LEGÁRD ILDIKÓ

A barát és ellenség megkülönböztetése a kibertérben

I. PROBLÉMAFELVETÉS

A 20. század végére a számítógépes rendszerek, valamint az általuk (is) reprezentált digitális világ lassan behálózták a mindennapi életünket, így már a fejlett társadalmak működése – a közigazgatáson, a mindennapi közműszolgáltatásokon, a telekommunikáción, a közlekedésen keresztül a gazdasági életen át a honvédelemig – elképzelhetetlen az információs technológiákra épülő infrastruktúrák alkalmazása nélkül. Napjainkra az egyik legértékesebb tényező az adat, az információ lett – Nicholas Negroponte szavaival élve az atomok világát felváltotta a bárhol és bármikor előállítható bitek korszaka[1] –, melyek megszerzéséért kíméletlen harc indult el, különböző „frontok" nyíltak, új „hadszínterek" keletkeztek, nemcsak a globalizált világgazdaságban, az államok és a transznacionális képződmények versengésében,[2] hanem az egyes államok társadalmi életének szinte minden területén. Az állítás igazsága különösen nyilvánvaló, ha az államok és szövetségeik közötti politikai-diplomáciai-katonai érintkezések békés és háborús formáit, a nyílt és rejtett, azaz a normál társadalom számára láthatatlan „hadszíntereket" vizsgáljuk. A modernitás legújabb fejleménye, hogy a hadszíntér „hagyományos" fizikai-szociális dimenziói kiegészültek az úgynevezett virtuális dimenziókkal, s kezdetét vette az államok információs rendszerei között zajló „virtuális" háború, amely különböző formákat ölt, s jelen van a társadalmi-kulturális élet szinte minden területén. Az új információs hadviselés egyik legfontosabb színtere a kibertér lett, melynek stratégiai jelentősége folyamatosan nő. A kibertérben végrehajtott támadások, az ún. kiberháború, a hagyományos hadviseléstől eltérő jellemzőkkel bír. A támadó fél kiléte gyakran minden kétséget kizáró módon nem bizonyítható, mivel a támadó cselekményt nem előzi meg hadüzenet, nem kapcsolódnak közvetve vagy közvetlenül fegyveres konfliktushoz, nem viselnek katonai egyenruhát vagy jelvényt, amely alapján meg lehetne különböztetni őket, és személyük felfedhetetlensége alapvető érdekük. Ebből következően annak megítélése, hogy a megtámadott fél kivel szemben alkalmazzon bármilyen védelmi intézkedést, esetleg ellentámadást, számos nehézségbe ütközik. A kibertámadások további

[1] Negroponte, 2002, 18., 129.
[2] Vö. Pongrácz, 2019.

jellemzője, hogy azokat a legváratlanabb pillanatban, sok esetben több fronton egyszerre követik el, sőt gyakran magára a támadásra sem azonnal derül fény, hanem csak a károk bekövetkezése esetén. A támadók jellemzően nem, vagy nemcsak egy másik állam fegyveres egységeit támadják, hanem az állami szerveket, a társadalmat a legkülönbözőbb területeken, illetve magát az egyént.

Ahhoz, hogy az államok ki tudják alakítani a kibertámadásokkal szembeni szükséges védelmi képességeket, hozzásegíthet, ha megértjük a 20. század egyik legjelentősebb jogtudósának, államelméleti gondolkodójának, a közjogász Carl Schmittnek a „politikairól" (das Politische) alkotott elméletét, amelyet *A politikai fogalma* (Der Begriff des Politischen) című írásában fejtett ki. Az írás első változata 1927-ben jelent meg, majd több átdolgozott kiadás után, 1963-ban jelent meg a véglegesnek tekinthető szövege, Előszóval és három korolláliummal kiegészítve.[3] Ugyanebben az évben jelentette meg a partizán politikai jelentőségét, világtörténelmi szerepét elemző munkáját *A partizán elmélete* (Theorie des Partisanen. Zwischenbemerkung zum Begriff des Politischen) címmel, amely a politikai fogalmának a kiegészítése, konkretizálása és továbbgondolása.[4] A partizánelméletnek *A politikai fogalmához* való tartozására nemcsak az írás alcíme utal, hanem az 1963-as kiadás Előszava is, amelyben külön kitér a két mű szoros összetartozására: „Az 1932-es újranyomtatott szöveget valamennyi hiányosságával együtt, mint dokumentumot kell a nyilvánosság elé terjeszteni. Tárgyilag az írás legfőbb fogyatékossága abban rejlik, hogy az ellenség különféle fajtáit – konvencionális, valóságos vagy abszolút ellenséget – nem különbözteti meg, és nem választja el világosan és kellő szabatossággal... A kérdés megvitatása ellenálhatatlanul folytatódik és valódi haladást idéz elő a tudatban. Mert a háború új, korszerű fajtái és módszerei az ellenségesség jelenségére való eszmélődésre kényszerítenek. Egy önálló, *A partizán elméletéről* szóló, e szöveg újranyomásával egyidejűleg megjelenő értekezésben ezt különösen aktuális és akut példán mutattam be. Egy másik hasonlóképpen nyomatékos példával szolgál az úgynevezett hidegháború."[5] Tekintettel a hidegháború utáni világrend új helyzetére, valamint az infokommunikációs állam és társadalom új struktúráira, Schmitt állításához hozzá kell illesztenünk, hogy a kiberhadviseléssel, mint az ellenségesség és a háború új formájával kell szembe nézni. A tisztán formális, a barát és ellenség megkülönböztetéseként és csoportosításaként meghatározott politikai fogalma, kiegészítve a partizánelmélettel, komoly segítséget nyújthat a politikai ellenségként azonosított kibertámadó megértéséhez, a vele szemben alkalmazandó komplex védelmi intézkedések meghatározásához.

[3] Vö. Schmitt, 2002b.
[4] Schmitt, 2002a.
[5] Schmitt, 2002b, 13.; A problémához lásd Szabó, 2003, 68., 73.; Cs. Kiss, 2020.

Ehhez kapcsolódva, Schmitt elmélete ugyancsak jelentős támaszt nyújthat a virtuális-kiber fronton is támadó, a 21. század egyik legintenzívebb és legsúlyosabb politikai fenyegetését jelentő terrorista „egzisztenciájának", lélektani-szociális-politikai mozgatórugóinak, s egyáltalán a kiberhadviselést is folytató modern terrorizmusnak az értelmezéséhez.

