

KELEMEN ROLAND

A kibertér jellemzőinek biztonság központú vizsgálata

ABSTRACT

An absolute concept and definition of cyberspace is an impossible undertaking due to its multidisciplinary nature. The information technology, social and natural science aspects of cyberspace would have to be included in such a concept. Consequently, the aim of this paper is not to create a generalised concept of cyberspace. Rather, it is to explore the fundamental characteristics of cyberspace in a multidisciplinary way. However, identifying these characteristics is not an end in itself, but aims at a better understanding of cyberspace from a national security perspective. Indeed, for the development of an effective national security framework, it is also necessary to have an in-depth understanding of the social reality of cyberspace, as both technology and society have an impact on each other and necessarily on security processes in traditional space. It is essential for the development of modern defence and security arrangements to understand and synthesise these.

Keywords: cyberspace ■ cyber geography ■ social networks ■ cyber psychology
■ cyber operation ■ NATO ■ national security

I. BEVEZETŐ GONDOLATOK

A kibertér fogalmának abszolút érvényű meghatározása, definíciója annak multidiszciplináris jellegéből adódóan lehetetlen, sőt kifejezetten tudománytalan vállalkozás volna, hiszen e fogalomban szerepelnie kellene az információtechnológiai megközelítésnek, a társadalomtudományok, így kifejezetten az állam- és jogtudományi, szociológiai, filozófiai, gazdaságtudományi diszciplínák kapcsolódásainak, valamint legalább ilyen hangsúlyban a természettudományi (geográfia, matematika, fizika) aspektusoknak, továbbá az elmúlt évtizedekben tapasztalható hadi, védelmi célú felhasználása okán a hadtudományi értelmezéseknek is. Ebből kifolyólag ezen tanulmány nem azt tűzi ki célul, hogy egy átfogó kibertér-fogalmat alkosson meg, hanem egy multidiszciplináris áttekin-

tését kívánja adni a kibertér fogalmi jegyeinek, amellyel megfelelő mélységben tudja megalapozni a későbbi tudományos diskurzust e területen.

A kibertér elnevezés William Gibson nevéhez köthető, aki 1984-es disztópikus sci-fijében, a Neurománchban tette közzé a kifejezést. A regényében egy olyan társadalmat ábrázol, ahol a kibertérhez való csatlakozás a normális emberi létezés alapfeltétele, ennek hiányában az egyén a társadalom peremére szorul. Magát a kibertérrel úgy mutatta be, mint egyfajta kollektív hallucinációt vagy benyomást, a számítógépes adatok grafikai reprezentációját.^[1] Maga Gibson sem gondolta azt, hogy az általa teremtett világ ilyen mértékben valósággá válik napjainkra. Természetesen merész állítás volna azt kijelenteni, hogy eme disztópia tökéletes leírása jelenkorunk államának vagy társadalmának, azonban a napjainkban tapasztalható folyamatok és jelenségek egyes jegyeiben hasonlóságot mutatnak a könyvében felépített világgal (gondoljunk itt példának okáért a közösség média kiterjedtségére és a felhasználói kultúrára), a háttérrendszerek további fejlődése pedig töretlen. Sőt ezen innováció folyamatosan gyorsul, ami abban fogható meg leginkább, hogy Moore-törvénye,^[2] amely szerint az egy chipben lévő tranzistorok száma körülbelül 18 havonta megduplázódik, napjainkra a technológiai óriásvállalatok álláspontja szerint megdőlt.^[3] Az infokommunikációs területnek ez a robbanásszerű fejlődése tehát sok tekintetben fizikai valósággá változtatta Gibson akkor még fikciónak vélt világát, mivel „a globális számítógépes hálózatokban végbemenő kölcsönhatások révén megszületett a kibertér (cyberspace), a kibernetikus világegyetem”.^[4] E kibertér rendkívül egyedi és összetett jelenség, hiszen leírható fizikai és földrajzi fogalmakkal, emellett azonban virtuális jellemzői is komoly relevanciával bírnak megismerése során, továbbá rendkívüli térnyerésének következtében újra kell gondolni olyan alapvető területeket is, mint a szociológia, a geopolitika, valamint a biztonságpolitika, vagy éppenséggel a védelmi jog.

II. A KIBERTÉR TÉRJELLEMZŐI

A kibertér összetettsége elvárhatóvá teszi, hogy annak fogalmi jellemzése is a multidiszciplinaritás talaján álljon. Ennek a szemléletnek megfelelően kézenfekvő kiindulási pontot ad a fogalom felbontása a kiber és a tér szavakra, így pedig a szemlélődés kezdőpontja a kibertér tér jellegének vizsgálata, amely a földrajztudomány, azon belül is a kibergeográfia vagy virtuális geográfia területére visz el minket. A hagyományos természettudományok elkülönült térértelmezéseket használnak. Megkülönböztetnek abszolutista és relativista térfelfogást. Az ab-

[1] Gibson, 1984, 5.

[2] Moore, 1965.

[3] LightReading: Moore's Law Is Dead.

[4] Nagy, 1999, 173.

szolutista szerint a tér egy változatlan befogadási közeg, amelyet a benne zajló folyamatok nem módosítanak, míg a relativista pontosan az ellenkezőjét gondolja, ugyanis ez alapján a tér a benne megjelenő folyamatok lévén nyer értelmet. A földrajzi tér fogalma valahol a kettő között helyezhető el, ugyanis az nem azonos a fizikai térrel, de attól nem is független.^[5] A földrajzi tér alatt egy összetett jelenséget értenek, amely számos alrendszerrel foglal magába, amelyek egymásra kölcsönösen hatnak. Ennek a földrajzi térnek az egyik legfontosabb sajátossága, hogy az ember és természet közötti interakció hozza létre, módosítja, alakítja és ennek köszönhetően fejlődik. „A földrajzi tér tulajdonképpen fizikailag létező struktúrák és az azokról alkotott képzetek, valamint teljesen virtuális, a fizikai térben kézzel nem fogható, ámbátor mindennapjainkban használt, vagy megélt hálózatok összességéeként fogható fel.”^[6] Ez a lényegében ember által formált tér olyan struktúrákat is magába foglal, amelyet a társadalmi viszonyrendszerek hoztak létre, így például a hatalmi struktúrákat vagy az etnikai és vallási struktúrákat.^[7] Megelőlegezve a későbbieket: érdekes kérdés, ha a földrajzi térnek része a virtuális tér is, akkor ezen struktúrák ott is megjelennek-e, illetve, ha igen, milyen módon.

Viszont, hogy erre a kérdésre választ tudjunk adni, tovább kell bontani a földrajzi tér fogalmát, és megvizsgálni, hogy a kibertér milyen viszonyban van a földrajzi tér egészével. A földrajzi tér esetében különböző felosztásokkal találkozhatunk. A vertikális metszeteket a vizsgálódás középpontjába helyező megközelítés szerint elkülöníthetünk társadalmi környezetet, épített környezetet, élő környezetet és élettelen környezetet, és akár ezt bővítve, virtuális környezetet. E szemlélődés lényege, hogy úgy különítenek el szférákat, hogy hasonló helyekből állítanak össze halmazokat. Egy másik felfogás szerint az egyén oldaláról osztjuk fel a földrajzi teret, amely az egyén észlelésén, tapasztalatain és tevékenységén nyugszik. E felosztás kettős: virtuális tér és fizikailag létező tér. Előbbi az individuális térből, kognitív térből,^[8] kibertérből és fiktív térből áll; utóbbi az individuális térből, antropológiai térből, biológiai térből és fizikai térből tevődik össze. Látható, hogy e felosztás szerint a virtuális tér jóval bővebb, mint, amit mi kibertérnek tekintünk, hiszen ebbe beletartozik az egyén képzelete és az azáltal leírt világ is.^[9]

Fentiekből adódóan a virtuális tér (kibertér) immanens részét képezi a földrajzi térnek, annak tág értelmében – lásd egyéni központi felosztás – és szűk értelmében is, vagyis, mint infokommunikációs közeg is. Érdekes azonban ezen körben kitérni arra, hogy a hagyományostér-szemléletet miként érintette a kibertér kialakulása és glóbuszt behálózó jellege. A virtuális geológia atyának

[5] Pirisi – Trócsányi, 2019, 39-40.

[6] Pirisi – Trócsányi, 2015.

[7] Pirisi – Trócsányi, 2019, 41.

[8] A kognitív infokommunikációról (CogInfoCom) és térjellemezőiről ld. bővebben: Erdős – Németh, 2019.

[9] Pirisi – Trócsányi, 2019, 58-61.

tekinthető Michael Batty szerint a kibertér önmagában megváltoztatja a valós (földrajzi) helyek szerepét, módosítja a hely és tér fogalmát és kapcsolatát, megváltoztatja a távolságdefiníciókat, leszűkíti a hely- és térfelfogás hagyományos értelmezését.^[10] Emellett azonban számos tekintetben kiszélesíti azt, hiszen a kibertér nem egy homogén térből áll, abban ugyanis számtalan, gyorsan növekvő kibertérület található, amelyek mindegyike másfajta interakcióra képes, miközben a technológiák gyors konvergenciája miatt új hibrid terek jönnek létre.^[11] Ezek a megállapítások át is visznek minket a terület legvitatottabb kérdésére, hogy a kibertérnek köszönhetően a tér, a földrajzi tér és azon belül a távolság egyáltalán értelmezhető fogalmak-e. A főként társadalomtudományi megközelítés szerint az információs társadalomban az információ mindenhová eljut és eljuttatható, vagyis az egyenes csatornák bárhová elérnek, így a tér, az idő és a távolság már irreleváns. Manuel Castells ezt úgy fogalmazta meg, hogy „az időtlen idő mint az idő technológia által történő megsemmisítésére irányuló törekvés... A technológia kisszámú, esetleges pillanatra sűríti az időt, ily módon szakítva meg a társadalom folyamatosságát és fosztva meg történetiségétől a történelmet.”^[12] Ezzel a felfogással szemben – főként a földrajztudomány képviselői – azon az állásponton vannak, hogy a földrajzi tér továbbra is releváns, amelynek hagyományostér-rétegei is hatással bírnak a kibertérre, nem elhallgatva, hogy „a digitális információs interakciók egy önálló és sajátos teret, egy párhuzamos kibertéri világot generálnak, mely azonban nem teljesen független a világunk fizikai-térbeli sajátosságaitól.”^[13]

Az igazság valójában a kettő közötti aranyközépponton található, ami Mészáros Rezső kibertérre leíró jellemzésében is tetten érhető: a kibertér „sok mesterségesen konstruált térből áll – ezek tervezőik, sőt gyakran használóik alkotásai, és csak akkor veszik fel a »földrajzi« (euklidészi) tér tulajdonságait, ha kifejezetten erre programozták őket. Sőt a terek gyakran tisztán olyan vizuális tárgyak, amelyeknek nincs se súlya, se tömege, sőt még az is bizonytalan, hogy mozdulatlanok-e (a terek egy szempillantás alatt megjelennek vagy eltűnnek). A kibertérnek anyagtalan és dinamikus térbeli és szerkezeti formái (felépítései) vannak, a szó fizikai (szoros) értelmében nem kézzel fogható, mert csak az agyunk segítségével vagyunk képesek megvizsgálni, de a metafora szintjén kapcsolatban áll testi tapasztalatokkal (érzékeléssel) is.”^[14] Erre kapcsolódik rá Jakobi Ákos is, aki szerint a kibertér nem más, mint „az új komputerizált világ sajátos, elvont tere”.^[15] Azonban ezek a fizikai valóság oldaláról történő megközelítések önmagukban nem elégségesek ahhoz, hogy pontos képet kapjunk a kibertér valós jellegéről és hagyományos térrel való kapcsolatáról, főként, hogy látható módon

[10] Batty, 1997, 337-352.

[11] Dodge - Kitchin, 2001, 1-33.

[12] Castells, 2007, 433.

[13] Jakobi - Lengyel, 2014, 42.

[14] Mészáros, 2006, 494.

[15] Jakobi, 2002, 1484.

egyres társadalomtudományi megközelítések a kibertér és a hagyományos tér kapcsolatáról élesen eltérő képet adnak. Így szükséges további vizsgálódás tárgyává tenni a kibertér tér jellegét.

Ennek megfelelően érdemes a kibertérrel kapcsolatos térfelfogásokra kitérni. A fizikai térhez legközelebb álló felfogás az infrastrukturális térfelfogás, amely a számítógépes hálózatok effektív kapcsolatait, vagyis a hardveres összeköttetést jelenti. Ettől már jóval árnyaltabb képet mutat a koncepcionális térfelfogás, mely a virtuális világ széles értelmezése, vagyis lényegében a körön belüli részelemek egymás közötti kapcsolatait jelenti. Ennek megfelelően a kibertér különböző kommunikációs rendszerek önálló belső tereiből épül fel, amelyek további téregységekre bonthatóak. „A kibertér így az információk és a kommunikáció áramlásának egyfajta koncepcionális tereként jellemezhető, amely a digitális világ hardver eszközei, a számítógépek szoftverei, a telekommunikációs hálózatok és az emberi elme szerves kombinációjából jött létre.”^[16] Utóbbi szemléletből mindenképpen kiemelendő, hogy a tér elkülönült részének tekintni a hardvert, a szoftvert és az egyént is. Ez pedig lehetővé teszi az egyik legegyszerűbb és leginkább kézenfekvő felosztás vizsgálatát, vagyis külső és belső tér fogalompárosának görcső alá helyezését. Ennek a két fogalomnak – külső kibertér vs. belső kibertér – felvázolása, majd későbbi alábontása lehetővé teszi annak a gordiuszi csomónak az átvágását, amely az eltérő tudományterületek sajátos kiindulópontjából következőleg néhol ellentétes következtetéseket enged levonni a kibertér és a hagyományos tér kapcsolatáról.

A külső kibertérnek „csak olyan tereket nevezhetünk, amelyekben meghatározhatóan jelen van a lokalizáció, a földi (földrajzi) térhez kapcsolódás momentuma...”, ebből adódóan a „kibervilág külső terének tehát a rendszerhez köthető infrastrukturális tartozékok földi térszerkezetét nevezzük”.^[17] A belső kibertér ennél sokkal nehezebben megfogható, ugyanis „a kibertér virtuális összetevői fizikailag nem létező dolgok, amelyek egyik része a valós világ bizonyos dolgainak helyettesítője, reprezentációja, másik része mögött létező valós dolog nem áll”.^[18] A belső kibertérről akkor beszélhetünk, amikor a kibertér „önmagában mutat térjellemzőket, egyenlőtlenséget és rendezettséget”.^[19] Ezzel pedig a kibertér egy alternatív földrajzi struktúrát hoz létre.

A kettő elválasztásából egyértelműen következhetne – és az esetek egy részében következik is – az, hogy a lokalizálható külső térben megjelenő erőforrások, szerkezetek, hálózati elemek körében a klasszikus jogi, védelmi, biztonságpolitikai fogalmak alkalmazhatóvá válhatnak, hiszen ezek esetében egyértelműnek hathat akár az állami főhatalom kérdése, akár a tulajdonosi jogok gyakorlása. A belső tér fogalma azonban ezt is relativizálhatja, tudniillik a kibertér mint technológia formálja a teret, mert mint technológia, egyedi térbeli viszonyokat

[16] Jakobi – Lengyel, 2014, 43.

[17] Jakobi, 2002, 1487.

[18] Szkála – Munka, 2018, 346-347.

[19] Jakobi, 2002, 1487.

hoz létre.^[20] Így a belső kibertér ön maga által létrehozott térjellemezőkkel rendelkezik, amelyek semmissé tehetik azt a hagyományostér-fogalmat, amelyet a külső kibertér fogalom is megtestesít, vagyis például, hogy egy-egy adathalmaz megjelenése egy lokalizálható szerveren, hálózaton nem egyértelműen jelenti akár a jogi felelősség megalapozhatóságát, akár az állami főhatalom tényleges kiterjeszhetőségét. Ez viszont azon alapszik, hogy a belső kibertér lokalizálható hely nélküli tér,^[21] vagyis a külső kibertér lokalizálható szegmensei nem egyértelműen azonosíthatók a belső tér szegmenseivel.

Önmagában a hagyományostér-fogalom gondolkodáscsapidába vezetheti akár a jogalkotást, akár biztonsági intézkedések mechanizmusának kialakítását, továbbá sok esetben külön mechanizmusokra és szabályokra van szükség a külső és belső tér esetében, azonban a valódi nehézségét az adja eme feladatnak, hogy mindvégig fenn kell tartani a két területre vonatkozó gondolkodás összhangját. Ehhez viszont az általánosnak ható – és némiképp meghaladott – külső és belső elhatárolásnál részletesebb, a napi folyamatokhoz jobban igazodó alábontás szükséges, hasonlóan a fentebb már bemutatott földrajzi tér szegmenseihez. Az egyik első ilyen modellt az ún. OSI-modellt (Open Systems Interconnection Model), a Nemzetközi Szabványügyi Szervezet dolgozta ki az 1980-as évek közepére. A modell létrehozásának a célja az volt, hogy megalkossanak egy referencia rendszert, amely biztosítja a hálózati együttműködést, mégpedig gyártósemleges módon. A modell azt írja le, hogy egyes rétegek esetében minek kell megvalósulnia, így elkerülve a hálózati protokollok túlburjánzását. Az OSI-modell hét réteget különít el: a fizikai (physical) réteget, az adatkapcsolati (data link) réteget, a hálózati (network) réteget, a szállítási (transport) réteget, a viszonyréteget (session), a megjelenítési (presentation) réteget és az alkalmazási (application) réteget. A modell túlzott bonyolultsága okán annak inkább csak egyes részeit használják.^[22] Ennek is köszönhető egy másik modellnek a térnyerése, a TCP/IP modellnek. A TCP/IP-modell kezdetei majd egy évtizeddel megelőzték az OSI-modellt, azonban dominánssá válása az ARPANET^[23]-ből kinövő internetnek köszönhető, illetve az OSI-hoz mért átláthatóságának. A TCP/IP-modell lényege is abban fogható meg, hogy az egyes rétegek meghatározott feladatokat látnak el, amely rétegek szolgálatelérési pontokon kommunikálnak. A TCP/IP-modell az alábbi rétegeket különíti el: kapcsolati réteg (network interface), internet (internet) réteg, szállítási (transport) réteg és alkalmazási réteg (application layer).^[24] Eme modelleket alapul véve dolgozták ki Werbach és Kulesza rétegfelfogásait,

[20] Blount, 2016, 4.

[21] Jakobi, 2002, 1488.

[22] Stokes, 2009, 16-17.

[23] Az ARPANET (Advanced Research Projects Agency Network) az Egyesült Államok Védelmi Minisztériuma által finanszírozott fejlesztésű hálózat a védelmi szféra területén érintett, főként tudományos intézetek közötti számítógép-hálózat. A Védelmi Minisztériumhoz való kapcsolata okán külső szereplők korlátozottan tudtak kapcsolódni a hálózathoz. Az ARPANET 1990-ig működött. Lásd: Wright.

[24] Stokes, 2009, 17.

amelyeket nevezhetünk a kibertér rétegméletének. Ezen alábontás lehetővé teszi a különböző, ugyanakkor egymással összefüggő technológiák funkciók szerinti csoportosítását, és feltárja, hogy az egyes önálló technológiák, rétegek hogyan kapcsolódnak egymásba.^[25] Werbach négy, míg Kulesza három réteget különít el. Werbach felosztása szerint fizikai réteg (physical layer), logikai réteg (logical layer), alkalmazás réteg (applications layer) és tartalmi réteg (content layer) adja a kibertér totalitását.^[26] Kulesza az alkalmazási réteget nem választotta külön.^[27] A fizikai réteg lényegében a hardver oldalt jelöli, vagyis a klasszikus felosztások szerinti külső kibertert. A logikai réteg zökkenőmentessé teszi az információ áramlását a hálózat egyes pontjai között, ez a réteg rendkívül szoros kapcsolatban van a fizikai réteggel, lényegében az adatok fizikai réteg számára továbbítható állapotba, formátumba alakítását, konverzióját segítik elő a szoftverprotokollok révén. Az alkalmazás vagy más néven szolgáltatás réteg a végfelhasználók számára megjelenő funkciók összességét jelenti. A tartalmi réteg pedig az adatok, információk összességét.^[28] Eme felosztás már könnyebben megfogható szinteket különít el a kibertér mint tér fogalmi vizsgálódásában. Utóbbi felosztás lehetővé teszi például jogi szabályozási területek leválasztását is, hiszen a fizikai és logikai réteg esetében a rendszerbiztonságra alkalmazható szabályok vonatkoznak, míg utóbbi két réteg esetén a tartalommal kapcsolatos elvárások határozhatóak meg, emellett pedig világossá teszi, hogy a külső és belső aspektusok, bár azonosíthatóan elkülönült szintjei vannak, azonban nem szétválaszthatóak, hiszen annak integritása csak egészében szavatolható, amennyiben bármelyik réteg sérül, az egész rendszer biztonsága sérül.

Az eddigieket összegezve tehát elmondhatjuk, hogy a kibertér a földrajzi tér egy sajátos szegmense, amely jelentős hatást gyakorol a hagyományos tér-, távolság- és időértelmezésünkre és -felfogásunkra, azonban azokat egészében nem tudja felülmúlni, és ebből adódóan, mivel a földrajzi tér totalitásának a része, így az abban megjelenő jellegadó tendenciák, folyamatok a kibertérben is megjelennek, arra is hatással vannak. Látszik viszont az is, hogy a valódi jellegadó folyamatok – bár a legtöbb esetben külső téri eredményeik is vannak – a belső térben zajlanak, mindazonáltal osztva mind Jakobi, mind a Pirisi, Trócsányi szerzőpáros véleményét, a hagyományos fizikai tér hatásai alól a kibertér sem mentesülhet.

III. A KIBERTÉR TÁRSADALMI JELLEMZŐI

A Moore törvényét meghaladó fejlődés a glóbusz egészére kiépült kibertér sajátos térjellemezői miatt az az elmúlt évtizedekben radikálisan megváltoztat-

[25] Blount, 2016, 37.

[26] Werbach, 2006, 59.

[27] Kulesza, 2012, 125.

[28] Werbach, 2006.

ja a társadalmi, kulturális, politikai, intézményi és gazdasági életet.^[29] Ennek a radikális átalakulásnak a kezdőpontja és motorja az ún. új gazdaság megjelenése volt az 1970-es években, amely szakított a fordista termelési rendszerrel – megteremtve a posztfordista rendszert –, ami fejlett ipari országoknál azt eredményezte, hogy a gyáripari tömegtermelés elkezdett visszaszorulni. Ennek az új gazdasági szemléletnek a fogalmi alapját jelentik az információgazdaság, a kreatív gazdaság, a kulturális gazdaság. Az információgazdaság az új gazdaság digitális oldalát jelenti, így a gazdasági játszótér két részre bomlott: hagyományos offline gazdaságra és online gazdaságra, azonban előbbi az utóbbi nélkül már nem tud versenyképes lenni, ugyanis a kulturális gazdasági átalakulásnak köszönhetően a fogyasztói szokások is jelentősen átalakultak, ami már odáig jutott, hogy a teljes gazdaság jelentős hányadát a szolgáltatásközpontúság jellemzi, amely pedig elválaszthatatlan a kibertértől és a hozzá kapcsolódó eszközöktől.^[30] E folyamatok során „... valóban forradalmi változások kezdődtek el, amikor a gazdasági, pénzügyi, társadalmi és politikai folyamatokat egyaránt a kibertérre alapozzák... Kialakul a közösségi (másnéven megosztott) gazdaság (shared economy), amely rátelepül a határokon átnyúló infokommunikációs hálózatokra. A közösségi gazdaság az olyan eddig állandónak bizonyult alrendszereket is érintheti, mint a nemzeti pénzkibocsátás, vagy a nemzetközi pénzügyi közvetítő rendszer.”^[31] Tehát a kibertér kiépülésének és az azt megalapozó gazdasági átalakulásnak köszönhetően beteljesedett a globalizáció a pénzügyi, gazdasági és a kulturális viszonyokban. Ennek a globalizációnak az egyik velejárója, de sok tekintetben katalizátora a digitális transzformáció, amely „... az új, áttörő technológiák elfogadása és integrálása a vállalati működésbe”.^[32] E tendencia révén pedig az egyes intézmények, szektorok biztonsági kockázatai csak fokozódnak.

E közegben, ahol a fogyasztói igények alakítása alapvető gazdasági igényként fogalmazódik meg, nem véletlen, hogy az egyén társadalmi helyzete, szerepe és gondolkodása jelentősen átalakul, ami erőteljesen köthető a kibertérhez is. Ennek kitűnő példája a WEB 2.0 megjelenése, amely meglehetősen bizakodó hangulatot eredményezett: az elvárást, hogy kialakulásával létrejön a korlátok nélküli kommunikáció terepe. Azonban – ahogy arra Gosztanyi Gergely kiválóan rámutat – csakhamar kiderült, hogy valóban a magáncenzúra (vagy óvatosabban: magánkuratálás) korszakába léptünk,^[33] ahol a szűrőbuborék-rendszer^[34] révén a kibertér egyes szereplői „képesek befolyással lenni az éntudatra és a közösségre.”^[35] E keretből pedig nincs menekvés, ugyanis – ahogy Manuel Castells spa-

[29] Dodge – Kitchin, 2001, 13.

[30] Baji, 2014, 119–120.

[31] Pintér, 2016, 330.

[32] Hortoványi – Szabó – Nagy – Stukovszky, 2020, 74.

[33] Gosztanyi, 2022, 84–86.

[34] Koltay, 2019, 4–7.

[35] Mészáros, 2006, 494.

nyol szociológus írja – a hálózathoz tartozás a létezés fokmérőjévé vált,^[36] ahol a „hálózati társadalom testetlenné teszi a hálózati viszonyokat”.^[37] Mary Aiken, a neves ír kiberpszichológus egyenesen odáig megy, hogy azt állítja, az egyén számára „a technológia olyan természetessé vált, mint a belélegzett levegő. Olyan szükség a 21. században való túléléshez, mint a testünket felüdítő víz. A környezetünk részévé vált.”^[38] Mindezt ismerve, Castells mégis megfogalmazta a hálózatba ágyazott individualizmus eszméjét, amely szerint a virtuális közösség énközpontú vagy személyre szabott közösség.^[39] Sherry Turkle *Alone Together* című könyvében kifejti, hogy a túlterhelt életvitelnek köszönhetően az emberek olyan kapcsolatokat alakítanak ki, illetve tartanak fenn, amelyek alacsony kockázatúak: Facebook-barátok, avatarok,^[40] IRC chat-partnerek, vagyis olyan hálózatokhoz akarunk tartozni, ami kényelmes számunkra – azonos világnézet, tényleges intimitás és a konfliktus hiánya –, és ahol a kontroll látszata fennáll.^[41] Tehát egy meglehetősen furcsa kettősséggel találkozunk: az ember számára a hálózathoz tartozás létszükséggé vált, és emellett mégis az énközpontúság jellemzi – ez pedig nyilvánvaló feszültséget okoz, egyénen és társadalmon belül is. Eme feszültség abban jelenik meg szélesebb spektrumú problémaként – ahogy Arturo Escobar erre felhívta a figyelmet –, hogy nemcsak a kibertér gyakorol hatást a hagyományos térre, hanem az is viszonzhatást gyakorol rá. A technológia ugyanis alapvetően társadalmi konstrukció, amely révén a hagyományos tér folyamatai nem szeparálhatók a kibertér folyamataitól; azok szorosan összefonódnak egymással.^[42] Megerősíti ezt, ha visszatartunk a kibertér földrajzi térben betöltött szerepére, ugyanis az egészében társadalmi eredetű, így nem lehet független az offline világtól és annak térbeli totalitásától sem.^[43]

Így a hagyományos tér társadalmi feszültségei – legyenek azok politikai, vallási, ideológiai, kriminológiai jellegűek – ebben a globális belső kibertérben szintén megjelennek. Castells is felhívja erre figyelmet, mikor rögzíti, hogy a hálózati társadalmakból – ahogy a korábbi korok társadalmáiból sem – nem hiányoznak a társadalmi konfliktusok.^[44] Eme feszültségek ezekben a személyre szabott globális közösségekben azonban – ahol az egyén sérelme, érdeke, világlátása hatványozott számban és mértékben tudja formálni a hálózat többi tagjának értékrendjét, éntudatát – fokozott intenzitással jelennek meg. Amerikai szociológusok is felhívták a figyelmet arra, hogy a kibertér alapvetően alkalmas volna arra,

[36] Pintér, 2007, 25.

[37] Castells, 2007, 433.

[38] Aiken, 2020, 103.

[39] Bell, 2007, 67.

[40] Avatar: virtuális én, valós énünk online reprezentációja. Ld. bővebben: Erdős – Németh – Bayboeva, 2023, 17.

[41] Turkle, 2011, 295.

[42] Escobar, 1994, 211-231.

[43] Jakobi – Lengyel, 2014, 43.

[44] Castells, 2007, 434.

hogy a társadalmi töréspontokat csökkentsék a civil szerveződések és az állam szociális szerveinek hatékonyságának a fokozása által, azonban a kibertér arra is tökéletesen alkalmas, hogy ezek megfelelő működése nélkül a hagyományos konfliktusok tovább éleződjenek.^[45] A növekvő társadalmi feszültséget a társadalmi mozgalmak is kifejezésre juttatják, és a saját eszközeiket, a globalizálódó technológiát és kultúrát fordítják szembe a hálózati világgal. Ebből kifolyólag a kibertér által nyújtott lehetőségeket kihasználva egyes terrorszervezetek, bűnszervezetek erősítik transznacionális jellegüket, és újfajta, hibrid biztonsági problémaként, kihívásként jelentkeznek.^[46] Nem véletlenül használják fel ezek a szervezetek hagyományos tevékenységük fokozására a kibertérrel, mivel „szinte végtelen számú búvóhely van itt...”,^[47] tehát a közeg tökéletesen alkalmas arra, hogy a problémás magatartások széles skálájának otthont adjon.^[48]

A biztonsági problémát fokozza, hogy a globális kibertérhez kapcsolódnak az egyes gazdasági, pénzügyi szereplők, valamint a nemzetállami és szupranacionális közösségek intézményei. Így a társadalmi feszültségből eredő és az államközi konfliktusok közvetlen célpontjává válhatnak a kibertérhez kapcsolódó, előbb felsorolt szereplők is. „Az információs társadalom fizikai életterét (hardverét) az állami és a nem állami szervek, valamint a velük közvetlen – ma leginkább elektronikus – kapcsolatban álló állampolgárok hálózata alkotja... az új társadalom »idegrendszere« az informatikai, hírközlési infrastruktúra, az immunrendszere pedig az informatikai biztonság és adatvédelem. A társadalom folyamatainak irányítását és vezetését (szoftverét) pedig azon stratégiák jelenthetik, amelyek képesek a közösség érdekei szerint megvédeni az értékeket, továbbá garantálják az élettér fenntartását és a társadalom különböző szegmenseinek biztonságos működését.”^[49] Kifejezetten növeli a sérülékenységet az államokban kibertérben, hogy elveszítették a kontrollt az információ felett – melyeket sok esetben viszont transznacionális vállalatok birtokolnak –, pedig az információ ellenőrzése már az információ kora előtt is az államhatalom alapja volt.^[50] Nem véletlen, hogy a kibertér, bár direktben nem, de közvetett módon a politikai hatalom gyakorlását is érinti,^[51] ott, ahol bírják a hatalom birtokosai az információt, ott ezt erősíti, ahol viszont nem rendelkeznek a szükséges információval, ott gyengíti a hatalom gyakorlását. Mindez pedig az állam geopolitikai helyzetét befolyásolja, működését hátráltatja, végső soron pedig a biztonságát is veszélyezteti.^[52] Nem véletlen, hogy Észtország 2017-ben, a világon elsőként

[45] Bainbridge, 2020, 1.

[46] Magyar – Simon, 2017, 57-68.; Simon – Magyar, 2017, 89-101.; Simon, 2015, 145-162.; Tóth, 2016, 26-42.

[47] Aiken, 2020, 295.

[48] Jegede – Ovia – Idam, 2016, 5.

[49] Simon, 2016, 72.

[50] Castells, 2006, 379.

[51] Blount, 2016, 5.

[52] Cattaruzza, 2019.

megállapodott külföldi adnatnagykövetség létrehozásáról, amely részeként a legfontosabb észt adatokat tartalmazó biztonsági mentést luxemburgi adnatnagykövetségen tárolja, ezzel megnehezítve azt, hogy egyes kibertámadások megbénítsák az országot. Hasonló törekvés figyelhető meg a közel-keleti arab államok körében is, igaz, ők inkább a befektetések biztonsága érdekében kívánnak kialakítani hasonló rendszereket.^[53]

IV. A KIBERTÉR NEMZETI BIZTONSÁGI DIMENZIÓJA

E körülményeket figyelembe véve a kibertér – és ezáltal a hagyományos tér – védelme és biztonsága érdekében szükséges, hogy az egyes államok fegyveres védelmi rendszerei,^[54] illetve ezen belül azok katonai karakterű szervei^[55] – és az e területtel foglalkozó kutatók – feltérképezzék és a hadtudományokhoz igazított értelmezését adják a kibertérnek, ezzel is elősegítve azt, hogy e szervek definiálni tudják a helyüket, szerepüket a kibertéri folyamatokban.

A kibertér eme szűkített értelmezésének szükségességét megerősíti az is, hogy az „információval bárki képes lehet életeket kioltani..., ugyanis: Az internetes és kommunikációs hálózatokra kapcsolt eszközök akár fegyverhez hasonló felhasználást is eredményezhetnek... a pusztítás eszköze, mértéke, illetve társadalmi hatása is inkább a háborúk, vagy az ipari és természeti katasztrófák jogilag csak speciálisan megítélhető következményeivel hasonlíthatók.”^[56] Ezt felismerve, a NATO 2016-ban a kibertérrel is hadszíntérré minősítette.

A definícióalkotás valódi nehézségét e területen az adja – ahogy azt S. Michael Pavelec megfogalmazta –, hogy a hagyományos katonai rendszerekhez képest a kibertér veszélye és előnye, hogy az kiterjed az egész társadalomra, kormányzatra/közigazgatásra, katonaságra, civil szférára és azok mindennapi életére, ennek okán elengedhetetlen, hogy a kibertérre sajátos katonai doktrínákat, stratégiákat dolgozzanak ki, hiszen ezek szükségesek annak megértéséhez és végső soron a hálózatnak és az ahhoz kapcsolódó személyeknek, szervezeteknek a megvédéséhez.^[57] Eme összetettséget hangsúlyozza ki Zachary M. Smith is, amikor a kiberbiztonságról, kibervédelemről ír, ugyanis rögzíti, hogy a kibervédelem nem önállóan állami tevékenység eredménye, hanem a kibertér jellege okán ahhoz elengedhetetlenül szükséges a civil (azaz a magán- és gazdasági) szféra is.^[58]

[53] Prakash, 2018, 145.

[54] Farkas, 2016; Farkas, 2017, 44-58.; Farkas, 2017, 5-20.

[55] Farkas, 2012, 3-6.

[56] Simon, 2016, 34., 41-42.

[57] Pavelec, 2015, 120-124.

[58] Smith, 2017, 62-66.

Steve Winterfeld és Jason Andress munkájukban úgy fogalmaztak, hogy a kibertérben a csatátér magába foglalja a hálózatokat, a számítógépeket, a hardvereket (ez magában foglalja a beágyazott számítógépes chipeket tartalmazó fegyverrendszereket), a szoftvereket (kereskedelmi és kormányzati fejlesztések), az alkalmazásokat (például parancs- és vezérlőrendszerek), a protokollokat, a mobil eszközöket és az embereket, akik működtetik az egyes eszközöket.^[59]

Az Egyesült Államok Védelmi Minisztériuma által létrehozott meghatározás szerint a kibertér az „informatikai (információs) környezetben értelmezett globális tartomány (domain), amely magába foglalja az IT infrastruktúrák egymással összefüggő elemeinek hálózatát, beleértve az internetet, a telekommunikációs hálózatokat, számítógépes rendszereket, valamint a beágyazott feldolgozó és vezérlő elemeket.”^[60] Szintén ad egy fogalmat a Magyar Honvédség Kibervédelmi szakmai koncepciója is: „a kibertér elektromágneses spektrum használatával meghatározható, dinamikusan változó tartomány, mely az összekapcsolt hálózatok, eszközök és kiegészítő fizikai infrastruktúrák közötti adatok kezelésére szolgál”.^[61] Mindkét meghatározás hiányossága az, amit e tanulmány bevezetőjében is írtam, hogy a kibertérnek annak technikai sajátosságai felől definiálja, és kihagyja annak a biztonság szavatolás oldaláról jelentős, más tudományterületeket is érintő jellemzőit, így például az egyén szerepét a rendszerek integritásában, vagy a térjellemzőiből és azok rétegeiből következő összetett sérülékenységi problematikáját.

A katonai karakterű szervek tevékenységéhez igazodó kibertérértelmezés tehát nem nélkülözheti annak civil sajátosságait, azonban, ahogy arra Haig Zsolték felhívják a figyelmet szükséges azt a civil sztereotípiáktól varázstalanítani. Ugyanis többek között, „a kibertér meghatározásával kapcsolatban – civil értelmezés szerint – általánosan elterjedt nézet, hogy az a számítógép-hálózatokkal és az internettel van összefüggésben. A kibertér katonai értelmezése azonban kiterjeszti ezt a dimenziót, és nemcsak a számítógép-hálózatok működési környezetét érti alatta.”^[62] Kassai Károly pedig emellett rögzíti a kibertér katonailag kiemelt sajátosságát, hogy „fizikai jellemzőkkel nehezen meghatározható, a képességek alakulása szerint dinamikusan változó tartalommal bír, beleértve az adatok és hozzáférési lehetőségek sokféleségét”,^[63] amelyek okán elengedhetetlenül szükséges a nemzetközi trendek és folyamatok ismerete, a sebezhetőségek azonosítása^[64] és a felhasználói tudatosság magas szinten tartása, amely magában hordozza a szövetségi és nemzeti szereplők közötti információáramlást.

A NATO fogalmi attitűdje azonban maradt technológiai központú. Alapvetően a kibertér egy összetett dinamikus környezetnek tekintik, amely a működési

[59] Winterfeld – Andress, 2013, 22.

[60] Joint Publication 1–02 Department of Defense Dictionary of Military and Associated Terms, 57.

[61] A honvédelmi miniszter 60/2013. (IX. 30.) HM utasítása, 1. melléklet, 2. pont 8.

[62] Haig – Kovács – Ványa – Vass, 2014, 23.

[63] Kassai, 2012, 129.

[64] A kibertér sebezhetőségét fokozó karakterisztikáiról ld. Németh, 2019, 307-325.

környezet egyik komponense.^[65] A 2020-ban közétett kiberműveleti doktrínában található fogalom már a fentieknek – Haig, Kassai – megfelelően tartalmaz új fogalmi elemeket is. Ugyanis a doktrína szerint a kibertér „az összes összekapcsolt kommunikációs, informatikai és egyéb elektronikus rendszerből, hálózattól és azok adataiból álló globális terület, beleértve az elkülönült vagy független rendszereket is, amelyek adatokat dolgoznak fel, tárolnak vagy továbbítanak”.^[66] Vagyis kiemelt részét képezi a fogalomnak az adatvagyon is. Emellett viszont a fogalmi elhatárolásban továbbra sem jelenik meg a kibertér társadalmi jellege, amely viszont a nemzeti biztonság szempontjából legalább annyira releváns, mint a technológiai oldal. Ugyanis például a jogi eljárások és szabályozás kialakítása terén – Escobar és Castells gondolatait továbbfűzve – a technológia és társadalom egymás esszenciális jellegét jelenthetik, hiszen mára a technológiának a társadalmi, a társadalomnak pedig a technológiai realitása megkérdőjelezhetetlen; a hatás–viszonytatás pedig mindkettő esetében strukturális változásokat eredményezhet. Így a jog mint társadalmi jelenség, a társadalmi totalitás egyik részobjektuma is ezen változó környezet része, amelyre ugyanúgy hatással van a technológia. Viszont a társadalom oldaláról biztonságos keretek kialakítását teszi lehetővé a megfelelő mélységű és színvonalú jogi szabályozás, a technológia fejlesztések, azok alkalmazása és továbbfejlesztése terén. Nem elhanyagolható e szempontból pedig, hogy az ezen nyugvó jogi környezet az állam biztonsági, védelmi, valamint államközi tevékenységének technológiai oldalát nézve is megfelelő, garanciális és nem utolsósorban jogállami foglalatát adhatja. Ehhez viszont szükségképpen fel kell ismerni, hogy a kibertérnek és a kibertér biztonságának nemcsak technológiai fogalmi jegyei vannak, hanem társadalmiak is.

V. UTÓSZÓ

A fenti fogalmak és jellemzők összegzéseként mindenképpen levonható az a következtetés, hogy a kibertér a földrajzi tér egy olyan sajátos, folytonosan változó része, amely a hagyományostér-elemekkel kölcsönhatásban van, de azoktól mégis elkülönült, egyedi térjellemzőkkel bíró térréteg. E virtuális téren keresztül milliós nagyságú információs áradat halad át egyetlen perc leforgása alatt. „Egyértelműen prognosztizálható: a kibertér rendszerei egyre nagyobbá, gyorsabbá és komplexebbé válnak”^[67] az elkövetkező években. Ezáltal még inkább mindenki számára könnyen hozzáférhetővé válik ez a folyamatosan bővülő entitás, amely valós hatást gyakorol az egyén, valamint a társadalom önképére, a társadalmi reflexiókra, a globális gazdaságra, és amelyben aktív szereplőként jelennek meg az államok igazgatási és katonai karakterű szervei.

[65] Munk, 2018, 115.

[66] Allied Joint Publication-3.20 Allied – Joint Doctrine for Cyberspace Operations. NATO standard, 4.

[67] Babos, 2011, 42.

A kibertér tehát ebben a felfogásban nemcsak a földrajzi tér része, hanem a társadalmi totalitás olyan részegysége, amely közvetlenül befolyásolja a társadalmi totalitás többi részegységét, így többek között az egyéneket, a társadalmi hálózatokat és a társadalmi struktúrát, az állami intézményrendszert és feladatellátást, a biztonsági rendszereket és a jogi szabályozást is. E hatás megkerülhetetlen velejárója, hogy a társadalmi totalitás érintett részkomplexumainak választ kell adniuk arra a kihívásra, amelyet a kibertér és a hozzá kapcsolódó technológiák jelentenek.

IRODALOM

- Aiken, Mary (2020): *Cyber-csapda – Hogyan változtatja meg az online tér az emberi viselkedést?* Harmat– Új ember, Budapest.
- Babos Tibor (2011): „Globális közös terek” a NATO-ban. In: *Nemzet és biztonság*. 2011/3. sz.
- Bainbridge, William Sims (2020): *The Social Structure of Online Communities*. Cambridge University Press, Cambridge.
- Baji Péter (2014): Az internet, a tér és az új gazdaság Budapesten. In: *Tér*. 2014/4. sz. DOI: <https://doi.org/10.17649/TET.28.4.2628>.
- Batty, Michael (1997): Virtual Geography. In: *Futures*. 1997/4–5. sz. DOI: [https://doi.org/10.1016/S0016-3287\(97\)00018-9](https://doi.org/10.1016/S0016-3287(97)00018-9).
- Bell, David (2007): *Cyberculture Theorists – Manuel Castells and Donna Haraway*. Routledge, London – New York.
- Blount, P. J. (2016): *Reprogramming the World: Cyberspace and the Geography of Global Order* (disszertáció). The State University of New Jersey, Newark.
- Castells, Manuel (2006): *Az információ kora: Gazdaság, társadalom és kultúra – Az identitás hatalma*. Gondolat Kiadó, Budapest.
- Castells, Manuel (2007): *Az információ kora: Gazdaság, társadalom és kultúra III. kötet – Az évezred vége*. Gondolat Kiadó, Budapest.
- Cattaruzza, Amaël (2019): *A digitális adatok geopolitikája – Hatalom és konfliktus a big data korában*. Pallas Athéné Books, Budapest.
- Dodge, Martin – Kitchin, Rob (2001): *Mapping Cyberspace*. Routledge, London–New York.
- Erdős, Ferenc – Németh, Richárd (2019): AMT-based Real-Time, Inter-Cognitive Communication Model. In: *Acta Polytechnica Hungarica – Journal of Applied Sciences*. Vol. 16, No. 6/2019. DOI: 10.12700/APH.16.6.2019.6.8.
- Erdős, Ferenc – Németh, Richárd – Bayboboeva, Firuza (2023): Virtual Teamwork in Gamified 3D Environment. In: *Infocommunications Journal*. 15., Special Issue. DOI: <https://doi.org/10.36244/ICJ.2023.SI-IODCR.3>.
- Escobar, Arturo (1994): Welcome to Cyberia – Notes on the Anthropology of Cyberculture. In: *Current Anthropology*. 1994/3. sz. DOI: <https://doi.org/10.1086/204266>.
- Farkas Ádám (2012): A katonai büntetőjog és igazságszolgáltatás helye, szerepe, létjogosultsága az állam és társadalom rendszereiben. In: *Hadtudomány*. 2012/elektronikus sz.
- Farkas Ádám (2016): *Tévelygések fogásában?: Tanulmányok az állam fegyveres védelmének egyes jogtani és államtani kérdéseiről, különös tekintettel Magyarországi katonai védelmére*. Magyar Katonai Jogi és Hadijogi Társaság, Budapest.

- Farkas Ádám (2017a): Adalékok az állam fegyveres védelmének rendszertani megközelítéséhez. In: *Honvédségi Szemle*. 2017/1. sz.
- Farkas Ádám (2017b): A terrorizmus elleni harc, mint kiemelt ágazatközi fegyveres védelmi feladat. In: *Szakmai Szemle*. 2017/3. sz.
- Gibson, William (1984): *Neuromancer*. ACE Publishing Group, New York.
- Gosztonyi Gergely (2022): *Cenzúra Arisztotelésztől a Facebookig – A közösségi média tartalomszabályozási gyakorlatának komplexitása*. Gondolat Kiadó, Budapest.
- Haig Zsolt – Kovács László – Ványa László – Vass Sándor (2014): *Elektronikus hadviselés*. Nemzeti Közszerkeleti és Tankönyv Kiadó Zrt., Budapest.
- Hortoványi Lilla – Szabó Zsolt Roland – Nagy Sándor Gyula – Stukovszky Tamás (2020): A digitális transzformáció munkahelyekre gyakorolt hatásai – Felkészültek-e a hazai vállalatok a benne rejlő nagy lehetőségre (vagy a veszélyekre)? In: *Külgazdaság*. 2020/március-április.
- Jakobi Ákos – Lengyel Balázs (2014): Egy online közösségi háló offline földrajza, avagy a távolság és a méret szerepének magyar empiriái. In: *Tér*. 2014/1. sz.
DOI: <https://doi.org/10.17649/tet.28.1.2590>.
- Jakobi Ákos (2002): A virtuális világ terei. In: *Magyar Tudomány*. 2002/11. sz.
- Jegede, Ajibade Ebenezer – E. Ovia – SC. Idam (2016): Cyberspace and Crime Engineering: A Sociological Review. In: *International Journal of Forensic Sciences*. 2016/1. sz.
- Kassai Károly (2012): Kiberveszély és a Magyar Honvédség. In: *Hadmérnök*. 2012/4. sz.
- Koltay András (2019): A social media platformok jogi státusa a szólásszabadság nézőpontjából. In: *In Medias Res*. 2019/1.
- Kulesza, Joanna (2012): *International Internet Law*. Routledge, London, New York.
- LightReading: Moore's Law Is Dead. Where Is Energy Saving Heading in the Electronic Information Industry? (Elérhető: <https://www.lightreading.com/moores-law-is-dead-where-is-energy-saving-heading-in-electronic-information-industry/a/d-id/781014> Le-töltés ideje: 2023.02.04.).
- Magyar Sándor – Simon László (2017): A terrorizmus és indirekt hadviselés az EU kiber-térben. In: *Szakmai Szemle – A Katonai Nemzetbiztonsági Szolgálat tudományos-szakmai folyóirata*. 2017/4. sz.
- Mészáros Rezső (2006): A kibertér, mint új földrajzi tér. In: Kiss Andrea – Mezősi Gábor – Sümeghy Zoltán (szerk.): *Táj, környezet és társadalom – Ünnepi tanulmányok Keveiné Bárány Ilona professzor asszony tiszteletére*. SZTE Éghajlattani és Tájföldrajzi Tanszék, Szeged.
- Moore, Gordon E. (1965): Cramming more components onto integrated circuits. In: *Electronics*. 1965/8. sz.
- Munk Sándor (2018): A kibertér fogalmának egyes, az egységes értelmezést biztosító kérdései. In: *Hadtudomány*. 2018/1. sz.
- Nagy Károly (1999): Titok és biztonság az információs társadalomban. In: *Belügyi Szemle*. 1999/4–5. sz.
- Németh Richárd (2019): Kibertámadások gazdasági vonatkozásai a vállalati szférában. In: Dernóczy–Polyák Adrienn (szerk.): *Kutatási jelentés I*. Universitas–Győr Nonprofit Kft., Győr.
- Pavelec, S. Michael (2015): Cyber Warfare in the Professional Military Education System. In: Spinger, Paul J. (szerk.): *Cyber Warfare*. ABC–CLIO, Santa Barbara–Denver–Oxford.
- Pintér István (2016): A virtuális tér geopolitikája. In: Pintér István (szerk.): *A virtuális tér geopolitikája – Geopolitikai Tanács Műhelytanulmányok*. Geopolitikai Tanács Közhasznú Alapítvány, Budapest.
- Pintér Róbert (2007): Úton az információs társadalom megismerése felé. In: Pintér Róbert: *Az információs társadalom – Az elméletől a politikai gyakorlatig*. Gondolat – Új Mandátum, Budapest.

- Pirisi Gábor – Trócsányi András (2015): *Általános társadalom- és gazdaságföldrajz*. (Elérhető: <http://tamop412a.ttk.pte.hu/files/foldrajz2/ch01s02.html>. Letöltés ideje: 2023.02.04.).
- Pirisi Gábor – Trócsányi András (2019): *Fejezetek a társadalomföldrajz világából*. Publikon Kiadó, Pécs.
- Prakash, Abishur (2018): *Új geopolitika – A világ jövője technológia, I-II. kötet*. Pallas Athéné Könyvkiadó, Budapest.
- Simon László – Magyar Sándor (2017): A terrorizmus és indirekt hatása a kibertérben. In: *Nemzetbiztonsági Szemle*. 2017/3. sz.
- Simon László (2015): A fokozódó terrorizmus Európában és annak hatása a katonai tömegrendezvények biztosítására. In: *Szakmai Szemle – A Katonai Nemzetbiztonsági Szolgálat tudományos-szakmai folyóirata*. 2015/2. sz.
- Simon László (2016): A titok speciális értelmezése az elmúlt 25 év kihívásainak, kockázatainak és fenyegetéseinek tükrében. In: *Felderítő Szemle*. 2016/1. sz.
- Simon László (2016): Az információ mint fegyver? In: *Szakmai Szemle*. 2016/1. sz.
- Smith, Zachary M. (2017): Cyber Security. In: Spinger, Paul J. (szerk.): *Encyclopedia of Cyber Warfare*. ABC-CLIO, Santa Barbara-Denver.
- Stokes, Christopher (2009): Chapter 2 – OSI Model and Then Some. In: Dale, Liu (szerk.): *Next generation SSH2 implementation: securing data in motion*. Burlington, Elsevier. DOI: <https://doi.org/10.1016/B978-1-59749-283-6.00002-7>.
- Szkála Károly – Munka Sándor (2018): A kibertér fogalma, értelmezése és fejlődése. In: *Földrajzi Közlemények*. 2018/4. sz.
- Tóth Zoltán Balázs (2016): Az Iszlám Állam online térhódítása. In: *Nemzetbiztonsági Szemle*. 2016/4. sz.
- Turkle, Sherry (2011): *Alone Together – Why We Expect more from Technology and Less from Each Other*. Basic Books, New York.
- Werbach, Kevon (2006): A Layered Model for Internet Policy. In: *Journal on Telecommunications and High Technology Law*. 2006/2. sz.
- Winterfeld, Steve – Andress, Jason (2013): *The Basics of Cyber Warfare Understanding the Fundamentals of Cyber Warfare in Theory and Practice*. Elsevier, Waltham.
- Wright, Gavin: ARPANET. In: *TechTarget/Networking*. (Elérhető: <https://www.techtarget.com/searchnetworking/definition/ARPANET> Letöltés ideje: 2023.02.04.).

JOGFORRÁSOK

- Allied Joint Publication-3.20 Allied – Joint Doctrine for Cyberspace Operations. NATO standard, January 2020. (Elérhető: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/899678/doctrine_nato_cyberspace_operations_ajp_3_20_1_.pdf. Letöltve: 2023.02.04.).
- Joint Publication 1–02 Department of Defense Dictionary of Military and Associated Terms, (Elérhető: https://fas.org/irp/doddir/dod/jp1_02.pdf Letöltés ideje: 2023.02.04.).
- A honvédelmi miniszter 60/2013. (IX. 30.) HM utasítása a Magyar Honvédség Kibervédelmi Szakmai Koncepciójának kiadásáról.