Kelemen Roland, Pataki Márta

A kibertámadások nemzetközi jogi értékelése

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 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.

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

Ezen hálózatok globális térben helyezkednek el, amit kibertérnek nevezünk. E kibertérnek azonban éppen úgy részei a bűnözök, 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 az,hogy az ezeket ért kibertámadás hetekre képes megzavarni az állam működését. A hivatalos becslés 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, ha igen akkor az állam önvédelmi jogosultsága meddig terjed, használhat-e hagyományos fegyvereket

---

[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.

az önvédelem során? Dolgozatunkban e kérdésekre kívánunk válaszokat adni.

1. A kibertámadások elkövetői köre

A számítógépek és az általuk működtetett információs rendszerek a modern társadalom és a modern állam alappilléreivé váltak, ennek következtében 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. Ezek a rendszerek, amelyek számos esetben összefogják, megkönnyítik a hétköznapokat, számtalan kockázatot rejtenek, amelyeket az informatikusok egy speciálisan képzett rétege kíván kihasználni. A veszély valódiságát mutatja, hogy „becslések szerint egy-egy érdekesebb szervert naponta 100-150 hacker próbál feltörni…”[5]

A szakemberek első csoportját a *hackerek* jelentik. „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.”[6] 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 határozható meg egy általános hacker definíció. Tudásuk erősorrendjében a

[5] Forrest, Dave: *Barát vagy ellenség? – A totális kontroll forgatókönyve,* Budapest, Focus Kiadó, 2005, 202. o.
[6] Kazári Csaba: i.m. (2003), 18. o.

hackereket a következőképpen rangsorolhatjuk: *(1) valódi hacker (2) dark-hacker, (3) light-hacker, (4) wannabe-hacker, (5) drifterek, (6) trollok.*[7] A következőkben ezen sorrendben kívánjuk bemutatni az egyes típusokat.

A (1) valódi hacker: „olyan kimagasló számítástechnikai tudással bíró személy, aki szigorúan segítő jelleggel… feltárja a számítógépes rendszerek/ alkalmazások előnyeit és hibáit, illetőleg javít azokon."[8] 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 a kormányhivataloknál.

A (2) *dark-hacker* a számítástechnikai tudása jelentős, de őt a nyereségvágy vagy éppen a bosszú motiválja, tevékenységét valamilyen ártó szándék vezeti. Az internetes vírusok legtöbbje e kategória képviselőitől származik. A dark-hacker szakértelme és szándéka is megvan a kiberbűncselekmények elkövetéséhez.

A (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[9] követnek el. A hacker társadalom e csoportot script-kiddienek nevezte el.

A (4) *wannabe-hacker* még nem valódi hacker, de arra törekszik, hogy azzá váljon. Tudásuk jóval elmarad az előzőekéhez,

---

[7] 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.

[8] Kazári Csaba: i.m. (2003), 18. o.

[9] 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 Csaba*: i.m. (2003) 154.o.

ebből kifolyólag más hackerek által kitalált úgynevezett hack-programokkal, és exploitokkal[10] munkálkodnak.

A (5) *drifterek* általában csak valamilyen információt vagy adatot keresnek az adott egyén gépén, tevékenységük kiterjed a személyes adatokra, üzleti titkokra stb., 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.

A (6) *trollok* „előképzettség nélkül gyakorlatilag céltalanul ténferegnek a világhálón, és tönkretesznek minden elébük kerülő és támadható dolgot a neten."[11] 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 *crack*ereket 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,"[12] 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."[13] A cracker fogalmának „… elsődleges jelentése szerint olyan kárt okozó személy, aki számítógépes rendszereket rongál, illetve adatokat tulajdonít el, vagy bármilyen egyéb módon kárt okoz."[14] A cracker a saját gépén lévő anyaggal dolgozik, munkássága népszerű, mivel tevékenykedéseinek eredményei az olcsó kalózmásolatok. A crackerek mindig ártó szándékkal törnek fel egy adott rendszert, szoftvert. „Másodlagos jelentése szerint… a cracker olyan valaki, aki megváltoztatja a kereskedelmi forgalomban lévő

---

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

11 Forrest, Dave: i.m. (2005), 205. o.

12 Forrest, Dave: i.m. (2005), 206. o.

13 Raymond, Eric S.: *The new hacker's dictionary*, Cambridge, MIT Press, 1996, 22. o.

14 Kazári Csaba: i.m. (2003), 19. o.

szoftverek kódját (ez már önmagában illegális tevékenység) annak érdekében, hogy a szóban forgó szoftver szabadon másolható, használható és terjeszthető legyen."[15]

Kiberbűnözőnek tekintendők a *phreaker*ek[16] is. 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."[17] Magyarországon ez a tevékenység még kialakulóban van.

A dark-hacherek mellett, ma a legnagyobb veszélyt a homogén csoportot alkotó HPAV-k jelentik (mozaikszó a Hacking, Phreaking, Anarchy, Virus szavakból áll össze). „A HPAV csapatok a létező legkártékonyabbak – vírusokat írnak, állami szervek munkáját teszik tönkre, magánszámítógépekbe törnek be, mindezt csak azért, hogy másoknak gondot okozzanak."[18] Ilyen jellegű csoportosulások létezéséről 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."[19] Egy HPAV tevékenykedése során bármely információs rendszer elleni bűncselekményt képes elkövetni. Sőt olykor még a terrorcselekmények elkövetésétől sem riadnak vissza.

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

15 Kazári Csaba: i.m. (2003), 19. o.
16 A „phonephreaker" kifejezésből ered.
17 Kazári Csaba: i.m. (2003), 20. o.
18 Kazári Csaba: i.m. (2003), 21. o.
19 Kazári Csaba: i.m. (2003), 21. o.

rendszerek válnak célpontjává, hogyan indul, mekkora lesz a veszteség, minden bizonnyal képesek lennénk megelőzni."[20] 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."[21]

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

A módszerek első csoportját azok képezik, amelyeknek célja az információs rendszer adatainak megszerzése, ezek pedig a következőek: (1) Ethernet- és Token Ring helyi hálózat elleni támadás; (2) jelszavak feltörése.

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."[22] 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

[20] Crume, Jeff: *Az internetes biztonság belülről- ...amit a hekkerek titkolnak,* Bicske, Szak Kiadó, 2003, 74. o.
[21] Haig Zsolt – Várhegyi István*: Hadviselés az információs hadszíntéren*, Budapest, Zrínyi Kiadó, 2005, 131. o.
[22] Crume, Jeff: i.m. (2003), 138. o.

technikát alkalmazza a Token Ring vezérjelgyűrűs hálózat is. Mindkét technológia esetén a hacker[23] 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. 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."[24]

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 csomagot, a kiszolgálóra történő belépési információt tartalmazó csomagokról másolatot készít, a többit pedig törli."[25] 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

[23] E fejezetben összefoglalóan a hacker fogalma alatt a valódi hackert, dark-hackert és HPAV-t kell érteni.

[24] Crume, Jeff: i.m. (2003), 142. o.

[25] Crume, Jeff: i.m. (2003), 140. o.

információszerzés érdekében kihasználni."[26] A social engineer (azaz a hacker) tehát, miután megszerezte a legfontosabb személyes adatokat azokat feltölti egy kódfeltörő programba, amely könnyedén megszerezheti titkos jelszavakat. Az úgynevezett Dictionary Hack eljárás azon alapul, hogy értelmes szavak variációit próbálgatja a kódfeltörés közben, amennyiben nem értelmes szó a jelszó, a hacker csak a Brute Force eljárással[27] járhat sikerrel.