II. A POLITIKAI FOGALMA

Schmitt az állam fogalmát a politikai fogalmával kapcsolja össze, véleménye szerint „az állam fogalma előfeltételezi a politikai fogalmát".[6] A politikai fogalma meghatározásához olyan sajátos, kizárólag a politikára jellemző kritériumok megállapítása szükséges, amelyekre minden politikai cselekvés visszavezethető. Ez a végső disztinkció nem más, mint a barát és ellenség megkülönböztetése, melynek értelme, hogy „megjelölje az összekapcsolódás vagy szétválás, az egyesülés vagy szétbomlás intenzitásának legvégső fokát. (...) A politikai ellentét a legintenzívebb, legvégső ellentét, és minden konkrét ellentétesség annál inkább politikaivá válik, minél inkább közeledik a legszélső ponthoz, a barát/ellenség csoportosításhoz."[7] Az ellenség nem versenytárs vagy ellenfél általában véve, fogalmához hozzátartozik a harc, a háború reális lehetősége, mint az ellenségesség legvégső, legszélsőségesebb megvalósítása.[8]

Schmitt szerint amíg egy nép a politikai szférájában, azaz államként létezik, addig e népnek magának kell meghatároznia a barát és ellenség megkülönböztetését, mivel ebben rejlik politikai egzisztenciájának lényege. Amennyiben már nem képes meghatározni, vagy helyette egy idegen határozza meg, hogy ki számít ellenségnek és ki ellen lehet vagy kell háborút folytatni, akkor ez az állam politikailag megszűnik létezni, népe pedig már nem szabad nép, politikailag betagozódik vagy alárendelődik egy másik politikai rendszernek.[9]

Schmitt hangsúlyozza, hogy a normális állam teljesítménye elsősorban abban áll, hogy saját területén megteremti a biztonságot, nyugalmat, megelégedettséget, és fenntartja a rendet. Ugyanakkor, ha úgy ítéli meg, hogy a konkrét konfliktushelyzetben saját egzisztenciája, életmódja veszélyeztetve van, saját maga dönthet úgy, hogy az idegent (külpolitikai) ellenségnek nyilvánítja, és ellene háborút indít. A háborúindítás joga, az úgynevezett *jus belli* egyrészt azt jelenti, hogy az állam megköveteli a saját népének bizonyos tagjaitól, hogy harcba menjenek és esetleg életüket adják a hazáért, másrészt életeket oltsanak ki az ellenség oldalán.[10] Amennyiben az államon belüli ellentétek

[6] Schmitt, 2002b, 15.
[7] Schmitt, 2002b, 21-22., 25.
[8] Schmitt, 2002b, 27.
[9] Schmitt, 2002b, 42.
[10] Schmitt, 2002b, 38.

nagyobb intenzitásra tesznek szert, mint a másik állammal szembeni közös külpolitikai ellentét, ha a pártpolitikai ellentétek politikai ellentétekké válnak és az államon belüli barát/ellenség csoportosítások lesznek a meghatározóak a fegyveres összecsapás szempontjából, ekkor már polgárháborúról kell beszélnünk. Tehát míg „a háború szervezett politikai egységek közötti fegyveres harc, a polgárháború fegyveres harc egy (ezáltal problematikussá váló) szervezett egységen belül".[11] Ahhoz, hogy az állam a külső és belső ellenséggel szemben egyaránt kialakítsa a megfelelő védelmi és reagálási képességeket, nélkülözhetetlen a fegyveres apparátusainak megerősítése, funkcionális és strukturális differenciálódása.

Történelmileg a XIX. század vége, XX. század eleje jelentős változást hozott az államok életében; kialakultak a korábbi központosító és professzionális igazgatásra épülő abszolutista államok, valamint a 19. századi polgári-liberális állam talaján a Schmitt által „totálisként" fémjelzett állam modellje, mely egyetlen tárgyi területtel, mint például vallás, kultúra, gazdaság stb. sem közömbös, potenciálisan minden területet megragad, és az állam, illetve társadalom azonosságát hangsúlyozza. Az állami beavatkozás szinte minden viszonyt áthat és érint. A totális államban ennek következtében „minden politikai, és az államra való hivatkozás képtelen arra, hogy a »politika« specifikus megkülönböztető ismertetőjegyét megindokolja".[12]

A 20. század azonban nemcsak az államok, hanem, ahogyan Schmitt fogalmaz, a háború totálissá válását is eredményezte. Az első és második világháború, az azt követő hidegháborús időszak, a fegyverkezési verseny és a hihetetlen léptékű technikai fejlődés visszafordíthatatlan következményekkel járt, melyek révén elvesztette jelentőségét a harctér és hátország közötti megkülönböztetés, a háború minden lehetséges hadszíntéren – földön, vízen, levegőben, napjainkra már a világűrben és a kibertérben is – egyszerre zajlik, megfeledkezve a polgári részvételről, valamint az ellenfelek minden lehetséges erőforrást bevetnek a győzelemért.[13] A háború totálissá válása lényege abban rejlik, hogy a nem katonai tárgyi területek (pl. gazdaság, a nem hadviselő felek) is érintetté válnak az összecsapásokban, megszűnik a katona és a polgár, az állam és a társadalom, a front és a haza közötti különbség, az ellenségesség még intenzívebbé válik. A győzelem érdekében az államok minden rendelkezésre álló anyagi és szellemi erőforrást központosítanak és bevetnek, tehát a totális háború totális erőfeszítést követel meg a résztvevőktől. A tömegpusztító fegyverek megjelenésével megjelent az ellenségesség abszolutizálásának új formája, mely az ellenség teljes megsemmisítésének reális lehetőségét hordozza magában.[14]

Schmitt a totális állam és a totális háború fogalmát a szuverenitás kérdésével

[11] Schmitt, 2002b, 27.
[12] Schmitt, 2002b, 19.
[13] Farkas, 2013, 166-167.
[14] Cs. Kiss, 2020, 492-493.

kapcsolja össze, mert szerinte „szuverén az, aki a kivételes állapotról dönt”.[15] A totális háború pedig kivételes állapotot eredményez, melyben a szuverén állam hoz politikai döntést az egzisztenciáját veszélyeztető ellenségről és az ellene alkalmazandó legszélsőségesebb eszközről, a háborúról.[16]

III. AKTUÁLIS FENYEGETÉSEK

A modern állam fejlődésének legújabb szakaszában, mint azt Schmitt pontosan előre jelezte, „roppant intenzitású új hatalmi eszközökkel és lehetőségekkel rendelkezik, melyek horderejének végső jelentőségét és következményeinek hatását egyelőre aligha sejtjük, mert szókincsünk és képzeletvilágunk mélyen a XIX. században gyökerezik”.[17] Schmitt a történelmi fejlődés ívét vizsgálva pontosan látta, hogy a totális állam és a totális háború 20. századi megjelenése olyan új, minden korábbinál összetettebb fenyegetések megjelenését vonja maga után, amelyek új típusú válaszok megfogalmazására késztetik az államalakulatokat.

