Simon László[1]

A fegyveres konfliktusokhoz kapcsolódó erőkivetés kognitív hatásai és lehetséges állami reflexiója

„Ez vagy valami, vagy megy valahova."[2]

Bevezetés

A különböző államformájú országok, a demokratikus államok kormányzatai eszmei meggyőződéstől függően igyekeznek környezetük (egyeduralmuk, szuverenitásuk, polgáraik, népük, nemzetük stb.) biztonságát, védelmét szavatolni. A társadalmak több ezer éves fejlődése kapcsán – minden pacifista célú törekvés ellenére – az országok és szövetségi rendszereik között kialakult konfliktusok rendre fegyveres összecsapásokban csúcsosodtak ki. Az államok fegyveres beavatkozásának és fegyverhasználatának joga a 20. században átélt borzalmakat követően – a háborúk viselésének közösségi legitimációja, illetve az illegitim cselekmények, agresszió szankciója ellenére is – fenyegetően aktuális kérdésként van jelen minden szempontból fejlettnek nevezett világunkban is.[3] A különböző lokális és globális válságok megoldásakor, a fenyegetések megszüntetésekor, a terror közvetlen vagy közvetett hatásainak enyhítése során – az államokon belül és az államok között – gyakorta elkerülhetetlen a jogos fegyverhasználat. A modern kor tanúsága szerint nem a békés időszakok növekedése és a világ-

[1] Alezredes; a Nemzeti Közszolgálati Egyetem Hadtudományi és Honvédtisztképző Kar Hadtudományi Doktori Iskolájának végzett doktorandusza. Kapcsolat: simon.laszlo@uni-nke.hu.

[2] Többször hallhattuk már a székely viccek egyik tréfás befejezéseként mottómat. Az eredeti idézet névtelen szerzőjének (vagy megalkotóinak) eredeti szándékától talán nem nagyon került messzire az a felhasználás, amelyet a technikai fejlődés egyik korszakának hajnalán kevésbé lehetne humorosnak ítélni. A viccnek több verziója lehet ismert, miszerint Áron bátyja és fia utazik a szekéren, és átsétál előttünk egy sündisznó (teknősbéka stb.). Az addig nem látott állat észlelése miatt a fiú megkérdezi, hogy vajon mi lehetett az, amit láttak. Áron bátyja hosszas „székelyes önmarcangolás és vívódás" után a lényt nem ismerve adta válaszában a talán tudományos értékelésnek is megfelelő, a mottóban szereplő reflexiót.

[3] Lásd még Farkas Ádám (szerk.): *A honvédelem jogának elméleti, történeti és kortárs kérdései.* Budapest, Dialóg Campus, 2018.

https://doi.org/10.36250/00920_24

béke közeledte valószínűsíthető. A globalizáció mellett akár fékként vagy ellenpólusként megjelenő hatalmi centralizáció, de a totalitárius államok kérdésköre is előtérbe helyezik a politikai szövetségek és eltérő szintű gazdasági hatalmak erőkivetítésének történelmi, katonai hagyományait. A Covid-19 jelöléssel illetett pandémia idején felsejlik egy új, digitális technológiára és hálózatokra épülő kor képe, amikor az infokommunikációs rendszerek nyújtotta virtuális terek felhasználása sokkal jelentősebb szerepet fog kapni. Meghatározó helyet fognak követelni a számítógépes programok és az általuk támogatott eszközök, robotok, automaták a konfliktusok kezelésében is. A humán erőforrás hiánya vagy a kockázatos emberi jelenlét sürgős kiváltása a hagyományos, politikai jellegű diskurzusok dogmatikus valóságától annyira távolra fog kerülni, hogy az egyéni és a közösségi elvárásoknak megfelelő, időszerű reflexiók elmaradása eredményezheti majd az újabb válságokat. Az időben logikusan elhúzódó, az elmúlt két évezredben megalapozott jogi és intézményi kereteihez „jogszabály-követően"[4] ragaszkodó válságkezelés esetenként képtelen lesz a gyors és biztonságos válaszok egységes megadására. A problémák hálózatalapú megosztása, a közösségekben kiváltott