2.2 Információs rendszert zavaró eszközök

A támadási módszerek következő csoportját képezik az információs rendszerek megzavarására irányuló eszközök (puffertúlcsordításos támadás, levélbomba támadás).

A puffertúlcsordításos támadás 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."[28] Ezeket a támadásokat könnyű észrevenni és nem is nehéz védekezni ellenük, csak egy biztonsági frissítésre van szükségünk.

E kategóriába sorolható a levélbomba támadás, mely során a támadó e-mail-ek sokasságát 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.

---

[26] Mitnick D. Kevin, Simon L. William: *A biztonság emberi tényezőinek irányítása, A legendás hacker – A megtévesztés művészete,* Budapest, Perfact – Pro, 2003, 1. o.

[27] 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.

[28] Crume, Jeff: i.m. (2003), 153. o.

2.3 Információs rendszert módosító, romboló és megsemmisítő eszközök

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…”[29], 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 kötött számítógépet) használva fegyverül. A támadó célja a célpont erőforrásainak lefoglalása.”[30] 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 kétféleképpen keletkezhetnek, az egyik, hogy egy automatizált eszköz kutatja fel és kapcsolja be az úgynevezett zombihálózatokba (más néven boot hálozatok) a sebezhető

[29] Crume, Jeff: i.m. (2003), 174. o.

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

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.”[31] 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 kibercselekmény 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

[31] Gyányi Sándor: *Cyber – támadások elleni védekezés és a válaszcsapások lehetőségei*, In. *Hadmérnők* III. évfolyam 2. szám, 116. o.

számítógép indításakor betölti az operációs rendszert."[32] 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."[33] 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 – pedig valójában a velejéig romlott."[34] 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."[35] Egy gyorsan ható féreg jelentős kárt tud okozni az információs rendszerben, melynek hatása igen pusztító lehet.

---

[32] Crume, Jeff: i.m. (2003), 188. o.

[33] Warren Peter, Streeter Michael: *Az internet sötét oldala – Vírusírók, adatrablók, hackerek – és amit tehetünk ellenük,* Budapest, HVG kiadó, 2005, 137. o.

[34] Crume, Jeff: i.m. (2003), 189. o.

[35] Crume, Jeff: i.m. (2003), 189. o.

E fejezet végén rögzítenünk kell, hogy az ismertetett eszközök listája nem taxatív, egyfelől annak okán sem lehet az, mert az 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.

3. A kibertámadás minősülhet-e fegyveres támadásnak?

A vesztfáliai békét követően kialakult az ún. vesztfáliai világrendben az állam szuverenitásának egyik attribútuma, a háború indításának a joga, azonban a korszak utolsó szakaszában már korlátozni kívánták e jogosultságot (lásd. Drago-Porter egyezmény, 1907), majd további korlátozást jelentett, jelenthetett volna a Nemzetek Szövetségének életre hívása vagy a Briand-Kellogg paktum (1928) megkötése, azonban általános jelleggel csak 1945-ben az ENSZ megalakulásával, az Alapokmány elfogadásával deklarálták – először az emberiség történelme során – *a fegyveres erőszak tilalmát*.

3.1 Erőszak általános tilalma, agresszió és fegyveres támadás a nemzetközi jogban

Az erőszaknak az általános tiltásával akarták elérni az államok a teljes és átfogó államközi erőszaktilalmat, amely nem csak a háborúra, hanem minden olyan cselekményre kiterjed, amely más állam területi épsége, vagy politikai függetlensége ellen irányul vagy az Egyesült Nemzetek céljaival össze nem férő bármely módon megnyilvánuló erőszak vagy azzal való fenyegetés formájában jelenik meg.[36] A fogalom meghatározásából következik, hogy az Alapokmány minden fegyveres erőszakot tilt, függetlenül annak súlyától, intenzitásától és az alkalmazott fegyver jellegétől.

[36] ENSZ Alapokmány, 2. cikk (4) bekezdés. Kihirdette: 1956. évi I. törvény az Egyesült Nemzetek Alapokmánya törvénybe iktatásáról.

Az általános erőszak tilalma alól csupán két kivétel van: a fegyveres erő Biztonsági Tanács felhatalmazásán alapuló alkalmazása és az egyéni és kollektív önvédelem jogának gyakorlása. A kollektív biztonság rendszerében a Biztonsági Tanács (továbbiakban BT) ezen kötelező határozatai prioritást élveznek az önvédelem jogával, annak gyakorlásával szemben. A BT-nek felhatalmazást biztosító 39. cikk ezen túl bevezeti a *támadó cselekmény (agresszió)* fogalmát, azonban e fogalmat az Alapokmány nem határozza meg, ezzel pedig felveti a kérdést, hogy minden az általános erőszak tilalmat megszegő cselekményt, támadó cselekményként kell-e értelmezni. A szöveg vizsgálatából viszont jól kitűnik, hogy ezen támadó cselekményeken a békét veszélyeztető vagy megszegő cselekmények melletti egyéb cselekmények értendők,[37] amelyet a nemzetközi közösség az agresszió fogalmával azonosítja.

A cselekmény *agresszióként* való azonosítására a BT jogosult, így az, erősen politikai kérdésnek, politikai döntésnek minősül, amelynek széles mozgásteret biztosít az Alapokmány. E nehezen megfogható fogalmi kört próbálja konkretizálni az ENSZ Közgyűlés 1974-ben elfogadott 3314. számú határozata, amely ajánlásként a jövőbeni jogalkotás irányát kívánja meghatározni. A határozat ekként definiálja az agresszió fogalmát: „fegyveres erő alkalmazása egy állam által más állam szuverenitása, területi integritása vagy politikai függetlensége ellen, illetve az Egyesült Nemzetek Alapokmányával össze nem férő bármely más módon."[38] A határozat exemplifikatív felsorolást tartalmaz a lehetséges agressziós cselekményekről, azonban ezt követően megjegyzi, hogy e felsorolás nem kimerítő és a BT más cselekményt is azzá minősíthet. Mindettől eltérően az jól látható, hogy az agresszió és a fegyveres erőszak rész egész viszonyban állnak, vagyis az agresszió a fegyveres erőszak részhalmaza. A határozat jelentősége, hogy jelzi annak tényét, hogy a

[37] ENSZ Alapokmány, 39. cikk. Kihirdette: 1956. évi I. törvény az Egyesült Nemzetek Alapokmánya törvénybe iktatásáról.

[38] ENSZ Közgyűlésének 3314.(XXIX) számú határozata. Az agresszió meghatározása 1. cikk.

nemzetközi jogban relevanciával bír a fegyveres erőszak intenzitása, továbbá azt, hogy fegyveres erőszakot közvetett módon is el lehet követni, valamint megerősíti az erőszak (itt az agresszió) államközi jellegét.