Az utóbbi évtizedekben bekövetkező hihetetlen léptékű technikai fejlődés, a globalizáció, az információs hálózatok elterjedése, a digitális világ, ahogy Simon László megfogalmazta *A partizán elmélete a premodern virtuális korban* című tanulmányában, „kinyitotta Pandóra virtuális szelencéjét, és a hálózati kapcsolatok révén mindenki áldozattá vált. A számítógépek és az »okos« eszközeink révén bárhol, bármikor, bárki megtámadható. A technológiai fejlettség kapcsán jelenleg még beazonosíthatatlan elkövetők, közvetlenül vagy közvetve törnek életünkre, okoznak felbecsülhetetlen anyagi, de még erkölcsi károkat is”.[18] Az Amerikai Egyesült Államokat ért 2001. szeptember 11-i terrortámadás és az azt „követő politikai és katonai lépések rávilágítottak a 21. század új kihívásaira, a gyakran arctalan ellenség képére, a fizikai térből kilépő és több dimenzióban, párhuzamosan folyó háborúk lehetőségére”.[19]

Az elkövetők nagyon gyakran a fizikai térben megvalósuló támadásokkal párhuzamosan, vagy anélkül önállóan alkalmazva, támadást indítanak a nehezen megragadható és láthatatlan virtuális térben, ahol „a műveletek célkitűzéseinek elérése érdekében, kognitív képességekkel (befolyásolás, tájékoztatás) közvetlenül, illetve technikai képességekkel (ellentevékenység, védelem) közvetetten hatásokat gyakorolnak a műveletekben részt vevő célközönség (szemben

[15] Schmitt, 1992; idézi: Farkas, 2015, 7.
[16] A totális állam és totális háború kérdésével jelen írás terjedelmi korlátai miatt részletesebben nem foglalkozom. A témához lásd Cs. Kiss, 2010, 19-40.; Cs. Kiss, 2017, 4-47.; Cs. Kiss, 2020; Farkas, 2015; Farkas, 2013; Farkas, 2018; Pongrácz, 2018.
[17] Schmitt, 2002a, 5.
[18] Simon, 2017, 236.
[19] Simon – Magyar, 2017, 90.

álló fél, saját erők, civil szereplők) szándékára, helyzetértelmezésére és képességeire".[20] Az úgynevezett információs műveletek,[21] és ennek révén a modern hadviselés egyik legfontosabb színterévé a kibertér vált.

IV. A KIBERTÉR, MINT ÚJ HADSZÍNTÉR

A kibertér fogalmát nem könnyű definiálni, hiszen a technológiai fejlődésnek köszönhetően annak tartalmi elemei folyamatos változáson mennek keresztül. A téma egyik legjelentősebb hazai szakértője, Haig Zsolt 2018-ban az alábbi meghatározást közölte: „Az ember által mesterségesen létrehozott, dinamikusan változó tartomány, amelyben az információ gyűjtését, tárolását, feldolgozását, továbbítását és felhasználását végző, egymással hálózatba kapcsolt és az elektromágneses spektrumot is felhasználó infokommunikációs eszközök és rendszerek működnek, lehetővé téve ezzel az emberek és a különféle eszközök közötti folyamatos és globális kapcsolatot."[22] Jól elkülöníthető a kibertér felől érkező fenyegetések négy fajtája: a kiberbűnözés, a hacktivizmus és kiberterrorizmus, a kiberkémkedés és a kiberhadviselés.[23] Ez utóbbi részeként a kiberműveleteknek három területét különböztethetjük meg: a kiber információszerzést, a kibervédelmet és a kibertámadást.[24] A hagyományos hadviseléshez képest azonban a kibertérben eddig még nem volt azonosítható kölcsönös támadások és ellentámadások eseményegyütteseként végrehajtott műveletsor.[25]

Bár a szakirodalom szerint a legelső dokumentált informatikai támadást 1997-ben egy Sri Lanka-i terrorszervezet, a tamil tigrisek követték el, számos szerző egyetért abban, hogy az 1982-es szibériai gázvezeték-robbanás[26] is már előrevetítette a jövő kibertámadásait. Az Egyesült Államok, nevezetesen a CIA – megakadályozandó, hogy a Szovjetunió embargós nyugati technológiához jusson – egy kanadai vállalaton keresztül szoftvert adott el a szovjeteknek, amelybe olyan hibákat építettek be, amelyek néhány hónapos kifogástalan működés után összezavarták a nyersanyagvezeték irányítási rendszerén keresztül a szállítási folyamatokat. Ennek eredménye az eddigi legnagyobb, nem nukleáris eredetű robbanás volt, amely a szovjet gazdaságot is megrázta.[27]

[20] Haig, 2018, 210.
[21] Információs műveletek: Az információs környezetben érvényesülő információs képességek integrált, összehangolt és koordinált alkalmazására irányuló tevékenységek összessége, amelyek a műveletek célkitűzéseinek elérése érdekében, kognitív képességekkel közvetlenül, illetve technikai képességekkel közvetetten hatásokat gyakorolnak a műveletekben részt vevő célközönség szándékára, helyzetértelmezésére és képességeire (Haig, 2018, 15.).
[22] Haig, 2018, 15.
[23] Krasznay, 2012, 143-144.
[24] Kelemen – Pataki, 2015, 72.
[25] Kralovánszky, 2019, 199.
[26] Wired.com, 2004.
[27] Berki, 2013, 174-175.

1999-ben szerb hackerek – a NATO szerbiai bombázásaira válaszul – megtámadták a NATO-parancsnokság szervereit, és néhányat DDoS (Distributed Denial of Service)[28] módszerrel tettek átmenetileg elérhetetlenné, valamint feltörtek számos weboldalt, és propaganda céllal üzeneteket helyeztek el rajtuk.

