Sorbán Kinga
Büntető Eljárásjogi és Büntetés-végrehajtási Jogi Tanszék
Témavezető: Finszter Géza egyetemi tanár

Az informatikai bűncselekmények elleni fellépés az Egyesült Államokban

1. Bevezetés

Az informatikai bűncselekmények elleni fellépés kialakulásának vizsgálata, illetve az ebbe a bűncselekményi körbe tartozó deliktumok vizsgálata során nem hagyhatjuk figyelmen kívül az Egyesült Államokat. Az Egyesült Államok az informatikai bűncselekmények őshazája, és az ország az elsők között ismerte fel azt, hogy az információtechnológiai eszközök fejlődése és a széles rétegek számára való elérhetősége a számtalan lehetőség mellett veszélyforrásokat is rejt magában. A tanulmányom célja annak bemutatása, hogy az Egyesült Államokban miként határozzák meg az informatikai bűncselekmények körébe tartozó deliktumokat, illetve mely szervezetek segítik az ilyen típusú bűncselekmények elleni hatékony fellépést. Az értekezés négy nagyobb témakörre bontható.

Az első rész azokat a definíciókat veszi számba, amelyekkel az Egyesült Államokban az informatikai bűncselekményeket leírják. Ahogy Európában, úgy az Amerikai Egyesült Államokban sincs egységes elnevezése az informatikai bűncselekményeknek. Általánosságban elmondható, hogy az egyes fogalmak jelentése és használata ugyanannyira zűrzavaros, mint a kontinentális jogban. A második rész azzal foglalkozik, hol helyezkednek el az Egyesült Államok jogrendszerében az egyes deliktumok. Mivel *„az Egyesült Államokban szövetségi rendszer működik, az informatikai bűncselekmények szabályozása is kétszintű: a szövetségi informatikai büntetőjog egységes, mindent magába foglaló rendszer, a területi hatálya az Amerikai Egyesült Államok teljes területére kiterjed, az állami informatikai büntetőjog azonban mindenhol eltérő, mind az 50 szövetségi állam (valamint a kolumbiai körzet) informatikai büntetőjoga csak az adott állam területén érvényes*."[1] Egyrészt terjedelmi okokból, másrészt azért mert az egyes államok rendszerei között sokszor nagy az átfedés,

[1] Eoghan CASEY 2011.: 85.

értekezésem kizárólag a szövetségi szintet tárgyalja. A harmadik rész taglalja az egyes deliktumokat, amelyeket a fenti törvények büntetni rendelnek. Az amerikai jogban megjelenő informatikai elemet tartalmazó bűncselekményeket többféleképpen lehet csoportosítani. Az egyik ilyen csoportosítás a számítógép bűncselekményben játszott szerepeit veszi alapul, létezik azonban történeti jellegű csoportosítás is. A tisztán informatikai jellegű bűncselekmények között bemutatom a hackelést, a kártékony programok (malware) készítését és terjesztését, valamint a számítógépes csalás egyes eseteit. Az informatikai elemet tartalmazó, de nem tisztán informatikai bűncselekmények körében igen sokféle tényállás található, amelyek között a legjelentősebbek a tartalommal kapcsolatos bűncselekmények (pl. a gyermekpornográfia, szerzői jog megsértése), a személyazonosság lopás, a zaklatás, valamint a napjainkban kialakult ún. cyberbullying. A negyedik rész az informatikai bűncselekmények elleni fellépés rendszerével foglalkozik, különös tekintettel azokra a nyomozó hatóságokra, amelyek az informatikai bűncselekmények elleni küzdelemben részt vesznek. A tanulmány a szövetségi szintű fellépésre koncentrálva mutatja be a Nemzeti Kiberbiztonsági és Kommunikációs Integrációs Központ (National Cybersecurity and Communications Integration Center), a titkosszolgálaton belül működő Elektronikus Bűncselekmények Elleni Munkacsoportok (Electronic Crimes Task Force), valamint a Szövetségi Nyomozóirodán belül működő kiberbűnözési egységek (Cyber Task Force) munkáját.

2. Az informatikai elemet tartalmazó bűncselekményeknél használt definíciók

Ahogy Európában, úgy az Amerikai Egyesült Államokban sincs egységes elnevezése az informatikai bűncselekményeknek. Általánosságban elmondható, hogy az egyes fogalmak jelentése és használata ugyanannyira zűrzavaros, mint a kontinentális jogban. Marije T. Britz az informatikai bűncselekményekkel kapcsolatban összesen 4 féle fogalmat azonosított[2], ezek:

- számítógépes bűncselekmény
- számítógéppel kapcsolatos bűncselekmény
- digitális bűncselekmény
- kiberbűncselekmény

A számítógépes bűncselekmény (*computer crime*) fogalmát Britz úgy határozza meg, mint olyan általános fogalmat, amelyet azokra a

[2] Marije T. BRITZ 2013.: 6.

bűncselekményekre használunk, amelyeket számítógéppel követtek el. Ez az általános fogalom magában foglalja mind az internetes, mind az offline cselekményeket, így például az alkatrészlopást, a hamisítást, a szerzői jog megsértését, a hackelést és a gyermekpornográfiát. Számítógéppel kapcsolatos bűncselekmények alatt (*computer related crime*) olyan cselekményeket ért, amelyekben a számítógép csak érintőlegesen van jelen, például amikor a lopás részleteit e-mailben beszélik meg az elkövetők. Digitális bűncselekménynek (*digital crime*) tekinti azokat a bűncselekményeket, amelyekben az elektronikus adat van kiemelt helyen, tehát az elektronikus adatokhoz való jogosulatlan hozzáférést, az elektronikus adatok jogosulatlan terjesztését, megváltoztatását, törlését vagy károsítását. Kiberbűncselekmény (*cybercrime*) elnevezés alatt pedig kifejezetten azokat a cselekményeket érti, amelyeket az interneten keresztül követtek el.

Hasonló rendszert állított fel Eoghan Casey is, aki a számítógépes bűncselekmény, illetve a számítógéppel kapcsolatos bűncselekmény kategóriáit nevesíti,[3] azonban nem ad egzakt definíciókat, hanem mindegyik kategóriát az általa lefedett bűncselekményi körbe tartozó deliktumok példálózó felsorolásával azonosítja. Megjegyzendő, hogy ezek a kategóriák egymástól nem függetlenek, hanem inkább rész-egész viszonyban állnak egymással, hiszen az egyes bűncselekmények egyszerre több kategóriába is sorolhatóak. Jó példa erre a hackerek tevékenysége, akik az interneten keresztül jogosulatlanul lépnek be egy számítógépre, ezáltal a tevékenységük egyben számítógépes bűncselekmény és kiberbűncselekmény is. A belépés során ezen felül hozzáférhetnek adatokhoz, megváltoztathatják, illetve törölhetik azokat, így a cselekedetük egyben digitális bűncselekménynek is minősül.

