# A kibertámadások nemzetközi jogi relevanciája és az elkövető büntetőjogi felelőssége

*Jelige:* Cyberwar

*Tagozat:* joghallgató

*Szekció*: büntetőjogi, 10. Internet és bűnözés – a 21. század kihívásai a bűnüldözésben és az igazságszolgáltatásban

2014.

## Tartalomjegyzék

## BEVEZETÉS

*„A civilizáció hajnalán az erő volt a legértékesebb és leghasznosabb tényező. Az erősebb győzött. Pár ezer évvel később a pénz vált a legfontosabbá – akinél a több pénz volt, az több mindent elérhetett. Mára a pénz elvesztette vezető szerepét – napjainkban az első és legértékesebb tényező, az információ. Aki birtokolja az információt, az nyert. És a hacker minden információhoz hozzáfér…"*[1]

A fenti idézettel párhuzamban vizsgálva hasonló következtetéseket vonhatunk le a hadviselés fejlődéséről is. A középkor háborúiban (pl. 100 éves háború, Oszmán Birodalom térhódítása) a döntő még a katonai erő fölötti győzelem volt, erre a korra a haderő integrálása volt a jellemző. Az 19. század fordulópontot jelentett, az ipari forradalom hatására olyan új találmányok jelentek meg, amelyek lehetővé tették a nagyszámú seregek gyors mozgatását, a decentralizált hadműveleteket, a villámháborúkat. Ekkortól a győzelem már nem csak a katonai erő legyőzését tette szükségessé, hanem az ipari infrastruktúra felett aratott diadal is szükségessé vált. Újabb fordulópontot jelentett a 20. század második felének hadviselése, mivel egy harmadik tényező is megjelent – az eddigieknél markánsabb módon – az információé, ekkortól a totális győzelemhez már az információk és adatok feletti teljes uralmat is meg kellett valósítani.

A 20. század végére a számítógépes hálózatok egyre jelentősebb szerepet töltenek be az emberek hétköznapi életében, a gazdasági életben, az államigazgatásban, és a fegyveres erőknél is. Ezen hálózatok globális térben helyezkednek el, amit kibertérnek nevezünk. E kibertérnek azonban éppen úgy részei a bűnözők, a terrorista csoportok is, amely újabb lehetőségeket biztosít számukra. Dennis C. Blair az Amerikai Egyesült Államok Nemzeti Hírszerzésének[2] igazgatója jelentésében hangsúlyozta, hogy *„a növekvő információs rendszerek közötti kapcsolat, az internet illetve egyéb infrastruktúrák lehetőséget teremtenek a támadóknak, hogy megzavarják a távközlési, villamos energia, a pénzügyi hálózatokat, finomítókat, valamint más létfontosságú hálózatokat."*[3] Véleménye szerint az ezeket ért kiber támadás hetekre képes megzavarni az állam működését. A Hivatal becslése szerint a kiberbűnözés évente az USA-nak 42 milliárd, világszerte pedig 140 milliárd dollár kárt okoz. Az Európai Unió véleménye is azonos, legújabb irányelvében úgy fogalmaz, hogy *„bizonyított az olyan, egyre veszélyesebb, ismétlődő és átfogó támadások előfordulása, amelyeket a tagállamok szempontjából, vagy a köz- és magánszféra bizonyos feladatai tekintetében gyakran kulcsfontossággal bíró információs rendszerek ellen intéznek."*[4]

Ebben a kibertérben, mint azt fentebb jeleztük az államok fegyveres ereje is jelen van, kérdéses, hogy az ő szerepüket, az általuk kivitelezett támadásokat, hogyan kell értékelni. Tekinthető-e egy kibertérben kivitelezett támadás az ENSZ Alapokmány 51. cikke szerinti fegyveres támadásnak? A humanitárius jog szabályai alkalmazhatóak-e a kiber hadviselésre?

---

[1] BlueBird (magyar hacker) – KAZÁRI CSABA: *Hacker, cracker, warez. A számítógépes alvilág titkai*, Budapest, Computer Panoráma, 2003, 97. o.

[2] 16 hírszerző tevékenységet végző szervezet munkáját kontrollálja. Többek között a CIA-t is.

[3] BLAIR C. DENNIS: *Annal Treat Assessment of the Intelligence Community for the Senate Select Committe on Intelligence. (2009. február 12.)* 38. o. http://archive.org/stream/AnnualThreatAssessmentOfTheIntelligenceCommunityForTheSenateSelect/20090212_testimony#page/n0/mode/2up (2014.03.30.).

[4] Európai Parlament és Tanács 2013/40/EU irányelv az információs rendszerek elleni támadásokról és a 2005/222/IB tanácsi kerethatározat felváltásáról (5) bekezdés.

A másik állam felelőssége megállapítható-e? Dolgozatunkban e kérdésekre kívánunk válaszokat adni. Ezen túl megvizsgáljuk az egyén büntetőjogi felelősségét a kibertámadások megvalósításáért, elkülönítve azt az esetett, ha fegyveres támadásnak minősül azoktól a szabályoktól, amelyek „egyszerű" kibertámadás esetén vonatkoznak az elkövetőre.
Tanulmányunk elkészítéséhez hazai és nemzetközi jogforrásokat, szakirodalmi forrásokat használtunk fel.

## 1. A KIBERTÁMADÁSOK ELKÖVETŐI KÖRE

A kibercselekmények szakértőinek csoportját két különböző szempontból kell elemeznünk, az egyik ilyen szempont a kiberszakembereknek az állammal való kapcsolata, míg a másik a cselekményeik elkövetéséhez szükséges szaktudás. Jelen fejezetben ezen két aspektusnak megfelelően határozzuk meg a kibertámadások elkövetőinek körét.
A kibercselekmények szakértőinek az állammal való kapcsolatuk szerint szintén két területre oszthatók, aszerint, hogy tényleges állammal való kapcsolatról van-e szó vagy éppen ennek ellenkezője, vagyis az állammal való kapcsolat teljesen hiányzik. Ennek megfelelően beszélhetünk állami szervekről, valamint azok személyi állományáról és a magánszemélyekről. Magánszemélyek esetében tehát teljesen hiányzik az állami irányítás, semmilyen kapcsolat nem fedezhető fel az állam és a magánszemély kibercselekménye között, azokat saját ideológiai meggyőződése, olykor a sérelmeikért való bosszú vezeti. Míg az állam szervei és annak személyi állománya esetén már az elnevezésük is előre vetíti, hogy ezen esetekben szoros kapcsolatról van szó, hiszen *„az állam közvetlenül nem cselekedhet, az állami cselekményeket mindig az állam szervei fejtik ki az állam nevében. Ezek az állami szervek viszont vagy egy konkrét személyt, vagy személyek csoportját, azaz valamely testületet jelentenek, így végső soron az állami cselekmények egyben mindig és szükségképpen emberi cselekmények."*[5] Továbbá a jogalkotói apparátus hozza létre ezen szerveket és határozza meg mely személyek lehetnek tagjai, illetve az államigazgatási szervezetrendszerben magasabb fokon álló szerv feladata a törvényességi ellenőrzése ezen hivataloknak, hatóságoknak. Fontos azonban megállapítani, hogy a gyakorlatban nem minden állami szerv esetén beszélhetünk kibercselekmény elkövetéséről. E körben inkább olyan államigazgatási szervekről van szó, mint a rendvédelmi szervek és a Nemzetbiztonsági Szolgálatok. A Nemzetbiztonsági Szolgálatok fő feladata az ország biztonsága, függetlensége, gazdasági vagy más fontos érdeke ellen irányuló sértő, veszélyeztető, valamint támadó tevékenységek, törekvések felderítése, elhárítása.
Ahhoz azonban, hogy teljes képet kapjunk a kibertámadások megvalósítóiról fontos megvizsgálni azt is, hogy e cselekmények elkövetői milyen szaktudású csoportokra különíthetők el, hiszen a számítógépek és az általuk működtetett információs rendszerek a modern társadalom és a modern állam alapköveivé váltak. Sem a hétköznapi ember élete, sem az állam szerveinek működése nem képzelhető el ma már információs rendszerek nélkül. Ilyen rendszerek üzemeltetik többek között az elektromos áramellátást, a tömegközlekedés egyes eszközeit, állami szinten az ingatlan-nyilvántartást, a társadalombiztosítást, továbbá számos katonai eszközt is. Azonban ezek a rendszerek, amelyek számos esetben összefogják, megkönnyítik a hétköznapokat számtalan kockázatot rejtenek, amelyeket a bűnözök egy speciálisan képzett rétege kíván kihasználni. A veszély valódiságát mutatja, hogy *„becslések szerint egy-egy érdekesebb szervert naponta 100-150 hacker próbál feltörni […]"*[6].
Az első ilyen típus a hacker: *„Az elnevezés az 50-es évekből származik, a MIT nagygépeket programozó végzős diákok és szakemberek kezdték magukra alkalmazni ezt a kifejezést, mégpedig azért, mert az akkori gépek korlátaival találkozva (nagyon kevés memória volt a számítógépekben akkoriban), megpróbálták minél kisebbre „összenyomni" a programokat és az operációs rendszereket, tehát belenyúltak a programokba, rendszerekbe, illetve átírták azokat."*[7] Mára ennek a fogalomnak a jelentéstartalma teljesen átalakult, a legkisebb mértékben sem egyeztethető össze a ma használt elnevezés az ötvenes évekbelivel, mivel a számítógépek térhódításával a kép jóval árnyaltabb lett, ennek köszönhetően ma már nem

[5] NAGY KÁROLY: *Az állam felelőssége a nemzetközi jog megsértése miatt*, Budapest, Akadémiai Kiadó, 1991, 61. o.
[6] FORREST, DAVE: *Barát vagy ellenség? – A totális kontroll forgatókönyve,* Budapest, Focus Kiadó, 2005, 202. o.
[7] KAZÁRI CSABA: i.m. (2003), 18. o.

határozható meg egy általános hacker definíció. Tudásuk erősorrendjében a hackereket a következőképpen rangsorolhatjuk: (1) valódi hacker (2) dark-hacker, (3) light-hacker, (4) wannabe-hacker, (5) drifterek, (6) trollok.[8]

A következőkben ezen sorrendben kívánjuk bemutatni az egyes típusokat:

1) *valódi hacker: „olyan kimagasló számítástechnikai tudással bíró személy, aki szigorúan segítő jelleggel […] feltárja a számítógépes rendszerek/ alkalmazások előnyeit és hibáit, illetőleg javít azokon."*[9] A valódi hacker kiválóan ért a számítógépekhez, fontos számára az internet biztonsága, ebből következőleg ez a csoport ritkán követ el információs rendszer elleni bűncselekményeket, inkább rendszergazdaként a biztonsági rendszerek hibáinak tesztelésével foglalkozik cégeknél vagy esetlegesen kormányhivataloknál.

2) dark-hacker: a számítástechnikai tudása jelentős, de őt a nyereségvágy vagy éppen a bosszú motiválja, megállapítható hogy mindenféleképpen valamilyen ártó szándékkal tevékenykedik. Az internetes vírusok legtöbbje e kategória képviselőitől származik. A dark-hacker szakértelme és szándéka is megvan a kiberbűncselekmények elkövetéséhez.

3) light-hacker: számítástechnikai tudása jóval elmarad a valódi hackerétől, tudásukat gyakorolgatva keresik a hibás és támadható felületeket a világhálón. A hírnévre vágyakozva főleg defacementeket[10] követnek el. Egyes vélemények szerint nem is tartoznak az igazi hackerek közé, ugyanis a hackerek nem követnek el bűncselekményeket, ők az internet biztonságáért dolgoznak, míg a „light-hackerek" honlapokat törnek fel. A hacker társadalom e csoportot script-kiddienek nevezte el.

4) wannabe-hacker: ezen kör tagjai még nem valódi hackerek, de arra törekednek, hogy azzá váljanak. Tudásuk jóval elmarad az előzőekéhez, ebből kifolyólag más hackerek által kitalált úgynevezett hack-programokkal, és exploitokkal[11] munkálkodnak, főként az információs rendszer vagy adat megsértése bűncselekményt követik el a kategória képviselői.

5) drifterek: ők általában csak valamilyen információt vagy adatot keresnek az adott egyén gépén, tevékenységük kiterjed a személyes adatokra, üzleti titkokra stb., és ha megtalálják a keresett adatot lemásolják saját gépükre és továbbállnak. A gépen való jelenlétük legtöbbször észrevétlen, csupán csak néhány jel utalhat egy drifter jelenlétére számítógépünkön.

6) trollok: *„A trollok előképzettség nélkül gyakorlatilag céltalanul ténferegnek a világhálón, és tönkretesznek minden elébük kerülő és támadható dolgot a neten."*[12] Ők a legfiatalabb „hacker" generáció, ezen csoport is előre mások által kitalált hack-programokkal dolgozik, de legtöbbször nem is nagyon tudják, mit csinálnak.

A kibercselekmények elkövetőinek második csoportját a crackereket a köznyelv sokszor összekeveri a hackerekkel, pedig két különböző fogalomról beszélhetünk, ezért elkülönülten kell őket elemezni. Az első és legfontosabb különbség köztük, hogy *„a cracker feltör, a hacker betör"*[13], azonban további különbségek is kimutathatók a két típus között, miszerint *„tapasztalatuk és szakértelmük az internet, az Unix vagy más több felhasználós rendszerek területén sem éri el a hackerekét."*[14] A cracker fogalmának *„[…] elsődleges jelentése szerint*

---

[8] A valódi hacker és a dark-hacker között tudásbeli differencia nem fedezhető fel csak szándékbeli különbségről beszélhetünk. Ezt kívántuk érzékeltetni a felsorolás során használt gondolatjellel.

[9] KAZÁRI CSABA: i.m. (2003), 18. o.

[10] Defacement: honlapok feltörése és megváltoztatása.*„Hacker nyelven egy adott weboldal/weboldalak kicserélését jelenti, ezáltal „szégyenítve" meg az adott oldalt üzemeltető céget, magánszemélyt. A deface egyfajta üzenőfelület is: a hackerek egyik kommunikációs csatornája; a megváltoztatott oldalakon adnak hangot véleményüknek, nemtetszésüknek." – Kazári*: i.m. 154.

[11] Exploit: védelmi hibát, biztonsági rést, illetve ezek kihasználását jelenti, kiválóan használhatók honlap feltörésekre.

[12] FORREST: i.m. (2005), 205. o.

[13] FORREST: i.m. (2005), 206. o.

[14] RAYMOND, ERIC S.: *The new hacker's dictionary*, Cambridge, MIT Press, 1996, 22. o.

*olyan kárt okozó személy, aki számítógépes rendszereket rongál, illetve adatokat tulajdonít el, vagy bármilyen egyéb módon kárt okoz."*[15] A cracker a saját gépén lévő anyaggal dolgozik, munkássága népszerű, mivel tevékenykedéseinek eredményei az olcsó kalózmásolatok. *„A cracker által okozott kár igazán csak a szoftvergyártóknak érdekes, tehát a kár inkább relatív jellegű […]"*[16].