Az első, kifejezetten állam ellen indított kibertámadást 2007-ben, Észtországgal szemben követték el, a tallini szovjet hősi emlékmű eltávolítása és az azt követő zavargások után pár nappal. A túlterheléses (DDoS) támadásokat minisztériumok, kormányhivatalok, a parlament, illetve telefontársaságok, bankok és médiacégek szerverei, tehát az ország elsősorban kritikus infrastruktúrái[29] ellen követték el. Az ország adatforgalmát irányító kulcsfontosságú szerverek naponta omlottak össze, sok állami intézmény hálózatát kénytelenek voltak ideiglenesen leválasztani az Internetről. Az elektronikus banki forgalom és kereskedelem részint megszűnt, részint erősen akadozott.[30] Az akció mind Észtországot, mind a NATO-t felkészületlenül érte, pedig kivitelezéséhez csekély erőforrásokra volt szükség.[31]

A 2008 augusztusában kitört orosz–grúz háborúnak is volt kiber aspektusa. A hosszú évek óta tartó grúz–oszét és a grúz–abház konfliktust a grúz elnök 2008. augusztus 8-án katonai úton próbálta megoldani az említett területek megtámadásával, melyre válaszul Oroszország fegyveres válaszcsapásokat indított, mellyel egyidőben megindult Grúzia ellen egy kiberhadjárat is. Az internetforgalmat Oroszország az ellenőrzése alá vonta, az ország kormányzati weboldalait kívülről megbénították, illetve tartalmukat kicserélték. Az orosz földről érkezett hackerek Mihail Szakasvili elnök portréját is manipulálták. Az államfő képére Hitler-bajuszt rajzoltak, és egy sor olyan képet tettek ki róla az oldalra, ahol a német diktátor pózaiban ábrázolták, vagy a történelem nagy gonosztevői közé kopírozták be az arcmását. A megtámadott oldalak között volt az elnök saját weblapja mellett a grúz külügy- és hadügyminisztérium is. Emellett olyan dezinformációs céllal létrehozott weboldalak is megjelentek a világhálón, melyek az ország lejáratására irányultak.[32]

[28] DDoS: Elosztott szolgáltatás-megtagadással járó támadás. Egy számítógép-hálózati szolgáltatás teljes vagy részleges megbénítása, helyes működési módjától való eltérítése ártó, támadó szándékkal, elosztottan, több forrásból (vö. Haig – Kovács, 2008, 61-70.).

[29] Hazánkban a kritikus infrastruktúrák védelmével kapcsolatos előírásokról a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény rendelkezik. Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény (továbbiakban: Ibtv.) 1.§ (1) 33. pontja meghatározása szerint létfontosságú információs rendszerelem az európai létfontosságú rendszerelemmé és a nemzeti létfontosságú rendszerelemmé törvény alapján kijelölt létfontosságú rendszerelemek azon elektronikus információs létesítményei, eszközei vagy szolgáltatásai, amelyek működésképtelenné válása vagy megsemmisülése az európai létfontosságú rendszerelemmé és a nemzeti létfontosságú rendszerelemmé törvény alapján kijelölt létfontosságú rendszerelemeket vagy azok részeit elérhetetlenné tenné, vagy működőképességüket jelentősen csökkentené.

[30] Berki, 2016, 265-266.

[31] Kovács – Krasznay, 2010, 45.

[32] Berki, 2013, 175-176.

2010-ben Irán ellen indult támadás, melynek során a Natanzban található urándúsító ellen bevetették a Stuxnet elnevezésű rosszindulatú kódot, mellyel az urándúsító centrifugákat akarták észrevétlenül tönkretenni, és a dúsítási folyamatot megzavarni. Ezt a célt a Stuxnet sikeresen el is érte, hisz legalább 1000 centrifugát tett használhatatlanná, és mértékadó vélekedések szerint legalább két évvel vetette vissza az iráni atomprogramot.[33]

Az új típusú támadások jelentőségét és gyakoriságát mutatja, hogy a NATO 2014-ben a kollektív védelem alapvető részévé nyilvánította a kibervédelmet, majd 2016-ban a varsói csúcson az állam- és kormányfők új műveleti környezetként ismerték el a kiberteret, melyben a NATO-nak ugyanolyan hatékonyan kell védekeznie, mint a szárazföldön, a tengeren vagy a levegőben.[34] Többek között kinyilvánították, hogy a számítógépes támadások veszélyt jelentenek a Szövetség biztonságára, amire ugyanolyan hatásuk lehet, mint a hagyományos fegyvereknek.[35]

Az elmúlt években minden kétséget kizáróan bebizonyosodott, hogy a kibertérben az államok fegyveres ereje jelen van, így nagyon fontos kérdés, hogy egy általuk kivitelezett támadást hogyan kell értékelni a nemzetközi jog és a megtámadott állam nézőpontjából. Tekinthető-e egy kibertérben indított támadás az ENSZ Alapokmánya 51. cikke[36] szerinti fegyveres támadásnak?[37] A kérdésnek azért is van kiemelkedő jelentősége, mert az ENSZ Alapokmánya (2. cikk (4) bekezdés) deklarálja a fegyveres erőszak tilalmát, mely alól pusztán két kivétel van: amennyiben az ENSZ Biztonsági Tanácsa felhatalmazást ad fegyveres erő alkalmazására, illetve fegyveres támadás esetén az egyéni és kollektív önvédelmi jog gyakorlása. Ez utóbbi, tehát az önvédelmi jog gyakorlása megítélésében a nehézséget az okozza, hogy a „fegyveres támadás" fogalmát sem az Alapokmány, sem későbbi dokumentumok nem határozzák meg.[38] A nemzetközi szokásjog alapján azonban a „fegyveres támadás" minősítéshez két feltételnek kell teljesülnie: 1) a cselekménynek el kell érnie egy rendkívüli súlyt vagy intenzitást; valamint 2) a támadást elkövető személyek cselekménye valamely másik államnak betudhatónak kell lennie.[39]

Annak eldöntése, hogy a támadás az önvédelem jogos gyakorlásához szükséges súlyt és intenzitást elérte-e, a megtámadott állam értékítéletén múlik, ez az érintett állam saját döntése. Ezzel a nemzetközi jog viszonylag széles mozgásteret enged az államoknak a politikai kérdésében (ki az ellenség?) való döntéshez, azaz „minden résztvevő maga dönti el, hogy az idegen más-léte a konkrétan fennforgó konfliktushelyzetben az egzisztencia saját fajtájának a tagadását jelenti-e, s ezért az idegent elhárítja vagy harcban legyőzi, hogy megőrizze saját,

[33] Vö. Berki, 2013, 176-178.
[34] Berki, 2016, 273.
[35] Simon – Magyar, 2017, 92.
[36] 1956. évi I. törvény az Egyesült Nemzetek Alapokmányának törvénybe iktatásáról.
[37] Kelemen – Pataki, 2015, 54.
[38] Kelemen – Pataki, 2015, 66-67.
[39] Sulyok, 2005, 34.; Kelemen – Pataki, 2015, 68.