Kiemelendő, hogy a számítógépes bűncselekmények kizárólag azoknak az eszközökkel összefüggésben követhetők el, amelyek az amerikai jog alapján számítógépnek minősülnek. Az Amerikai Egyesült Államok Kódexe a 18. cím 1030. §-ban határozza meg a számítógép fogalmát. A törvény szerint *„a számítógép olyan elektronikus, mágneses, optikai, elektrokémiai vagy egyéb nagysebességű adatfeldolgozó eszközt jelent, amely logikai, matematikai vagy tárolási funkciókat lát el, ezen felül magában foglal olyan adattárolásra vagy kommunikációra szolgáló szerkezetet, amely közvetlenül kapcsolódik az eszközhöz vagy párhuzamosan működik azzal, kivéve az automatizált írógépeket, zsebszámológépeket és hasonló eszközöket.*[4]*”* Mint láthatjuk a törvény a számítógép kifejezést rendkívül

[3] Eoghan CASEY 2011.: 37.

[4] U.S. Code 18. cím 47. fejezet 1030 § (e)(1) - http://uscode.house.gov/view.xhtml?req=granuleid:USC-prelim-title18-section1030&num=0&edition=prelim (2016. 02.11.)

tág értelemben használja, szemben annak hétköznapi értelmével. A számítógép kifejezést a mindennapi szóhasználatban hajlamosak vagyunk kizárólag az asztali számítógépekre vagy laptopokra vonatkoztatni, elfeledkezünk azonban arról, hogy az információtechnológia fejlődése rendkívüli mértékben megnövelte a fenti komplex számítási feladatok elvégzésére képes eszközök körét. Ennek megfelelően számítógépnek minősülnek a desktopok (asztali számítógép) és a laptopok mellett a táblagépek, a játékkonzolok, az okostelefonok, a szervergépek, PDA-k és egyes nyomtatók is.

3. Az informatikai elemet tartalmazó bűncselekményekkel kapcsolatos jogszabályok kialakulása és fejlődése

„Mivel az Egyesült Államokban szövetségi rendszer működik, az informatikai büntetőjognak két szintje van: a szövetségi informatikai büntetőjog, valamint az állami informatikai büntetőjog. A szövetségi informatikai büntetőjog egységes mindent magába foglaló rendszer; a területi hatálya az Amerikai Egyesült Államok teljes területére kiterjed. Az állami informatikai büntetőjog azonban mindenhol eltérő; mind az 50 szövetségi állam (valamint a kolumbiai körzet) informatikai büntetőjoga csak az adott állam területén érvényes. [5]" Az Egyesült Államokban először 1984-ben született olyan törvény, amelyben kifejezetten informatikai bűncselekményekkel kapcsolatos rendelkezéseket is találunk, ez az 1984. évi átfogó bűnüldözési törvény (*Comprehensive Crime Control Act,* 1984). Az úgynevezett „hackertörvényt" azonban számtalan kritika érte, Marije T. Britz szerint[6] például a jogszabály azért sem bizonyult hatékonynak mivel a nyelvezete kétértelmű volt, ezen felül túl nagy hangsúlyt fektetett a pénzügyi jellegű információkra. A rendelkezéseket 1986-ban módosította a számítógépes csalásról és számítógépes visszaélésekről szóló törvény *(Computer Fraud and Abuse Act,* 1986), amelynek a megalkotása óta több rendelkezése is módosult. A módosítások között említést érdemel az 1996. évi nemzeti információs infrastruktúra védelméről szóló törvény, (*National Information Infrastructure Protection Act*), amely több ponton módosította elődjét, és megalkotására Marije T. Britz szerint[7] azért volt szükség, mert az 1986-os törvény csak a hackerek illetve az olyan egyének felelősségre vonására volt alkalmazható, akik jogosulatlanul léptek be vagy jogosultságukat túllépve bent maradtak egy számítógépes rendszerben. Nem fedte le azonban az olyan egyéb bűncselekményeket, amelyeket

[5] Eoghan CASEY 2011.: 85.
[6] Marije T. BRITZ 2013.: 191.
[7] Marije T. BRITZ 2013.: 193.

számítógép felhasználásával követtek el, illetve amelyek számítástechnikai eszközökkel álltak kapcsolatban. A nemzeti információs infrastruktúra védelméről szóló törvény kiegészítette az 1986-os hackertörvényt olyan új tényállásokkal, amelyek a számítógépekhez kapcsolódó informatikai bűncselekményeknek jóval szélesebb körét fedik le.

Az informatikai bűncselekmények kapcsán említést kell tennünk a gyermekpornográfia elleni fellépés érdekében született törvényekről is. A gyermekpornográfia ugyan nem tisztán informatikai jellegű bűncselekmény, de az elkövetésében (gyermekpornográf anyagok elkészítése, tárolása, terjesztése) az internet anonim jellegének köszönhetően ma már domináns az információtechnológiai elem. Az Egyesült Államokban az első gyermekpornográfia kérdésével foglalkozó törvény az 1977. évi a gyermekek szexuális kizsákmányolástól való védelméről szóló törvény volt, ez azonban még nem tartalmazott semmilyen technológiára utaló elemet. Az 1996. évi gyermekpornográfiától való védelemről szóló törvény (*Child Pornography Protection Act – CPPA*) azonban kiterjesztette a tilalmat azokra a képekre is, amelyeket digitálisan módosítottak és ezáltal válnak gyermekpornográfiának minősülő anyagokká. Marije T. Britz leírja,[8] hogy ez a rendelkezés sok vitát váltott ki, a Legfelsőbb Bíróság pedig később alkotmányellenessé nyilvánította azt. Az Ashcroft vs. Free Speech Coalition ügyben[9] a bíróság kimondta, hogy a gyermekpornográfia fogalma, amennyiben magába foglalja az olyan anyagokat, amelyekről úgy tűnk, hogy valódi gyermekeket ábrázolnak, alkotmánysértő. A döntésben a bíróság kifejtette, hogy az igazi gyermekeket ábrázoló pornográf anyagok betilthatók, mivel való gyermekek válnak áldozattá. A virtuális gyermekpornográfia azonban nem büntethető, mivel véleménynyilvánításnak minősül, és az ilyen anyagok megalkotása semmilyen emberi lénynek nem okoz sérelmet. Az Ashcroft döntést követően fogadta el a kongresszus a gyermekek kizsákmányolása elleni büntető-eljárásjogi intézkedésekről és egyéb eszközökről szóló törvényt 2003-ban (*Prosecutorial Remedies and Other Tools to End the Exploitation of Children Today - PROTECT)*.