[4] Elnézést kérek minden olvasótól és érdeklődőtől, de meg kell szakítanom a bevezetést egy személyes közbevetéssel. E mű születésének egyik céljaként határoztam meg, hogy a téma legkimerítőbben tudja tartalmazni mindazt a diszkurzív elemet, amely első pillanattól kezdve jellemezte a Cs. Kiss Lajossal folytatott, barátinak tekinthető beszélgetéseket. E találkozók helyszíne a Nemzeti Közszolgálati Egyetem Szenátusának üléseit jelentette, és annak gyakorta nem csak a szüneteit. A Rektor Úr figyelmes és tiszteletteljes jelzései ellenére folytattuk eszmecserénket. Ugyan a testület munkáját ez nem zavarta, de esetenként a szavazógomb lenyomásának elmulasztásával a szenátorok is megbizonyosodhattak, hogy a két intézet által delegált szenátusi tag nemcsak egymás mellett ül, hanem eddigi életükhöz híven magukat meghazudtolni nem tudva tárgyal. Bár akik ismerik Professzor Urat, Cs. Kiss Lajost, azok tudják, hogy én jó hallgatóként többnyire olyan kérdéseket fogalmaztam meg, vagy olyan felületes kijelentéseket tettem, amelyek mellett Ő nem tudott és nem is akart még udvariasan és diplomatikusan sem elmenni. Az első tudományos folyóiratba tervezett írásom leadása előtt épp arról beszélgettünk, hogy jómagam olyan területen kutatok (írok), ahol a jog kevésbe vagy abszolút nem alkalmazható. A válságok megelőzésében, kialakulásában, felszámolásában vagy a béke fenntartásában, kikényszerítésében a nem működő államok, akkori megfogalmazásom szerint a *nemzetközi és a nemzeti jog* ellenére áthidalhatatlan akadályt jelentenek, vagyis érvelésem szerint az addig fennálló jogrendszer a belső és külső környezeti hatásokra nem tud megfelelő jogi válaszokat adni. Most már tudom, hogy akkori alaptézisem nem volt helytálló. Cs. Kiss Lajos kezdeti verbális mentorálása kapcsán egyre inkább elfordultam az általános, a megszokott értelmezésű és dogmatikus megfogalmazásoktól. A különböző államok esetében az alapjogokból következő jogszabályok követése nem csupán az állam és polgárainak szerződése, így több, mint jogtudományi kérdés. A jog azon esetekben is jelen van, amikor az aktuális jogrendszer, jogértelmezés vagy szokásjog már társadalmi, szociális, katonai, környezeti vagy akár gazdasági szempontok alapján, továbbá ezen szektorokat érintő újszerű vagy annak tűnő folyamatok miatt nem alkalmazható. Az adott „intés" vagy inkább „intuíció" az általam gyakorta elemzett válságokat megelőző, illetve a válság eszkalációját követő időszak katonai nemzetbiztonsági jellegű kritikai vizsgálatát alapvetően határozta meg.

negatív hatások, valamint a lokális események globális támogatása, a szolidaritás növekedése mind-mind hálózatalapú szolgáltatásért kiáltanak. Az elkülönülő és egymásra ható klasszikus szegmensek, mint a társadalom, a gazdaság, a politika vagy a kultúra „tökéletesen virtuális" kialakítása egy teljesen új korszakot fog eredményezni mind az emberi kapcsolatokban, mind az élet egészét tekintve. Nemcsak a mérnökök és háziorvosok helyett fognak robotok tervezni, illetve diagnosztizálni, hanem robotkatonák fognak drónokkal összetűzni. A hálózatalapú megközelítéssel a jogos önvédelemre hivatkozva országrészeket vagy akár földrészeket lehet majd félelemben tartani, a fegyverek használata nélkül akár földrajzi tereket lehet majd annektálni. A hálózatokban alkalmazott információfegyver gazdaságilag, társadalmilag, kulturálisan is átalakíthat valóságos közösségeket, kognitív hatása az akaratuk ellenére is mássá formálja az egyéneket. A globalizációval világfaluvá vált életterünk a „virtuális valósággal" kiegészülve az ott szerveződő közösségek számára az újszerű infokommunikációs képesség megszerzését teszi elengedhetetlenné. Ez a fizikai biztonságunkat is alapjaiban fogja befolyásolni, pozitív, illetve negatív értelemben egyaránt. Az új programok, alkalmazások és technológiák (az „okos" eszközök, robotok vagy a mesterséges intelligencia alkalmazása), azok párosítása, összekötése a régi, hagyományos eszközeinkkel az információs hálózatok olyan rendszerét alkotják, amely az agresszió közvetett és az erőkivetítés közvetlen meghatározó közege lesz. Ebből adódik, hogy a fegyveres konfliktusok esetében a fizikai és a logikai célpontok legitim vagy önvédelmi célú fegyveres támadása mellett a résztvevők szándékának befolyásolásával, a félelem fenntartásával folyamatossá válik az agresszió és a terror.