léte jellegének megfelelő életmódját".[40] Természetesen ez a joga csak addig tart, ameddig az ENSZ Biztonsági Tanácsa nem teszi meg a szükséges intézkedéseket a béke és a biztonság helyreállítása érdekében.[41]

A második feltétel, tehát a támadó kiléte a kibertámadások esetében nehezen bizonyítható, még akkor is, ha valószínűsíthetően valamely állam áll a támadás mögött. Természetesen, ha a súlyos mértékű és intenzitású kibertámadást egy állami szerv követte el, valamint ez kétséget kizáróan bizonyítható, akkor az fegyveres támadásként azonosítható, és amennyiben a szükségesség és arányosság követelményének megfelel,[42] akkor vele szemben akár fegyveres támadás is indítható. Azonban a kibertámadások hátterében legtöbbször feltételezett elkövetőként megjelölt Egyesült Államok, Izrael, Oroszország, Kína vagy Észak-Korea sosem ismerte el egyik esetben sem érintettségét, és minden kétséget kizáró bizonyítékot sem lehetett felmutatni velük szemben.[43]

A fő kérdés jelen esetben, hogy a megtámadott állam hogyan, mi alapján értékelje az ellene indított támadást, ha a támadó fél kiléte egyértelműen nem határozható meg, hogyan dönthet így az ellenséggé nyilvánításról és a támadóval szemben alkalmazandó válaszlépésekről?

A nemzetközi joggyakorlat alapján, ha magánszemély(ek) és azok csoportjai valósítják meg a támadást valamely állam utasítása, irányítása vagy ellenőrzése alatt, akkor fennállhat a betudhatóság. Az ellenőrzés fogalma vitatott ugyan a nemzetközi jogban, azonban a Nemzetközi Bíróság 2007-es döntésében megerősítette a tényleges kontroll elvének alkalmazását.[44]

Ugyanakkor az utóbbi években olyan új „szereplők" jelentek meg a hadszíntéren, akik kilépnek a klasszikus, addig ismert ellenség képéből, és már nemcsak háborúban, hanem békeidőkben is fenyegetik az államokat és lakosokat egyaránt. A terrorizmus[45] és annak virtuális térben folyó, számítógépes változata,

[40] Schmitt, 2002a, 35.

[41] ENSZ Alapokmány 51. cikk, 1956. évi I. törvény az Egyesült Nemzetek Alapokmányának törvénybe iktatásáról.

[42] „A szükségesség követelménye azt jelenti, hogy az önvédelmi jog gyakorlása kizárólag a támadás elhárítására és visszaverésére irányulhat." „Az arányosság követelménye azt jelenti, hogy az önvédelem jogával élve alkalmazott erőszaknak minden esetben igazodnia kell a fegyveres támadás mértékéhez." (Kelemen – Pataki, 2015, 82-83.).

[43] Kralovánszky, 2019, 200.

[44] Kelemen – Pataki, 2015, 88.

[45] Alex P. Schmid és Albert J. Jongmann a következőképpen határozta meg a terrorizmus ENSZ által elismert fogalmát. A terrorizmus „olyan, a félelem kiváltására alkalmas módszer, amelyet (félig) titkosan cselekvő személy, csoport vagy állam követ el ismételten, egyéni beállítottságból fakadó bűnügyi vagy politikai okok miatt, amelyben, a gyilkossággal ellentétben, az erőszak közvetlen célpontjai nem a fő célpontok. Az erőszak közvetlen emberi áldozatait véletlenszerűen (a lehetőség célpontjai) vagy kiválasztással (képviselő vagy szimbolikus célpontok) jelölik ki valamely célcsoportból, és üzenethordozónak szánják. A terrorista (szervezet) és veszélyeztetett áldozatok és a fő célpontok közötti fenyegetésen alapuló kommunikációs eljárásokkal a fő célpontot (célközönséget, célcsoportokat) manipulálja, amelyet ezáltal a rettegés célpontjává, követelések célpontjává vagy a félelem célpontjává változtatja, attól függően, hogy elsődlegesen megfélemlítést, kényszerítést vagy propagandát akarnak-e ezzel elérni" (Simon, 2018, 21.).

a kiberterrorizmus állandó, közvetlen és közvetett fenyegetést jelent, erőszakos és arctalan támadások veszélyét hordozza a legváratlanabb pillanatokban az élet bármely területén.

A terrorizmus működése megértésében, a terrorista lét megismerésében, valamint kezelésükben Carl Schmitt partizánelmélete lehet a kulcs. A második világháború végéig alapvetően az államokhoz és a hadseregeikhez kötődő erőszak volt a meghatározó, a harcot a térben és időben összemérhető, a politikai és a katonai erők tekintetében „egyenrangú" felek küzdelme határozta meg.[46] Schmitt azonban rávilágított arra a tényre, hogy a 20. század folyamán, az állami hatalom fokozatos háttérbe szorulásával megjelent a „partizánféle" harcos, aki az ellenségfogalom újragondolására készteti a szuverén államokat. Megfogalmazásában az tekinthető partizánnak, aki „kerüli, hogy fegyvereit nyíltan viselje, aki lesállásból támadva harcol, aki álcázása érdekében nemcsak az ellenség egyenruháját használja fel, nemcsak rögzített vagy kötetlen rangjelzéseket alkalmaz, hanem a legkülönfélébb civil ruhákat ölti magára. A partizán legerősebb fegyvere a titokzatosság, a sötétség és a homály, amelyekről nem mondhat le becsületes módon anélkül, hogy ezáltál el ne veszítené az irregularitás terét, vagyis anélkül, hogy ezáltal meg ne szűnne partizánnak lenni."[47] A partizán tehát nem tagja az állam szervezett hadseregének, nem reguláris katona, jellemzője az illegalitás, valamint a nemzetközi jogon kívüliség.

