Mezei Kitti*

A DDoS-támadások büntetőjogi szabályozása az Egyesült Államokban, Európában és Magyarországon

informatikai bűnözés – DDoS-támadás – botnet – Computer Fraud and Abuse Act – 2013/40/EU irányelv

Az internet többféle informatikai támadásnak nyújt lehetőséget, ezek közül a legrégebbi támadási formák közé tartozik a szolgáltatásmegtagadással járó, avagy túlterheléses támadás, a DDoS-támadás, amely a hálózat sebezhetőségét használja ki a megtámadott rendszerhez való hozzáférés nélkül. Elkövetésének száma, összetettsége évről évre növekvő tendenciát mutat, ami köszönhető annak, hogy egyszerűen és gyorsan végrehajtható, azonban egyszerűsége ellenére jelentős társadalmi, gazdasági és anyagi kárt képes okozni. Az elkövetést továbbá segíti az is, hogy az informatikai bűnözés egy szolgáltatásalapú iparággá nőtte ki magát az elmúlt években. A különböző online feketepiacokon keresztül könnyen hozzá lehet jutni a támadások alapját képező botnet infrastruktúrákhoz és egyéb eszközökhöz, mintegy szolgáltatásként.

A tanulmány célja, hogy bemutassa először röviden a DDoS-támadások technikai alapját, majd a támadások mögött húzódó lehetséges motivációkat, ezt követően a büntetőjogi szabályozásra tér ki, különösen az Egyesült Államok *Computer Fraud and Abuse Act* (a továbbiakban: CFAA) rendelkezéseire, az Európai Unió fellépésére a botnetekkel szemben a *2013/40/EU irányelvet* figyelembe véve, végül a hazai tényállásokra.

1. A DDoS-támadásokról általában

A szolgáltatásmegtagadással járó támadás egy olyan támadási forma, amelynek célja az információs rendszerek, szolgáltatások vagy hálózatok erőforrásainak oly mértékben történő túlterhelése, hogy azok elérhetetlenné váljanak, vagy ne tudják ellátni az alapfeladatukat. Az ilyen elektronikus támadást intézők a jogosult felhasználókat akadályozzák a szolgáltatás igénybevételében,[1] (pl. e-mail-fiókhoz, más ban-

* Dr. Mezei Kitti tudományos segédmunkatárs, MTA Társadalomtudományi Kutatóközpont Jogtudományi Intézet; PhD-hallgató, Pécsi Tudományegyetem Állam- és Jogtudományi Kar Doktori Iskola, mezei.kitti@tk.mta.hu. A tanulmány az Emberi Erőforrások Minisztériuma ÚNKP-17-3-I kódszámú Új Nemzeti Kiválóság Programjának támogatásával készült.

[1] Nagy Zoltán András: *Bűncselekmények számítógépes környezetben.* Ad Librum, Budapest, 2009, 115.

ki vagy egyéb fiókokhoz való hozzáférésben, a weboldal elérésében) – innen a szolgáltatásmegtagadással járó elnevezés is – amelynek a leggyakoribb formája, amely a webszerver elérését és rendeltetésszerű használatát gátolja a mesterségesen generált és megnövelt adatforgalommal.[2]

Az elnevezés a támadás angol megfelelőjének rövidítéséből ered, amely során az említett támadás egyetlen számítógéptől származik, több közbeiktatott gép nélkül: *Denial of Service (DoS)*. Amennyiben a támadás összetettebb, mert összekapcsolt rendszerek csoportjától, egyszerre sok – lehetőleg minél több – helyről indul, akkor használatos a *Distributed Denial of Service (DDoS),* vagyis az elosztott szolgáltatásmegtagadással járó támadás elnevezés. Ebben az esetben a feladatot nem egyetlen eszköz végzi el, mint a DoS-támadásnál, hanem a rendszert alkotó – egymástól akár nagy távolságban lévő – eszközök (pl. asztali gépek, okos mobiltelefonok vagy routerek stb.) párhuzamosan.[3]

A támadás technikai alapja leegyszerűsítve a következőképpen néz ki: a DDoS-támadás során a támadó egy hálózatot alkotó számítógépek adatcsomagjaival elárasztja a célzott szervert akkora forgalommal, hogy az képtelen lesz az adatcsomagok fogadására, illetve válaszolására, ezzel akár a rendszer teljes leállását is eredményezhetik, azonban a funkcionális működésképtelenséghez elegendő a nagymértékű lelassulás is, ami a válaszidő megnövekedett mértékéből adódik.[4]

A felhasználó tudta nélkül megfertőzött számítógépeket, amelyek távolról irányíthatók, *„zombi"*-nak nevezik. Másik elnevezésük a robot és network szavak összevonásából eredő *„botnet",* amely a több bot összekapcsolásával keletkezett hálózatot jelenti. A botnet irányítóját, aki kiosztja a feladatot a fertőzött eszközöknek, *„botmaster"*-nek, illetve több irányító esetén *„botherder*"-nek nevezik. A botnethálózat tagjait a fertőzött zombi számítógépek alkotják. Azt a központi vezérlő eszközt, amely vezérli a botnetakciókat *„controller"*-nek hívjuk. A controller általában az ún. *„drop server"*-re csatlakozik, amely a botnet által gyűjtött adatok tárolására szolgáló tárhelyet jelenti, ami hozzáférhető a botnethálózat tagjai és a botmaster részére is. A botmaster és botnet közti kapcsolatot és az utasítások eljuttatását biztosító kommunikációs útvonal az ún. *Command&Control (C&C) szerver*.[5]

A botnetek a kiberbűnözői infrastruktúrának az alapját képezik, mérhetetlen erőforrást biztosítanak számukra a rendelkezésre álló számítógép-kapacitás és sávszélesség tekintetében.[6] A botnetek a DDoS-támadások indításán kívül alkalmasak

[2] Kormányzati Eseménykezelő Központ: Elosztott szolgáltatásmegtagadásos támadás, http://www.cert-hungary.hu/ddos (2017. 09. 21.).

[3] Gyányi Sándor: *Az információs terrorizmus által alkalmazott támadási módszerek és a velük szemben alkalmazható védelem*. PhD-értekezés, Budapest, 2011, 88.

[4] Nagy Zoltán András: A sértett szerepe néhány kibertérben elkövetett bűncselekményben – alkalmazott viktimológia. In: Finszter Géza–Kőhalmi László–Végh Zsuzsanna (szerk.): *Egy jobb világot hátrahagyni… Tanulmányok Korinek László professzor tiszteletére*. PTE ÁJK, Pécs, 2016, 487.

[5] Gyányi (2011): i. m., 89.

[6] European Parliament's Policy Department for Citizens' Rights and Constitutional Affairs: *Cybersecurity in the European Union and Beyond: Exploring the Threats and Policy Responses.* 2015, 36, http://www.europarl.europa.eu/RegData/etudes/STUD/2015/536470/IPOL_STU(2015)536470_EN.pdf (2017. 09. 24.).

spamküldésre, adathalászatra,[7] hálózatfigyelésre, billentyűzetfigyelésre, különböző rosszindulatú programok, ún. malware-k (pl. ransomware, vagyis zsarolóvírus) terjesztésére, illetve az internetes reklámokhoz a klikkelések begyűjtésére.

A DDoS-támadásokat a botok terjeszkedési fázisa előzi meg, amely során a malware eljuttatása a cél, hogy megfertőzzenek vele minél több rendszert, melynek révén végül átveszik a gépek feletti irányítást, és az összehangolt támadáshoz felhasználják azokat.[8] Minél több, illetve nagyobb erőforrással rendelkező fertőzött taggal bővül a botnethálózat, annál nagyobb szabású támadást lehet végrehajtani,[9] bár az Europol[10] felhívja a figyelmet arra, hogy ezek a nagyszabású támadások már könnyen megvalósíthatók kisebb számú, de ellenállóbb botnetekkel is.[11] Kezdetben 100 Gbps támadások voltak megfigyelhetők, napjainkra a 300 Gbps-ot is meghaladja, sőt az Europol jelentése szerint 600 Gbps támadásra is sor került és 24 óránál tovább is tarthatnak.[12]

Fontos megjegyezni, hogy bármely felhasználó számítógépe bármikor válhat könnyedén „zombigéppé". A káros botnetkódok ugyanúgy jutnak el az óvatlan felhasználó számítógépeire, mint bármely más fertőzések. A számítógépek a számítógépes hálózatra történő csatlakozással már ki vannak téve a veszélynek, a kockázat pedig különösen megnövekedett *az új mobilinformatikai és Internet of Things (IoT) eszközök* elterjedésével, főleg azért, mert utóbbinak még nincs megfelelően biztosított informatikai védelme (pl. a Mirai botnetvírus közel 150 000 routert és biztonsági kamerát fertőzött meg, a segítségével szokatlanul erős DDoS-támadást hajtottak végre az USA egész keleti partján, ahol több óráig az internetszolgáltatás szünetelt).[13]

Napjainkban a botnetek a technológiai fejlődésnek köszönhetően már megosztott hálózatokon, fájlmegosztó rendszereken, Peer-to-Peer (P2P) hálózatokon, közösségi oldalakon keresztül is terjedhetnek.

Az informatikai bűnözés egy szolgáltatásalapú üzleti modellé vált az elmúlt években, új trendként jelent meg, hogy a DDoS-támadások indítására szolgáló botneteket, illetve a létrehozásukra szolgáló eszközöket, programokat mint egy szolgáltatásként bérelni *(DDoS-for-hire vagy DDoS-as-a-Service)* – napi vagy havi díjjal átlagosan 5$ és 1000$ közötti áron –, vagy akár megvásárolni lehet manapság a fekete online piacokon és fórumokon keresztül (pl. Alphabay és Exploit). Ezek a piacok az

[7] A botnetek képesek nagy mennyiségű személyes vagy egyéb titkos adat megszerzésére. Általában jól ismert cégek – főleg bankok, pénzintézetek – nevében e-mail-üzeneteket küldenek, melyekben azt kérik a felhasználótól, hogy lépjen be elektronikus úton fiókjába. A levél általában egy linket is tartalmaz, hogy az áldozat könnyebben eljuthasson a honlapra. A link azonban nem a cég weblapjára mutat, hanem egy ahhoz kísértetiesen hasonlító – esetleg kívülről nem is megkülönböztethető – álhonlapra, amely többnyire a botnet valamely tagján fut.

[8] Farago Márton–Mészáros Tamás: *Anonim rendszer botnet forgalom felismerésére és szűrésére*. TDK dolgozat, 2009, 10, http://math.bme.hu/~slovi/farago_meszaros_TDK.pdf (2017. 09. 21.).

[9] Gyányi Sándor: A botnetek, a túlterheléses támadások eszközei. *Magyar Rendészet*, 2013, Különszám, 24.

[10] Európai Rendőrségi Hivatal.

[11] European Parliament's Policy Department for Citizens' Rights and Constitutional Affairs: i. m., 36.

[12] Europol: *The Internet Organised Crime Assessment (IOCTA).* 2016, 35, https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2016 (2017. 10. 24.).

[13] Internet Security Threat Report. 2017/22, https://www.symantec.com/content/dam/symantec/docs/reports/istr-22-2017-en.pdf (2017. 11. 05.).

ún. *Darkneten* találhatók és nehezen lenyomozhatók, ami köszönhető annak, hogy a speciális és egyben magas fokú anonimitást biztosító *Tor böngészőn* keresztül érhető csak el. A nyomozó hatóságok számára további nehézséget okoz az is, hogy az elkövetők általában pszeudoanonimitást biztosító, nehezen lenyomozható *virtuális fizetőeszközöket* használnak, mint például a *Bitcoin*. A szolgáltatás igénybevételével a hozzá nem értő felhasználók is olcsón, egyszerűen és gyorsan tudnak támadást indítani, mert csak a célpontot kell kiválasztaniuk és egy egérkattintás az egész, sőt sokszor a végrehajtáshoz még technikai segítséget is kapnak.[14]

2. A DDoS-támadások mögött húzódó motiváció

2.1. Anyagi haszonszerzés

A túlterheléses támadásokat sokszor *anyagi haszonszerzés* céljából indítják. Például egyre gyakoribb, hogy *zsarolás* során használják fel, amit az áldozatoktól online fizetés – általában Bitcoin – formájában követelnek. Az elkövetők elsősorban olyan cégek oldalait választják ki, amelyek folyamatos és zavartalan működést követelnek meg (pl. webshopok, online szerencsejáték és fogadócégek, energia- és pénzügyi szféra). 2016-ban az Europol sikeres akciót hajtott végre, és letartóztatta a zsarolásokban élen járó *DD4BC (Distributed Denial of Service for Bitcoin) Team hackercsoportnak* a kulcsfontosságú tagjait, akik számos DDoS-támadást indítottak európai cégekkel szemben. Az általuk alkalmazott zsarolóséma a következőképpen néz ki: felmérik a célpont hálózati sérülékenységét, majd kisebb DDoS-támadásokat indítanak a céggel szemben, ezt követően a további támadások indításának elkerülése érdekében Bitcoin formájában fizetséget kérnek a cégtől. Abban az esetben, ha az áldozat ennek a követelésnek nem tesz eleget, akkor további, erőteljesebb támadásokat indítanak a cég oldalával szemben, amely annak akár a teljes elérhetetlenségéhez is vezethet. Azonban nem javasolt, hogy fizessenek a zsarolóknak, mert nincs garancia a fizetség esetén sem a további támadás elkerülésére. A DD4BC csapatnak a módszere egyre elterjedtebbé vált, és már „copycat" hackercsoportok is megjelentek, akik másolják őket.[15]

[14] Europol: *The Internet Organised Crime Assessment (IOCTA)*. 2014, 19–21, https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2014 (2017. 10. 25.).

[15] Connelar, Phillip: Pokerstars, DDoS Attackers Arrested by Europol, Extortion Group Also Alleged to Have Targeted Betfair, Neteller. (Cardchat News, 2016. január 29.) https://www.cardschat.com/news/pokerstars-ddos-attackers-arrested-by-Europol-extortion-group-also-alleged-to-have-targeted-betfair-neteller-18629 (2017. 09. 18.). Nemzeti Elektronikus Információbiztonsági Hatóság: DDoS-támadások, http://neih.gov.hu/zsarolo-ddos (2017. 09. 21.).

2.2. Gazdasági célzat

Az anyagi haszonszerzésen kívül gyakori a *gazdasági célzat,* ami az üzleti versenytársak technológiai folyamatai ellen intézett támadásokban nyilvánul meg. A támadók általában tudatosan, jól időzítve olyan időpontokat választanak a támadásokhoz, amikor az adott célpont nagyobb bevételre számíthat – így ezáltal nagyobb kárt is tudnak okozni –, pl. ilyen a Cyber Monday, Black Friday, a karácsonyi időszak vagy a sportfogadások tekintetében az amerikai Super Bowl. A weboldalak működésének a megszakítása költséges terhet jelent bármely weboldal üzemben tartója számára, legyen szó kis- és középvállalkozásról vagy nagyobb cégről. A támadással járó pénzügyi veszteség esetenként különbözhet és nem kizárt, hogy az adott vállalkozás működésére hosszú távon is hatással lehet. Ez megnyilvánulhat a kieső és pótolhatatlan bevételben, illetve akár presztízsveszteséget is okozhat, mivel az ügyfelek nem tudják elérni a támadással célzott cég honlapját, sem igénybe venni a cég által kínált szolgáltatást, ezért inkább a konkurens vállalkozásokat választják és lemorzsolódnak az adott cégtől (pl. a pénzügyi ágazaton belül, különösen az értéktőzsde, értékpapír-kereskedés piacán ez pillanatok alatt súlyos és jelentős kárt okozhat).[16]

2.3. Politikai vagy ideológiai indíttatás

A túlterheléses támadások hátterében politikai vagy ideológiai indíttatás is állhat, amit az ún. *hacktivizmus*[17] elnevezéssel illetnek. A hacktivista nem egy csalárd hacker, aki profit érdekében személyes információkat szerez meg vagy egyéb súlyos kárt okoz, hanem tevékenységével az a célja, hogy felhívja a figyelmet egy politikai vagy társadalmi ügyre. Számára a hacktivizmus egy internet által biztosított stratégia, amely lehetővé teszi a polgári engedetlenség gyakorlását (pl. a DDoS-támadások indításával, a weboldal felülírásával, azaz „defacement"-tel, információk jogosulatlan megszerzésével, illetve azok későbbi nyilvánosságra hozatalával vagy egyéb virtuális szabotázsakciókkal).[18]

Az egyik legismertebb hacktivista csoport *az Anonymous,*[19] akiknek a támadásai rendszerint valamilyen általuk fontosnak vélt, közös ügyet szolgálnak, például az emberi jogokat, szólásszabadságot vagy információszabadságot. A csoport nevében intéztek már támadást amerikai, izraeli, tunéziai, ugandai és brazil kormányzati, illetve gyermekpornográfia tartalmú oldalakkal, valamint szélsőségesen rasszista

[16] Urcuyo, Michael S.: From Internet Trolls to Seasoned Hackers: Protecting Our Financial Interests from Distributed-Denial-Of-Service Attacks. *Rutgers Computer & Technology Law Journal,* 2016/2, 300–330.

[17] A hacktivizmus, avagy a „hactivism" elnevezés a „hacking" és az „activist" szavak összevonásából ered.

[18] Hactivism. (Techopedia. The IT Program for Leaders.) https://www.techopedia.com/definition/2410/hacktivism (2017. 10. 21.).

[19] Török Szilárd: Anonymous a világban és Magyarországon. *Felderítő Szemle,* 2014/1, 192. Az Anonymous egy nemzetközi hackercsoport, amely formálisan 2003-tól létezik, és 2008 óta indít támadásokat. Több, egymástól független sejtből áll, a világ számos országában vannak aktivistái. A csoport megalakulását a „4chan" internetes oldalhoz kötik, és a Guy-Fawkes álarc használatával váltak ismertté.

szervezetekkel szemben (mint például a Westboro Baptist Church), de nagyvállalatok is váltak már célpontjukká. A másik ismert csoport a *LulzSec,* akiknek hasonló támadásaik voltak ugyanúgy kormányzati (pl. CIA szervere elleni túlterheléses támadás) és nagyvállalati rendszerek ellen (pl. Sony).[20]

2012-ben önkéntes, hacktivisták által koordinált DDoS-támadásokra került sor, amikor a támadók a *Low Orbit Ion Cannon (LOIC)* szoftvert használták azzal a céllal, hogy a számítógépük felhasználható legyen az összehangolt és nagyobb erejű támadások végrehajtásához.[21] Ezt a módszert az Anonymous-tagok alkalmazták a *Wikileaks* és egyben a szólásszabadság melletti szimpátiaakciójuk során, ami az *Operation Payback* néven futott, és olyan szervezetekkel szemben, akik részt vettek az internetes cenzúrában.[22] A Wikileaks pénzeit zároló pénzügyi szolgáltatókat – többek között a PayPal, Visa és Mastercard köztük volt – is ennek tekintették, így a támadásaik fő célpontjait képezték.[23]

Vannak olyan szerzők, akik úgy értékelik, hogy a hacktivisták által indított DDoS-támadások hasonlóságot mutatnak a valóságban utcán zajló tiltakozásokkal, és megfelelő védelemben kellene részesíteni az ilyen megmozdulásokat is és nem feltétlenül bűncselekményként értékelni.[24] Ezt a problémakört elsősorban amerikai kutatók járták körbe, így az amerikai szabályozást vizsgálom röviden. Fontos megjegyezni, hogy ezek az online akciók nincsenek elfogadva a véleménynyilvánítás szabad gyakorlásának módjaként és a CFAA hatálya alá tartoznak.[25] Felmerül az a kérdés, hogy egyáltalán, ha eltekintünk a támadások bűncselekményként való minősítésétől, akkor van-e lehetőség a korlátozástól mentes, szabad véleménynyilvánításra a támadással érintett oldalakon. Az elsődleges akadályt a hacktivizmus alkotmányos védelmének biztosításában *az Egyesült Államok Alkotmányának Első Módosítása* jelenti, amely a szólásszabadsággal és a véleménynyilvánítás szabadságával foglalkozik. Az Első Módosítás alkotmányos védelmet csak a kormányzattal szemben nyújt és meghatározott környezetben, az ún. „nyilvános fórumon". Azonban kérdés, hogy a magántulajdonban lévő oldalak, illetve a kormányzati tulajdonban lévő oldalak – amelyek általában a hacktivisták célpontjait képezik – nyilvános fórumnak minősülnek-e. A Legfelsőbb Bíróság utóbbi megállapításához az ún. *nyilvános* fórum doktrínát alkalmazza, amely során azt kell meghatározni, hogy az adott oldal a következő három kategória közül melyiknek minősül. Ennek megfelelően változik a kormányzati tulajdon használatával kapcsolatos korlátozás mértéke: hagyományos vagy kijelölt nyilvános fórumnak tekinthetők, amelyek alkotmányos védelemben részesülnek, vagy nem nyilvános fórumnak, ahol a kormányzat már szabadabban korlátozhatja a fórum használatát.

[20] Török: i. m., 196.

[21] Gragido, Will–Molina, Daniel–Pirc, John–Shelby, Nick: *Blackhatonomics – An Inside Look at the Economics of Cybercrime.* Syngress, 2013, 55.

[22] O'Malley, George: Hactivism: Cyber Activitism or Cyber Crime? *Trinity Law College Review,* 2013/16, 142.

[23] Kovács László: Kiberháború? Internetes támadások a Wikileaks ellen és mellett. *Nemzet és Biztonság – Biztonságpolitika,* 2011/1, 4.

[24] Lásd Malley: i. m., 137–160.

[25] Joseph Cox: DDoS Isn't Going to Be a Legal Form of Protest Any Time Soon. (The Daily Dot. 2014. június 19.) https://www.dailydot.com/layer8/ddos-attack-political-protest/ (2017. 09. 29.).

A magántulajdonban lévő oldalak nem minősülnek nyilvános fórumnak, illetve a magántulajdon védelme elsőbbséget élvez a szólásszabadsággal szemben, ezért ezeken nem gyakorolható szabadon a véleménynyilvánítás, és a tulajdonos korlátozhatja a használatukat. Az online térben lényegében minden valakinek a tulajdonát képezi, valamennyi weboldal egy fizikai szerverhez kapcsolódik, amely egy cég vagy magánszemély tulajdonában áll és üzemelteti azt. Ez a megközelítés ugyanúgy igaz a kormányzati tulajdonban lévő oldalak esetében is, mert a kormányzatot is megilleti az, hogy a tulajdonának a cél szerinti használatát ellenőrizze, így az Első Módosítás által nyújtott védelem itt sincs biztosítva. A doktrína besorolása szerint a kormányzati oldalak nem tekinthetők tradicionális értelemben vett vagy kijelölt nyilvános fórumnak, ezért ezeken a kormányzat a véleménynyilvánítást korlátozhatja, amennyiben ez indokolt és nem diszkriminatív módon történik.[26]

2.4. Kiberháború, kiberhadviselés

Egyre gyakrabban megfigyelhető, hogy a hackerek nem önállóan cselekednek, hanem mögöttük már felsorakoznak a nemzetállamok is, így az államok által szponzorált kibertámadásokról van szó, amelyek stratégiai és katonai célt szolgálnak és ezeket általában a hivatásos állományban lévő informatikusok vagy megbízott hackerek hajtják végre[27] (pl. az Egyesült Államok Védelmi Minisztériuma 2010-ben létrehozta a katonai Kiberparancsnokságot, míg Kína és Oroszország tagadja, hogy rendelkeznének kiberhadsereggel).[28]

Azt a jelenséget nevezzük *kiberhadviselésnek*, amikor egy állam egy másik állam ellen informatikai támadást indít, amelynek célja az adott ország társadalmi és gazdasági működésének akadályozása vagy ellehetetlenítése. Ez általában egy átfogó támadássorozat, amelynek a kiterjedése és az okozott kár mértéke hatalmas és az egész ország működését veszélyeztetheti. Például a túlterheléses támadások kivitelezése a kibertérben stratégiai és taktikai jelentőségű lehet, mert a valós térben zajló katonai támadásokkal okozott káoszhoz hozzájárulhat, és további potenciált adhat a fizikai támadásokhoz. [29]

Az *első kiberháborúra* 2007 áprilisában került sor, amikor a helyi orosz kisebbség tiltakozása ellenére a tallinni szovjet második világháborús emlékművet lebontották és áthelyezték. Ezt követően utcai tüntetések és zavargások törtek ki, mert Oroszország élesen tiltakozott az eset miatt. Az emlékmű áthelyezését követően hamarosan megindultak a DDoS-támadások is a kormányzat rendszereivel és oldalaival

[26] Xiang, Li: Hacktivism and the First Amendment: Drawing the Line Between Cyber Protest and Crime. *Harvard Journal of Law & Technology,* 2013/1, 313–315, https://www.dailydot.com/layer8/ddos-attack-political-protest/ (2017. 11. 29.).

[27] Nagy Zoltán András: Kiberbűncselekmények, kiberháború, kiberterrorizmus – avagy ébresztő Magyarország! *Magyar Jog,* 2016/1, 21–22.

[28] Berki Gábor: Kiberháborúk, kiberkonfliktusok. In: Dornfeld László–Keleti Arthur–Barsy Miklós–Kilin Józsefné–Berki Gábor–Pintér István: *Műhelytanulmányok – A virtuális tér geopolitikája.* Geopolitikai Tanács Közhasznú Alapítvány, Budapest, 2016, 274.

[29] Stephenson, Peter–Gilbert, Keith: *Investigating Computer-Related Crime.* CRC Press, 2013, 35.

szemben (négy napig internetelérés nélkül volt), valamint támadások érték számos napilap online kiadását, telefontársaságokat (a média és telekommunikációs cégek részleges működésképtelenségéhez vezetett), bankokat (24 órát meghaladó ideig nem vagy csak részleges banki szolgáltatások voltak elérhetőek, ezzel több millió euró veszteséget okozva).[30]

Az észtországi események után 2008 augusztusában az ötnapos orosz–grúz konfliktus volt az első olyan fegyveres összecsapás, amikor a fegyveres harc mellett, azzal párhuzamosan a kibertérben is hatalmas küzdelem folyt (az oroszok adatözönnel árasztották el a grúz elnök, a minisztériumok, hírszolgáltatók oldalait). Azonban a támadások forrása még mindig vita tárgyát képezi, bár a rendelkezésre álló bizonyítékok alapján vélhetően orosz bűnszervezet volt a felelős értük, de egyértelműen a mai napig nem tudják megállapítani és a felelősségre vonást kezdeményezni.[31]

Reagálva ezekre az eseményekre a NATO Kibervédelmi Kiválósági Központ munkatársai elsőként készítették el *a kibervédelmi* kézikönyvet *(Tallinn Manual),* amely jogi kereteket ad az informatikai hadviseléshez a nemzetközi jogban már meglévő rendelkezések megfelelő alkalmazásával.[32]

A 2010-ben megjelent *Stuxnet* féregvírussal új fejezet kezdődött a kiberhadviselésben, ami mögött vélhetően az amerikai és izraeli szakemberek álltak. A Stuxnet volt az első komoly célzott támadás, amelyet ipari rendszerek ellen vetettek be. Az első kártékony kód volt, amely a kritikus infrastruktúra elemeinek a fizikai károkozásával is járt – sőt ezzel a céllal fejlesztették ki –, és ezáltal Irán atomprogramját lényegében megbénították, mert további több évre volt szükség egy atomfegyver előállításához szükséges dúsított urán legyártásához. Ma már tudjuk, a Stuxnet csak az első ilyen eszköz volt a sorban, testvérei a Duqu, a Gauss vagy a Flamer bizonyítják ezt.[33]

A Stuxnetet követően válaszként – 2011 és 2013 között – rendszeresen indítottak DDoS-támadásokat – amelyek akkoriban rekordokat döntöttek meg a támadások tekintetében – amerikai bankok és pénzintézetek ellen, amelyek között szerepelt a JP Morgan, a Wells Fargo, az American Express kártyatársaság és az AT&T telekommunikációs cég. Az amerikai Igazságügyi Minisztérium hét iráni hackert vádolt meg az elkövetéssel, akik vélhetően az iráni kormány megbízásából hajtották végre a támadásokat a kritikus infrastruktúrákkal szemben. Az Egyesült Államok kormánya szerint Irán megtorlásnak szánta a támadássorozatot a gazdasági szankciók

[30] Kovács László: *Kiberhadviselés Magyarországon (előadás)*. http://uni-nke.hu/uploads/media_items/7-kovacs-laszlo.original.pdf (2017. 01. 25.).

[31] Appazov, Artur: *Legal Aspects of Cybersecurity.* University of Copenhagen, Faculty of Law, 2014, 21–22, http://justitsministeriet.dk/sites/default/files/media/Arbejdsomraader/Forskning/Forskningspuljen/Legal_Aspects_of_Cybersecurity.pdf (2017. 10. 21.).

[32] Lásd Schmitt, Michael N.–Vihul, Liis (eds.): *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations.* Cambridge University Press, Cambridge, 2017.

[33] Nagy Zoltán András: A kiberháború új dimenzió – a veszélyeztetett állambiztonság (Stuxnet, DuQu, Flame – a Police malware). Pécsi Határőr Tudományos Közlemények XIII., 2012, 225–226.

és korábbi informatikai támadások miatt.[34] Tovább bonyolítja a helyzetet, hogy Kína megjelenése a kibertérben hatalmas kihívást jelent, hiszen gyakorlatilag korlátlan anyagi és humán erőforrás áll a rendelkezésére.

3. A DDoS-támadások szabályozása az Egyesült Államokban

Az Egyesült Államokban a CFAA az első *szövetségi szintű,* számítógépes csalással és visszaéléssel foglalkozó törvény, amely 1984-ben lépett hatályba és azóta nyolc alkalommal módosították. A hatályos CFAA hét számítógépes bűncselekményt tartalmaz, ezek közül az egyik az 1030. § (a)(5)(A) pontban szabályozott *számítógépben vagy információban való károkozás* vétsége, amely szerint büntetendő az, *„aki tudatosan olyan programot, információt, kódot vagy parancsot továbbít, amelylyel szándékosan és jogosulatlanul kárt okoz egy védett számítógépben”*. Az 1030. § (a)(5) bekezdés további két (B)–(C) pontjában meghatározott esetekben azonban a szándékos és jogosulatlan hozzáférés a feltétel, amely alapján felelősségre vonható az elkövető, ha jogosulatlanul hatol be a számítógépbe, még akkor is, ha nem terjedt ki a szándéka a károkozásra. Ezzel ellentétben az (A) pontban szabályozott esetben csak a tudatos továbbítás és a szándékos károkozás a feltétele a bűncselekmény megvalósulásának, ami történhet a számítógéphez való hozzáférés nélkül is, például amikor a támadó elárasztja az egyik weboldalt olyan mennyiségű adatcsomaggal a DDoS-támadás révén, amelynek eredményeképpen a honlap hozzáférhetetlen lesz, akkor a károkozás szándékos, azonban az elkövető a támadás során nem fér hozzá a honlaphoz. Az 1030. § (a)(5)(A) bekezdés szerint felelősségre vonható az, aki a DDoS-támadást végrehajtja, illetve az is, aki a rosszindulatú programot ilyen céllal felhasználja vagy továbbítja. Ez következik abból, hogy a DDoS-támadás általában magában foglalja a káros kód továbbítását, amellyel a számítógépeket zombigépekké változtatja és azon kód továbbítását, amelyet arra használ fel az elkövető, hogy az irányítása alá vont zombik számára kiadja a parancsot a támadásra a meghatározott célponttal szemben.[35]

A bűncselekmény elkövetési tárgya *a védett számítógép*, amely: az (A) pont szerint *„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 e cselekmény befolyásolja a számítógépnek a használatát”.* Továbbá a (B) pont szerint *„amelyet államközi kereskedelemre vagy nemzetközi kereskedelemre, illetve államközi vagy 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*

[34] Menn, Joseph: Cyber Attacks Against Banks More Severe Than Most Realized. (Reuters. 2013. május 18.) https://www.reuters.com/article/us-cyber-summit-banks/cyber-attacks-against-banks-more-severe-than-most-realize-idUSBRE94G0ZP20130518 (2017. 11. 29.).

[35] Brenner, Susan W.: *Cybercrime and the Law: Challenges, Issues and Outcomes*. Northeastern University Press, 2012, 49.

az Egyesült Államok államközi kereskedelmére vagy nemzetközi kereskedelmére, vagy kommunikációjára". Orin Kerr kritikával illette a „védett számítógép" elnevezést, mert valamennyi internetre csatlakoztatott számítógépet államközi kereskedelemre vagy nemzetközi kereskedelemre, illetve kommunikációra használnak, hiszen az internet maga egy nemzetközi hálózat, amelyet ezekre a célokra használnak. Tehát ezt szem előtt tartva, bármely internetre csatlakoztatott számítógép lehet a CFAA-ban szabályozott bűncselekmény célpontja, így megfelelőbb lenne a „számítógép" elnevezés használata a „védett számítógép" helyett.[36]

Jelenlegi formájában a CFAA nem kellően elrettentő a DDoS-támadások esetében. További problémát jelent, hogy *nincs egy kiforrott esetjogi háttere* az ilyen típusú ügyeknek, ami abból is következik, hogy nehéz azonosítani és bíróság elé állítani az elkövetőket. Elsősorban nem a CFAA nyújt az ügyészek számára segítséget arra vonatkozólag, hogy hogyan folytassák le a túlterheléses támadás miatt elrendelt eljárást, hanem az igazi útmutatást *az Igazságügyi Minisztérium kézikönyve* adja.[37] Az 1030. § (a)(5)(A) alapján az eljárás megindításához kettő feltétel megléte szükséges: *a továbbítás, illetve a kár.* A bűntettet megalapozó eljáráshoz még egy feltétel szükséges: *a törvényben felsorolt minősített esetek közül legalább egynek meg kell valósulnia.*

Az említett szakasz megtiltja a tudatos DDoS-támadás végrehajtását károkozási célzattal a védett számítógéppel szemben. A törvény szövegében szereplő *„program, információ, kód vagy parancs" továbbítása* tágan magában foglalja azokat az eseteket, amikor a továbbítás képes a számítógép működését befolyásolni. A DDoS-támadás ezt a feltételt teljesíti, mert lényegesen akadályozza a funkcionális működését a megtámadott számítógépnek azáltal, hogy túlterheli az illegitim adatforgalommal.

A következő feltétel, hogy az elkövető kárt okozzon a számítógépben, ami magában foglalja az információ vagy számítógép hozzáférhetetlenné tételét. A *kár fogalma* a következő: *„bármely károsodás, amely az adat, program, rendszer vagy információ hozzáférhetőségének integritását sérti".* Kár akkor is keletkezik, amikor az adott cselekmény a szolgáltatónál lelassulást vagy csökkentett kapacitást eredményez. A túlterheléses támadásnál pedig erről van szó, mert a szerver vagy weboldal – következésképpen a rajta található információ – elérhetetlenné válik és a sértettnél ezáltal kár realizálódik.

Végül ahhoz, hogy bűntett megállapítására kerüljön sor az 1030. § (a)(5)(A) pontja értelmében, legalább egy esetnek meg kell valósulnia a törvényben felsoroltak közül:
– legalább 5000 $ értékű veszteség egy év alatt;
– az egészségügyi ellátás akadályozása;
– fizikai sérelem okozása;
– fenyegetést jelent a közegészségre és közbiztonságra nézve;
– az Egyesült Államok kormánya által vagy érdekében, az igazságszolgáltatásban,

[36] Wang, Qianyun: *A Comparative Study of Cybercrime in Criminal Law: China, US, England, Singapore and the Council of Europe.* PhD Thesis. Erasmus University Rotterdam, 2016, 72–73,108–111.

[37] Lásd Department of Justice: *Prosecuting Computer Crimes.* 2014, https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ccmanual.pdf (2017. 09. 05.).

a honvédelemben vagy a nemzetbiztonságban használt számítógép sérelmére elkövetés;
– károkozás tíz vagy több védett számítógép sérelmére egy év alatt.

A CFAA tágan definiálja *a veszteség fogalmát: „bármely kiadás a sértett részéről, ami magában foglalja a jogsértésre adott válaszokat, kárfelmérést, illetve azt az adatot, programot, rendszert vagy információt, amely a jogsértést megelőző állapotra történő helyreállításával kapcsolatos költségként felmerül és bármely bevételkiesést, költséget, vagy egyéb károsszeget, amely a szolgáltatás szüneteltetésével összefüggésben keletkezett"*. Ezt a legegyszerűbb bizonyítani, mert általában azt a pénzösszeget jelenti, amitől elesik az áldozat a szolgáltatás szüneteléséből adódóan. Amennyiben a leállás minél hosszabb ideig tart, annál nagyobb veszteség keletkezik. A bíróságok egy része azonban a cég jó hírnevét kizárta a veszteségi körből, de például a helyreállítással megbízott alkalmazott munkadíja, a weboldalon elszalasztott hirdetési és értékesítési bevételek is idetartozhatnak.

A CFAA azokkal a támadásokkal szemben is véd, amelyek akadályozzák *„egy vagy több személynek az orvosi vizsgálatát, diagnózisát, kezelését vagy gondozását"* és ez a DDoS-támadásokra is alkalmazandó, amennyiben az egészségügyi ellátást akadályozzák. Azonban a sérelemnek nem kell jóvátehetetlennek vagy jelentősnek lennie, illetve pénzügyi veszteségnek sem kell bekövetkeznie. A bizonyítékokkal elegendő annak az alátámasztása, hogy az elkövető tevékenysége legalább egy betegnek az egészségügyi nyilvántartását potenciálisan érintette. Ez a pont erős védelmet nyújt a kórházak, klinikák és más egészségügyi intézmények rendszerei és a bennük tárolt érzékeny adatok részére.

A harmadik pont akkor valósul meg, ha *„a fizikai sérelem bármely személynél következik be".* Például a forgalmi jelzőlámpák működésének megzavarásával autóbaleset történik és ennek következtében a gépjárművezetők megsérülnek.

A negyedik pont esetében elegendő, ha *a közegészség és közbiztonság veszélybe kerül* a DDoS-támadással, például a forgalmi jelzőlámpák működésének leállása következik be – a közlekedési infrastruktúra elleni túlterheléses támadásnak köszönhetően –, azonban az nem jár fizikai sérelemmel, de az elkövető felelősségre vonható már azért, mert potenciális veszélyhelyzetet idézett elő. Ez a pont elsősorban a kritikus infrastruktúrák[38] (pl. energia-, közlekedési, egészségügyi és pénzügyi ágazat stb.) elleni támadásokkal szemben lép fel, melyek igen jelentős kárt tudnak okozni.

A CFAA kiemelten tiltja *az Egyesült Államok kormánya által vagy érdekében használt számítógépekkel szembeni támadásokat, különösen amelyek, az igazságszolgáltatást, a honvédelmet és a nemzetbiztonságot érintik.* A Kongresszus célja ezzel a ponttal az volt, hogy fokozottan védje a kormányzati funkciók, illetve valamennyi

[38] Az Egyesült Államok 1998-ban elnöki irányelvben határozta meg a kritikus infrastruktúra fogalmát, amely 2001-ben lépett hatályba a PATRIOT törvénnyel: „mindazon fizikai vagy virtuális rendszerek és berendezések, amelyek oly létfontosságúak az Egyesült Államok számára, hogy azok korlátozása vagy megsemmisülése meggyengítő hatással lenne a nemzetbiztonságra és a nemzetgazdaság biztonságára, a közegészségre, közbiztonságra vagy ezek bármely kombinációjára". https://www.selectagents.gov/resources/USApatriotAct.pdf (2017. 12. 29.).

kormányzati ág zavartalan működését és a felelősségre vonásra sor kerüljön a sikertelen támadás esetén is (pl. ebben az esetben a DDoS-támadásnál nem szükséges, hogy a tényleges kár bekövetkezzen).

Végül az utolsó pont a leggyakoribb eset, amely *a tíz vagy több védett számítógépben való károkozást határozza meg egy év alatt.* Ezt az esetkört a DDoS-támadás könnyen kimeríti, mert minden támadás végrehajtásához általában több fertőzött számítógépre van szükség.

A CFAA 1030. § (b) bekezdése értelmében büntetendő az 1030. § (a) bekezdéseiben szabályozott bűncselekményeknek *a kísérlete és az elkövetésben való megállapodása* (előkészületi cselekménye) is.

Aki tudatosan továbbít programot, információt, kódot vagy parancsot és szándékosan kárt okoz a védett számítógépben, de nem eredményezi a korábban felsorolt hat sérelem közül egyiket sem, az vétséget követ el és *egy évig terjedő szabadságvesztéssel és/vagy pénzbüntetéssel büntetendő*. A visszaeső *tíz évig terjedő szabadságvesztéssel büntethető*.

Amennyiben a tudatos továbbítás és szándékos károkozáson felül megvalósul a hat sérelem közül legalább az egyik, akkor az elkövető bűntett miatt *maximum tíz évig terjedő szabadságvesztéssel és/vagy pénzbüntetéssel büntetendő*.

Maximum húsz évig terjedő szabadságvesztéssel büntethető az, aki az 1030. § (a)(5)(A) pont megsértésével bűntettet követ el és elítélik a CFAA hatálya alá tartozó más bűncselekmény elkövetéséért is.

2002-ben a Kongresszus további rendelkezést vezetett be és a büntetési tételt megemelte, ha súlyos fizikai sérülés következik be eredményként. Amennyiben az elkövető szándékosan kárt okoz a védett számítógépben és megkíséreli vagy tudatosan, vagy gondatlanságból súlyos fizikai sérülést okoz, akkor *a maximum szabadságvesztés húsz évre emelkedik*. Végül életfogytig tartó szabadságvesztést szabhat ki a bíróság akkor, ha az elkövető tudatosan vagy gondatlanságból halált okoz vagy megkíséreli.[39]

4. Az információs rendszerek elleni támadásokkal szembeni fellépés Európában

Az Európai Unióban *az információs rendszerek elleni* támadásokról szóló *2013/40/EU irányelv* váltotta a 2005/222/IB tanácsi kerethatározatot, amely két fő célt tűzött ki: *a minimumszabályok meghatározását* az információs rendszer elleni bűncselekményekre, a büntetőjogi szankciókra vonatkozóan és *az együttműködés elősegítését* a nemzeti rendvédelmi szervek és az erre specializálódott uniós szervek között, nevezetesen az Europol, az EC3,[40] az Eurojust[41] és az ENISA[42] között.

[39] URCUYO: i. m., 300–330; Department of Justice: i. m., 35–49.

[40] Számítástechnikai Bűnözés Elleni Európai Központ.

[41] Az Európai Unió Igazságügyi Együttműködési Egysége.

[42] Az Európai Unió Hálózat- és Információbiztonsági Ügynöksége.

Az irányelv meghatározza a 2. cikk *a)* pontjában az információs rendszer fogalmát[43] és a 3–7. cikkekben a következő bűncselekményeket szabályozza: az információs rendszerekhez való jogellenes hozzáférést, a rendszert érintő jogellenes beavatkozást, az adatot érintő jogellenes beavatkozást és a jogellenes adatszerzést. A tagállamoknak rendelkezniük kell arról, hogy ezekkel a bűncselekményekkel szemben hatékony, arányos és visszatartó erejű büntetőjogi szankciókat alkalmazzanak.

A DDoS-támadás az irányelv 3. cikke szerinti *rendszert érintő jogellenes beavatkozásnak minősül*, amely szerint valamely információs rendszer működésének számítógépes adatok szándékos és jogosulatlan bevitele, továbbítása, megrongálása, törlése, minőségi rontása, megváltoztatása vagy elrejtése, vagy ilyen adatok szándékos és jogosulatlan hozzáférhetetlenné tétele révén történő súlyos akadályozása vagy megszakítása, legalább a súlyosabb esetekben a tagállamoknak bűncselekményként kell értékelniük. A bűncselekmény elkövetésének minden esetben szándékosnak kell lennie. A bűncselekményre való felbujtás, az azokban való bűnrészesség, valamint bűnpártolás, illetve az elkövetésükre irányuló kísérlet is büntetendő.

Az irányelv először hívta fel a figyelmet *a botnetekre mint veszélyforrásokra*, mert felismerték, hogy általuk egyre veszélyesebb, ismétlődő és átfogó támadásokat tudnak végrehajtani, amelyek gyakran kulcsfontosságú információs rendszereket (pl. kritikus infrastruktúrákat) érintenek. Az irányelv először állapít meg büntetőjogi szankciót a botnetek létrehozására, amelyek súlyos kárt képesek okozni, de ennek meghatározása, hogy mi minősül súlyosnak, az a tagállamok döntési jogkörébe tartozik (pl. fontos és közérdekű rendszerszolgáltatások megzavarása, jelentős költségek okozása vagy személyes adatok, illetve különleges adatok, információk elvesztése stb.).

Súlyosító körülménynek minősül, ha egy bűncselekményt – az irányelv meghatározása szerint – *bűnszervezetben követtek el,* illetve az *súlyos kárt vagy alapvető érdeksérelmet okozott.* Büntetendő és súlyosabb szankció megállapításának van helye, ha: *a támadás átfogó*, azaz jelentős számú információs rendszert érint vagy súlyos kárt okoz, ideértve azokat a támadásokat is, amelyek célja egy botnet létrehozása, vagy amelyeket botnet révén hajtanak végre, és ezáltal súlyos kárt okoznak. Helyénvaló arra az esetre is súlyosabb szankciókat megállapítani, ha a támadás *valamely tagállam vagy az Unió kritikus infrastruktúrája*[44] *ellen irányul*. Ez azért indokolt, mert a kritikus infrastruktúrák egyes elemeinek működése, illetve együttműködése oly mértékben függnek az információs rendszerektől, hogy azok

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

[44] 2008/114/EK tanácsi irányelv az európai kritikus infrastruktúrák azonosításáról és kijelöléséről, valamint védelmük javítása szükségességének értékeléséről. HL L 345, 2008. 12. 23., 77.: *„kritikus infrastruktúra: a tagállamokban található azon eszközök, rendszerek vagy ezek részei, amelyek elengedhetetlenek a létfontosságú társadalmi feladatok ellátásához, az egészségügyhöz, a biztonsághoz, az emberek gazdasági és szociális jólétéhez, valamint amelyek megzavarása vagy megsemmisítése e feladatok folyamatos ellátásának hiánya miatt jelentős következményekkel járna valamely tagállamban".*

összeomlása vagy megsemmisülése súlyos következményekkel járhat nemcsak az adott infrastruktúrára nézve, hanem más kritikus infrastruktúrákra nézve is. A támadások éppen ezért általában az infrastruktúrán belül az ún. *kritikus információs infrastruktúra* részeit célozzák. Ezek azok az infokommunikációs rendszerek, amelyek önmagukban is kritikus infrastruktúra-elemek, vagy lényegesek az infrastruktúra működésének szempontjából (pl. számítógép-hálózat és programok stb.).[45] Érdemes felhívni a figyelmet arra, hogy az uniós rendvédelmi szervekhez bejelentett, kritikus infrastruktúrákat érintő támadások között a DDoS-támadások dominálnak és egyre gyakoribbak a célzott támadások.[46]

A támadásokat a legkülönbözőbb módokon követik el, amit lehetővé tesz a hardverek és szoftverek gyors ütemű fejlesztése. Az irányelv éppen ezért minden olyan eszközre utal, amit a benne felsorolt bűncselekmények elkövetésére lehet használni, különösen ilyenek a rosszindulatú programok, főleg amelyek a botnetek létrehozására is alkalmasak. Ezért az ilyen eszközök jogosulatlan és bármely irányelvben említett bűncselekmény elkövetéséhez való felhasználásának szándékával való előállítását, árusítását, használatra történő beszerzését, behozatalát, forgalomba hozatalát vagy egyéb módon történő hozzáférhetővé tételét legalább a súlyosabb esetekben bűncselekménynek kell minősíteniük a tagállamoknak. Fontos, hogy az objektív kritériumok megléte mellett a szándéknak is arra kell irányulnia, hogy az eszközt egy vagy több bűncselekmény elkövetéséhez használják fel.[47]

Az irányelv az együttműködéssel kapcsolatban kihangsúlyozza, hogy a tagállamoknak a megfelelő információcsere érdekében gondoskodniuk kell a saját operatív nemzeti kapcsolattartó pontjuk létrehozásáról és a szükséges információk eljuttatásáról az Europol és az ENISA részére. Az Europolon belül az EC3 támogatja a bűnügyi nyomozásokat, és elősegíti az egész Unióra kiterjedő megoldásokat a számítástechnikai bűnözéssel szemben. Az EC3-n belül *a Focal Point Cyborg* lép fel a tisztán számítástechnikai bűncselekményekkel – köztük a botnet infrastruktúrákkal és DDoS-támadásokkal – szemben, amelyek az uniós kritikus infrastruktúrát és információs rendszereket érintik.[48]

5. A magyar szabályozás

Az uniós irányelvnek megfelelően – eleget téve a jogharmonizációs kötelezettségnek – az új 2012. évi C. törvény a Büntető Törvénykönyvről (a továbbiakban: Btk.) átalakította az informatikai bűncselekményekre vonatkozó szabályozást mind elnevezésben és mind tartalmilag: külön a XLIII. fejezetbe kerültek a *„A tiltott adatszer-*

[45] Muha Lajos: a Magyar Köztársaság kritikus információs infrastruktúrájának védelme. PhD-értekezés. Zrínyi Miklós Nemzetvédelmi Egyetem, Budapest, 2007, 36–37, http://real-phd.mtak.hu/74/1/1228916.pdf (2017. 12. 19.).

[46] Europol: *The Internet Organised Crime Assessment (IOCTA).* 2017, 26, https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2017 (2017. 12. 29.).

[47] Az Európai Parlament és a Tanács 2013/EU irányelve (2013. augusztus 12.) az információs rendszerek elleni támadásokról és a 2005/222/IB tanácsi kerethatározat felváltásáról. HL L 218, 2013. 08. 14., 8–13.

[48] European Parliament's Policy Department for Citizens' Rights and Constitutional Affairs: i. m., 53–54.

zés és információs rendszerek elleni bűncselekmények" címmel, illetve a korábbi *„számítástechnikai rendszer"* terminológia helyébe az *„információs rendszer"* lépett, ami a kor kihívásainak jobban megfelel. Az új Btk. értelmében egy DDoS-támadás végrehajtása a 423. § szerint *az információs rendszer vagy adat megsértésének minősül,* és a (2) bekezdés *a)* pontja szerint büntetendő, *aki az információs rendszer működését jogosulatlanul vagy jogosultsága kereteit megsértve akadályozza.*

A bűncselekmény elkövetési tárgya *az információs rendszer,*[49] amelynek a betöltött funkciója a meghatározó.[50] A törvény azonban nem határozza meg a releváns elkövetési magatartásokat, ezért bármely cselekmény tényállásszerű lehet, amely az információs rendszer működésének akadályozását eredményezi. *Akadályozáson* nem kizárólag azt kell érteni, hogy a rendszer nem működik vagy nem megfelelően működik, hanem azt is, *ha a rendszer nem alkalmas a rendeltetésének megfelelő feladat ellátására*. Az elkövető tudatának át kell fognia azt a tényt, hogy cselekményével jogosulatlanul akadályozza az információs rendszer működését. Az elkövetési magatartás megkezdésével a kísérlet valósul meg és a tényállásszerű eredmény, az akadályozás bekövetkezésével válik befejezetté a bűncselekmény.[51] *A minősített eset* állapítható meg, ha a (2) bekezdésben meghatározott bűncselekmény *jelentős számú információs rendszert érint*, azonban a törvény nem határozza meg, hogy mi tekinthető jelentős számúnak, ez a jogalkalmazókra hárul, hogy egy erre vonatkozó gyakorlatot dolgozzanak ki. A minősített esetre a DDoS-támadás jó példa, hiszen a végrehajtása során a támadó sok száz vagy több ezer felhasználó gépei felhasználásával kísérel meg kapcsolatot létesíteni a megtámadott számítógéppel. E sok száz vagy ezer zombigép egy botnetet alkot, amelyet a támadó vezérel. Az egyszerre küldött nagy mennyiségű adatkérés és továbbítás bénítja a megtámadott információs rendszert.[52] A másik minősített esetben a büntetés két évtől nyolc évig terjedő szabadságvesztés, ha *a bűncselekményt közérdekű üzem ellen követik el*. A Btk. az értelmező rendelkezések között a 459. § 21. pontjában meghatározza exemplifikatív felsorolással, hogy mi minősül közérdekű üzemnek: a közmű, a közösségi közlekedési üzem, az elektronikus hírközlő hálózat, az egyetem és a postai szolgáltató közérdekű feladatainak teljesítése érdekében üzemeltetett logisztikai, pénzforgalmi és informatikai központok és üzemek. Ezzel a probléma az, hogy *a közérdekű üzem és a kritikus infrastruktúra fogalma*[53] *nem fedi egymást,* így a cselekmény minősí-

[49] Btk. 459. § (1) bekezdés 15. pont: *„információs rendszer: az adatok automatikus feldolgozását, kezelését, tárolását, továbbítását biztosító berendezés, vagy az egymással kapcsolatban lévő ilyen berendezések összessége".*

[50] Tóth Mihály: Alkothatók-e az informatikai bűnözés változatos formáit lefedni képes büntetőjogi tényállások? In: Gál István László–Nagy Zoltán András (szerk.): *Informatika és büntetőjog.* PTE ÁJK, Pécs, 2006, 184.

[51] Molnár Gábor: XLIII. fejezet – Tiltott adatszerzés és az információs rendszer elleni bűncselekmények. In: Kónya Sándor (szerk.): *Magyar Büntetőjog – Kommentár a gyakorlat számára (Harmadik kiadás).* HVG-ORAC, Budapest, 2016, 948.

[52] Nagy Zoltán András: XLIII. fejezet. A tiltott adatszerzés és az információs rendszer elleni bűncselekmények. In: Tóth Mihály–Nagy Zoltán András (szerk.): *Magyar Büntetőjog: Különös rész.* Osiris, Budapest, 2014, 598.

[53] A Kritikus Infrastruktúra Védelem Nemzeti Programjáról szóló 2080/2008. (VI. 30.) kormányhatározat 1. sz. melléklet 3.2. pontja: *„kritikus infrastruktúrának minősülnek azon hálózatok, erőforrások, szolgáltatások, termékek, fizikai vagy információtechnológiai rendszerek, berendezések, eszközök és azok alkotórészei, melyek működésének meghibásodása, megzavarása, kiesése vagy megsemmisítése, közvetlenül vagy közvetetten, átmenetileg vagy hosszú távon súlyos hatást gyakorolhat az állampolgárok gazdasági, szociá-*

tése vitatott lehet, in concreto a szociális jólét, a közegészség intézményei ellen intézett támadások esetében. Erre azért is fontos felhívni a figyelmet, mert 2017 óta bevezetésre került az elektronikus egészségügyi rendszer, ami azt jelenti, hogy ettől kezdve valamennyi személyes adatot és az intézményi ellátási dokumentumokat elektronikus úton tárolják, ezáltal fokozott veszélynek vannak kitéve az esetleges informatikai támadásokkal szemben.

Ahogy korábban említettem, a túlterheléses támadások kivitelezését rendkívül megkönnyíti az, hogy könnyen hozzá lehet jutni a bűncselekmény elkövetéséhez szükséges ismeretekhez, programokhoz, akár a már kész botnet-infrastruktúrához, és ezért is fontos, hogy már az *előkészületi cselekmények sui generis bűncselekményként kerüljenek meghatározásra*. Ennek megfelelően a Btk. 424. §-ban szabályozza *az információs rendszer védelmét biztosító technikai intézkedés kijátszásának vétségét*. A bűncselekmény elkövetési tárgya az információs rendszer felhasználásával elkövetett csaláshoz vagy az információs rendszer vagy adat megsértésének *elkövetéséhez szükséges, vagy azt megkönnyítő jelszó, számítástechnikai program, valamint az ezek készítésére vonatkozó gazdasági, műszaki, szervezési ismeret.* A (3) bekezdés értelmező rendelkezése meghatározza, hogy a jelszó: az információs rendszerbe vagy annak egy részébe való belépést lehetővé tevő, számokból, betűkből, jelekből, biometrikus adatokból vagy ezek kombinációjából álló bármely azonosító.

A bűncselekmény elkövetési magatartásai két fordulatban kerülnek meghatározásra. Az *a)* pont szerinti fordulat *elkövetési magatartásai a jelszó vagy számítástechnikai program készítése, átadása, hozzáférhetővé tétele, megszerzése vagy forgalomba hozatala.* A készítés eredménye például a kész program. Az átadás történhet a birtokba adáson kívül, a rendelkezésre bocsátással, illetve a megfelelő ismeret átadásával. A hozzáférhető tételnek minősül minden olyan tevékenység vagy mulasztás, amelynek köszönhetően hozzáférhetővé válik a jelszó vagy program az arra nem jogosult részére. A megszerzés a rendelkezési lehetőség megteremtését foglalja magában. A forgalomba hozatal esetén az elkövető több személynek juttatja el a jelszót vagy a programot.

A *b)* pont szerinti fordulat *elkövetési magatartása a jelszó vagy számítástechnikai program készítésére vonatkozó szervezési ismeret másnak a rendelkezésére bocsátása.* A rendelkezésre bocsátás azt jelenti, hogy az érintett személy a tényállásba foglalt ismeret birtokába jut. Ezt kimeríti a tudomásszerzés, de előfordulhat az is, hogy az ismereteket valamely tárgy tartalmazza, és ezt bocsátják a rendelkezésére.

A bűncselekmény mindkét fordulata *csak szándékosan – egyenes szándékkal – követhető el,* és az elkövető szándéka arra kell, hogy irányuljon, hogy akár ő maga vagy tőle különböző személy az információs rendszer felhasználásával elkövetett csalást vagy az információs rendszer vagy adat megsértését elkövesse.

A bűncselekmények *rendbelisége* az informatikai rendszerek számához igazodik.[54]

Külön érdekesség, hogy a magyarországi botnetfertőzöttségre figyelmeztető 2015-ös Symantec-tanulmány szerint Magyarország a botnetvírussal fertőzött

lis jólétére, a közegészségre, közbiztonságra, a nemzetbiztonságra, a nemzetgazdaság és a kormányzat működésére".

[54] Molnár: i. m., 946–954.

számítógépek számát tekintve a 6. legfertőzöttebb ország a világon – Kína, USA, Tajvan, Törökország és Olaszország előz meg minket –, és a 2. helyet foglalja el az európai országok között.[55] 2016-ban pedig a magyar kormányzati informatikai rendszert és oldalakat is sorozatos DDoS-támadás érte, aminek köszönhetően több óráig nem voltak elérhetőek a különböző szolgáltatások.[56]

6. Zárógondolatok

A legtöbb informatikai támadás az Egyesült Államok ellen irányul, ami következik abból, hogy politikai és gazdasági nagyhatalomról van szó, így elsődleges célpontja ezeknek a támadásoknak. Éppen ezért az Egyesült Államokhoz fűződik az első számítógépes bűnözésre vonatkozó önálló törvénynek a megalkotása, 1984-ben. A CFAA szabályozza a DDoS-támadásokra vonatkozó rendelkezéseket is részletesen.

A DDoS-támadások száma évről évre növekszik, egyre gyakoribbak a célzott és komplexebb támadások, különösen, amelyek a kritikus infrastruktúrákat érintik, ezért az Európai Uniónak is válaszolnia kellett-e jelenségre. A 2013/40/EU uniós irányelv hívta fel először a figyelmet a botnetekre, és határozta meg a kriminalizálandó magatartások, valamint büntetőjogi szankciók körét, és ennek megfelelően módosult a hazai szabályozás is. Európában az amerikai megoldástól eltérően nem az jellemző, hogy külön törvényt alkotnak a számítógépes bűncselekmények szabályozására, hanem a nemzeti büntető törvénykönyvbe integráltan, annak részeként határozzák meg azokat.

A botnetek és a DDoS-támadások egy komplex problémát jelentenek, amelyhez többlépcsős megoldási stratégiára van szükség. Az információs rendszereket érintő támadásoknál az egyik legnagyobb gondot az elkövetők felderítése okozza, mert a nyomozó hatóságok nem tudják meghatározni a pontos fizikai helyét az elkövetőknek, vagy a bűnözői infrastruktúrának, az elektronikus bizonyítéknak, amelyek a nyomozás szempontjából kiemelt jelentőségűek. A túlterheléses támadás esetén általában az elkövetők hamis IP-címeket használnak fel, ami miatt a támadók, vagy akár a támadás céljából felhasznált számítógépek nem vagy nehezen azonosíthatók.

További problémát jelent, hogy sokszor az elkövetők, sértettek, adatok és az infrastruktúra különböző országokban találhatók, ami pedig joghatósági kérdést vet fel, mégpedig, hogy melyik ország jogosult eljárni az ügyben és mely ország jogrendszere szerint. Ez eredményezheti azt is, hogy az ügyben érintett országok párhuzamosan indítanak büntetőeljárást.

A másik problémát az egyes államok büntetőjogi szabályozásának különbözősége jelenti, például eltérések mutatkoznak az egyes kriminalizált magatartások között, mert van, ahol az adott cselekmény bűncselekménynek minősül, míg másik

[55] Internet Security Threat Report. 2015/20. https://www.symantec.com/content/en/us/enterprise/other_resources/21347933_GA_RPT-internet-security-threat-report-volume-20-2015.pdf (2017. 09. 05.).

[56] Lásd a Belügyminisztérium által közzétett jelentést: http://www.kormany.hu/hu/belugyminiszterium/hirek/senki-nem-vallalta-magara-a-kormanyzati-informatikai-rendszerek-elleni-tamadast (2017. 09. 09.).

országban nem, és ezáltal menedéket biztosít az elkövetők számára. Ez részben köszönhető annak, hogy a tagállamok hiányosan veszik át a nemzeti jogukba a nemzetközi dokumentumokat. A hiányosságokat kompenzálhatná egy meglévő kiforrott esetjog is, azonban ez hiányzik mind az Egyesült Államokban, illetve Európában és hazánkban is. A másik probléma a szabályozás hiánya egyes kérdésekben például az online feketepiacokra és a virtuális fizetőeszközökre vonatkozóan.

Az informatikai bűnözéssel szembeni hatékony fellépéshez nélkülözhetetlen a nyomozó hatóságok és a magánszektor közötti együttműködés. A privát szektor nemcsak a bizonyítékok megőrzése szempontjából fontos, hanem kulcsszerepet játszik a bűnözői infrastruktúrák felszámolásában, illetve a jogellenes tartalmak eltávolításában is. Az együttműködés azért is különösen fontos, mert lehetővé tesz egy proaktívabb és gyorsabb megközelítést az információs rendszereket célzó támadásokkal szemben. Ehhez azonban szükség lenne konszenzusra a jogszabályi alap megteremtéséhez, ami elősegítené a bizalmon alapuló együttműködést, egyúttal a jogi és átláthatósági kérdéseket is rendezné az együttműködéssel kapcsolatban.

A nemzetközi együttműködés a rendvédelmi szervek között is kiemelt jelentőségű, amely során a kölcsönös jogsegélynek van főszerepe, aminek célja a bizonyítékok határokon átnyúló összegyűjtése. Azonban jelenleg ez igen lassú és nem túl hatékony rendszer, köszönhetően az országonként különböző jogrendszereknek.

Összefoglalva, fontos a harmonizált, egységes nemzetközi szabályozás megteremtése mind anyagi, mind eljárásjogi tekintetben. A fokozott együttműködés elősegítése is lényeges elem a magánszektor és a bűnüldöző hatóságok között, illetve az egyes bűnüldöző hatóságok között. Szükséges továbbá, hogy az új kihívásokra a jogalkotók adekvát módon és gyorsan reagáljanak, mint például az online feketepiacokra és a virtuális fizetőeszközökre, a célzott támadásokra, az új platformok védelmére, különösen az IoT és mobilinformatikai eszközök sebezhetőségek kihasználásának megakadályozására és a kritikus infrastruktúrák biztonságának a biztosítására.

Abstract

The Internet offers an opportunity to launch y wide range of cyberattacks such as Distributed Denial of Service (DDoS) attack, which exploits the vulnerabilities of the system network without access. DDoS attacks continue to grow in intensity and complexity. Due to the Crime-as-a-Service business model and online criminal markets DDoS attacks have become accessible to anyone willing to pay for such services. It can be launched easily, although it may cause serious social and economic damage. The aim of this paper to present the criminal provisions of the DDoS attack in the United States, Europe and Hungary.