A fegyveres konfliktusokhoz kapcsolódó erőkivetés – a polarizált felek küzdelme

A „civilizációk harca a civilizációk ellen" örökre a múlté. Az aszimmetrikus hadviselés és az élettérháborúk[5] is kilépnek a barát-ellenség ellentétpárjával azonosítható valóságos küzdelmekből, és kiegészülnek a kognitív szférában folytatott katonai jellegű műveletekkel, S mindez beláthatatlan pusztítást eredményezhet. A kibertérben elkövetett bűncselekményként azonosíthatatlan támadások ma még megoldhatatlannak tűnő bűnügyi és rendészeti problémái (az elkövető azonosítása vagy a kriminalisztika hét alapkérdésének hálózati felderítése) a közeljövőben a matematikának, az analitikának és az adatbázisok mesterséges intelligenciájával megvalósított feldolgozásának köszönhetően meggyőződésem szerint feloldhatóvá válnak. A számítógépes bűncselekmények szankcióinak rendszere

[5] Vö. Az MHTT Konferenciája: Az aszimmetrikus hadviselés. *Hadtudomány,* 25. (2015), 1–2.

a „virtuális cselekmények" megkezdése előtt olyan következményekkel fognak fenyegetni, amelyek ismeretében csökkenhetnek a szándékos károkozások, illetve az erőszakos verbalitásra épülő támadások. Ugyanakkor az információ mint fegyver alkalmazása – a fegyveres összecsapások alkalmával vagy azok mellett – a teljes erőfölény kialakításának alapelemévé válik. A jelenleg és a jövőben megjelenő fegyveres konfliktusok hibrid mibenlétük kapcsán bár nem sorolhatók be klasszikusan az államok közötti közvetlen konfliktusok közé[6] – mint a mottóban említett folyamat, jelenség esetében –, az azonosítható jellemzők (indikátorok) segítségével mégis egyértelműen meghatározhatók a válság összetevői, de még a krízis rendezését szolgáló cselekmények irányvonalai is.[7] A hadtudomány területén a bipoláris világrend átalakulása a „kis háborúk" felé fordította a szakértők figyelmét. A jogelmélet területén a nemzetközi válságkezelésben nemcsak az egyes ellenséges országokhoz köthető fegyveres összeütközések jogáról szükséges diskurzust folytatni, hanem a jól azonosítható ön- és honvédelem – az önrendelkezés, illetve az emberiesség – jogáról is.

Az amerikai terrortámadás (9/11) eseményét követően a válságkezelésben az államok működése is a tudományos vizsgálatok tárgyává vált. Ennek kapcsán két alapvető megvilágítást különböztethetünk meg. (1) Az egyik Oszáma bin Láden tevékenysége és az általa irányított terrorszervezet állami kapcsolata, amely egyértelműen köthető volt egy kevésbé jól működő országhoz, Afganisztánhoz. (2) A másik az Iszlám Állam elnevezésű terrorszervezet, az ISIS, amely Szíria kulcsfontosságú részein működtetett pszeudoállamot. Az egészségügy megszervezésével, adók kivetésével, valamint az „önvédelmi" célú fegyveres küzdelem megszervezésével, továbbá a hozzá kapcsolódó infokommunikációs, közvetett hadműveletek és elektronikus propaganda terjesztésével[8] az ISIS működése, de a felszámolása is olyan államelméleti kérdéseket vetnek fel, amelyek mellet

[6] Az Ukrajnában jelenleg is zajló orosz–ukrán fegyveres konfliktus nem Ukrajna és az Oroszországi Föderáció közötti hagyományos értelmű háború, vagy csak az ukrán állami erők és az ukrajnai orosz szakadárok államépítő kontra államromboló legitim harca.

[7] Ez akkor is igaz, ha a cselekmények sorozata több együttműködést és ad hoc szövetségek kialakítását igényli. A szíriai válságban a harcoló felek polarizáltak, így a két szemben álló fél nem azonosítható. A fegyveres konfliktus még 2020-ban, több mint hat év elteltével is várat magára.

[8] Leegyszerűsítve: az ISIS olyam állami funkciók megszervezésével lehetett kvázi államalkotó erő, kormányzat, amely az érintett területek lakosságának alapvető életvitelét és életbiztonságát szolgálta. Olyannyira lehetett „sikeres", hogy nemcsak az érintett földrajzi területen élvezett támogatást, hanem a világ bármelyik pontján képes volt mozgósítani, akár terrorcselekmények elkövetésére is ösztönözni. A megvalósított politikai célú agressziót ebben az esetben sem lehet csak jogelméleti módon megítélni. Az elkövetők tetteit pedig bűncselekményként értékelni rendre hibának minősült, mivel újabb és újabb legitimációs alapot adott az ideológiai és kulturális értelemben másként gondolkodóknak: a szabadságharcosok nem bűnözők. Az ő támogatásuk nem bűnpártolás, hanem szolidaritás és lelkiismereti kötelesség. E felismerésem tárgyalása Cs. Kiss

nem mehetünk el szó nélkül. A következmények, a megtervezett események nem a hagyományos katonai célok és célpontok legitim „szabályozott rendszereként" azonosíthatók. Nincsenek törésvonalak, nincsenek jól körülhatárolható életterek. A lakosság támogatása mellett a fizikai értelemben is túlerőben lévő fél ellen bármilyen eszköz és módszer bevethetőnek minősült. A terror kiegészült a hagyományos fegyverek mellett a virtuális terekben is hirdetett információkkal. Az állam e „kis háborúk" esetében reflexióként rendre önkorlátozó és a legtöbb esetben a lakossága számára elfogadható, támogatható, a legkevésbé katonai eszközöknek adhat szerepet.

Az államok egymás között is rendelkezésre álló szövetségesi, valamint alkotmányos érték- és érdekrendszerével szemben fellépő aszimmetrikus erők creveldi értelemben nem maradhatnak helyi szintű konfliktusok. A regionális térben folyó fegyveres erőszak az 1991 előtt fennálló bipoláris világrenden túlmutatva már nem az ellenség és barát összefüggéseit mutatja, hanem egy többszereplős hálózat – céljaiban és szövetségeiben folyamatosan változó – polarizált rendszerét. Sem a válság elmélyítésében, sem a válság kezelésében nem mutatható ki állandóság, csak valamiféle „érdek- és dacszövetség". A fegyveres összeütközések során ugyanazok az erők (katonai alakulatok, fegyveres csoportok, terrorista sejtek stb.) egyik célkitűzésük alapján a kormányerőket támogatva, más célok esetében a kormányerőkkel szemben fellépőkkel együtt harcolnak, amint azt például Szíriában 2011 óta tapasztaljuk. A polarizált felek küzdelmében, az aszimmetrikus erők összecsapásában, a válság felszámolásában közvetlen és közvetett módon az információs műveletek kerültek a középpontba. A konfliktusok felszámolása a hadviselés hagyományos dimenzióiban (az erő, a tér, az idő és az információ szegmensében) a hadviselés kultúrájából eredően más és más reakciókat követelnek. A jogilag is szabályozott állami reflexiók puha *(soft power)* és kemény *(hard power)* módszerei mellett a közepes erőként (*medium power*ként) jellemezhető csoportokkal és erőkivetítéssel (az államok szintje alatt jelentkező politikai, gazdasági és/vagy katonai terrorral szemben) is fel kell mutatni az ország szuverenitásának védelmét és a polgárok biztonságát szavatoló intézkedéseket. A közepes erők egyre növekedő jelentőségű reakciói kapcsán a háború, az erőszak már nem a politikai hatalommal bíró államok vagy szatellitországok között folyik, hanem egyéb polarizált felek részvételével. E csoportok fegyveres és információs cselekményeinek megítélésében nem minden esetben alkalmazható a büntetőjog. A terrorcselekmények esetében rendre előkerül a forradalmár és a partizán harca, amely a cselekményeik legitimációját tekintve nem bűnözők, hanem harcoló

Lajossal olyan kutatási részeredmény ígéretével kecsegtetett, amely a politikai elméletéhez kapcsolódva kulcsfontosságú lehet a kiberteret is felhasználó fegyveres agresszió pontos és nem kevésbé fontos katonai és bűnügyi elkülönítéséhez.

felek küzdelme. Az erőszak monopóliumának kérdésköre már nem kapcsolódhat szorosan az egyes államokhoz.

A globalizáció átalakította az egyéni és az államok közötti kapcsolatokat. A születő világtársadalom és világkultúra nyitott gerinchálózata működik, de az információk a legcsekélyebb mértékben sem mutatnak nyíltságot. Értékelésem szerint minél nyíltabb információk jelennek meg e nyitott társadalmakban, annál inkább felértékelődik a személyes, gazdasági-pénzügyi, de a szolgálati titkok védelmének kérdése is. A „világpolgárok" biztonsági szempontból kiszolgáltatottakká válhatnak, az egyének és a közösségek önvédelmének monopóliumai pedig feloldódnak. A polarizált, ad hoc ellenség számára a nyitott társadalmak nyílt információi és a világkultúrában meg nem jeleníthető személyes értékek és érdekek könnyen elérhető, pusztítandó célpontokká válhatnak.[9]

A kibertérben jelen lévő agresszió és erőkivetítés lehetséges állami reflexiói

A kibertér és a hálózatalapú infokommunikációs terek fejlődése, valamint ezek közvetlen kapcsolata az emberek kognitív szférájával kihívást jelentenek a modern hadviselés, a modern jogalkotás és a jogalkalmazás számára is. A dolgok és az információk okos vagy intelligens hálózatán, a belső és a külső kibertér (a szoftverek és hardverek) mellett a rendszerben áramló információk és azok tartalmának hatásait is érteni kell. A modern államok szervezetei a társadalom alapvető létfunkcióit biztosítják a kibertér támogatásával. Ez a változás jelentős hatást gyakorol az egyének és a közösség öntudatára; egyetértve Castellsszel: a hálózathoz való tartozás a létezés fokmérője.[10] Mivel a technológia (így a digitális és a virtuális tér is) összefonódik a hagyományos tér folyamataival, a léttel összekapcsolódó feszültségek szintén visszatükröződnek, azok reflexiót igényelnek. Amikor a számítógép, a televízió vagy a mobiltelefon előtt ülünk, felértékelődnek azok az egyéni készségek, kompetenciák, amelyek az egyén részéről biztonságtudatos gondolkodást igényelnek. Ugyanakkor nem kell bizonygatni, hogy az erőszak és az erőkivetítés, a támadások természete ezen a szinten túlmutathat, vagyis nem állhat mindenki mellett az infokommunikációs térben egy matematikus, egy informatikus, egy rendőr, egy katona vagy egy olyan bármikor megjelenő

[9] Vö. Kereki Ádám: A kritikus infrastruktúra meghatározásának módszerei, különös tekintettel a magyar honvédelmi infrastruktúrára. In Farkas Ádám (szerk.): *A honvédelem jogának elméleti, történeti és kortárs kérdései.* Budapest, Dialóg Campus, 2018. 151–166.

[10] David Bell: *Cyberculture theorists – Manuel Castells and Donna Haraway.* London – New York, Routledge, 2007. 67.

intelligens megoldás, amely polihisztorként a bennünket érő támadásokat megelőzi, elhárítja vagy kezeli az egyes következményeket.

A kibertér sebezhetősége tehát nemcsak a hálózatban szereplő intézmények és felhasználók virtuális sérülékenységéből fakad, hanem a természetes és a technológiai nyitottságukból, vagyis a hálózatos és hálózaton kívüli összeköttetéseikből. Az emberi erőszak kiterjesztése a digitális hálózatokban átformálta a humán biztonság jelentőségét. Felbecsülhetetlen értékként és az emberiség szempontjából mérhetetlen pusztításként is megmutatkozott az eltérő kultúrájú és felfogású államok, illetve államok szövetségének legitim és kevésbé legitim beavatkozása. Az egyes államokhoz jogilag nem köthető szereplők (bűnözői, illetve terrorista csoportok) alacsony intenzitású fegyveres küzdelme – azok katonai jellegű felszámolását követően is – fenntarthatónak és újraszervezhetőnek bizonyult. A fizikai terror hálózati megjelenése, annak kognitív túlsúlya hosszú távon biztosíthatja a terrorszervezetek polgári támogatását a katonai erejük csökkenését követően is.