Schmitt a partizán három alaptípusát különbözteti meg: a gerillát, a forradalmárt és a terroristát. Az elnevezések egy történeti fejlődési ívet is kifejeznek, hiszen a gerilla a haza védelmezőjeként lép fel, jellemzően védekezésként az idegen, megszálló seregekkel szemben. A forradalmárok szintén civil harcosok, azonban tipikusan nem területvédő, hanem valamilyen ideológiai céllal, és tevékenységük szélsőséges esetben forradalomhoz vagy polgárháborúhoz vezethet. A terrorista a „világuralomra törő agresszív aktivista",[48] aki bármilyen eszközt képes felhasználni céljai elérése érdekében, bárhol, bármikor, a legváratlanabb pillanatban támadást intézhet a kiszemelt célpontok ellen, és jellemzően nem a reguláris haderő, hanem a civil lakosság vagy az állami szervek a célpontjai. Az ő személyük képviseli a partizán alakjának legszélsőségesebb formáját. A világméretű informatikai, digitális fejlődésnek köszönhetően cselekményeikhez sikerrel használják fel a legmodernebb technológiai eszközöket, infokommunikációs rendszereket és a közösségi médiát is, így az általuk jelentett fenyegetés mára már megjelent a virtuális térben is. A „gerilla hadviselés a 21. században egy információ-centrikus és hálózat központú hadviselési kultúrává fejlődött,"[49] és ahogy Simon László fogalmazott egy előadásában a schmitti analógiával élve, a kibertérben mára már megjelent a „kiberpartizán" alakja. Simon szerint a kiberpartizán elméleti alakja jelenti a kulcsot ahhoz,

[46] Simon, 2017, 235.
[47] Schmitt, 2002a, 24.
[48] Schmitt, 2002a, 19.
[49] Simon, 2017, 239.

hogy a kibertér totalitását, illetve az ott közvetített fenyegetést megértse, valamint kezelhesse mind az állam, mind az állampolgár.[50]

A reguláris haderőtől függetlenedett partizán schmitti alakja napjainkra önálló fenyegetéssé vált, mely az államokat teljesen újfajta, ún. totális biztonsági kihívások elé állítja. Ezek olyan komplex veszélyek, amelyek nem tisztán katonai vagy belbiztonsági jellegűek, hanem „szürke zónát" képviselnek a klasszikus háború és a belbiztonsági kihívások között, és amelyek a fenyegetés mértéke szerint a szélsőértékek között mozognak. Velük szemben szükséges a védelem újragondolása, totalizálása, a többfrontos védekezés megteremtése, a gyors, hatékony, operatív reagálás lehetőségének biztosítása.[51]

V. KIBERMŰVELETEK: AZ ÁLLAMOK MOZGÁSTERE

Az államnak, mint a legitim fizikai kényszer és az ellenségmeghatározás monopóliumával rendelkező politikai egységnek[52] kötelessége, hogy hasonló hatékonysággal és proaktivitással járjon el a kibertérből érkező támadásokkal szemben, mint az államok működését meghatározó hagyományos dimenziókban. A legitim állami kényszernek a kibertérben is meg kell jelennie, annál is inkább, mivel a fenyegetések, támadások többségében a szereplők azonosítása, cselekményeik megelőzése „csak az állam speciális totalitásának elérésével, és az egyéni szint közvetlen bevonásával, nemzetbiztonsági tudatosságának növelésével" biztosítható.[53]

A hagyományos (szárazföldi, légi vagy haditengerészeti) hadszíntérhez képest azonban a kibertérben történő műveletek speciális felkészültséget igényelnek, a korábban kidolgozott nemzetközi jogi fogalmi keretek nem minden esetben alkalmazhatóak a virtuális térre. A kiberfenyegetések felismeréséhez, felderítéséhez és kezeléséhez, a támadások megelőzéséhez, elhárításához, vagy az esetleges károk enyhítéséhez kimagasló tudással rendelkező informatikusokra és egyéb, az elektronikus információbiztonság területén jártas szakemberekre, a megfelelő szabályozási környezet kialakítására, a kibertámadások elleni képességek fejlesztésére, a kutatás és fejlesztés, valamint a szaktudás és az általános biztonságtudatosság növelésére, illetve a nemzetközi együttműködés fokozására van szükség.[54] A kibertámadások ellen csak akkor lehet felvenni a harcot, ha a megfelelő személyi, szervezeti és tárgyi feltételek biztosítása mellett a szuverén, az alkotmányos garanciákat biztosítva, „széles körben határozza meg a cselekvés lehetőségét és módjait".[55]

[50] Pongrácz, 2018, 149.
[51] Farkas, 2015, 9-12.
[52] Az államfogalom meghatározásához lásd Weber: Szociológiai alapfogalmak (Weber, 1988, 77-80.).
[53] Simon László előadását idézi Pongrácz Alex (Pongrácz, 2018, 149.).
[54] Simon – Magyar, 2017, 98-100.
[55] Farkas, 2013, 168.

A kiberműveletek közül a kiber információszerzés nem minősül fegyveres támadásnak, célja valamely adatbázisban tárolt adat vagy információ megszerzése. A kibervédelem szintén nem tartozik a fegyveres támadás fogalmi körébe; célja, hogy megvédje a saját információkat, illetve fenntartsa az információkhoz való hozzáférést, továbbá elősegítse az információs rendszerek hatékony használatát.[56] A kibervédelem passzív eszközei (a tűzfalak; a vírusirtók; a hozzáférés-szabályozás, valamint a behatolás-detektálás és adaptív válaszlépések) bármikor, még természetesen nem fegyveres támadás esetén is alkalmazhatóak, azonban az aktív eszközök használatára, mint a megelőző támadás, ellentámadás vagy az aktív megtévesztés, csak és kizárólag fegyveres támadás esetén kerülhet sor, amennyiben a megtámadott felet megilleti a már említett önvédelem joga.[57] Ugyanakkor az alkalmazott aktív eszközöknek ebben az esetben is meg kell felelniük a szükségesség és arányosság követelményeinek. A kiberműveletek harmadik típusa a kibertámadás,[58] melynek célja lehet információ- és adatszerzés, az információs rendszer megzavarása vagy az információs rendszer elpusztítása, eszközeit tekintve pedig lehet fegyveres vagy nem fegyveres támadás is.[59]

Annak ellenére, hogy jelenlegi ismereteink alapján a kibertérben eddig „csak" támadó műveletek fordultak elő, vagyis a támadáshoz mérhető ellentámadás a megtámadott fél részéről nem történt, ez nem jelenti azt, hogy a megtámadott fél védekező műveletet ne hajtott volna végre.[60] Az aktív eszközök alkalmazása érdekében a védekező műveletek részeként is szükséges a támadási képességek kialakítása és biztosítása, mely az állam, mint a legitim fizikai kényszeralkalmazás monopóliumával rendelkező politikai egység feladata. Ugyanakkor a komplex feladatok ellátása, továbbá a biztonság megteremtése érdekében a megfelelő kibervédelmi képességet, valamint ennek keretében a sikeres megelőzést, észlelést és reagálást csak a katonai és polgári szervek központi koordinációja, illetve együttműködése biztosíthatja. Az előre nehezen megjósolható és lokalizálható, meglepetésszerű támadásokkal szemben már a hagyományos katonai, rendészeti és nemzetbiztonsági eszközök nem nyújtanak megfelelő megoldást; velük szemben e szervek együttműködésére, a totális védelem kialakítására van szükség.[61]

[56] Bányász, 2017, 115.
[57] A kibervédelem eszközeiről részletesebben lásd Haig – Kovács – Ványa – Vass, 2014, 29.
[58] A támadó jellegű információs hadviselés célja, hogy a speciális érdekekre vagy speciális fenyegetésekre választ adva hatást gyakoroljanak a másik félre (Bányász, 2017, 115.).
[59] Kelemen – Pataki, 2015, 70-76.
[60] Kralovánszky, 2019, 200.
[61] A totális védelem kérdéséről lásd Farkas, 2015; Farkas, 2013; Farkas, 2018.