1998-ban fogadták el a személyazonosság lopás és személyazonosság másolás elleni fellépésről szóló törvényt (*Identity Theft and Assumption Deterrence Act - ITADA)*, amely az első olyan törvény, amely bűncselekménnyé nyilvánítja egy másik személy személyazonosságával való visszaélést. Részben a személyazonossággal kapcsolatos

[8] Marije T. BRITZ 2013: 194.
[9] Eoghan CASEY 2011.: 97.

visszaéléseket szabályozza a 2003-ban elfogadott Tisztességes és Pontos Hitelügyletekről szóló törvény (*Fair and Accurate Credit Transactions Act* - FACTA), amely olyan fogyasztóvédelmi rendelkezéseket tartalmaz, amelyek lehetővé teszik a személyazonosság csalás, illetve lopás hatékony bejelentését. 2004-ben a kongresszus elfogadta a személyazonosság lopás büntetési tételének növeléséről szóló törvényt (*Identity Theft Penalty Enhancement Act*), amely növeli azoknak a személyazonosság lopásoknak a büntetési tételét, amelyeket egy másik bűncselekmény elkövetése céljából követnek el. A törvény továbbá kötelezővé teszi a szabadságvesztés büntetést az olyan bizalmi pozícióban lévő alkalmazottakkal illetve egyénekkel szemben, akik személyazonosságlopás elkövetése céljából adatokat loptak. 2008-ban vezették be a Személyazonosság lopással kapcsolatos rendelkezések végrehajtásáról és kárpótlásról szóló törvényt (*Identity Theft Enforcement and Restitution Act*), amely kiterjesztette azoknak a tevékenységeknek a körét, amelyek személyazonosság lopásnak minősülnek, további olyan intézkedéseket vezetett be, amelyek elősegítik az áldozatoktól ellopott vagyon visszaszerzését.

4. Az informatikai elemet tartalmazó bűncselekmények csoportosítása

A fenti részben bemutattam azokat a törvényeket, amelyekben az informatikai elemet tartalmazó bűncselekmények megjelennek. Ebben a részben azokat a deliktumokat tárgyalom, illetve csoportosítom, amelyek az egyes törvényi tényállásokban megjelennek. Az amerikai jogban megjelenő informatikai elemet tartalmazó bűncselekményeket többféleképpen lehet csoportosítani. Az egyik ilyen csoportosítás a számítógép bűncselekményben játszott szerepeit veszi alapul. Eohan Casey[10] a számítógép lehetséges szerepeinek vizsgálatakor egy Donn Parker által összeállított csoportosításra hivatkozik, mely szerint:

- a számítógép fizikai valójában az elkövetés tárgya: ez a helyzet azoknak a bűncselekményeknek az esetében, amikor a számítógép fizikai komponensére követik el a bűncselekményt, pl. ellopják, vagy megrongálják azt. Az informatikai elem ezekben a bűncselekményekben valójában csak esetleges, így ezek a deliktumok nem számítanak számítógépes bűncselekményeknek;
- a számítógépes környezet az elkövetés tárgya azokban az esetekben, amikor az adott bűncselekményt, számítógépes

[10] Eoghan CASEY 2011.: 40.

rendszerre, programra, vagy számítógépben tárolt adatra követik el. Ezek a bűncselekmények a klasszikus számítógépes bűncselekmények pl. a hackelés, a számítógép megfertőzése kártékony programokkal (malware) stb.;

- a számítógépes környezet a bűncselekmény eszköze, amikor az elkövető olyan bűncselekményt követ el információtechnológiai környezetben, amely egyébként számítógép felhasználása nélkül is elkövethető lett volna. Ebbe a körbe tartoznak a tartalommal kapcsolatos bűncselekmények, mint a gyermekpornográfia, illetve a szerzői jog megsértésével kapcsolatos bűncselekmények;
- a számítógép lehet az elkövetés szimbóluma: ez utóbbi esetben a számítógépnek nem kell feltétlenül jelen lennie a bűncselekmény elkövetése során, elkövető csupán arra hivatkozik. A szerző olyan csalást hoz fel példaként, amelyben az elkövető a megtévesztés során arra hivatkozott, hogy hozzáférése van bizonyos speciális számítógépes programhoz.

Véleményem szerint azonban a számítógép bűncselekményben játszott szerepei nem, illetve csak részben szolgálhatnak alapul az informatikai bűncselekmények tényleges csoportosításához. Ha a számítógépek bűncselekményekben játszott szerepeit vennénk alapul maguknak az informatikai bűncselekményeknek a csoportosításában, akkor könnyen azt találnánk, hogy a világ összes bűncselekménye informatikai bűncselekménynek minősül. E tekintetben fontosnak tartom hangsúlyozni, hogy meg kell egymástól különböztetni az információtechnikai elemet tartalmazó bűncselekményeket a szűkebb értelemben vett informatikai bűncselekményektől. Az előbbi csoportosítás utolsó eleme pl., azaz amely szerint a számítógép az elkövetés szimbóluma is lehet, nem olyan ismérv, amely alapján egy bűncselekményt informatikai bűncselekménynek lehetne minősíteni (noha kétségtelen, hogy megjelenik információtechnikai elem). A számítógépre illetve a számítógépes programra való hivatkozás itt csupán igen távoli összefüggésbe vonható a tényleges információtechnológiai környezettel.

Marije T. Britz[11] történeti jellegű csoportosítást használ, s ez alapján két kategóriába sorolja az informatikai elemet tartalmazó bűncselekményeket:

- tradicionális számítógépes bűncselekmények: ezek azok, amelyek a fejlettebb infokommunikációs eszközök szélesebb rétegek számára való elérhetővé válásával egyidőben jelentek meg. Tradicionális számítógépes bűncselekménynek számít a hackelés, a phreaking, az

[11] Marije T. Britz 2013.

alkatrészlopások, valamint a szellemi tulajdon megsértésével kapcsolatos korai bűncselekmények;

- kortárs számítógépes bűncselekmények: ezek megjelenését Britz az internet széles körben való elterjedésének tulajdonítja. A kortárs számítógépes bűncselekmények között 6 alkategóriát különböztet meg, ezek:
  - beavatkozás a számítógép jogszerű működésébe: DOS támadások, kártékony programok (vírusok, férgek) használata, kiberterrorizmus;
  - információlopás és szerzői jogsértés: ipari kémkedés, személyazonosság lopás, személyazonosság csalás;
  - tiltott anyagok terjesztése: gyermekpornográfia, tiltott szerencsejáték, rasszista anyagok;
  - fenyegető kommunikáció: zsarolás, zaklatás, „cyberbullying”;
  - csalás: aukciós csalás, hitelkártyacsalás stb.;
  - kiegészítő bűncselekmények: pénzmosás.

Britz felosztásával az a legfőbb probléma, hogy a technológia rendkívül gyors ütemű fejlődése miatt a határvonal a tradicionális és a kortárs informatikai bűncselekmények között egyre elmosódottabbá válik. A felosztás már a hackelés esetében is kérdéses, hiszen igaz, hogy a jelenség már az 1960-as években jelen volt az Egyesült Államokban, a személyi számítógépek és mobil eszközök rohamos elterjedésével reneszánszát éli a cselekmény. Megjegyzendő továbbá, hogy a csoportosításnál olyan szempontokra lenne szükség, amelyek időállóak és amennyiben lehetséges technológia-semlegesek.