A katonai lehetőségek és a NATO fogadalma[11]

Az információfegyver köztes hatalmi erőként *(medium power)* csekély anyagi ráfordítás mellett hatékony eszközzé fejlődött. A reflexió kialakításának hagyományos védelmi kérdései a három alapvető katonai dimenzióban (térben, időben, erőben) már nem kezelhető. Az információ (legyen az nyílt vagy titkos) mint a hatalmi aktivitás egyik folyamatosan jelenlévő eleme a közvetlen fizikai erőszak alkalmazása nélkül, pusztán az erőkivetítés révén mind a támadások, mind a támadások elleni állami fellépések, reflexiók jellemző, meghatározó része. A kiberműveletek az információfegyver alkalmazásának egyik legjelentősebb részét alkotják. A NATO által bevont szakértők által összeállított Tallinn Manual és a Tallinn Manual 2.0 elnevezésű dokumentumokban a kollektív védelmet már a kibertérben is értelmezik.[12] A NATO a kiberhadviseléssel kapcsolatos politikai nehézségek miatt, a már említett védelem legszélesebb körű biztosítása okán, olyan mechanizmusok és egyértelmű jogi normák kidolgozásának

[11] Vö. Farkas Ádám – Pongrácz Alex: Az állam fegyveres védelmének állam- és jogelméleti alapjai. In Farkas Ádám (szerk.): *A honvédelem jogának elméleti, történeti és kortárs kérdései.* Budapest, Dialóg Campus, 2018. 9–30; Kelemen Roland – Simon László: A kibertérben megjelenő fenyegetések és kihívások kezelésének egyes nemzetközi jogi problémái. In Farkas Ádám – Végh Károly (szerk.): *Új típusú hadviselés a 21. század második évtizedében és azon túl – intézményi és jogi kihívások.* Budapest, Zrínyi, 2020. 150–171.

[12] Michael N. Schmitt (szerk.): *Tallinn Manual 2.0 on the international law applicable to cyber operations – Prepared by the International Groups of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence.* Cambridge, Cambridge University Press, 2017. 354.

szükségességéről nyilatkozik, amelyek egyértelmű iránymutatásul szolgálhatnak.[13] A szervezet 2014-es walesi csúcsértekezletének záródokumentumában kimondta, hogy a NATO alapvető feladatainak teljesítéséhez továbbfejleszti a kibervédelmi politikát.

> „A politika megerősíti a szövetségesek biztonságának, valamint a megelőzésnek, a felderítésnek, a rugalmasságnak, a helyreállításnak és a védelemnek a megosztására vonatkozó elveket. Emlékeztet arra, hogy a NATO alapvető kibervédelmi felelőssége, hogy megvédje saját hálózatait, és hogy a szövetségeseknek nyújtott segítséget a szolidaritás szellemében kell kezelni, hangsúlyozva a szövetségesek felelősségét a nemzeti hálózatok védelméhez megfelelő képességeik fejlesztése érdekében."[14]

A NATO 2016-os varsói csúcstalálkozóján elfogadott dokumentumában (angolul: Cyber Defence Pledge) állami, nemzeti szintű reflexiókat vállaltak, miszerint fejlesztik és még inkább kiterjesztik a nemzeti kibervédelmet, a kialakult kibervédelmi gyakorlatokat, szisztémákat, a fenyegetéssekkel kapcsolatos ismereteket, tapasztalatokat a „legjobb gyakorlat" kialakítása céljából a szövetségesek kicserélik, és támogatják a képzéseket, a tréningeket vagy a közös gyakorlatokat egy közös tudásbázis kialakításához.[15]

A kiberpartizán a kulcs[16]

A korábban megfogalmazott és vállalt védelmi kötelezettségek teljesítését, az állami reflexiók mindegyikét annak a tudásnak a birtokában javasolt megtenni, amely gátolja a terror spiráljának kialakulását. Ennek kulcsa egyértelműen az agressziót, a terrort jogosan alkalmazó harcos és a jogtalanul használó elkövető elkülönítése, a katonai és a bűnügyi jelleg alapvető elhatárolása. A nemzetközi jog elfogadott értelmezése szerint a partizánkatona cselekedetei jogosak. A partizán harcának, agressziójának a középpontjában mindig is a folyton fejlődő technikai eszközök fegyverként történő alkalmazása áll. A fegyveres konfliktusokhoz kapcsolódó erőkivetés kognitív hatásainak vizsgálata során a leghatékonyabb

[13] Terence Check: Book review: Analyzing the effectiveness of the Tallinn Manual's Jus Ad Bellum Doctrine on cyberconflict: A NATO-centric approach. *Cleveland State Law Review,* 63. (2015), 2. 500–501.

[14] Kelemen–Simon (2020): i. m. 167.

[15] Cyber defence pledge. *NATO Press Release,* 2016. július 8.

[16] Az itt használt partizánfogalmat a Cs. Kiss Lajossal folytatott „erőszak-félelem-biztonság" diskurzus alapozta meg. A hagyományos és nemzetközi jogi értelemben a harcoló és a fegyveres agressziót elkövető személyek fogalmi elhatárolására szolgáló elnevezésként javaslom a fogalom értelmezését. Vö. Carl Schmitt: *A politikai fogalma*. Ford. Cs. Kiss Lajos. Budapest, Osiris – Pallas Stúdió – Attraktor, 2002.

technikai eszközöknek az infokommunikációs rendszerek bizonyulnak. A kibertérben megjelenő agresszor elkülönítése tehát akkor szolgálhatja az erőszak felszámolását, ha az a partizánelmélet alapján történik. Vagyis a cselekmények során kiemelt figyelmet kell fordítani az elkövető politikai céljaira és össztársadalmi jelentőségű célpontjaira. A már említett polarizált egyének és közösségek társadalmi és állami kötelezettségtől mentesen, akkor is partizán módjára kívánják befolyásoló küzdelmüket folytatni, ha törekvésük mögött más, társadalmilag inkább elítélhető bűnelkövetési szándék áll.

Az agresszió legkézzelfoghatóbb közege jelenleg a kibertér, és a fent említett logika alapján a biztonsági szegmensek fejlődése ellenére is az marad. Az infokommunikációs tér adta lehetőségek felmérése és felhasználása mind az elkövetők azonosítására, mind az ellenük szükséges fellépés megszervezésére alkalmasnak bizonyulhat. A fizikai és a földrajzi határokon túl- és átlépő terror ellen csak a tudatos és hiteles kommunikáció lehet az ellenszer – vagyis az információfegyver nemzeti szintű alkalmazása, amely a társadalom tagjainak legszélesebb támogatásával bír. Ez azt jelenti, hogy az „egyének valós idejű tájékozottságának növelése, illetve biztonságtudatosságuk fejlesztése elengedhetetlen közös érdek".[17] A kibertérben, a hadviselés legújabb hadszínterén olyan legitim információs műveletek hajthatók végre, amelyek egyéni és közösségi megítélése nem megosztó. A támadások elleni fellépés során az egyéni reflexiók sikeressége pontosan a kognitív hatások elmaradása miatt elhanyagolható. Az arctalan, etikus hacker támadása egy másik hacker ellen a „virtuális virtusok" szintjén értelmezhető. A társadalmi reflexiók esetében a NATO eddigi válaszai viszont elvezethetnek egy olyan egyensúlyi helyzethez, amelyben pontosan a virtuális térben felmutatott állami szintű erőkivetítés révén fejthető ki a szükséges kognitív hatás. Amennyiben tehát a NATO által is nemzeti szinten megvalósíthatónak vélt válaszok, állami reflexiók képesek lesznek azonosítani az információfegyver alkalmazóját, és bizonyítják az agresszió jogelméletileg legitim vagy illegitim voltát – a támadás katonai jellegét –, akkor az elkövető elleni ön- és honvédelmi (katonai) megalapozott fellépés meghozhatja a közösség támogatását. A kognitív szférában közvetetten megjelenő katonai cselekményekre adott legitim katonai válaszok rövid és hosszú távon is csökkenthetik a félelemérzetet, még akkor is, ha valóságos fegyveres konfliktusokhoz kapcsolódnak. A kibertérben kialakítandó védelem megszervezése során a kiberpartizán fogalmának társadalmi elmélyítése valós biztonságérzetet eredményezhet. A fegyveres harcok a történelemben eddig is rendre az erősebb fél győzelmével zárultak. A kibertér, amely a valós fegyveres küzdelem kiegészítő, ugyanakkor akár egyenrangú és önálló hadszíntere is

[17] Simon László – Magyar Sándor: A terrorizmus és indirekt hatása a kiberterében. *Nemzetbiztonsági Szemle,* 5. (2017), 3. 89–101.

lehet, az erőkivetítés révén éri el értelmét. Amennyiben valamennyien megértjük Schmitt[18] kiemelését, miszerint „a partizán problémája a reguláris és irreguláris harc viszonyának problémája", akkor meggyőződésem szerint nemcsak a hagyományos hadszíntereken és a kibertérben tudjuk az egyének és a közösségek szintjén elfogadhatóan megszervezni a védelem szempontjából fontos és szükséges intézkedéseket, de új értelmet tudunk adni azon társadalmi elvárásoknak is, amelyek államelméleti szempontból érzékelhető jelenségek és történések jogelméleti változását vagy megalkotását is eredményezhetik.[19]

[18] Schmitt (2002): i. m.

[19] Álljon itt tehát köszönetem is Cs. Kiss Lajos támogatásáért, hiszen az általam jogelméleti problémaként megfogalmazott kérdésre, miszerint „arra az ismeretlennek tűnő valamire, ami megy valahova" arra lehet-e reagálni, bölcsen olyan tudományos inspirációval reflektált, amely eredményeiben meggyőződésem szerint kiállja majd az idő próbáját, legalább olyannyira, mint a mottómban szereplő székely vicc.

Felhasznált irodalom

Az MHTT Konferenciája: Az aszimmetrikus hadviselés. *Hadtudomány,* 25. (2015), 1–2. Online: http://mhtt.eu/hadtudomany/2015/1_2/2015_1_2_7_KONFERENCIA.pdf

Bell, David: *Cyberculture theorists – Manuel Castells and Donna Haraway.* London – New York, Routledge, 2007. Online: https://doi.org/10.4324/9780203357019

Check, Terence: Book Review: Analyzing the effectiveness of the Tallinn Manual's Jus Ad Bellum Doctrine on cyberconflict: A NATO-centric approach. *Cleveland State Law Review,* 63. (2015), 2. 500–501. Online: https://engagedscholarship.csuohio.edu/clevstlrev/vol63/iss2/12

Cyber defence pledge. *NATO Press Release,* 2016. július 8. Online: www.nato.int/cps/en/natohq/official_texts_133177.htm

Farkas Ádám (szerk.): *A honvédelem jogának elméleti, történeti és kortárs kérdései.* Budapest, Dialóg Campus, 2018. Online: https://tudasportal.uni-nke.hu/tudastar-reszletek?id=123456789/12623

Farkas Ádám – Pongrácz Alex: Az állam fegyveres védelmének állam- és jogelméleti alapjai. In Farkas Ádám (szerk.): *A honvédelem jogának elméleti, történeti és kortárs kérdései.* Budapest, Dialóg Campus, 2018. 9–30. Online: https://tudasportal.uni-nke.hu/tudastar-reszletek?id=123456789/12623

Kelemen Roland – Simon László: A kibertérben megjelenő fenyegetések és kihívások kezelésének egyes nemzetközi jogi problémái. In Farkas Ádám – Végh Károly (szerk.): *Új típusú hadviselés a 21. század második évtizedében és azon túl – intézményi és jogi kihívások.* Budapest, Zrínyi, 2020. 150–171. Online: http://real.mtak.hu/113201/1/Bartk%C3%B3-Farkas.pdf

Kereki Ádám: A kritikus infrastruktúra meghatározásának módszerei, különös tekintettel a magyar honvédelmi infrastruktúrára. Farkas Ádám (szerk.): *A honvédelem jogának elméleti, történeti és kortárs kérdései.* Budapest, Dialóg Campus, 2018. 151–166. Online: https://tudasportal.uni-nke.hu/tudastar-reszletek?id=123456789/12623

Schmitt, Carl: *A politikai fogalma.* Ford. Cs. Kiss Lajos. Budapest, Osiris – Pallas Stúdió – Attraktor, 2002.

Schmitt, Michael N. (szerk.): *Tallinn Manual 2.0 on the international law applicable to cyber operations – Prepared by the International Groups of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence.* Cambridge, Cambridge University Press, 2017. Online: https://doi.org/10.1017/9781316822524

Simon László – Magyar Sándor (2017): A terrorizmus és indirekt hatása a kiberterében. *Nemzetbiztonsági Szemle,* 5. (2017), 3. 89–101. Online: https://folyoirat.ludovika.hu/index.php/nbsz/article/view/1685