VI. ÖSSZEGZÉS

Az utóbbi évtizedekben bekövetkező technológiai fejlődés eredményeképpen az infokommunikációs eszközökkel és digitális hálózatokkal átszőtt világunk talán sosem volt olyan sebezhető, mint napjainkban. E változások nemcsak a társadalom és a mindennapi ember életét változtatták meg alapjaiban, hanem az államok berendezkedését is, melyeknek működése nem képzelhető már el e fejlett technológiák alkalmazása nélkül. A megváltozott, immáron információs környezetnek köszönhetően a hadszíntér fizikai dimenziói kiegészültek az úgynevezett virtuális dimenziókkal, megjelent a hadviselés új formája, az információs hadviselés és annak részeként a számítógéphálózati műveletek, melynek meghatározó elemei a kiberműveletek: a kiber információszerzés, a kibertámadás és a kibervédelem.[62]

A 20. század második felében, a 21. században megjelenő új típusú kihívások már nem írhatók le a klasszikus háborúk esetében alkalmazott kategóriákkal, megoldásokkal. A támadások a legváratlanabb pillanatban, számos megjelenési formában, több fronton érkezhetnek egyszerre, és nemcsak az államot és intézményeit, valamint annak szimbólumait, hanem az egész társadalmat támadják.

A kibertér egy speciális tartománya az információs hadszíntérnek, mely komplex kihívások elé állítja az államokat, amelyekre újszerű válaszok és megoldások kidolgozása szükséges. A problémák alapvetően két területre koncentrálnak, az egyik a kibertámadás elkövetőjének meghatározása, a másik pedig annak megítélése, hogy vele szemben milyen válaszlépéseket tehet meg egy állam.

Az elkövető személyének azonosítása nélkülözhetetlen ahhoz, hogy a megtámadott állam felvegye a harcot az egzisztenciáját, létezését veszélyeztető támadóval szemben, valamint a saját maga védelmében megtegye a megfelelő intézkedéseket. A politikai schmitti fogalma pontosan jelzi, hogy kizárólag az állam rendelkezik a politikai monopóliumával, azaz legitim módon egyedül az állam dönthet arról, ki a barát és ki az ellenség, s hogy az ellenséggel szemben hogyan kell eljárni. Ez teljes világossággal nyilvánul meg az államot érő külső vagy belső támadás helyzetében, ekkor az államnak, mint szuverénnek kell döntenie a támadás jellegének a megítéléséről, valamint a támadóval szemben alkalmazandó eljárásról. Schmitt szerint a barát és ellenség megkülönböztetése a „politikai" olyan esszenciális kritériuma, melynek hiányában az állam, mint mértékadó politikai egység megszűnik létezni. Az ellenséggé nyilvánítás magában foglalja a harc, a háború potenciális lehetőségét is, mint a legszélsőségesebb politikai eszköz megnyilvánulását.

[62] Haig – Kovács – Ványa – Vass, 2014, 271.

Amennyiben egy megtámadott állam minden kétséget kizáróan bizonyítani tudja, hogy a támadó fél mely állam volt, vagy hogy a cselekményt mely állam utasítása, irányítása vagy tényleges ellenőrzése alatt követték el, valamint a támadás megfelelő súlyúnak és intenzitásúnak bizonyult, úgy a támadóval szemben megilleti őt az önvédelem joga. Ez azt jelenti, hogy a megtámadott államnak lehetősége van nemcsak passzív, hanem aktív védelmi intézkedések foganatosítására is, például megelőző támadás formájában.

A kibertérben megjelenő kíméletlen, sok esetben a határtalan pusztításra törekvő, gyakran arctalan ellenség, a terrorizmus megjelenésével az államoknak fel kell készülniük az agresszióra adható válaszlépésekre, megelőzésükre, megakadályozásukra, illetve a károk enyhítésére. Ahhoz, hogy a terroristatámadásokkal szemben érdemben fel lehessen lépni, szükséges, hogy megértsük létük és működésük mozgatórugóit, melyben Schmitt partizánelmélete és az általa bemutatott partizán három alakja lehet meghatározó. „A modern partizán sem jogot, sem kegyelmet nem vár el az ellenségétől. Elfordult a megszelídített védelmi intézményekkel körülbástyázott háború konvencionális ellenségességétől és egy másik terület, a valóságos ellenségesség területe felé vette az irányt, amely a terrorral és ellenterrorral egészen a megsemmisítésig fokozódik."[63] Az ellenségesség abszolutizálásának a logikája – melyben a szembenálló idegen egzisztenciálisan válik megsemmisítendő ellenséggé, és ebben az értelemben totálissá[64] – a jelenkori terrorizmusban rávilágított az egyéni és kollektív biztonság összekapcsolódásának és összetettségének a tényére, amely megköveteli az államoktól, hogy az új típusú biztonsági kihívásokkal szembeni védelmet új alapokra helyezzék. A fenyegetések azonosítása, a megelőzés, elhárítás vagy semlegesítés érdekében a védelem hagyományos szervei, az állami erőszak monopóliumát biztosító honvédség, rendőrség és nemzetbiztonsági szolgálatok mellett az állami nem fegyveres erők, a civil szereplők bevonására, valamint a lakosság egyéni szerepvállalására is szükség van.

Schmitt *A politikai fogalma* című művében megfogalmazott előremutató gondolatai a kibertérből érkező támadások kapcsán is bizonyítják aktualitásukat, és amellett, hogy komoly segítséget nyújtanak a napjainkban jelentkező új típusú fenyegetések működési mechanizmusának megértésében, elvezetnek minket a kihívásokra érdemben reagálni képes, a minősített erőszak alkalmazását garantáló szervek, valamint a civil szféra együttműködésén és munkamegosztásán alapuló, komplex védelem megvalósításáig, a szükséges kibervédelmi képességek kialakításáig.

[63] Schmitt, 2002a, 7.
[64] Cs. Kiss, 2020, 486.