A crackerek mindig ártó szándékkal törnek fel egy adott rendszert, szoftvert. *„Másodlagos jelentése szerint […] a cracker olyan valaki, aki megváltoztatja a kereskedelmi forgalomban lévő szoftverek kódját (ez már önmagában illegális tevékenység) annak érdekében, hogy a szóban forgó szoftver szabadon másolható, használható és terjeszthető legyen."*[17]

A következő típusa a kiber bűnözőknek a phreaker: a „phonephreaker" kifejezésből ered. *„A phreaker-ek a telekommunikáció szakértői, „… átprogramoznak távközlési berendezéseket, ingyen mobiloznak és interneteznek (vonalat „lopnak"), értenek a lehallgatáshoz, és mindenféle mobiltelefont képesek kikódolni, átprogramozni, titkosítani stb."*[18]. Magyarországon ez a tevékenység még kialakulóban van. A telekommunikációs hálózat átprogramozásához tökéletes 2600 Hz-es hang kiadására van szükség, mely az úgynevezett in-band jelzés, mellyel elérhető az ingyen távolsági hívás, ugyanis a gép az in-band jelzés hatására kezdeményezi a hívást. Ma ennek a hangnak az előállítására a blue box szerkezetet használják.

Homogén csoportot alkotnak a HPAV-k, amely mozaikszó a Hacking, Phreaking, Anarchy, Virus szavakból tevődik össze. *„A HPAV csapatok a létező legkártékonyabbak – vírusokat írnak, állami szervek munkáját teszik tönkre, magánszámítógépekbe törnek be, mindezt csak azért, hogy másoknak gondot okozzanak."*[19] Ilyen jellegű csoportosulásokról Európa területén kevés információval rendelkezünk, Magyarországon is csak egy ismert csapatról van tudomásunk a Lukundo-féle HPAV-ról. *„A HPAV scene tagjai a szó szoros értelmében vett számítógépes bűnözők […]. Legismertebb képviselőik a vírusokat író programozók és csapatok."*[20] Egy HPAV tevékenykedése során bármely információs rendszer elleni bűncselekményt képes elkövetni. Sőt olykor még a terrorcselekmények elkövetésétől sem riadnak vissza.

[15] KAZÁRI CSABA: i.m. (2003), 19. o.
[16] FORREST: i.m. (2005), 206. o.
[17] KAZÁRI CSABA: i.m. (2003), 19. o.
[18] KAZÁRI CSABA: i.m. (2003), 20. o.
[19] KAZÁRI CSABA: i.m. (2003), 21. o.
[20] KAZÁRI CSABA: i.m. (2003), 21. o.

## 2. A KIBERCSELEKMÉNYEK MÓDSZEREI

Az alábbiakban tárgyalandó fejezet célja, hogy bemutassa a kibertámadások eszközeit, figyelembe véve, hogy *„a sikeres támadás mindig a meglepetés erejével hat. Ha tudnánk, mikor jön, mely rendszerek válnak célpontjává, hogyan indul, mekkora lesz a veszteség, minden bizonnyal képesek lennénk megelőzni."*[21] Illetve részletes képet kíván adni, arról hogy a kibertámadások elkövetői milyen módszerekkel valósíthatják meg ezen támadásokat. Szükséges átlátni azon módszerek körét, amelyek potenciális eszközei lehetnek egy esetleges kibertámadásnak, mivel a módszerek eredményétől nagyban függ, hogy fegyveres támadásnak minősülhetnek-e az egyes cselekmények, hiszen *„a fenyegetések motiváló tényezői különböző politikai, gazdasági, pénzügyi, katonai, […], regionális vagy egyéni célok elérése lehet."*[22]
A kibercselekményeket céljuk alapján három nagy csoportba lehet osztani: (1) információ és adatszerzés; (2) információs rendszer megzavarása; (3) információs rendszer elpusztítása. Következőkben ezeket mutatjuk be.

### 2.1 INFORMÁCIÓ- ÉS ADATSZERZŐ ESZKÖZÖK

Az információs rendszerek elleni támadási módszerek első csoportját azon eszközök képezik, amelyek célja az információs rendszer adatainak megszerzése. Ezen eszközök között említhetők meg a helyi hálózatok ellen irányuló támadások, ilyen az ún. Ethernet- és a Token Ring helyi hálózat elleni támadás. Az Ethernet egy üzenetszórásos helyi hálózat, melynek lényege, hogy *„ha az ügyfél állomás a kiszolgálótól adatot kér, adatcsomagot állít össze, amelyhez hozzácsatolja a megfelelő fejlécet, megcímzi a kiszolgálónak, majd útjára indítja a vonalon, ahol eljut a címzetthez."*[23] A más állomásnak szánt adatcsomagot tovább engedi, fontos itt megjegyezni, hogy az állomások csak a csomag fejlécét olvassák és abból észlelik, hogy a csomagot nekik címezték-e, ezt a technikát alkalmazza a Token Ring vezérjelgyűrűs hálózat is.
Mindkét technológia esetén a hacker[24] a hálózatba hatolva az állomásokat promiszkuitív módba kapcsolva képes megszerezni az összes adatcsomagot. A Lan-csatoló ugyanis promiszkuitív módban nem csak az adatcsomag fejléce alapján rá vonatkozó adatcsomagokat menti le, hanem egy mappában rendszerezve az összes a helyi hálózat által továbbított üzenetet. Egy ilyen támadás esetében a hálózat összes adatcsomagjának birtokában a terrorcselekmény információs rendszer vagy adat megsértésével bűncselekmény elkövetését is megalapozhatja, melynél jelentősége van annak, hogy az információs rendszer vagy adat megsértése bűncselekmény alap, illetve minősített esetét valósítja meg az elkövető. A hacker jelen esetben a hálózatba való betöréshez ugyanazt a követőprogramot (sniffert) használja, amelyet a teljes helyi hálózat megfigyelésére alkalmaznak a hálózati szakemberek. A támadás ellen kifejlesztettek egy AntiSniff elnevezésű programot. *„Az AntiSniff különböző szaglászótechnikákat ötvöz egy programban, és így teszteli a gyanítottan promiszkuitív módban futó rendszereket."*[25]
Továbbá az információs rendszer adatainak megszerzése körében gyakori elkövetési mód a jelszavak feltörése. A jelszavak kinyeréséhez és feltöréséhez a leghatékonyabb eszköz *„a L0phtCrack hálózatfigyelő program beépített Server Message Block (kiszolgáló-üzenetblokkoló) csomag elfogó funkciója, amely megfigyel a helyi hálózaton átmenő minden*

[21] CRUME, JEFF: *Az internetes biztonság belülről- …amit a hekkerek titkolnak,* Bicske, Szak Kiadó, 2003, 74. o.
[22] HAIG ZSOLT – VÁRHEGYI ISTVÁN*: Hadviselés az információs hadszíntéren*, Budapest, Zrínyi Kiadó, 2005, 131. o.
[23] CRUME: i.m. (2003), 138. o.
[24] E fejezetben összefoglalóan a hacker fogalma alatt a valódi hackert, dark-hackert és HPAV-t kell érteni.
[25] CRUME: i.m. (2003), 142. o.

*csomagot, a kiszolgálóra történő belépési információt tartalmazó csomagokról másolatot készít, a többit pedig törli."*[26] Ezzel a programmal a hacker listát kap a felhasználói azonosítókhoz tartozó titkosított jelszavakról, melyeket a hálózat figyelő programmal egyúttal fel is tud törni.
A jelszavak feltörésére további módszerek is alkalmazhatók, ilyen például a Social Engineering. *„A social enginering a befolyásolás és rábeszélés eszközével megtéveszti az embereket, manipulálja vagy meggyőzi őket, hogy a social engineer tényleg az, akinek mondja magát. Ennek eredményeként a social engineer – technológia használatával vagy anélkül – képes az embereket információszerzés érdekében kihasználni."*[27] Tehát a social engineer (azaz a hacker) miután megszerezte tőlünk a legfontosabb személyes adatainkat azokat feltölti egy kódfeltörő programba, amely könnyedén megszerezheti titkos jelszavainkat. Az úgynevezett Dictionary Hack eljárás azon alapul, hogy értelmes szavak variációit próbálgatja a kódfeltörés közben.Amennyiben nem értelmes szót választottunk, a hacker csak a Brute Force eljárással[28] járhat sikerrel jelszavunk megfejtésében.

### 2.2 INFORMÁCIÓS RENDSZERT ZAVARÓ ESZKÖZÖK

A támadási módszerek következő csoportját képezik az információs rendszerek megzavarására irányuló eszközök. Ezen kategóriába tartozik a puffertúlcsordításos támadás, melynek következtében *„a hacker egyszerűen több adatot küld, mint amennyit a vevő vár, és ha a vevő rendszere nem végez elegendő hibaellenőrzést, váratlan helyzet állhat elő. Néhány esetben a vevő programja egyszerűen összeomlik. Más esetekben a jogosult felhasználók nem tudják elérni a rendszert."*[29] Ezeket a támadásokat könnyű észrevenni és nem is nehéz védekezni ellenük, csak egy biztonsági frissítésre van szükségünk.
Ide sorolható a levélbomba támadás, mely során a támadó e-mail-ek sokaságát küldi el egy program segítségével a felhasználónak, mellyel túlterheli a levelezőrendszert, mert rákényszeríti, hogy az összes tárhelyet felhasználja a nem fontos adatok, üzenetek tárolására, így a fontos üzenetek nem tudnak bejutni.

### 2.3 INFORMÁCIÓS RENDSZERT MÓDOSÍTÓ, ROMBOLÓ ÉS MEGSEMMISÍTŐ ESZKÖZÖK

Végezetül az információs rendszerek elleni eszközök harmadik nagy csoportját azon rosszindulatú szoftverek képezik, melyeket az információs rendszerbe juttatva megsemmisítik, lerontják, módosítják, használhatatlanná teszik az adott adatbázist, szolgáltatást. Ebbe a kategóriába sorolhatjuk a Dos típusú támadásokat, a vírusokat, a trójait, a férgeket, valamint a zombihálózatokat.
A DoS típusú- egyfajta szolgálatmegtagadásos támadások, következtében *„ A DoS- támadó nem fér hozzá fontos rendszerhez, nem lop el bizalmas információkat […]"*[30], hanem valós vagy vélt sérelmének hangot adva rongálja meg az adott webhelyet. *„A támadás irányulhat a célpont hálózati kapcsolatának, vagy pedig a célpont rendszerben működő valamely - szolgáltatást nyújtó - alkalmazásának túlterhelésére. Ennek megfelelően szokás a támadásokat hálózati vagy alkalmazási rétegben végrehajtott típusokra osztani,[..]. A hagyományos DoS támadások során az elkövetők a célpontot egyetlen pontból támadják, általában egy "feltört", megfelelő adottságokkal rendelkező hálózati végpontot (hálózatra*

[26] CRUME: i.m. (2003), 140. o.
[27] MITNICK D. KEVIN, SIMON L. WILLIAM: *A biztonság emberi tényezőinek irányítása, A legendás hacker – A megtévesztés művészete,* Budapest, Perfact – Pro, 2003, 1. o.
[28] Brute Force eljárás: *„Ennek a lényege, hogy a kódtörő program minden variációt kipróbál – de ez nagyon időigényes, és a jelszavak tekintetében nem is az a cél, hogy ne lehessen feltörni, hanem, hogy sokáig tartson!"* – KAZÁRI CSABA: i.m. (2003), 61. o.
[29] CRUME: i.m. (2003), 153. o.
[30] CRUME: i.m. (2003), 174. o.

*kötött számítógépet) használva fegyverül. A támadó célja a célpont erőforrásainak lefoglalása."*[31] A támadás eredménye, hogy a rendszer megtagadja a felhasználóktól a hozzáférést a különböző szolgáltatásokhoz, amelyekre egyébként jogosultak lennének. Tehát a kritikus erőforrás lefoglalásával gátolja a webhely tevékenységét. A Dos típusú támadások körébe tartozik a DDos támadás, amely elosztott szolgáltatásmegtagadással járó támadás. Ilyen DDos támadóállomások két féleképpen keletkezhetnek, az egyik, hogy egy automatizált eszköz kutatja fel és kapcsolja be az úgynevezett zombihálózatokba (más néven boot hálozatok) a sebezhető számítógépeket, illetve a másik formája, hogy számítógépes vírusokkal vagy trójai faló programokkal csatolják be a számítógépeket ezen hálózatokba. *„A DDoS támadás során egy időben, nagyszámú internetes végpontról végzik a célpont megbénítására szolgáló adatcsomagok küldését, emiatt a támadó végpontok – vagy legalább az általuk generált adatforgalom – semlegesítése nem megoldható."*[32] A zombihálózatokat, azaz boot hálózatokat azért kell itt megemlíteni, mert ezen hálózatok számítógépek sokaságát foglalhatják magukba, melyek segítségével nagyobb támadásokat lehet indítani. A zombihálózatba kapcsolt gépeket valaki más távolról irányítja. Többnyire személyes adatok, illetve titkos információk lopásához használják, de használható gyorsan terjedő férgek szétküldésre is, mely megbéníthatja az adott információs rendszert.

A back orifice (hátsó nyílás) támadás esetében a hacker a back orifice nevű rosszindulatú programot az elnevezéséből is adódóan a „hátsó ajtón" juttatja be az információs rendszerbe, melyet egy jóindulatú programba rejtve juttat el a felhasználóhoz, amit gyanútlanul feltelepít a gépére abban a hiszemben, hogy valamilyen hasznos, jóindulatú programot telepít fel. A telepítés után a rosszindulatú program létezésének minden látható jele eltűnik, közben a hacker teljes mértékben átveheti és távolról irányíthatja a számítógépet. Ebben az esetben a kirbercselekmény elkövetése a támadás azon tulajdonsága, miszerint a feltelepítés után a program létezésének látható nyomait eltűnteti nagyon hatékony a kibertámadások területén. Tovább menve, ha a hálózathoz mikrofon és videokamera is van csatlakoztatva, a hacker az eszközök bekapcsolásával figyelheti meg a felhasználót.

A vírus támadás definíciója szerint *„a számítógépes vírus olyan program, amely a futtatáskor lemásolja magát (vagy egy részét). Kapcsolódhat a felhasználó merevlemezén lévő más futtatható állományokhoz, de akár az indítórekordhoz is, amely a számítógép indításakor betölti az operációs rendszert."*[33] A lassabb lefolyású vírusok óriási területet fertőzhetnek meg, nem úgy, mint a gyorsabb lefolyású társaik, mert a gyors lefolyás miatt a gazdagép hamar megsemmisül. *„A vírusnak valamihez hozzá kell kapcsolódnia, egy programhoz, egy dokumentumhoz vagy a merevlemez boot szektorához."*[34] Kibertámadás elkövetéséhez az egyik legideálisabb módszer, mivel a lassabb lefolyású vírus esetén fokozatosan nagy kárt lehet elérni vele, míg a gyorsabb lefolyású vírus esetén elemi csapás mérhető az adott információs rendszerre.

