Vírusok és zombik a büntetőjogban

Az információs rendszer és adatok megsértésének büntető anyagi és eljárásjogi kérdései

SORBÁN KINGA*

1. Bevezetés

A kiberbűnözés napjainkban már nem csupán olyan jelenség, amelyet a hollywoodi filmek világából ismerünk, a hírekben egyre gyakrabban jelennek meg információs rendszereket érintő komoly támadások, amelyek között egyre sűrűbben lehet hallani magyar vonatkozású esetekről is. A 2017 májusában lezajlott világméretű zsarolóvírus-támadás Magyarországot is érintette, a Kormányzati Eseménykezelő Központ májusban adott ki riasztást a kártevő gyors terjedése miatt,[1] a Hvg.hu cikke szerint a WannaCry zsarolóvírussal mintegy 45 magyar állami szerv rendszerei fertőződtek meg,[2] s a támadás hatásait az átlagfelhasználók is megtapasztalhatták. Hasonlóan nagy port kavart 2017 júniusának végén a Petya nevű zsarolóvírus,[3] amely szintén elérte a magyar felhasználók számítógépeit.

Egyre jelentősebbek a botnethálózatok felhasználásával elkövetett elosztott túlterheléses támadások (DDoS) is – a Symantec 2015-ös jelentésében hazánk a globális botfertőzöttségi lista 5. helyén szerepelt.[4] 2017 novemberében a Magyarországi Szcientológia Egyház weboldalát érte túlterheléses támadás,[5] az Index.hu pedig 2016 májusában számolt be magyar kormányzati szolgáltatások megtámadásáról.[6] A felsorolás természetesen csak példálózó jellegű, a Symantec 2018-as jelentése már a második helyre sorolja Magyarországot az e-mailben terjedő *malware*-ek számát tekintve, a jelentés szerint minden 108 e-mailből egy *malware*-t tartalmaz,[7] vagyis a jelenség jóval nagyobb volumenű, mint amiről a sajtó beszámol.

* PhD-hallgató, Eötvös Loránd Tudományegyetem, Állam- és Jogtudományi Doktori Iskola. E-mail: kinga.sorban@gmail.com

1 http://neih.gov.hu/wannacry-20170513

2 http://hvg.hu/tudomany/20170516_wannacry_zsarolovirus_magyar_fertozesek

3 http://hvg.hu/tudomany/20170629_petya_zsarolovirus_fertozottsegi_terkep_magyarorszag

4 https://www.symantec.com/content/en/us/enterprise/other_resources/21347933_GA_RPT-internet-security-threat-report-volume-20-2015.pdf

5 http://hvg.hu/tudomany/20171101_ddos_tulterheleses_tamadas_hackertamadas_magyar_szcientologia_egyhaz

6 https://index.hu/tech/2016/05/06/tobb_kormanyzati_szolgaltatast_tamadtak_a_hekkerek/

7 https://www.symantec.com/security-center/threat-report

Az információs rendszereket érintő támadások esetében kulcsfontosságú szerepe van a megelőzésnek, amiről a kiberbiztonság kapcsán számtalanszor hallunk. A védekezés szükségességének hangsúlyozása mellett azonban kevés szó esik arról, hogy mi történik, ha már megtörtént a baj. Annak ellenére, hogy Magyarország a *malware*-fertőzöttség tekintetében élen jár, az informatikai bűncselekmények leírására használt fogalmak még a szakirodalomban sem bírnak azonos jelentéssel, márpedig az eredményes fellépés érdekében nagyon fontos, hogy a használatban lévő kifejezéseket egységes jelentéstartalommal kezeljük. Ezért tanulmányom első felében igyekszem rendszerezni és elhatárolni az informatikai bűncselekmények leírására szolgáló kifejezéseket. Noha manapság a legtöbb bűncselekmény nyomozása során megjelenik az eljárásban valamilyen technikai elem – gondoljunk csak a híváslisták és a cellainformációk ellenőrzésére –, az információs rendszer vagy adat megsértésével kapcsolatos bűncselekmények már a nyomozás szakaszában speciális, gyakran nemzetközi kezelést igényelnek. A tanulmány másik célja a szűken értelmezett informatikai bűncselekmények (az információs rendszer vagy adat megsértése, az információs rendszer védelmét biztosító technikai intézkedés kijátszása) nyomozásával kapcsolatos speciális eljárási kérdések bemutatása. Mivel 2018-ban hatályba lépett az új büntető-eljárási kódex, bemutatom, hogy a megújuló szabályok milyen lehetőségeket nyitnak meg az ilyen ügyek nyomozásában, illetve milyen kihívásokkal kell szembenézniük a jövőben a nyomozó hatóságok tagjainak.

2. Informatikai bűncselekmények szűk értelemben

Az eljárási kérdések vizsgálata előtt elsősorban azt tartom fontosnak tisztázni, mit ért jelen tanulmány informatikai bűncselekmény kifejezés alatt. Ez idáig sem a gyakorlat, sem a jogalkotás nem dolgozott ki egységes terminológiát az informatikai bűncselekmény fogalmának meghatározására, sőt még a témával foglalkozó egyetemi jegyzet is arról tesz említést, hogy nem alakult ki általánosan elfogadott fogalomrendszer e bűncselekményi kör leírására.[8] A szakirodalomban számtalan fogalom kering az információtechnikai elemet tartalmazó bűncselekményekkel kapcsolatban, a legtöbb szerző azonban nem azonos tartalommal használja az egyes kifejezéseket. Noha a témával hatalmas mennyiségű külföldi és egyre bővülő magyar szakirodalom is foglalkozik, az informatikai bűncselekményekkel kapcsolatban felmerülő fogalmak a mai napig meglehetősen tisztázatlanok, az egyes kifejezések elhatárolása pedig nem mutat egységes képet. A terminológiai káosz mellett az is problémát jelent, hogy az információtechnológiai elemet tartalmazó cselekmények köre gyorsabban változik, mint ahogyan arra a jogalkalmazás reagálni tudna: egyes bűncselekmények egyszerűen 'kimennek a divatból', mások elkövetése az új technikák elérhetővé válása miatt átalakul. A tanulmány e része a következő terminusok jelentését és egymáshoz való viszonyát tárgyalja: „számítógépes bűncselekmény", „számítógéppel kapcsolatos bűncselekmény", „informatikai bűncselekmény", „kiberbűncselekmény", „digitális bűncselekmény", „e-bűncselekmény", „csúcstechnológiás bűncselekmény".

[8] Simon Béla: *Csúcstechnológiai bűnözés és nyomozása: egyetemi jegyzet.* Budapest, Nemzeti Közszolgálati Egyetem, Rendészettudományi Kar, 2012. 9.

2.1. A számítógépes bűncselekmény *(computer crime)*

Marjie Britz a számítógépes bűncselekményeket általános fogalomként használja, és minden olyan bűncselekményt idesorol, amelyet számítógép használatával követtek el.[9] A számítógépes bűncselekmény fogalmát kiterjesztően értelmezi, így ideérti azokat a cselekményeket, ahol az információs rendszer vagy adat az elkövetés tárgya, és azokat is, amelyekben az információs rendszer az elkövetés eszköze. Hasonlóan értelmezi a számítógépes bűncselekmény fogalmát Eoghan Casey,[10] aki egzakt definíciójával nem szolgál, de könyvében jelzi, hogy a számítógépes bűncselekmény kategória nem vonatkoztatható minden olyan cselekményre, amelyben információtechnológiai elem kap szerepet, kizárólag azokra, amelyek szorosabb kapcsolatot mutatnak a számítógépes környezettel, tehát amelyekben a számítógép a bűncselekmény eszköze vagy tárgya.

A magyar jogirodalomban az előbbiekben említett külföldi szerzőkhöz hasonló fogalmat dolgozott ki Szabó Imre, aki úgy határozta meg a számítástechnikai bűncselekményeket, mint azok a „deliktumok, melyek egy számítógépes rendszerrel vagy számítástechnikai adattal kapcsolatba hozhatók, akár úgy, hogy az elkövetés eszközeként jelennek meg, vagy pedig a bűncselekmény elkövetési tárgyát képezik".[11] Azokat a cselekményeket, amelyeknek az információs rendszer, illetve adat az elkövetési tárgya, tisztán informatikai bűncselekményeknek is nevezzük, ami arra utal, hogy ezek a cselekmények kizárólag a virtuális térben értelmezhetők.

Azok a cselekmények, amelyekben a számítógép az elkövetés eszköze, csak másodlagos jelleggel minősülnek számítógépes bűncselekménynek, mivel itt a számítógép nem feltétele az elkövetésnek, hanem egy azt megkönnyítő eszköz, illetve közvetítő csatorna. Ezekben az esetekben a cselekmények nem köthetők kizárólagosan a virtuális térhez, ugyanúgy elkövethetők a való/fizikai világban is. Az ide tartozó cselekmények rendkívül színes képet mutatnak – lehetnek tartalommal kapcsolatos bűncselekmények, mint a szerzőijog-sértések vagy a gyermekpornográfia, illetve egy adott személy vagy csoport sérelmére elkövetett cselekmények (gyűlöletkeltés, zaklatás, rágalmazás, becsületsértés).

2.2. Számítógéppel kapcsolatos bűncselekmény *(computer related crime)*

A szakirodalomban gyakran bukkan fel a számítógéppel kapcsolatos bűncselekmény fogalma is, amely hasonlósága ellenére nem fedi teljesen az előbbiekben ismertetett számítógépes bűncselekmény fogalmát. E körben elsőként ismét a Britz által meghatározott fogalmat vehetjük irányadónak,[12] amely szerint számítógéppel kapcsolatos minden olyan bűncselekmény, melyben a

[9] Marjie T. Britz: *Computer Forensics and Cyber Crime: An Introduction.* London, Pearson, 2013. 3. kiadás, 6.

[10] Eoghan Casey: *Digital Evidence and Computer Crime.* Amsterdam, Elsevier, 2012. 3. kiadás, 37.

[11] Szabó Imre: Informatikai bűncselekmények. In: Dósa Imre (szerk.): *Az informatikai jog nagy kézikönyve*. Budapest, CompLex, 2008. 547.

[12] Britz i. m. (9. lj.) 6.

számítógép bármilyen módon, akár közvetetten is jelen volt. Ebbe a kategóriába is beletartoznak a számítógépes bűncselekmények, továbbá azok a cselekmények is, amelyekhez a számítógép jelenléte csupán esetlegesen kapcsolódik. Jó példa erre az, amikor emberrablásnál az elkövetők e-mailben követelnek váltságdíjat. Látjuk, hogy itt magából a cselekményből, vagyis a személyes szabadság megsértéséből csak nagyon hosszú logikai láncon keresztül lehet arra a következtetésre jutni, hogy számítógépes bűncselekmény történt.

Az információs rendszerek manapság már a legtöbb büntetőeljárás során fontos bizonyítékkal szolgálhatnak a hatóság számára: az elkövető IP-címének ismeretében könnyebben azonosítható a gyanúsított, a cellainformációk segíthetnek a terhelt és a helyszín összekapcsolásában. A számítógéppel kapcsolatos bűncselekmény kategóriáját Britzcel azonosan határozza meg Casey is.[13] A magyar jogirodalomban már nem ennyire egyértelmű a fogalom jelentése. Siegler Eszter ugyan megkülönbözteti a számítógépes bűncselekmények és a számítógéppel kapcsolatos bűncselekmények fogalmait, jóval szűkebben értelmezi őket, mint külföldi kollégái.[14] Siegler számítógéppel kapcsolatos bűncselekmények alatt kizárólag azokat a cselekményeket érti, amelyeknél a számítógép az elkövetés eszköze vagy elkövetési tárgy, a számítógépes bűncselekmény fogalmát pedig szűkítően, kizárólag azokra a deliktumokra alkalmazza, amelyek kifejezetten számítógépes rendszer és adatok ellen irányulnak (tehát ahol a számítógépes rendszer mint elkövetési tárgy van jelen).

2.3. Informatikai bűncselekmény, információs rendszerrel kapcsolatos bűncselekmény

Az informatikai bűncselekmény nem új keletű fogalom, Nagy Zoltán András már 1991-ben használta.[15] A magyar jogrendszerben a 2012. évi Büntető törvénykönyv[16] (a továbbiakban: Btk.) lecserélte a számítógép fogalmát – nagyon helyesen – az információs rendszerére, ennek következtében a számítógépes bűncselekmény fogalma is némiképp kikopott a szóhasználatból, átadva helyét az informatikai bűncselekmény, információs rendszerrel kapcsolatos bűncselekmény, illetve a későbbiekben tárgyalt kiberbűncselekmény fogalmaknak. A Btk. megújult fogalomhasználatának hátterében az áll, hogy a köznyelvi számítógép-fogalom az eszközöknek viszonylag szűk körére, a személyi számítógépekre értendő, ugyanakkor a tárgyalt bűncselekmények tárgyai, illetve eszközei lehetnek az olyan információtechnológiai eszközök is, mint a táblagépek, az okostelefonok, a nyomtatók vagy az adattovábbítást és a kapcsolatfelvételt biztosító műszaki berendezések (pl. a hálózati forgalmat irányító routerek). Az információs rendszer kifejezés magába foglal minden, az adatok automatikus feldolgozását, kezelését, tárolását, továbbítását biztosító berendezést vagy az egymással kapcsolatban lévő ilyen berendezések összes-

[13] Casey i. m. (10. lj.) 37.

[14] Siegler Eszter: A számítógéppel kapcsolatos és a számítógépes bűncselekmények. *Magyar Jog,* 1997/12., 736–742.

[15] Nagy Zoltán András: Az informatika és a büntetőjog. *Magyar Jog,* 1991/1., 21–26.

[16] 2012. évi C. törvény a Büntető törvénykönyvről.

ségét, tehát a végpontokat és a hálózatot egyaránt. A Btk. az információs rendszer fogalmat azonban a korábbi számítástechnikai rendszer fogalommal azonos tartalommal definiálja, ezért a számítógéppel és az információs rendszerrel kapcsolatos bűncselekmény fogalmak lényegében szinonimaként értelmezhetők. Pusztán utalás szinten említendő, hogy az informatika és a számítástechnika kifejezések jelentéstartalma nem teljesen azonos, ez a különbség azonban jogi szempontból elhanyagolható.

2.4. Kiberbűncselemény *(cybercrime)*

Napjainkban igen divatos, mégis nehézkesen értelmezhető kifejezés a kiberbűncselekmény. Sokan az informatikai bűncselekmény, illetve a számítógépes bűncselekmény fogalmával szinonim értelemben használják a fogalmat, amely az angolszász *cybercrime* kifejezés nyomán honosodott meg a magyar nyelvben. A másik értelmezés szerint azonban a kiberbűncselekmény kizárólag azokra a számítógépes bűncselekményekre vonatkozik, amelyekben valamilyen módon megjelenik az információs rendszereket összekötő hálózat (például az internet). Britz a kifejezést azokra a deliktumokra használja, amelyeket a hálózatban az internet felhasználásával követtek el. Röviden Casey is utal arra, hogy a kiberbűncselekmény kategória a számítógépes hálózatot érintő cselekményekre értendő.[17] Susan W. Brenner ugyan nem nevesíti közvetlenül a hálózatot mint az elkövetés eszközét, a kiberbűncselekmény lényegének meghatározásakor kiemeli, hogy ezeknél a cselekményeknél a kibertér (a számítógépeket összekötő virtuális közeg) válik a cselekmény elkövetésének eszközévé vagy tárgyává.[18] A számítógépes bűnözésről szóló budapesti egyezmény (a továbbiakban: Cybercrime-egyezmény) is a *cybercrime* kifejezést használja, a fogalom normajellegű definíciójának megalkotásával azonban adós maradt. Az egyezmény preambuluma mindazonáltal több esetben kiemeli a számítógépes hálózatok szerepét a modern bűnözésben. Ennek ellenére az ott felsorolt bűncselekmények elkövetése – noha jellemzően valóban hálózaton keresztül valósul meg – nem elképzelhetetlen offline környezetben sem, így kijelenthetjük, hogy ezen a területen is szükség lenne a fogalmak tisztázására és esetleges újragondolására. A fogalom tisztázatlanságának problémájára remekül rávilágít az Egyesült Nemzetek Szervezete (ENSZ) 2013-ban készült átfogó tanulmánya,[19] amelynek hátteréül egy kiterjedt kérdőíves kutatás szolgált. A tanulmány szerint a felmérésben részt vevő országok kevesebb mint 5%-a használja a *cybercrime* kifejezést, inkább a számítógépes bűncselekmény, az elektronikus bűncselekmény és a csúcstechnológiás bűncselekmény fogalmak elterjedtebbek. A fogalmat még azok az országok sem határozták meg, amelyek egyébként jogszabályi szinten is alkalmazzák a kiberbűncselekmény kifejezést, a tanulmány szerint az elemzett jogforrások többnyire definiálás helyett csupán utaltak a jogszabályban meghatározott bűncselekmények körére.

[17] Casey i. m. (10. lj.) 37.

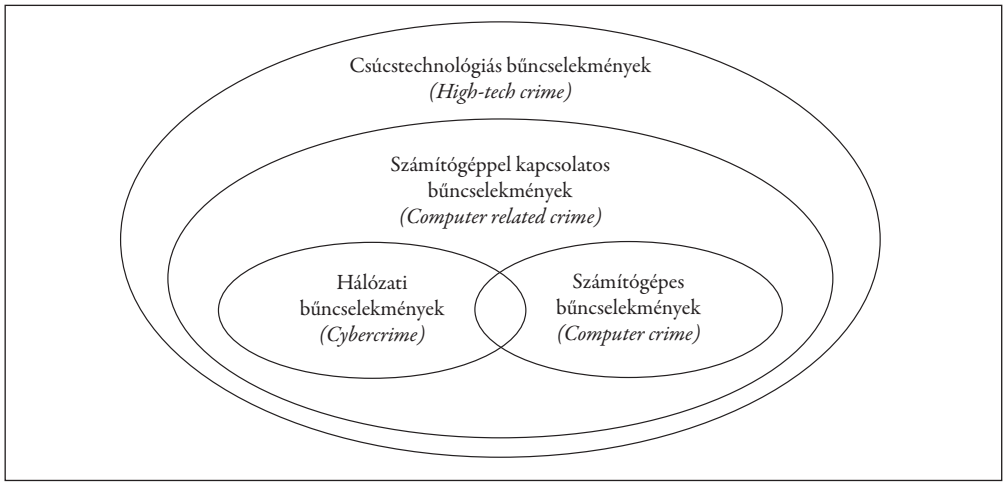
[18] Susan W. Brenner: *Criminal Threats from Cyberspace*. Santa Barbara, Praeger, 2010. 39.

[19] http://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf

2.5. Digitális bűncselekmény, e-bűncselekmény és csúcstechnológiás bűncselekmény *(digital crime, e-crime, high-tech crime)*

Pusztán a teljesség kedvéért indokolt utalni arra, hogy számos egyéb fogalom is létezik a számítógépes bűncselekmények leírására, ezek azonban kevésbé elterjedtek. Britz a digitális bűncselekmény fogalmat azokra a cselekményekre alkalmazza, amelyek az elektronikusan tárolt adatokhoz kapcsolódnak, tehát amelyekben az adatokhoz való jogosulatlan hozzáférés, adatok jogosulatlan terjesztése, megváltoztatása, törlése történik, akár hálózaton keresztül, akár offline formában. Az *e-crime* fogalommal főleg az Egyesült Királyságban találkozhatunk, ahol a rendőrfőnökök egyesületének (Association of Chief Police Officers) *e-crime*-stratégiája úgy definiálja, mint a hálózatba kötött számítógépek vagy az internet használata bűncselekmények elkövetésére vagy a bűncselekmény elkövetésének megkönnyítésére.[20] Az *e-crime* tehát lényegében a kiberbűncselekménnyel azonos. Jóval nehezebb dolgunk van a csúcstechnológiás bűncselekmények fogalmának definiálásával, erre ugyanis nem találhatunk meghatározást a szakirodalomban. Azt, hogy mégis bevett és használatban lévő kifejezésről van szó, mutatja, hogy az Europol honlapja is külön kategóriaként nevesíti ezeket a cselekményeket,[21] illetve a Budapesti Rendőrfőkapitányság szervezetén belül is megtalálható az úgynevezett Pénzhamisítási és Csúcstechnológiai Bűnözés Elleni Osztály.[22] A csúcstechnológiás bűncselekmény kategóriába tartozik minden olyan offline vagy online környezetben elkövetett cselekmény, amelyben az elkövetés eszköze vagy az elkövetés tárgya a tudomány mai állása szerint a technológia élvonalába tartozik. Ez tehát a legtágabb fogalom, tartalma viszont meglehetősen relatív, hiszen a tudomány és a technológia folyamatos fejlődésben, változásban van. Az egyértelműség kedvéért jelen tanulmány az egyes fogalmakat az alábbi ábra szerinti értelmezésben alkalmazza:

1. ábra



[20] http://library.college.police.uk/docs/acpo/Ecrime-Strategy-2009.pdf

[21] https://www.europol.europa.eu/crime-areas-and-trends/crime-areas/cybercrime

[22] http://www.police.hu/sites/default/files/szervezeti_felepites_pdf/BRFK%20%C3%A1grajz%20A3%20
2017.02.01.pdf

3. Információs rendszerrel kapcsolatos bűncselekmények a Btk.-ban

A tisztán számítógépes bűncselekményeket a Btk. két fejezetben, négy szakaszban tárgyalja. A XLIII. fejezet szól a tiltott adatszerzésről, valamint az információs rendszer elleni bűncselekményekről, így az információs rendszer vagy adat megsértéséről, valamint az információs rendszer védelmét biztosító technikai intézkedés kijátszásáról. A XXXVI., vagyon elleni bűncselekményekről szóló fejezetben kapott helyet az információs rendszer felhasználásával elkövetett csalás (375. §), ami lényegében az információs rendszer vagy adat megsértésének károkozással járó alakzata. A fenti rendelkezések 2004 óta képezik a magyar jog részét – Magyarország ekkor ratifikálta az Európa Tanács 2001. november 23-án Budapesten elfogadott, a számítástechnikai bűnözésről szóló egyezményét,[23] aminek alapján kötelezettséget vállalt arra, hogy megalkotja a megfelelő jogszabályokat az egyezményben meghatározott cselekmények kriminalizálása érdekében.

Az előbbiekben nevesített nemzetközi egyezmény mellett röviden szólnunk kell az uniós jogról is, hiszen az Európai Unió tagjaként hazánk jogrendszerének is szerves részét képezik az uniós normák. Az Európai Parlament és a Tanács 2013/40/EU irányelve (2013. augusztus 12.) az információs rendszerek elleni támadásokról és a 2005/222/IB tanácsi kerethatározat felváltásáról lényegében a Cybercrime-egyezménnyel azonos szabályokat fektet le. Az irányelv, sok egyéb európai uniós normához hasonlóan, a *minimumharmonizáció* elvét követi, vagyis a tagállamok annak szabályainál részletesebb, illetve szigorúbb szabályokat szabadon megállapíthatnak. Jelen tanulmány szempontjából az információs rendszer vagy adat megsértése tényállásának van jelentősége, amiről a Btk. 423. §-a rendelkezik. Az e szakasz által kriminalizált elkövetési magatartások köznyelvi elnevezése általában sokkal beszédesebb – ezek a bekezdések szabályozzák a hekkelést, a kártékony szoftverek, például vírusok terjesztését, a botnethálózatok kiépítését és a túlterheléses támadásokat. A Btk. 423. §-a által szabályozott tényállás valójában háromféle elkövetési magatartással is megvalósítható, ezek:

– az információs rendszerbe történő jogosulatlan belépés[24] [(1) bekezdés],
– a rendszer működésének akadályozása [(2) bekezdés *a)* pontja], valamint
– az információs rendszerben tárolt adatokkal végzett jogosulatlan műveletek [(2) bekezdés *b)* pontja].[25]

E bekezdés szövegén látszik, hogy a technológiasemlegesség jegyében fogalmazták meg, így az alkalmazott technológiától és az elkövetés módszerétől függetlenül büntetendő minden olyan magatartás, amely a meghatározott eredményre vezet.

A 9/2012. számú büntető elvi döntés szerint a „védett jogi tárgy a számítástechnikai rendszerek működéséhez, a bennük tárolt, feldolgozott, továbbított adatok megbízhatóságához, va-

[23] Az egyezményt Magyarországon a 2004. évi LXXIX. törvény hirdette ki.

[24] „Aki információs rendszerbe az információs rendszer védelmét biztosító technikai intézkedés megsértésével vagy kijátszásával jogosulatlanul belép, vagy a belépési jogosultsága kereteit túllépve vagy azt megsértve bent marad, vétség miatt két évig terjedő szabadságvesztéssel büntetendő."

[25] „(2) Aki *a)* az információs rendszer működését jogosulatlanul vagy jogosultsága kereteit megsértve akadályozza, vagy *b)* információs rendszerben lévő adatot jogosulatlanul vagy jogosultsága kereteit megsértve megváltoztat, töröl vagy hozzáférhetetlenné tesz, bűntett miatt három évig terjedő szabadságvesztéssel büntetendő."

lamint titokban maradásához fűződő érdek". Az információs rendszer rendeltetésszerű működésének akadályozására a modern technológia állása szerint különösen alkalmasak a különféle kártékony programok, ezért a 423. §-ban szabályozott cselekmény két legtipikusabb elkövetési magatartása a *malware*-, illetve a botnettámadás. A régi Btk.[26] *Kommentár*ja a számítástechnikai rendszer megsértésének egyik eszközeként a számítógépes vírusokat említi.[27] A számítógépes vírus azonban csak egyike azoknak a kártékony programoknak *(malware),* amelyek alkalmasak a számítógép működésének kedvezőtlen befolyásolására. A kártékony programok közös jellemzője, hogy olyan szoftverek, amelyek akadályozzák a számítógép működését, illetve korlátozzák a rendeltetésszerű használatát. A legismertebb *malware*-fajták az alábbiak.[28]

– Vírus *(virus):* vírusnak nevezzük azokat a szoftvereket, amelyek képesek a felhasználó tudta nélkül egyik számítógépről a másikra, vagy akár ugyanazon a gépen belül több helyre észrevétlenül reprodukálódni. Általában fertőzött program segítségével terjednek. A vírusok csoportosításának egyik lehetséges módszere a fertőzött alrendszerek, illetve programok szerinti csoportosítás. Ezek alapján megkülönböztethetjük az alábbi vírustípusokat:
  = programvírusok *(file-infector virus):* a programvírusok bináris futtatható (pl. exe) fájlokba ágyazódnak. Népszerűek mostanában az úgynevezett zsarolóvírusok *(ransomware),* amelyek a rendszert megfertőzve állományokat titkosítanak, és csak akkor adják meg a feloldáshoz szükséges kódot, ha a felhasználó átutalt egy megadott számlaszámra bizonyos összeget. Magyarországon 2013-ban egy zsarolóvírus került a figyelem középpontjába,[29] amely a fertőzést követően azt az üzenetet jelenítette meg a sértett számítógépének képernyőjén, hogy a „Magyar Rendőrség Osztály Elleni Kiberbűnözés" *(sic!)* zárolta a komputert, mivel illegális tartalmak találhatók rajta, a titkosítás feloldásáért pedig meghatározott összeg befizetését kérte.
  = adatfájlokban lévő vírusok: idetartoznak a makrovírusok, valamint az érvénytelen fájlformátumot kihasználó vírusok. A makrovírusok olyan vírusok, amelyek a Microsoft Office programjaiba ágyazódva különböző kártékony hatásokat fejtenek ki. Az érvénytelen fájlformátumra épülő vírusok azoknak a programoknak a hibáit használják ki, amelyek egy-egy meghatározott fájlformátummal dolgoznak.
– Féreg *(worm):* a féreg olyan önmagában működő szoftver, amely képes önmagát reprodukálva egyik számítógépről a másikra terjedni. Abban különbözik a vírustól, hogy önmagában is működik és életképes, nem kapcsolódik egyéb szoftverekhez. Az önsokszorosításon kívül a féreg számtalan dologra programozható – ezek a másodlagos funkciók a *payload.*
– Trójai faló *(trojan horse):* trójai szoftvereknek nevezzük azokat a kártékony szoftvereket, amelyek magukat általában ártalmatlan vagy segítő célú szoftvernek álcázva települnek fel a számítógépre. Hasonlóan a számítógépes férgekhez, a rendszerbe kerülésüket követően

[26] 1978. évi IV. törvény a Büntető Törvénykönyvről.

[27] Varga Zoltán (szerk.): *Nagykommentár a Büntető törvénykönyvről szóló 1978. évi IV. törvényhez*. Budapest, KJK–KERSZÖV, 2004.

[28] A csoportosítás és a fogalommagyarázat a http://www.cert-hungary.hu/tudatosito-anyagok felhasználásával készült.

[29] http://hvg.hu/tudomany/20130218_Rendorsegi_virus_miatt_nyomoz_a_rendorseg

számtalan dologra programozhatók, például a számítógépen található állományok titkosítására, zombiszámítógép létrehozására, személyes adatok összegyűjtésére és elküldésére, a felhasználó webkamerájának használatára, az operációs rendszer távoli használatára stb.
– *Rootkit:* olyan szoftvereszközök, amelyek elrejtenek egyes folyamatokat vagy adatokat az operációs rendszerben, vagy hozzáférést tesznek lehetővé bizonyos alrendszerekhez vagy programokhoz.
– Hátsó ajtó *(backdoor):* olyan program, amely a felhasználó tudta nélkül távoli hozzáférést tesz lehetővé. Ezek a programok általában egy előre meghatározott TCP- vagy UDP-portot nyitnak, amelyre az elkövető rácsatlakozhat.
– Kémprogram *(spyware):* célja a számítógépről információ megszerzése. Lehet webalapú, mint egy káros weboldal, települhet is webről, de megeshet, hogy maga az ártani kívánó fél telepíti fel a gépre [pl. billentyűleütés-naplózó program *(keylogger),* amely megjegyzi az összes leütött billentyűt].
– Kéretlen reklám *(adware):* olyan szoftver, amely automatikusan reklámokat jelenít meg. Bár ez nem következik a definíciójából, általában negatív értelemben használják a jelzőt olyan programokra, amelyeket nem szívesen látunk a számítógépen. Ilyennek minősülhet akár legális szoftver is, mint például egy másik szoftverrel feltelepült böngészőeszköztár *(toolbar).*

Az előbbiekben felsorolt kártékony programok általában nem egymástól elhatárolhatóan működnek, az előbbi kategóriák a mai környezetben inkább az egyes programfunkciók leírására szolgálnak. Egy-egy kártevő több funkció ellátására is programozható, így valójában a modern *malware*-ek esetében a fentiek valamilyen csomagba szerkesztett változatát jelentik.

A magyar jogrendszerben nem nevesítik külön, az európai büntetőjogi gondolkodásban azonban kiemelt figyelmet kapnak az úgynevezett botnethálózatok. A botnet a robot és a network szavak összekapcsolásából ered, és vírussal fertőzött számítógépek hálózatára utal, amelyeket az elkövető(k) távolról küldött utasítások sorozatán keresztül képes(ek) irányítani, ezáltal tömegesen felhasználni bűncselekmények elkövetéséhez. A botnettámadások jelentősége abban áll, hogy tipikusan nem az egyéni felhasználók, hanem kritikus infrastruktúrák, nagyvállalati rendszerek ellen irányulnak, és komoly károkat tudnak okozni. A botnet kifejezést európai uniós dokumentumban először 2006-ban említik. A spamekről szóló közleményében az Európai Bizottság a kéretlen üzenetek küldésére szolgáló eszközként jellemezte a botnethálózatokat. A 2007 májusában kiadott, a kiberbűncselekmények elleni fellépés általános megközelítéséről szóló közlemény már jóval nagyobb szerepet tulajdonított a botneteknek, és ezeket az infrastruktúrákat tette felelőssé az olyan átfogó, információs rendszerek elleni támadásokért, mint amilyen az észtországi kritikus infrastruktúrák elleni támadás volt 2007-ben.[30]

Az információs rendszerek elleni támadásokról szóló irányelv kiemelten foglalkozott a botnethálózatok elleni fellépés kérdésével.[31] Ez az uniós norma már a célját is abban határozza meg, hogy „[büntetőjogi] szankciókat állapítson meg a botnetek létrehozására, vagyis azon cse-

[30] https://index.hu/tech/net/eszt290507/

[31] Az Európai Parlament és a Tanács 2013/40/EU irányelve (2013. augusztus 12.) az információs rendszerek elleni támadásokról és a 2005/222/IB tanácsi kerethatározat felváltásáról.

lekményre vonatkozóan, amellyel célzott informatikai támadások révén jelentős számú számítógép felett veszik át a távvezérelt irányítást oly módon, hogy rosszindulatú számítástechnikai programokkal fertőzik meg őket".[32] Az irányelv arról is rendelkezik, hogy az olyan támadások esetében, amelyek célja botnet létrehozása, vagy amelyet botnet révén hajtanak végre, a tagállamok megállapíthatnak súlyosabb szankciót.[33] Ezt a szabályt a Btk. akképp ültette át, hogy az információs rendszer vagy adat megsértése bűntettének minősített esete valósul meg, ha a cselekmény jelentős számú információs rendszert érint.[34] A botnet számos funkciót elláthat, Nagy Zoltán és Mezei Kitti a következő botnetfunkciókat különbözteti meg: DDoS támadások indítása, spamküldés, adathalászat, hálózatfigyelés, billentyűzetfigyelés, internetes reklámokhoz kapcsolódóan klikkelések begyűjtése.[35] Újabban a botnethálózatokat gyakran használják kriptovaluták (pl. bitcoin) bányászására.

A botnethálózatok funkciói közül talán az egyik leghírhedtebb a túlterheléses támadás *(denial of service attack – DoS).* A túlterheléses támadások esetében az elkövető azzal akadályozza a rendszer működését, hogy olyan adatmennyiséget zúdít a célrendszerre, amelyet az képtelen kezelni. A túlterheléses támadások manapság leggyakrabban úgynevezett elosztott túlterheléses támadással *(distributed denial of service attack – DDoS)* történnek, ami annyit jelent, hogy a megfertőzött zombiszámítógépek a megcélzott szervereknek folyamatosan kéréseket – adatcsomagokat – küldenek, és ha több ezer csomag érkezik egyszerre, a forgalmazás mértékét a támadott rendszer nem bírja el, és ez a rendszer teljes összeomlását eredményezheti. (Lásd a *2. ábrát.*) Ugyanakkor az információs rendszer működésének akadályozásához nem feltétel a célrendszer teljes megbénulása, ahogy Nagy és Mezei is kiemelik: a „funkcionális működésképtelenséghez elegendő a nagymértékű lelassulás is, ami a válaszidő megnövekedett mértékéből adódik."[36] A Btk. szerint a cselekmény minősített esetét követi el, aki a 423. §-ban szabályozott magatartásokat közérdekű üzem ellen követi el.

Az elosztott túlterheléses támadások esetében érdemes röviden foglalkozni a tettesség kérdésével. A törvény *Kommentár*ja alapján a Btk. 423. § (2) bekezdése szerinti cselekmények elkövetője bárki lehet, azonban azok csak szándékosan valósíthatók meg.[37] Mivel a botnetek esetében a támadásban zombiként, távoli vezérléssel részt vevő rendszerek tulajdonosainak gyakran arról sincs tudomásuk, hogy a gépük vírusfertőzés áldozata, a támadással érintett információs rendszer tekintetében az akadályozási szándék egyértelműen kizárható. A szándék általában a mestergép tulajdonosa, a *botherder* oldalán jelenik meg, az ő cselekménye szándékos és egyben célzatos. Az elkövető ebben az esetben nemcsak a túlterheléses támadással célzott információs rendszer működését akadályozza, hanem az összes olyan információs rendszer működését is, amelyet megfertőzött és távoli hozzáféréssel támadásra utasított.

32 Uo., (1) preambulumbekezdés.

33 Uo., (13) preambulumbekezdés.

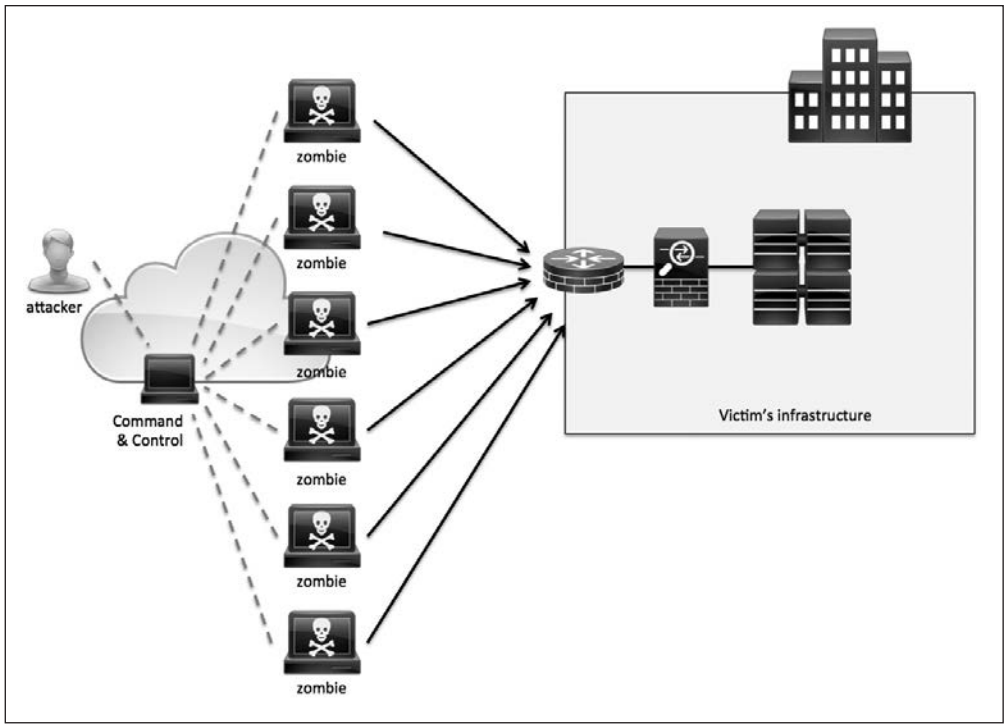
34 Btk. 423. § (3) bekezdése.

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

36 Uo., 164.

37 Karsai Krisztina (szerk.): *Kommentár a Büntető törvénykönyvről szóló 2012. C. törvényhez*. Budapest, Wolters Kluwer, 2017.

2. ábra: **Elosztott túlterheléses támadás**[38]



4. A malware-ek elleni fellépés eljárásjogi kérdései, figyelemmel a nyomozás során okozott kihívásokra

Annak ellenére, hogy a magyar sajtó többször számolt be arról, hogy nyomozás van folyamatban információs rendszer és adatok megsértésének bűntette miatt, a médiában nagy port kavart események utóéletéről, a vádelemelésről és az esetleges ítélethirdetésekről már szinte soha nem lehet hallani. A Bűnügyi Statisztikai Rendszer (BSR) adatai szerint 2012 és 2017 között összesen 5643 esetben indult eljárás információs rendszer és adatok megsértésének ügyében.[39] A nyomozás az ügyésznek vagy a nyomozó hatóságnak hivatali hatáskörében, valamint a nyomozó hatóság tagjának hivatali minőségében tudomására jutott adatok alapján vagy feljelentésre indul meg.[40] Feljelentést a törvény szerint bárki tehet, a feljelentő ebben az esetben lehet az

[38] Forrás: http://www.cisco.com/c/dam/en_us/about/security/images/csc_child_pages/white_papers/ddos_fig02.jpg

[39] https://bsr.bm.h

[40] 2017. évi XC. törvény a büntetőeljárásról, 375. § (1) bekezdés.

internetszolgáltató, amely gyanús, megnövekedett hálózati forgalmat észlel, a felhasználó (sértett), aki a számítógépe és az internetkapcsolata működése során észleli a cselekményt, illetve az információs rendszer üzemeltetője (a vállalkozás, amelynek a szerverét támadás éri).

A BSR adatai szerint 2013 és 2017 között az esetek nagy részében, 3015 esetben maga a sértett kezdeményezte az eljárást, 483 olyan eljárás zajlott, amely a bűncselekményt észlelő egyéb személy kezdeményezésére indult, a rendőrség bűnügyi szerve pedig 187 esetben indított eljárást saját észlelés alapján. Vádemelésre azonban már csak az ügyek 13%-ában, azaz 789 esetben került sor. A feljelentést 501 esetben utasították el, 1583 esetben pedig a nyomozás megszüntetésére került sor. A statisztika szerint 2501 esetben zárult 'egyéb' módon az eljárás. 2017 nyarán kérdőívet küldtem az Országos Rendőr-főkapitányság (ORFK) részére, amelyben a feljelentés elutasításának,[41] a nyomozás megszüntetésének indokaira,[42] valamint az eljárás 'egyéb' módon történő befejezésének részleteire kérdeztem. Az ORFK tájékoztatása szerint mind a feljelentés elutasításának, mind a nyomozás megszüntetésének gyakori indoka a cselekmény elévülése, valamint az, hogy gyermekkorú az elkövető, ami büntethetőséget kizáró ok. Érdekesség, hogy az 'egyéb' befejezés kategóriájába tartozik a nyomozás felfüggesztése, amelynek leggyakoribb esete, hogy nem volt megállapítható az elkövető kiléte. Az adatokból az látszik, hogy az ilyen jellegű bűncselekményeknél az egyik legnagyobb nehézséget az elkövető azonosítása okozza.

Az online környezet viszonylag nagymértékű anonimitást biztosít a benne mozgó szereplőknek, de alapesetben az elkövető az IP-cím alapján azonosítható. Az IP-cím a hálózati környezetben az egyes eszközök, például a számítógépek azonosítására használt egyedi megjelölés. Az IP-cím forgalmazási és személyes adat, ezért a tárolására és kezelésére szigorú szabályok vonatkoznak. A hírközlési adatvédelmi irányelv[43] arra kötelezi a tagállamokat, hogy biztosítsák a nyilvánosan elérhető elektronikus hírközlési szolgáltatások segítségével történő közlések és az azokra vonatkozó forgalmi adatok – így az IP-címek – titkosságát. E szabály alól az irányelv

[41] A kérdőív megválaszolásakor hatályos, a büntetőeljárásról szóló 1998. évi XIX. törvény szerint a nyomozás megszüntetésének esetei a következők voltak: a cselekmény nem bűncselekmény, a bűncselekmény gyanúja hiányzik, a büntethetőséget kizáró ok (Btk. 15. §) állapítható meg, eljárás halál, elévülés vagy kegyelem folytán nem indítható, a magánindítvány vagy feljelentés hiányzik, a cselekményt már jogerősen elbírálták, a cselekmény elbírálására a magyar hatóságnak nincs joghatósága.

[42] A kérdőív megválaszolásakor hatályos, a büntetőeljárásról szóló 1998. évi XIX. törvény szerint a nyomozás megszüntetésének esetei a következők voltak: a cselekmény nem bűncselekmény, a nyomozás adatai alapján nem állapítható meg bűncselekmény elkövetése, és az eljárás folytatásáról sem várható eredmény, nem a gyanúsított követte el a bűncselekményt, illetve ha a nyomozás adatai alapján nem állapítható meg, hogy a bűncselekményt a gyanúsított követte el, büntethetőséget kizáró ok állapítható meg, a gyanúsított halála, elévülés, kegyelem miatt, a törvényben meghatározott egyéb büntethetőséget megszüntető ok miatt, ha a magánindítvány, kívánat vagy feljelentés hiányzik, és az már nem pótolható, a cselekményt már jogerősen elbírálták, az Európai Unió tagállamaival folytatott bűnügyi együttműködésről szóló törvény szerinti konzultációs eljárás eredménye alapján a büntetőeljárást az Európai Unió másik tagállama folytatja le, a gyanúsított cselekménye már nem veszélyes, vagy oly csekély fokban veszélyes a társadalomra, hogy a törvény szerint alkalmazható legenyhébb büntetés kiszabása vagy más intézkedés alkalmazása is szükségtelen, a cselekmény elbírálására a magyar hatóságnak nincs joghatósága.

[43] Az Európai Parlament és a Tanács 2002/58/EK irányelve (2002. július 12.) az elektronikus hírközlési ágazatban a személyes adatok kezeléséről, feldolgozásáról és a magánélet védelméről (Elektronikus hírközlési adatvédelmi irányelv).

akkor enged kivételt, ha a kérdéses adatok megismerése a nemzetbiztonság, a nemzetvédelem és a közbiztonság védelme érdekében, valamint a bűncselekmények, illetve az elektronikus hírközlési rendszer jogosulatlan használata megelőzésének, kivizsgálásának, felderítésének és üldözésének biztosítása érdekében szükséges. E szabály nyomán az elektronikus hírközlésről szóló törvény[44] (a továbbiakban: Eht.) rendelkezései közt is találhatunk olyan szabályt, amely bizonyos adatfajták estében megőrzési kötelezettséget ír elő az elektronikus hírközlési szolgáltatást nyújtók számára.

A törvény szabályai értelmében a megőrzéssel érintett adatok köre kizárólag az előfizető személyével (előfizető neve, számlázási címe), valamint a forgalmazás tulajdonságaival (IP-cím, portszám, MAC-cím) kapcsolatos adatokra terjed ki, a közlésnek a tartalmára nem. A nyomozó hatóság megkereséssel kérhet adatszolgáltatást a hírközlési szolgáltatóktól ezen adatok megismerése érdekében. Az ORFK tájékoztatása szerint az informatikai jellegű bűncselekmények nyomozása során minden esetben megkeresik az internetszolgáltatókat, és mindig érdemi választ kapnak, ami nagyban segíti a hatóság munkáját.

Az Eht. szabályai azonban csak a Magyarország területén végzett vagy területére irányuló elektronikus hírközlési tevékenységre vonatkoznak; a szolgáltatók által tárolt adatfajták és az adatok megőrzésének időtartama országonként igen eltérő lehet. Ugyanakkor az informatikai bűncselekmények nincsenek tekintettel az országhatárokra: az információs rendszereket megfertőző kártékony programok terjedése nem áll meg a határoknál – a fertőzöttség a kártevő népszerűségétől függ, nemritkán globális. E nemzetközi jellegből fakadóan egy ország nyomozó hatósága ritkán elegendő a teljes hálózat felderítéséhez és az irányító-vezérlő központ lekapcsolásához. A fertőzések országhatárokon belüli felszámolása csak a távközlési és a biztonságtechnikai piac segítségével valósítható meg, ráadásul csak ideig-óráig hatásos, hiszen ha az irányító központ fennmarad, a kártevő újra képes lesz fertőzni.

Az ENSZ korábban már hivatkozott tanulmánya arról számolt be, hogy a jelentéskészítésben közreműködő országok több mint fele nyilatkozott úgy, hogy a kiberbűncselekmények, amelyekkel a rendőrség találkozik, 50–100%-ban tartalmaznak nemzetközi elemet.[45] A magyar tapasztalatok egybevágnak az ENSZ tanulmányában foglaltakkal: az ORFK úgy nyilatkozott, hogy – mivel a számítógépes bűnözés a legtöbb esetben országhatárokon átnyúló bűnelkövetési módszerekkel történik – szinte minden esetben szükség van nemzetközi bűnügyi együttműködésre. A tapasztalatok azt mutatják, hogy nehézkes a közvetlen kapcsolatfelvétel a külföldi internetszolgáltatókkal, azonban néhány esetben angol nyelvű megkeresésre már érdemi válasz érkezett. Az esetek túlnyomó többségében azonban csak bűnügyi jogsegélykérelem keretében lehetséges tőlük adatokat beszerezni.

A gyakorlatban könnyen előfordulhat, hogy mire a jogsegélykérelem átfut, a megkereséssel érintett adatok már rég nincsenek a szolgáltató birtokában. A Cybercrime-egyezmény ugyan lehetővé teszi a tárolt és a forgalmi adatok megőrzésére kötelezést (16–17. cikk), a gyakorlat azt mutatja, hogy ez a jogintézmény nem funkcionál megfelelően. Problémát jelenthet, hogy az IP-cím elfedésére többféle, hozzáértést különösebben nem igénylő lehetőség van. A Tor böngé-

[44] 2003. évi C. törvény az elektronikus hírközlésről.

[45] http://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf

ső például proxy szervereken keresztül bonyolítja a hálózati forgalmazást a végpontok között, és ismertek olyan proxy szerverek, amelyek úgy biztosítanak anonimitást a felhasználónak, hogy a külvilág felé hamis IP-címet mutatnak. Az anonimizáló proxy szerverek láncolatán keresztül technikailag visszafejthető a kapcsolat a hálózati kommunikáció kiindulópontjáig, ez azonban a proxy szerverek tipikusan külföldi elhelyezkedése miatt idő- és erőforrás-igényes, ráadásul ha a szerver olyan országban található, mint például Thaiföld vagy Venezuela, a jogsegélykérelem eredménytelen is lehet. Az elkövetői körökben népszerű Tor használata esetén a kapcsolat nem fejthető vissza.

Kiterjedt *malware*-fertőzés, például botnethálózat esetében az elkövető által használt eszköz, vagyis a rendszer irányítójának azonosítása is többlépcsős folyamat eredménye. Egy botnet hálózati infrastruktúrájának feltérképezése a megfertőzött végpontok (zombik) kommunikációjának megfigyelésén keresztül az irányító szerverek (Command & Control server) meghatározásával lehetséges, ez azonban műszaki tudást és jellemzően több ország nyomozó hatóságainak együttműködését igénylő feladat, a bűnügyi területen zajló nemzetközi együttműködések részletes tárgyalása azonban túlmutat e tanulmány keretein. Lényegében ha el akarunk jutni a botnethálózat irányítójához, vissza kell fejtenünk a hálózati kommunikációt több lépcsőben addig, amíg el nem érünk a kiindulópontjáig, ami műszaki értelemben lehetséges, az egyes technikák alkalmazásának viszont nemritkán jogi korlátja van.

Egy, az Európai Uniós Hálózat- és Információbiztonsági Ügynökség (ENISA) által készített tanulmány kifejezetten a botnetek vonatkozásában tárgyalja a felderítéssel, a fertőzöttség mérésével, illetve az ilyen hálózatok felszámolásával kapcsolatos lehetőségeket, azonban az általa javasolt megoldások a legtöbb olyan *malware*-fajtánál alkalmazhatók, amelynél aktív hálózati kommunikáció zajlik.[46] Az infrastruktúra feltérképezésére a tanulmány aktív és passzív technikákat javasol. Passzív technikák azok az eszközök, amelyek esetében olyan jeleket keresnek, melyek a botnet tevékenységre utalnak, az adatgyűjtés pedig kizárólag megfigyelésen alapul, és nem kerül sor a hálózati kommunikációba való beavatkozásra. Ezek: adatcsomag-elemzés *(packet inspection),* adatfolyam-analízis (*flow*-rekordok elemzése), DNS-alapú megközelítések, spamlisták elemzése, az applikációk naplófájljainak elemzése, csapdaállítás (*honeypot*ok létrehozása), az antivírusszoftverek jelentéseinek elemzése. Az aktív technikák már a megfigyelt eszközökkel történő kapcsolatfelvételt is magukban foglalják, ezek a kifejezetten invazív technikák már nemcsak a hálózat azonosítására adnak lehetőséget, hanem a beavatkozásra és a lekapcsolásra is (pl. az ún. *sinkholing* technika). A passzív és aktív technikák elhatárolása azért releváns, mert míg a passzív technikák – az alkalmazásukkal okozott jogkorlátozás súlyának figyelembevételével – hagyományos adatszerző tevékenység, illetve titkos felderítés körében alkalmazhatók, az aktív technikák a jog szürkezónájában mozognak, alkalmazásuk pedig egyes országokban kifejezetten tilos. A passzív technikák között is differenciálhatunk a tekintetben, hogy vannak olyanok, amelyek a forgalmazási adatok elemzésén alapulnak, és olyanok is, amelyek a kommunikáció (adatcsomag) tartalmának elemzéséből engednek következtetni a *malware*-fertőzés jellemzőire.

[46] https://www.enisa.europa.eu/publications/botnets-measurement-detection-disinfection-and-defence/at_download/fullReport

A korábban tárgyalt, forgalmazásra vonatkozó adatok esetében a szolgáltatónak törvényből eredő megőrzési kötelezettsége van bizonyos adatfajták tekintetében, a kommunikáció tartalmának megismerését lehetővé tévő technikák viszont már leplezett eszközöknek (korábban a titkos információgyűjtés, illetve a titkos adatszerzés körébe tartozó eszközöknek) minősülnek. Gyányi Sándor – szintén botnetek vonatkozásában – kiemeli, hogy a forgalmazási információk elemzése kevésbé erőforrás-igényes, a botnet tagjairól pedig az „adatfolyam jellemzői (forrás- és célcím, portcímek, alkalmazott magasabb rétegbeli protokollok, az adatfolyam időtartama, mérete) árulkodhatnak".[47] A forgalmazási adatok ismerete azonban még nem biztos, hogy elégséges egy hálózat felderítéséhez – Gyányi is rávilágít, hogy azokban az esetekben, ahol a 'normális' hálózati kommunikáció közé vegyül a gyanús akció nyoma is, csak igen összetett szűrési módszerekkel lehetne pusztán fejlécinformációkból azonosítani a gyanús kommunikációt.[48]

A mélyreható adatcsomag-elemzés *(deep packet inspection)* részletesebb információt ad a hálózati kommunikáció tartalmáról is. Az adatcsomag-elemzés a fejléc (címzés) adatainak vizsgálatán túl lehetővé teszi a tartalomnak az elemzését is. Az elektronikus hírközlési szolgáltatók a kommunikáció tartalmát nem tárolják az átvitelhez szükséges időtartamnál tovább, és nem is ismerik. Egyes országokban a közlés tartalmának internetszolgáltató általi megismerése még a szolgáltató büntetőjogi felelősségének kérdését is felveti. A NATO és az ENISA közös tanulmánya a német szövetségi büntető törvénykönyv szabályai mentén mutatja be az internetszolgáltatók felelősségének témáját, és arra a megállapításra jut, hogy az internetszolgáltatók csak *ad hoc* jelleggel vizsgálhatják az adatcsomagokat és a forgalmazási adatokat, amennyiben a telekommunikációs rendszerek hibáinak feltárása és kijavítása érdekében szükség van rá, máskülönben e tevékenységük tiltott adatszerzésnek minősül.[49]

A magyar internetszolgáltatók is végezhetnek ilyen tevékenységet – a Telekom általános szerződési feltételei szerint „a [s]zolgáltató a tevékenysége során alkalmazott, a jelek továbbítását végző berendezéseinek adatait rendszeresen elemzi, valamint a hálózaton időszakos ellenőrzéseket végez a hálózat egysége és biztonságos működése érdekében".[50] A Btk. szintén ismeri a tiltott adatszerzés tényállását, a magyar jogban ez a cselekmény viszont célzatos, vagyis a büntetendőséghez a személyes adat, magántitok, gazdasági titok vagy üzleti titok jogosulatlan megismerésének célja szükséges, ami az internetszolgáltatók oldalán nem áll fenn, amennyiben céljuk a kártékony kódokat tartalmazó kommunikáció szűrése.

A 2018. június 30-áig hatályban lévő szabályok értelmében az elektronikus kommunikáció a nyomozás megkezdését megelőzően titkos információgyűjtés, azt követően pedig titkos adatszerzés keretében volt megismerhető az erre hatáskörrel rendelkező szerveknek. Mind az 1998. évi XIX. törvény, azaz a régi büntetőeljárásról szóló törvény (Be.), mind a 2018. június 30-ig

[47] Gyányi Sándor: *Túlterheléses informatikai támadási módszerek és a velük szemben alkalmazható védelem*. PhD-értekezés, Budapest, 2011. http://archiv.uni-nke.hu/downloads/konyvtar/digitgy/phd/2012/gyanyi_sandor.pdf

[48] Uo., 109.

[49] https://ccdcoe.org/sites/default/files/multimedia/pdf/VihulCzosseckZiolikowskiAasmannIvanovBr%C3%BCggemann2012_LegalImplicationsOfCounteringBotnets.pdf

[50] Telekom: Lakossági általános szerződési feltételek, 2/C melléklet, https://www.telekom.hu/static-tr/sw/file/lakossagi-aszf-2c-melleklet-szolgaltatasok-tartalma-internet-20180701.pdf

hatályos, a titkosszolgálati eszközök és módszerek folytatására feljogosított szervek jogállásáról szóló törvény lehetőséget teremtett a számítástechnikai eszköz vagy rendszer útján továbbított (pl. LAN) vagy tárolt (pl. merevlemez) adatok megismerésére, valamint az elektronikus hírközlési szolgáltatás útján továbbított (pl. a nyílt interneten zajló) kommunikáció megfigyelésére. A 2017. évi XC. törvény, azaz az új Be. jelentős mértékben változtatott a szabályokon, és „leplezett eszközök" megnevezéssel összevonta a titkos információgyűjtésre és a titkos adatszerzésre vonatkozó szabályokat, valamint bevezette az úgynevezett előkészítő eljárás intézményét, amelynek célja annak megállapítása, hogy fennáll-e a bűncselekmény gyanúja.

Az új kódexet már a hatálybalépése előtt számos kritika érte, amelyek közül a legnagyobb hangsúlyt kétségtelenül az kapta, hogy az a tény, hogy a nyomozó hatóság az előkészítő eljárás keretében alkalmazhat leplezett eszközöket a bűnügyi felderítéshez, látszólag nem érintette a büntetőeljáráson kívüli titkos információgyűjtésre vonatkozó szabályokat. Ennek kapcsán ismét előtérbe került a bűnügyi és a rendészeti felderítés elválasztásával kapcsolatos, már az előző eljárási kódex rendelkezései kapcsán is folytatott vita. Finszter Géza különbséget tesz a bűncselekmény elkövetőinek és a bizonyítás eszközeinek felkutatását célzó bűnügyi felderítés és a közbiztonságot és a közrendet veszélyeztető tevékenységek elhárítására irányuló rendészeti felderítés között.[51] A felderítés egyes típusai indokolttá teszik az eltérő szabályozást, amihez hozzátartozik a még elfogadható jogkorlátozással járó eszközök körének eltérő meghatározása is.

Ebből az aspektusból vizsgálva, a kiterjedt *malware*-fertőzések, illetve a botnethálózatok igen érdekes kérdéseket vetnek fel. A botnethálózatok esetében a bűnügyi és rendészeti célok kumuláltan vannak jelen. A botnethálózat kiépítésével már eleve a felhasználókat tömegesen érintő jogsértés történik, ezért ezzel szemben indokolt lehet a bűnügyi felderítés eszközeinek alkalmazása. Az ilyen hálózatok végső célja azonban ritkán merül ki fertőzött gépekből álló hálózatok puszta kialakításában, így egy zombigépekből álló hálózat létrehozása tipikusan eszközcselekménye valamilyen egyéb deliktumnak. Ahogy arról korábban esett szó, egy botnet számos további cselekmény elkövetésére, például DDoS támadások lefolytatására, spamküldésre, tömeges adatvisszaélésre felhasználható, amelyek megelőzése már rendészeti cél.

Aggodalomra ad okot a rendőrségről szóló törvénynek[52] (a továbbiakban: Rtv.) az a 2018 nyarán hatályba lépett rendelkezése, amely lehetőséget teremt arra, hogy a rendőrség a titkos információgyűjtés keretében azonosítsa a kommunikációhoz használt információs rendszert, illetve megszerezze a hollétének megállapításához szükséges adatokat.[53] *Malware*-fertőzések esetén nem tudjuk, hogy a végpontokból kiindulva hány felhasználó kommunikációjának vizsgálata szükséges, amíg el nem jutunk a megfertőzött rendszerekkel kommunikáló irányítószerverig. Egy botneten belül például nem ritka, hogy 600 ezer végpont *(host)* található – ha csak a töredéküket kommunikációját vizsgálják, még az is tömeges jogkorlátozással jár, aminek elszenvedői ráadásul olyan harmadik személyek, akik semmilyen kapcsolatban nem állnak az elkövetéssel, sőt mivel rendszerük fertőzés áldozata, ők a sértettek. Ilyenkor ráadásul még a bírói enge-

51 Finszter Géza: *A rendészet elmélete.* Budapest, KJK–KERSZÖV, 2003. 37.

52 1994. évi XXXIV. törvény a rendőrségről.

53 Rtv. 66. § (1) bekezdésének *e)* pontja.

délyhez kötött eszközök esetében alkalmazandó arányossági tesztet sem kell elvégezni, tehát nem kötelező vizsgálni, hogy az érintett eszköz alkalmazása aránytalanul korlátozza-e az érintett vagy más személy alapvető jogát.

Árnyalja ugyan a képet, hogy az egyes közlések tartalma az internetes kommunikáció csomagkapcsolt jellegéből fakadóan nem fejthető vissza, vagy csak nehezen, hiszen minden közlés részekre bontva érkezik és távozik, ezenkívül a hálózati kommunikáció vizsgálata során az adatcsomag-elemzést automatizált eszközök végzik, amelyek mintákat keresnek, így képesek a kártékony kommunikációra utaló nyomokat tartalmazó adatcsomagok szűrésére. Ugyanakkor a jogbiztonság szempontjából célszerű lenne tisztázni, hogy az Rtv. e pontja milyen módszerek alkalmazását teszi lehetővé a kommunikációhoz használt információs rendszer azonosítása érdekében bírói engedélyhez nem között eszközként, illetve hogy ez a rendelkezés felhatalmazást ad-e a rendőrségnek arra, hogy egy botnet vagy egyéb *malware* irányító szerverének lokalizálása érdekében olyan leplezett eszközöket alkalmazzon, amelyek egyébként bírói engedélyhez kötött eszközök lennének. További garanciális szabály lehet annak megfogalmazása, hogy az olyan hálózati kommunikáció megfigyelése, amely nagyszámú végpont forgalmát érinti, kizárólag csak olyan automatizált eszközzel történhet, amely megfelelően képes szűrni *malware* tevékenységre utaló kommunikációt a hálózaton zajló egyéb forgalomból.

Az új Be. és a hatálybalépésekor módosuló ágazati jogszabályok különbséget tesznek az információs rendszer titkos megfigyelése és a lehallgatás között. A két intézmény közötti lényeges különbség, hogy az információs rendszer megfigyelése esetében magának az eszköznek és a benne zajló folyamatoknak a vizsgálata (pl. alkalmazások naplófájljainak vizsgálata) történik, a lehallgatás ellenben a rendszer elektronikus hírközlő hálózaton folytatott kommunikációjának a megfigyelését teszi lehetővé. A törvény felhatalmazást ad arra, hogy a megfigyelés érdekében a nyomozó hatóság *malware*-t telepítsen a célrendszerre, azonban ezt virágnyelven akként fogalmazza meg, hogy az „ehhez szükséges elektronikus adat az információs rendszerben […] elhelyezhető”.[54] A lehallgatás szintén történhet az információs rendszer megfigyelésével, az elektronikus kommunikáció megfigyelése pedig közvetlenül a szolgáltatást biztosító internetszolgáltató segítségével. Mivel a hálózati kommunikáció megfigyelésére a hozzáférést lehetővé tévő hírközlési hálózat üzemeltetőjének rendszerén keresztül van lehetőség, az új Be. az eljárás sikerének érdekében rögzíti, hogy a hírközlési szolgáltatást, információs rendszerben tárolt adatok továbbítását, feldolgozását, kezelését végző szervezetek kötelesek együttműködni a titkos információgyűjtés folytatására, illetve leplezett eszközök alkalmazására törvényben feljogosított szervezetekkel. E szervezetek kötelezettségeiről az Eht. szól részletesen,[55] amely külön cím alatt szabályozza a titkos információgyűjtés és a leplezett eszközök alkalmazása érdekében való együttműködést. A törvény alapján a szolgáltató köteles biztosítani a továbbított küldemények, közlések, kezelt adatok megismeréséhez szükséges eszközök és módszerek alkalmazási feltételeit, köteles megfelelő műszaki rendszert, így különösen alapkiépítésű monitoringalrendszert létesíteni (amelynek költségét a szolgáltató viseli).

A büntetőeljárás keretében alkalmazott leplezett eszközök továbbra is csak meghatározott személyi körrel szemben alkalmazhatók. Leplezett eszközt főszabály szerint azzal szemben lehet

[54] Az új Be. 232. § (1) bekezdése.

[55] Eht. 92. §.

alkalmazni, aki gyanúsított, illetve aki bűncselekmény elkövetésével gyanúsítható, ilyen személy azonban a botnet-infrastruktúrák felderítésének megkezdésekor még nincs, és lehetséges, hogy a későbbiek folyamán is csak az irányítószerverig, pontosabban a szerver üzemeltetőjéig jut el a nyomozó hatóság, az elkövetőig már nem. A kiberbűncselekményekről szóló tankönyv is említi azt a problémát, hogy vannak olyan szerverhoszting szolgáltatások, amelyek a szerverszolgáltatás mellett többletszolgáltatásként anonimitást is kínálnak az ügyfeleiknek.[56] Az előkészítő eljárás részeként mással szemben kizárólag akkor lehet leplezett eszközt alkalmazni, ha megalapozottan feltehető, hogy a bűncselekmény elkövetőjeként szóba jöhető személlyel közvetlenül vagy közvetve kapcsolatot tart, vagy ha kívülálló személyt elkerülhetetlenül érint. A *malware*-ek esetében mindkét kitétel meglehetősen rugalmas értelmezést tesz lehetővé, mivel a kártékony szoftverekre építő hálózati infrastruktúráknál technikai értelemben van kapcsolat a sértett fertőzött rendszere és a fertőzést kihasználó elkövető információs rendszere között, ez a kommunikáció azonban sokszor a sértett tudta nélkül folyik. Nyitott kérdés, hogy a sértettek *malware*-rel fertőzött rendszereinek megfigyelése indokolható-e a bűnüldözési érdekre hivatkozással. Az Alkotmánybíróság is rávilágított,[57] hogy a bűnös kapcsolattartás megítélése meglehetősen szubjektív.

5. Jó példák a botnetek elleni fellépésre

A szűk értelemben vett informatikai bűncselekményeket tekintve egyelőre még igen sok a nyitott kérdés, kezdve azzal a problémával, hogy az információs rendszerekkel kapcsolatos bűnözés mint jelenség általánosan elfogadott fogalomrendszerének kidolgozása még várat magára, egészen annak pontos meghatározásáig, hogy a kibertérben folyó nyomozás során meddig terjednek a hatáskörrel rendelkező szervek lehetőségei. Ezeket a kérdéseket vélhetően és remélhetőleg a kiberbűncselekmények nyomozásában jártas szakemberek az eljárások során gyűjtött tapasztalatok alapján megválaszolják majd. Már manapság is többször olvashatunk sikeres, átfogó nemzetközi együttműködésen alapuló megoldásokról: az Europol már több pozitív tapasztalatról is beszámolt, például 2017-ben az Andromeda nevűre botnethálózatot sikerült nemzetközi együttműködés keretében lekapcsolni,[58] 2015-ben a Ramnit botnetet,[59] 2014-ben pedig a Gameover Zeust.[60]

---

[56] Simon i. m. (8. lj.) 210.

[57] 2/2007. (I. 24.) AB határozat.

[58] https://www.europol.europa.eu/newsroom/news/andromeda-botnet-dismantled-in-international-cyber-operation

[59] https://www.europol.europa.eu/newsroom/news/botnet-taken-down-through-international-law-enforcement-cooperation

[60] https://www.europol.europa.eu/newsroom/news/international-action-against-gameover-zeus-botnet-and-cryptolocker-ransomware