Az általános erőszak tilalom ius cogens szabálya alóli másik kivétel az *önvédelem joga*, amellyel kapcsolatban az Alapokmány úgy rendelkezik, 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."[39] Az önvédelemi jog gyakorlásának alapvető feltétele a fegyveres támadás, amelynek fogalmát azonban sem az Alapokmány sem a későbbi dokumentumok nem definiálják, ennek okán egy cselekmény ekként minősítése a gyakorlatban „… módfelett szubjektív döntésen alapul: ugyanaz a tény, ugyanazon jog alapján, eltérő minősítésekkel illethető."[40] 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 e nélkül 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 az egyetlen kivétel az Alapokmányban, amely esetén az államoknak vagy közösségeiknek lehetőségük van fegyveres erőszak alkalmazására. „Mivel azonban az alapokmány mellőzi a fegyveres támadás kifejezés definiálását, semmi nem zárja

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

[40] 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.

ki az önvédelem analógia útján való alkalmazásának lehetőségét." [41] *A fegyveres támadásnak azonban két feltételnek is meg kell felelnie: (1) a cselekménynek el kell érnie egy rendkívüli súlyt vagy intenzitást; valamint (2) a támadást elkövető személyek cselekménye valamely másik államnak betudhatónak kell lennie.*

Az első kritérium szerinti eltérés fogalmi szinten megjelenik az Alapokmányban, ugyanis míg a 2. cikk (4) bekezdése erőszak alkalmazásáról beszél, addig az 51. cikk fegyveres támadást rögzíti, ekként értelmezve utóbbi fogalom az első minősített esetének tekintendő, vagyis a fegyveres erőszak és a fegyveres támadás rész egész viszonyban állnak egymással, tehát – az agresszióhoz hasonló módon – a fegyveres támadás részhalmaza az erőszaknak (sőt ezen belül még az agressziónak is részhalmaza). Ezen értelmezés következik az Alapokmány szellemiségéből is, ugyanis, ha a két fogalom jelentése azonos volna, ebben az esetben bármilyen erőszak alkalmazása lehetővé tenné az önvédelem alkalmazását, így egy-egy kisebb súlyú, intenzitású cselekmény is könnyen eszkalálódhatna, míg ha megszorítanánk az erőszakká minősítést, ebben az esetben megszűnne az erőszak általános tilalma. Ennek okán a megfelelő értelmezés az, hogy minden államközi erőszakos cselekmény sérti az erőszak tilalmának ius cogens szabályát, de ezek közül csak a jelentősebb súlyú és intenzitású cselekmények – fegyveres támadások – azok, amelyek esetén lehetőség van az önvédelem jogszerű gyakorlására, a többi esetet békés úton kell rendezni, amely jelentheti akár a BT vagy Nemzetközi Bíróság előtti eljárást is.

A fegyveres erőszak szintjének meghatározása roppant nehéz kérdés, röviden megfogalmazva a probléma úgy is megfogalmazható, hogy mi az a szint, amely esetében már fegyveres támadásról beszélhetünk. A legegyszerűbben az agresszió fogalmából lehet kiindulni, hiszen – mint az korábban megállapításra került – mindkettő az erőszak egyik részhalmazát jelenti. A Nemzetközi Bíróság kimondta, hogy a fegyveres támadás az erőszak

[41] Sulyok Gábor: *A terrorcselekmény elkövetéséhez használt polgári légi jármű lelövésének nemzetközi jogi és alkotmányjogi megítélése,* In. *Fundamentum* 2005/3. szám, 34. o.

legsúlyosabb esete.[42] „Ennek következtében az agresszió legsúlyosabb esetei minősülnek „csak" fegyveres támadásnak."[43] Tehát e fogalmak is rész egész viszonyban állnak egymással.

A fegyveres támadás másik ismertető jegye, hogy a támadásnak minden esetben betudhatónak kell lennie egy másik államnak. Fegyveres támadást tehát csak állam tud elkövetni. Nyilvánvaló tény, ha egy állam reguláris csapatai követnek el meghatározott intenzitású támadást ebben az esetben az fegyveres támadásnak minősül. Kérdéses viszont magánszemélyek vagy csoportjaik által megvalósított támadás betudható-e az államnak, és ha igen, akkor milyen szintű kapcsolatnak kell fennállnia. A fentebb már említett 3314. számú közgyűlési határozat rögzítette, hogy irreguláris csapatok tevékenysége is tekinthető államok közötti agressziónak,[44] ezt erősítette meg a Nemzetközi Bíróság, amely szerint ennek határozatba foglalása a nemzetközi szokásjogot tükrözi, ennek okán irreguláris egységek tevékenysége is betudható az államnak.[45] Kérdéses viszont a kapcsolatnak milyen szintűnek kell lennie ahhoz, hogy az betudható legyen az államnak. Elfogadott nézet, hogy a magánszemélyek és csoportjaik cselekményei kizárólag akkor tudhatók be egy államnak, ha azok állam utasítása, irányítása vagy ellenőrzése alatt tevékenykednek. Az ellenőrzés mértéke azonban szintén nincs meghatározva. A Nemzetközi Bíróság Nicaragua-ügyben hozott ítéletében még a tényleges ellenőrzést (effective control) tette szükségessé,[46] míg a volt Jugoszlávia

---

[42] 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. 191.

[43] Kajtár Gábor: *A terrorizmus elleni önvédelem a XXI. században,* In. *Kül-Világ – a nemzetközi kapcsolatok folyóirata* 2011/1-2. szám, 10. o.

[44] ENSZ Közgyűlésének 3314.(XXIX) számú határozata. Az agresszió meghatározása 3. cikk g) pont.

[45] Kajtár Gábor: i.m. (2011), 12. o.

[46] 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.

területén történt humanitárius jogot sértő cselekmények feltárására felállított nemzetközi törvényszék szerint már elegendő az állam általános ellenőrzése (overall control) is.[47] A Bosznia és Hercegovina és Szerbia és Montenegró ügyben a Nemzetközi Bíróság, azonban ismételten megerősítette a tényleges ellenőrzés elvét, azzal kiegészítve, hogy az általános ellenőrzés, mint kritérium alkalmazása jelentősen kiszélesíteni az önvédelmi jogosultságot és ezáltal ellentétes lenne, annak eredeti rendeltetésével.[48] 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."[49]

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-alkotásra e cselekmények után sem került sor, azonban általánosan elfogadott tény lett, hogy fegyveres támadásnak nem csak hagyományos fegyverrel elkövetett cselekmény tekinthető.

3.2 A kibertámadások értékelése a fegyveres támadás fogalmi elemei alapján

A hadviselés átalakulásával megjelentek olyan új eszközök, hadviselési módszerek, amelyek alapvető rendeltetésük szerint nem értelmezhetőek fegyverként, azonban több gyakorlati példa mutatja (Észtország esete 2007, Stuxnet 2010), hogy alkalmasak lehetnek

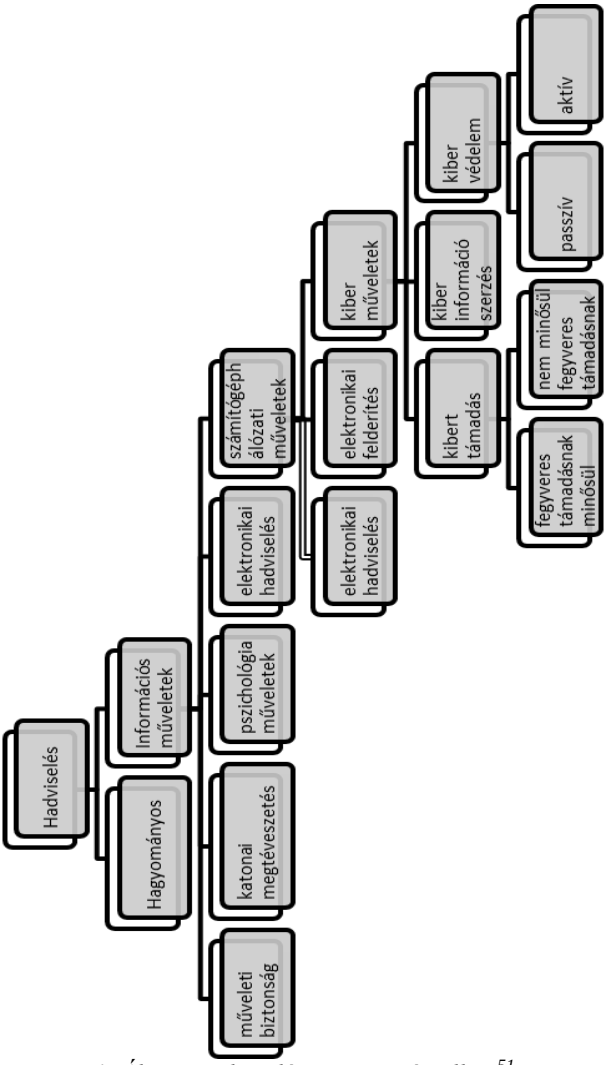
[47] Prosecutor versus Dusko Tadic, Judgement, Appeals Chamber, Case No. IT-94-1, 15 July 1999, para. 145.

[48] Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro) Summary of the Judgment of 26 February 2007, para 406.

[49] Sulyok Gábor: i.m. (2005), 35. o.

arra, hogy fegyverként alkalmazzák ezeket az eszközöket, ennek okán pedig, hasonlóan a polgári légi járművek esetkörére szükséges nemzetközi jogi értékelésük. Ilyen eszközöket alkalmaznak az egyes hadseregek információs műveleteik során. Az információs műveletek célja „az ellenség vagy a potenciális szemben álló fél döntéshozatali folyamatának befolyásolása, megzavarása, lerontása vagy korlátozása, illetve a saját döntéshozatali folyamat védelme."[50] Ezen információs műveletek egyik eleme a számítógépes-hálózati műveletek, melynek részét képezik a témánk szerinti kiberműveletek is.

[50] Haig Zsolt, Kovács László, Ványa László, Vass Sándor: *Elektronikus hadviselés*, Budapest, Nemzeti Közszolgálati és Tankönyv Kiadó Zrt., 2014, 19. o.



1. Ábra: Hadviselés a XXI. században[51]

[51] Haig Zsolt, Kovács László, Ványa László, Vass Sándor: i.m. (2014) felhasználása alapján szerkesztették a szerzők.

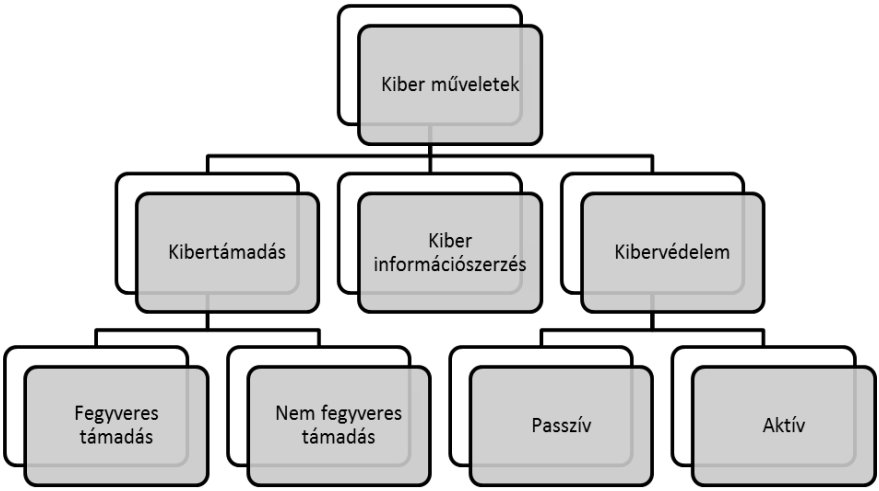
Az internet elterjedésének köszönhetően „a globális számítógépes hálózatokban végbemenő kölcsönhatások révén megszületett a kibertér (cyberspace) a kibernetikus világegyetem."[52] E kibertér rendkívül egyedi és összetett, hiszen nem csak fizikai és földrajzi fogalmakkal jellemezhető, hanem virtuális jellemzői is rendkívüli relevanciával bírnak jellemzése során. Az Egyesült Államok Védelmi Minisztériuma meghatározta a kibertér katonai fogalmát: „informatikai (információs) környezetben értelmezett globális tartomány (domain), amely magába foglalja az IT infrastruktúrák egymással összefüggő elemeinek hálózatát, beleértve az internetet, a telekommunikációs hálózatokat, számítógépes rendszereket, valamint a beágyazott feldolgozó és vezérlő elemeket."[53] E kibertéren keresztül milliós nagyságú információ áradat halad át egyetlen perc leforgása alatt. „Egyértelműen prognosztizálható: a kibertér rendszerei egyre nagyobbá, gyorsabbá és komplexebbé vállnak,"[54] 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

[52] Nagy Károly: *Titok és biztonság az információs társadalomban,* in. *Belügyi Szemle* 1999/4-5. szám, 173. o.

[53] Joint Publication 1-02 Department of Defense Dictionary of Military and Associated Terms, 77. o.

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

között."[55] A kibertérben végrehajtható műveletek összetettségét kellőképpen mutatja a Magyar Honvédség Kibervédelmi koncepciójában található kiberművelet fogalom: „a kibertérben végzett elektronikus adatkezelés és az adatkezelő képességek működésével kapcsolatos tevékenységek, illetve a tágan értelmezve az ezek védelmére és befolyásolására irányuló tevékenységek, folyamatok."[56] Ezek alapján három terület különíthető el: (1) kiber információ-szerzés; (2) kibertámadás; (3) kibervédelem.



2. ábra: A kiberműveletek tipológiája (a szerzők saját szerkesztése)

A *kiber információszerzés*, amelynek célja adatbázisban tárolt adat vagy információ megszerzése nem minősíthető fegyveres támadásnak. Ezt támasztja alá a Tallinn Manual elnevezésű NATO

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

[56] A honvédelmi miniszter 60/2013. (IX. 30.) HM utasítása a Magyar Honvédség Kibervédelmi Szakmai Koncepciójának kiadásáról, 1. melléklet, 2. pont 6).

szakértők által elkészített kézikönyv (szakértői vélemény) is, mely szerint a hír- és adatszerző tevékenységek nem minősíthetőek fegyveres támadásnak.[57] Katharina Ziolkowski véleménye szerint „a kémkedés önmagában nem ellenkezik a nemzetközi joggal, és ezért nem is nemzetközi jogot sértő cselekmény."[58] 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"[59] 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."[60] 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 a büntető igényét érvényesítheti az állam.

---

57 Schmitt, Michael N.: *Tallinn Manual on International Law applicable to cyber warfare*, Cambridge, Cambridge University Press, 2013, 55. o.

58 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.

59 Szalai Anikó: *Kémkedés: nem tilos, mégsem szabad*, http://drszalaianiko.hu/2013/11/22/kemkedes-nem-tilos-megsem-szabad/ (letöltve: 2014.04.10.).

60 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 *kibervédelem* esetköre szintén nem tartozik a fegyveres támadás fogalmi körébe, azt témánk szerint az önvédelemről szóló fejezetben fejtjük ki.

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 a támadásnak… precíz támadásokat csak államok vagy nagyon erős bűnözői csoportok indíthatnak."[61] 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?

A *kibertámadás ténye önmagában nem feltétlenül elegendő ahhoz, hogy egy államot önvédelmi helyzetbe hozzon, ugyanis a támadás* intenzitása az egyik döntő tényező. Mint korábban is jeleztük nincs elfogadott fogalma a fegyveres támadásnak, azonban egyetérthetünk azzal a felfogással, mely szerint azokat a támadásokat, amelyek nagyszámú ember életét veszélyeztetik vagy kioltják, illetve az infrastruktúrában jelentős károkat okoznak, fegyveres támadásnak lehet tekinteni.[62]

Tehát az olyan kibertámadást, amelynek eredménye eléri ezt a súlyos hatást vagy intenzitást fegyveres támadásnak kell tekinteni. Ilyen eredményű támadás lehet a kibertérben az atomerőművek, atomreaktorok elleni támadás, amelyre több példa is volt az elmúlt években: a Blaster-féreg 2003-ban és Stuxnet-vírus 2010-ben.

---

[61] 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.)

[62] Tallin Manual (2013), 55. o.

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."[63] 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."[64]

Kevésbé ismert az a 2012-es eset,[65] 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

---

63 Schneier, Bruce: *Schnier a biztonságról*, Budapest, HVG Kiadó, 2010, 144. o.

64 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.

65 Lewis, James Andrew: Incidensek a kibertérben, 17. o. http://www.biztonsagpolitika.hu/Incidensek_a_kiberterben_biztonsagpolitika.hu.pdf (letöltve: 2014.03.27.)

esetek mindegyikében amennyiben pusztítás lett volna az elsődleges cél az meg is valósult volna. Egy atomerőmű elpusztításával járó kibertámadást nyilván az államok mindegyike fegyveres támadásnak minősítene, a támadás következménye akár azonos is lehet a nukleáris fegyverekével (gondoljunk itt a sugárszennyezésre). Ilyen támadás végrehajtásának eszköze lehet az előző fejezetben ismertetett back orifice, a vírusok, a trójai falovak és számítógépférgek.

A Nemzetközi Bíróság 1996. július 8-án az ENSZ Közgyűlésének kérésére tanácsadó véleményében kifejtette, hogy ha 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.[66] Így tehát analógiával élve, az a kibertámadás, amelynek célja és eredménye valamely más állam atomerőművének megsemmisítése, az sérti az Alapokmányban rögzített erőszak tilalmának szabályát, és a nemzetközi jogot súlyosan sértő 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 minősítené, de a támadás következményei már átléphetik azt a határt, hogy az eredeti támadás annak minősüljön. 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.[67] Egy ilyen típusú támadás akár több tízezer

---

66 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.

67 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*

polgári személy halálát is eredményezheti, sőt a hálózat méretétől függően milliós nagyságú áldozatokkal is járhat.[68] 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,[69] ezért ennek okán az ilyen támadás fegyveres támadásnak minősíthető akár csekély számú áldozat esetén is.

Kiemelendő, hogy a Tallini Kézikönyv összeállítói szerint a kibertámadásokat a radioaktív, a biológia és a vegyi fegyverek alkalmazásához kell hasonlítani,[70] vagyis a szerzők elsősorban analógia útján látják alkalmazhatónak a nemzetközi jog már létező szabályait.

Eltérően az eddigi esetköröktől akár fegyveres támadásnak minősíthető egy tisztán kibertérben elkövetett olyan támadás is, amely egy állam kommunikációs hálózatát bénítja meg, ehhez azonban természetesen szintén szükséges a kellő intenzitás. Az Egyesült Államok által szimulált ilyen típusú támadás eredményeként, „a megtámadott ország vezetési rendszere és az

---

Relations and Diplomacy, Tallinn, NATO CCD COE Publication, 2013, 56. o.

[68] E körben említhető más kritikus infrastruktúra is, mint például a földgáz hálózat.

[69] 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 vegyi fegyverek kifejlesztésének, gyártásának, felhalmozásának és használatának tilalmáról, valamint megsemmisítéséről szóló, Párizsban, 1993. január 13-án aláírt egyezmény kihirdetéséről (184 része állam).

[70] Tallin Manual (2013), 54. o.

ország működőképessége kettő-négy nap alatt összeomlott,"[71] amely közrend felbomlását eredményezte. A megtámadott ország anarchiába süllyedt, a szociális hálózata pedig összeomlott. Az 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."[72] A Magyar Honvédség Kibervédelmi szakmai koncepciója szerint egy ilyen típusú támadás, lehetséges negatív hatásai lehetnek, hogy a katonai infrastruktúra esetében a Honvédség vezérkara a vezetési és irányítási képességét elveszíti, a közigazgatási feladatok ellátása akadozik vagy teljesen ellehetetlenedik, továbbá MH Kormányzati Célú Elkülönült Hírközlő Hálózat rendelkezésre állása és szolgáltatásainak hatékonysága csökken vagy teljesen megszűnik.[73]

Hasonló támadás érte 2007-ben Észtországot, valamint Grúziát 2008-ban, amely támadások még nem voltak kellően intenzívek és hosszan tartóak a fenti eredmény eléréséhez, azonban előre jelezték az ilyen típusú támadások szisztémáját, vagyis a kormányzati szervek megbénításával egyidejűleg, a bankhálózat, a rendőrségi, katonai 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.

Az eddig felvázoltak szerint jól látható, hogy egyes kibertámadások intenzitásuk alapján minősülhetnek fegyveres támadásnak, azonban ehhez szükséges megvizsgálni a kritérium másik körét a betudhatóságot. Kibertámadások esetében sem vett fel

---

71 Haig Zsolt – Kovács László: *Fenyegetések a cybertérből*, in. *Nemzet és biztonság* 2008/5. szám, 67. o.

72 Lattmann Tamás: i. m. (2013), 212. o.

73 A honvédelmi miniszter 60/2013. (IX. 30.) HM utasítása a Magyar Honvédség Kibervédelmi Szakmai Koncepciójának kiadásáról, 4.2. pont.

kérdést az, ha az állam szerve (ma már több állam rendelkezik a hadseregben elkülönült kiberhadtestekkel) követi el a támadást, amennyiben eléri a szükséges intenzitást egyértelműen fegyveres támadásról beszélhetünk. Szükséges azonban megvizsgálni, azt az esetkört is, ha magánszemélyek vagy azok csoportjai valósítanak meg támadásokat. A fentebb bemutatott szabályok, vagyis az irányítás, utasítás, ellenőrzés hármasa közül bármelyik fennállása az államnak való betudhatóságot eredményezné. Az ellenőrzés körében kizárólag a tényleges ellenőrzést (effective control) tudjuk elképzelni a kibertámadások esetében, mivel az általános ellenőrzés elméletének alkalmazása egyfelől rendkívül kiszélesítené a betudhatóság körét, azontúl pedig nyilvánvalóan az internet szabadságának (amely több államban így például Finnországban, Észtországban is alkotmányos alapjognak számít) korlátozását és jóval szigorúbb állami ellenőrzését eredményezné. Szükséges azonban megvizsgálni milyen esetkörök tartozhatnak a tényleges ellenőrzés alkalmazási körébe. Mivel ezen kérdéskörben nincs nemzetközi gyakorlat ezért ismételten szükséges analógiával élni és megvizsgálni a terrorszervezetekre vonatkozó gyakorlatot. Kardos Gábor véleménye szerint a terrorszervezetek esetében fennáll a tényleges ellenőrzés, amennyiben az állam erőforrásokat biztosít, kiképzőbázisokat megtűr vagy ilyen szervezet tagjainak menedéket nyújt.[74] Véleményünk szerint ezen kritériumok alkalmazhatóak kibertámadás elkövetőivel vagy azok csoportjaival szemben is, azzal a kiegészítéssel, hogy a toborzás lehetőségének biztosítása is betudhatóságot eredményezne.

Kérdéses viszont azon esetkör, amikor az állam a tevékenységről „csak" tudott, de az ellen nem tett vagy nem képes semmit tenni, hasonló esettel kapcsolatban állapította meg Lattman Tamás és Nagy Boldizsár, hogy „a célba vett állam erőszakkal is felléphet, ha sem a területi állam nem képes a területéről támadókat ellenőrzése alá vonni, sem a nemzetközi közösség (BT kényszerintézkedések formájában) nem lép fel. Jogos a védelem

[74] Kardos Gábor: *Vannak-e jogai a terroristáknak?* In. Tálas Péter: *Válaszok a terrorizmusra II. A politikai marketing csapdájában*, Budapest, Mágustudió, Budapest, 2006, 89. o.

tehát, ha arányos és megvalósítása a hadviselés szabályaival összhangban van."[75] Ezen esetkör is betudhatóvá teszi a kibertámadást. Ezt erősíti, hogy „az államok jelenkori gyakorlata szerint, az erőszak alkalmazására vonatkozó szabályok és az önvédelem joga párhuzamosan fejlődik, hogy megakadályozza az erőszak alkalmazásával felmerülő veszélyeket."[76] Ennek okán az önvédelem jogának gyakorlása során szükséges, hogy figyelembe vegyük a nemzetközi jog által kimunkált feltétlenül alkalmazandó normáit, különösen a humanitárius jog nemzetközi szabályait. Így a fegyveres támadás nemcsak az önvédelem jogát, hanem a humanitárius jog alkalmazását is szükségessé teszi, továbbá megállapítható, hogy „a sic utere tuo" elvből eredően az államok kötelezettsége, hogy megakadályozzák a rosszindulatú számítógépes tevékenységeket, amelyek károsíthatják az államok jogait."[77] Ezen esetkörben azonban nyomatékosan szükséges leszögezni, hogy a betudhatóságot csak és kizárólag az eset összes körülményeinek mérlegelése alapján lehet megállapítani.

4. Önvédelem a kibertámadások körében

A kibertámadások azon esetkörében, ahol e támadás fegyveres támadásnak minősíthető, szintén érvényesül a nemzetközi szokásjog részét képező és a Webster-doktrínából eredeztethető az önvédelem jogának gyakorlásával szemben megkövetelt két elv, az arányosság és a szükségesség. A szükségesség követelménye azt jelenti, hogy az

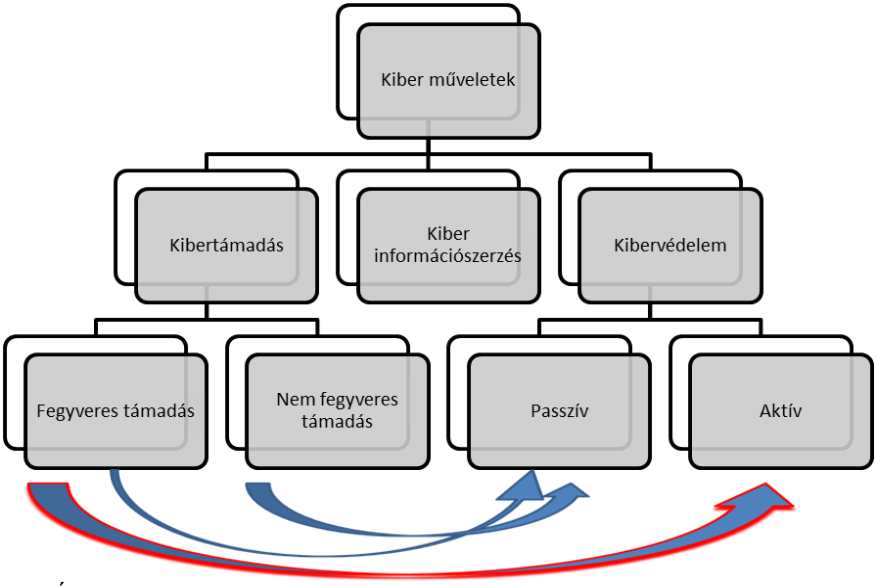
---

[75] Lattman Tamás, Nagy Boldizsár: *Támadható-e Bejrút vagy Tel-Aviv?* In. *Élet és Irodalom* 2006/33. szám, 2. o.

[76] Newland, Zachary: *Collusion and Confusion: Evaluating the right of self-defense against private actors*, http://www2.okcu.edu/english/stellar2009.pdf, letöltés ideje: (2014.04.02.)

[77] Ziolkowski, Katharina: *General principles of International Law as Applicable 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, 185. o.

önvédelmi jog gyakorlása kizárólag a támadás elhárítására és visszaverésére irányulhat, „vagyis a fegyveres erőszak alkalmazása nem lehet megtorló, büntető, vagy jövőbeli esetleges újabb támadásokat általánosan megelőző jellegű. Ezek a fegyveres erőszak jogtalan alkalmazásával járó önsegélynek, vagy szintén jogellenes fegyveres represszáliának minősülnek.”[78] Az arányosság követelménye azt jelenti, hogy az önvédelem jogával élve alkalmazott erőszaknak minden esetben igazodnia kell a fegyveres támadás mértékéhez.



3. Ábra: Arányosság a kiberműveletekben (a szerzők saját szerkesztése)

E két zsinórmérték határozza meg az önvédelem során alkalmazható eszközök körét és azok alkalmazásának intenzitását. Mint azt az ábra mutatja a kibervédelemnek vannak passzív (tűzfal, vírusirtó, adaptív válaszlépés stb.) és aktív (megelőző támadás, ellentámadás, aktív megtévesztés) eszközei. Nyilvánvaló, hogy a

78 Kajtár Gábor: i.m. (2011), 14. o.

passzív eszközök minden – így fegyveres támadásnak nem minősülő – kibertámadások esetén is alkalmazhatóak. Szintén minden esetben alkalmazhatóak minden támadás esetén a nem fegyveres represszália eszközei. Aktív védelmi eszközök alkalmazása azonban nyilvánvalóan csak és kizárólag fegyveres támadás esetében fordulhat elő.

Felmerül a kérdés, hogy a védekező állam gyakorolhatja-e önvédelmi jogát akár hagyományos fegyverek útján is. Véleményünk szerint elképzelhető olyan szituáció, amikor alkalmazhat hagyományos fegyvereket is. Ilyen esetkörök lehetnek, amikor a támadás drón(ok), vagy légi irányítás információs rendszere ellen irányul és azt felhasználva követnek el fegyveres támadásnak minősülő cselekményt. Több példa is említhető, ilyen rendszereket ért támadásra: 2009 februárjában confickr elnevezésű vírus támadta meg a francia katonai adatbázist, amelynek következtében felszállási tilalmat rendeltek el a haditengerészet gépeinél; 2009 decemberében pedig iraki felkelők meghackelték az amerikai légerő pilóta nélküli gépét (egy laptoppal és egy 25 dolláros fájlmegosztó programmal) aminek következtében követhették a gép által közvetített képet.[79] Amennyiben drónok felett sikerül átvenni az irányítást és fegyveres támadásnak minősülő cselekményt valósítanak meg azt vagy azokat felhasználva (vagyis kellően intenzív cselekményt és más államnak betudható módon), ebben az esetben, a forrás megfelelően pontos azonosítása esetén, az ezeket a gépeket irányító személyeket hagyományos fegyverekkel is likvidálhatják. Légi irányítás információs rendszere elleni támadás esetén, ha a rendszert felhasználva követnek el fegyveres támadást (akár a repülőgépek megsemmisítését, akár polgári személyek életének kioltását okozva) a forrás pontos azonosítása után alkalmazható hagyományos fegyver. Fontos feltételek véleményünk szerint, hogy a további támadás lehetőségének még fenn kell állnia és a kibertérben való sikeres és hatékony önvédelem esélye csekély.[80]

[79] Lewis, James Andrew: i.m. 5. és 7. o.

[80] Természetesen a fegyveres támadás korábban ismertetett kritériumainak is meg kell felelnie az önvédelmet aktiváló támadásnak.

Szintén kérdéses azon magánszemélyekkel szembeni fellépés eszközrendszere, akik a támadáshoz erőforrást biztosítanak. A Tallini Kézikönyv elkülöníti a támadásban résztvevő magánszemélyek körét aktív, szándékos magatartást tanúsítókra és passzív, gondatlan elkövetőkre. Előbbi esetén rögzíti, hogy a polgári személy elveszíti védettségét és támadhatóvá válik informatikai és egyéb jogszerű módszerekkel. Az egyéb jogszerű módszert nem határozták meg, azonban mivel itt is csak arányos és szükséges mértékű lehet az önvédelmi jog gyakorlása, ezért nyilvánvaló, hogy ezen eszközök alkalmazása csak az eredményhez való hozzájárulás mértékét érhetik el. Ellenkező esetben likvidálható volna olyan személy is, aki gépe erőforrását engedi át a művelet megvalósításához több száz, ezer, vagy akár százezer másik felhasználóval együtt. A passzív elkövetőkkel szembeni fellépésről nem nyilatkozik a kézikönyv, e hallgatás arra utal, hogy velük szemben nem jogosult fellépni a megtámadott állam, véleményünk szerint az önvédelmi jog gyakorlása során kizárólag kibertéri önvédelmi műveletek az arányosság és szükségesség mértékéig velük szemben is gyakorolhatóak, amennyiben ez elengedhetetlenül szükséges a veszély elhárítása érdekében, de a passzív résztvevő felelőssége nem állapítható meg a fegyveres támadásért.

E kérdések mellett alapvetően fontos az önvédelem jogának időbeli korlátozottsága is. E körben rögzíti az Alapokmány, hogy az önvédelem érdekében alkalmazott erőszak gyakorolható „mindaddig, amíg a Biztonsági Tanács a nemzetközi béke és a biztonság fenntartására szükséges rendszabályokat meg nem tette. A tagok az önvédelem e jogának gyakorlása során foganatosított rendszabályaikat azonnal a Biztonsági Tanács tudomására tartoznak hozni és ezek a rendszabályok semmiképpen sem érintik a Biztonsági Tanácsnak a jelen Alapokmány értelmében fennálló hatáskörét és kötelességét abban a tekintetben, hogy a nemzetközi béke és biztonság fenntartása vagy helyreállítása végett az általa szükségesnek tartott intézkedéseket bármikor megtegye.”[81] Tisztázni

81 ENSZ Alapokmány 51.cikk.

kell azt is, hogy mikortól illeti meg ezen jog a megtámadott államot. Az 51. cikk világosan fogalmaz, vagyis az önvédelmi jog jogszerű gyakorlásának megnyílásához fegyveres támadásnak kell bekövetkeznie, ez két okból is szükséges, egyfelől csak így köthető az erőszak jogszerű alkalmazása egy megfelelően magas szinthez, másodsorban csak bekövetkezett fegyveres támadás esetén értelmezhető az arányosság és szükségesség követelménye. Parttalanná tenné az önvédelem alkalmazását a be nem következett támadáshoz fűzött következmény, nem beszélve arról, hogy nehezen vagy egyáltalán nem bizonyítható, hogy a támadás tényleg bekövetkezett volna, és ha igen annak milyen intenzitása lett volna. Az erőszak általános tilalmát ezen esetkörben nem lehetne értelmezni, hiszen a megelőző védelem lehetőséget biztosítana az államok számára arra, hogy erre való hivatkozással veszélyt vizionálva erőszakkal jogszerűen lépjenek fel.

A Nemzetközi Bíróság viszont nem foglalt állást abban a kérdésben, hogy közvetlen vagy közvetett veszéllyel szemben az önvédelem gyakorlása jogszerű vagy jogszerűtlen-e.[82] Az Egyesült Államok ezt kihasználva próbálta nemzetközi jogilag elfogadhatóvá tenni a 2002-ben kiadott nemzetbiztonsági stratégiáját az ún. Bush-doktrínát. E dokumentum szerint lehetősége lenne egy államnak preemptív önvédelem alkalmazására terroristák és tömegpusztító fegyverrel rendelkező államok konkrét fenyegetésével szemben.[83] Az USA-nak erre az iraki háború megindításához volt szüksége, azonban felmerül a kérdés, hogy mi minősülhet konkrét fenyegetésnek? A konkrét fenyegetés meghatározásának a hiánya egybemossa a preemptív (küszöbön álló támadás, közvetlen veszély) és a preventív (nem küszöbön álló támadás, absztrakt és távoli veszély) önvédelem fogalmi körét és relativizálja az erőszak általános tilalmát. „Ez – a vélt vagy valós okoktól teljesen függetlenül – az ilyen módon megalapozott intervenciót az agresszióval rokonítja. A jogsértésre alapuló intervenciók

[82] Kajtár Gábor: i.m. (2011) 15. o.

[83] Dunay Pál: *Az iraki háború és a nemzetközi jog: a kezdetektől a végéig*, In. Külügyi Szemle 2007/2-3. szám 230. o.

ismétlődése, illetve azok eltűrése viszont marginalizálhatja a háború indítás tilalmára alapuló nemzetközi jogot. Félő, hogy bármely hasonló magatartás bárminemű elfogadottsága alááshatja azt a helyzetet, amely a nemzetközi jogot a 20. század második felétől a béke jogaként azonosítja."[84] A nemzetközi közösség pedig tartotta magát ezen állásponthoz, és nem igazolta egyetlen döntésével sem az Egyesült Államok ezen irányú törekvéseit.

Osztva Pradler Árpád azon álláspontját, hogy „az önvédelem tehát nem lehet preventív, megelőző lépés… nem lehet hivatkozni állítólagos veszélyre, provokációra, a saját állam állampolgáraival szemben elkövetett méltánytalanságokra, mint ürügyre."[85] Ennek okán úgy véljük megelőző támadás (legyen az preventív vagy preemptív) az agresszió tilalmába ütközik, ennek alkalmazása nem kérdőjelezhető meg a kibertérben megvalósított műveletek esetében sem.

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. Ezen fejlődéssel párhuzamosan a hadviselés átalakuláson ment keresztül és megjelentek az információs műveletek, információs hadviselés, ennek önállósult részeként a század végére kialakult a kiberművelet átfogó területe, mely három jól elkülöníthető tevékenységre bontható fel: (1) kibertámadásra, (2) kiber információszerzésre, valamint a (3) kibervédelemre. Az Egyesült Államokat ért 2001. szeptember 11-i támadás világossá tette, hogy a nemzetközi jog alkalmazhatósága érdekében át kell értelmezni a hagyományos fegyveres támadás fogalmi körét, mert olyan új típusú fenyegetések jelentek meg,

[84] Dunay Pál: i.m. (2007), 233. o.

[85] Prandler Árpád: *Az ENSZ Biztonsági Tanácsa*, Budapest, Közgazdasági és Jogi Könyvkiadó, 1974, 137-138. o.

amelyek a szabályok megalkotói számára még ismeretlenek voltak. Kiberműveletek esetében ez az Észtországot és Grúziát ért támadásokat követően vált világossá.

Szükségessé vált annak megvizsgálása, hogy a kibertérben megvalósított műveletek minősülhetnek-e nemzetközi jogi értelemben vett fegyveres támadásnak. Tanulmányunkban kifejtettük, hogy a három kiberműveleti terület közül kizárólag a kibertámadás lehet a vizsgálat tárgya, hiszen az információszerzés semmilyen esetben sem minősülhet támadásnak, míg az önvédelem jellegéből adódóan nem vehető számításba.

A fegyveres támadásként való azonosításnak meg kell felelnie mennyiségi és minőségi kritériumoknak. A mennyiségi kritérium azt jelenti, hogy az alkalmazott erőszaknak el kell érnie egy súlyos mértéket, intenzitást, míg a minőségi kritérium rögzíti azt a feltételt, hogy kizárólag államközi viszonyban értelmezhető a fogalom. E kritériumot nem különösen kell magyarázni állami szerv megfelelő súlyú cselekménye esetén, azonban magánszemélyek és csoportjaik esetében csak akkor állhat fenn a betudhatóság, ha ezek a személyek az állam utasítása, irányítása vagy ellenőrzése alatt követték el cselekményüket. Az ellenőrzés fogalma vitatott a nemzetközi jogban, hiszen a Nicaragua-ügyben tényleges ellenőrzést várják el, addig a Tadic-ügyben – igaz egyéni büntetőjogi felelősség kérdésében – elegendőnek bizonyult az általános kontroll. A Nemzetköz Bíróság 2007-es döntésében, azonban megerősítette a tényleges kontroll elvének alkalmazását.

Ennek megfelelően egy kibertámadás, akkor minősülhet fegyveres támadásnak, ha intenzitása elér egy meghatározott magas szintet, ez két körben képzelhető el. Egyfelől a hagyományos fegyverekkel analóg módon értelmezett támadások esetén, így például atomreaktor, atomerőművet, víztisztító és ellátó rendszer vagy más egyéb kritikus infrastruktúrát ért támadás esetében, akkor tekinthető fegyveres támadásnak, ha hatásuk oly pusztító, hogy akár a nukleáris, biológia vagy vegyi fegyverekkel azonos hatású. Ezt az álláspontot erősíti a Tallini Kézikönyv állásfoglalása is. Másfelől pedig a kibertámadás egy önálló alakzataként értelmezhető az a

támadás, amely oly intenzív, hogy az állam működését megbénítja. Ez azt jelenti, hogy a hadsereg vezetése elveszíti az irányítás és ellenőrzés képességét, másfelől az állami közigazgatás működése nagymértékben akadozik vagy teljesen megszűnik, a szociális ellátás megbénul, a bankszféra és a gazdaság pedig működésképtelenné válik.

A minőségi feltétel nyilvánvalóan teljesül, amennyiben a megfelelő súlyú támadást az állam szerve (kiberhadteste) követi el, kérdéses viszont az irreguláris elkövetés esetköre. Itt sem vitatott azon esetkör, ha irányítása vagy utasítása alatt cselekszik. Ellenőrzés esetkörében úgy véljük két okból csak a tényleges ellenőrzés az elfogadható, egyfelől az általános ellenőrzés jelentősen kiszélesítené a fegyveres támadás esetkörét és ezzel relativizálná az erőszak általános tilalmát, másfelől pedig ezen elvárás hatására az államok erősen korlátoznák az internet szabadságát, amely egyes államokban már alkotmányos jogként is megjelenik (Észtország, Finnország). A tényleges ellenőrzés alatt – a terrorszervezetekre vonatkozó gyakorlat analógiája alapján – betudható az államnak, ha erőforrásokat biztosít, kiképzőtáborokat megtűr, tagjainak menedéket nyújt, Kardos Gábor ezen ismérveit kiegészítjük a tevékenységre való toborzás támogatásával, vagy eltűrésével. Szintén betudhatónak tekintjük, amikor az állam tud a tevékenységről, de nem tesz ellene semmit ebben az esetben is megalapozza saját felelősségét.

A kibertámadás a fenti kritériumok fennállása esetén fegyveres támadásnak minősítendő, amely esetén a megtámadott államot megilleti az önvédelem joga. Az önvédelem jogának gyakorlásának vannak időbeli és tárgyi korlátai. Időbeli korlátozása kiolvasható az Alapokmány 51. cikkéből, hiszen csak bekövetkezett fegyveres támadás esetén élhet ezen jogával és csak addig amíg az ENSZ BT nem tesz megfelelő lépéseket a béke és biztonság helyreállítása érdekében. Így kibertámadás esetében sem beszélhetünk preventív vagy preemptív önvédelemről, hiszen ezzel az általános erőszak tilalom alkalmazhatatlanná válna.

Tárgyi korlátozása az önvédelemnek, hogy csak a fegyveres támadás mértékével arányos és szükséges mértékű lehet az

önvédelmi jog gyakorlása. Ez azt jelenti, hogy kibervédelem területének passzív eszközei bármikor alkalmazhatóak (még nem fegyveres támadás esetén is), aktív eszközei csak fegyveres támadás esetén és ekkor is csak az ellentámadás és aktív megtévesztés jellegű eszközök. Hagyományos fegyver is alkalmazható, amennyiben ezzel az arányos és szükséges mérték nem sérül és az önvédelem joga másképpen nem gyakorolható célszerűen.

Azon polgári személyek, amelyek a támadásban „csak" erőforrást biztosítanak, ha ezt szándékosan teszik, velük szemben alkalmazható informatikai és egyéb jogszerű lépés is, azonban csak az arányosság és szükségesség követelményét figyelembe véve, vagyis közreműködésük arányában. Passzív vagy gondatlan erőforrás biztosítása esetén – bár erről a Tallini Kézikönyv nem rendelkezik – informatikai eszközök alkalmazását biztosítani kellene a megtámadott államnak szintén a követelmények figyelembe vételével, azonban ezen személyek esetében felelősségről nem beszélhetünk.

Összességében úgy gondoljuk, hogy *a kibertámadásnak legfeljebb szűk köre minősülhet fegyveres támadásnak*, azonban az emberek és sok esetben az állami vezetők is leginkább csak akkor képesek ennek felismerésére és megértésére, 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 volt.