Susan W. Brenner szerint[12] az informatikai bűncselekmények 3 csoportba sorolhatóak:

- azok a bűncselekmények, amelyekben az információs rendszer az elkövetés tárgya (célpontja). Ide tartozik a hackelés, a malware-ek, azaz a kártékony programok terjesztése és a DDoS (vagyis a túlterheléses) támadás;
- azok a bűncselekmények, amelyekben a számítógép az elkövetés eszköze. Ebbe a kategóriába tartozik a számítógépes csalás, a zaklatás, a hamisítás, a terrorizmus, a tiltott szerencsejáték, a rágalmazás, a gyűlöletkeltés és a gyermekpornográfia;
- azok a bűncselekmények, amelyekben a számítógép csak esetlegesen van jelen, vagyis nem a bűncselekmény tárgya és nem is annak eszköze, azonban például értékes bizonyítékok találhatóak rajta. A szerző Melanie McGuire esetét hozza példának, amelyben az

[12] Susan W. BRENNER 2010.: 39.

elkövető egy internetes keresőszolgáltatást használt arra, hogy ismereteket szerezzen arról, hogy *„hogyan kell elkövetni egy gyilkosságot”* és *„hogyan lehet illegálisan lőfegyvert vásárolni*”.[13]

Mivel az utóbbi csoportosítás mutatja a legnagyobb mértékű hasonlóságot az európai – a kiberbűnözésről szóló egyezmény által felállított – rendszerhez, a továbbiakban ezt a csoportosítást használom.

4.1. Bűncselekmények, melyekben az információs rendszer az az elkövetés tárgya

A számítógép kétféle minőségében is lehet az elkövetés tárgya: egyrészt mint a fizikai térben létező tárgy, másrészt mint a virtuális térben létező program. Amennyiben a hardware, azaz a számítógép fizikai térben megjelenő komponense az elkövetés tárgya, nem beszélhetünk valódi informatikai bűncselekményről, hiszen az, hogy a cselekményt egy számítógép „ellen” követték el, még nem olyan különös tulajdonság, ami indokolná az adott deliktumra vonatkozó általános szabályoktól való megkülönböztetést. A rongálás például nem minősül másképp akkor, ha az elkövetési tárgy egy számítógép, mint akkor, ha egy gépjármű, az információtechnológiai jelleg kiemelése ilyen szempontból nem logikus és nem is indokolt.

Informatikai bűncselekményről beszélhetünk ellenben azokban az esetekben, amelyekben az információs rendszer programkörnyezete az elkövetési tárgy, hiszen ezekben az esetekben megkülönböztető elem, hogy a cselekmény a virtuális térben valósul meg és elkövetéséhez speciális szaktudás és eszközkészlet szükséges. Az információs rendszer az elkövetés tárgya az úgynevezett „hackelés” (információs rendszer megsértése), a malware-ek (kártékony programok) terjesztése, illetve a DDoS (túlterheléses) támadások esetén.

4.1.1 Hackelés

Hackelésen, azaz a számítógépes rendszer megsértésén az amerikai szövetségi jog azt érti, ha valaki jogosulatlanul belép egy számítógépes rendszerbe (külsős hackelés – *outsider hacking*), illetve a jogosultsága kereteit meghaladva fér hozzá a rendszer egyes részeihez (belsős hackelés – *insider hacking*). Ez utóbbi eset típuspéldája a vállalat alkalmazottja, aki a rendszer azon részeihez, illetve a rendszerben tárolt olyan adatokhoz fér hozzá, amelyekre egyébként nem lenne jogosult. A szövetségi büntetőjog azonban az egyszerű, további motiváció nélküli

[13] Susan W. Brenner 2010.: 46.

belépést, illetve bent maradást, vagyis az úgynevezett „egyszerű hackelést” (*simple hacking*) nem, illetve csak bizonyos feltételek fennállása esetén kriminalizálja. Susan W. Brenner kiemeli, hogy az egyszerű hackereket *„nem az motiválja, hogy adatlopást, szabotázst, vagy bármilyen más hagyományos bűncselekményt kövessenek el.”*[14] Amennyiben az elkövető a jogosulatlan hozzáférést azért hajtja végre, hogy ezáltal bármilyen egyéb deliktumot elkövethessen, a hackelés puszta eszközcselekménnyé minősül. Az egyszerű hackelést mindössze három esetében rendeli büntetni az U.S. Code, ezek az 1030. § (a)(3) bekezdésében és az 1030. § (a)(5) bekezdésének (B) és (C) pontjaiban találhatóak:

Az 1030. § (a)(3) így szól: *Aki*

- *szándékosan, az Egyesült Államok bármely minisztériumának vagy ügynökségének nem nyilvános számítógépéhez való hozzáférési jogosultság nélkül hozzáfér olyan minisztériumi vagy ügynökségi számítógéphez, amely kizárólag az Egyesült Államok kormányának használatában van; illetőleg*
- *hozzáfér olyan számítógéphez, amelyet az Egyesült Államok kormánya használ, de ez a használat nem kizárólagos és ezzel a tevékenységével befolyásolja a számítógépnek az Egyesült Államok kormánya általi illetve annak érdekében történő alkalmazását*

a (c) bekezdésben meghatározottak szerint büntetendő.

Az 1030. § (a)(5) pedig a következőket mondja:

Aki (B) szándékosan jogosulatlanul fér hozzá védett számítógéphez és tevékenységének eredményeképp gondatlanul kárt okoz; vagy

(C) szándékosan, jogosulatlanul fér hozzá egy védett számítógéphez és tevékenysége eredményeképp kárt vagy veszteséget okoz

a (c) bekezdésben meghatározottak szerint büntetendő.

A fenti tényállások két kulcselemét indokolt bővebben is megvizsgálnunk. Közös elem, hogy a hackelés csak a már korábban tárgyalt „külsős hackelés” esetében minősül büntetendőnek, vagyis abban az esetben, amikor az elkövető nem rendelkezik jogosultságokkal a rendszer tekintetében. A fenti cselekmények tehát a „belsős” elkövető, vagyis az alkalmazottak tekintetében nem minősülnek tényállásszerűnek. Az Egyesült Államok Szenátusának Igazságszolgáltatási Bizottsága[15] több alkalommal is értelmezte, miért indokolt ezen tényállások tekintetében a külsős és a belsős hackelés megkülönböztetése. Az (a)(3) esetében azzal érveltek, hogy a jogalkotó szándékosan nem kriminalizálja azt az esetet,

[14] Cybercrime: Criminal Threats from Cyberspace (Crime, Media, and Popular Culture) 1st Edition 51.
[15] United States Senate Commitee on the Judiciary https://www.judiciary.senate.gov/

amikor egy alkalmazott csupán túllépi a jogosultsága kereteit a saját szervezetén belül. *„Nem nehéz elképzelni olyan alkalmazottat, aki rendelkezik ugyan jogosultsággal egy minisztériumi számítógép tekintetében, azonban elolvas a minisztérium által kezelt olyan adatokat, amelyeket neki nem lenne szabad. Ez különösen igaz ott, ahol a kérdéses szervezetnek nincs egyértelmű módszere arra, hogy elhatárolja, mely személyek milyen adatokhoz jogosultak hozzáférni. A Bizottság ezért úgy hiszi, hogy a közigazgatási szankciók sokkal megfelelőbbek, mint a büntetőjogi szankció*." [16]

Szintén közös elem a tényállásokban, hogy speciális az elkövetési tárgyuk, hiszen az (a)(3) a kormányzati számítógépeket az (a)(5) pedig a védett számítógépeket nevezi meg elkövetési tárgyként. A védett számítógép az amerikai jog szerint tágabb fogalom és magában foglalja a kormányzati számítógépeket is. A U.S. Code szerint *„(e) A védett számítógép olyan számítógépet jelent, amely*

(A) pénzintézet, vagy az Egyesült Államok kormányának kizárólagos használatában áll, illetőleg olyan számítógép, amely nem áll kifejezetten ilyen használatban, de pénzintézet vagy az Egyesült Államok kormánya által vagy annak érdekében használják és a bűncselekményt megvalósító cselekmény befolyásolja a számítógépnek a pénzintézet vagy a kormány általi illetve ezek érdekében történő használatát. Továbbá

(B) amelyet államközi kereskedelemre vagy nemzetközi kereskedelemre, illetve államközi illetve nemzetközi kommunikációra használnak, illetve amelynek a használata érinti ezeket, beleértve azt a számítógépet is, amely az Egyesült Államokon kívül található, azonban olyan módon használják, hogy az hatással van az Egyesült Államok államközi kereskedelmére vagy nemzetközi kereskedelmére, vagy kommunikációjára." Kormányzati számítógépek ehhez képest kizárólag azok a számítógépek, amelyeket kizárólag az Egyesült Államok kormánya használ, illetve amelyeket az Egyesült Államok kormányának érdekében használnak, továbbá azok a számítógépek, amelyek nem állnak ugyan az Egyesült Államok kormányának kizárólagos használatában, de a használatuk befolyásolja a kormányzati illetve az annak érdekében végzett használatot. A fenti körbe tartozó védett számítógépeken való elkövetésen túl a szövetségi jog nem rendeli büntetni a hackelést, tehát a számítógép feltörése magánhasználatú számítógép esetében nem bűncselekmény. Ismét fel kell hívnunk azonban a figyelmet arra, hogy jelen tanulmány kizárólag a szövetségi jogot vizsgálja, az egyes tagállamok helyi büntetőtörvényei kriminalizálják a hackelést a

[16] Charles Doyle 2014.: 4.

magánhasználatban lévő számítógépek esetében is. A tényállások további kulcseleme a szándékosság, vagyis az elkövetőnek tudatában kell lennie annak, hogy jogszerűtlenül fér hozzá egy információs rendszerhez. Brenner szerint a hackelés egyébként is olyan tevékenység, amely magas szintű hozzáértést igényel, így nem követhető el „véletlenül".

4.1.2. Malware

A malware (*malicious software*) az összefoglaló neve a rosszindulatú számítógépes programoknak. A rosszindulatú szoftverek közé tartoznak a trójai programok, vírusok, férgek, kémprogramok (*spyware*), illetve az agresszív reklámok (*adware*). A rosszindulatú számítógépes programok fajtái folyamatos változásban vannak, hiszen folyamatosan újabb és újabb típusok jelennek meg a piacon. Az Egyesült Államok büntetőjoga az európai, köztük a magyar gyakorlattól eltérően a kártékony programok készítését nem kriminalizálja, kizárólag azokat a magatartásokat rendeli büntetni, amelyek az ilyen programok felhasználásával hozhatók kapcsolatba. A U.S. Code 1030 (a)(5) (A) bekezdése alapján a malware terjesztés tényállása a következő: *Aki tudatosan olyan programot, információt, kódot vagy parancsot továbbít, amellyel szándékosan és arra jogosulatlanul kárt okoz egy védett számítógépben a (c) szakasz szerint büntetendő.*[17] A kártékony programok terjesztésének körében érdemel pár szót az úgynevezett elosztott szolgáltatásmegtagadással járó támadás *(distributed denial of service attack – DdoS*), amely különleges a többi malware terjesztést megvalósító cselekményhez képest, hiszen ebben az esetben a fertőzött számítógép és a megtámadott számítógép különböznek. A DDoS támadások esetében az történik, hogy az elkövető kártékony programmal fertőz meg több számítógépet, amelyek ezáltal a „mester" számítógép által irányítható „zombiszámítógépekké" válnak. A zombiszámítógépek csoportját a botnetet az elkövető arra utasítja, hogy a célszámítógép részére adatcsomagokat küldjenek, olyan mértékben, hogy azok túlterheljék a rendszert. A DDoS támadásokkal kapcsolatban felmerülő legnagyobb probléma, hogy a tényleges elkövetőhöz nagyon nehéz egy lépésben eljutni, hiszen magát a rendszer elleni támadást is „vétlen" fertőzött számítógépek hajtják végre, amelyeknek a tulajdonosai ráadásul lehet, hogy nem is érzékelnek semmit abból, hogy a számítógépük fertőzött lett.

[17] Az Amerikai Egyesült Államok Törvénykönyve (Code of Laws of the United States of America). https://www.law.cornell.edu/uscode/text (2016.05. 23.)

4.2. Bűncselekmények, melyekben az információs rendszer az az elkövetés eszköze

Rendkívül színes képet mutatnak azok a cselekmények, amelyekben a számítógép csupán az elkövetés eszközeként van jelen. Ebben a kategóriában megjelennek egyrészt azok az információval való visszaélés jellegű bűncselekmények, amelyeknél a hackelés eszközcselekményként van jelen (számítógépes kémkedés, minősített információkkal való visszaélés, csalás, tiltott jelszó-kereskedelem, illetve a számítógépes zsarolás egyik formája), valamint azok az igen változatos deliktumok, amelyek a számítógép tömeges elterjedése előtt is büntetendőek voltak, a számítógép csak az elkövetés módszerén változtatott. Ez utóbbi kategóriába tartoznak az olyan nem tisztán informatikai jellegű bűncselekmények, mint a személyazonossággal való visszaélés, az internetes zaklatás és zsarolás, a gyermekpornográfia, a szerzői jogsértések. Terjedelmi okokból jelen tanulmány csak a tisztán informatikai jellegű bűncselekményeket vizsgálja részletesen.

4.2.1. A számítógépes kémkedés (computer espionage)

A számítógépes kémkedés tényállása vegyíti a hagyományos kémkedés illetve a számítógépes rendszer megsértésének az elemeit: *Aki (1) jogosulatlanul vagy a jogosultsága kereteit túllépve szándékosan hozzáfér egy számítógépes rendszerhez és e cselekedetével olyan információkat szerez meg, amelyeket az Egyesült Államok kormányának végrehajtási rendelete vagy törvénye szerint – honvédelmi, vagy külkapcsolati okok miatt - védeni kell a jogosulatlan nyilvánosságra hozataltól, vagy olyan adatokhoz fér hozzá, amelyek az 1954. évi atomenergia törvény 11. §-ának y bekezdése által meghatározott bizalmas adatoknak minősülnek, továbbá alappal feltételezhető, hogy az ily módon megszerzett információt fel lehet használni az Egyesült Államok sérelmére, illetve bármely külföldi nemzet előnyére, továbbá ezeket az információkat akaratlagosan olyan személy részére, aki megszerzésükre nem jogosult, közli, továbbítja vagy átadja, hozzájárul ezen információk közléséhez, továbbításához vagy átadásához, illetve az előbbieket megkísérli, vagy aki ezeket az információkat visszatartja és nem adja át őket az Egyesült Államok erre jogosult tisztjének vagy tisztviselőjének, a (c) bekezdésben meghatározottak szerint büntetendő.*[18] A bűncselekmény jogi tárgya kettős, hiszen szerepet játszik egyrészt a honvédelemmel, a külkapcsolatokkal, valamint az atomenergiával kapcsolatos titkosnak

[18] Az Amerikai Egyesült Államok Törvénykönyve (Code of Laws of the United States of America). https://www.law.cornell.edu/uscode/text (2016.05. 23.)

minősülő adatok integritásához és titokban maradásához fűződő érdek, másrészt az Egyesült Államok állambiztonságához fűződő érdek. Az elkövetési tárgy szintén kettős jellegű, hiszen egyrészt maga a számítógép, másrészt a számítógépben tárolt honvédelmi vagy külkapcsolati okok miatt védettnek minősített információ és az atomenergia törvény által bizalmasnak minősített adat is elkövetési tárgyak. Az elkövetési tárgy kapcsán fel kell hívnunk arra figyelmet, hogy a cselekmény csak akkor valósul meg, ha a számítógép valóban tartalmazza a fenti tényállásban meghatározott információkat és az elkövető meg is szerzi ezeket. Az elkövetési magatartások több fordulattal is megvalósíthatók: a megszerzett információk közlésével, továbbításával, átadásával, ezeknek a kísérletével, illetve azáltal, ha az elkövető a megszerzett információkat visszatartja.

4.2.2. Információszerzés jogosulatlan hozzáféréssel (Obtaining Information by Unauthorized Computer Access)

Az egyszerű hackelést követő lépcsőfok az, amikor valaki a jogosulatlan, illetve a jogosultsága kereteit túllépő hozzáférést arra használja, hogy bizonyos védett információkat megismerjen. A törvényszöveg így szól: *Aki (2) szándékosan jogosulatlanul, vagy a jogosultsága kereteit túllépve belép egy számítógépbe és így*

(A) olyan információkat szerez, amelyeket pénzintézet, vagy az e törvény 15. címének 1602. szakasza által meghatározott kártyakibocsátó pénzügyi feljegyzésekben tárol, vagy amelyeket a fogyasztó tájékoztatási ügynökség által a fogyasztóról tárolt fájl tartalmaz, a Fair Credit Reporting Act-nek megfelelően;

(B) információt szerez az Egyesült Államok bármely minisztériumáról vagy ügynökségéről; vagy

(C) információt szerez védett számítógépről

a (c) bekezdésben meghatározottak szerint büntetendő.[19]

A korábban tárgyalt tényállásokkal ellentétben ez a cselekmény már elkövethető a meglévő jogosultság kereteit túllépve, azaz „belsős" elkövetőként is. A tényállás azonban csak azokra az esetekre vonatkozik, amikor az elkövető a tényállásban nevesített védett információkat pusztán megszerzi és a birtokába jutott információkkal nem tesz semmit.

4.2.3 Számítógépes csalás (computer fraud)

A számítógépes csalás tényállása a U.S. Code szerint következő: *Aki, (4) szándékosan, csalási célzattal, jogosulatlanul, vagy a jogosultsága kereteit*

[19] Az Amerikai Egyesült Államok Törvénykönyve (Code of Laws of the United States of America). https://www.law.cornell.edu/uscode/text (2016.05. 23.)

túllépve hozzáfér egy védett számítógéphez és ezáltal végrehajtja a tervezett csalást és bármilyen értékkel bíró dolgot megszerez, kivéve, ha a csalás tárgya, illetve a megszerzett dolog kizárólag a számítógép használatát foglalja magában és a használat értéke egy éves időtartam alatt az 5000 $-t nem haladja meg, a (c) bekezdésben meghatározottak szerint büntetendő. A szakasz érdekessége, hogy az elkövetéshez egyrészt szükséges a csalási célzat már a cselekmény megkezdésekor, másrészt az, hogy az elkövető a hozzáférése során végre is hajtsa a tervezett csalást. „*Az „ezáltal végrehajtja a tervezett csalást*" fordulat azért került a jogszabály szövegébe, hogy kizárja azokat az eseteket, amelyekben a számítógépet csupán nyilvántartási céllal használja az elkövető."[20] Kizárja a bűnösséget a törvény azokban az esetekben is amikor az elkövető csupán kis értékű gépidőt szerez.

4.2.4 Számítógépes zsarolás (Extortion)

Az 1030 § (a) (7) bekezdése rendeli büntetni a számítógépes zsarolást: *Aki azzal a szándékkal, hogy egy személytől pénzt vagy más értékkel bíró dolgot zsaroljon ki, olyan államközi illetve külkereskedelmi kommunikációt folytat, amelyben*

(A) védett számítógép sérelmére elkövetett károkozással fenyeget;

(B) jogosultság nélkül, vagy a jogosultság kereteinek túllépésével védett számítógépen tárolt információ megszerzésével, vagy a védett számítógépről származó jogosultság nélkül, vagy a jogosultság kereteinek túllépésével megszerzett információk bizalmasságának megsértésével fenyeget; vagy

(C) védett számítógépnek okozott kárral összefüggésben pénzt vagy más értékkel bíró dolgot kér vagy követel, amennyiben a károkozásra a zsarolás elkövetése érdekében került sor

a (c) bekezdésben meghatározottak szerint büntetendő.[21]

A (B) valamint (C) pontokban nevesített tényállások 2008-ban az Igazságügyi Minisztérium ajánlását követően kerültek a törvénybe, annak érdekében, hogy az *„azokat az eseteket is lefedje, amelyekben az elkövető már ellopta az információkat és azzal fenyeget, hogy nyilvánosságra hozza őket."*[22] Ezeknek az eseteknek jó példái a hazánkban is elterjedt úgynevezett zsarolóvírusok (*ransomware*). A zsarolóvírusok működési elve, hogy a kártékony program zárol bizonyos fájlokat a számítógépen és a zárolás feloldásáért cserébe azt kéri, hogy

[20] Charles DOYLE 2014.: 52.

[21] Az Amerikai Egyesült Államok Törvénykönyve (Code of Laws of the United States of America). https://www.law.cornell.edu/uscode/text (2016.05. 23.)

[22] Charles DOYLE 2014.: 64.

a tulajdonos meghatározott összeget utaljon át megadott bankszámlára.

4.2.5 Illegális jelszókeresedelem (trafficking in computer access)

Az illegális jelszókereskedelmet akkor rendeli büntetni az amerikai szövetségi büntetőjog, amennyiben arra szándékosan, csalási célzattal kerül sor. A törvény szövege úgy szól, hogy:

Aki … (6) szándékosan, csalási célzattal olyan jelszóval, vagy hasonló információval kereskedik, amely jogosulatlan hozzáférést biztosít egy számítógéphez, amennyiben –

(A) az ilyen kereskedelem hatással van az államközi kereskedelemre vagy a külkereskedelemre; vagy

(B) olyan számítógéphez biztosít hozzáférést, amelyet az Egyesült Államok Kormánya használ, illetve annak érdekében használnak

a (c) bekezdésben meghatározottak szerint büntetendő.[23]

Ez a tényállás a jelszavak és egyéb azonosítók ellopásának és nyilvánosságra hozatalának tömeges elterjedése miatt került be külön a szövetségi büntetőjogba, nem kevés példa van ugyanis arra, hogy a felhasználóktól ellopott adatok tömegesen jelennek meg az interneten. Fel kell hívni a figyelmet azonban arra, hogy a szövetségi szabályok szerint az illegális jelszókereskedelem csak akkor tényállásszerű, ha ez a tevékenység hatással van a tagállamok közötti, illetve a külkereskedelemre, vagy ha az ellopott és kínált azonosító olyan számítógéphez tartozik, amelyet a kormányzat használ, vagy a kormányzati működéssel kapcsolatosan használnak.

4.2.6. Személyazonosság lopás (Identity theft)

„Az amerikai szövetségi jog két személyazonosság lopással kapcsolatos rendelkezést is tartalmaz: a U.S. Code 18. címének 1028(a)(7) szakasza határozza meg a személyazonosság lopás alapesetét, a U.S. Code 18, címének 1028A szakasza pedig a minősített eseteit."[24] A személyazonosság lopás alapesete a következő: *Aki a (c) bekezdésben meghatározott esetekben szándékosan jogosultság nélkül egy másik személyhez tartozó azonosítót átad, birtokol, vagy használ, azzal a szándékkal, hogy olyan jogtalan cselekményt kövessen el, amely a szövetségi jogot sérti, vagy az alkalmazandó tagállami vagy helyi jog szerint bűntettnek minősül, továbbá, aki az ilyen cselekmények*

[23] Az Amerikai Egyesült Államok Törvénykönyve (Code of Laws of the United States of America). https://www.law.cornell.edu/uscode/text Letöltés időpontja: 2016.05. 23

[24] Eoghan CASEY 2011.: 94.

elkövetéséhez segítséget nyújt, illetve ezek elkövetésére felbujt, ezen szakasz (b) bekezdése szerint büntetendő.[25] A rendelkezéssel kapcsolatban ki kell emelni, hogy az azonosítók jogtalan átadása birtoklása és használata önmagában még nem minősül bűncselekménynek. Két további feltétel együttes teljesülése is szükséges: az egyik feltétel, hogy az azonosítók jogtalan kezelésére a (c) bekezdésben meghatározott esetekben (például akkor, amikor úgy tűnik, hogy azt az Egyesült Államok valamely hatósága állította ki) kerüljön sor, másrészt az, hogy a cselekmény a szövetségi vagy a tagállami büntetőjog szerint bűncselekménynek minősüljön.

Az 1028A (a)(1) szakaszban található tényállások a személyazonosság lopás minősített eseteit tartalmazzák. Az (1) azokban az esetekben súlyosabban rendeli büntetni a személyazonosság lopást, ha arra bizonyos bűntettek elkövetése során (többek között az állampolgársággal kapcsolatos, valamint lőfegyverek megszerzésével kapcsolatos esetekben), illetve azokkal összefüggésben kerül sor, a (2) bekezdés pedig a terrorcselekmények vonatkozásában rendeli büntetni ugyanezt.

5. Az informatikai bűncselekmények elleni fellépés szervezetrendszere

Az Egyesült Államokban a rendvédelmi feladatok megoszlanak a tagállami illetve a szövetségi szint között. Tagállami szinten a feladatok tovább osztódnak az egyes kisebb közigazgatási egységek között, így a helyi (önkormányzati vagy városi rendőrség), a megyei (seriff) valamint az állami szint között. A legfontosabb rendvédelmi szervek szövetségi szinten a Belbiztonsági Minisztérium (*Deparment for Homeland Security*), valamint az Igazságügyi Minisztérium (*Department of Justice*) alá tartoznak. A kiberbűncselekmények felderítése és nyomozása szempontjából az alábbi szövetségi rendvédelmi szervek bírnak kiemelkedő jelentőséggel:

1. Belbiztonsági Minisztérium alá tartozó szervek:
   a. Nemzeti Kiberbiztonsági és Kommunikációs Integrációs Központ (*National Cybersecurity and Communications Integration Centre*): A Központ tevékenységének célja, hogy elősegítse a kártékony kibertevékenységek helyzetére vonatkozó információk megosztását, ennek érdekében napi 24 órában üzemelő eseménykezelő és

[25] Az Amerikai Egyesült Államok Törvénykönyve (Code of Laws of the United States of America). https://www.law.cornell.edu/uscode/text (2016.05. 23.)

tudatosság növelő központként funkcionál. A Központ 4 nagyobb szervezeti egységre tagozódik, ezek:

aa) Műveleti és Integrációs Egység (*Operations and Integrations*): ellátja a tervezést, koordinációt, annak érdekében, hogy összehangolja, az elemzéssel, az információ-megosztással, valamint az eseménykezeléssel kapcsolatos feladatokat az egyes ágazatok között;

ab) *United States Computer Emergency Readiness Team*[26]: A CERT feladata, hogy kezelje a jelentősebb eseményeket, elemezze a fenyegetéseket és kritikus kiberbiztonsági információkat cseréljen a világszerte megtalálható megbízható partnereivel. Tevékenysége a következőket foglalja magába:

- a szövetségi szinten működő civil ügynökségek számára biztosítja a megfelelő védelmet, különösen azáltal, hogy felismeri a behatolásokat, illetve megelőzi azokat;
- időszerű és használható információkat nyújt a szövetségi szerveknek és ügynökségeknek, az állami, a helyi és a regionális kormányoknak, a kritikus infrastruktúrák tulajdonosainak és üzemeltetőinek, az ipari szereplőknek és a nemzetközi szervezeteknek;
- kezeli az egyes incidenseket és elemzi azokat az adatokat, amelyek a kiberfenyegetésekre vonatkoznak;
- együttműködik más kormányokkal és nemzetközi jogalanyokkal.

ac) *Industrial Control Systems Response Team*[27]: Feladata a kritikus infrastruktúrák ipari ellenőrzőrendszereit érintő kockázatok csökkentése. Ennek érdekében együttműködik a rendvédelmi szervekkel, a hírszerző szervekkel, koordinálja a szövetségi, állami és helyi kormányok tevékenységét.

ad) *National Coordinating Centre for Communications*[28]: folyamatosan figyelemmel kíséri a nemzeti és nemzetközi incidenseket és eseményeket, amelyek hatással lehetnek vészhelyzeti kommunikációra.

b) Titkosszolgálat (*United States Secret Service*)[29]:

ba) Elektronikus Bűncselekmények Munkacsoport (*Electronic Crimes Task Force*): a Titkosszolgálat az Egyesült Államokon belül 39 ECTF-et működtet. Ezek célja, az elektronikus bűncselekmények megelőzése, felderítése és nyomozása,

[26] https://www.us-cert.gov/
[27] https://ics-cert.us-cert.gov/About-Industrial-Control-Systems-Cyber-Emergency-Response-Team
[28] https://www.dhs.gov/national-coordinating-center-communications#
[29] http://www.secretservice.gov/investigation/#cyber

beleértve a kritikus infrastruktúrák és fizetési rendszerek elleni terrorista támadásokat;

c) A Bevándorlási és Vámhatóság Belbiztonsági Nyomozó hivatala (Immigrations and Customs Enforcement[30] Homeland Security Investigations):

ca) Kiberbűnözési Központ (*Cyber Crimes Centre - C3*): A szervezet fő prioritása, hogy felvegye a küzdelmet az interneten vagy az internet segítségével elkövetett bűncselekményekkel. A C3 *három szervezeti egységből* áll, amelyek a következők:

- Kiberbűnözési Egység (Cyber Crimes Unit): ellátja az ügynökségek informatikai elemet tartalmazó nyomozásainak igazgatását és felügyeletét, azzal, hogy azokra a nemzetközi bűnszervezetekre koncentrál, amelyek információtechnológiai eszközöket használnak a bűncselekmény elkövetése során. Az egység képzéssel, nyomozási támogatással és iránymutatással segíti a kirendeltségek munkáját, valamint szakértelmével hozzájárul az alábbi területeken folytatott informatikai jellegű nyomozásokhoz: személyazonosság csalás, pénzmosás, pénzügyi csalás (beleértve az online fizetési csalást és az internetes szerencsejátékokkal kapcsolatos csalást), kereskedelmi csalás, kábítószer- kereskedelem, illegális exporttevékenység;
- Gyermekek Kizsákmányolása Elleni Nyomozócsoport (*Child Exploitation Investigations Unit*): az egység azokat az elkövetőket üldözi, akik szexuálisan kihasználják a gyermekeket, gyermekpornográfiát gyártanak, reklámoznak vagy terjesztenek, illetve elősegítik a szexturizmust, mindehhez pedig az internetet, vagyis weboldalakat, e-mailt, chatszobákat és fájlcserélőket használnak. Az egység feladatainak ellátása érdekében több rendszert üzemeltet, illetve nemzeti és nemzetközi programokat koordinál:
  - Ragadozó hadművelet (*Operation Predator*): célja a szexuális ragadozók, a gyermekpornográfia készítők, valamint a szexturisták utáni nyomozás;
  - Globális Virtuális Munkacsoport (*The Virtual Global Task Force*): a Csoport nemzetközi szövetség, melynek tagjai rendvédelmi szervek, illetve a magánszektor egyes szereplői. Céljuk, hogy

[30] https://www.ice.gov/cyber-crimes

felvegyék a harcot a gyermekek online szexuális kizsákmányolásával szemben;
- Nemzeti Gyermekáldozat Azonosító Rendszer (*National Child Victim Identification System*): a rendszer célja, hogy segítse a rendvédelmi szerveket az áldozatok azonosításában;
- Áldozatazonosításai program (*Victim Identification Program*): a program célja, hogy azonosítsa és kiemelje azokat a gyermekeket, akik pornográf anyagokban szerepelnek.

○ Igazságügyi Informatikai Egység (*Computer Forensics Unit*): ez a szervezeti egység igazságügyi szakértői tevékenységet végez, és ellátja a sérülékeny digitális bizonyítékokkal kapcsolatos feladatokat. Az egység munkatársai a HSI területi irodában szétszórtan dolgoznak.

2. Igazságügyi Minisztérium alá tartozó szervek:

a) Szövetségi Nyomozóiroda (*Federal Bureau of Investigations* - FBI):

aa) Kibermunkacsoportok (*Cyber Task Forces*)[31]: a munkacsoportok a Szövetségi Nyomozó Iroda 56 területi irodája mellett működnek, céljuk, hogy összehangolják a kiberbiztonság területén a helyi és a szövetségi szintű fellépést. Reagálnak az egyes incidensekre és sértett-alapú nyomozásokat folytatnak, ezen felül feltérképezik és kezelik a fenyegetéseket, sérülékenységeket, valamint kapcsolatot tartanak a fontosabb vállalatokkal, közintézményekkel és egyéb szereplőkkel.

6. Összegzés

Az Egyesült Államokban az informatikai bűncselekmények szabályozása, valamint az informatikai bűncselekmények megelőzése és a velük szemben való fellépés jóval részletesebben szabályozott, mint hazánkban. Ennek egyik indoka, a tagállami és a szövetségi szintű jogalkotás, illetve a rendvédelem elválnak egymástól. Azonban ha pusztán a szövetségi szintű rendelkezéseket vizsgáljuk, akkor is azt találjuk, hogy a tényállások mind számban, mint összetettségükben megelőzik a hazai rendelkezéseket. Az Egyesült Államok jelenleg hatályos jogszabályaira nagy hatással volt az esetjog, így kimondhatjuk, hogy olyan szabályozásról beszélünk, amelyet gyakorlati tapasztalatok mentén, a gyakorlatban felmerült szabályozási

[31] https://www.fbi.gov/about-us/investigate/cyber/cyber-task-force-fact-sheet

igényeknek megfelelően alakítottak ki. A csekély számú magyar bírósági ítélet tükrében ez azonban hazánkról nem mondható el.

Felhasznált irodalom

Susan W. BRENNER: Cybercrime: Criminal Threats from Cyberspace (Crime, Media, and Popular Culture) 1st Edition, 2010.

Marije T. BRITZ: Computer Forensics and Cyber Crime, Third Edition, Pearson 2013.

Eoghan CASEY: Digital Evidence and Computer Crime, 3rd edition, Academic Press, 2011.

Charles DOYLE: Cybercrime: An Overview of the Federal Computer Fraud and Abuse Statute and Related Federal Criminal Laws. Congressional Research Service. 2014.: https://www.fas.org/sgp/crs/misc/97-1025.pdf (2016.05. 23.)

***

Combatting cybercrime in the United States
Summary

The United States was among the first countries that realized the significance of information technology in the development of criminal activities, therefore when one researches the origins of cybercrime legislation the close examination of the United States cybercrime laws is of paramount importance. The aim of this study is to provide a summary of the offences that constitute a cybercrime in the U.S. and to identify those law enforcement agencies that's main task is to prevent and investigate criminal activities related to information technology.