VERESS CSONGOR BALÁZS

KIBERTÁMADÁS: JOGOS OK HÁBORÚ INDÍTÁSÁHOZ?

„A jövő háborúit nem csupán felfegyverzett katonák és bombákat szóró repülőgépek vívják majd. Ezeket a háborúkat egy egérkattintással el lehet kezdeni, akár a világ túlsó végén úgy, hogy e célra készített komputerprogramok bénítsák meg vagy pusztítsák el a kritikus infrastruktúrát az ellenséges országban: a szállítást, a kommunikációt, az energiahálózatot. Megbéníthatják a katonai hálózatokat is, amelyek a csapatok vagy a repülőgépek mozgását irányítanák."

LIAM O'MURCHU

■ Egyre gyakrabban olvashatjuk a sajtóban, hogy hackertámadás ért különböző honlapokat, közösségi médiát, kormányzati szervet, esetleg kiszivárogtak kényes adatok biztonságosnak tartott helyről. Felmerülhet a jogos kérdés az olvasóban, amennyiben nyilvánvalóvá válik, hogy a kibertámadás külföldről érkezett, és súlyos károkat okozott, hogyan léphet fel egy állam. Megtorolhatja-e hagyományos eszközökkel, esetleg megtámadhat-e egy másik országot, ha kiderült, hogy az állt az informatikai támadás mögött?

Tanulmányomban azt vizsgálom meg, hogyan lehetséges a nemzetközi jog eszközével védekezni az informatikai hadviselés ellen. A kiberhadviselés történetét és tulajdonságait bemutatva felvázolom a támadások lehetséges formáit, majd megpróbálok mindegyik esetre megoldást javasolni. A kutatásban a „kiberhadviselés" fogalmát szinonimaként fogom használni a sorozatos célzott informatikai támadásokra.

Informatikai támadások vagy a hadviselés lehetséges formái

■ Lattmann Tamás annak függvényében, hogy az informatikai támadások állami háttérrel vagy sem, illetve háború alatt vagy békeidőben történnek, négy lehetséges esetet vázolt fel.[1] A gondolatmenetét követve megvizsgálom, mikor léphet fel egy állam offenzíven a nemzetközi jog szerint. A támadások szempontjából különböző lehetséges helyzetek fordulhatnak elő:

– nincs fegyveres konfliktus, nincs állami háttér;
– nincs fegyveres konfliktus, de van állami háttér;
– folyamatban van fegyveres konfliktus, és a támadás mögött van állami háttér;
– folyamatban van fegyveres konfliktus, de a támadás mögött nincs állami háttér.

A második világháború óta egyre ritkábbak a nemzetállamok között hagyományos erőkkel, eszközökkel és eljárásokkal vívott háborúk. A támadások már nemcsak katonai infrastruktúrák ellen irányulnak, hanem elsősorban a civil infrastruktúrák vagy maguk a civilek ellen. Ezen újfajta konfliktusok fő jellemzője az aszimmetria. Jelen tanulmányban a kiberhadviselést fogom behatóbban vizsgálni, holott a leírtak éppúgy érvényesek egyszeri informatikai támadás esetében is. Ahhoz, hogy megvizsgáljuk a jog viszonyát a kiberhadviseléshez, először magát ezt a hadviselési nemet kell behatóbban tanulmányoznunk.

A hadviselés rövid történeti áttekintése

■ A technikai fejlettségnek köszönhetően jutott el a hadtudomány arra a szintre, hogy az ellenséges országoknak nem kell fizikai kontaktusba kerülniük; kisebb, de

akár nagyobb csapásokat is végre tudnak egymás infrastruktúrái ellen hajtani a világhálón keresztül. Régebb természetesen mindez elképzelhetetlen lett volna. A következőkben röviden vázolom a modern hadviselés történetének az alakulását. A különböző korok hadviseléseit részletesen feldolgozta a szakirodalom. Egy lehetséges rendszerezés négy generációra osztja fel a modern hadviselést, melynek kezdete a vesztfáliai béke (1648).[2] Azért ezt tekintjük kiindulópontnak, mert a bonyolult alárendeléses feudális rendszer helyét átvette a meghatározott terület és az ott élő nép fölött korlátlan szuverenitást gyakorló államok rendszere, így lett az állam monopóliuma a hadviselés. Az újkori hadviselés korszakolásáról nincs teljes konszenzus a szakértők között, de egyik lehetséges felosztást William S. Lind dolgozta ki,[3] amely a következőképpen tagolja az érákat.

A hadviselés *első* generációja a 19. század közepéig tartott, jellemzői a különböző alakzatokban (vonalban, oszlopban és négyszögben) harcoló gyalogság. Nagy hangsúlyt fektetnek a csapatok alapos kiképzésére, ebben a korszakban vezettek be egyfajta sorkatonaságot, nyíltak a tisztek kiképzésére alkalmas iskolák. Ebben a korban különült el látványosan a civil és a katona közötti különbség (egyenruha, tisztelgés, díszszemle).

A *második* generáció az ipari forradalom korára esik, így ennek vívmányait a hadviselés is felhasználja: sorozatlövő fegyverek, távíró, vasút, harckocsik, harci repülőgépek. A második generációs hadviselés csúcspontja az első világháború volt, ahol még a harceljárások lineárisak maradtak, de megjelent a tűzerőkoncentrálás az élőerő-koncentráción alapuló harceljárások helyettesítőjeként.

A *harmadik* generációs hadviselés jellemzője az összfegyvernemi erőkoncentráció és a háború a hátországra történő kiterjesztését eredményező totalitás. A harc ebben a korban már nem lineáris, így jelenik meg a hátország bombázása mint demoralizálási eszköz. A II. világháború végén megjelenő nukleáris fegyver alkalmazásával kezdődik a több évtizedes átmenet a következő generációba, mely Izrael 1967-ben és 1973-ban aratott győzelmei után veszi kezdetét.

A *negyedik* generációs hadviselés korában a nagyhatalmak tömegpusztító fegyvereinek nagy száma gátolja a közvetlen összeütközéseket. Az indirekt hadviselés jellemzője, hogy jelentős tényezővé válnak a nem állami hadviselők, így az állam elveszti hadviselési monopóliumát. Elmosódnak a háború–béke, a katona–civil, a harcoló–nem harcoló közötti határok és különbségek.

Megjelenik a hálózati háború, ahol az állami vagy nem állami szereplők felhasználják az információs forradalom olyan előnyeit, mint az internet vagy a közösségi oldalak, majd olyan támadásokat indítanak, ahol nincs felismerhető harctér. Ezekben a konfliktusokban nincs egyértelmű győzelem, sem vereség, a felek nem tartják magukra nézve kötelezőnek a hadviselés általánosan elfogadott szabályait és hagyományait.

A biztonsági területek köre az utóbbi időben kibővült egy új résszel, a kiberbiztonsággal. Az információbiztonság egy törékeny rendszer, amelyet egyre többször, egyre több ponton és egyre keményebb támadások érnek, amelyeket kezelni kell egyéni, állami és nemzetközi szinten egyaránt. Az utóbbi években az államok sorra fogadták el kiberbiztonsági stratégiájukat, és állították fel az állami kibervédelmi szerveiket annak következtében, hogy évről évre emelkedik a kibertámadások száma, és az érintett államok köre is folyamatosan bővül. Ugyanakkor az egyes vállalatok is igyekeznek magukat a lehető legteljesebben megvédeni a hackerekkel szemben – több-kevesebb sikerrel.

Jóllehet a fentiekben az informatikai hadviselést mutattam be, a következőkben tárgyaltak éppúgy érvényesek lesznek egyszeri informatikai támadásra is, nem szükséges a műveleteknek többszöri előfordulása.

A nemzetközi jog válasza az informatikai támadásokra

■ A bevezető után a négy lehetséges esetet mutatnám be. Abban az esetben, amennyiben külföldről érkezik kibertámadás vagy azok sorozata, de mögötte *nincs állami háttér*, illetve az országok – a támadás kiinduló, valamint a célországa – nem *állnak hadban* egymással, akkor a támadások az azokat elszenvedő ország bűncselekménynek minősíti, és a belső jog szerint bünteti. Ebben az esetben a nemzetközi jog csak kiegészíti a nemzetit azáltal, hogy az államok közötti büntető együttműködés kereteit és előírásait meghatározza. Ilyen a 2004-től hatályos, az Európa Tanács által kidolgozott Convention on Cybercrime, számítógépes bűnözés elleni egyezmény, melyhez csatlakozott az Egyesült Államok, Ausztrália és Japán is. Habár a konvenció célja elsősorban nem a kibertámadások elleni védekezés, hanem a számítógépekkel elkövetett gazdasági kárt okozó bűncselekmények elleni védekezés, tartalmában meghatározza ezen bűncselekmények körét, és megszabja az országok közötti együttműködést.

A négy lehetséges eset közül jogilag a legegyszerűbb az, amikor az informatikai támadás mögött *van állami háttér, és a támadás fegyveres konfliktus során* történik meg, mivel így a támadás betudható a háború egyik aktusának. Ezekre az informatikai támadásokra is a *ius in bello* előírásai, a 1949-ben elfogadott Genfi egyezmények által szabályozott humanitárius jog lesz az alkalmazandó.

Egy másik lehetséges eset akkor fordulhat elő, ha egy informatikai támadás végrehajtója nem állami szereplő, és a támadás mögött *nincs állami háttér a háborúban álló országok között.* Ezt a helyzetet a nemzetközi jog nem igazán tudja értelmezni, mivel egy természetes személy követ el támadást. Hasonló helyzetre próbál megoldást találni a III. Genfi egyezmény, amely konfliktus idején felosztja a lakosságot civilekre és jogszerű harcosokra. Ez a megkülönböztetés azért fontos, mert másképp kezelendő a polgári lakosság, és másképp a kombattánsok, illetve cselekedeteik is más jogi besorolás alá esnek. Az informatikai hadviselés helyzetében az összeütköző feleknek folyamatosan különbséget kell tenniük a személyek között annak alapján, hogy tevékenységük a nemzetközi jog alapján jogszerű-e. A IV. Genfi egyezmény szól a polgári lakosság védelméről.

Az utolsó eset a legfontosabb dolgozatom szempontjából, mégpedig *a fegyveres konfliktus nélküli informatikai támadás állami háttérrel.* Ebben az esetben is bűncselekménynek minősül a támadás, de nagyban bonyolítja a helyzetet, ha az elkövetés hátterében állami szerv és megbízás áll, mivel ez felveti a támadó állam felelősségét. Ilyenkor az a kérdés, hogy a megtámadott államnak milyen nemzetközi jogi eszközök állnak rendelkezésére: hogyan védekezhet a támadás ellen, sőt alkalmazhat-e erőt, vagy megtámadhatja-e a másik államot. Az idén 75 éves ENSZ Alapokmánya szabályozza ezt a helyzetet a *ius ad bellum* előírásaival, útbaigazít, hogy milyen esetben jogszerű egy támadás indítása, vagy hogy egy állam jogszerűen alkalmaz-e erőt egy másik állammal szemben.

Az erőszak nemzetközi tilalma

■ Kajtár Gábor a témában[4] kifejti, hogy 1945-ig nem létezett a háborúindításra vonatkozó általános nemzetközi jogi tilalom, annak csupán részleges korlátozásai jelentek meg. Ezen a helyzeten változtatott a második világháború szörnyűségei miatt az ENSZ Alapokmánya, amelyben az erőszak általános tilalmának rendszere került bevezetésre. Történetileg az *igazságos háború* (bellum iustum) elmélete uralta a nemzetközi jogot, amely igazságos és igazságtalan háború között tett különbséget. A teória szerint háború és béke joga élesen elkülönül, a háború beálltával megszűnnek a nemzetközi diplomáciai kötelezettségek, jogon kívüli állapottá téve a háborút. A 20. században megjelenik a *bellum legale* fogalom, amely jogszerű háborút jelent, így megteremtve a jogszerű és jogellenes háború felosztást.

Az 1899-es hágai békekonferencián jelenik meg először a háborúindítás szabadságának jogi korlátozása. Az itt elfogadott I. egyezmény 2. cikke alapján a szerződő felek kötelezettséget vállaltak arra, hogy vitájuk békés rendezése érdekében más államok közvetítését veszik igénybe, mielőtt fegyveres erőszakhoz folyamodnának.

Az első világháború után létrejövő Nemzetek Szövetsége ahhoz a feltételhez kötötte a háborúindítás jogát, hogy a részes felek addig nem indíthatnak háborút, amíg a választott bíróság elé nem viszik a vitáikat.

A Briand–Kellogg-paktum 1928-ben került ratifikálásra, amelyet az akkor létező országok majdnem mind aláírtak, és lemondtak a háborúról mint a nemzetközi viszályok elintézésének módjáról. Ez volt az első olyan multilaterális szerződés, amely átfogó jelleggel tiltotta meg a háborúindítást, azzal együtt, hogy megszegése esetére nem létezett szankciórendszer.

A következő nagy mérföldkő az ENSZ Alapokmányának kidolgozása volt, amely nem a háborúról, hanem az erőszakkal való fenyegetésről és annak alkalmazásáról szól: 2. cikkének (4) bekezdése szerint „a szervezet összes tagjainak nemzetközi érintkezéseik során más állam területi épsége, vagy politikai függetlensége ellen irányuló vagy az Egyesült Nemzetek céljaival össze nem férő bármely más módon nyilvánuló erőszakkal való fenyegetéstől vagy erőszak alkalmazásától tartózkodniuk kell".

Ebbe a bekezdésbe beletartozik a nemzetközi határokat megsértő erőszak alkalmazása. Az államok így akartak teljes és átfogó államközi erőszaktilalmat elérni. Kivételek az erőszak tilalma alól mégis léteznek:

– *a Biztonsági Tanács felhatalmazásával alkalmazott fegyveres erő joga* (Alapokmány 39. cikk)

– *és az önvédelem joga* (Alapokmány 51. cikk).

A sorrendből észrevehető, hogy a BT határozatai alapján alkalmazott fegyveres erőszak megelőzi az önvédelemhez való jogot. A BT-nek van döntő szerepe a viták békés rendezésében, ezért rendelkezik erőszak-monopóliummal.

Az önvédelem joga szűk kivételként marad meg: „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 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."

A fegyveres támadás szükségessége, majd az önvédelmi jog gyakorlásának arányossága a nemzetközi szokásjog része. Az idézetben szereplő „természetes" jog kifejezés egyes vélemények szerint az államok egyoldalú és korlátozhatatlan lehetőségére utal, hogy megvédhessék magukat. Ezen, kisebbségi, vélemények szerint nemcsak fegyveres támadás esetén lehet önvédelmet gyakorolni. Lehetőség lenne a külföldön megtámadott saját állampolgárokat is megvédeni, vagy akár megelőző önvédelemre vagy az önvédelemre későbbi támadások megelőzése céljából.

A fegyveres támadás fogalmának meghatározása az önvédelmi jog lényege, melynek a térbeli és az idődimenzión túl van egy kvantitatív és egy kvalitatív összetevője is. A fegyveres erőszaknak el kell érnie egy bizonyos szintet ahhoz, hogy az fegyveres támadásnak minősüljön.

Szembetűnhet a különböző fogalomhasználat: a 2. cikk (4) bekezdése az erőszak alkalmazását tiltja, de az 51. cikk az önvédelmi jog feltételének a fegyveres támadás létét várja el. Az Alapokmány szerzői ezzel azt akarták elérni, hogy ne lehessen önvédelemre hivatkozni minden kisebb fegyveres erőszaknál. Ezek sze-

rint az államok minden erőszakos államközi cselekménye sérti az általános erőszaktilalmat, de csak nagyon súlyos esetekben, fegyveres támadás bekövetkezésekor folyamodhatnak önvédelemhez. Fegyveres támadásról csak akkor beszélhetünk, ha egy állam ellen jelentős fegyveres erőszakot alkalmaznak, amely betudható egy másik államnak.

Létezik azonban olyan agressziós cselekmény, amelyet fegyveres támadás hiányában is el lehet követni, például agressziónak minősül az is, ha egy állam megengedi, hogy egy másik állam rendelkezésére bocsátott területét agresszió elkövetésére használják fel.

Következtetés

■ A fent leírtak alapján a leglényegesebb kérdés, hogy fegyveres támadásnak minősülhet-e az informatikai támadás a nemzetközi jog szerint. A téma szakértői ezt nem igazán támogatják, mivel félő, hogy egy kisebb informatikai támadás ürügyét felhasználva egy állam, önvédelemre hivatkozva, megtámad egy másikat. Vagyis egy informatikai támadás valós, fegyveres hadviseléshez vezetne. Azonban láthatjuk., hogy a gyakorlat megengedőbb az önvédelemre hivatkozó államokkal szemben, így a szakértők sem zárkóznak el teljesen attól, hogy a kibertámadásokat tényleges fegyveres támadásnak tekintsünk: „Erre jó példaként szolgál Stéphane Abrial tábornok, a NATO Szövetséges Átalakítási Parancsnokság (NATO ATC) vezetőjének 2011-ben közzétett véleménycikke a New York Times hasábjain, valamint a NATO CCD COE által 2012-ben kiadott útmutató, amely kijelenti, hogy egy informatikai támadás adott esetben beilleszthető az agressziós cselekmények fogalmi körébe, és ezzel egyidejűleg kiválthatja az önvédelem gyakorolhatóságát is. A Nemzetközi Bíróság a nukleáris fegyverek alkalmazhatóságával kapcsolatos tanácsadó véleményében korábban úgy értelmezte az »erő alkalmazásának tilalma« fogalmát, hogy az bármilyen eszközzel megsérthető, az előírás nem meghatározott fegyverekre vonatkozik – ebből következően érvelhetővé válik, hogy egy informatikai támadás is alkalmas lehet e tilalom megsértésére.”[5]

Tovább játszhatunk a gondolattal, amennyiben fegyveres támadásnak fogadjuk el az informatikait, így a megtámadott élhet az önvédelemmel. A kérdés az, hogy milyen legyen a válaszlépés? Informatikai támadásra informatikai? Vagy fegyveres? Elméletben lehetséges mind a kettő, vagyis a sértett ugyancsak kibertámadást hajt végre, de az is elképzelhető, és pont ez a kényesebb helyzet, ha informatikai támadásra fegyveres erővel válaszol. Az első esetben az is kérdés lehet, hogy a sértettnek feltétlenül a támadó állami szervet kell megtámadnia, vagy dönthet úgy, hogy az agresszor állam egy más intézménye ellen indít informatikai hadviselést.

A nemzetközi jog megengedi egy támadással szemben az azonos mértékű és jellegű ellentámadást, amely teljesíti az önvédelemmel kapcsolatos egyéb kritériumokat is, így nem válik az ellenintézkedés retorzióvá. Ezek a következők:

– *szükségességi kritérium*, vagyis a támadás elhárítására nincs más mód,
– *arányossági kritérium*, vagyis az nem okoz nagyobb kárt,
– *azonnalisági kritérium*, vagyis közvetlenül a támadás után.

A nemzetközi jog gyakorlata tolerálja a nem fegyveres ellenintézkedések során a represszáliát, retorziót, ami nem az adott jogsértő cselekmény közvetlen elhárítását, hanem a további ilyenektől való távoltartásra serkentést jelenti.

A mai világban könnyen elképzelhető, hogy egy informatikai támadásnak több emberáldozata legyen, mint egy klasszikus fegyveres támadásnak, elég csak például egy olyan közlekedési rendszer elleni kibertámadásra gondolni, mint a légi irányítás.

Üdvözlendő, hogy a 2020 áprilisában elfogadott új magyar Nemzeti Biztonsági Stratégia már megoldást kínál az informatikai támadás besorolására és a lehetséges válaszok adására:

„100. Érdekünk a hibrid hadviselés elleni nemzeti és elsősorban az EU és NATO kereteiben, a többnemzeti válaszadási képesség fejlesztése.

101. Magyarország a fizikai biztonságot veszélyeztető vagy jelentős anyagi károk okozására képes kiberképességeket fegyvernek, alkalmazásukat fegyveres *agressziónak* tekinti, amelyre a fizikai térben megvalósuló válaszadás is lehetséges. A kiberműveletek sokszor nehezen bizonyítható attribúciójára, az elkövető azonosítására, megnevezésére való tekintettel a válaszlépések különösen körültekintő, eseti elbírálást igényelnek az érintett kormányzati szervezek bevonásával."[6]

Véleményem szerint a kibertér műveleti területté nyilvánítása mellett a másik hatalmas előrelépés az új Nemzeti Biztonsági Stratégiában a kiberképességek fegyverként való definiálása és alkalmazásukat fegyveres agressziónak tekintése. A jogszabály a kibertérben történő támadásokra a fizikai térben megvalósuló válaszadás lehetőségét is kodifikálja. Ezzel egy olyan problémát oldott meg a hadijog területén, melyre az informatikai hadviselés megjelenése óta nem volt egyértelmű válasz.

Megoldás: új, digitális genfi egyezmény?

■ A második világháború tapasztalataiból okulva 1949. augusztus 12-én Genfben fogadták el a négy modern jegyzőkönyvnek nevezett nemzetközi jogi szabályokat, melyeket 1977-ben két kiegészítő jegyzőkönyvvel bővítettek. Az *első* egyezmény a hadi sebesültek, a *második* a haditengerészeti állomány, a *harmadik* a hadifoglyok, a *negyedik* a polgári lakosság helyzetéről, míg a *kiegészítések* a nemzetközi és nem nemzetközi fegyveres összeütközések áldozatainak védelméről szólnak. A genfi konvenciók a fegyveres konfliktusokban alkalmazandó nemzetközi humanitárius jog alapdokumentumai.

Szakmailag rendkívül izgalmas az a helyzet, amikor háború nem lévén egy ország több tíz vagy száz ország ellen intéz kibertámadást *malware*[7] vagy vírus formájában. Így történt ez 2017-ben, amikor nemzetközi szakértők egybehangzó véleménye[8] szerint Észak-Korea egy nap leforgása alatt támadott meg 150 országot, több mint 200 ezer gépet megfertőzve a Wannacry zsarolóvírussal. Ezek után az USA, Nagy-Britannia, Ausztrália, Japán is kiberháborús agresszióval vádolta meg a phenjani vezetést.

Megszületett az igény az interneten zajló hadviselés szabályozására, a genfi egyezmények mintájára. Ezt a digitális korszakra igazított kezdeményezést az ENSZ, a NATO és a legnagyobb technikai cégek is támogatják, az előkészítése több mint egy éve zajlik.[9] Céljai között szerepel a civil felhasználók védelme, az etikus hackerkedés szabályozása, valamint az állami és magánszektor együttműködésének elősegítése. Mindezt úgy lehetne, hogy hasonlóan a tömegpusztító fegyverekhez a kiberfegyvereket is korlátozni kéne.

A probléma csak az, hogy egy hagyományos tömegpusztító fegyver vagy egy hadviselés árához képest a kiberfegyverek vagy a kiberhadviselés ára eltörpül, főleg ha figyelembe vesszük az ár-érték arányt: jóval kisebb befektetéssel lehet ugyanolyan nagyságú, akár nagyobb kárt okozni. A másik felmerülő gond a bizonyíthatóság kérdése, az államok mindig tagadják, hogy a támadásokhoz közük lenne. A Wannacry esetében Észak Korea tagad, a Stuxnet esetében Izrael meg az Egyesült Államok.

■ SZAKIRODALOM

Couzigou, Irène: *The Challenges Posed by Cyber Attacks to the Law on Self-Defence*. European Society of International Law 2014. 16.

Eberle, Christopher J.: *Just Cause and Cyber War*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2048447 (Letöltés ideje: 2020.03.11.).

Rid, Thomas and Buchanan, Ben: *Attributing Cyber Attacks*. https://ridt.co/d/rid-buchanan-attributing-cyber-attacks.pdf (Letöltés ideje: 2020.03.11.).

Rid, Thomas: *Cyber War Will Not Take Place*. Journal of Strategic Studies 2012. 35.

Stenersen, Anne: *The Internet: A Virtual Training Camp?* Terrorism and Political Violence 2008. 20.
Stevens, Tim: *A Cyberwar of Ideas? Deterrence and Norms in Cyberspace*. https://core.ac.uk/download/pdf/43778654.pdf (Letöltés ideje: 2021.03.11.).
Stone, John: *Cyber War Will Take Place!* Journal of Strategic Studies 2013. 36.
Tallinn Manual on the International Law Applicable to Cyber Warfare. 2013 Cambridge University Press. https://www.peacepalacelibrary.nl/ebooks/files/356296245.pdf (Letöltés ideje: 2021. 08. 21.).

JEGYZETEK

1. 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, 2013.
2. Simicskó István: *A hibrid hadviselés előzményei és aktualitásai.* Hadtudomány 2017/3–4.
3. William S. Lind et al.: *The Changing Face of War: into the Fourth Generation.* Marine Corps Gazette 1989. 73. 10.
4. Kajtár Gábor: *Az erőszak tilalma.* In: Jakab András – Fekete Balázs (szerk.): Internetes Jogtudományi Enciklopédia. http://ijoten.hu/szocikk/azeroszak-tilalma Letöltve 2021. 08. 20.
5. Lattmann Tamás: *Nemzetközi jogi szabályozás célzott kibertámadások esetén.* In: Deák Veronika (szerk.): *Célzott kibertámadások.* Bp., 2018.
6. 1163/2020. (IV 21.) Kormányhatározat Magyarország Nemzeti Biztonsági Stratégiájáról.
7. Ebben az esetben ransomware, ami zsarolóvírus. (forrás: Nemzeti Kibervédelmi Intézet).
8. Thomas P. Bossert.: *It's Official: North Korea Is Behind WannaCry* https://www.wsj.com/articles/its-official-north-korea-is-behind-wannacry-1513642537. Letöltve 2021. 08. 21.
9. Hanula Zsolt: *A világháború már elkezdődött, és nincs hozzá szabálykönyv* (https://index.hu/tech/2018/02/24/digitalis_genfi_egyezmeny_kiberhaboru/) Letöltve 2021. 08. 20.