IRODALOM

- Bányász Péter (2017): A közösségi média, mint az információs hadszíntér speciális tartománya. In: *Hadmérnök.* XII. Évfolyam „KÖFOP" szám.
- Berki Gábor (2016): Kiberháborúk, kiberkonfliktusok. In: Pintér István (szerk.): *A virtuális tér geopolitikája*. Geopolitikai Tanács Közhasznú Alapítvány, Műhelymunkák, Budapest.
- Berki Gábor (2013): A kibertéri konfliktusok változásai. In: *Hadmérnök.* VIII. Évfolyam 1. szám.
- Cs. Kiss Lajos (2017): Államelméleti helyzetkép [State Theories – An Overview]. In: *Pro Publico Bono – Magyar Közigazgatás (2).*
- Cs. Kiss Lajos (2010): Totális állam elmélete és mítosza. In: *Világosság*. 2010 ősz.
- Cs. Kiss Lajos (2020): Totális állam és jogállam: mítosz és elmélet. In: Cs. Kiss Lajos (szerk.): *A politikai korrektség ellen – Carl Schmitt recepció a társadalomtudományokban*. Kézirat. Budapest.
- Farkas Ádám (2015): *A totális államtól a totális háborún át a totális védelemig.* MTS Law Workings Papers, Frankfurt am Main.
- Farkas Ádám (2013): *A totális védelemről – Gondolatok a modern állam fegyveres védelmének történeti konstellációjáról, Carl Schmitt totális állam és totális háború toposzai kapcsán*. Doktori Műhelytanulmányok. SZE Állam- és Jogtudományi Doktori Iskola, Győr.
- Farkas Ádám (2018): Gondolatok a 21. századi biztonságról, államról, védelemről. In: *Hadtudomány.* 2018. évi elektronikus lapszám.
- Haig Zsolt (2018): *Információs műveletek a kibertérben.* Dialóg Campus Kiadó, Budapest.
- Haig Zsolt – Kovács László (2008): Fenyegetések a cybertérből. In: *Nemzet és Biztonság: Biztonságpolitikai szemle.* 1:(5) 2008.
- Haig Zsolt – Kovács László – Ványa László – Vass Sándor (2014): *Elektronikai hadviselés.* Nemzeti Közszolgálati és Tankönyv Kiadó Zrt., Budapest.
- Haig Zsolt – Várhegyi Zsolt (2014): *Hadviselés az információs hadszíntéren.* Zrínyi Kiadó, Budapest.
- Kelemen Roland – Pataki Márta (2015): A kibertámadások nemzetközi jogi értékelése. In: *Katonai Jogi és Hadijogi Szemle.* 2015/1. szám.
- Kettmann, Steve (2004): Soviets Burned By CIA Hackers? (Elérhető: http://www.wired.com/culture/lifestyle/news/2004/03/62806. Letöltés ideje: 2020. május 20.).
- Kovács László – Krasznay Csaba (2010): Digitális Mohács. In: *Nemzet és Biztonság: Biztonságpolitikai szemle.* 2010: (1).
- Kovács Márk Károly (2019): Gerilla-hadviselés és a terrorizmus kapcsolatrendszere napjainkban. In: *Hadtudományi Szemle.* 2019. XII. évfolyam, 1. szám.
- Kralovánszky Kristóf (2019): A kibertér fejlődése. In: *Hadmérnök.* 14. évfolyam 4. szám.
- Krasznay Csaba (2012): A polgárok védelme egy kiberkonfliktusban. In: *Hadmérnök.* 7. évfolyam, 4. szám.
- Muha Lajos – Krasznay Csaba (2014): *Az elektronikus információs rendszerek biztonságáról vezetőknek.* NKE Vezető és Továbbképzési Intézet, Budapest.
- Negroponte, Nicholas (2002): *Digitális létezés* (Fordította: Csaba Ferenc). Typotex Kiadó, Budapest.
- Pongrácz Alex (2019): *Nemzetállamok és új szabályozó hatalmak a globális erőtérben – avagy megszelídíthető-e a globalizáció?* Dialóg Campus, Budapest.
- Pongrácz Alex (2018): Totalitás és új típusú biztonsági kihívások a 21. században. In: *Katonai Jogi és Hadijogi Szemle.* 2018/1. szám.

• Schmitt, Carl (2002a): A partizán elmélete. Közbevetett megjegyzés a politikai fogalmához. In: Schmitt, Carl (2002): *A politikai fogalma. Válogatott politika- és államelméleti tanulmányok* (a fordított változatot szerkesztette: Cs. Kiss Lajos). Osiris – Pallas Stúdió – Attraktor, Budapest.
• Schmitt, Carl (2002b): A politikai fogalma. In: Schmitt, Carl (2002): *A politikai fogalma. Válogatott politika- és államelméleti tanulmányok* (a fordított változatot szerkesztette: Cs. Kiss Lajos). Osiris – Pallas Stúdió – Attraktor, Budapest.
• Schmitt, Carl (1992): *Politikai teológia*. ELTE–ÁJK, Budapest.
• Simon László (2017): A partizán elmélete a premodern virtuális korban. In: *Jog–Állam–Politika.* 2017/4. szám.
• Simon László (2018): *A partizán elmélete a premodern virtuális korban*. Nemzeti Közszolgálati Egyetem, Budapest (kézirat, megjelenés alatt).
• Simon László – Dr. Magyar Sándor (2017): A terrorizmus és indirekt hatása a kibertérben. In: *Nemzetbiztonsági Szemle.* MMXVII/III.
• Sulyok Gábor (2005): A terrorcselekmény elkövetéséhez használt polgári légi jármű lelövésének nemzetközi jogi és alkotmányjogi megítélése. In: *Fundamentum.* 2005/3.
• Szabó Márton (2003): A politikai fogalmának elmélyítése Carl Schmitt partizánelméletéről. In: *Világosság.* 2003/7-8. szám.
• Szabó Márton (2007): Ellenség és ellenfél a politikában. In: *Politikatudományi Szemle.* XVI. évfolyam, 2007/1. szám.
• Takács Péter (2011): Államelmélet a XX. században, A jogi, a társadalmi és a politikai államfogalom. In: *Pro Publico Bono Online.* 2011/2.
• Weber, Max (1988): *Gazdaság és társadalom. A megértő szociológiai alapvonalai* (fordította: Erdelyi Ágnes). Közgazdasági és Jogi Könyvkiadó, Budapest.

JOGFORRÁSOK

• 1956. évi I. törvény az Egyesült Nemzetek Alapokmányának törvénybe iktatásáról. (Elérhető: https://net.jogtar.hu/jogszabaly?docid=95600001.tv. Letöltés ideje: 2020. május 21.).
• A létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény.
• Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény.