepben, azaz önmagának utaljon

[46] Nagy Zoltán András: A szervezett bűnözői jelenségek a számítógépes hálózatokon. Belügyi Szemle 60. 2012.6. 108-125.o.
[47] Farkas Imre – Jávorszky József: Az illegális pénznyerő-automaták felderítése. Rendészeti Szemle, XXXI. évfolyam. 1993.5. 58-59. o.

pénzeket, de akár „munkavállaló” egy harmadik személynek.[48] Az adó- és járulékfizetés elkerülhető, ami némileg magasabb jövedelmet eredményezhet.
Nem kétséges, hogy nagyobb pénzösszegek mozgatása kirívó, ám többszöri kis összegek - ismétlem önmagának vagy egy másik személynek, P2P technikával történő utalása egyszersmind a pénzek „tisztára mosására” alkalmas.

Igen népszerűek az Interneten az *online játékok*, amelyek közül a fizetős játékok kis összegű pénzmosási lehetőségek is. Az online játékok népszerűsége 1997-ben Ultima Online-nal indult. Azóta szerepjátékok, háborús játékok és más típusú játékok tízezrei hódítják, vonzzák és teszik függővé a falhasználókat. Az online játékok játszhatók anyagi hozzájárulással vagy anélkül. Igen izgalmas például a sakk schnell-partik a világ bármely tájékán az Internethez csatlakozott játékossal, a nap bármely percében. Ugyanakkor más online játékban, tipikusan szerep-, életútjátékokban lehetőséget biztosítanak a játékírói, hogy a játékos befektetése fejében áruk, szolgáltatások, szerepek vásárlásához, vagy a játékban történő továbbjátszáshoz. A „Second Life” játékban például az US dollárhoz igazított Linden-dollárért virtuális földbirtok, más ingatlan licitálható, vásárolható, illetőleg eladható egy másik játékosnak. Ahogy a való életben, itt is dolgok, ingatlanok, ruhák és más napi tárgyak, háziállatok vásárolhatók, szerencsejátékok űzhetők. Sőt, ahhoz, hogy előbbre jusson, pénzbefizetéssel ez is elérhetővé lesz. Népszerű, pénzfizetéses játék a World of Warcraft vagy a Star Wars - The Old Republic, ez utóbbi a filmeposz évenkénti bemutatója állandó reklámját jelenti a játéknak. Azok az online játékok, amelyekben két vagy több személy között pénzforgalom lehetséges, egyszersmind a pénzmosásra is alkalmasok.[49]

Az *offshore* angol kifejezés, közelítő fordításban „parton kívülit” az „el a parttól” szavakat jelent. A fordítás lényegre törő, mert az adózás elkerülésére utal. Léteznek offshore cégek, ezen belül offshore bankok. Offshore cégek azok, amelyeket olyan országokban jegyeznek be, ahol nem folytatnak tevékenységet, és a külföldön végzett tevékenységük után nem kell adót fizetniük. Ennek fejében a „fogadó országban” általában csekély összegű átalányadót kell megfizetniük évente. Jellemző, hogy nem származik bevételük abban az országban, ahol bejegyezték őket, csak annak határain kívül. A cél nyilvánvaló, ezek a cégek

[48] A külföldi szakirodalom már felfigyelt a pénzmosás ilyen formájára is.
http://www.wired.co.uk/article/money-laundering-online [2016.12.18.]
http://www.antifraudnews.com/inside-online-money-laundering-scams/[2016.12.18.]
[49] A külföldi szakirodalom már felfigyelt az online-játékok pénzmosási lehetőségeire:
https://www.technologyreview.com/s/520501/the-secrets-of-online-money-laundering/ [2017.03.18.]

nem kívánnak magas vagy annak vélt adót fizetni. Félő az, ha valamennyi onshore (belföldi) adózó cég, magánszemély ezt az utat választja. „A törvényhozóknak szembesülniük kell a hazai tőke és a multinacionális vállalatok konfliktusából fakadó jogkövetési problémákkal, hiszen a külföldieknek biztosított előnyöket a hazai cégek előbb-utóbb kikényszeríthetik."[50] Ne legyenek illúzióink ebben a kérdésben sem.

Az offshore, mint tevékenység tulajdonképpen átfogó elnevezés, többféle formája ismert:

- Adóparadicsomok, minimális átalánydíjas adózással (Európában Gibraltár, Jersey-sziget, Man-sziget stb.)
- Alacsony adókulcsú országok – az onshore adózóknál kisebb mértékű adózással terhelt (a kontinensen Nagy-Britannia [az EU-ból való kilépés népszavazás, a Brexit előtt], Luxemburg, Málta, Svájc stb.).
- Elmaradott területek fejlesztése fejében adómentesség (Európában Írország).
- Szabadkereskedelmi övezetek az EU-n kívül Írország, Montenegró.
- A tőkeparadicsomokban a tőkeadó vagy kamatadó alacsony vagy nem létezik (a kontinensen Liechtenstein, Svájc stb.).
- „Offshore" adózási (quasi offshore) országokban offshore kedvezmények hiányában, ám rendkívül alacsony nyereségadóval teszik vonzóvá magukat (Európában Hollandia, Luxemburg, Málta, Svájc).[51]

Valamennyi offshore megoldásra jellemző az anonimitás, a diszkréció biztosítása, a minimális bürokrácia a cégbejegyzéssel, sőt névleges cégvezetői lehetőségek biztosítása. Ezek a tényezők mind – mind vonzóvá teszik a befektetni, vagy a pénzüket bármely okból elrejteni szándékozók számára.

Véleményünk az, ha az offshore célja pusztán a jövedelmek külföldre vitele, az költségvetési csalásként értékelhető, mivel az adózó a „költségvetésbe történő befizetési kötelezettség … vonatkozásában mást tévedésbe ejt … , valótlan tartalmú nyilatkozatot tesz vagy a valós tényt elhallgatja." (Btk. 396.§ (1) bekezdés). „Gyakorta eszköze egy offshore társaság ….. az adócsalásnak, a jogtalanul megszerzett jövedelmeket ugyanis előszeretettel mentik ki ilyen cégekbe, és az is tény, hogy a spekulációban leginkább érdekelt személyek keresik az offshore-hoz hasonló létformákat."[52]

---

[50] Szilovics Csaba: Csalás és jogkövetés: Gondolat KK Budapest, 2003. 15. o.

[51] Gál István László: Gazdasági büntetőjog, gazdasági bűnözés és a jelenlegi gazdasági válság. Pécs, 2012. 78-79.o.

[52] Erdős Éva - Kovács Kitti: Az adóoptimalizálás egyik eszköze: az offshore jelenség térnyerése és gyakorlati nehézségei. Gazdaság és Jog, 2010/1. 17-21. o.

Az ilyen célú offshore-ozás szankcionálására szolgálhatnak további igazgatási vagy civiljogi szankciók. Ugyanis akik külföldre viszik jövedelmüket, hogy elkerüljék az adózást, tehát nem járulnak hozzá a társadalmi költségekhez, azoknak minden olyan tevékenységért, lehetőségért, amelyet az állami költségvetés fedez (ingyenes általános iskola, ingyenes orvosi ellátás [ennek minőségét ne vegyük górcső alá most], mentők, tűzoltók, rendőrség törvényi kötelezettségei, közokiratok stb.) e tevékenységek teljes költségét kellene kifizetni.

Az, hogy az offshore bankokban nyitott számlák, illetőleg az ezeken folyó tranzakciók közül mennyi szolgál legális célokra és mennyi bűncselekmény, ezen belül pénzmosás céljára az kideríthetetlen, statisztikailag megbecsülhetetlen.

Az offshore - akár mindezekkel együtt - a legbiztosabb lehetőségét nyújtja a bűncselekményből származó pénz bújtatására – terítésére – végül legalizálására.

Hiszen az, hogy az offshore cégek számlájára honnan és hogyan kerül pénz pl. egy másik offshore cég számlájáról, vagy készpénz befizetéséből (schengeni övezeten belül gyakorlatilag a bőrönd mérete határozza meg a készpénz-forgalmat), majd ezt követően az ottani bankszámláról merre „vándorol" a pénz kideríthetetlen. A befektető személye, a befektetés iránya vagy helye nyújthat egy nem túl megalapozott gyanút, sejtést, hogy itt és most pénzmosás történt.

Azt konstatálhatjuk, hogy az off-shore cégeken keresztül jellemzően komoly nagy összegek, míg az egyéni bankszámlákon keresztül kisebb összegek pénzmosása valószínűsíthető.

Az Internet, - katonai felhasználás[53] céljából született és évtizedeken keresztül az USA hadügyminisztériuma, a Pentagon felügyelete alatt működött, - az 1990-es évektől kommercializálódott.

A szakirodalom az *Internetes kereskedelem* irányait a következőképpen csoportosítja:[54]

- B2B (Business to Business): az üzleti szereplők kapcsolata, pl. hirdetések, továbbá a kapcsolatfelvétel különböző formái, tudakozódás, ajánlat- illetőleg referenciakérés- vagy ezek nyújtása, szerződéskötés, információkérés, vagy - adás, információcsere, meghívások konferenciákra, vásárokra.
- B2C (Business to Consumer): az üzleti szféra az egyéni fogyasztóhoz kíván eljutni, pl. hirdetésekkel, termék- és szolgáltatások felkínálásával, értékesítésével.

[53] Az 1975-es a sikeres szovjet nagyhatótávolságú rakéta kilövés okozta sokk és félelem hívta életre, több vezetési pontot kellett az USA hadvezetésének létrehoznia, és azokat földalatti kábelekkel kötötték össze.
[54] http://www.digitsmith.com/ecommerce-definition.html [2016.12.08.]

- C2B (Consumer to Business): a fogyasztó fordul az üzleti szférához (pl. termék-, szolgáltatás rendelése, ügyvédi, orvosi szolgáltatás, segítség kérése.
- C2C (Consumer to Consumer): a fogyasztó a másik fogyasztót kívánja elérni, - a fentebb már említett second hand termékértékesítési -, aukciós -, hirdető - (electronic bulletin board) oldalakon történő termékelhelyezésekkel, vásárlásokkal, csereüdülésekkel, üdülési jogok hirdetésével és más árú- vagy szolgáltatás hirdetésével. De e körbe vonható a magánmunka keresés- és felajánlás (pl. bébiszitter-, takarítónői munka, gépelés, fordítás felajánlása).

Míg a fenti, első három esetben általában a szolgáltatás - ellenszolgáltatás realizálódik, az adózási kötelezettség teljesül, addig tipikusan a C2C relációban a pénz útja már nehezebben követhető, fiktív üzletkötések és pénzfizetések már előfordulhatnak. A bűncselekményből származó, „piszkos pénzek" a hirdető-, üzletet ajánló személy legális számláira „vándorolhatnak", vagy vice - versa is, a bűncselekmény elkövetése által szerzett dolog értékesítésére (orgazdaság megvalósítására) is alkalmas. A fogyasztók egymás közötti kapcsolata, üzletelése az Internet segítségével zajlik. Bár orgazdaság, kisebb összegű pénzmosás és persze sok más bűncselekmény a valós térben is vásárokban, zugpiacon történhet, házalással, ügynöki tevékenységgel vagy annak álcázva is folytatható.
Az Interneten zajló üzleti - kereskedelmi kapcsolatok kis mennyiségű pénz legalizálására alkalmasak csupán, de arra eredményesen, mivel egyfelől az összeg nagysága nem ad erre gyanút, másfelől a szolgáltatás – ellenszolgáltatás teljesedése leplezhető.

Adat- és személyiséglopás

A személyiséglopás nem a modern kor találmánya. Krúdy Gyula kisregénye, az "Ál-Petőfi" (A lehullt csillag fénye) című kisregényében tulajdonképpen ezt a témát dolgozza fel. Az 1848/49-es forradalom és szabadságharc leverését követően az országot, olyan emberek járták, akik magukat – miután Petőfi sorsáról sokféle egymásnak ellenmondó hír keringett - a bujdosó Petőfinek adták ki, így kívánva szerezni maguknak pénzt és élelmet.

Az Internet világában a technika teremtette alkalmazásokkal élve (online vásárlás, kommunikáció, közösségi oldalak), ezeket használva sajnos, egyre több adatot osztunk meg magunkról, sokszor felelőtlenül, nem gondolva a veszélyekre, nem gondolva a későbbi évtizedek munkavállalási lehetőségben és párkapcsolatban esetlegesen jelentkező hátrányokra.

Minél több személyes adatot teszünk online elérhetővé, ezzel egyenes arányban annál inkább kitesszük magunkat a személyiséglopás veszélyének, amelynek során a bűnözők bizalmas személyes adatokat szereznek meg. Sok-sok nyomot hagynak a felhasználók magukról, szokásaikról a közösségi oldalakon, gyakorta változtatják a profilképet, csinos, fürdőruhás képekkel dicsekednek fiatal lányok ismerőseiknek, és ezt kiberbűnözők kihasználják.

A visszaélések változatos formát ölthetnek a közösségi oldalakon (Facebook, Messenger, Instagram) a kattintások (clickjagging) és like-ok „ellopása" révén.

A felhasználó nevében oszthatnak meg olyan tartalmat, amivel nem ért egyet, csatlakoztatják olyan csoportokhoz, személyekhez, akikhez - egyébként - eszük ágában sem volna tartozni, az Interneten rendelnek árut, szolgáltatást, számlát nyithatnak, hitelt vehetnek fel, netán, ha hozzáférnek elektronikus bankfiókukhoz, akkor a számlán levő pénzt is ellophatják (elkölthetik), a fürdőruhás képeket szex-oldalakon használnak fel.

A személyiséglopás megelőzéséért a felhasználók tehetnek, tehetnének a legtöbbet, mert az elkövetők többnyire nem azonosíthatók.

A visszaélések formáihoz igazodik a jogi felelősség:

- aki személyes adat jogosulatlan megszerez, az tiltottan szerez adatokat (Btk. 422.§),
- aki jogosulatlan megszerzett személyes adatokkal árut, szolgáltatást rendel stb. az információs rendszer felhasználásával valósítja meg a csalást (Btk. 375.§),
- aki a jogosulatlan megszerzett fényképet szexuális szolgáltatás hirdetésére, szexuális tartalomhoz felhasznál haszonszerzés céllal, az személyes adatokkal visszaél (Btk. 219.§).

Tradicionális csalás

A számítógép, mint eszköz jelenik meg a klasszikus *csalási* cselekményekben.

A megtévesztés lényege adatmanipuláció, vagy hamis adatok bevitele (in-put csalás). Ehhez a modi operandi egyes tipikus formái a szakirodalomban ironikus, sokszor groteszk elnevezéssel ismertek.

- Data-diddling (adatok "lóvá tétele") nem más, mint adatváltoztatás az in-put fázisban.
- Trojan Horse (a "trójai faló"): a normál programmal egyidőben jogosulatlan műveleteket is végeztet a számítógéppel.
- Salami - technique programmal "lecsíphető" a számítógép üzemidejéből vagy a kezelt adatokból.
- Masquerad (álarcos bál) programmal az elkövető más személy nevét, kódját felhasználva veszi igénybe a számítógép szolgáltatásait.
- Piggyback (háton lovagol) programmal az elkövető az elektronikus adatfeldolgozó rendszerbe történő jogszerű belépést és/vagy használatot követően hajtja végre jogosulatlan cselekményét.
- Supperzapp ("csak veszély esetén használni") olyan program indítása, amikor a számítógépes rendszer leáll, vagy hibásan működik, és kizárt a rendszert újraindítani a szokásos eljárásokkal. Viszont ezzel lehetővé is válik jogosulatlan beavatkozás az elektronikus adatfeldolgozás- és átvitel folyamatába.[55]

Néhány gyakorlati esettel illusztráljuk a csalás végrehajtását:

1a. Az elkövető adatok betáplálásával igyekszik jogtalan haszon elérésére:

1.aa. Az elkövető vagy általa más személy számára fiktív számlát vagy folyószámlahitelt nyit. (A Stanley Mark Rifkin-eset szolgál például.)

1.ab. Fiktív vagy valódi számlára jogtalan kifizetéseket eszközöl.

A hazai OTP alkalmazottja egy külföldi ügyfél számlájára fiktív kamatot íratott jóvá.

A (volt) Német Szövetségi Köztársaságban egy programozó több kiskorú gyermek után járó családi pótlékot utaltatott át nagyanyjának, aki mellesleg 80. esztendős volt.

1.ac. Fiktív átutalásokat végez saját vagy harmadik személy számlájára. Az Amerikai Egyesült Államokban U.D. Savings Bank pénztárosa a pénzintézet inaktív számláiról saját

[55] Council of Europe Legal Affairs: Computer – Related Crime. Recommendation No.R 89) 9. Strasbourg, 1990. 18. o.
Ralph. M. Stair Jr.: Computers in Today's World. Illinois, 1986. 506. o.

számlájára utaltatott 290.000.- dollárt.[56] A japán Agricultural Coop alkalmazottja a cég komputere segítségével 48 millió yent utaltatott át bátyja bankszámlájára. [57]

Hazánkban 1997-ben, az egyik legnagyobb kereskedelmi banknál, amely a kétszintű bankrendszer megteremtése előtt kizárólag devizaműveletekkel foglalkozott, egy 170 millió forintos számítógépes csalás kísérletét hiúsította meg a bank belső ellenőrzése. Az elkövetők idegen magánszemélyek számlájáról emelték le a pénzt, és azt szerették volna saját, illetve ismerősük számlájára utalni, ám cselekményüket leleplezték.[128]

1.b. Az elkövető adatok törlésével igyekszik jogtalan haszon elérésére:

1.ba. Az elkövetőnek vagy harmadik személynek az adósságát részben vagy egészben törli. Hazánkban az elkövető a számítógépterembe beosonva a 2.900.- ft-os vállalati lakbérhátralékát 3.000.- ft. bebillentyűzésével "egyenlítette ki".

1.c. Az elkövető a jogszerű szolgáltatást vagy kifizetést (pl. bér, egyéb járandóság átutalását) megsokszorozza stb.

1.d. Ilyen, és ehhez hasonló aktív magatartások mellett nagyon - nagyon ritkán *mulasztással* valósul meg a bűncselekmény. Az NSZK-ban egy programozó nem törölte a nyugdíjasok névsorából azok nevét, akik időközben elhunytak, hanem ezek nevére érkező járandóságokat a saját számlájára utalta.[58]

2. A megtévesztések másik fő formája a számítógép programjának manipulálása.

Az egyik müncheni bank dolgozója olyan programot szerkesztett, amelyben az aritmetikai utasítás a pénzösszeg tizedeire, a kifizetés pedig kerekített összegre vonatkozik. Az így keletkezett különbséget utalta saját számlájára. Ez az összeg nem elhanyagolható, hiszen fél év alatt kb. 500.000.- német márkát "gyűjtöget össze".[59]

Egy bostoni bank alkalmazottja programjával minden betétes számlájáról "lecsípett" egy - egy centet, amit a névsorban szereplő utolsó betétes számlájára utalt át. Ugye, nem nehéz kitalálni kinek a nevére.[60]

Egy minneapolisi bank részére egy "külsős" programozó, olyan programot szerkesztett, amely később az ő nevére szóló, de fedezetlen kártyáját is feldolgozta. "Ötletével" 135.733.- dollár kárt okozott.[61]

---

[56] 30A.N. Smith – W.J. Alexander – D.B. Medley: Advanced Office Systems. Cincinatti, Ohio 1986. 402. o.
[57] Atsushi Yamaguchi: Computer - related Crime in Japán. Tokyo, 1992. (Kézirat a würzburgi konferenciára.) 5.o.
[128] http://www.nepszabadsag.hu/Redakcio/Doc.asp?SID=5&IID7933&CID760&AID7333712 [2017.01.12.]
[58] Pusztai László: Komputerb˝unözés és a büntet˝ojogi reform az NSZK-ban. MJ. 34. 1987.11.sz. 958. o.
[59] Pusztai: i.m. 959.o.
[60] adja hírül Almási M.: Léghajó Manhattan felett. Bp. KJK. 1992. 102-103. o.
[61] A.N. Smith - W.J. Alexander - D.B. Medley: i.m. 402. o.

Egy hazai nagyban vidéki fiókjánál olyan programot juttat a bank telefonhálózatán keresztül a szerverre, amely 140.- millió forintot átutalt a megadott számlaszámra, majd önmagát megsemmisítette.[133]

A programmanipuláció - szintén - kivételesen, de mulasztással is elérhető pl. ha a programozó programjából "kifelejti" az ún. ellenőrzési mechanizmusokat és ezzel teszi lehetővé bűncselekmény elkövetését.

[133] Adja hírül a Magyar Hírlap, 1998. március 3-i száma, a 17. oldalon

Információs rendszer felhasználásával elkövetett csalás

Akik jogtalan haszonszerzés végett információs rendszerbe adatot bevisznek, az adatot megváltoztatják (manipulálják), törlik, vagy hozzáférhetetlenné teszik, illetve egyéb műveletek (jogszerű kifizetések, megrendelések megtöbbszörözésével) végzésével az információs rendszer működését befolyásolják, és ezzel kárt okoznak (Btk. 375.§).

A weboldalakon általában a hirdetők ingyenesen kapnak megjelenési lehetőséget, és csak akkor, és annyit fizet, ha hirdetésére rákattintanak (ráklikkelnek). Tehát minél többet kattintanak a hirdetésre, annál többet fizet a hirdető a weboldal tulajdonosának, vagy üzemeltetőjének.

A *kattintásos csalásnak* ma három ismert módszere van:

- egy olyan program, amely meghatározott időközönként hívást („kattintást") generál a weboldal valamely hirdetésére,
- olcsó béren, vagy munkanélkülieket kérnek fel, hogy a weboldal hirdetéseire klikkeljenek,
- a konkurencia kattint a reklámokra azért, hogy minél nagyobb költség kifizetésére kényszerítsék a hirdetőt.

A jelenséget a szakirodalom kattintásos csalás (clickjaggingnek) nevezte el, ez tetten érhető a közösségi oldalakon is, amikor pl. egy-egy érdekesnek tűnő hírhez történő odakattintás.

Az Internet megteremtette lehetőségét a licitre bocsátott tárgyak megvásárlását földrajzi, és a licit végéig időrendi korlátok nélkül.

A licitáló a kiválasztott tárgyat megtekintheti fényképen, elolvashatja róla a rövid ismertetőt, és ennek ismeretében licitálhat, órák, napok elteltével, akár többször is.

Az aukciós csalás során számos megtévesztő magatartással idézhető el a kár.

Lássunk néhány tipikus esetet:

1. A sikeres licitálást követően a nyertes vevő a vételár kiegyenlítését követően:

- Hamis, vagy (a licitálásra felkínált tárgyhoz képest) gyenge minőségű árut kap.
- Egyáltalán nem kapja meg a kifizetett árut a vevő.

Mindkét esetben a licitáláson nyertesek a postai utánvéttel történő áruátvétellel védhetjük ki az ilyen jellegű átveréseket. Más kérdés, hogy az aukciós szabályzat megengedi-e az utánvétes áruvásárlást, vagy azonnal, bankkártyával történő kiegyenlítéséhez ragaszkodnak a licitálást szervezők.

2. A másik módszer már bizonyos szervezetszerű csalás elkövetését mutatja.

a. Shill-csalás: ebben az esetben a licitálás során egy harmadik személy, egy hamis licitáns, vagy maga az eladó - hamis e-mail–címről, hamis azonosítóval – „tornássza fel" a licitárat. Kockázat nincs, hiszen, ha a shill-re marad az áru, nem történik semmi.
b. Shield-csalás: ebben az esetben is a licitálás során egy harmadik személy, egy hamis licitáns, vagy maga a vevő - hamis e-mail–címről, hamis azonosítóval – „tornássza fel" a licitárat. Majd amikor a legmagasabb árral a shield magára marad, akkor alacsonyabb árért átengedi az igazi licitálóra.
Az ehhez hasonló ajánlatokról magyar nyelvű tájékoztatást is kaphatunk az Interneten.

Korábban az Internethez történő csatlakozás a telefonvezeték harmadik szálán történt, talán ma már egyre kevesebb az ADSL vagy az IDSL csatlakozás. Ezt technikai lehetőséget használták fel az elkövetők az ún. *betárcsázós csalásra*. Az Interneten böngészők miközben bizonyos honlapokra (tipikusan casino-, gambling-, sex- oldalakra) látogatnak egy program kúszik fel számítógépükre. Ezek a „betárcsázós" programok bontják a normál kapcsolatot, ehelyett újat építenek fel, általában egy emelt díjas, tengerentúli vagy éppen műholdas számot tárcsáznak több száz forint/perc díjért. A modemes Internetezők sok esetben maguk sem tudtak, tudnak erről. Csak a következő havi telefonszámlájuk jelzi, hogy bizony itt egy „betárcsázós csalás" sértettjeivé váltak.

Az Internetes csalások ellen többféleképpen *védekezhetünk.*
A. Ne bánjunk könnyelműen e-mail címünkkel, e-mail címeinkkel! Ne osszuk meg feleslegesen e-mail címeinket.
B. Mielőtt bármit rendelnénk, vásárolnánk, kitöltött kérdőívet visszaküldenénk a számítógépünkön levő „Keresőprogramunkban" („browser" – programban: Internet Explorer, Netscape, Opera stb.) nézzünk utána a bennünket megkereső cégnek. Talán még magyar nyelvű tájékoztatást is kaphatunk róla.
C. Részletesen olvassuk el a vásárlás-, rendelés-, vagy licitálás feltételeit, különösen a szolgáltatásra-ellenszolgáltatásra vonatkozó rendelkezéseket. Idegen nyelvű ismertető esetében – saját érdekünkben – törekedjük annak tökéletes fordítására!
D. Ne töltsünk ki, ne küldjünk vissza olyan válaszokat, aminek a tartalmával nem vagyunk tisztában, bizonytalanok vagyunk, különösen, ha az idegen nyelvű.
Magyar pénzintézetek soha nem kérnek információt e-mailben!

E. Bizonyos időközönként keressünk rá az Internetes csalásokról szóló írásokra, hogy lássuk, milyen új módszerek terjednek el.[62]

A számítástechnikával foglalkozó weboldalakról hasznos tanácsok leshetők el!

F. Betárcsázós programok ellen a modemes felhasználók feltétlenül telepítsenek gépeikre malware-kereső programokat.

G. Bátran kérjünk tanácsot a számítástechnikában jártas szakemberektől!

[62] http://www.fraudbureau.com/directory/m.php3/Fraud_on_the_Net [2016.09.31.]

Számítógépes hamisítás

A számítógépes hamisítás jellemzően adatmanipulálást jelent. Ez történhet adatbeviteli (in-put) szakban, illetőleg az elektronikus adatfeldolgozásba történő beavatkozással. Veszélyessége abban rejlik, hogy a hamisítványok tökéletesek lehetnek, azaz az eredetivel, a valódival összekeverhető.

A számítógéppel történő hamisítás esetei:

- a közokiratok hamisítása.
- a készpénz-helyettesítő fizetési eszközök hamisítás,
- a pénzhamisítás.

Közokiratok hamisításának a veszélyessége. A számítógépek nagy tömegű és gyors adatkezelésének előnyei a közigazgatási területén is elvitathatatlan. Viszont az adatváltoztatás *számítógépben vagy más adathordozón tárolt közokirat készítéséhez felhasznált adatok hamisításának* veszélyére fel kell figyelnünk.

Az adatok tartalmának sokrétűsége miatt nemcsak vagyoni értékeket jelölhetnek, hanem állami - társadalmi - gazdasági - jogi - igazgatási kapcsolatokat megalapozó tényeket is, amelyek valódiságukkal megalapozzák, igazolják e viszonyok létezését, funkcionálását vagy megszűntét. Az elektronikus adatfeldolgozás keretében ezen adatokat ugyanúgy közhitelesnek kell tekintenünk, mint a papíron rögzített közokirat esetében.

A közhitelesség, mint kiemelkedő érték, és érdek védelmére az állam büntetőjogi eszközöket is igénybe vesz. Az eddigi jogfejlődés során, a közhitelességen alapuló közbizalom (publica fides) büntetőjogi védelme akkor jött, és jön szóba, ha az adatok, tények, nyilatkozatok, intézkedések illetve határozatok köz- vagy magánokirat formájában öltenek testet.

Napjainkban az adatok manipulásával vagy az elektronikus adatfeldolgozás egyéb módon történő jogosulatlan befolyásolásával létrejövő adatok a közhitelességbe vetett bizalmat rendítik meg azáltal, hogy annak bizonyítására alkalmatlanná válnak.

A magyar büntetőjogban mind a hamis közokirat készítése, közokirat meghamisítása és mindezen cselekmények előkészülete is büntetni rendelt (Btk. 342.§ (1) bekezdése a) pont és (2) bekezdése).

Bár a pénzhamisítás nem tartozik a tipikus számítógépes környezetben elkövetett bűncselekmények közé, de a hamisításhoz szükséges szoftverek készítése (írása), beszerzése a pénzhamisítás elősegítését meríti ki (Btk. 390.§). Amennyiben ezek a pénzhamisítás

közvetlen céljával valósulnak meg, akkor a pénzhamisítás előkészülete miatt büntetendők (Btk. 389.§ (3) bekezdése). A nyomtatásról, akár szkennelésről, akár már hamis pénz készítéséről beszélhetünk (Btk. 389.§ (1) pontja). Az out-put hamis pénz minősége nem bír jogi relevanciával, lehet primitív másolat vagy akár profi, felismerhetetlen, összetéveszthető bankjegy.

A számítógéppel végrehajtható tökélyig /?/ véghezvihető hamisítás kapcsán felrémlik George Orwell negyvenes évek végén írott démoni látomása a dokumentumok meghamisításának veszélyességéről, amely természetesen túlmutat a büntetőjogi felelősség problémakörén: "Mihelyt..... szükségessé vált valamennyi javítást végrehajtották és ellenőrizték, a szóban forgó számot újranyomtatták, az eredeti példányt megsemmisítették, és a javított példányt tették a helyére. Ezt az állandó változtatási eljárást alkalmazták nemcsak az újságokban, hanem a könyvekben, folyóiratokban, pamfletekben, plakátokon, röpiratokban, filmeken, hanglemezeken, karikatúrákon és fényképeken is - azaz minden olyan irodalmi vagy ideológiai szempontból jelentősége lehetett. A múltat napról napra, sőt szinte percről percre a jelenhez igazították. ..... nem tűrték, hogy egyetlen olyan hírnek vagy kinyilatkoztatásnak nyoma maradjon, amely ellentétben volt a pillanatnyi követelményekkel."[63]

[63] George Orwell: 1984., Budapest, 1989. 47-48. o.

Szerzői jogi jogsértések az Interneten

A számítástechnikai eszközök elterjedése, az Internet széleskörű elérése, a kompiláció, a többszörözés technikai feltételeihez jutás a szerzői jogsértések tömegességét tettek, teszik lehetővé.

Megszűnt a szerzői jogi alkotások készítésének, másolásának, terjesztésének eddig működött monopóliuma.

A szerzői jogi törvény tételesen felsorolja, a védendő szellemi alkotások körébe vonja a szerzői jogi védelemben részesülő irodalmi, tudományos és művészeti alkotásokat, a szabadalmazható találmányt, az oltalmazható használati mintát, az oltalmazható növényfajtát, az oltalmazható formatervezési mintát és a mikroelektronikai félvezető termék oltalmazható topográfiáját (a chipet). (Szjt. 1999. évi LXXVI. törvény 1.§ (2) bekezdése).

Már nem ritka az az eset, hogy a szerzők – többféle ok, elképzelés folytán - az Interneten mutatja be alkotásait, és az elérésük lehetőségét.

A felhasználók pedig a saját igényüknek, ízlésüknek megfelelő zenei-, filmes-, képi stb. válogatásokat készítenek maguknak, és környezetüknek a már forgalomban kapható, vagy az Interneten elérhető szerzői alkotásokból. Nem szükséges ugyanazon, vagy más előadóktól tucatnyi CD-t vásárolni, hogy kedvenc felvételeit bárki is egy CD-n hallgathassa. A felhasználó nem függ a kereskedelmi kínálattól. De nem szükséges drága művészeti albumokat vásárolni, ha valaki egy művész, egy korszak művészeti alkotásaiért rajong. Ezek az alkotások digitalizálhatók, letölthetők az Internetről, CD-re másolhatók, színes nyomtatón kinyomtathatók, kiváló minőségben, vagy DVD-lejátszóval televízión keresztül nézhető. Sőt, mindehhez zene, más hanghatás illeszthető, és ezzel tehető az élmény teljessé.

A régi vinyl-klorid, (köznapi nevén: bakelit) lemezekről .mp3 vagy más formátum készíthető (rippelhető), amely aztán CD-re felírható, így a régi zenei felvételek (kisebb minőségromlással ugyan, de) megőrizhetők évtizedekig.

A DVD-n, VCD-n kiadott filmek Magyarországon általában nem szinkronizáltak (ehhez kicsi a hazai piac), így ez annak élvezetét csökkenti. Viszont ez a kellemetlenség is elhárítható, mert kis leleménnyel a filmek elláthatók szinkronnal. A videófájlok ún. konténerformátumok, azaz több adatfolyamot tartalmaz. A DVD VOB-fájljaiban levő MPEG-2 videófájl leválasztható az AC-3, MPEG-2, PCM hangfájljaitól, és így mind a videó-sáv, mind az audió-sáv önállóan felhasználható. Ez teszi lehetővé, hogy a DVD-n, VCD-n levő

kiváló minőségű képhez egy videó-kazettáról (amely akár gyári, akár a tv-műsorról) ugyanazon filmhez magyar nyelvű szinkron illeszthető.

Természetesen nem szükségszerű, hogy a modern technikai eszközöket, technológiákat szerzői jogi jogsértések elkövetésére használják.

Szerző alkotások megjelenése:

- A szöveget tartalmazó fájlok leggyakoribb kiterjesztései: .doc, .rtf, .txt, .wri stb.

Különlegesek a filmekhez készült feliratok, amelyek .srt, .sub stb formátumban szerepelnek.

- Az adatfájlok leggyakoribb jelölései: .xls, .dat, .dbf, .lst stb.
- A kép- és grafikai fájlokat a .bmp, .gif, .jpg, .png, .pcx, .tif, .xpm, .w1, .wmf., .ai és más kiterjesztések jelölik.

- A hangfájlokat a következő jelölések mutatják: .au, .aiff, .mp3, .rm, .ogg, .wav stb.
- A videó fájlok kiterjesztései: .asf, avi, .mpg, .mpeg, .mov, .wmv stb.

A szerzői művek teljes köre *digitalizálható*. Ezáltal az elektronikus adatfeldolgozó- és adatátviteli rendszerekben valamely fájlformátumban megjeleníthető, ezzel nagy tömegben, gyorsan, gyakorlatilag bárki által elérhető, többszörözhető, cserélhető, adathordozókon rögzíthető, továbbadható, (és akár jogtalan haszonszerzés végett) forgalmazható.

A szerzői jogi jogsértések tipikus helyei az Interneten:

- Weboldalakon szerzői mű a szerző engedélye nélkül történő megjelenítése,
- E művek ingyenes, vagy díjfizetés ellenében történő letöltésének engedélyezése weboldalakról, FTP - vagy más szerverekről.
- Szoftverek védelmi programjának feltöréséhez “crack”- “patch”- “keygeneretor”-programok weboldalakra, FTP-. IRC- vagy más szerverekre történő feltöltése, és onnan letöltés engedélyezése.
- Szerzői jogi műveket megjelenítő fájlok “cserélgetése”, küldése.
- Hálózaton keresztül történő (jogszerű, vagy jogellenes) belépés, és a számítógépről szoftverek lemásolása, használata, terjesztése stb.

A szerzői jog tömeges megsértésének lehetősége a számítógép megjelenésével kezdődött, lehetőség nyílott a szerzői művek digitalizálására, másolására, többszörözésére hajlékonylemezre, compact disc (CD)-re. E tömegesség mellé napjainkban a file-sharing (fájlmegosztás, fájlcsere) tömegessége járul..

Fájlcsere során a felhasználók egy fájlcsere-program segítségével összekapcsolódnak, azaz hálózatot alkotnak. Létezik centralizált (egyszerverhez kapcsolódó) illetőleg decentralizált (több szerverhez kapcsolódó) modell, ezen kívül a torrent-technológia. Valamennyi

felhasználó „feltöltéssel” felkínálja a saját számítógépén levő szerzői alkotásokat, annak fejében, hogy ő pedig „letölt” más felhasználó számítógépén levő szerzői alkotásokat. Létrejön a két felhasználó között egy zárt ún. P2P (Peer-to-peer) kapcsolat.

Ha Surface Weben történik a szerzői jogi jogsértés, például egy warez vagy más letöltő oldalról, akkor a felelősség kérdései a következők:

- a feltöltő büntetőjogi felelősséggel tartozhat (Szerzői vagy szerzői joghoz kapcsolódó jogok megsértése, Btk. 385.§), mivel a szerző engedélye nélkül (Szerzői jogi tv. 10.§ (1) – (2) bekezdései) és ezzel vagyoni hátrányt okoz,
- a tárhelyszolgáltató, aki tárhelyet (pl. szervert, weboldalt) biztosít a Btk. 385.§ fizikai bűnsegédjeként vonható felelősségre,
- a letöltő akkor felel, ha a letöltés kárértéke 500.000.- forintot (Btk. 385.§ (5) bekezdése utal az (1) bekezdésre) meghaladja a letöltés,
- további felelősségi kérdés, ha emelt díjas telefonszámmal lehet hozzáférni a letölteni kívánt fájlokhoz, akkor az emelt díjas telefonszolgáltatást biztosító távközlési vállalkozás a dogmatika szabályai szerint a távközlési vállalkozás is a Btk. 385.§ fizikai bűnsegéde.

Torrent klienssel történő letöltés esetében a helyzet bonyolultabb. A torrent-szerver üzemeltetőjénél nem található fájl, csupán közvetít, azaz egy linket ad tovább, amit a feltöltő biztosít a feltöltést felkínáló és a letöltő személyek között. Ugyanakkor a feltöltőnél vagy megvan a teljes szerzői alkotás vagy annak egy része, szelete. A feltöltőnél lévő fájlszeleteteket továbbadja annak a letöltőnek, akinek a szerzői alkotás teljességéhez ez a fájlszelet hiányzik. Cserébe a feltöltő egyszerre letöltő is, mert a fájlszeletek továbbadása fejében megkapja azokat a fájlszeleteket, amelyek neki hiányzik a szerzői alkotás teljességéhez.

A feltöltő szerzői jogsértést követ el, a letöltő a fentebb említett értékhatárig nem büntethető.

A szerzői jog védelmével felmerül az az aggály, hogy a szórakoztató elektronikai terméket gyártók olyan fájlformátumok lejátszására alkalmas készülékeket gyártanak, amely fájlformátumok kereskedelmi forgalomban nem lehet beszerezni (xvid, divx és más tömörítésű technológiával tömörített filmeket nem lehet beszerezni legális forrásból). Ezek a fájlformátumok általában illegálisan érhetők el az Interneten.

A hazai jogi szabályozás kialakításánál egyfelől a társadalmi és technikai realitásából, másfelől a szerzői jog és a szerzői jogra épülő iparág érdekeiből kell kiindulni. Ez utóbbi érdek a szerző személyes és vagyoni jogainak érvényre juttatását, továbbá a szerzői

alkotásokat előállító, forgalmazó iparág (a CD-, DVD-, könyvgyártás a kereskedelmi egységekig, moziig terjed) létét jelenti. Az ehhez vezető nem egyszerű kompromisszumhoz a 2001/29-es EK Irányelv nyújthat segítséget.

Az Európai Parlament és a Tanács 2001. május 22-i 2001/29/EK Irányelve (Directive) „az információs társadalomban a szerzői és szomszédos jogok egyes vonatkozásainak összehangolásáról" 38. cikkelye, e törekvést a tagországok számára kötelezővé emeli:

„A tagállamok számára lehetővé kell tenni, hogy méltányos díjazás biztosítása fejében a hang, kép- és audiovizuális anyagok magáncélú többszörözésének egyes fajtái tekintetében a többszörözés joga alól kivételt, illetve korlátozást állapítsanak meg. Ide tartozhat a jogosultakat ért hátrányok ellentételezése érdekében alkalmazott díjazási rendszer bevezetése, illetve fenntartása is. Bár az ilyen díjazási rendszerek közötti különbségek hátrányosan befolyásolják a belső piac működését, az analóg magáncélú többszörözés tekintetében valószínűleg nem gyakorolnak jelentős hatást az információs társadalom fejlődésére. A digitális magáncélú többszörözés valószínűleg jóval nagyobb mértékben terjed el, és gazdasági jelentősége is nagyobb lesz.

A digitális és az analóg magáncélú többszörözés közötti különbségeket ezért kellőképpen figyelembe kell venni, és bizonyos vonatkozásokban különbséget kell tenni köztük."

E cikkely értelmezése akképp is történhet, hogy míg az analóg másolásnál ragaszkodhatunk a szerzői jog ma is hatályos szabályaihoz, addig a digitális másolásnál már más szempontok figyelembe vétele lenne kívánatos (pl. a digitálisan rögzített szerzői alkotások védelmére egy meghatározott ideig zérótolerancia vonatkozna, ám azt követően már visszafogottabb lehetne a szigor, esetleg a hozzáférést biztosító szolgáltatóknak letöltés arányosan kellene az előfizetési díjat fizetni, de más megoldások is szóba jöhetnek).

A jogtalan adatkikémlelés

A számítástechnika fejlesztésének egyik mozgatórúgója a nagytömegű és a gyors adatkezelés igénye és szükségessége. A szilíciumchipek méretcsökkentése és a számítógépek működési sebessége már közel került a fizikai megvalósíthatóság határához. Bár ez a megállapítás, mindig csak a következő ámulatot keltő komputer piacra dobásáig igaz.

Az elektronikus adatfeldolgozó- és átviteli rendszerek terjedésével, az adatok tartalma sokszínű. Véges felsorolás talán nem is adható arról, hogy a számítógépeinken tárolt, a számítógépes rendszereken kezelt adatok milyen tartalmat jelenítenek meg.

Az elektromos impulzusok jelölhetnek:

- különböző titokfajtákat (tipikusan intézmény zárt Intranet rendszerén),
- más fontos adatok (titoknak nem minősülő, ám pl. kémkedés tárgyául szolgáló információ tipikusan intézmény zárt Intranet rendszerén),
- személyes, különleges személyes adatokat /tipikusan a felhasználók saját számítógépein, az intézmények szerverén levő e-mailekben),
- a jog megítélése szerint neutrális tartalommal bíró adatokat (pl. a büntetőjogilag irreleváns hírek, képek az Interneten)

Az adatok sokrétűsége miatt (is) azok jogosulatlan megszerzésére, megismerésére irányuló igyekezet is felerősödött.

Az előtérbe került ipari - gazdasági hírszerzés, az ún. "versenyinformációk" (pénzügyi - gazdasági, technológiai, értékesítési információk, stratégiai tervek stb.) megkaparintása mellett számítógépes környezetben a személyes adatok, a felhasználóhoz köthető információk (e-mail cím, fájlállomány stb.), Internetezési szokások (a felhasználó érdeklődését reprezentáló böngésző-program használatának, látogatott oldalaknak a stb.) megismerésére irányul egyre gátlástalanabb, és kiterjedtebb törekvés.

Az angolszász szakirodalomban elterjedt a "bitnapping" kifejezés, amely egy szellemes szójáték a "kidnapping" (a gyermekrablás, tágabban értelmezve az emberrablás) analógiájára.

Az adatállományokat a legkülönfélébb módon igyekeznek védeni az illetéktelen "szemek" elől, kezdve az elektronikus adatfeldolgozó- és átviteli rendszer fizikai (hozzáférési) biztosításától, a számítógép jogszerű (engedéllyel bíró) használatán, vagy adatók kódolásán át, az adatállományok jelszóval történő védelméig.

Mivel nem létezik abszolút védelem, megfejthetetlen kód, ezért "csupán" arra lehet törekedni, hogy a kód feloldása több időt vagy anyagi ráfordítást igényeljen, mint amennyit az adat "ér".

Ezzel együtt az adatok jogosulatlan megismerésének és megszerzésének, az adatlopások módjai is változatosak:

A. A rendszerbe történő jogszerű belépést vagy jogellenes behatolást követően az adatok a számítógép memóriájából vagy egyéb adathordozóról behívhatók, megtekinthetők monitoron, átmásolhatók más adathordozóra vagy kinyomtathatók stb. Ebben az esetben k ö z v e t l e n ü l férkőzhet az adatokhoz.

A közvetlen módszerek közé tartozik ma már a telefon- és adatátviteli vonalak "megcsapolása", valamint passzív módon megvalósítható a monitorok elektromágneses sugarainak "lehallgatása" is. (A magyar MHB "társbérlőjével" levő Puma magyarországi leányvállalatával 1992-ben vitába keveredik, mert a bank biztonsági megfontolásokból, a számítógépek monitorai sugárzásának jogosulatlan "lehallgatását" megakadályozandó befalaztatott egy olyan bejárati ajtót, amelyet a Puma cég dolgozói használtak.)

B. Az adatok megismerhetők k ö z v e t e t t e n is, így pl. a mágneslemezek-, szalagok, lyukkártyák- és szalagok, a hajlékony-, floppy, CD-, DVD- lemezek, a számítógép (laptop, notebook esetében tipikus lehet), az ebből kiszerelhető merevlemez eltulajdonításával is, majd tartalmának térben és időben távolabb történő megismerése.

C. Különféle kémprogramok (spyware-eket) telepíthetők a felhasználó tudtán és akaratán kívül, amelyek álcázva, más programok, letöltött fájlok részeiként bújnak meg, és amelyek megfigyelik számítógépünket, és jeleznek a címzettnek tevékenységünkről, fájlainkról, Internetezési szokásainkról, e-mail-címünkről stb.

Az adatkikémlelés fogalma tehát - felöleli az elektronikus adatok bármilyen módon történő jogellenes megismerését.

A számítástechnikai rendszer (ideértve a mobiltelefonokat, iPhone-okat, iPadokat, tableteket és más elektronikus üzenetet tárolni képes technikai eszközöket) biztonsága, integritása a „házijog” körébe tartozik. Így ezen eszközökön található elektronikus adatok megszerzése, az elektronikus adatátviteli, távközlési hálózatok lehallgatása akár a végpontokon, akár rácsatlakozva tiltott adatszerzésnek minősül (Btk. 422.§).

Az elektronikus adatok tartalma szerint lehetnek:

Jogszabályi alapjai vannak a személyes adat illetőleg az üzleti titok fogalmának.

Személyes adat: az érintettel kapcsolatba hozható adat – különösen az érintett neve, azonosító jele, valamint egy vagy több fizikai, fiziológiai, mentális, gazdasági, kulturális vagy szociális azonosságára jellemző ismeret –, valamint az adatból levonható, az érintettre vonatkozó

következtetés. (Az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény 3.§ 2. pontja).

Üzleti titok: a gazdasági tevékenységhez kapcsolódó minden olyan tény, információ, megoldás vagy adat, amelynek nyilvánosságra hozatala, illetéktelenek által történő megszerzése vagy felhasználása a jogosult - ide nem értve a magyar államot - jogszerű pénzügyi, gazdasági vagy piaci érdekeit sértené vagy veszélyeztetné, és amelynek titokban tartása érdekében a jogosult a szükséges intézkedéseket megtette. (A PTK-ról szóló 2013. évi V. tv. 2:47.§ (1) bekezdése.)

A magán- illetőleg a gazdasági titok fogalmát a gyakorlat alakította ki, az üzleti titoknak létezik szabatos, törvényben definiált meghatározása.

Magántitoknak tekinthetünk minden olyan tény, adat vagy körülmény, amelynek megőrzéséhez a sértettnek méltányolható - tehát másokat nem veszélyeztető - érdeke fűződik. Idetartozhatnak a személy egészségügyi, vagyoni és más titok.

Gazdaság titok minden olyan adat, tény vagy információ, amelynek titokban maradásához a titokgazda gazdasági szereplőnek gazdasági érdeke fűződik.

Zaklatás és gyermekpornográfia az Interneten

Az Interneten számtalan kommunikációs lehetőség és alkalmazás vehető igénybe, a közösségi oldalak, a chat, a twitter, messenger, skype, stb. amely nem más, mint írásban, valós időben (real-time) folytatott, folytatható „beszélgetés", ha azonnal reagál a másik fél.

A világhálót leginkább a fiatalabb korosztály használja tanulás, ismeretszerzés, szórakozás, vagy egyszerűen unaloműzés céljára, azaz szörfözik, levelezik, chatel. Mindezt leginkább egyedül.
Egyedül, mert a szülők munkavégzés, szórakozás, vagy más ok folytán távol vannak otthonuktól, vagy ha otthon is tartózkodnak, nem értenek a számítógéphez, az Internethez.
A kiskorú is keresi az egyedüllétet a világhálóval, mivel felfedezte azt, hogy olyan információkat érhet el a virtuális térben, amiktől a valódi térben el van zárva.

A világháló legveszedelmesebb jelenségei közé tartozik: a gyermekek zaklatása és a gyermekpornográfia.

Napjainkban a zaklatás (bullying)[64], különösen az elektronikus zaklatás (cyberbullying) jelenségének vizsgálata előtérbe kerül a közösségi média népszerűségének és a mobil eszközök széleskörű elterjedésének köszönhetően.

Számos olyan magatartás van, amely önálló tényállásként büntetendő és a megfélemlítés határán helyezkedik el, vagy elkövetési magatartása a bullying eszközcselekménye. Ilyen például a magánlaksértés, az online kommunikációs eszközök lehallgatása, az identitáslopás, az online becsületsértés, rágalmazás és a személyes adatok engedély nélküli készítése és közzététele. Utóbbival a cyberbullying irodalom az ún. „revenge porn", azaz a kompromittáló videók, fényképek bosszúból történő online megosztásával, és az ún. „slut shaming" jelenséggel külön foglalkozik. A slut shaming során általában a fiatalok az áldozatról megszégyenítő videókat készítenek például házibuli során, miután bedrogozták és levetkőztetik az elkábult fiatalt (ezt szexuális erőszak is követheti).[65]

---

[64] Parti Katalin: A megfélemlítése (cyberbullying) szabályozása Magyarországon és külföldön. In Medias Res 2016/1. 115. o.: A bullying három konjuktív elemet tartalmaz:

- fizikai, verbális vagy pszichológiai támadás vagy megfélemlítés, amelynek célja félelem vagy stressz vagy egyéb ártalom okozása;
- a fizikai vagy pszichikai erőegyensúly hiánya, amelyet kihasználva az erősebb személy vagy személyek nyomást gyakorolnak a gyengébbre;
- rendszeresen ismétlődő vagy huzamosabb ideig, folyamatosan fennálló helyzet két személy vagy személyek között. Cyberbullying esetén nincs szükség a tett ismétlődésére, hiszen például egyetlen megosztással is hatalmas kárt tudnak okozni.

[65] Parti (2016/1): i.m. 114-146. o.

A cyberbullying típusai:

- *Flaming („lángháború")* Online veszekedés dühös és trágár nyelvezet használatával, illetve - sokszor nem az adott témába vágó -, támadó jellegű hozzászólások küldése valakiről nyilvános fórumra.
- *Harrassment (támadás-sorozat):* Bántó, valótlan üzenetek küldése online.
- *Denigration (befeketítés):* Kegyetlen, a hírnév rontására alkalmas pletykák vagy szóbeszéd küldése, kiposztolása, terjesztése valakiről.
- *Exclusion (kiközösítés):* Az online közösség egy tagjának a csoportból való kirekesztése.
- *Impersonation (személyiséglopás):* Az elkövető egy másik, létező személy online profiljában jelenik meg, és hírnevének rontására alkalmas üzeneteket küldözget a nevében.
- *Outing (kibeszélés):* Titkok, pletykák vagy egyéb személyes információk engedély nélküli megosztása másokkal.
- *Trickery („trükközés", becsapás):* Személyes adatok csalással, megtévesztéssel történő megszerzése valakitől, majd ennek az információnak, adatnak a megosztása a közösséggel.
- *Cyberstalking (online zaklatás):* Az áldozat online szokásainak megfigyelése, folyamatos figyelemmel kísérése és támadó jellegű kijátszása.
- *Cyberthreats (online fenyegetések):* Olyan, közvetlen fenyegetések vagy nyugtalanító kijelentések, amelyekből úgy tűnik, hogy a szerző érzelmileg felkavart, és fontolgatja, hogy valaki mást, vagy magát bántja, illetőleg öngyilkosságot követ el.
- *Sexting:* A kifejezést olyan helyzetekre használják, amelyekben az elkövető szexuálisan provokatív és saját maga által készített meztelen vagy félig meztelen képeket vagy nyíltan szexuális tartalmú szöveget küld el online valakinek. A legnagyobb figyelmet a meztelen képek küldése kapja, mert az ilyen felvételek további, széleskörű terjesztése sokkal valószínűbb, és a fiatalokat nagyobb kockázatnak teszi ki.[66]

A cyberbullyingre nincs egyértelműen ráilleszthető tényállás, a joggyakorlat ezzel adós marad. Azonban az elektronikus zaklatás egyes esetekben a zaklatás[67] tényállásának minősül, nem különíthető el, különösen a telekommunikációs eszközzel elkövetett esetekben: például

[66] Domonkos Katalin: Cyberbullying: zaklatás elektronikus eszközök használatával. Alkalmazott pszichológia 2014/14(1) 60.o.
Péli-Tóth Viktória: Kortárs online zaklatás, a cyberbullying jelenség. In: Elek Balázs – Fázsi László (szerk.): Az ítélőmesterség dilemái. Tanulmányok Dr. Remes Zoltán bíró emlékére, Debrecen, Printart-Press, 2015. 39-40.o.

[67] Btk. 222. § (1) Aki abból a célból, hogy mást megfélemlítsen, vagy más magánéletébe, illetve mindennapi életvitelébe önkényesen beavatkozzon, őt rendszeresen vagy tartósan háborgatja, ha súlyosabb bűncselekmény nem valósul meg, vétség miatt egy évig terjedő szabadságvesztéssel büntetendő.

az ún. „happy slapping” esetén, amikor a sértett bántalmazását képekre vagy videóra rögzítik, majd ezt a közösségi oldalra feltöltik.[68]

Az új Btk. létrehozott olyan új tényállást is, amely a 21. századi kihívásoknak megfelelően biztosítja a magánszféra védelmét. 2013 óta hatályos a becsület csorbítására alkalmas hamis hang- vagy képfelvétel készítése, illetve annak nyilvánosságra hozatala (Btk. 226.§/A-B).

A szabad, távoli és gyors kommunikációt kihasználják azok a beteges pedofil hajlamú személyek, akik az anonimitás mögé rejtve ilyen módon (is) ismerkednek a kiskorúakkal. Nem szükséges, hogy óvodák, iskolák, diszkók előtt álldogálva, felfedve kilétüket keressék a kapcsolatot kiskorúakkal. Az Interneten a kiskorúak legveszélyeztetettebb helye az ún. chat-szobák, illetve a már széleskörben elérhetővé vált mobil eszközök és azok applikációi, amelyek segítségével könnyedén a gyermekek csatlakoznak a különböző közösségi oldalakhoz (Facebook, Twitter, Instagram stb.), közvetlen kommunikációt biztosító alkalmazásokon (pl. WhatsApp) keresztül üzeneteket váltanak. Az ún. „grooming” jelenség, a gyermekek szexuális célzatú kapcsolatfelvétele egyre veszélyesebbé vált a technológiai fejlődésnek köszönhetően, mert a gyermekeknek komoly sérelmet lehet okozni online is és ugyanolyan kockázatnak vannak kitéve, mint a való életben például a „screen-to-screen” chat vagy webkamerával történő videokommunikáció során szemtanúi lehetnek vagy könnyen rábeszélhetők kifejezetten szexuális tevékenyég tanúsítására a kamera előtt, és tovább nehezíti a helyzetet, hogy ezek a funkciók már szélesebb körben, a mobil alkalmazásokon keresztül is elérhetők.[69]

A pedofil személy bekapcsolódik bármely kommunikációs lehetőségben egy-egy beszélgetésbe, majd az egyik résztvevőt, akit már ismer, vagy szimpatikus számára, azt „privibe hívja”, azaz olyan (privát) beszélgető csatornába, amelyben csak ketten társaloghatnak tovább (chaten, Facebookon, skype-on stb.). A legtöbb esetben a grooming kezdeti folyamata részét képezi az ún. „sextortion”, vagyis a szexuális zsarolás. Az elkövető a gyermek bizalmába férkőzik úgy, hogy például a felnőtt fiatalkorúnak adja ki magát és barátkozik, gyakorta képeket küld a kiskorúak, amelyeken a szex, mint játék, mint vidám csínytevés szerepel, ezzel próbál kedvet csinálni és majd az áldozatról is kér kompromittáló képeket, amelyet követ a zsarolás. A sextortion lényegében azt jelenti, hogy az elkövető kényszeríti, zsarolja az áldozatát, hogy szexuális szívességet teljesítsen a részére, vagy

[68] Monori Zsuzsanna Éva: Zaklatás-e a cyberbullying? In Medias Res 2016/2. 252. o.

[69] Lanzarote Bizottság véleménye a Lanzarote Egyezménynek és indoklásának a 23. cikkével kapcsolatban https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000168046ebc8 [2016.12.21]

további kompromittáló képeket vagy videókat küldjön magáról, amennyiben a kérésnek nem tesz eleget, akkor a már birtokában lévő felvételnek a megosztásával fenyeget (pl. a közösségi médián keresztül), és ezzel már irányítása alá vonja a gyermeket.[70] Kihasználva a gyermek naivitását, a „közös (zenei, film, futballklub stb.) érdeklődésre", a „közös titkokra", apróbb ajándékok adására (kabalafigurák, filmplakátok, futballklub mezek, sálak stb.) hivatkozva találkozót kér a kiskorútól, és ezen a találkozón előfordul az ún. randi erőszak (date rape). Majd a kierőszakolt randevún a pedofil – gyakorlati eset bizonyítja, sajnos - hogy arra fog hivatkozni, miszerint a gyermeke, unokája beteg és gyógyulását segítené, ha meglátogatná őt a lakásán. De ugyanígy ismert az is, amikor édességet, süteményt kínálva, amikor a gyermek kezei foglaltak, kezdi a pedofil fogdosni a gyermeket.

A büntetőjogi minősítés, az életkorok és elkövetési módok sokrétűsége miatt többféleképpen lehetséges:

Ha az elkövető a szexuális kényszerítést erőszakkal, illetve az élet vagy a testi épség elleni közvetlen fenyegetéssel követi el, védekezésre vagy akaratnyilvánításra képtelen állapotát szexuális cselekményre használja fel akkor a szexuális erőszakért felel (Btk. 197.§).

De büntetendő akkor is, ha a kényszerítés nem minősül a fentiek szerint, akkor szexuális kényszerítésért felel (Btk. 196.§).

Ha a sértett 12. életévét nem töltötte be és erőszak, valamint fenyegetés hiányában történt a szexuális cselekmény, akkor a védekezésképtelenre állapotra tekintettel (amely praesumptio juris et de jure) szexuális erőszak alapesetéért felel az elkövető (Btk. 197.§ (1) bekezdése).

Ha erőszak és élet, testi épség elleni közvetlen fenyegetéssel történik, akkor már ugyanezen bűncselekmény minősített esetéért vonandó felelősségre (Btk. 197.§ (2) bekezdése).

Ha a sértett 14-18 év között van, akkor, ha a szexuális cselekményt erőszak, élet, testi épség elleni közvetlen fenyegetés előzte meg, akkor a szexuális erőszak minősített esetéért felel az elkövető (Btk. 197.§ (3) bekezdése a) pontja).

Ha a sértettel szembeni kényszerítés nem minősíthető az előzőek szerint, akkor a szexuális kényszerítés minősített esetéért felel. (Btk. 196.§ (3) bekezdése a) pontja).

A 12-14 év közötti sértett esetében a szexuális cselekmény szexuális visszaélésként értékelendő (Btk. 198.§ (1) bekezdése).

[70] EUROPOL – Internet Organised Crime Threat Assesment (IOCTA) 2014. 30. o.

A „randi erőszak” (date rape) *megelőzése*

A gyermekek világhálón való böngészését, kommunikációját nem lehet, és nem is szabad megtiltani.

A szülők kötelessége az, hogy óva intsék gyermekeiket az ismeretlenekkel történő kapcsolatfelvétel reális veszélyére!

Legyen ez az egyik, ha nem a legnyomósabb érv arra, hogy a szülők belemélyedjenek a számítógép, az Internet világába.

Ugyanígy a számítástechnikai ismereteket oktató, vagy más tanároknak is figyelmeztetniük kell a kiskorúakat erre!

Az Internet-rendőrség, ahogy teszi is, a chat-szobákat kell ellenőriznie, megpróbálva kiszűrni a több száz, vagy több ezer chatelőből a pedofil céllal odalátogatókat.

Rendkívül súlyos veszélyeket rejt a gyermekpornográfia megjelenése a világhálón. Megalázó, megszégyenítő és egészséges fejlődésükre rendkívül negatív hatással van, ha ezekkel a képekkel találkozik. Felnőttek perverz, beteges vágyainak kiszolgáltatott kiskorúakról készült képek kerülnek a bárki által elérhető hálózati oldalakra, szerverekre. E perverzióra sajnálatosan, üzlet épül (pénzért adhatók - vehetők, nézhetők a fényképek és a videófelvételek), sőt a szervezett bűnözés egyik jövedelemszerző tevékenysége.

A gyermekeket ábrázoló pornográf felvételekről az életkor, a készítés ideje, helye nem azonosítható, azok rossz minőségűek, eltorzítottak, hamisítványok (pl. felnőttkorúak arcát hamisítják). Mindezek a bűncselekmény bizonyítását megnehezítik.

A büntetőjog több magatartást minősít bűncselekménynek e körben (Btk. 204.§ (1) bekezdése).

- Megszerzés: a kép-, fényképfelvétel bármilyen magatartással, módon történő birtokbavételét jelenti. Akár a valóságos-, akár a virtuális térben ingyenesen-, vagy visszterhesen, lopással, rablással, csalással, cserével stb., bármilyen technikai megoldással.

  Számítógépes környezetben idetartozhat a hálózatról történő letöltés számítógépre-, vagy valamely adathordozóra, számítógépről számítógépre, adathordozóra történő másolás, adathordozóról adathordozóra történő másolás, memóriakártya beolvasása számítógépbe, nyomtatóba, adathordozó, memóriakártya birtokbavételével stb.
- Tartás: a kép- és fényképfelvétel tényleges birtoklását jelenti, készüljön az bármilyen technikai megoldással készült is, illetőleg tárolt, megjelenített.
- Készítés fogalmán az ilyen tárgyú video-, film- valamint fényképfelvételek bármilyen technikával történő előállítását, megjelenítését értjük. Mivel a grafikai ábrázolásra nem utal a törvényhely, így a kiskorúról készült pornográf grafika kívül reked a tényállás keretein.

- A forgalomba hozatal nemcsak e felvételek átadása, ajándékozása jelenti, hanem tág értelemben minden olyan magatartást, amellyel mások számára hozzáférhetővé teszi a felvételt. A kereskedés a forgalomba hozatalnál szélesebb körű tevékenység, mely magában foglalja az ilyen felvételek forgalmazásában való közreműködést (pl. szervezést, közvetítői tevékenységet, e felvételek továbbítását stb.).

  Büntetendő az ilyen cselekményekhez nyújtott anyagi eszközök szolgáltatása is, ez felöleli e tevékenységhez való pénz-, és technikai eszközök (pl. számítógép, bármilyen fényképezőgép, filmfelvevő, videófelvevő, vagy képolvasó) biztosítását az elkövető számára. (Delictum sui generis fizikai bűnsegédi alakzatot határoz meg (Btk. 204.§ (3) bekezdése).

  Még súlyosabban minősül, ha a sértettet szexuális tartalmú műsorba szerepelni hívják vagy szerepeltetik.

  További minősített esetek:

  - tizennyolcadik életévét be nem töltött személyt vagy személyeket pornográf felvételen való szereplésre felhív,

  - olyan pornográf műsoron vesz részt, amelyben tizennyolcadik életévét be nem töltött személy szerepel vagy ilyen személyek szerepelnek,

  - tizennyolcadik életévét be nem töltött személy vagy személyek pornográf műsorban való szerepeltetéséhez anyagi eszközöket szolgáltat.

  - Aki tizennegyedik életévét be nem töltött személyről vagy személyekről pornográf felvétel készítéséhez, forgalomba hozatalához vagy az azzal való kereskedelemhez szükséges vagy azt könnyítő feltételeket biztosítja, vétség miatt két évig terjedő szabadságvesztéssel büntetendő (Btk. 204.§ bekezdései).

Kiberterrorizmus

A valós térben vívott harcok mellett vagy helyett új „fegyver” jelenik meg, a terroristák a virtuális teret ugyanúgy használják vagy visszaélnek azokkal, mint más felhasználók.

A virtuális tér nem szűkül le a Surface-webre, sőt a rendkívül veszélyességű cselekmények a Dark-weben (Tor-szervereken) történnek (fegyver-, kábítószerüzletek, „bérgyilkos” bérlése, hamis okiratok kérése, készítése stb.). Sőt, a virtuális térben vívott harc lehetőségét már államok is használják.

A számítógépes hálózatok, és különösen az Internet, amely a hálózatok hálózata[71], a gyors, nagy tömegű adatátvitel adottsága, az anonimitás[72] relatív fenntarthatósága, a világháló viszonylagos ellenőrizhetetlensége, a véleménynyilvánítás és kommunikáció szabadsága és szabadossága. Mára az Internet logisztikai és operációs támogatására is alkalmas. A multimédiás eszközök sokrétűségét jelzik, pl. sokkoló lefejezések bemutatása.

A valóságos és a virtuális tér terrorcselekményei céljaiban és motívumaiban ugyanazok:

- Állami, politikai, etnikai, vallási stb. célok és egyes elszigetelt, szélsőséges csoportok céljai. A célpontok a támadások irányát és módszereit is jelzik.
- Az Internet, mint média különösen alkalmas a terrorszervezetek számára a figyelem felkeltésére, mivel több százmillió felhasználó böngész az Interneten.
- Valós térben a terrorcselekmények szimbolikus értelműek, bár az Interneten a célpontok leszűkülnek az ellenségnek tartott elektronikus adatfeldolgozó- és átviteli rendszerek ellen.
- Az Interneten keresztül vívott harcban a terrorszervezet neve általában nem, de a terrorista arca relatíve rejtve marad. Ténykedéséről, más azonosítójáról (álnév, monogram, trükkök, IP-szám stb.) tudomást szerezhet a világ, de beazonosításához más eszközökre van szükség.
- A HTML-oldalak széles technikai eszköztárát (színes videó- és képfelvételek, sztereóhangzásban, jelenetek újrajátszásával, lassításával, stb.) is felhasználják propagandájukra, a velük egyet nem értők megfélemlítésére, sokkolására.

---

[71] Az Internetet is a katonai kutatás hívta életre.1957-ben az akkori Szovjetunió az űrbe juttatott szputnyik fellövésével „üzent” az Egyesült Államoknak és szövetségeseinek, hogy nagy hatótávolságú rakétái immár bármit elérnek. Erre válaszol az USA a hadseregének vezénylési pontjait biztonsági okokból megtöbbszörözte és ezeket földalatti kábellel kötötte össze. Később erre a hálózatra csatlakoztak más katonai intézmények, egyetemek.

[72] lásd részletesebben: Dr. Jármy Tibor: Fantom.net – avagy anonimitás az Interneten Belügyi Szemle, 2002. 40. évf. 4. szám 151-159. o.

Internet, mint a propaganda eszköz a terroristák céljaihoz:

A Surface Web-felületen:

- Hírszolgálat: naprakész politikai, gazdasági és más információk.
- Propaganda: a többnyelvű, teljes körű multimédiás tájékoztatás nyújtása.
- A multimédiás lehetőségek teljes eszköztárának felhasználásával információkat, és nyilván dezinformációkat közölnek a szervezetükről, tényked̈ésükről, eszméikről (sikereiket, befolyásukat, taglétszámukat eltúlozzák, vesztéségüket, jelentéktelenségüket elbagatellizálják).
- Gyakorta nem terrorszervezet neve alatt, de lényegében annak a propagandáját folytató („fedő"), vagy azzal szimpatizáns weboldalak találhatók az Interneten.
- A propaganda eszköze a megfélemlítés is (akcióik-, túszok kivégzése, bosszú bemutatása) eszköze is lehet.
- Tagtoborzásra is alkalmasak a számítógépes hálózatok. Vonzó kivitelezésű, nem a terrorszervezet nevén megjelenő weboldalakon mélyen vallásos tartalmak vagy a fiatalokat megcélzó opciók igen gyakoriak, pl. kiterjedt a fájlcsere, vagy fájl-letöltés lehetősége korábban pl. palesztin weboldalak, ahol sokszor az egyesült államokbeli bemutató előtt lehetett elérni filmeket) - már csak az ellenségnek tartott országok „bosszantására".[73]

A számítógépes hálózatok alkalmas *terrortámadások végrehajtásához* (terheléses támadások, „férgek"-, logikai bombák-, trójai-, vírusprogramok az általuk ellenségnek tartott ország elektronikus adatfeldolgozó- és átviteli rendszerei ellen, illetőleg az ellenségnek tartott weboldalak defacelése propaganda és dezinformáció terjesztése céljából).

A gyors, anonim akár legális, akár illegális *pénzügyi műveletek, tranzakciók* akciók, terroristák finanszírozásához, a pénzmosás végrehajtásához. Online kaszinók, segélyszervezetek legálisan működnek az Interneten, ahová legálisan fizetnek be, ám onnan a pénz a terrorcsoportokhoz (vagy más szervezett bűnözői csoporthoz) megy. Kideríthetetlen és felbecsülhetetlen mennyi pénz mozog „feketén" a számítógépes hálózatokon, nem is csak a nyilvános web-felületen keresztül az elérhetetlen országokba, szigetekhez. Az Internet számtalan pontján ütközhetünk olyan oldalakba, ahová a belépés jelszó vagy más azonosítót igényel (tipikusan ilyenek a web-felületről is elérhető FTP-szerverek). Egyébként ezek az oldalak a search engine cache tárában sem érhetők el, így abszolút bennfentesség szükséges

[73] http://boingboing.net/2003/08/20/palestinian-p2p-netw.html [2016.09.30.]

az ilyen oldalakhoz. Egyébiránt a szakirodalom ezt az esetet „fordított pénzmosás”-nak nevezi.[74]

A hálózati kommunikáció lehetőséget nyújt az ellenségesnek tekintett számítógépes rendszerekben kezelt *adatok, információk kikémlelésére* is. Az adatok, felhasználók aktvitásai, a rendszer működése kikémlelésének egyik legújabb eszköze a Flame vagy Gauss malware-ek, amelyek tulajdonképpen egyesíti az eddig ismert és használatos spywarek „tudását”.

Az egymás közötti, és a kívülállókkal történő *kommunikáció* gyors és kódolt formában megvalósuló lebonyolításához az Internet ideális terep. A terrorszervezetekhez tartozók tipikusan Internet-kávézókban kommunikálnak egymással (akár azonos időben a világ különböző pontjain), vagy fogadják e-mailes üzeneteiket, továbbá ezek az anonim Internetes-helyek ideálisak a vírus-, továbbá más pusztító programok feltöltéséhez a világhálóra.

Az elektronikus levél, a chat, a fájlcsere, a telefon, a web- és FTP-oldalak, mint hirdetőtáblák mind-mind a terroristák szolgálatára állnak, mozgósíthatják az ún. alvó ügynököket, az akciók egyeztethetők stb. Várhatóan a tömeges látogatottsággal bíró chat-szobákban (sport, szex stb.) „találkoznak” a terroristák. A kétoldalú kommunikáció mellett titkos információk küldésére a weboldalak kiválóan alkalmasak. A szteganográfia szerepe felértékelődik. Egy-egy weboldalon titkos üzenet is elrejthető szöveg-, kép-, hang-, videófájlban. Ma egy a biztos, hogy nem biztos, hogy az a tartalom van, amit látunk egy weboldalon. Ugyanis ma már szinte „gyerekcsíny” üzeneteket egy ártatlan képfájlban, szövegfájlban, egy szövegben más tartalmú kódolt üzenetet elrejteni.

A terrorcselekmények elkövetését segítik azok az oldalak, amelyek *pusztító fegyverek, bombák* házilagos, egyszerű elkészítéséhez nyújtanak tanácsot. Elektronikus hirdetőtáblákon, chat-szobákban lelhetők fel tanácsok, illetve információk, „jó tanácsok” ahhoz, hogy melyik weboldalon kaphatunk részletes leírást. Korábban a szaúd-arábiai Muaskar el Battar (Katonai tábor) újság ismertetőit töltötték fel angol arab nyelven, ábrákkal illusztrálva a bomba-, és fegyverkészítés és használatuk fortélyait. Az újságot a helyi hatóságok felszámolták, de a feltöltött oldalak még elérhetők.[75]

---

[74] Gál István László: A pénzmosás és a terrorizmus finanszírozása. Emlékkönyv Irk Albert egyetemi tanár születésének 120. évfordulójára.
(Szerkesztette: Dr. Korinek László – Dr. Kőhalmi László – Dr. Herke Csongor.) PTE ÁJK Pécs, 2004. 39. o.

[75] http://datadump.galeropia.org/Al%20Qaida/al-battar_training_camp_7.pdf
http://www.intelcenter.com/Qaeda-Targeting-Guidance-v1-0.pdf [2016.12.30.]

Háború a kibertérben

A kibertérben nemcsak magányos bűnözők, szervezett bűnözői csoportok, ezen belül terroristák, hanem államok is vívják háborúikat. A kibertérben a hadviselés megelőzi, azzal egyidőben zajlik vagy netán követik a valós térben vívott támadásokat.

Ahogy fentebb többször utaltunk rá, a számítógépes hálózatokon is elkövethetők olyan támadások, amelyek a *valós térben is* megvalósíthatók. Így háborúk esetében a célpont felderítése, a kémkedés, a propaganda – hírverés az ellenség irányában (információk – dezinformációk terjesztése), az ellenség/ellenzék hangjának elfojtása, az ellenség kommunikációjának kiiktatása és egyéb cselekmények- természetesen más eszközökkel, más technikai feltételekkel, más módon és élő erővel.[76]

Ugyanakkor, akár a kibertérben a fentiekkel paralel megvalósíthatók olyan cselekmények, amelyek *kibertérhez, számítástechnikai eszközökhöz kötöttek*, azaz e technikai feltételek hiányában nem hajthatók végre. E körben említhetők a hacking (elektronikus betörés), malware-ek (malicious software – rosszindulatú szoftverek) megosztása, célzott feltöltése, terheléses támadás végrehajtása, programok manipulálása, szabotálása, e technika teremtette kommunikáció (e-mail, videó-kommunikáció) kifürkészése, lehetetlenné tétele, defacing és más cselekmények.

A kibertérben valamennyi támadás-típust általában *bármely felhasználó ellen és többféle célból* el lehet követni. Potenciális áldozat lehet minden olyan intézmény, szervezet, amelynek tevékenysége döntő mértékben függ a számítógépes hálózatok és adatbázisok működőképességétől.[77] Azonban egyes támadás-típusok jellemzően egy-egy felhasználói kör ellen irányul, így például egy terheléses támadást az átlag-felhasználónak általában nem kell elszenvednie, de kritikus infrastruktúrák vagy más politikai, gazdasági, katonai célpontok már veszélyeztettek lehetnek, hasonlóan a Stuxnet, amely egy meghatározott művelet (urándúsítás) szabotálására íródott, és amely hosszas előkészület és alapos célfelderítés előzött meg. De mivel a Stuxnet, és klónja (?),[78] a DuQu már „kinn van a szabadpiacon", így az a technika-technológia, ötlet, amely egyetlen célra, egyetlen művelet megbénítására szolgál, felhasználható a katonai ellenség, a gazdasági és a politikai ellenfelekkel szemben is.

---

[76] Will Gragido – John Pirc: Cybercrime and Espionage. Elsevier Amsterdam-Heidelberg-London. 2011.3-5. o.
M. Chawki – A. Darwish – M.A. Khan – S. Tyagi: Cybercrime, Digital Forensics and Jurisdiction. Springer International Publishing, Switzerland, 2015. 7-8. o.
Nagy Zoltán András: Bűncselekmények számítógépes környezetben. Budapest, Ad-Librum Kiadó, 2009. 189-191. o.

[77] NBH Évkönyv 2006. Budapest, 2007. 58. o.

[78] Bár ma még nem (köz)ismert, nincs arról információ, hogy melyik malware volt előbb, melyiket fejlesztették ki a másikból. Egyáltalán van-e közük egymáshoz.

A Flame, a Gauss és más szuper kémprogramok pedig azt jelzik, hogy már nemcsak egy-egy alkalmazásra, műveletre, személyre stb. vonatkozó információgyűjtésre írt programok léteznek, hanem ennél összetettebb, több funkciót tudó programok is, amely minden olyan információt összegyűjthet, ami az adatbázisról, az adatkezelés menetéről, a felhasználókról nyújt egyszerre információkat.

A kibertérbe lépéssel a hadviselés, és a terror is átlép egy határt, - nemcsak a valóságban, hiszen a hadviselő felek a velük hadban álló ország területét sértik meg, de - jelképesen is, mivel a hadviselés egy új dimenzióját jelentik, amelyek a propagandától a pusztításig terjedhetnek, és amelyek akár önállóan, akár a valós térbeli harci tevékenységekkel egy időben, azokat megelőzve, vagy követve azokat.

A számítástechnika tehát hadviselő felek számára egyfelől e cselekmények végrehajtásához új eszközt és/vagy helyszínt nyújt, másfelől új veszélyforrást is teremtett, mert védelmezni kell a számítógépes hálózatokat, az azokat érő támadásokat elhárítani, és ha szükséges újraépíteni, újratelepíteni kell.

A virtuális térben végrehajtott támadások lehetőségével a – fentebb idézett - clausewitzi háború fogalma is eltűnik, a háború fogalmát is újra kell gondolni.

A hadviselés során alkalmazható információs műveletek elemei:

- lélektani műveletek,
- katonai megtévesztés,
- műveleti biztonság,
- fizikai megsemmisítés,
- elektronikus hadviselés,
- számítógép-hálózati műveletek.[79]

Ez utóbbi műveletek közül a számítógép – hálózati támadásokat emeljük ki, bár hálózati támadás lehet a web-tartalmak defacelése, amelynek célja a köznyugalom megzavarása, lakosság megtévesztő tájékoztatásával köznyugalom megzavarása (a harctéri eseményekről, kül- és belpolitikai történésekről), illetőleg cél lehet a megfélemlítés is. Továbbá terheléses támadás vagy egy-egy malware alkalmas a megtámadott számítógép működésének szabotálására, megbénítására

A támadások végrehajtói – szemben egy átlagos kiberbűncselekménnyel – felsőfokú képzésben részt vett, felkészült profik, akiknek ez a terület a hivatása. Ma az Egyesült

[79] Haig - Kovács – Ványa: Az elektronikus hadviselés a SIGINT és cyberhadviselés kapcsolata. Felderítő Szemle. Budapest, MK KFH 2011. 1-2. szám 185. o.

Államoknak, Izraelnek és más nyugat-európai országnak kiberhadserege van, amelyet kiegészíthetnek önkéntesek, akik magukkal hozzák ismeretüket, netán botnetjeiket a támadások végrehajtásához.

2007 áprilisában zajlott le az államok közötti az első kiberháborúnak nevezhető (WW1 - Web War 1) kölcsönös támadás-sorozat.[80] Az orosz-észt konfliktus okául (ürügyül?) a szovjet háborús emlékművek áprilisban történő eltávolítása és a kettős (köztük orosz) állampolgárok választásból történő kizárása szolgált. Oroszországban az észt politikai döntések ellen utcai tiltakozások és kibertérben háború zajlott. Orosz hackerek Internetes fórumokon, blogokban, bulletin boards-kon botneteket szerveztek, majd ezeket egyeztetve egy időben hajtottak végre támadásokat észt miniszterelnök, miniszterek, kormányzati szerverek ellen. A támadások néhány bank pénzügyi tevékenységét sikerrel zavarták meg. A terheléses támadások mindennap zajlottak. A kiberháború Győzelem Napján csúcsosodott ki, amikor is 95 Mbps adatforgalmat regisztráltak. Naivitás volna azt hinni, hogy mindez orosz patrióták, nacionalisták hazafias akciója lett volna. 2008-ban a NATO a Cooperative Cyber Defence Center of Excellence nevű „hivatalt" hozott létre az észt fővárosban, amely a kiberháború körülményeit vizsgálta.

Ugyanebben az évben izraeli ügynökök vezető szír politikusok számítógépére *spyware-(eke)t* telepítettek egy londoni szállodában, amikor a politikusok laptopjaikat a szobájukban hagyva eltávoztak. A cél az volt, hogy a Szíriában titokban, észak-koreai segítséggel épülő al-kibari atomerőműről minden információt begyűjthessenek. Ezen információk alapján és az USA légi támogatásával bombázták le az Szíria északkeleti részén épülő al-kibari atomerőművet szeptember 6-án.[81]

A 2008-ban vívott, 5 napos orosz – grúz háború előzménye az április elején lezajlott NATO-csúcs, amelyen a tagállamok közötti vita elodázta Ukrajna és Grúzia Szövetség Tagsági Akciótervéhez (Membership Action Plan – MAP) történő csatlakozást. Ez a határozott döntésképtelenség azonban Oroszországot arra bátorította, hogy a két ex-szovjet ország NATO-hoz való közeledését (melynek vége a csatlakozás lett volna) megakadályozza, ellehetetlenítse. Oroszország terveit segítette az, hogy a grúz kormány folyamatosan nyomást igyekezett gyakorolni Dél-Oszétiában és Abháziában, és már csak a háború időpontja volt kétséges. Oroszország áprilisban, két ízben is felderítő repüléseket végeztek Abházia légterében, a gépeket a grúz légierő ártalmatlanított. Majd májusban 400 katonát küldött

[80]Clay Wilson: Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress. CRS Reports for Congress, updated January, 2008. Washington, 7-9. o.

[81]http://www.spiegel.de/international/world/the-story-of-operation-orchard-how-israel-destroyed-syria-s-al-kibar-nuclear-reactor-a-658663.html

Abháziába vasútépítés ürügyével. Még a valós térben lezajlott orosz provokációk sorát gyarapította, a valóstérbeli konfliktus kirobbanása előtt július végén terheléses támadással megbénította Miheil Szaakasvili grúz elnök honlapját, a weboldal több napig elérhetetlen volt. Majd a valós térben kirobbant háborúval egy időben a kibertérben az Észtország elleni óriási adatözönnel árasztották el az oroszok a grúz elnök, a minisztériumok, hírszolgáltatók weboldalait. A források szerint az adatáramlás a 800 Mbps-t is elérte. Néhány ellencsapás detektálható volt a grúzok, illetőleg a Grúziával szimpatizálók részéről. Több grúz weboldal „költözött" más államok szerveire, így például az elnök weboldalát pl. az USA-ba tükrözték, de lengyelországi szerverekről is került hivatalos grúz tartalom Internetre. Ez volt az első alkalom, hogy a valós térbeli hadműveletekkel egy időben, a kibertérben is támadás zajlott le. Ugyanakkor mindenképp figyelmet érdemel az, hogy az orosz támadásokhoz török telefonhálózatot használtak.

A kéretlen kereskedelmi küldemények (spam-ek)

Az Interneten zajló szabad kommunikáció egyik eszköze, megvalósulási módja az elektronikus levél (e-mail). Bárkinek írhatunk levelet, küldhetünk mellékleteként - egyelőre még nem túl nagy méretben (tipikusan 5 Mb.-nyi) - szöveges, képi, zenei és egyéb tartalmú fájlokat tömörítetten, vagy tömörítetlenül. A levelezőprogramok zöme biztosítja azt, hogy egy-egy levelet meghatározatlan számú felhasználó megkaphasson, már akinek az e-mail címe ismert a feladó számára.

A *spam* elektronikus levél csatolt fájljaként érkező nem kívánt kereskedelmi tájékoztatás (pl. reklám, kérdőíves felmérés). A szó a nálunk is ismert szatirikus „Monty Python's Flying Circus" brit tv-sorozat (1969-74) egyik epizódjában hangzott el először. A „Vikingek jelenet"-ben, az étteremben betérő vikingek ételt rendelnek, mire a pincér, vagy a választék-hiányt elkendőzve, vagy a brit éttermek egyoldalú választékára utalva a „spic pork and ham" (fűszeres sertéshús, és sonka) szavakat ismételgette többször, más-más sorrendben, amiből a vikingek a „spam" szót értették ki. Ez a poén képletesen utal a kéretlen levél tartalmára, azaz „tetszik, nem tetszik, ezt kapjuk". Korábban kissé nehézkes elnevezéssel bírt a spam. Unsolicited Commercial Email (UCE)-nek Unsolicited Bulk Email (UBE)-nek nevezték.

Akárcsak a valóságos térben a postaládákat elhalmozó reklámok, reklámújságok, úgy virtuális érben az elektronikus postaládát telíti ez az „elektronikus szemét".

A spam-ek okozta *problémák:*
E-mail címünket olyan személy használja, akinek nem bocsátottuk rendelkezésre, azaz ebben az esetben visszaélnek e-mail címünkkel.
Zaklatja a felhasználót a számára érdektelen levél.
A szex-, kábítószert népszerűsítő és egyéb oldalakra hívó reklám a kiskorú felhasználó számára jelent veszélyt.
Ahogy a valóságos térben a postaládát eltömítik a reklámújságok, kiadványok, úgy a levelezőprogramokat is telítik a spam-ek. A cégek, magánfelhasználók nem olcsó számítógép-idejéből vesz el a levelek betöltése, törlése. A cégek esetében a rendszergazdának ad mindennap munkát a spam-ek törlése a cég levelezőrendszeréből.
A nagy adatmennyiség egyben lassítja az Internetet.

A spam-ellenes programok beszerzése, telepítése, karbantartása (frissítése) költséges, időigényes.

A spam-ek küldői e-mail címeinket legális és illegális formában szerezhetik meg.

Az e-mail címek legális forrásai a valóságos térben a céges telefonkönyvek, szakmai és egyéb kiadványok, névjegykártyák stb. ahol az adott névhez tartozó e-mail címeket közlik.

A virtuális térben a hírcsoportok (news group), elektronikus hirdető táblák (bulletin board), fórum-rovatok, levelezési listák archívumaiban, blog-bejegyzésekben, saját weboldalon olvasható e-mail cím.

Sajnos, a felhasználók is gyakran szolgáltatják ki feleslegesen e-mail címüket.

Különösen:

- ha szerencsejátékban azonosíthatatlan weboldalon nyeréssel kecsegtetnek,
- ha mindenféle hihetetlen árral kecsegtető vásárlási-, nyeremény- akcióra jelentkezünk, kérdőíveket töltünk ki,
- levelezőlistákra iratkozunk fel, apróhirdetésekre jelentkezünk e-mail címünkkel stb.

Technikai védelem lehetőségei a spam-ekkel szemben:

- spamszűrő programok alkalmazása,
- a levelező programunkban letilthatunk bizonyos tartalmú jelzéssel érkező levelet (pl. make money (pénzkereset) fast money (gyors meggazdagodás), sex, porno, xxx (a pornográf tartalom általános jelölése), vagy – ha egy címről érkeztek a spamek – akkor letilthatunk címeket is, azaz az onnan érkező leveleket nem veszi át a program.

A spamekkel szembeni *jogi védelem* eszköztára:

A nem kívánt kereskedelmi tájékoztatás visszaszorításához (is) nyújt elvi útmutatást az EK 2000/31. sz. Irányelve „A belső piacon az információs társadalommal összefüggő szolgáltatások, különösen az elektronikus kereskedelem, egyes jogi vonatkozásairól”.

„Azokban a tagállamokban, amelyek engedélyezik a nem kívánt kereskedelmi tájékoztatás elektronikus levélben történő küldését, ösztönözni kell és meg kell könnyíteni a szakma általi, a megfelelő szűrésre irányuló kezdeményezéseket; ezen túlmenően szükséges, hogy a nem kívánt reklámok minden esetben ilyenként egyértelműen azonosíthatóak legyenek az átláthatóság javítása és az említett szakmai kezdeményezések érvényesítésének megkönnyítése

érdekében; az elektronikus levélben küldött nem kívánt kereskedelmi tájékoztatás a címzett számára nem eredményezhet további kommunikációs költséget." (30. pont)[82]

A magyar szabályozás szigorúan követi az EK Irányelv normatíváit, amikor 2001. évi CVIII. törvény „Az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről"
A törvény 14.§(1) bekezdésében rögzíti, hogy az információs társadalommal összefüggő szolgáltatás felhasználásával küldött reklámnak világosan, és *egyértelműen azonosíthatónak kell lennie*, amint az hozzáférhetővé válik az igénybe vevő számára.
Kizárólag az igénybe vevő egyértelmű, előzetes hozzájárulásával küldhető elektronikus úton, levelezés során reklám.
E rendelkezés ellenőrzésére a 16. § (5) bekezdése a Hírközlési Felügyeletet jogosítja fel, hogy A (6) bekezdés alapján 500.000 Ft-ig terjedő bírság szabható ki.

A 2002/58 EK. „Az adatvédelemről szóló" Irányelve már határozottabban fogalmazza meg a felhasználók védelmének szükségességét, amikor kimondja, hogy „biztosítani kell az előfizetők magánéletének a védelmét a kéretlen, közvetlen üzletszerzés célját szolgáló, különösen automatizált hívóberendezés, telefax valamint elektronikus levél – beleértve a rövid szöveges üzenetet – útján továbbított közleményekkel szemben."[83]

[82] http://eur-lex.europa.eu/LexUriServ/site/hu/dd/13/25/32000L0031HU.pdf [2017.03.31.]
[83] http://www.hte.hu/cd_rom/magyarweb_eu.html [2017.03.31.]

Minden számítógép rendelkezik egy ún. TCP/IP-vel (Transmission Control Protocol/Internet Protocol). Az Internethez, más hálózathoz kapcsolt minden egyes számítógépnek (host) egyedi azonosítója van, az ún. IP szám. Az IP szám 4 darab pontokkal elválasztott 8 bites szám. Minden byte értéke 0 és 255 között lehet. Például: 195.199.100.65. A világon nincs két számítógép, amelyeknek azonos IP-számuk van.

Egyszerűsítve a folyamatot, amikor a felhasználó (kliens) összekapcsolódik egy szerverrel, a szerver azonosítja magát a kliens felé, és fordítva a kliens is azonosítja magát a szerver felé. Ha az azonosítások helyesek, akkor kérhető művelet a szervertől. A szerver, amelyen keresztül kapcsolódik a hálózathoz, rögzíti (naplózza) azt, hogy melyik számítógépen (azaz az IP-számám), melyik felhasználó, mikor lépett be, ott meddig tartózkodott, az Interneten milyen weboldalt látogatott, mekkora és milyen adatállományt töltött le, milyen-e-mail címre írt, és milyen e-mail címről kapott levelet stb. Figyelése, rögzítése (naplózása) a letöltött tartalomnak technikailag megoldható. Ezek az információk a bűncselekmény elkövetésének bizonyítását, és elkövetőjének azonosítását megkönnyítik. Bár a profi elkövetők (pl. hamis felhasználó névvel, és mellé hamis IP szám generálásával) megpróbálnak rejtve maradni. A nemtelen célokat követő felhasználók nagy előszeretettel használják az anonim public proxy szervereket, amelyek „mögé" elbújhatnak. Ezek az a szerverek olyan országokban működnek, amelyek a nemzetközi bűnüldözésben – diplomatikusan szólva – nem mindig partnerek. Az *anonim proxy*-nál egyel biztonságosabb az úgynevezett *distorting proxy*. Ez a fajta proxy nem csak, hogy nem adja tovább az IP címet, de szándékosan hamis IP-t szolgáltat. A „legbiztonságosabbak" a *high anonimity proxy*-k. Ezek kifelé nem is proxynak mutatják magukat, a céljuk kifejezetten az felhasználó IP címének elrejtése. A terroristacsoportok saját biztonságuk miatt, valamint a terrorelhárítók működésének megnehezítése céljából „utazó IP-címet" használnak, amelyek a szerverek lokalizálását, és azok gyors légi, vagy szárazföldi beavatkozással történő felszámolását lehetetlenítsék.

Az „utazó IP-címet" meg kell különböztetnünk a „dinamikus IP-címtől", amely – leegyszerűsítve – az Internet - szolgáltató, minden egyes csatlakozás során kioszt a felhasználónak egy új IP címet. Bár sok esetben ugyanazt. A nyomozati munkát a dinamikus IP-cím nem nehezíti, mivel a szolgáltató naplózza a kiosztott IP-címhez tartozó felhasználót.

A nyomozás során viszont gyakori nehézség az, hogy bár az IP szám alapján az előfizető neve, lakcíme – pillanatok alatt – tisztázható, ám az még mindig kérdés, hogy ki is használta a számítógépet (és az Internetet) az adott időpontban.

Ugyanakkor azonosítási problémát jelent az Internetre egy routeren keresztüli kapcsolódó számítógép azonosítása. Különösen a publikus, nyílt wifi hálózat esetében, amelyhez bárki, azonosítás nélkül csatlakozhat.

Ilyen esetekben a notebookot, tabletet használó személy azonosításához jó szolgálatot tehetnek a helyiségben kihelyezett kamerák, amelyek rögzítik a tett elkövetése idején a helyiségben számítógépet használók személyét.

Akár a vezetékes-, akár privát wifi hálózat használata esetén a TC/IP szám alapján a felhasználó, mint előfizető neve, címe pillanatokon belül kideríthető, ám mindezen információk csak valószínűsítik azt, hogy ki használta az adott időpontban a számítógépet. Ennek kiderítésére a „hagyományos" valós térbeli nyomozati megoldásokra kell támaszkodni, ideértve szöveges tartalom feltöltése esetén a grafológiát.

A kiberelkövetők, mivel az Internet az életterük, más aktivitásban is jelen vannak. Lehetséges, hogy kétségbevonhatatlan tudásuk, közlési vágyuk, hencegésük, túlzott magabiztosságuk miatt más fórumokon (chat szobákban, twitteren, közösségi oldalakon) nyomokat hagynak maguk után (azonos szövegjegyek, hasonlatosságot felmutató nick name-ek, felhasználói nevek, nem álcázott IP-címek stb.)

Elektronikus adatok, mint bizonyítékok a büntetőeljárásban

A számítógépes környezetben elkövetett bűncselekmények, nemcsak az anyagi büntetőjog számára jelentettek új kihívást, hanem a büntető- eljárásjog és a kriminalisztika számára is. A számítógépes adatok "testetlensége", "láthatatlansága", - mint ezen bűncselekmények egyik jellemzője - az anyagi büntetőjogot új tényállások megalkotására ösztönözték.

Az elektronikus adatok, mint elektronikus impulzusok, mint bizonyítékok beszerzéséhez, vizsgálatához nem minden esetben nyújtanak kielégítő megoldást a tradicionális eljárásjogi szabályok. Ne feledjük, hogy ezen "testetlen", "láthatatlan" elektronikus adatok megjelenítéséhez technikai eszközökre van szükség.

A nyomozati cselekmények a következő elektronikus adatok megszerzésére irányulnak:

A. Elektronikus dokumentumok

Az elektronikus impulzusok jelölhetnek szöveg-, kép-, audió- és videófájlokat. Tartalmuk szerint rendkívül sokrétűek lehetnek, funkciójuk szerteágazó. Jelölhetnek vagyoni értéket, személyes adatokat, vállalati nyilvántartásokat, szerzői alkotásokat, különböző titkokat (pl. állam-, szolgálati-, bank-, üzleti-, adó-) más releváns tartalmat stb.

B. Elektronikus nyomok

A számítástechnikai eszközökön olyan – tipikusan időlegesen – rögzült adatok vannak, amelyek a számítástechnikai eszköz működése közben keletkeztek. Egy átlagos felhasználó nem is szerez erről tudomást. Ezek az „elektronikus nyomok" a számítástechnikai rendszer működéséhez elengedhetetlenül szükségesek.

Több program működése közben ideiglenes állományokat hoz létre a számítógép háttér tárolóján. Ezeket az adatokat a program befejezését követően törli. De a törölt adatok – ha azokat nem írták felül újabb adatokkal – visszaállítható, elolvasható egy másik egyszerű programmal.

A visszaállított adatokból szinte minden ismeret megszerezhető, megismerhető, amik a nyomozáshoz szükséges.

Ilyen elektronikus nyomok nemcsak a számítógép háttértárolóin vannak, hanem más számítástechnikai eszközön, perifériákon. Például megismerhető, hogy egy nyomtatóval készített hamisítvány hány példányban készült. A festékpatron használtsága elárulja a kinyomtatott példányok mennyiségét. Ugyanígy a scanner is visel árulkodó jelet.

C. Napló- és regisztrációs adatok

A számítógépes hálózatba történő bejelentkezést a számítógépen levő hálózati programok biztosítják.

Ahhoz, hogy az Interneten levő sokféle fajtájú, és teljesítményű számítógép kommunikálni tudjon egymással, kell egy közös szabvány. Ezen keresztül az cserélik számítógépek az elektronikus adatokat.

Bár több ilyen szabvány is van, a legelterjedtebb az ún. TCP/IP protokoll (Transmission Control Protocol over Internet Protocol). Leegyszerűsítve a következőképpen működik: Minden az Interneten megjelenő számítógépnek van egy egyedi azonosítója, ez az ún. IP szám. Az adatforgalom kis csomagokra bontva történik. A csomagok mindegyikére sok más adat mellett rá van írva a küldő és a címzett IP száma. A csomagokat egyik gép továbbítja a másiknak, míg el nem jutnak a címzetthez. A címzett számítógépe a megkapott csomagokat sorba rendezi, kibontja, tartalmukat értelmezi. A rendszer előnye, hogy teljesen eltérő nagyságú, fajtájú számítógépek is képesek kommunikálni egymással, és az őket összekötő hálózati útvonal valamint annak technikai kivitelezése is tetszőleges lehet (telefonvonal, üvegszál, mikrohullám, műhold), sőt meg is változhat, akár a kommunikáció közben.

Naplózott fájlok lehetnek:

- a különböző szervereken történő fel- és letöltések,
- a ki- és bejövő elektronikus levelek,
- a postafiók elérését regisztráló adatállományok,
- hálózat-biztonsági programok,
- tűzfalak stb.

Az elektronikus dokumentumok minden esetben egy adathordozón kerülnek rögzítésre. Ez lehet a számítógép háttértára, vagy hordozható adattároló (pl. floppy-, CD-, DVD-lemez, USB RAM, memória kártya, külső tároló).

Ezek az eszközök az elektronikus dokumentumokat szabványos formátumban tárolják. Megőrzik a rajta levő adatokat, akkor is, ha a számítógépből kimásolják azokat. Az adattárolók egy része újraírható (felülírható) pl. az egyre ritkább floppy-lemez, vagy a CD-RW-, DVD-RW, winchester, USB RAM, külső tároló). Azaz a rajta levő adatállományok gyorsan változtathatók, törölhetők. Az adattárolók másik részét olyan eszközök alkotják, amelyek nem változtathatók (pl. CD-R, DVD-R, DVD+R).

A CD-, és DVD-lemezek, de különösen az USB RAM kis mérete miatt – pl. egy gyufásdobozban is - könnyen elrejthetők, megtalálásuk nehézzé válhat.

Az elektronikus dokumentumok, és nyomok – jellemzően – a számítógép winchesterén keletkeznek.

Szintén a számítógép winchesterén keletkeznek a naplófájlok is.

A naplófájlokat többféleképpen lehet csoportosítani. Mi most azt a tipizálást választjuk, amely a büntetőeljárás célját szolgálja.

1. Azok az elektronikus adatok, amelyek a számítógép-, vagy számítógéprendszer működéséről szolgálnak információt, vagy a rendszer védelme érdekében keletkeznek stb.
2. Azok az elektronikus adatok, amelyeket amiatt naplózzák, mert törvény, más jogszabály írja elő. (Pl. Internet-, vagy távközlési szolgáltatók esetében.)

Ha a nyomozó hatóság észleli, hogy valamelyik számítógépes hálózaton, FTP-szerveren, weboldalon stb. jogsértés történt, akkor megkeresi a szolgáltatót.

A megkeresés célja az, hogy a regisztrációs és napló adatokból az elkövetőre vonatkozó információkat beszerezze. A regisztrációs adatokból kiderül, hogy a gyanúsított milyen információkat adott meg regisztráció során (pl. név, lakcím, telefonszám, más elérhetőség stb.).

A napló adatokból pedig megismerhető az, hogy az adott felhasználó:
mikor, melyik szerverrel létesített kapcsolatot. Melyik weboldalt látogatta, onnan milyen fájlt (szöveg-, kép-, audió-, vagy videófájlt), milyen méretben töltött fel, vagy töltött le. Hova, milyen e-mail címre írt levelet, mikor, milyen e-mail címről kapott levelet, az e-mail címet rejtő nevet, az e-mail cím IP száma stb.
A szolgáltatók esetében a magyar Büntetőeljárási törvény megőrzési kötelezettséget is előír. Elektronikus levelet is biztosítania kell. Irreleváns az, hogy az e-mail eljutott-e a címzetthez, vagy sem.
Megkeresés esetében a kódolt, rejtjelezett, más módon titkosított adatokat értelmezhető formában kell átadni a nyomozó hatóságnak.
Az adatszolgáltatást minimum 8, maximum 30 napon belül kell teljesíteni. Vagy közölni kell, hogy milyen törvényi rendelkezés alapján nem tehet eleget a megkeresésnek.
Az inkriminált adatok történhetnek az adathordozó lefoglalásával, a winchester kiszerelésével és lefoglalásával, a winchesteren tárolt adatok egyszer írható adathordozóra történő kimásolásával, csekély adatmennyiség esetében - pl. egy könyvtárállomány esetében – a monitoron megjelenítve, annak lefényképezésével.

A számítógépes nyomozás hatékony megvalósulásához szükség van jól felkészült (és megfizetett) szakembereknek. Felkészítésükön nem szabad takarékoskodni. A bűnözők előtt kell járni, nem mögöttük.

Az új büntetőeljárásról szóló törvény már külön nevesíti az elektronikus adatot is a bizonyítási eszközöknél. 205. § (1)-(2) értelmében 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. Ahol a törvény tárgyi bizonyítási eszközt említ, azon a törvény eltérő rendelkezése hiányában az elektronikus adatot is érteni kell. Az elfogadott törvény Indoklása szerint korábban az egyes büntetőeljárási cselekmények szabályozásában az elektronikus adat kategóriája nem minden esetben volt kezelhető a fizikai dolgok analógiájára. Azokban az esetekben, amikor az elektronikus adatokra és a tárgyi bizonyítási eszközökre közös rendelkezések alkothatók, ott a törvény eltérő rendelkezés hiányában az elektronikus adatot is tárgyi bizonyítási eszközként kezeli. A kényszerintézkedések között továbbra is szerepel az elektronikus adat ideiglenes hozzáférhetetlenné tétele, amely az elektronikus hírközlő hálózat útján közzétett adat feletti rendelkezési jog ideiglenes korlátozása és az adathoz való hozzáférés ideiglenes

megakadályozását jelenti, amit kizárólag bíróság rendelhet el. Az elektronikus adat ideiglenes hozzáférhetetlenné tételét akkor lehet elrendelni, ha az eljárás olyan közvádra üldözendő bűncselekmény miatt folyik, amellyel kapcsolatban elektronikus adat végleges hozzáférhetetlenné tételének van helye, és az a bűncselekmény megszakítása érdekében szükséges. Az elektronikus adat ideiglenes hozzáférhetetlenné tétele elrendelhető: az elektronikus adat ideiglenes eltávolításával, vagy az elektronikus adathoz való hozzáférés ideiglenes megakadályozásával, előbbi eredménytelensége esetén (335.§ (1)-(4)). Továbbá kiegészül egy új rendelkezéssel a felhívás az elektronikus adat önkéntes eltávolítására, amit az ügyészség és a nyomozó hatóság kezdeményezhet, ha az a büntetőeljárás érdekeit nem sérti, azonban ennek a teljesítése nem kötelező erejű (338.§). A lefoglalás szabályai között külön szerepel az elektronikus adat lefoglalására és a megőrzésére kötelezésre vonatkozó rendelkezések (315-318.§). Az elektronikus adat ideiglenes eltávolítása és az elektronikus adat megőrzésére kötelezés együttesen is elrendelhető.

A Btk. az elektronikus adat végleges hozzáférhetetlenné tételét mint intézkedést szabályozza a 77.§ (1)-(2) bekezdésében: hozzáférhetetlenné kell tenni azt az elektronikus hírközlő hálózaton közzétett adatot,

a) amelynek hozzáférhetővé tétele vagy közzététele bűncselekményt valósít meg,

b) amelyet a bűncselekmény elkövetéséhez eszközül használtak, vagy

c) amely bűncselekmény elkövetése útján jött létre.

Az elektronikus adat végleges hozzáférhetetlenné tételét akkor is el kell rendelni, ha az elkövető gyermekkor, kóros elmeállapot, vagy törvényben meghatározott büntethetőséget megszüntető ok miatt nem büntethető, illetve ha az elkövetőt megrovásban részesítették.

Nemzetközi dokumentumok és szervezetek a számítástechnikai bűnözés elleni küzdelemben

A hatékony fellépés ezzel a bűncselekmény típussal szemben megköveteli a nemzetközi bűnügyi együttműködést, illetve a büntetőjogszabályoknak a nemzetközi összehangolását, a szükséges minimumszabályoknak a megalkotását. A következőkben a nemzetközi szabályozást és szervezetek mutatjuk be, amelyek a számítástechnikai bűnözéssel szembeni küzdelmet erősítik. Az információs rendszerek felhasználásával elkövetett bűncselekmények száma is fokozatosan növekszik évről évre, és emiatt különösen fontos, hogy a jogalkotók is gyors ütemben tudjanak válaszolni ezekre a változásokra.

OECD jelentés

Az első fontos nemzetközi jogi dokumentum a *Gazdasági Együttműködési és Fejlesztési Szervezet (OECD)* által 1986-ban kibocsátott jelentése volt, amelyben iránymutatást kívántak adni a számítógépes környezetben elkövetett bűncselekmények megismeréséhez és a kodifikáció elősegítése volt a cél. A büntetendő cselekményeket a következőképpen rendszerezte a számítógépes csalás nélkül:

a. számítógépes adatok és/vagy programok bevitele, módosítása, törlése vagy elrejtése jogtalan vagyoni eszközök vagy más értékek megszerzése céljából;
b. számítógépes adatok és/vagy programok bevitele, módosítása, törlése vagy elrejtése hamisítás céljából;
c. számítógépes adatok és/vagy programok bevitel, módosítása, törlése vagy elrejtése vagy a számítógépbe történő bármely más beavatkozás abból a célból, hogy a számítógépes vagy telekommunikációs rendszerek funkcióinak megakadályozása céljából;
d. a védett számítógépes programok tulajdonosai exkluzív jogainak megsértése a program jogosulatlan hasznosítása vagy forgalomba hozatala révén;
e. a számítógépes vagy telekommunikációs rendszerbe az arra jogosult engedélye nélkül vagy a biztonsági intézkedések megsértésével vagy más tisztességtelen vagy bűnös szándékkal történő belépés vagy annak lehallgatása.

Az Európai Tanács 9. (89.) és 95. (13.) számú ajánlása

Az első uniós dokumentum *az Európai Tanács (a továbbiakban: ET) 9 (89). számú ajánlása (Computer-Related Crime),* amely tartalmaz egy minimum listát. Ez a lista

iránymutatásul szolgál a tagállamok jogalkotói számára, amennyiben ilyen típusú bűncselekmény esetében új jogszabályokat hoznak, vagy a régiek kerülnek átalakításra, akkor abban az esetben kötelezve vannak arra, hogy az ajánlással összhangban járjanak el.

A minimumlista a következőket tartalmazza:

- a számítógépes csalás,
- a számítógépes hamisítás,
- a számítógépes adatokban és programokban történő károkozás,
- a számítógépes szabotázs,
- a jogellenes behatolás: a számítógépes rendszerbe vagy hálózatba történő jogosulatlan bejutás a biztonsági intézkedések megsértése révén,
- a jogellenes titokszerzés,
- védett számítógépes programok jogellenes másolása.

Továbbá tartalmaz egy fakultatív listát is, amelynek az elemei pedig a következőek:

- A számítógépes adatok és/ vagy programok megváltoztatása,
- A számítógépes kémkedés,
- A számítógép jogellenes használata,
- Védett programok jogellenes használata.

Az *ET. 95. (13.) számú ajánlása* pedig az információs technológiákkal kapcsolatos büntető eljárási problémákra törekedett megoldást nyújtani mint például a házkutatás és lefoglalás; technikai megfigyelés; kötelezettség a nyomozó hatóságokkal való együttműködésre; elektronikus bizonyítékok; titkosítás használata; statisztika és képzés; nemzetközi együttműködés során felmerülő kérdésekre ad választ.[84]

G-8 fórum és High Tech Crime csúcstalálkozó

1997-ben a G-8[85] fórum létrehozta a high-tech bűnözés elleni szakértő csoportot és számítógépes bűnözés elleni tíz alapelvet fogalmazta meg.[86]

2000 januárjában a Washington DC-ben megrendezett High Tech Crime csúcstalálkozón *Eric H. Holder, Jr.* három kategóriába csoportosította a számítógéppel kapcsolatos bűncselekményeket:

[84] Stein Schjolberg: The history of global harmonization on cybercrime legislation – the road to Geneva. 5. o.

[85] G-8 a következő államokból áll: Kanada, Franciaország, Olaszország, Japán, Oroszország, Egyesült Királyság, Németország és az Egyesült Államok.

[86] Deres Petronella: Internetes bűnözés. In: Tóth András (szerk.): Technológia jog – új globális technológiák jogi kihívásai. Budapest, 2016. 245. o.

1. a számítógép mint szoftver és hardver együttese ellen irányuló bűncselekmények (hacker-támadás, jogosulatlan behatolás, vírusterjesztés, adatlopás),
2. azok a bűncselekmények, amelyeknél a számítógép mint egy médium az elkövetéshez szükséges eszköz jelenik meg (számítógépes csalás, szerzői vagy szomszédos jogok megsértése, illegális termékek, szolgáltatások online értékesítése, zaklatás, online megvalósított szexuális bűncselekmények),
3. azok a tényállások, amelyeknél a számítógép, mint egy tároló eszköz jelenik meg, amelyen lévő adatok bizonyítékként szolgálhatnak valamely más bűncselekmény megállapításához (pl.: kábítószer-kereskedő vevőinek listája).[87]

Számítástechnikai Bűnözésről Szóló Egyezmény

2001 novemberében, az Európa Tanács által előkészített és Budapesten aláírt *„Számítástechnikai Bűnözésről Szóló Egyezmény" (Convention on Cybercrime)* (a továbbiakban: Budapesti Egyezmény) az egyetlen olyan kötelező erejű, multilaterális jogi dokumentum, amelynek célja a számítástechnikai bűnözés elleni küzdelem. Az egyezmény az aláíró felek számára keretet biztosít a nemzetközi együttműködéshez és olyan államok számára is nyitott a ratifikációja, amelyek nem tagjai az Európa Tanácsnak. Valamennyi a kiberbűnözést szabályozni célzó új, nemzetközi dokumentumnak, kezdeményezésnek az alapjait a Budapesti Egyezmény adja és a mai napig a legjelentősebb egyezménynek számít ezen a területen. Az eddigi ajánlásokhoz képest tovább lépést jelentett és újabb jogi normákat fogalmazott meg. A számítógépes technikai fogalmakat definiálja és ezáltal egységes értelmezést nyújt (számítógépes rendszer, számítógépes adat, internetes szolgáltató, átmenő adat). Mind az anyagi és eljárásjogi szabályozást tartalmazza. Az anyagi jogban a bűncselekménytípusok köre kibővült és újabb jogsértési típusok jelennek meg (pl. eszközökkel való visszaélés, a gyermekpornográfiával kapcsolatos bűncselekmények). Az egyes bűncselekménytípusokat logikusan csoportokba rendezi. Az egyezmény kimondja, hogy minden szerződő fél megteszi azon jogalkotási és egyéb intézkedéseket, melyek ahhoz szükségesek, hogy belső jogával összhangban bűncselekménynek minősüljön az alábbi cselekmények jogosulatlan és szándékos elkövetése:

I. cím: A számítástechnikai rendszer és a számítástechnikai adatok hozzáférhetősége, sértetlensége és titkossága elleni bűncselekmények

[87] Szabó Imre: Internetes bűncselekmények különöse tekintettel az internetes csalásra. In: Kiss Daisy (szerk.): E-akták. Tanulmányok az internetjog világából. (Studia Collegii De Stephano Bibo Nominati) Bibó István Szakkollégium Internetjogi Kutatócsoport, Budapest, 2003. 302. o.

- 2. cikk: A jogosulatlan belépés
- 3. cikk: A jogosulatlan kifürkészés
- 4. cikk: A számítástechnikai adat megsértése
- 5. cikk A számítástechnikai rendszer megsértése
- 6. cikk: Eszközökkel való visszaélés

II. cím: A számítógéppel kapcsolatos bűncselekmények

- 7. cikk: A számítógéppel kapcsolatos hamisítás
- 8. cikk: A számítógéppel kapcsolatos csalás

III. cím: A számítástechnikai adatok tartalmával kapcsolatos bűncselekmények:

- 9. cikk: A gyermekpornográfiával kapcsolatos bűncselekmények
- 10. cikk: Szerzői vagy szomszédos jogok megsértésével kapcsolatos bűncselekmények

2003-ban az egyezményt kiegészítették a számítástechnikai rendszerek útján megvalósított rasszista és idegengyűlölő cselekmények büntetendővé nyilvánításáról szóló kiegészítő jegyzőkönyvvel. A Budapesti Egyezmény azonban egyes számítástechnikai cselekmények szabályozását nem tartalmazza mint például a személyazonosság lopást, a gyermekekkel történő szexuális célú kapcsolattartást, kiberterrorizmusra, illetve a kéretlen levélre (spam) sem tér ki. Magyarországon a 2004. évi LXXIX. törvénnyel hirdették ki, ezzel összhangban a Büntető Törvénykönyvbe (a továbbiakban: Btk.) a 300/C. § a Számítástechnikai rendszer és adatok elleni bűncselekmény tényállását felvette, valamint egyéb más törvényi tényállásokat kiegészített a meghatározottak szerint.

Ugyanebben az évben *az Európai Tanács 2001/413/IB kerethatározata* került elfogadásra a nem készpénzes fizetőeszközökkel összefüggő csalás és hamisítás elleni küzdelemről.[88]

2002-ben került elfogadásra az Európai Parlament és a Tanács 2002/58/EK *„Elektronikus Hírközlési Adatvédelmi Irányelve”*, amelynek célja, hogy biztosítsa a felhasználóknak az elektronikus hírközlési és technológiai szolgáltatások iránti bizalmát. Ezek a szabályok különösen a „spamek” betiltására, a felhasználó előzetes beleegyezését kérő (opt-in) rendszerre és a cookie-k telepítésére vonatkoznak. Ez az irányelv 2009-ben egészült ki az ún. „süti” (cookie) irányelvvel, amely alapján a viselkedésalapú reklám célba juttatásához használt cookie-k kizárólag az érintettek hozzájárulását követően helyezhetők el a felhasználók számítógépein.[89]

[88] http://www.rendeszetelmelet.hu/Graphics/pdf/Nagy_Zoltan_Andras_A_2013_40_es_Unios_direktiva.pdf [2016.12.21.]; http://www.pecshor.hu/periodika/XIII/gyaraki.pdf 237-239. o. [2016.12.21.]
[89] http://adatvedelmiaudit.hu/2011/06/cookie-k-csak-hozzajarulassal/ [2016.11.21.]

Az EUROPOL szervezetén belül 2002-ben hozták létre *a Csúcstechnológiai Bűnözési Központot (High Tech Crime Centre).*[90]

Az Európai Hálózat- és Információbiztonsági Ügynökség (ENISA)

Az Európai Tanács 2004/97/EK határozattal létrehozták az *Európai Hálózat- és Információbiztonsági Ügynökséget (ENISA)*, amely az Unió, a tagállamok, a magánszektor és az európai polgárok szolgálatában álló hálózat- és információbiztonsági szakértői központ. Jelenleg az 526/2013/EU rendelet szabályozza a szervezet működését. Az ENISA gyakorlati tanácsokat és megoldásokat nyújt az EU-tagállamok köz- és magánszektor szereplőinek és az uniós intézményeknek a hálózat- és információbiztonság területén. Ennek keretében:

- egész Európára kiterjedő kiberbiztonsági gyakorlatokat szervez;
- segíti a tagállamokat nemzeti kiberbiztonsági stratégiájuk kifejlesztésében;
- elősegíti az együttműködést a hálózatbiztonsági vészhelyzeteket elhárító csoportok és a kapacitásépítésért felelős szervezeti egységek között.

Az ENISA emellett jelentéseket és tanulmányokat tesz közzé a kiberbiztonság témájában. Az ENISA segít a hálózat- és információbiztonságra vonatkozó uniós szakpolitikák és jogszabályok megszövegezésében is.[91]

2005/222/IB tanácsi kerethatározat

2005-ben pedig az információs rendszerek elleni támadásokról szóló *2005/222/IB tanácsi kerethatározat* elfogadására került sor,[92] amelynek a célja számítógépes bűnözés elleni küzdelem és az információbiztonság előmozdítása. A transznacionális bűnözés ezen új formáját tekintve a kerethatározat fő célja az igazságügyi és egyéb illetékes hatóságok közötti együttműködés javítása az információs rendszerek elleni támadások területére vonatkozó büntetőjogi szabályok közelítése által a következő területeken: információs rendszerekhez való jogsértő hozzáférés, rendszerekbe való jogsértő beavatkozás, adatokba való jogsértő beavatkozás. A kerethatározatnak megfelelően vette át a magyar szabályozás is az információs rendszer szóhasználatát az ilyen típusú bűncselekményeknél. Fogalommeghatározásokat is tartalmaz, amit a kerethatározatot felváltó új irányelv, át is vesz, ezért annak a részletesebb szabályozására térünk ki a későbbiekben, hiszen az teljes mértékben a kerethatározatra épül.

[90] Szalárdi Gábor: A csúcstechnológiai bűnözés elleni küzdelem támogatása. Belügyi Szemle 2012/6. 98-99. o.
[91] https://europa.eu/european-union/about-eu/agencies/enisa_hu [2016.11.21.]
[92] http://eur-lex.europa.eu/legal-content/HU/ALL/?uri=CELEX:32005F0222 [2016.11.21.]

Az Európai Unióról szóló és az Európai Unió működéséről szóló szerződés 83. cikk (1) bekezdése pedig kimondja, hogy:

„Az Európai Parlament és a Tanács rendes jogalkotási eljárás keretében elfogadott irányelvekben szabályozási minimumokat állapíthat meg a bűncselekményi tényállások és a büntetési tételek meghatározására vonatkozóan az olyan különösen súlyos bűncselekmények esetében, amelyek jellegüknél vagy hatásuknál fogva a több államra kiterjedő vonatkozásúak, illetve amelyek esetében különösen szükséges, hogy az ellenük folytatott küzdelem közös alapokon nyugodjék. Ezek a bűncselekményi területek a következők: terrorizmus, emberkereskedelem és a nők és gyermekek szexuális kizsákmányolása, tiltott kábítószer-kereskedelem, tiltott fegyverkereskedelem, pénzmosás, korrupció, pénz és egyéb fizetőeszközök hamisítása, *számítógépes bűnözés* és szervezett bűnözés."

Erre tekintettel „A polgárokat szolgáló és védő, nyitott és biztonságos Európa" című 2010-ben kiadott a tamperei és hágai programot követő *ún. stockholmi program* az Európát érintő jövőbeli kihívások között említi a számítógépes bűnözést.

Az Európai Parlament és Tanács 2011/92/EU számú Irányelve

2011-ben *az Európai Parlament és Tanács 2011/92/EU számmal Irányelvet* fogadott el a gyermekek szexuális bántalmazása, szexuális kizsákmányolása és a gyermekpornográfia elleni küzdelemről. Ezzel összefüggésben 2012-ben kezdetét vette egy nemzetközi összefogás „Globális szövetség a gyermekek online szexuális kizsákmányolása ellen", amelyhez az uniós országokon kívül más országok is csatlakoztak.

Számítástechnikai Bűnözés Elleni Európai Központ (EC3)

2013. január 11-től kezdte meg működését *a Számítástechnikai Bűnözés Elleni Európai Központ (EC3),* amely az európai polgárok és vállalkozások számítástechnikai bűnözéssel szembeni védelméhez nyújt segítséget. A központot az Európai Rendőrségi Hivatal (Europol) hágai székhelyén hozták létre. A számítástechnikai bűnözés elleni központ megnyitása fontos változást jelez a számítástechnikai bűnözés uniós kezelési módjában. Először is, a központ hosszú távon és átfogó módon gondolkodik. Egybegyűjti a szaktudást és az információkat, támogatja a bűnügyi nyomozásokat és elősegíti az egész Unióra kiterjedő megoldásokat. Aktív szerepet vállal több ügynökség is a központ portfóliójának a kialakításában. A legfőbb partnerek ebben: ENISA, az Európai Unió Bűnüldözési Képzési Ügynöksége (CEPOL), EUCT és az INTERPOL. A központ a számítástechnikai bűnözés következő területeit célozza:

- a szervezett bűnözői csoportok által elkövetett számítástechnikai bűncselekmények, különösen azok, amelyek tetemes, jogellenesen szerzett nyereséget érnek el, például az online csalás;
- azok a számítástechnikai bűncselekmények, amelyek súlyos kárt okoznak áldozataiknak, így például a gyermekek szexuális kizsákmányolása; továbbá
- azok a számítástechnikai bűncselekmények (köztük a célzott weboldalak megbénítására irányuló szolgáltatásmegtagadással járó támadás), amelyek az EU-n belüli kritikus infrastruktúrát és információs rendszereket érintik.

A központ funkciói pedig a következők:

- a számítástechnikai bűnözésre vonatkozó információk összegyűjtése;
- a szakértelem összefogása az uniós tagállamok kapacitásépítésének támogatása céljából, különösen a rendőrség és igazságszolgáltatás személyzete részére nyújtott képzések tartása révén;
- műveleti támogatás nyújtása a tagállamok részére, közös nyomozócsoportok létrehozásával;
- az európai számítástechnikai bűnügyi nyomozók egységes, közös álláspontját képviseli, amely átfogja a bűnüldözés és az igazságszolgáltatás területét is.[93]

Az Európai Parlament és Tanács 2013/40/EU számú Irányelve

2013 augusztusában az Európai Parlament és Tanács *2013/40/EU számmal Irányelvet*[94] fogadott az információs rendszerek elleni támadásokról, amely a 2005/222/IB kerethatározatot váltotta fel és célja a számítástechnikai bűnözés elleni küzdelem megerősítése az információbiztonság előmozdítása, a szigorúbb nemzeti büntetőjogi szankciók és az illetékes hatóságok hatékonyabb együttműködése révén. Számos új szabályt vezet be a számítástechnikai bűncselekmények büntetendőségének és szankciójának harmonizálására. Az új szabályok közé tartozik az ún. botnetek - számítógép-hálózatok távoli irányítására tervezett rosszindulatú számítástechnikai programok - törvényen kívül helyezése is. Felhívja a figyelmet arra, hogy valamennyi tagállamban hatékony fellépésre van szükség, ezért biztosítani kell, hogy ugyanaz a bűncselekmény valamennyi tagállamban büntetendő legyen és a bűnüldöző hatóságok számára biztosítani kell a fellépéshez szükséges, az egymás közötti együttműködést elősegítő eszközöket. Az irányelv a büntetőjogi rendszereknek az

[93] http://europa.eu/rapid/press-release_IP-13-13_hu.htm [2016.12.20.]
http://eur-lex.europa.eu/legal-content/HU/TXT/?uri=URISERV%3A230806_1 [2016.12.20.]
[94] http://eur-lex.europa.eu/legal-content/HU/TXT/?uri=uriserv:OJ.L_.2013.218.01.0008.01.HUN [2016.12.20.]

uniós országok közötti közelítését és az igazságügyi hatósági együttműködés bővítését sürgeti az alábbi területeken:

- információs rendszerekhez való jogellenes hozzáférés;
- információ rendszerekbe való jogellenes beavatkozás;
- adatokba való jogellenes beavatkozás;
- jogellenes adatszerzés.

A tagállamoknak közös megközelítést kell kialakítaniuk a bűncselekmények tényállás elemeire vonatkozóan az információs rendszerhez való jogosulatlan hozzáférés, illetve az adatokat érintő jogellenes beavatkozás, valamint a jogellenes adatszerzés egységes bevezetése révén „Adatszerzés különösen a kommunikáció tartalmának lehallgatása, ellenőrzése vagy figyelemmel kísérése és az adattartalmak közvetlenül, az információs rendszerhez való hozzáférés és az információs rendszer használata által történő, vagy közvetetten, elektronikus megfigyelő vagy lehallgató eszközök révén történő megszerzése.”.

Továbbá a tagállamoknak a legalább a súlyosabb esetekben bűncselekménynek kell minősíteniük azokat az eseteket, amikor az irányelvben foglalt bűncselekmények elkövetéséhez felhasználnak eszközöket (pl.: számítógépes programok készítése, belépési kódok, jelszavak felhasználása az információs rendszerhez való hozzáféréshez).

A közös fogalommeghatározások fontosságát hangsúlyozza ki, hasonlóan, mint a korábbi kerethatározat (információs rendszer[95], számítógépes adatok,[96] jogi személy és jogosulatlanul[97]). A bűncselekmény elkövetésének minden esetben szándékosnak kell lennie. Valamennyi az irányelvben foglalt bűncselekményre való felbujtás illetve az elkövetéshez nyújtott bűnsegélynek bűncselekménynek kell minősülnie. Az adatot érintő jogellenes beavatkozás és jogellenes adatszerzés esetében pedig a kísérlet is büntetendő. Azonban az irányelv nem állapít meg büntetőjogi felelősséget abban az esetben, ha az ezen irányelvben felsorolt bűncselekmények objektív kritériumai teljesülnek, azonban a cselekményeket nem jogsértő szándékkal követték el (pl.: az adott személynek nincs tudomása arról, hogy az adott hozzáférés jogosulatlan).

---

[95] „információs rendszer”: minden olyan eszköz, illetve összekapcsolt vagy kapcsolódó eszközökből álló eszközcsoport, amelyek közül egy vagy több valamely program alapján automatikus adatfeldolgozást hajt végre számítógépes adatokon, valamint a működése, használata, védelme és karbantartása céljából az ezen eszköz vagy eszközcsoport által tárolt, feldolgozott, helyreállított vagy továbbított számítógépes adatokon;

[96] „számítógépes adatok”: tények, információk vagy fogalmak megjelenítése olyan formában, amely alkalmassá teszi azokat egy információs rendszer általi feldolgozásra, beleértve azon programokat is, amelyek alkalmasak valamely funkciónak egy információs rendszer általi elvégeztetésére;

[97] „jogosulatlanul”: ezen irányelvben említett olyan magatartás, ideértve a belépést, beavatkozást vagy adatszerzést, amelyet a rendszernek vagy a rendszer részének tulajdonosa vagy egyéb jogosultja nem engedélyezett, vagy amelyet a nemzeti jog nem tesz lehetővé.

A tagállamoknak hatékony, arányos és visszatartó erejű szankciókat kell alkalmazniuk, és szabadságvesztést és/vagy pénzbüntetést is magukban kell foglalniuk.

Súlyosabb szankció megállapításának van helye, ha az információs rendszer elleni támadást bűnszervezetben követik el, vagy ha a támadás átfogó, azaz jelentős számú információs rendszert érint, vagy súlyos kárt okoz, abban az esetben is, ha a támadás valamely tagállam vagy az Unió kritikus infrastruktúrája ellen irányul. A tagállamoknak a jogrendszerük által a súlyosító körülményekre vonatkozóan megállapított szabályokkal összhangban súlyosító körülményeket kell meghatározniuk a nemzeti jogukban. De lege ferenda szükségesnek mutatkozik például a magyar szabályozásra nézve, hogy a minősített eseteket bővítse a szervezett bűnözés keretében.

Az informatikai támadásokat számos körülmény megkönnyítheti, például ha az elkövetőnek alkalmazotti minőségében hozzáférése van az érintett információs rendszerek részét képező biztonsági rendszerekhez. A magyar jognak szintén feladatot tűz ki ezzel az irányelv, mert a jelenlegi szabályozás nincs tekintettel az alkalmazottak általi elkövetésre.

Továbbá az irányelv felhívja a figyelmet a személyazonosság-lopás illetve a személyazonossághoz kapcsolódó egyéb bűncselekmények elleni hatékony fellépés relevanciájára, a magyar büntetőtörvénykönyvben szükséges lenne a jövőben ennek a bűncselekménytípusnak a szankcionálása.

A hatékony prevenció érdekében a hatóságoknak együtt kell működniük a magánszférával és a civil társadalommal (pl.: ez kiterjedhet a szolgáltatók általi a potenciális bizonyíték megőrzésére, együttműködési és partnerségi hálózat kiépítésére a szolgáltatókkal és a gyártókkal).

A jogi személyek felelősségét és a velük szemben alkalmazandó szankciókat a kerethatározathoz hasonlóan tartalmazza. Továbbá a joghatósági kérdésekre is választ ad.

A tagállamok megállapítják joghatóságukat az információs rendszer elleni bűncselekmények tekintetében, amennyiben a bűncselekményt:

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.

Az a) pont szerinti joghatóság megállapításakor 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.

A tagállamok tájékoztatják a Bizottságot, ha úgy döntenek, hogy a területükön kívül elkövetett bűncselekményekre vonatkozóan további joghatóságot állapítanak meg, többek között amennyiben:

a) az elkövető szokásos tartózkodási helye a területükön van; vagy
b) a bűncselekményt a területükön letelepedett jogi személy javára követték el.

A hatékony fellépés érdekében a tagállamok gondoskodnak saját operatív nemzeti kapcsolattartó pontjuk létrehozásáról, és arról, hogy igénybe veszik a meglévő, a hét minden napján 24 órában rendelkezésre álló operatív kapcsolattartó hálózatot. A tagállamok olyan eljárások működését is biztosítják, amelyek révén sürgős segítségkérés esetén az illetékes hatóság a kézhezvételtől számított 8 órán belül jelezheti legalább azt, hogy teljesíti-e a segítségkérést, valamint hogy ezt milyen formában és várhatóan mikor teszi. Továbbá tagállamoknak biztosítani kell egy olyan rendszer meglétét, amely rögzíti, előállítja és rendelkezésre bocsátja ezekre a bűncselekményekre vonatkozó statisztikai adatokat.

Az irányelvet a tagállamoknak 2015. szeptember 4-ig kellett implementálniuk a nemzeti jogukba.

A 2012. évi C. Büntető Törvénykönyvünk a következő bűncselekményeket rendeli büntetni, amelyek az információs rendszereket érintik: a vagyon elleni bűncselekmények között az információs rendszer felhasználásával elkövetett csalás (Btk. 375.§), illetve külön csoportot képez a tiltott adatszerzés és az információs rendszer elleni bűncselekmények (Btk. 422-424.§), amelyekhez tartozik értelemszerűen a tiltott adatszerzés, információs rendszer vagy adat megsértése, illetve az információs rendszer védelmét biztosító technikai intézkedés.

A jogalkotás, jogalkalmazás felkészülése

A jogalkotás irányába különösen fontos lenne a kibertér jövő veszélyek, visszaélések megismerése, jogi szempontú megértése a jogalkotásban érdekeltek számára. A törvényhozó sem érdeklődik igazán az új eredmények iránt. Holott fentebb láttunk néhány ellentmondást, például a wardriving nem egyszerűen hacking. Vagy ha a phishing csupán a kár bekövetkeztével válik bűncselekménnyé [csalás, Btk. 373.§], az azt lehetővé tevő az adathalászat büntetlen maradhat? Nemcsak a büntetőjogban keletkezett anomália. A gyülekezési jogot, mint Alaptörvénybeli jogot [VIII.cikk (1)] érintő flash-mob (villámgyülekezést) is törvényi rendezésért kiált. Vajon mit tesz a hatóság, ha egy flash-mob-ot észlel? Ha ez a mindenkori kormányra kínos, kritikus hangú, akkor szabálysértési vagy büntetőeljárás indul?[98] Ha nem, akkor továbbfolyhat a flash-mob. Az anomáliákat ne folytassuk…

A jogalkalmazás kapcsán kérdés, ahogy dolgoznak, nagy szakmai tudással, elismertséget kivívó közlekedési-, gazdasági és más ügyekre szakosodott bírák, ügyészek, rendőrök, ugyanúgy, ma már szükség lenne az információ-technológia jogi vonatkozásaival tisztában levő jogalkalmazókra is.

[98]Pécsett néhányan a menekültkérdéssel foglalkozó plakátoknál flashmobot szerveztek, ahonnan a főszervezőt elvezették és ellene büntetőeljárást indítottak. http://okpecs.hu/birosag-ele-allitjak-a-pecsi-plakatrongalot-aki-nem-is-rongalta-meg-a-plakatot/ [2016.10.25.]
http://tasz.hu/gyulekezesi-jog/ha-flashmob-ot-szervezel-nem-kell-bejelentened-rendorsegen [2016.10.25.]
Az Alkotmánybíróság 75/2008. (V. 29.) határozata elismeri a flash-mob létét, bár további kommentárt nem fűz hozzá. Értelmezési vita folyik arról, hogy a 2012 előtti AB-határozatok relevánsak-e vagy sem.

Általános tanácsok a megelőzéshez

Számítógépünk védelmét éppúgy meg kell szerveznünk, mint vagyontárgyaink (pl. lakás, autó) védelmét.

Az “elektronikus betörés” elleni védekezés főbb pillérei:

1/a. A számítógép, a hálózat fizikai védelme. Így irodák, termek, laboratóriumok, lakószobák biztonságának megteremtése (beléptető-rendszer különböző azonosításokkal, és/vagy térfigyelő kamerák, zárak, riasztók alkalmazása, továbbá más szempontból tűzbiztonsági követelmények teljesítése stb.).

1/b. A számítógépek fizikai védelme. (Elzárt helyen történő tárolás, kikapcsolt állapotban, hagyás, különböző hozzáférés védelmi megoldások).

2. A szoftverek (különösen az operációs rendszer, a levelezőprogram, a portok) biztonsági megoldásai, továbbá a tevékenység (munkafolyamat) naplózása.

3. A felhasználó óvatossága, kellő körültekintése. Tanácsos a jelszavainkat viszonylag nem hosszú időközönként cserélni. Jelszavaink tartalmazzanak kis- és nagy betűket, számokat egyaránt. Óvakodjunk az értelmes szavak, szeretteink, kisállataink neveinek, gépkocsink rendszámának jelszóként történő megadásától, azaz minden olyan szótól, amely az azonosítást megkönnyíti.

Ne hagyjunk jelszavunkat a gép mellett egy papír cetlin, vagy a monitorra ragasztva. Ne közöljük senkivel azt!

4. A számítástechnikával foglalkozó weboldalakról hasznos tanácsok leshetők el!

5. Bátran kérjünk tanácsot a számítástechnikában jártas szakemberektől!