A trójai faló támadást a vírusok után kell megemlítenünk, mivel technikailag nem vírus ugyan, de hasonló károkat okoz az információs rendszerben. A vírustól való megkülönböztetést viszont az indokolja, hogy a trójai falovak nem feltétlenül másolják le önmagukat, mégis rosszindulatú programok, melyek hatalmas károkat tudnak okozni. Az információs rendszerbe jóindulatú programba rejtve kerülhetnek be. *„A trójai faló a felszínen hasznos, sőt mi több, szórakoztató funkciókat mutat, így teljesen ártalmatlannak tűnhet –*

---

[31] GYÁNYI SÁNDOR: *Robothadviselés 7. Tudományos Szakmai Konferencia*, http://www.zmne.hu/hadmernok/kulonszamok/robothadviseles7/gyanyi_rw7.html (letöltés ideje: 2014.03.26.)

[32] GYÁNYI SÁNDOR: *Cyber – támadások elleni védekezés és a válaszcsapások lehetőségei*, in. Hadmérnők III. évfolyam 2. szám, 116. o.

[33] CRUME: i.m. (2003), 188. o.

[34] WARREN PETER, STREETER MICHAEL: *Az internet sötét oldala – Vírusírók, adatrablók, hackerek – és amit tehetünk ellenük,* Budapest, HVG kiadó, 2005, 137. o.

*pedig valójában a velejéig romlott."*[35] A vírusokhoz való hasonlósága miatt, úgy véljük, a második legideálisabb módszer lehet a trójai faló a kibertámadások eszköztárában.
A számítógépféregnek a vírushoz hasonlóan nem kell valamihez kapcsolódnia, egymaga egy kész, egész program. *„A számítógépféreg olyan szoftverparazita, amely tulajdonképpen mindent felfal, ami az útjába kerül. Időről időre újra meg újra lemásolja magát, ezáltal a folyamat során felemésztheti a memóriát, a lemezterületet, vagy a sávszélességet."*[36] Egy gyorsan ható féreg jelentős kárt tud okozni az információs rendszerben, melynek hatása igen pusztító lehet.
E fejezet végén rögzítenünk kell, hogy az ismertetett eszközök listája nem taxatív, egyfelől annak okán sem lehet az, mert IT ágazat az, amely a leggyorsabban fejlődik a világon, másodsorban csak azon eszközök szerepelhetnek itt, amelyek létezéséről már tudomásunk van. Azonban e rövid ismertetésből is világossá válik, hogy ezen eszközök, módszerek egy megfelelően képzett szakember kezében fegyverként is funkcionálhatnak.

[35] CRUME: i.m. (2003), 189. o.
[36] CRUME: i.m. (2003), 189. o.

## 3. A KIBERTÁMADÁS MINŐSÜLHET-E FEGYVERES TÁMADÁSNAK?

E kérdésre adott válasz relevanciája igen nagy súlyú a nemzetközi jog területén, hiszen az Egyesült Nemzetek Szervezetének Alapokmánya, az erőszak tilalmának ius cogens szabálya alól kivételként rögzíti, hogy *„a jelen Alapokmány egyetlen rendelkezése sem érinti az Egyesült Nemzetek valamelyik tagja ellen irányuló fegyveres támadás esetében az egyéni vagy kollektív önvédelem természetes jogát mindaddig, amíg a Biztonsági Tanács a nemzetközi béke és a biztonság fenntartására szükséges rendszabályokat meg nem tette."*[37] Azonban sem az Alapokmány sem későbbi dokumentumok nem definiálják a fegyveres támadás fogalmát, amelynek megállapítása a gyakorlatban *„… módfelett szubjektív döntésen alapul: ugyanaz a tény, ugyanazon jog alapján, eltérő minősítésekkel illethető."*[38] A döntés szubjektív voltát erősíti, hogy a megtámadott állam állásfoglalása az irányadó, ahhoz nem kell Biztonsági Tanács által elfogadott határozat – amelynek feltétellé tétele az önvédelem lényegét vonná el – , az állam anélkül is megkezdheti az erőszak önvédelmi célú alkalmazását. E jog gyakorlása az 51. cikk értelmében addig tart *„amíg a Biztonsági Tanács a nemzetközi béke és a biztonság fenntartására szükséges rendszabályokat meg nem tette."*

A fegyveres támadás, mint fogalom általánosan elfogadott jelentésének kiszélesítését tette szükségessé az Amerikai Egyesült Államokat ért 2001. szeptember 11-i támadás, amelyet polgári légi járművekkel hajtottak végre. Eme cselekmény ismét világossá tette, hogy az emberi kreativitás nem ismer korlátokat, ha pusztításról van szó. Fogalom alkotása e cselekmények után sem történt, azonban általánosan elfogadott tény lett, hogy fegyveres támadásnak minősíthető egy ilyen cselekmény.

Az internet elterjedésének köszönhetően *„a globális számítógépes hálózatokban végbemenő kölcsönhatások révén megszületett a kibertér (cyberspace) a kibernetikus világegyetem."*[39] E kibertér rendkívül egyedi és összetett, hiszen nem csak fizikai és földrajzi fogalmakkal jellemezhető, hanem virtuális jellemzői is rendkívüli relevanciával bírnak jellemzése során. A kibertéren keresztül milliós nagyságú információ áradat halad át egyetlen perc leforgása alatt. *„Egyértelműen prognosztizálható: a kibertér rendszerei egyre nagyobbá, gyorsabbá és komplexebbé vállnak,"*[40] azonban sebezhetőségük pontosan ebben a komplexitásban rejlik. E sebezhetőség veszélye abban áll, hogy mára már nem csak a magánszemélyek, gazdasági szereplők, hanem az állam alapvető struktúrái, a szociális háló, valamint fegyveres szervei is a kibertér részét képezik. Ennek okán az államot ugyan úgy érheti támadás a kibertérben, mint a hétköznapi értelemben vett valóságban. *„Ilyen körülmények között nem csak helyes, hanem egyenesen szükséges is az államok békés kapcsolatait és együttműködését rendező legfontosabb szabályok megvizsgálása, nem azért, hogy azokat megváltoztassák és másokkal helyettesítsék, hanem azért, hogy kibővítse és új szemszögből nézve tisztázzák értelmüket és jelentőségüket a világ gyorsan változó körülményei között."*[41] Szükséges tehát megvizsgálni, hogy az államot a kibertérben ért támadás esetében is megilleti-e az önvédelem joga és mikor tekinthetjük ezt a támadást fegyveres támadásnak?

E kérdések merültek fel 2007 májusában is mikor Észtországot átfogó kibertámadás érte a tallinni második világháborús szovjet emlékmű áthelyezése miatt. Andrus Ansip észt miniszterelnök szerint a balti államot ért kibertámadás célja egy kiberháború szimulálása volt. E cselekmény is sürgetővé tette annak megállapítását, hogy a kibertámadás fegyveres

[37] ENSZ Alapokmány, 51. cikk. Kihirdette: 1956. évi I. törvény az Egyesült Nemzetek Alapokmánya törvénybe iktatásáról.

[38] SULYOK GÁBOR: *Az egyéni vagy kollektív önvédelem joga az Észak-Atlanti Szerződés 5. cikkének tükrében,* in. Állam és Jogtudomány 2002/1-2. szám, 108. o.

[39] NAGY KÁROLY: *Titok és biztonság az információs társadalomban,* in. Belügyi Szemle 1999/4-5. szám, 173. o.

[40] BABOS TIBOR: *„Globális közös terek" a NATO-ban,* in. Nemzet és biztonság 2011/3. szám, 42. o.

[41] HERCZEGH GÉZA: *Az erőszakkal való fenyegetésnek és az erőszak alkalmazásának tilalma a mai nemzetközi jogban,* in. Állam és Jogtudomány 1963/3. szám, 360. o.

támadásnak minősíthető-e. *„Mivel azonban az alapokmány mellőzi a fegyveres támadás kifejezés definiálását, semmi nem zárja ki az önvédelem analógia útján való alkalmazásának lehetőségét.”* [42] Ehhez azonban két feltételnek is meg kell felelnie az adott támadásnak: (1) a cselekménynek el kell érnie egy rendkívüli súlyt vagy intenzitást; (2) a támadást elkövető személyek cselekménye valamely másik államnak betudható legyen.
Az első kritérium, vagyis a rendkívüli súly vagy intenzitás a fegyveres támadás szubjektív volta miatt nehezen meghatározható, hiszen egyes államoknál az ingerküszöb biztosan eltérő. Ennek ellenére bizonyos támadások egyértelműen fegyveres támadásként aposztrofálhatók ilyen például egy másik állam területén fekvő település folyamatos és módszeres ágyúzása, polgári légi jármű kritikus infrastruktúrának vezetése (pl. atomerőmű). Sokan vitatják azt, hogy ilyen erejű támadás végrehajtható a kibertérben is.
Ahhoz, hogy ezt meg tudjuk cáfolni át kell tekinteni a kiberhadviselés egyes típusait. A kiberhadviselés – ahogy a tradicionális is – három területre különíthető el: (1) felderítés; (2) támadás; (3) védelem.
A kiberfelderítés, amelynek célja adatbázisban tárolt adat vagy információ megszerzése nem minősíthető fegyveres támadásnak. Ezt támasztja alá a Tallinn Manual elnevezésű NATO szakértők által elkészített kézikönyv (szakértői vélemény) is, mely szerint hír- és adatszerző tevékenységek nem minősíthetőek fegyveres támadásnak.[43] Katharina Ziolkowski véleménye szerint *„a kémkedés önmagában nem ellenkezik a nemzetközi joggal, és ezért nem is nemzetközi jogot sértő cselekmény.”*[44] Ezzel szemben Szalai Anikó úgy érvel, hogy *„az első írásos nemzetközi hadijogi egyezmények (Hágai egyezmények 1899, 1907, Genfi egyezmények 1949, 1977) pedig tulajdonképpen nem a kémkedést tiltják, hanem csak azt, ha tetten érik a kémet”*[45] továbbá *„a nemzetközi jog szinte egyáltalán nem tartalmaz szabályokat a kémkedésre, a se nem jogszerű, se nem jogellenes határán helyezkedik el. A meglévő – bizonytalan – szabályok egyáltalán nem követték a technikai fejlődést, és például az 1961. évi bécsi egyezmény a diplomáciai kapcsolatokról csak szellemiségében értelmezhető a mai helyzetre.”*[46] Ami azonban biztos a kémkedést megvalósító állam vagy egyén felelőssége megállapítható és velük szemben a sértett állam felléphet, azonban e fellépés nem lehet fegyveres erőszak. Az ilyen állammal szemben nem fegyveres szankciókkal lehet csak élni (politikai, gazdasági, diplomáciai), míg az egyénnel szemben büntető igényét érvényesítheti az állam.
A kibervédelem esetköre főszabályként szintén nem tartozik a fegyveres támadás fogalmi körébe.
A kibertámadás szintén több típusú lehet, mint azt az előző fejezetben is felvázoltuk vannak olyan támadások, amely a kommunikáció megbénítására vagy adat illetve információ hozzáférhetetlenné tételére irányulnak, míg a támadások egy másik csoportjának a célja a pusztítás: vagy magának a rendszernek vagy a rendszer által irányított, felügyelt infrastruktúrának. *„A kibertámadás – amelynek célja csak a károkozás – lehet kifinomult vagy primitív, attól függően, hogy a támadó milyen kapacitással rendelkezik, illetve mi a célpontja*

---

[42] SULYOK GÁBOR: *A terrorcselekmény elkövetéséhez használt polgári légi jármű lelövésének nemzetközi jogi és alkotmányjogi megítélése,* in. Fundamentum 2005/3. szám, 34. o.
[43] SCHMITT, MICHAEL N.: *Tallinn Manual on International Law applicable to cyber warfare*, Cambridge, Cambridge University Press, 2013, 55. o.
[44] ZIOLKOWSKI, KATHARINA: *Peacetime Cyber Espionage – New Tendencies in Public International Law*, in ZIOLKOWSKI, KATHARINA (szerk.): *Peacetime Regime for State Activities in Cybersp ace International Law, International Relations and Diplomacy*, Tallinn, NATO CCD COE Publication, 2013, 456. o.
[45] SZALAI ANIKÓ: *Kémkedés: nem tilos, mégsem szabad*, http://drszalaianiko.hu/2013/11/22/kemkedes-nem-tilos-megsem-szabad/ (letöltve: 2014.04.10.).
[46] SZALAI ANIKÓ: *Az 1979-es iráni forradalom éleslátása*, http://drszalaianiko.hu/2013/11/04/az-1979-es-irani-forradalmarok-eleslatasa/ (letöltve: 2014.04.10.).

*a támadásnak… precíz támadásokat csak államok vagy nagyon erős bűnözői csoportok indíthatnak."*[47]

A kibertámadás ténye azonban önmagában nem elegendő ahhoz, hogy aktiválja egy állam önvédelmi mechanizmusát, annak intenzitása a döntő tényező. Mint korábban is jeleztük nincs elfogadott fogalma a fegyveres támadásnak, azonban az elfogadott, hogy az olyan támadások, amelyek nagyszámú ember életét veszélyeztetik vagy kioltják illetve az infrastruktúrában jelentős kárt okoznak, azokat fegyveres támadásnak lehet tekinteni.[48]

Vagyis olyan támadás, amelynek közvetlenül súlyos hatása van az fegyveres támadás. Ilyen eredményű támadás lehet kibertérben az atomerőművek, atomreaktorok elleni támadás, amelyre több példa is volt az elmúlt években: a Blaster-féreg 2003-ban és Stuxnet-vírus 2010-ben. A Blaster-féreg 2003. augusztus 14-én az Egyesült Államokban és Kanadában okozott áramszünetet, *„mivel a kritikus riasztási rendszerek csődöt mondtak, a FirstEnergy dolgozói nem állították le az eseménysorozatot, mert nem tudták, mi történik."*[49] Közel egy óra leforgása alatt a Blaster a teljes riasztási funkciót működtető fő szerverszámítógépet összeomlasztotta, így a dolgozók nemhogy, azt nem vették észre, hogy veszélyben van a rendszer működése, de azt sem, hogy a rendszerkörülmények megváltoztak. Az esetben az volt a szerencse, hogy a Blaster a megfertőzött gépekben nem végzett rosszindulatú pusztítást, csak felemésztette azok erőforrásait.

A Stuxnet vírus az erőművekre közvetlen veszélyt nem jelentett célpontjai az iráni urándúsító berendezések voltak, amelyeket olyannyira hatékonyan támadott, hogy több évvel visszavetette az iráni állam atomprogramját. *„A Stuxnet mögötti állami háttér lehetőségét alátámasztja, hogy maga a szoftver igen komplex, szofisztikált kivitelezésű volt, tevékenysége során pedig célzott különbségtételt alkalmazott, egy előre kiválasztott irányító rendszerek köre tekintetében."*[50]

Kevésbé ismert az a 2012-es eset,[51] amikor egy malware vírust jutattak be két Egyesült Államok területén lévő erőmű irányítórendszerébe, amely hozzáfért minden létfontosságú hálózathoz, ismételten szerencse, hogy nem támadó célú volt a cselekmény.

