Balogh Péter

Aszimmetrikus fenyegetések és a hibrid hadviselés jelenkori sajátosságai és hálózatai

Bevezetés

A tanulmány keretében arra vállalkozunk, hogy az aszimmetrikus és hibrid fenyegetések kérdéskörével kapcsolatos kutatásaink némely releváns eredményét bemutassuk.

A munka első részében a koncepcionális és fogalmi keretek felvázolásával igyekszünk megragadni ezt a meglehetősen szerteágazó és így sokrétűen értelmezett jelenségkört. Olyan megközelítésmódokat és modelleket tekintünk át, amelyek egyrészt hatékony segítséget nyújthatnak e komplex kérdéskör interpretációjához, másrészt megfelelő alapot képezhetnek empirikus vizsgálataink számára.

A tanulmány folytatásaként bemutatjuk a munkánk során alkalmazott kutatásmódszertant, majd az ennek fényében elkészített esettanulmányok révén illusztráljuk főbb kutatási eredményeinket. Kitérünk a terrorizmus bizonyos új évezredbeli jellegzetességeire, valamint az érdekérvényesítés komplex formáira – mindezt a hálózatelemzési szemléletmód fókuszba helyezésével.

Az írásmű végén az eredmények összefoglalása mellett lehetséges további kutatási irányokra is utalunk.

1. Problémafelvetés

1.1. Átalakuló hadviselés az új évezredben

A nemzetközi konfliktusok, a fegyveres szembenállás és háború formája, jellege, lefolyása terén az utóbbi időszakban egyfajta átalakulás jelei figyelhetők meg.[1] Számos olyan fogalmi keret, koncepció, kifejezés került előtérbe vagy jelent meg – a teljesség igénye nélkül: hibrid háború, nemlineáris hadviselés, határok nélküli hadviselés, nem konvencionális hadviselés, szürkezóna-konfliktus, irreguláris hadviselés, nem kinetikus hadviselés, információs hadviselés, politikai hadviselés, hálózati háború, kiberhadvise-

[1] Lásd ehhez például: Resperger István – Somkuti Bálint: Hybrid Warfare or the Ever Changing Face of War. *Defence Review,* 144. (2016), 1. 73–79.

https://doi.org/10.36250/01104_02

lés, lélektani hadviselés, *soft power* –, amely a jelenség eme megváltozott aspektusára, illetve újszerű megoldásaira utal.[2]

A háború transzformációja és pluralizációja – a technológiai fejlődés egyértelmű meghatározó jellegén túl – egyrészt tehát magában foglalja a fegyveres konfliktusok új típusainak megjelenését.[3] A hagyományos vagy 1. régi háború mellett a 2. új háború kibontakozásának lehettünk tanúi, amelynek alapja, illetve sajátos ismertetőjegye az erőszak privatizált formáinak előtérbe kerülése. Részben eltérő aspektusban jelent átalakulást a 3. virtuális háború formája, illetve kibontakozása, amely jelentősen összekapcsolódik a nyilvánosság és a közvélekedés terén végbement fejleményekkel. A 4. globalizált terrorkockázat mint a háború különálló – meghatározott elméleti megfontolások alapján kialakított – típusa pedig – nem meglepő módon – a 2001. szeptember 11-i támadások nyomán megjelenő, sajátosan elkülönülő konfliktusformára reflektál.[4] Ugyanakkor a típusalkotás mellett a változások strukturális jellege talán lényegesebb aspektus. A háború pluralizációjának gondolata éppenséggel – jellemzően – azt a szerveződésbeli, a háború tágabb társadalmi kontextusára vonatkozó átalakulást ragadja meg, amely a transzformációnak különös jelentőséget kölcsönözhet. Meghatározó eleme, hogy a fegyveres konfliktusok és az ezektől mentes időszakok, illetve területek egymástól való diszkrét elkülöníthetősége megkérdőjeleződik, problematikussá válik. A háború és a béke – pontosabban a béke érzete – nem válik el egymástól, illetve az az iránti igény és a valós háború a társadalmi dimenzióban egyszerre lehet jelen, egyfajta imázsteremtés eredményeként.[5]

