3. A kiberbűncselekmények fogalma és csoportosítása

Nagy Zoltán

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

3.1. A kiberbűncselekmények fogalma

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

---

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

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

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

https://doi.org/10.36250/00782_03

3.2. A kiberbűncselekmények csoportosítása

3.2.1. Tradicionális visszaélések, bűncselekmények az új színtéren

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

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

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

3.2.2. Az informatikai rendszerhez és térhez kötött visszaélések, bűncselekmények

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Vírusok fajai:

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

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

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

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

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

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

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

3.3. Veszélyek a közösségi hálózatokon

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

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

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

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

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

3.4. A szerzői jog számítógépes környezetben

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

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

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

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

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

3.5. *Defacing* (webtartalom felülírása)

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

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

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

3.6. A terheléses vagy szolgáltatásmegtagadással járó támadások

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

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

3.7. Az elektronikus adatok kifürkészése

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

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

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

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

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

3.8. A *card not present* esetköre

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

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

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

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

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

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

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

3.10. Az informatikai rendszer mint eszköz, cél és tárhely

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

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