Ezen esetek rávilágítanak arra, hogy az erőművek megtámadása kiber eszközökkel nem lehetetlen vállalkozás, a fenti esetek mindegyikében amennyiben pusztítás lett volna az elsődleges cél az meg is valósult volna. Egy atomerőmű elpusztításával járó kibertámadást az államok mindegyike fegyveres támadásnak minősítene, a támadás intenzitása akár azonos is lehet a nukleáris fegyverekével. Ilyen támadás végrehajtásának eszköze lehet az előző fejezetben ismertetett back orifice, a vírusok, a trójai falóvak és számítógépférgek

A Nemzetközi Bíróság 1996. július 8-án az ENSZ Közgyűlésének kérésére tanácsadó véleményében kifejtette, hogy a nukleáris fegyver használata vagy az azzal való fenyegetés, amennyiben az ENSZ Alapokmány 2. cikk 4. bekezdésével ellentétes és nem felel meg az 51. cikkben foglaltaknak akkor jogellenes.[52] Így tehát analógiával élve, az a kibertámadás, amelynek célja és eredménye valamely más állam atomerőművének megsemmisítése, az sérti

---

[47] ORBÓK ÁKOS: *A kibertér, mint hadszíntér* in Biztonságpolitika.hu 2013, 2. o. http://www.biztonsagpolitika.hu/documents/1375084295_Orbok_Akos_A_kiberter_mint_hadszinter_-_biztonsagpolitika.hu.pdf (letöltve: 2014.03.27.)

[48] SCHMITT, MICHAEL N: i.m. (2013) 55. o.

[49] SCHNEIER, BRUCE: *Schnier a biztonságról*, Budapest, HVG Kiadó, 2010, 144. o.

[50] LATTMANN TAMÁS: *A nemzetközi jog lehetséges szerepe az informatikai hadviselés területén*, in. CSAPÓ ZSUZSANNA (szerk.): *Emlékkötet Herczegh Géza születésének 85. évfordulójára – A ius in bello fejlődése és mai problémái*, Pécs, Kódex Nyomda, 2013, 211. o.

[51] LEWIS, JAMES ANDREW: Incidensek a kibertérben, 17. o. http://www.biztonsagpolitika.hu/Incidensek_a_kiberterben_biztonsagpolitika.hu.pdf (letöltve: 2014.03.27.)

[52] Legality of the threat or use of nuclear weapons, Advisory opinion of 8 July 1996, I. C. J. Reports 1996, 266., para 105. (2) C.

az alapokmányban rögzített erőszak tilalmának szabályát, tehát jogellenes, így fegyveres támadásnak minősül, amely következtében a megtámadott állam élhet az önvédelem jogával.
A kibertámadások egy másik típusa, amelynek a támadáskor kifejtett hatása nem éri el azt a küszöbértéket, amely azt fegyveres támadássá tenné, de a támadás következményei már átléphetik azt a határ, hogy az eredeti támadást annak minősítsék. Ilyen kibertámadásnak tekinthető az, amely egy állam ivóvízrendszerét, vagy víztisztító rendszerét támadja. E támadás közvetlen hatása, hogy nem működik megfelelően az infrastruktúra, közvetett hatása viszont a szennyezett ivóvíz, amely súlyos következményekkel járhat a polgári lakosság körében. Ilyen támadás érte Haifa ivóvízrendszerét is.[53] Egy ilyen típusú támadás akár több tízezer polgári személy halálát is eredményezheti, sőt a hálózat méretétől függően milliós nagyságú áldozatokkal is járhat.[54] Egy ilyen támadás estén analógia vonható a biológiai támadással vagy vegyi támadással. Mivel mindkét harcászati mód a nemzetközi közösség jelentős része által tilalmazott multilaterális egyezmények útján,[55] ezért ennek okán az ilyen támadás fegyveres támadásnak minősíthető akár csekély számú áldozat esetén is.
Egy állam kommunikációs hálózatát megbénító támadások szintén a közvetlen veszélyt jelentő támadások közé sorolandók, hiszen egy olyan támadás – amit az Egyesült Államokban szimuláltak –, amely során *„a megtámadott ország vezetési rendszere és az ország működőképessége kettő-négy nap alatt összeomlott”*[56] a közrend felbomlását eredményezi. A megtámadott ország anarchiába süllyed, a szociális hálózata pedig összeomlik. Eredmény kialakulását elősegíti, hogy a támadás *„… bizalmatlanságot kelt a rendszeresített eszközöket üzemeltető saját szoftverek irányában, a kiszámíthatatlanság keltésével, a biztonságérzet csökkentésével pedig komoly bizonytalanságot is eredményez.”*[57] Hasonló támadás érte 2007-ben Észtországot, amely támadás még nem volt kellően intenzív és hosszantartó a fenti eredmény eléréséhez, azonban előre jelezte az ilyen típusú támadások szisztémáját. A kormányzati szervek megbénításával egyidejűleg, a bankhálózat, a rendőrségi kommunikáció és ezt követően a polgári kommunikációs rendszerek teljes megbénítását. Nem előrelátható, hogy egy ilyen volumenű támadás milyen infrastrukturális és humanitárius károkat okozna a gazdasági és politikai következményeken túl. Annak a lehetősége is fennáll, hogy egy ilyen támadás esetén a megtámadott állam nem is lenne képes az önvédelmi jogának gyakorlására.
A fegyveres támadás megállapításához szintén elengedhetetlenül szükséges hogy, a támadást elkövető személyek cselekménye valamely másik államnak betudható legyen. Nyilvánvalóan betudható egy másik államnak saját nemzetbiztonsági szolgálta vagy fegyveres erejének tagjai által elkövetett cselekmény. Az államhoz szervezetileg nem kapcsolódó egyének vagy csoportok esetében viszont már kérdéses, hogy azok cselekménye mikor tudható be az államnak. A Nemzetközi Bíróság Nicaragua-ügyben hozott ítéletében még a tényleges ellenőrzést (effective control) tette szükségessé[58], míg a volt Jugoszlávia területén történt humanitárius jogot sértő cselekmények feltárására felállított nemzetközi törvényszék szerint

[53] PIRKER, BENEDIKT: *Territorial Sovereiguty and Integrity and the Challenges of Cyberspace*, in. ZIOLKOWSKI , KATHARINA (szerk.): *Peacetime Regime for State Activities in Cybersp ace International Law, International Relations and Diplomacy*, Tallinn, NATO CCD COE Publication, 2013, 56. o.
[54] E körben említhető más kritikus infrastruktúra is, mint például a földgáz hálózat.
[55] 1971. évi egyezmény a bakteriológiai (biológiai) és toxin-fegyverek fejlesztésének, gyártásának és tárolásának eltiltásáról és megsemmisítéséről, Kihirdette: 1975. évi 11. törvényerejű rendelet a bakteriológiai (biológiai) és toxin-fegyverek kifejlesztésének, előállításának és tárolásának megtiltásáról és e fegyverek megsemmisítéséről szóló, az Egyesült Nemzetek Szervezete XXVI. ülésszakán, 1971. december 10-én elfogadott egyezmény kihirdetéséről (158 részes állam); 1993. évi párizsi egyezmény, Kihirdette: 1997. évi CIV. törvény a vegyifegyverek kifejlesztésének, gyártásának, felhalmozásának és használatának tilalmáról, valamint megsemmisítéséről szóló, Párizsban, 1993. január 13-án aláírt egyezmény kihirdetéséről (184 része állam).
[56] HAIG ZSOLT – KOVÁCS LÁSZLÓ: *Fenyegetések a cybertérből*, in. Nemzet és biztonság 2008/5. szám, 67. o.
[57] LATTMANN TAMÁS: i. m. (2013), 212. o.
[58] Case concerning Military and Paramilitary Activities in and against Nicaragua (Nicaragua versus United States of America), Judgement of 27 June 1986, I.C.J. Reports 1986, 64-65, para. 115.

már elegendő az állam általános ellenőrzése (overall control) is[59]. A Nemzetközi Jogi Bizottság véleménye szerint az ellenőrzés kívánt mértékét esetről esetre annak sajátosságait vizsgálva kell megállapítani. *„Az állam felelősségének megállapítása tehát az előkészítés részleteinek pontos ismeretét feltételezi."*[60]
Annak megállapítása a kibertérben, hogy ki az elkövető és kinek az ellenőrzése alatt követte el a cselekményt jóval nehezebb, mint a tradicionális támadások esetén, hiszen a kibertér nagyfokú anonimitást biztosít az elkövetőknek. Így volt az Észtországot ért támadáskor és a Stuxnet-vírus esetében is. Az államok közvetve tudták csak bizonyítani, hogy az Észtországot ért támadás mögött Oroszország, míg Iránt ért támadás mögött pedig Izrael állt. A fegyveres támadásnak minősítéshez azonban közvetlen bizonyítékok szükségesek.
E probléma megoldást jelentheti a Kínában már alkalmazott új internet protokoll használata (IPv6), ezen új generációs internet *„egyik legfontosabb eleme egy biztonsági intézkedés lesz, amit SAVA néven emlegetnek. A betűszó a Source Address Validation Architecture (forrásazonosító architektúra) ez a rendszer a hálózatra csatlakozó számítógépek IP címének azonosítását végzi, és ezek alapján adatbázist épít, amiben a számítógép és az IP cím egyaránt szerepel. Ha az azonosítás során a számítógép vagy az IP cím nem egyezik, a hálózat megtagadja az adatcsomagok továbbítását."*[61] Ezen rendszer tehát alkalmas lehet a támadó azonosítására, azonban probléma, hogy míg Kína már az IPv6 internetes protokoll generációt alkalmazza, addig a világ többi részén még az IPv4-et, így jelenleg csak az ázsiai ország rendelkezik a támadó azonosítására alkalmas rendszerrel. További lehetőséget jelenthet a back-tracing eszközök fejlesztése, amelyek csökkentik a kibertér által nyújtott anonimitást, hiszen egyre jobban visszakövethetővé teszik a kibertérben elkövetett támadásokat.[62]

[59] Prosecutor versus Dusko Tadic, Judgement, Appeals Chamber, Case No. IT-94-1, 15 July 1999, para. 145.
[60] SULYOK GÁBOR: i.m. (2005), 35. o.
[61] ORBÓK ÁKOS: i.m. (2013), 5. o.
[62] MAUNO PIHELGAS: *Back-tracing and anonymity in cyberspace*, in. ZIOLKOWSKI, KATHARINA (szerk.): *Peacetime Regime for State Activities in Cybersp ace International Law, International Relations and Diplomacy*, Tallinn, NATO CCD COE Publication, 2013, 58. o.

## 4. KIBERTÁMADÁSOK ÉS A HUMANITÁRIUS JOG KAPCSOLATA

*„A nemzetközi humanitárius jog – egyik lehetséges meghatározása szerint – azon szerződéses vagy szokásjogi szabályok összességét jelenti, melyek a nemzetközi vagy a nem nemzetközi fegyveres összeütközésekből közvetlenül eredő humanitárius problémák megoldását célozzák, oly módon, hogy egyfelől korlátozzák a hadviselő feleknek a hadviselés eszközei és módszerei szabad megválasztásához fűződő jogát, másfelől pedig védik a konfliktus áldozatául eső személyeket és javakat."*[63] Egyes vélemények szerint a humanitárius jog legnagyobb erénye, hogy az egyéneknek nyújt védelmet a háború borzalmaiban, azáltal, hogy meghatározott keretek közé szorítja a feleket, ezzel segítve az emberi jogok érvényesülését a nemzetközi vagy a nem nemzetközi fegyveres konfliktusok idején[64], ennek előfeltétele, hogy *„kötelező a felekre a ius in bello, teljesen függetlenül attól, hogy mit hisznek vagy valójában mi is a helyzet a háború jogossága tekintetében."*[65]

Az állam önvédelmi jogosultságát aktiváló kibertámadással összefüggésben a fenti definícióban említett két fegyveres összeütközés közül a nemzetközi fegyveres támadásnak van relevanciája. A nemzetközi fegyveres összeütközés tartalmát az 1949. genfi egyezmények közös 2. cikke határozza meg: *„Azokon a rendelkezéseken kívül, amelyeknek már a béke idején is hatályba kell lépniök, a jelen Egyezmény alkalmazást nyer a két vagy több Magas Szerződő Fél között bekövetkező megüzent háború vagy minden más fegyveres összeütközés esetén, még ha a hadiállapot fennállását közöttük valamelyik nem is ismeri el. Az Egyezmény alkalmazást nyer valamely Magas Szerződő Fél területe egészének vagy egy részének bármilyen megszállása esetében is, még akkor is, ha ez a megszállás nem ütközik semmiféle katonai ellenállásba."*[66]

A humanitárius jog szabályai *„az összeütközés első mozzanatától kezdve automatikusan alkalmazandók, azaz az első támadás bekövetkezésének pillanatától… védik az ellenségeskedések áldozatául eső személyeket és javakat."*[67] Vagyis a kibertámadásokat megvalósító államnak a támadás kivitelezésekor figyelemmel kellene lennie e jogi rezsimre. Ennek ellenére a fent említett lehetséges fegyveres támadások több humanitárius jogi szabály ellen véthetnek.

Az összes fent ismertetett támadás beleütközik a megkülönböztetés nélküli támadások tilalmának rendelkezésébe, hiszen *„nem meghatározott katonai célpontok ellen irányul"*[68] és *„olyan támadás, amely a polgári lakosság körében feltehetően annyi áldozatot követel és annyi sebesülést okoz, valamint a polgári javakban akkora károkat idéz elő, hogy azok önmagukban, vagy együttesen meghaladnák a támadástól várható konkrét és közvetlen katonai előny mértékét."*[69]

Az ivóvíztisztító rendszer elleni támadás a létfenntartáshoz szükséges eszközök elleni támadás tilalmát is megvalósítja, amelyet nevesít is az 1977-es első kiegészítő jegyzőkönyv (továbbiakban: Jegyzőkönyv) 54. cikke.

---

[63] SULYOK GÁBOR: i.m. (2005), 36. o.

[64] ROSAS, ALAN; STENBACK, PAR: *The Frontiers of International Humanitarian Law,* in. Journal of Peace Research 1987/3, 219. o.

[65] GELLÉR BALÁZS JÓZSEF: *Nemzetközi büntetőjog Magyarországon, adalékok egy vitához (egyes jellemzők leírása és diagnózis kísérlet),* Budapest, Tullius Kiadó, 2009, 16. o.

[66] 1949. évi genfi egyezmények közös 2. cikke, Kihirdette: 1954. évi 32. törvényerejű rendelet a háború áldozatainak védelmére vonatkozóan Genfben, az 1949. évi augusztus hó 12. napján kelt nemzetközi egyezményeknek a Magyar Népköztársaságban való törvényerejéről.

[67] SULYOK GÁBOR: i.m. (2005), 36. o.

[68] 1977. évi I. kiegészítő jegyzőkönyv a háború áldozatainak védelméről 51. cikk (4) a) pont Kihirdette: 1989. évi 20. törvényerejű rendelet a háború áldozatainak védelmére vonatkozóan Genfben, 1949. augusztus 12-én kötött egyezmények I. és II. kiegészítő jegyzőkönyvének kihirdetéséről.

[69] 1977. évi I. kiegészítő jegyzőkönyv 51. cikk (5) b) pont.

*„A veszélyes erőket tartalmazó üzemek, vagy berendezések, nevezetesen gátak, töltések és áramszolgáltató atomerőművek ellen akkor sem szabad támadást intézni, ha azok katonai célpontot képeznek; amennyiben a támadás veszélyes erőket szabadíthat fel, és ennek következtében súlyos veszteségeket okozhat a polgári lakosság körében."*[70] Tehát az atomerőművek elleni támadás e vonatkozásban is sérti a humanitárius jogot, kivéve, *„ha katonai műveletek rendszeres, jelentős és közvetlen támogatására szolgáltat elektromos energiát, ha a támadás a támogatás megszüntetésének egyetlen lehetséges módja."*[71] Ez azonban esetünkben nem forog fent. Az atomerőművek elleni támadás könnyen belátható módon sérti a természetes környezet védelmének szabályait is hiszen *„nagyarányú, hosszan tartó és súlyos károsodást"*[72] okoz.

A Jegyzőkönyv szerint súlyos jogsértésnek minősül többek között: (1) a polgári lakosság vagy polgári személyek elleni támadás; (2) a polgári lakosságot vagy polgári javakat érintő megkülönböztetés nélküli támadás és (3) veszélyes erőket tartalmazó művek vagy létesítmények elleni támadás indítása annak tudatában, hogy az polgári lakosság körében nagyszámú halálos áldozatot követel, vagy sebesülést okoz, illetve a polgári javakban nagymérvű károkat idéz elő.[73] A fent bemutatott kibertámadások közül az atomerőművek elleni támadás mindhárom esetkörbe beletartozik, a létfenntartó infrastruktúrák elleni támadás és a kommunikációs hálózat elleni fegyveres támadásnak minősíthető kibertámadások pedig az első két kategóriába tartoznak. A Jegyzőkönyv ezeket a cselekményeket háborús bűnnek[74] minősíti, amelyek elkövetőjével szemben büntetőjogi szankciókat kell az államnak alkalmaznia. A Jegyzőkönyv rögzíti azt is, hogy ha *„megsértését alárendelt személy követte el, nem mentesíti feletteseit az eset körülményeitől függően a büntetőjogi vagy fegyelmi felelősség alól, ha tudták, vagy a szükséges értesülések birtokában az adott körülmények között tudhatták volna, hogy az érintett személy jogsértést követ el, vagy készül elkövetni és ha tőlük telhetően nem tettek meg minden intézkedést a jogsértés megakadályozására, illetve megtorlására."*[75] E kitétel a fegyveres támadásnak minősíthető kibertámadás esetén azt jelenti, hogy az azt elrendelő vagy arról tudó katonai vagy állami vezető – hiszen a fegyveres támadás alapvető feltétele az államnak való betudhatóság – felelőssége is megállapítandó, amely az állam felelősségét is előre vetíti e cselekményekért.

[70] 1977. évi I. kiegészítő jegyzőkönyv 56. cikk (1) bekezdés
[71] 1977. évi I. kiegészítő jegyzőkönyv 56. cikk (2) b) pont
[72] 1977. évi I. kiegészítő jegyzőkönyv 55. cikk (1) bekezdés
[73] 1977. évi I. kiegészítő jegyzőkönyv 85. cikk (3) bekezdés
[74] 1977. évi I. kiegészítő jegyzőkönyv 85. cikk (5) bekezdés
[75] 1977. évi I. kiegészítő jegyzőkönyv 86. cikk (2) bekezdés

## 5. A KIBERTÁMADÁSOKÉRT VALÓ FELELŐSSÉG

Ezen fejezetben a kibertámadásokért való felelősség szabályait mutatjuk be. E fejezetet két alfejezetre bontjuk, az elsőben az állam nemzetközi jogi felelősségét tekintjük át a másodikban pedig az egyén büntetőjogi felelősségét.

### 5.1 AZ ÁLLAM KIBERTÁMADÁSOKÉRT VALÓ NEMZETKÖZI JOGI FELELŐSSÉGE

A nemzetközi jogi felelősség lényege, hogy az adott állam jogsértése egy sajátos jogviszonyt hoz létre, mely létre jöhet a jogsértő állam és a jogaiban megsértett állam között, ezáltal kétoldalú jogviszonyt létre hozva, vagy a jogsértő állam és a nemzetközi közösség, mint egész között keletkeztethet több oldalú jogviszonyt, melynek következtében a jogsértő állam köteles jóvátenni, valamint ezen túlmenően ha a helyreállítási kötelezettségének nem tesz eleget a sértett/sértettek szankciókat alkalmazhatnak a jogsértővel szemben. A kibertámadások esetén többoldalú jogviszony létrejöttéről beszélhetünk, hiszen a technikai fejlődés eljutatta arra a szintre az információs rendszerek elleni támadásokat, hogy ezeket fegyveres támadásoknak tekinthessük, amelyek az erőszak tilalmába ütköznek. Ennek okán az ilyen kibertámadás, mint jogsértő cselekmény ún. imperatív normát sért, amelynek következtében a jogsértő állam és a nemzetközi közösség, mint egésze között jön létre a jogviszony.
A nemzetközi jogi felelősség megállapítható – mint már érintőlegesen elhangzott – az államnak a nemzetközi joggal ellentétes cselekménye folytán, melynek lényeges elemei a Nemzetközi Jogi Bizottság tervezete szerint a következők: *„a) a nemzetközi jog alapján betudható az államnak és b) és az állam nemzetközi kötelezettségét sérti.”*[76] Tehát az állam azon cselekménye, amely bármilyen nemzetközi kötelezettség megszegését eredményezi nemzetközi jogsértésnek minősül.
*„A nemzetközi jog különbséget tesz a magánszemély és az állami magatartások között, és a nemzetközi jog alapján csak az utóbbi, az állam felelőssége állapítható meg.”*[77] A nemzetközi jogsértés elkövetője, ahogy az első fejezetben meghatározásra került, a magánszemélyek, az állam; állami szervek. Az egyén illetve magánszemély kivételes esetekben, például a kalózkodással elkövetett nemzetközi jogsértés miatt vonható felelősségre a nemzetközi jog alapján, ebben az esetben tehát nem a lobogó szerinti állam tartozik felelősséggel. Az állam jogsértő cselekményének elkövetője az államigazgatási szervek és a fegyveres erők tagjai, hiszen az állam felelősséggel tartozik minden rendű és rangú szerve által elkövetett jogsértő cselekménye miatt, ha a jogsértő cselekmény egy külállam ellen irányul. A fegyveres erők tagjait azért is sorolhatjuk ide, mivel hatáskörükben eljárva hatósági feladatokat valósítanak meg. E körben kell még meg említeni a Nemzetbiztonsági Szolgálatok hivatásos állományú tagjait, hiszen elképzelhető, hogy ezen személyek egy másik állam területén az állam utasítására kibertámadások elkövetésével jogsértő cselekményeket fejtenek ki.
Az állam felelőssége alapvetően objektív felelősség, hiszen a felróhatóság alapja nem az állam, állami szerv vétkessége, hanem az a jogi kapcsolat, amely állam és az állam szervei között fennáll, így elég csak azt bizonyítani, hogy az eljáró szerv tevékenysége és a jogsértő cselekmény között okozati összefüggés van. Ettől eltérően azon kibertámadások esetén, melyek az erőszak tilalmába ütköznek véleményünk szerint a jogsértő cselekmény elkövetése szándékos, tehát itt az állam vétkessége egyértelműen megállapítható, ezért vétkesség szempontjából vegyes felelősség, hiszen ebben az esetben a vétkesség a jogsértés fogalmi eleme.

[76] Draft Articles on Responsibility of States for Internationally Wrongful Acts, adopted by the International Law Commission at its fifty-third session, 2001, Article 2.
[77] CHIA LEHNARDT: *Private Militärfirmen und völkerrechtliche Verantwortlichkeit*, Tübingen, Mohr Siebeck, 2011, 82. o.

Problémás azonban, azaz eset, amikor az állam nevében eljáró tisztviselő a belső jogot is megsértve, hatáskörén túllépve, az utasításoknak nem megfelelően cselekszik. A belső jog megsértése következtében aktusai jogellenesnek minősülnek, ezáltal semmisek, *„hiszen nehéz állami aktusnak tekinteni az olyan cselekményeket, amelyek az állam jogának megsértését jelentik, mivel ilyenkor az állami funkcionárius az állam akaratával ellentétesen járt el. Az ilyen cselekmények, amikor egy idegen államnak nemzetközi jogsérelmet okoznak, egyben a saját állam ellen is irányulnak és tényleg problematikusnak látszik felelőssé tenni az államot egy olyan cselekmény miatt, amelynek — belső jogi szempontból — ő is sértettje."*[78] Erre ad választ a Nemzetközi Jogi Bizottság 2001-es tervezetének 7. cikke, mely szerint *„a kormányhatalom alkotóelemeinek gyakorlására felhatalmazott szerv magatartását, amennyiben a szerv ilyen minőségében járt el, a nemzetközi jog szerint az állam cselekedetének kell tekinteni, még akkor is, ha adott esetben a belső jog szerinti hatáskörét túllépte vagy a tevékenységét illető utasításokat szegett meg."*[79] Tehát az állam felelőssége megállapítható, olyan kibertámadások esetén is, melyeket az állami szervek személyi állománya hatáskörüket túllépve, az utasításokat megszegve követett el. Szintén megalapozza az állam felelősségét, ha az állam funkcionáriusa az utasításoknak és a belső jognak megfelelően járt el, de az állam belső joga ellentétes a nemzetközi joggal.

A nemzetközi jogban is találhatunk, olyan körülményeket, amelyek hatással vannak a jogellenes cselekmény megítélésére, ennek megfelelően kizárják a jogellenességet. A Nemzetközi Jogi Bizottság 2001-es tervezetének 20-26. cikkei szerint ezek a körülmények a következők: 1) a sértett állam beleegyezése, 2) az önvédelem, 3) a nemzetközi jogsértő cselekménnyel szembeni ellenintézkedések, 4) a vis major, 5) a szükséghelyzet, 6) a végszükség, 7) ha az állam a nemzetközi jog imperatív normáját érvényesíti. Nagy Károly szerint nem teljes ezen körülmények felsorolása, véleménye szerint ki kell egészíteni a hivatalos minőség hiányával, a hatáskör nyilvánvaló hiányával és végül a sértett önhibájának enyhítő illetve kizáró körülményével.[80] Véleményünk szerint a kibertámadások esetén, ha az eljáró állami szerv tisztviselője nem hivatalos minőségében, hanem mint magánszemély jár el, az kizárja az állam felelősségét, hiszen nem a jogsértő cselekmény a lényeges elem, hanem az, hogy az adott állami szerv tisztviselője milyen minőségben követte el azt. A hatáskör teljes hiányáról, mint kimentő okról a kibertámadások esetében nem beszélhetünk, mivel lényeges feltétele, hogy a hatáskör hiánya olyannyira nyilvánvaló, hogy a másik félnek arról tudnia kellett volna. A kibertámadások esetén ez azért problémás, mert a támadások sokszor rejtve fejtik ki hatásukat, továbbá zombihálózatok esetén nehéz megállapítani a tényleges elkövetőt. A jogellenességet kizáró okok közül kizárhatóak a beleegyezés, a vis major, a szükséghelyzet, a végszükség, mivel a kibertámadások az állam szándékos cselekményei.

Az állam nemzetközi jogsértő magatartása végezetül létrehozza a nemzetközi felelősség lényeges elemét azt a sajátos jogviszonyt, mely fenn állhat a jogsértő állam és a jogaiban sértett állam között vagy a nemzetközi közösség, mint egész között, melynek következtében a jogaiban sértett állam/államok felelősségi igénye fakad. Ezt az igényt érvényesíthetik a sértettek, hiszen a nemzetközi jogsértéseknek különféle jogkövetkezményei lehetnek. *„A jóvátételre vonatkozó általános szabályként tehát csak az arányosság elve, valamint azon elv szögezhető le, hogy a kötelezettség mértékét és tartalmát az érdekelt felek megállapodása határozza meg."*[81] A jóvátétel, mint a jogsértés jogkövetkezménye csupán egy gyűjtő fogalom, magába foglalja az eredeti állapot helyreállítását (in integrum restitutio), az elégtétel

[78] NAGY KÁROLY: *A vétkesség szerepe a nemzetközi jogi felelősségi jogviszonyban*, in. Jogtudományi Közlöny 1978/ 10. szám, 585. o.
[79] Draft Articles on Responsibility of States for Internationally Wrongful Acts, Article 7.
[80] NAGY KÁROLY: *Nemzetközi jog*, Budapest, Püski Kiadó, 1999, 541. o.
[81] NAGY KÁROLY: *A jóvátétel problémája a nemzetközi jogban*, in. Jogtudományi Közlöny 1981/ 8. szám, 667. o.

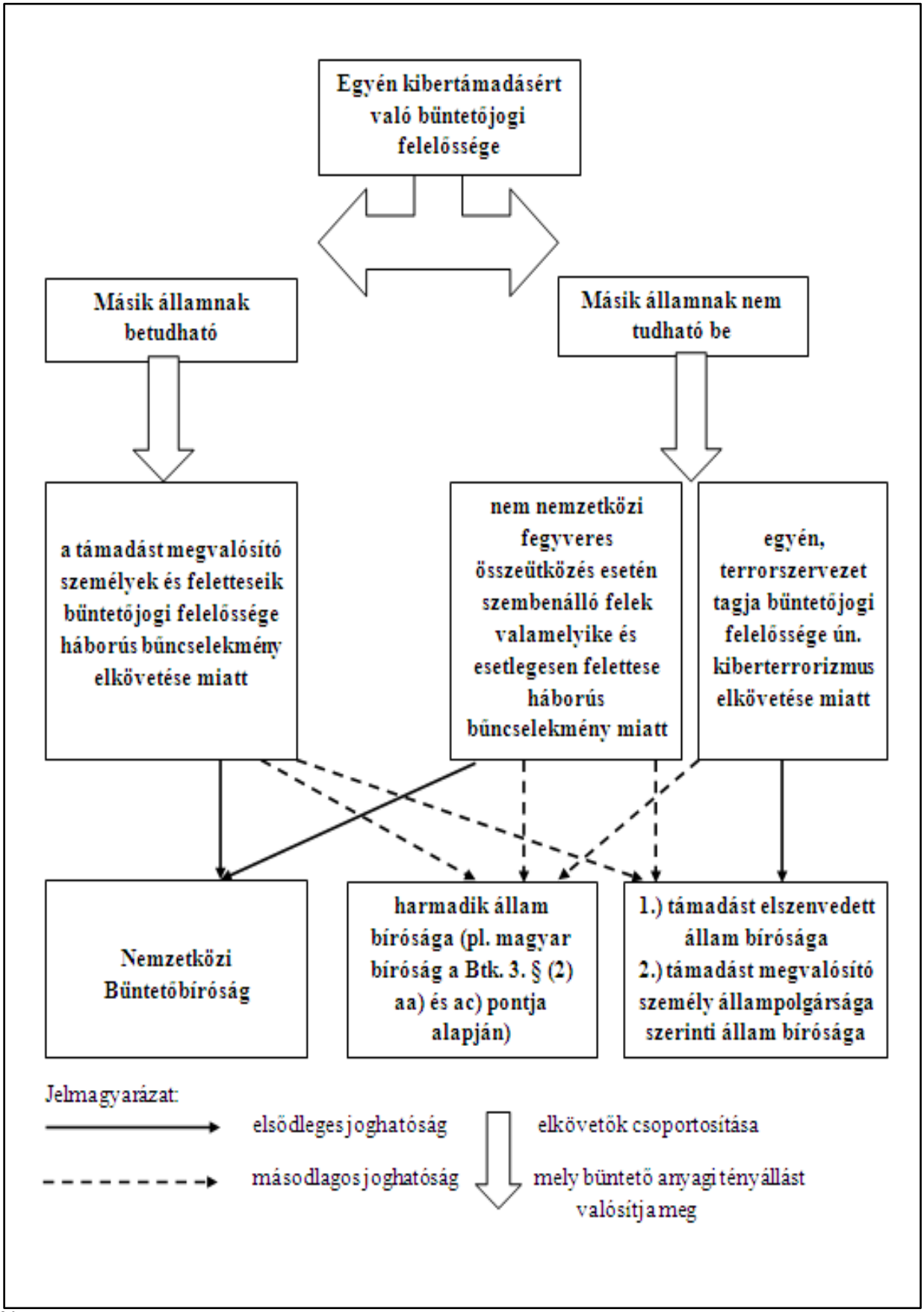
adását (statisfactio), valamint az okozott kár megtérítését. A jogaiban sértett állam ezen jóvátételeket kérheti és amennyiben a jogsértő állam megtagadja azok teljesítését, a sértett állam szankciókat alkalmazhat azok kikényszerítésére. Az eredeti állapot helyreállítása elsősorban a jogsértő magatartás abbahagyását jelenti a jogsértő állam részéről, másodsorban jelentheti például anyagi javak elvétele esetén az eredeti dolog visszaadását, vagy helyettesíthető dolog esetén más hasonló dolog átadását. Ha azonban a jogsértés jellegénél fogva az eredeti állapot helyreállítása nem lehetséges, akkor a jogaiban sértett állam kérheti az okozott kár megtérítését, melynek fontos feltétele, hogy a kár pénzben kifejezhető legyen. A kár fogalma alatt értjük a közvetlen illetve a közvetett kárt is. A Nemzetközi Bíróság gyakorlatában közvetett kárnak minősül az olyan jövőben bekövetkező kár, mely a jogsértő cselekménnyel okozati összefüggésben van. Az elmaradt haszon nem minősül közvetett kárnak, hiszen az minden esetben meghatározható és megítélhető. Az elmaradt haszon körében állapítja meg a Nemzetközi Bíróság a kamatot is.[82] Elégtétel adására akkor kerülhet sor, ha a jogsértő állam a sértett állam méltóságát, egyéb nem anyagi érdekeit sértette meg, melynek a legenyhébb kifejeződési formája, melynek következtében a jogsértő állam sajnálkozását fejezi ki a sértett állam felé. Véleményünk szerint a kibertámadások esetén a jóvátételként a jogsértő magatartás abbahagyása és az okozott kár megtérítése igényelhető a jogaiban sértett állam részéről, az elégtétel adása megítélésünk szerint önmagában nem alkalmazható, az csak valamely másik jóvátételi formával együtt vehető igénybe, mivel jelen esetben a jogsértés olyan fokával állunk szemben, amelyre a jóvátételek közül a legenyhébb forma alkalmazása önmagában nem elegendő a jogsértés jogkövetkezményeinek orvoslására.
Összegezve tehát a kibertámadások esetén többoldalú jogviszony létrejöttéről beszélhetünk, amelyek az erőszak tilalmába ütköznek. Ennek okán a kibertámadás, mint jogsértő cselekmény ún. imperatív normát sért, amelynek következtében a jogsértő állam és a nemzetközi közösség, mint egésze között jön létre a jogviszony. A jogsértő cselekmény elkövetése szándékos, tehát itt az állam vétkessége egyértelműen megállapítható. Az állam felelőssége megállapítható, olyan kibertámadások esetén is, melyeket az állami szervek személyi állománya hatáskörüket túllépve, az utasításokat megszegve követett el. A kibertámadások esetén, ha az eljáró állami szerv tisztviselője nem hivatalos minőségében, hanem mint magánszemély jár el, az kizárja az állam felelősségét, hiszen nem a jogsértő cselekmény a lényeges elem. A hatáskör teljes hiányáról, mint kimentő okról a kibertámadások esetében nem beszélhetünk, mivel lényeges feltétele, hogy a hatáskör hiánya olyannyira nyilvánvaló, hogy a másik félnek arról tudnia kellett volna.

[82] SHAW, MALCOLM N.: *Nemzetközi jog*, Budapest, Osiris Kiadó, 2002, 488. o.

## 5.2 AZ EGYÉN KIBERTÁMADÁSOKÉRT VALÓ FELELŐSSÉGE

Az egyén jogalanyisága a nemzetközi jogban kettős, egyfelől rendelkezik aktív jogalanyisággal, vagyis emberi jogokkal, valamint passzív jogalanyisággal, vagyis a nemzetközi bűncselekményekért való egyéni felelősséggel. A nemzetközi büntetőjog kezdetének Peter von Hagenbach 1474-es perét szokás tekinteni, aki Breisach városának helytartójaként a város lakosságával szemben súlyos kegyetlenkedéseket követett el. Elvi alapját Hugo Grotius rögzítette A háború és béke joga című művében. E könyvben fogalmazta meg az aut dedere, aut judicare (vagy kiadni, vagy büntetni) elvet, amely *„mind a mai napig a nemzetközi bűnügyi együttműködés vezérfonalának tekinthető”* és, amely *„Grotius szerint minden államnak alapvető kötelessége, mert a nemzetközi közösség csak így védhető meg hatékonyan és így biztosítható, hogy bűncselekmény megtorlatlanul ne maradjon.”*[83]
A nemzetközi büntetőjog olyan bűncselekményeknek a közös meghatározása és üldözése, amelyek az emberiség valamint a nemzetközi közösség egyetemes értékeit támadják. Az ilyen cselekmény elkövetőit nevezhetjük hostis humanis generisnek, vagyis az emberiség közös ellenségének.
A 19. század közepétől figyelhető meg e téren tényleges együttműködés, amikor is egyezmények sorát alkották meg.[84] Az első világháború után merült fel először annak igénye, hogy a nemzetközi erkölcs és szerződéses jog megsértése miatt büntetőjogi felelősségre vonásnak lenne helye, ezt a Versaillesi Szerződés 227. cikke rögzítette is, azonban II. Vilmos felelősségre vonása elmaradt. *„A második világháborút követően viszont a nemzetközi bűncselekmény már olyan fogalom lett, amelynek alapján büntetést alkalmaztak. A nürnbergi és a távol-keleti perekben nemzetközi bűncselekményekért ítélték el a vádlottakat, s az ítéletet nem egy-egy állam büntető kódexére alapították.”*[85] Az 1948-as genocídium egyezményben határozták meg az emberiség elleni bűncselekmények fogalmát. Az apartheid egyezmény (1973) pedig a faji elkülönítés egy sajátos fajtájának nemzetközi pönalizálását eredményezte.
Ma egyre újabb területek kerülnek a nemzetközi büntetőjog terrénuma alá: kábítószer-kereskedelem, pornográfia, prostitúció, pedofília, nemzetközi terrorizmus, nemzetközi korrupció valamint a témánk szerinti számítógépes hálózatokba való behatolás, adatszerzés és támadás.
A kibertámadások elkövetőinek büntetőjogi felelősségre vonása eltérő törvényi tényállás alapján és eltérő fórum előtt valósulhat meg annak fényében, hogy nemzetközi jogi értelemben a támadás fegyveres támadásnak minősül vagy esetlegesen nem nemzetközi fegyveres összeütközés valamely alanya hajtja végre vagy a tettes olyan kibertérben elkövetett támadást hajt végre, amely nem tudható be más államnak.

[83] POLT PÉTER: *A nemzetközi büntetőjog fejlődésének néhány kérdése*, in. Jogtudományi Közlöny 1987/4. szám, 173. o.
[84] 1841-től tilalom alá került a rabszolga-kereskedelem; 1856-ban a párizsi konferencián az államok betiltották a kalózlevelek kiállítását; hágai konferenciákon (1899, 1907) pedig lefektették a hadviselés minimum szabályait.
[85] WIENER A. IMRE: *Nemzetközi büntetőjog – nemzetközi bűncselekmények*, in. Jogtudományi Közlöny 1986/6. szám, 259. o.



[86]

[86] Szerzők által készített ábra.

Az utóbbi esetben ítélhető meg legegyszerűbben a joghatóság és alkalmazandó jog kérdése, hiszen a kibertámadás elkövetésében résztvevő személy(ek) felelősségét, az aut dedere, aut judicare elv alapján a megtámadott állam büntető igazságszolgáltatási szervezete jogosult megállapítani, vagy pedig követelni a másik államtól a felelősség megállapítását. E területen alkalmazandó büntető anyagi jogi szabályok egyre egységesebb képet mutatnak a nemzetközi büntetőjogi együttműködés révén. A kibertérben elkövetett bűncselekmények törvényi tényállásának meghatározása terén két szabályozási technika alakult ki, az egyik az Európában, így Magyarországon is alkalmazott egységes büntetőjog elvén nyugvó Btk.-ban történő szabályozás, a másik technika, pedig az indiai, ahol a büntetőkódexen kívül szabályozzák a kibercselekményeket egy ún. IT Act-ben. A következőkben e két modellt tekintjük át.

Európában az első egységesítést célzó egyezmény az Európa Tanács 2001-ben Budapesten elfogadott Informatikai bűnözésről szóló Egyezménye (Cybercrime Egyezmény), amely révén a 2001. évi CXXI. törvénnyel a jogalkotó új tényállásokat hozott létre. Ezen bűncselekmények voltak a számítástechnikai rendszer és adatok elleni bűncselekmény, valamint a számítástechnikai rendszer védelmét biztosító technikai intézkedés kijátszása.[87] A törvénymódosítás orvosolta a számítógépes rendszer fogalmának[88] büntető törvénykönyvi hiányát is. *„Az új tényállás – az új formában megjelenő számítógépes csalás mellett – büntetni rendelte a számítástechnikai rendszerbe történő jogosulatlan belépést, valamint a számítástechnikai rendszer és az abban tárolt, feldolgozott, kezelt vagy továbbított adatok sértetlensége elleni cselekményeket is.”*[89]

A 2003. évi II. törvénnyel a terrorizmus eszközcselekményeként határozták meg a számítástechnikai rendszer és adatok elleni bűncselekményt. A célcselekmények taxációjával *„[…] elkészült a köztörvényes bűncselekményeknek azon tételes listája, melyet a terroristák legitimnek hitt céljaik elérése érdekében elkövetnek. Dogmatikailag egy új típusú delictum complexum került ezzel megalkotásra, ahol az eszközcselekmény nem önmagában egy elkövetési magatartás, hanem egyenesen egy önálló bűncselekmény.”*[90] Igényként merült fel azonban újabb számítógéppel elkövethető cselekmények pönalizálása, mint például a számítógépes adatok megszerzése.

A tényállás fejlődésében előképet jelentett az Unió 2005/222/IB Kerethatározata, melyből kitűnt, hogy a kodifikáció jövőbeli iránya a számítógépes rendszerrel elkövetett csalás és számítástechnikai rendszer és adatok elleni bűncselekmény szétválasztása. Ennek magyarázata, hogy az utóbbi alá egyre több típusú elkövetési magatartás tartozhat, és ezek szükségessé tették önálló tényállásként való szabályozását. Hiszen ekkor a tényállás csak a számítógépes rendszerben tárolt adatokkal kapcsolatos tényállási elemeket tartalmazott, míg a kerethatározat már információs rendszerhez való jogsértő hozzáférést, a rendszerben való jogsértő beavatkozást is büntetendő cselekményként kezelte.[91]

A két bűncselekmény különválasztása a 2012. évi C. törvényben, vagyis az új Büntető törvénykönyvben történt meg. A terrorizmus új kiber eszközcselekménye az információs

[87] 2001. évi CXXI. törvény a Büntető Törvénykönyvről szóló 1978. évi IV. törvény módosításáról 57-58. §.

[88] *„Számítástechnikai rendszer az adatok automatikus feldolgozását, kezelését, tárolását, továbbítását biztosító berendezés vagy az egymással kapcsolatban lévő ilyen berendezések összessége*”- 1978. évi IV. törvény a Büntető törvénykönyvről 300/F. §.

[89] BELOVICS ERVIN, MOLNÁR GÁBOR MIKLÓS, SINKU PÁL: *Büntetőjog – Különös rész,* Budapest, HVGorac Lap- és Könyvkiadó, 2009, 591. o.

[90] BARTKÓ RÓBERT: *A terrorcselekmény, mint nemzetközi bűncselekmény*, in. Rendészeti Szemle 2010/5. szám, 216. o.

[91] Európai Unió Tanácsának 2005/222/IB Kerethatározat az információs rendszerek elleni támadásokról 2-3. cikk.

rendszer vagy adat megsértése elnevezésű tényállást lett.[92] Mely teljes egészében megfelel az Uniós szabályozási kritériumainak.
Az Európai Unió és Tanács 2013 nyarán új irányelvet fogadott el – amely felváltotta 2005-ös kerethatározatot – amelyben az Unió újraszabályozta a kiberbűnözés típusait és azokhoz kapcsolódó tényállásokat. A magyar szabályozásban tényállási szinten biztosan változást eredményez a jogellenes adatszerzés kiberbűnözésként való megjelenése. Az irányelv kimondja, hogy *„… az információs rendszeren belülre, kívülre vagy azon belül továbbított, nem nyilvános számítógépes adatok – többek között az információs rendszerekből érkező, ilyen adatokat hordozó elektromágneses sugárzás – technikai eszközökkel történő, szándékos és jogosulatlan megszerzése, legalább a súlyosabb esetekben bűncselekménynek minősüljön.”*[93] Az már a jogalkotó saját hatásköre, hogy új tényállást alkot vagy a 423. szakasz részévé teszi, mint új elkövetési magatartást.
Az irányelv kimondja még, hogy az ezen bűncselekmények elkövetési eszközeinek előállítóit, forgalomba hozóit szintén büntetni kell. A magyar jog ezt már a jelenlegi szabályozással is megteszi, így itt nincsen feladata a törvényhozásnak. Általánosságban elmondható, hogy az irányelv szabályai szigorodtak a kerethatározathoz képest, ami jól lemérhető az általa nyújtott szankciónálási lehetőségben. Mivel a 2005-ös kerethatározat a büntetés maximumaként 3 évet jelölte meg, addig a 2013-as irányelv már 5 évben maximál. Az irányelvből kitűnik az információs rendszerek fontossága, hiszen ezek, mint fogalmaz *„…a politikai, a társadalmi és a gazdasági interakció kulcstényezői az Unióban.”*[94] Ezen infrastruktúrák védelme alapvető Uniós érdek és ezt a nemzeti büntetőjogi szabályoknak is tükrözniük kell. Ezért véleményünk szerint a tiltott adatszerzés alapesetei közül az elektronikus hírközlő hálózat – ideértve az információs rendszert is – útján másnak továbbított vagy azon tárolt adatot kifürkész, és az észlelteket technikai eszközzel rögzíti fordulat szerinti tényállást is a terrorcselekmény eszközcselekményévé kellene tenni, mivel mint, ahogy arra már korábban is kitértünk a mai társadalomban az egyik legfontosabb hatalmi forrás az információ, amelynek birtokosa azt akár fegyverként is fel tudja használni a társadalom széles tömegeivel, az állammal és akár nemzetközi szervezetekkel szemben is.
India 2000-ben az elsők között alkotta meg saját törvényét kiberbűnözés területén. Sajátos módon azonban nem a bűntető törvénykönyv részeként, hanem önálló független törvényként, amely a kódexhez hasonlóan büntetési tételek is megállapít, azonban attól eltérően államszervezetet érintő rendelkezéseket is tartalmaz. A törvény a kibertér egészére nézve definiálja annak részeit, így többek között meghatározásra került a számítógépes hálózat, az információs hálózat, az adat, az elektronikus információ, az elektronikus irat, a kulcspár, a biztonsági rendszer.[95] Ezt követően szintén ilyen részletességgel kifejti az ezekre vonatkozó állami szabályokat. Ezt követően kerülnek csak meghatározásra azok a deliktumok, amelyek ezeket a rendszereket sértik. Témánk szempontjából kiemelendő a 66/F. szakasz, amely szerint: *„(1) bárki (A) aki szándékosan fenyegeti vagy veszélyezteti az Indiai Állam egységét, integritását, biztonságát, szuverenitását vagy az állampolgárokat vagy azok bármely csoportját azzal,*
*i.) hogy lehetetlené teszi a hozzáférést az számítógépes erőforrásokhoz*[96] *vagy*
*ii.) engedély nélkül vagy azt meghaladva megpróbál behatol vagy felhasználni a számítógépes erőforrás vagy*

[92] 2012. évi C. törvény a Büntető Törvénykönyvről 314. § (3) i) pont.
[93] Európai Parlament és Tanács 2013/40/EU irányelv az információs rendszerek elleni támadásokról és a 2005/222/IB tanácsi kerethatározat felváltásáról 6. cikk.
[94] Európai Parlament és Tanács 2013/40/EU irányelv az információs rendszerek elleni támadásokról és a 2005/222/IB tanácsi kerethatározat felváltásáról (2) bekezdés.
[95] Indian IT Act 2008 2. § (1) a-z pontok.
[96] Számítógépes erőforrás: számítógép, kommunikációs eszköz, számítógépes rendszer, számítógépes hálózat, adatok, számítógépes adatbázis vagy szoftver. Indian IT Act 2 (1) k) pont.

*iii.) valamilyen módon megfertőzni*
*és ezzel a cselekménnyel halált vagy személyi sérülést, vagyon megsemmisülését vagy károsodását, az áruk vagy szolgáltatások rendszerében kárt vagy zavart okoz vagy hátrányosan befolyásol létfontosságú infrastruktúrákat az büntetendő.*
*(B) Szándékosan engedély nélkül vagy azt meghaladva információs rendszerekbe behatol és ezáltal olyan információhoz, adathoz, adatbázishoz jut, amely minősített adatot tartalmaz az államról vagy annak kapcsolatairól vagy egyéb bizalmas adatról és ezzel veszélyezteti az Indiai állam biztonságát, szuverenitását, kapcsolatát más államokkal vagy előnyt szerez idegen országnak, csoportnak vagy más személynek kiberterrorizmust követ el."*[97]
Az európai gyakorlattól eltérően, az indiai törvény külön szabályozza azon kibercselekményeket, amely az állam integritását sértik, továbbá szintén külön törvényi tényállás a kiberterrorizmus is.
Eltérő kodifikációs módszereket követnek az egyes államok az információs rendszereket ért támadások büntető szabályozása során, azonban az látható, hogy a pönalizált cselekmények köre nagyon hasonló, így e területen eredményes a nemzetközi büntetőjognak az egységesítésre vonatkozó törekvése.
Mint azt korábban megállapítottuk a kibertámadást elkövető személy és annak feletesse az Jegyzőkönyvbe foglaltak alapján a humanitárius jog súlyos megsértése következtében háborús bűncselekmények elkövetése miatt felelős. Az igazságszolgáltatás számára jelentősebb nehézségekkel jár ezen cselekmények értékelése annak okán, hogy az államok többsége elismeri és büntető kódexében alkalmazza az egyetemes büntetőhatalom elvét. Ezen elv alkalmazásával a jogalkotók *„a kultúrállamok által elismert jogtárgyak közös büntetőjogi védelmét"*[98] kívánják megteremteni. Az egyetemes büntetőhatalom elvének alkalmazási körébe jelenleg a Nemzetközi Büntetőbíróság Statútumában (továbbiakban Statútum) felsorolt bűncselekmények tartoznak.
Az egyetemes büntetőhatalom elve szerint, tehát gyakorolhatja büntetőhatalmát a sértett állam, az az állam, amely állampolgára elkövette a cselekményt, de akár harmadik államok is.
Véleményünk szerint a büntető igazságszolgáltatás hatékonysága, az ítélet végrehajthatósága szempontjából ez számos problémát vett fel, ezek pedig a következőek:
Ha a (1) nem nemzetközi fegyveres összeütközés esetén elkövetett háborús bűntettel – bármely oldalon álló személy is követte el azt – kapcsolatban az adott állam bírósága hoz ítéletet, annak legitim voltát az állammal szemben álló személyek vitatni fogják, tovább mélyítve a válságot. Ilyen ügyben a harmadik állam bírósága által hozott ítéletet, pedig az összeütközésben érintett állam tekintheti belügyeibe való beavatkozásnak.
Problémát jelenthetett az, hogy a (2) fegyveres támadást megvalósító állam nem kíván ténylegesen büntetőeljárást lefolytatni vagy a jogszabályoknak megfelelő büntetést kiszabni, ebben az esetben a Statútum alapján a Nemzetközi Büntetőbíróság eljárásának van helye. Szintén további nemzetközi konfliktust forrása lehet az is, ha a sértett, megtámadott állam nem fogadja el a támadó állam bírósága által hozott ítéletet és továbbra is érvényesíteni kívánja büntető hatalmát.
A nemzetközi jog szabályaiból eredő dilemma (3) a diplomáciai mentesség kérdése. A diplomáciai mentességet élvező személy, aki a parancs kiadója volt vagy ellenőrzése mellett valósították meg a cselekményt nem vonható felelősségre sem harmadik, sem a sértett állam bírósága előtt, kivéve, ha a küldő állam megszünteti a mentességét. E kérdés merült fel Yerodia kongói külügyminiszter ügyében is, akivel szemben Belgium harmadik államként kívánt fellépni, azonban Kongó az 1961. évi bécsi szerződésre hivatkozva eljárást kezdeményezett a Nemzetközi Bíróságnál, amely kimondta, hogy *„a külügyminisztereket*

[97] Indian IT Act 66/F.
[98] LIGETI KATALIN: *Büntetőjog és bűnügyi együttműködés az Európai Unióban*, Budapest, KJK-KERSZÖV Jogi és Üzleti Kiadó, 2004, 47. o.

*megillető mentesség nem személyhez kapcsolódik, hanem a betöltött funkcióhoz, tehát ahhoz, hogy külföldi államot képviselnek. A Bíróság döntésében arra a következtetésre jutott, hogy a hivatalban lévő külügyminiszterek külföldön teljes mentességet élveznek a büntető joghatóság alól és sérthetetlenek. E körben nem lehet különbséget tenni a külügyminiszterek cselekedeteiben aszerint, hogy azokat hivatali működésük során vagy magánemberként követték el."*[99] Természetesen a joghatóság alóli mentesség és a büntetlenség között nem tehető egyenlőség. Az ilyen személy bűnösségét megállapíthatja saját államának bírósága, más állam bírósága, abban az esetben, ha a küldő állam megszünteti a diplomáciai mentességet vagy a hivatali ideje lejárt. Ezekben az esetekben az előző pontokban megfogalmazott problémákhoz térhetünk vissza. Tényleges megoldás, hogy a nemzetközi törvényszékek előtt ezeket a mentességeket nem lehet érvényesíteni, így rendelkezik a Statútum 27. cikke[100] is.

A bíróságok által meghozott ítéletekben jelentős különbségeket okozhatnak az (4) eltérő anyagi jogi szabályok is. Erre példaként szolgál a közvetett parancsnoki felelősség[101] korábbi Btk.-beli szabályozása, ugyanis a nemzetközi jogi szabályok (1977. évi I. kiegészítő jegyzőkönyv 86. cikk 2. bekezdés, Statútum 28. cikk a) pontja) az egyéni büntetőjogi felelősség formái között tárgyalják a katonai parancsnok büntetőjogi felelősségét, míg a korábbi Btk. 361. §-a önálló tényállásként nevesítette a cselekményt, mint az elöljárói intézkedés elmulasztása. A Statútum által szabályozott cselekmény Btk.-ban meghatározott alapeset büntetési tétele 5-10 évi szabadságvesztés büntetés, míg az önálló tényállás minősített esetének legmagasabb tétele az öt évi szabadságvesztés volt. Az új Btk. korrigálta e visszásságot, hiszen a nemzetközi jogi szabályoknak megfelelően rendeli bünteti a 159. §-ban a parancsnok közvetett felelősségét. Előrelépés, hogy a hivatalos személyek esetében is lehetőség van közvetett felelősség megállapítására, azonban visszás az a helyzet, hogy a nemzetközi jog gyakorlatával ellentétben – ahogy azt korábban a Dusko Tadic-ügyben bemutattuk – még a tényleges ellenőrzés esetében rendeli csak büntetni a cselekményt, a nemzetközi jogban alkalmazott és a mai viszonyoknak jobban megfelelő általános ellenőrzés (*overall control*) helyett.

A felvázolt problémákból jól kiviláglik, hogy az egyetemes büntetőhatalom elvének alkalmazása helyett jóval hatékonyabb és célravezetőbb volna, ha a Nemzetközi Büntetőbíróság szubszidiárius joghatóságát általános joghatósági szabállyá változtatnák az államok a Statútumba foglalt bűncselekmények (népirtás bűncselekménye, emberiesség elleni bűncselekmények, háborús bűncselekmények, agresszió bűncselekménye (2017-től)) esetében. Ezzel megkönnyítve a nemzetközi büntetőjog feladatának érvényesülését, vagyis *„azoknak a jogtárgyaknak a védelmét, amelyeknek a védelmére a belső jogrend már nem elégséges. A nürnbergi bűncselekmények ugyanis azt mutatták, hogy mindegyiket vagy az állam nevében, vagy legalábbis hallgatólagos beleegyezésével követték el,"*[102] és ez volt megfigyelhető később Pol Pot Kambodzsájában, Milosevic Jugoszláviájában vagy a ruandai népirtás során is.

---

[99] WIENER A. IMRE: *A büntető joghatóság és gyakorlása, kivált az Európai Unióban,* in. Állam- és Jogtudomány 2002/3-4. szám, 186-187. o.

[100] Nemzetközi Büntetőbíróság Római Statútumának 27. cikke, magyar nyelvű szöveg: T/4490. számú törvényjavaslat az Egyesült Nemzetek Diplomáciai Konferenciája által, a Nemzetközi Büntetőbíróság Rómában, 1998. július 17-én elfogadott Statútumának kihirdetéséről.

[101] A parancsnok valamely alárendeltje bűncselekményt valósít meg – amely cselekmény megvalósítására nem a parancsnoktól kapott utasítást – és a parancsnok annak ellenére, hogy tudott vagy tudhatott az elkövetésről nem tett meg mindent ami hatásköréből eredt, hogy az elkövetést megakadályozza vagy az elkövető felelősségre vonását nem kezdeményezte.

[102] WIENER A. IMRE: *Büntető joghatóság és a nemzetközi jog,* in. Állam- és Jogtudomány 1993/3-4. szám, 197. o.

## ÖSSZEGZÉS

A 20. század végére az internet révén az egyes információs rendszerek globális hálót alkotnak. Ezen hálózat részét képezik a civil személyeken és gazdasági társaságokon túl az államok létfontosságú rendszerei is. A 1990-es évek végére a hadviselés új arcát mutatta a számítógépes hadviselés révén. A számítógépek fejlődésével egy ütemben nő azon szakemberek száma, akik képesek az állam alapvető rendszereiben a kibertéren keresztül kárt tenni. A köznyelv ezen elkövetőket hackereknek nevezi. Hibásan, hiszen ezen elnevezés igen tág kategória, magába foglalja a valódi hackert, a dark-hackert, a light-hackert, a wannabe hackert és így tovább. Ezen személyek szakmai tudása és szándéka között igen jelentős eltérések vannak. Ezen személyek igen szűk köre képes valódi kibertámadás végrehajtására, ezek a valódi hackerek, a dark-hackerek és HPAV csoportok. A valódi hackerek inkább a rendszerek védelmével foglalkoznak, azonban állami szervezet részeként parancsra támadást is végrehajthatnak. A dark-hackerek illetve a HPAV-k, esetében erkölcsi kérdések sem merülnek fel, ez a személyi kör az, amely az állami szervezeten kívül is hajlandó az állam támadó típusú utasításait megvalósítani.

A fenti szakemberek által alkalmazott eszközök körét azok célját alapul véve három nagy csoportba lehet osztani: (1) információ és adatszerzés; (2) információs rendszer megzavarása; (3) információs rendszer elpusztítása. Utóbbi kettő az, amely eszköze lehet a fegyveres támadásnak.

Ezek a támadások valóban az ENSZ Alapokmány 51. cikke szerinti fegyveres támadásnak minősíthetők? Véleményünk szerint igen, azonban önmagában csak akkor, ha a támadás eredménye, következménye vagy együttes hatása fizikai végkifejlethez vezet és ezen eredmények pusztító hatása – bár normatív fogalma nincs, de általánosan elfogadott küszöbértékként kezelhetően – nagyszámú emberi életeket veszélyeztet vagy olt ki illetve az infrastruktúrában jelentős kárt okoz.

Ilyen végkifejletű támadás lehet egy atomerőmű elleni támadás, amely annak megsemmisítését eredményezi, amely a nukleáris fegyverekkel analóg módon sérti az ENSZ alapokmány 2. cikk (4) bekezdését és az 51. cikket is. De ilyen eredményt érhet el egy olajfinomítót, a légiközlekedést, a vasúti közlekedést irányító információs rendszerek elleni támadás is.

Az olyan offenzívát is ide lehet sorolni, amelynek közvetlen következménye nagy számú ember életének veszélyeztetése vagy kioltása. Ilyen lehet a víztisztító hálózatot ért támadás, amely eredményeként szennyezett ivóvíz kerül a rendszerbe. Analóg módon ezt lehet vegyi vagy biológiai támadásnak kezelni, ezeket a fegyvereket viszont multilaterális egyezmények tiltják, amelyeket szinte a teljes nemzetközi közösség aláírt, így egy ilyen támadás már kisebb számú áldozat esetén is fegyveres támadásnak minősíthető. Ilyen típusú támadás érheti a földgáz vagy a távhőszolgáltatók rendszerét is.

Szintén közvetlen következményekkel járó támadás lehet az Észtországot ért támadáshoz hasonló is, azonban erre csak egy jóval hosszabb ideig tartó és jóval intenzívebb támadás lehet alkalmas, amely kettő-négy nap alatt megbénítja az állam működését és azt anarchiába süllyeszti. Ebben az esetben azonban kérdéses, hogy az állam egyáltalán képes-e önvédelmi jogával élni.

Fontos kritériuma a fegyveres támadásnak, hogy az egy másiknak államnak betudható legyen, ennek megállapítása a kibertérben még fokozottabb nehézségekkel jár, mint hagyományos hadszíntéren. Erre megoldás lehet a Kínaiak által használt SAVA rendszer, amely képes lehet az elkövetők azonosítására.

Annak okán, hogy fegyveres támadásnak minősülhet egy kibertámadás, azzal az állammal szemben, amelynek ez betudható, érvényesítni lehet a nemzetközi felelősség erőszak alkalmazásának megsértésére vonatkozó nemzetközi jogi szabályokat.

Az egyén büntetőjogi felelősségnek területén az egyetemes büntetőhatalom elvének alkalmazása helyett a Nemzetközi Büntetőbíróság szubszidiárius joghatóságát általános joghatósági szabállyá kellene módosítani a Statútumba foglalt bűncselekmények esetében. Ennek oka, hogy az elv alkalmazása joghatósági és anyagi jogi összeütközéseket okoz, továbbá a nemzetközi jog egyes szabályai (pl. diplomáciai mentesség) alkalmazhatatlanná teszik a nemzeti büntetőjogi szabályokat.
A közvetett parancsnoki felelősséget szabályozó Btk. 159. § a) pontjába foglalt tényleges ellenőrzési kritérium helyett – a nemzetközi jog fejlődésével összhangban – az általános ellenőrzést (*overall control*) kellene a büntethetőség feltételévé tenni.
Összességében úgy gondoljuk, hogy a kibertámadások minősülhetnek fegyveres támadásnak, azonban az emberek és sok esetben az állami vezetők is csak abban az esetben veszik ezt tudomásul, ha olyan pusztító eseményhez tudják párosítani gondolatukban, mint a polgári légi jármű eltérítésével megvalósítható fegyveres támadás esetkörében az Amerikai Egyesült Államokat ért 2001. szeptemberi támadás.

## FORRÁSJEGYZÉK

### IRODALOMJEGYZÉK


[1.] BABOS TIBOR: *„Globális közös terek" a NATO-ban,* in. Nemzet és biztonság 2011/3. szám

[2.] BARTKÓ RÓBERT: *A terrorcselekmény, mint nemzetközi bűncselekmény*, in. Rendészeti Szemle. 2010/5. szám

[3.] BELOVICS ERVIN, MOLNÁR GÁBOR MIKLÓS, SINKU PÁL: *Büntetőjog – Különös rész,* Budapest, HVGorac Lap- és Könyvkiadó, 2009

*[4.]* BLAIR, C. DENNIS: *Annal Treat Assessment of the Intelligence Community for the Senate Select Committe on Intelligence. (2009. február 12.)* http://archive.org/stream/AnnualThreatAssessmentOfTheIntelligenceCommunityForTheSenateSelect/20090212_testimony#page/n0/mode/2up (2014.03.30.)

[5.] CRUME, JEFF: *Az internetes biztonság belülről- ...amit a hekkerek titkolnak,* Bicske, Szak Kiadó, 2003

[6.] FORREST, DAVE: *Barát vagy ellenség? – A totális kontroll forgatókönyve,* Budapest, Focus Kiadó, 2005

[7.] GELLÉR BALÁZS JÓZSEF: *Nemzetközi büntetőjog Magyarországon, adalékok egy vitához (egyes jellemzők leírása és diagnózis kísérlet),* Budapest, Tullius Kiadó, 2009

[8.] GYÁNYI SÁNDOR: *Cyber – támadások elleni védekezés és a válaszcsapások lehetőségei*, in. Hadmérnők III. évfolyam 2. szám

[9.] GYÁNYI SÁNDOR: *Robothadviselés 7. Tudományos Szakmai Konferencia*, http://www.zmne.hu/hadmernok/kulonszamok/robothadviseles7/gyanyi_rw7.html (letöltés ideje: 2014.03.26.)

[10.] HAIG ZSOLT – KOVÁCS LÁSZLÓ: *Fenyegetések a cybertérből*, in. Nemzet és biztonság 2008/5. szám

[11.] HAIG ZSOLT – VÁRHEGYI ISTVÁN*: Hadviselés az információs hadszíntéren*, Budapest, Zrínyi Kiadó, 2005

[12.] HERCZEGH GÉZA: *Az erőszakkal való fenyegetésnek és az erőszak alkalmazásának tilalma a mai nemzetközi jogban,* in. Állam és Jogtudomány 1963/3. szám

[13.] KAZÁRI CSABA: *Hacker, cracker, warez. A számítógépes alvilág titkai*, Budapest, Computer Panoráma, 2003

[14.] LATTMANN TAMÁS: *A nemzetközi jog lehetséges szerepe az informatikai hadviselés területén*, in. CSAPÓ ZSUZSANNA (szerk.): *Emlékkötet Herczegh Géza születésének 85. évfordulójára – A ius in bello fejlődése és mai problémái*, Pécs, Kódex Nyomda, 2013

[15.] LEHNARDT, CHIA: *Private Militärfirmen und völkerrechtliche Verantwortlichkeit*, Tübingen, Mohr Siebeck, 2011

[16.] LEWIS, JAMES ANDREW: Incidensek a kibertérben, http://www.biztonsagpolitika.hu/Incidensek_a_kiberterben_biztonsagpolitika.hu.pdf (letöltve: 2014.03.27.)

[17.] LIGETI KATALIN: *Büntetőjog és bűnügyi együttműködés az Európai Unióban*, Budapest, KJK-KERSZÖV Jogi és Üzleti Kiadó, 2004

[18.] MAUNO PIHELGAS: *Back-tracing and anonymity in cyberspace*, in. ZIOLKOWSKI, KATHARINA (SZERK.): *Peacetime Regime for State Activities in Cyberspace International Law, International Relations and Diplomacy*, Tallinn, NATO CCD COE Publication, 2013

[19.] MITNICK, D. KEVIN, SIMON, L. WILLIAM: *A biztonság emberi tényezőinek irányítása, A legendás hacker – A megtévesztés művészete,* Budapest, Perfact – Pro, 2003

[20.] NAGY KÁROLY: *A jóvátétel problémája a nemzetközi jogban*, in. Jogtudományi Közlöny, 1981/ 8. szám

[21.] NAGY KÁROLY: *A vétkesség szerepe a nemzetközi jogi felelősségi jogviszonyban*, in. Jogtudományi Közlöny, 1978/ 10. szám
[22.] NAGY KÁROLY: *Az állam felelőssége a nemzetközi jog megsértése miatt*, Budapest, Akadémiai Kiadó, 1991
[23.] NAGY KÁROLY: *Nemzetközi jog*, Budapest, Püski Kiadó, 1999
[24.] NAGY KÁROLY: *Titok és biztonság az információs társadalomban,* in. Belügyi Szemle 1999/4-5. szám
[25.] ORBÓK ÁKOS: *A kibertér, mint hadszíntér,* in Biztonságpolitika.hu 2013, http://www.biztonsagpolitika.hu/documents/1375084295_Orbok_Akos_A_kiberter_mint_hadszinter-biztonsagpolitika.hu.pdf (letöltve: 2014.03.27.)
[26.] PIRKER, BENEDIKT: *Territorial Sovereiguty and Integrity and the Challenges of Cyberspace*, in. ZIOLKOWSKI , KATHARINA (szerk.): *Peacetime Regime for State Activities in Cybersp ace International Law, International Relations and Diplomacy*, Tallinn, NATO CCD COE Publication, 2013
[27.] POLT PÉTER: *A nemzetközi büntetőjog fejlődésének néhány kérdése,* in. Jogtudományi Közlöny 1987/4. szám
[28.] RAYMOND, ERIC S.: *The new hacker's dictionary*, Cambridge, MIT Press, 1996
[29.] ROSAS, ALAN; STENBACK, PAR: *The Frontiers of International Humanitarian Law* in. Journal of Peace Research 1987/3
[30.] SCHMITT, MICHAEL N.: *Tallinn Manual on International Law applicable to cyber warfare*, Cambridge, Cambridge University Press, 2013
[31.] SCHNEIER, BRUCE: *Schnier a biztonságról*, Budapest, HVG Kiadó, 2010
[32.] SHAW, MALCOLM N.: *Nemzetközi jog*, Budapest, Osiris Kiadó, 2002
[33.] SULYOK GÁBOR: *A terrorcselekmény elkövetéséhez használt polgári légi jármű lelövésének nemzetközi jogi és alkotmányjogi megítélése,* in. Fundamentum 2005/3. szám
[34.] SULYOK GÁBOR: *Az egyéni vagy kollektív önvédelem joga az Észak-Atlanti Szerződés 5. cikkének tükrében,* in. Állam és Jogtudomány 2002/1-2. szám
[35.] SZALAI ANIKÓ: *Az 1979-es iráni forradalom éleslátása*, http://drszalaianiko.hu/2013/11/04/az-1979-es-irani-forradalmarok-eleslatasa/ (letöltve: 2014.04.10.)
[36.] SZALAI ANIKÓ: *Kémkedés: nem tilos, mégsem szabad*, http://drszalaianiko.hu/2013/11/22/kemkedes-nem-tilos-megsem-szabad/ (letöltve: 2014.04.10.)
[37.] WARREN, PETER, STREETER, MICHAEL: *Az internet sötét oldala – Vírusírók, adatrablók, hackerek – és amit tehetünk ellenük,* Budapest, HVG kiadó, 2005
[38.] WIENER A. IMRE: *A büntető joghatóság és gyakorlása, kivált az Európai Unióban,* in. Állam- és Jogtudomány 2002/3-4. szám
[39.] WIENER A. IMRE: *Büntető joghatóság és a nemzetközi jog,* in. Állam- és Jogtudomány 1993/3-4. szám
[40.] WIENER A. IMRE: *Nemzetközi büntetőjog – nemzetközi bűncselekmények*, in. Jogtudományi Közlöny 1986/6. szám
[41.] ZIOLKOWSKI, KATHARINA: *Peacetime Cyber Espionage – New Tendencies in Public International Law*, in ZIOLKOWSKI, KATHARINA (szerk.): *Peacetime Regime for State Activities in Cybersp ace International Law, International Relations and Diplomacy*, Tallinn, NATO CCD COE Publication, 2013

**JOGFORRÁSOK**

[1.] 1949. évi genfi egyezmények közös 2. cikke, Kihirdette: 1954. évi 32. törvényerejű rendelet a háború áldozatainak védelmére vonatkozóan Genfben, az 1949. évi augusztus hó 12. napján kelt nemzetközi egyezményeknek a Magyar Népköztársaságban való törvényerejéről

[2.] 1971. évi egyezmény a bakteriológiai (biológiai) és toxin-fegyverek fejlesztésének, gyártásának és tárolásának eltiltásáról és megsemmisítéséről, Kihirdette: 1975. évi 11. törvényerejű rendelet a bakteriológiai (biológiai) és toxin-fegyverek kifejlesztésének, előállításának és tárolásának megtiltásáról és e fegyverek megsemmisítéséről szóló, az Egyesült Nemzetek Szervezete XXVI. ülésszakán, 1971. december 10-én elfogadott egyezmény kihirdetéséről
[3.] 1977. évi I. kiegészítő jegyzőkönyv a háború áldozatainak védelméről Kihirdette: 1989. évi 20. törvényerejű rendelet a háború áldozatainak védelmére vonatkozóan Genfben, 1949. augusztus 12-én kötött egyezmények I. és II. kiegészítő jegyzőkönyvének kihirdetéséről
[4.] 1993. évi párizsi egyezmény, Kihirdette: 1997. évi CIV. törvény a vegyifegyverek kifejlesztésének, gyártásának, felhalmozásának és használatának tilalmáról, valamint megsemmisítéséről szóló, Párizsban, 1993. január 13-án aláírt egyezmény kihirdetéséről
[5.] 2001. évi CXXI. törvény a Büntető Törvénykönyvről szóló 1978. évi IV. törvény módosításáról
[6.] 2012. évi C. törvény a Büntető Törvénykönyvről
[7.] ENSZ Alapokmány Kihirdette: 1956. évi I. törvény az Egyesült Nemzetek Alapokmánya törvénybe iktatásáról
[8.] Európai Parlament és Tanács 2013/40/EU irányelv az információs rendszerek elleni támadásokról és a 2005/222/IB tanácsi kerethatározat felváltásáról
[9.] Európai Unió Tanácsának 2005/222/IB Kerethatározat az információs rendszerek elleni támadásokról
[10.] Indian IT Act 2008
[11.] Nemzetközi Büntetőbíróság Római Statútuma, magyar nyelvű szöveg: T/4490. számú törvényjavaslat az Egyesült Nemzetek Diplomáciai Konferenciája által, a Nemzetközi Büntetőbíróság Rómában, 1998. július 17-én elfogadott Statútumának kihirdetéséről

**EGYÉB FORRÁSOK**

[1.] Draft Articles on Responsibility of States for Internationally Wrongful Acts, adopted by the International Law Commission at its fifty-third session, 2001
[2.] Case concerning Military and Paramilitary Activities in and against Nicaragua (Nicaragua versus United States of America), Judgement of 27 June 1986, I.C.J. Reports 1986, 64-65
[3.] Legality of the threat or use of nuclear weapons, Advisory opinion of 8 July 1996, I. C. J. Reports 1996
[4.] Prosecutor versus Dusko Tadic, Judgement, Appeals Chamber, Case No. IT-94-1, 15 July 1999