Ebben a kettősségben nem kis szerepe van a háború virtualizálódásának, amely a hadviselő fél – jellemzően a kezdeményező – számára abból a szempontból kiemelt jelentőségű, hogy a lehetséges kockázatokat és a felmerülő áldozatokat lehetőség szerint saját társadalma számára[6] valami távoli, érdemi kihatással nem vagy csak kismértékben teheti bemutathatóvá s ezáltal elfogadhatóbbá. A virtuális dimenzió felértékelődésében kiemelt jelentőségre tesz szert a háborúk megvívása szempontjából az egyre inkább kiszélesedő, globalizálódó nyilvánosság, a nemzetközi vagy világnyilvánosság. A szélesebb szintű társadalmi elfogadás, legitimáció – részben legalábbis, de egyre jelentősebb mértékben – áttevődik a nemzetközi színtérre, helyet adva a kozmopolita legitimáció térnyerésének. A nemzetközi nyilvánosság szerepe tehát felértékelődik a fegyveres konfliktusok elfogadtatása terén, mivel ahhoz immár nem elegendő csupán a nemzeti,

[2] Lásd ehhez például: Kiss Álmos Péter: A hibrid hadviselés természetrajza. *Honvédségi Szemle,* 147. (2019), 4. 17–37.; Nagy Bianka: Az orosz nem lineáris hadviselés és az ellene irányuló önvédelem lehetőségei. *Felderítő Szemle,* 17. (2018), 1. 143–150.; Resperger István: A nemzetbiztonsági szolgálatok tevékenysége – biztonsági kihívások, kockázatok és fenyegetések. In Resperger István (szerk.): *Nemzetbiztonsági alapismeretek*. Budapest, Dialóg Campus Kiadó, 2018. 29–93.

[3] Ulrich Beck: *Világkockázat-társadalom. Az elveszett biztonság nyomában.* Szeged, Belvedere Meridionale, 2008.

[4] Beck (2008): i. m. 181–183.

[5] Manuel Castells: *A hálózati társadalom kialakulása.* Budapest, Gondolat Kiadó – Infonia Kiadó, 2005.

[6] Sajátos és figyelemre érdemes esetet jelent, amikor a kezdeményező hadviselő fél a megtámadott fél társadalma számára igyekszik kisebbíteni, akár elkendőzni műveletei céljait. Lásd erről később a hibrid hadviselés kapcsán.

saját társadalom részéről kapott felhatalmazás, az új viszonyok között mértékadó, globális szintű elfogadottság – posztnemzeti legitimáció – szükséges.[7]

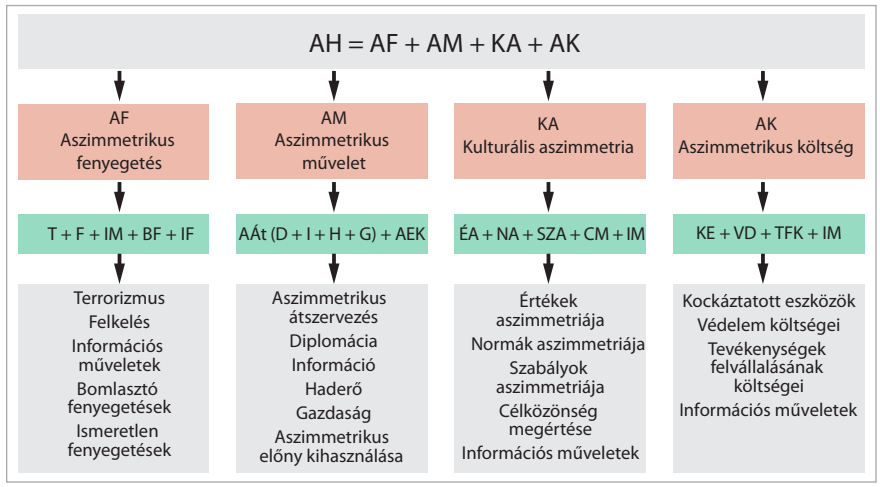
Lényegessé válik tehát a közvélekedés és a nyilvánosság a konfliktusok megvívása, lebonyolítása és kezelése terén, aminek egyik – egyre markánsabbá váló – aspektusa a megkérdőjelezhetőség és a tagadhatóság mint lehetőség és követelmény.[8] A műveleteket végrehajtó feleknek jelentős előnyük származhat abból, ha képesek elhárítani maguktól a felelősséget a nyilvánosság – legalábbis egy részének – eredményes meggyőzésével arról, hogy a kérdéses tevékenység nem hozzájuk kötődik, vagy az nem bizonyítható. Az alkalmazott eljárások egyre inkább azt kívánják, hogy az elérni szándékozott hatások minél inkább közvetett formában merüljenek fel: 1. közvetlen kontroll átadja helyét a 2. bizonyos kérdések terén meglévő érdekközösség alapján szerveződő tevékenységnek vagy 3. a döntéshozás érdekelt fél számára kedvezően történő alakításának.[9]

1.2. Aszimmetria, hadviselés, terrorizmus

Az *aszimmetrikus hadviselés,* a *negyedik generációs háború,* továbbá az *új terrorizmus* koncepciói a fegyveres konfliktusok utóbbi időszakban tapasztalható átalakulásának tekintetében felmerülő hasonló tendenciákra vezethetők vissza. Az aszimmetrikus hadviselés arra vonatkozik, hogy meghatározó változások, illetve újdonságok jellemzők a hadviselés terén az alkalmazott erő, illetve a fenyegetések költségessége tekintetében (1. ábra).

Az idődimenzió terén hasonlóan jelentős eltérések figyelhetők meg (például adott elkövető, illetve katona bevethetőségéhez szükséges kiképzési idő hossza), de az *alkalmazott módszerek* és célkitűzések is sajátosan jelennek meg az aszimmetrikus támadások esetében.[10] Az elkövetők *új megközelítések* alkalmazására törekszenek az ellenség támadása vagy éppen az azzal való szembeszállás terén. A műveletek kezdeményezői között gyakran jelennek meg *nem állami szereplők,*[11] így lényeges tényező, hogy az állam erőszak-monopóliumának elve sérül, aminek messzemenő következményei lehetnek.[12] Könnyen előfordulhat, hogy egy államnak olyan harctéren szükséges érvényesítenie akaratát, illetve erőfölényét, ahol akár több, kisebb méretű, lazán, hagyományos bürokratikus forma nélkül megszervezett, megszerveződött csoport áll vele szemben, amely jellemzően szokatlan eljárásokat alkalmazva igyekszik elkerülni a közvetlen összecsapásokat.[13]

[7] Beck (2008): i. m. 185–189.
[8] Lásd ehhez például: Kiss (2019): i. m. 26–27.
[9] Raphael S. Cohen – Andrew Radin: *Russia's Hostile Measures in Europe. Understanding the Threat.* Santa Monica, RAND Corporation, 2019.
[10] Resperger István: A XXI. század fegyveres konfliktusainak hatása a hadtudományra. In Resperger István – Kiss Álmos Péter – Somkuti Bálint (szerk.): *Aszimmetrikus hadviselés a modern korban. Kis háborúk nagy hatással.* Budapest, Zrínyi Kiadó, 2015. 13–47.
[11] Somkuti Bálint: A negyedik generációs hadviselés. In Resperger et al. (2015): i. m. 48–65.
[12] Kiss Álmos Péter: Generációk a hadviselésben – a negyedik generáció. In Resperger et al. (2015): i. m. 66–80.
[13] Resperger et al. (2015): i. m. 25.



1. ábra: Az aszimmetrikus hadviselés (AH) egyenlete

Forrás: David L. Buffaloe: Defining Asymmetric Warfare. *The Land Warfare Papers,* (2006), 58. alapján a szerző szerkesztése

A negyedik generációs hadviselés esetében ugyancsak fontos tényezővé válik a *decentralizálódás* mint a konfliktus megkülönböztető jegye, valamint még nagyobb hangsúlyt kap – a már a harmadik generációs hadviselésből átöröklődő – önállóság és kezdeményezőkészség. A nem állami szereplők felemelkedése és a központi erőszak-monopólium visszaszorulása ebben az esetben is lényeges fejlemény, azonban további elem a konfliktusok mögötti *kulturális tényezőknek* a(z újbóli) megjelenése.[14] Az önszerveződő hálózati struktúra megjelenésével – a decentralizáció mellett – a kapcsolódó hálózati rendszerek egyre kevésbé centralizálttá és sűrűvé válnak.[15] Viszonylagos egyetértés mutatkozik abban, hogy mind a negyedik generációs hadviselés,[16] mind az aszimmetrikus fenyegetések egyik leginkább látható formájának a *nemzetközi terrorizmus* tekinthető.[17]

Mindazonáltal a terrorizmus jelensége is átalakulni látszik. Az ezen a téren megjelenő jelentősebb változások értelmezésének egyik irányát jelentheti az új terrorizmus koncepciója,[18] amelynek értelmében a terrorizmus alapvetően diffúz, területiségétől megszabadult, abból kiszakított *(deterritorializált)* formát ölt, nemzetállami keretekből kilépő, azokon átívelő, hálózatos szerveződési formával.[19] Az új terrorizmus mögött

[14] William S. Lind: Understanding Fourth Generation War. *Antiwar.com,* 2004. január 15.

[15] Kiss (2015): i. m. 71. Fel is merül ebben a tekintetben az a koncepcionális vita, hogy a hadviselés első három generációjának folytatása logikailag a hálózatközpontú hadviselés volna (Somkuti [2015]: i. m. 56.).

[16] Somkuti (2015): i. m. 60.

[17] Resperger (2015): i. m. 14.

[18] Peter R. Neumann: Old and New Terrorism. *Socialeurope.eu,* 2009.

[19] A terrorizmus vonatkozásában a hálózati szerveződési mód tekintetében érdemes megkülönböztetni az eleve meglévő hálózatokban rejlő hatékonyságot elsősorban a toborzás és a mozgósítás terén, míg a hierarchikus és központosított szerveződési mód elsősorban a védelem és a stratégiaalkotás szolgálatába állítható. Lásd ehhez: David Tucker: Terrorism, Networks, and Strategy. Why the Conventional Wisdom is Wrong. *Homeland Security Affairs,* 4. (2008), 42.

meghúzódó motivációs elemek jellemzően vallási jellegűek, és a támadások jóval erőszakosabb formát öltenek, a „régi" terrorizmushoz képest gyakoribbá válnak a tömeges áldozatokat követelő műveletek. Hasonló értelmezést jelent az erőszak eme formája tekintetében a *transznacionális aszimmetrikus terrorizmus* koncepciója, amely a kockázatok széles körűvé válásának gondolatára, valamint arra épül, hogy az ilyen jellegű események csak időszakosan fordulnak elő, ezért az ellenük való fellépés is sajátos szemléletmódot tenne szükségessé.[20]

1.3. Hibrid hadviselés a szürke különféle árnyalataiban

A hibrid hadviselés és a szürke zónás konfliktusok eltérő terminológiai keretek között, de lényegében nagyon hasonló jelenségre vonatkoznak, azonban a kétértelműség nemcsak fogalmilag,[21] hanem tartalmilag is meghatározó sajátossága ezen konfliktusformának.[22] Meglehetősen komplexnek, összetettnek bizonyul ugyanis a hadviselés eme formája az alkalmazott módszerek, a taktikai megoldások és a stratégiai gondolkodás tekintetében egyaránt. Mindezek terén a hibrid hadviselés általános célja a fennálló – jelenleg alapvetően a nyugati világ, mindenekelőtt az USA számára előnyös – nemzetközi rend módosítása, megváltoztatása vagy éppenséggel fenntartása.[23] Ennek érdekében a hibrid hadviselés, illetve a szürke zónás kihívások keretében az érintett felek a módszerek széles spektrumát alkalmazhatják.[24] A hagyományos eszközök, a *hard power* eszközrendszere mellett egyéb, nem konvencionális taktikák és eljárások kapnak kiemelt jelentőséget, ezáltal olyan sokoldalú kihívást hozva létre, amely katonai és politikai is egyben,[25] továbbá amelyben a társadalmi dimenzió is rendkívül hangsúlyossá válik.[26] Ennek megfelelően – ebben az esetben is – a szereplők között az államok mellett hangsúlyossá válhatnak egyéb csoportok, például terrorista vagy különféle transznacionális szervezetek.[27] A hibrid műveletek sokrétűségét illusztrálja a 2. ábra, amely egy egyszerű hibrid támadás lehetséges tovagyűrűző hatásait szemlélteti adott, több szegmensre tagolódó műveleti környezet, illetve célpontország esetében.

[20] Raphael F. Perl: Asymmetric Warfare. A Doctrine to Fit the Times. In Álmos Péter Kiss (szerk.): *Asymmetric Warfare. Conflict of the Past, the Present and the Future. Proceedings of the Conference in Budapest, Hungary, 9–10 November 2016.* Budapest, Dialóg Campus Kiadó, 2017. 43–47.

[21] A tartalmi-fogalmi dimenzió, amelyet ezen terminusok lefednek, visszaköszön az orosz és a kínai hadtudományi gondolkodásban is, amennyiben az orosz doktrína a hibrid hadviselést egy, az USA által alkalmazott megközelítésmódnak tartja, illetve a kínai katonai akadémiai gondolkodók által használt határok/kötöttségek nélküli hadviselés *(„unrestricted warfare")* is hasonlóképpen értelmezhető (International Security Advisory Board: Report on Gray Zone Conflict. *2009-2017.state.gov,* 2017. január 3.; Qiao Liang – Wang Xiangsui: *Unrestricted Warfare.* Beijing, PLA Literature and Arts Publishing House, 1999).

[22] Hal Brands: Paradoxes of the Gray Zone. *Fpri.org,* 2016. február 5.; United States Special Operations Command White Paper: The Gray Zone. *Publicintelligence.net,* 2015. szeptember 9. 1., 4.

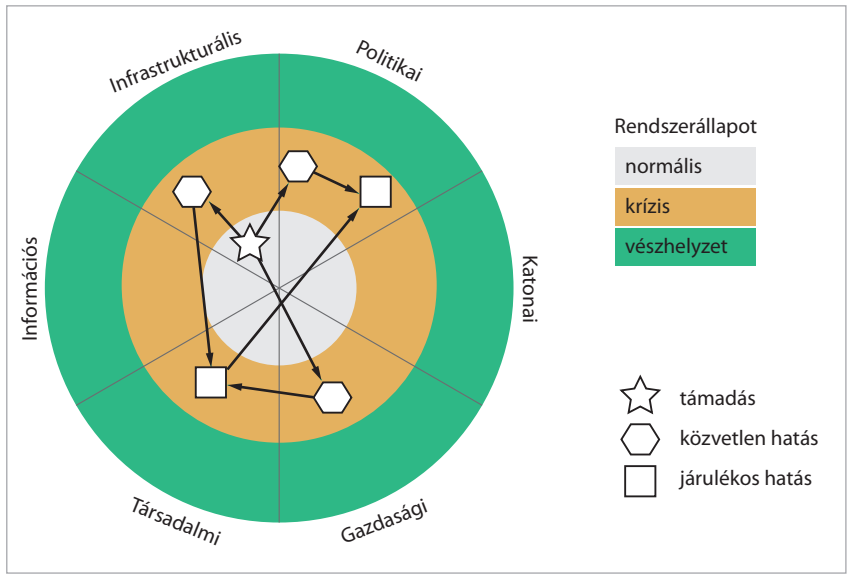
[23] United States… (2015): i. m. 5.; Brands (2016): i. m. 2., 6.

[24] International Security Advisory Board (2017): i. m. 1.

[25] Brands (2016): i. m. 2., 6.; International Security Advisory Board (2017): i. m. 2.

[26] United States… (2015): i. m. 7.

[27] International Security Advisory Board (2017): i. m. 4.



2. ábra: A hibrid hadviselés vázlata
Forrás: Kiss (2015): i. m. 23.

A hibrid műveletek tekintetében talán fokozottan utalhatunk a konfliktusok virtualizálódásának korábban felvázolt tendenciájának relevanciájára, így a hadviselés eme megközelítésmódja esetében mind magasabb stratégiai szinten, mind pedig taktikai, illetve a harc megvívásának gyakorlati dimenziója szempontjából fontos és érdekes kérdéskört jelent a *befolyásolás* problematikájának[28] előtérbe kerülése, amennyiben az ily módon kivívott előny a harc sikeres megvívásának meghatározó elemei közé sorolható.[29] A kibertér kibontakozásával, majd dominánssá válásával párhuzamosan a lélektani műveletek ezen virtuális tartományban történő megjelenésével ez a jelentőség időközben csak még meghatározóbbá vált.[30]

A *befolyásolási műveletek* egyfajta kettős természetű jelenségként – a lélektani és az információs műveletekhez kapcsolódóan – értelmezhetők, amennyiben a lélektani műveletek egyrészt az emberek tudati viszonyai, véleménye, vélekedései és cselekvései terén fejtik ki hatásukat,[31] másrészt alapelemük a tudás és az ismeret, azaz az aktuális helyzetre vonatkozó információ. A lélektani műveletek valamilyen, a kezdeményező által kívánt végállapot, illetve vélekedés és cselekvés adott formájának elérésében érik el céljukat. Ez az adott célcsoport függvényében lehet pozitív vagy negatív, illetve

[28] Pix Gábor: *A lélektani műveletek jellemzőinek vizsgálata.* PhD-értekezés. Budapest, NKE, 2005. 13.
[29] Horváth Pál: *A katonai nemzetbiztonsági szolgálatok helye, szerepe, feladatai a válságkezelő műveletek során.* PhD-értekezés. Budapest, ZMNE HDI, 2007. 67.
[30] Deák Veronika: Social engineering alapú információszerzés a kibertérben megvalósuló lélektani műveletek során. *Hadtudományi Szemle,* 12. (2019), 3. 96–97.; Szternák György: Gondolatok a hatásalapú- és a hálózatközpontú katonai műveletekről. *Hadtudományi Szemle,* 1. (2008), 3. 4.
[31] Pix (2005): i. m. 10–11.

csoportviszonyok szempontjából egyesítő vagy megosztó.[32] Az információs műveletek hatásterületének három szintje különíthető el: 1. a *fizikai* dimenzióban az információs infrastruktúra támadása, illetve védelme merül fel elsődlegesen, 2. az *információs* terület az adatszerzés, illetve -feldolgozás elektronikus csatornáinak manipulálását tűzi ki célul, s végül 3. a *kognitív* terület testesíti meg a célcsoport gondolkodásának megváltoztatását.[33] Kutatások, szakirodalmi források kiemelik, hogy az új évezred sajátos hadviselési formáinak, mindenekelőtt a hibrid hadviselésnek,[34] de az aszimmetrikus konfliktusoknak ugyancsak,[35] illetve akár a kibertérben zajló műveleteknek[36] egyaránt meghatározó, sőt egyre inkább felértékelődő elemeiként találjuk meg a lélektani és információs műveleteket.

1.4. A hálózatok jelentősége, a szemléletmód relevanciája

A munkánkban alkalmazott megközelítésmód fő dimenzióját a hálózatok vizsgálatára vonatkozó értelmezések és megállapítások jelentik. Természetesen a hadtudomány előtt korántsem ismeretlenek a hálózati szerveződési mód előnyei, elegendő itt csak a hálózatközpontú hadviselés koncepciójára[37] gondolni vagy a hálózatokra mint az információ hasznosításához elengedhetetlen struktúrákra utalni.[38] A hálózatok mint komplex rendszerek az alábbi négy fő tulajdonsággal rendelkeznek: kisvilágság, skálafüggetlenség, egymásbaágyazottság, valamint gyengekapcsoltság.[39] Az aszimmetrikus kihívások vonatkozásában előbbiek közül akár mind a négy jellemző vizsgálatra érdemes lehet például a terrorista hálózatok tanulmányozásakor, de akár az egymásbaágyazottságra mint

[32] Pix (2005): i. m. 11.

[33] Haig Zsolt – Várhegyi István: A cybertér és a cyberhadviselés értelmezése. *Hadtudomány,* 18. (2008), 1–12.; Lőwi Ildikó: Információs hadviselés hatása az idegenellenességre. *Hadtudományi Szemle,* 9. (2016), 1. 251.

[34] Krajnc Zoltán – Csengeri János: A légierő képességei a hibrid fenyegetésekkel szemben. *Hadtudományi Szemle,* 10. (2017), 4. 114.

[35] Kassai Károly: *A Magyar Honvédség információvédelmének – mint a biztonság részének – feladatrendszere.* PhD-értekezés. Budapest, ZMNE, 2007.

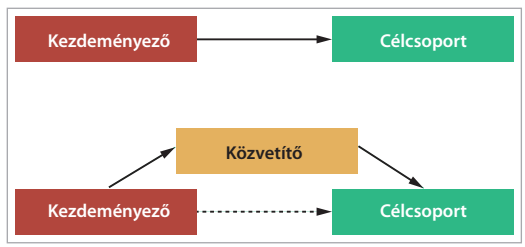
[36] Kovács László: *Biztonságpolitika: a kibertérben.* Budapest, NKE, 2019.

[37] Szternák (2008): i. m.

[38] Tóth András: *A hálózat nyújtotta képesség megvalósításának lehetőségei a Magyar Honvédség kommunikációs rendszerében.* PhD-értekezés. Budapest, NKE HDI, 2015. 21–25.

[39] 1. Kisvilágság *small-worldness:* a társadalmi életben előforduló valós hálózatok alkotóelemei közötti távolságok rövidek – „ha [a hálózat] átlagos úthossza a […] random gráfok meglehetősen kis átlagos úthosszához közel esik, de ugyanakkor a hálózat csoporterősségi együtthatójánál sokkal magasabb”; 2. skálafüggetlenség *(scale-freeness)*: a hálózatok alkotóelemei közül kiemelkedik néhány olyan szereplő, amelynek a többiekhez képest jóval magasabb a kapcsolódásai száma (fokszám), s ezáltal a kapcsolathálózat meghatározó szereplője ebben a tekintetben; 3. egymásbaágyazottság *(nestedness)*: a hálózatok alkotóelemei nem puszta pontként értelmezhetők, hanem azok is további hálózatokat foglalnak magukban; 4. gyengekapcsoltság *(weak-linkness)*: a gyenge kapcsolatok többségben vannak egy hálózaton belül (Csermely Péter: *A rejtett hálózatok ereje. Mi segíti a világ stabilitását?* Budapest, Vince Kiadó, 2005. 288.). Ezek „a gyenge kapcsolatok szükségesek a kisvilágság kialakulásában, a skálafüggetlenség egyik következményei és nagy szerepet játszanak az egymásbaágyazottság kialakulásában is. […] ők adják a hálózatokon belüli kapcsolatok döntő többségét”. Csermely (2005): i. m. 44.

szerveződési módra a hibrid fenyegetések feltárásakor is fókuszálhatnak az elemzések. Jelen munka keretében azonban ebben a tekintetben egy további, a hálózati szerveződési módban rejlő, egyedinek tekinthető aspektust is kiemelünk, nevezetesen a közvetett hatás kifejtésének, egyfajta indirekt érdekérvényesítésnek[40] a lehetőségét. A hálózati megközelítés ilyen szempontú alkalmazása elősegítheti például a befolyásolási műveletek hatásmechanizmusának megragadását, értelmezését: ennek keretében azt feltételezzük, hogy a kezdeményező fél a célcsoport felé kifejteni szándékozott hatását elsősorban nem közvetlen csatornán keresztül igyekszik realizálni, sokkal inkább közvetítő szereplő(k) beiktatásával (3. ábra) kísérli ezt meg, amiből a kezdeményezőnek számos előnye származhat.



3. ábra: A befolyásolási műveletek hálózati modellje
Forrás: a szerző szerkesztése

A tanulmány további részében – rövid módszertani ismertetést követően – empirikus kutatómunkánk eredményeiből válogatva olyan esettanulmányokat mutatunk be, amelyek illusztrálhatják az előbbiekben felvázolt koncepcionális keretek mentén kirajzolódó megközelítésmód gyakorlati alkalmazását.

2. Módszertani keretek

Kutatómunkánk keretében jellemzően kvantitatív szemléletmódban készített esettanulmányokat dolgoztunk ki. Olyan esettanulmányokat választottunk, amelyek lehetőség szerint négyes feltételrendszernek tesznek eleget:

1. kapcsolódnak az aszimmetrikus kihívások vagy a hibrid fenyegetések kérdésköréhez,
2. az új évezredben jelen levő, aktuális problémára reflektálnak,
3. a szakmai érdeklődés mellett esetlegesen gyakorlati relevanciájuk is van, továbbá
4. rendelkezésre állnak vagy összegyűjthetők olyan adatok, információk, amelyek lehetőséget biztosítanak a kvantitatív elemzőmunka alkalmazására.

Utóbbihoz kapcsolódóan a vizsgálatokhoz meglévő adatbázisok másodelemzését végeztük el, vagy online elérhető információforrásokból szerkesztettünk elemzésre alkalmas

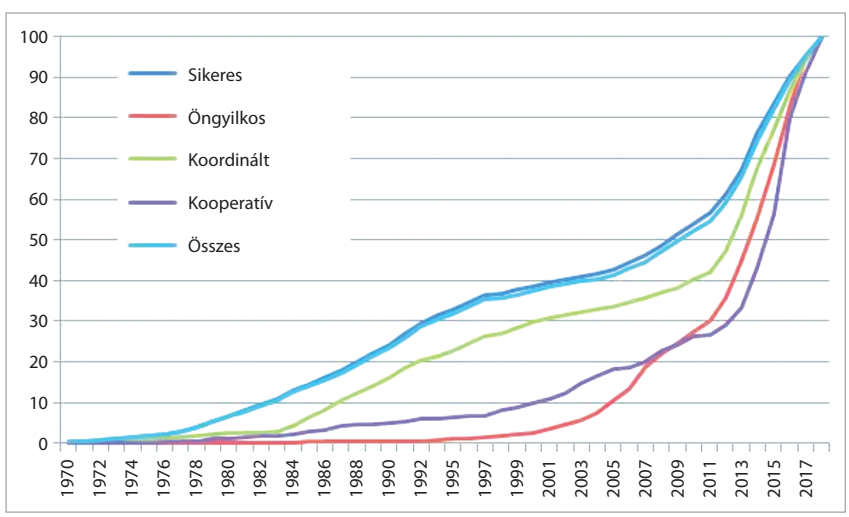
[40] Rózsa Tibor: A befolyásolás művészete. *Hadtudományi Szemle,* 7. (2014), 2. 46.

adatbázisokat. Bizonyos esetekben az adatbázisok összekapcsolására is sor került egyes információforrások összehasonlíthatósága érdekében. Az adatok elemzésekor egyszerű statisztikai módszereket és a hálózatelemzés némely eljárását hívtuk segítségül, az elemzések eredményeinek megjelenítéséhez grafikus elemeket (diagramok, hálózati gráfok) használtunk fel.

3. Esettanulmányok

3.1. I. A terrorizmus globális (hibrid) hálózata

Amennyiben a terrorizmust mint az aszimmetrikus kihívások egy jellemző formáját tekintjük, érdemes áttekinteni, hogy az miként alakult az új évezredben. A kutatásaink keretében készített kimutatások közül azokat választottuk ki illusztrációként, amelyek adekvátak és egyben szemléletesek az erőszak aszimmetrikus volta tekintetében. Mindenekelőtt idesoroltuk az *öngyilkos támadásokat* – amelyek esetében az aszimmetria a támadó saját életének tervezett, szándékos feláldozásában jelenik meg –, a koordinált akciókat – ahol az elkövetők egyszerre több, helyileg, illetve időben összehangolt támadást kísérelnek meg vagy hajtanak végre, ezzel is komplexebbé téve a támadás elleni védekezés lehetőségét –, valamint a kooperatív műveleteket. Utóbbiak olyan esetekre vonatkoznak, amikor több terrorszervezet egymással együttműködésben szervez meg egy támadást, összeadva erőforrásaikat, kompetenciáikat, információikat s növelve a sikeresség valószínűségét, illetve az ilyen sajátos kooperatív támadás pusztítási potenciálját.

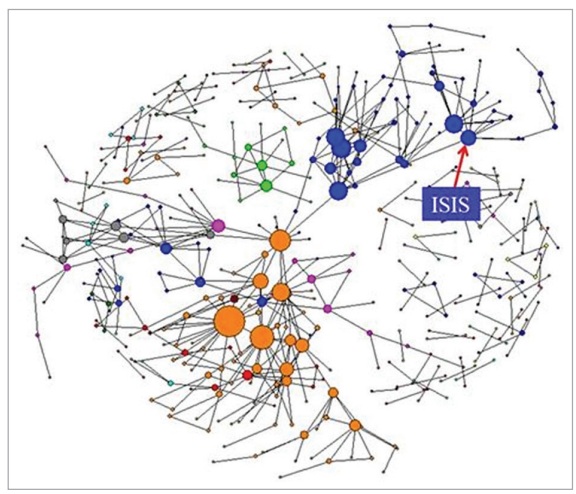


4. ábra: Az aszimmetrikus terroristaműveletek időbeli alakulása (%)

Forrás: a szerző számítása és szerkesztése a GTD (Global Terrorism Database, a terrorizmus globális adatbázisa) adatai alapján

Az adatok alapján megfogalmazható, hogy az aszimmetria illusztrálására jelen esettanulmány keretében kiválasztott terrorista támadási formák időbeli eloszlása hasonló mintázatot mutat (4. ábra): a 90-es évek közepe és az új évezred első évtizedének vége közötti időszakban alacsonyabb növekedési ütem figyelhető meg, amely a 2010-es évek elején intenzívebb növekedési ütemre váltott át. Az ebben az időszakban kezdődő arab tavasz eseményei valószínűsíthetően jelentős szerepet játszottak a trendváltásban, amely legszemléletesebben kétségkívül a több szervezet együttműködésében kivitelezett, kooperatív támadások esetében jelenik meg, indokolttá és érdekessé téve az ily módon kialakuló hálózat vizsgálatát.

A kooperációban végrehajtott terrorista akciók globális hálózati rendszere[41] korántsem egységes: mind a szereplők számában,[42] mind a résztvevők közötti kapcsolatok tekintetében jelentős különbségek rajzolódnak ki regionálisan is, illetve természetesen az egyes szervezetek pozíciója tekintetében is (1. gráf). A központi szereplők feltárása előtt azonban röviden megvizsgáljuk a globális kooperációs struktúra egészét.

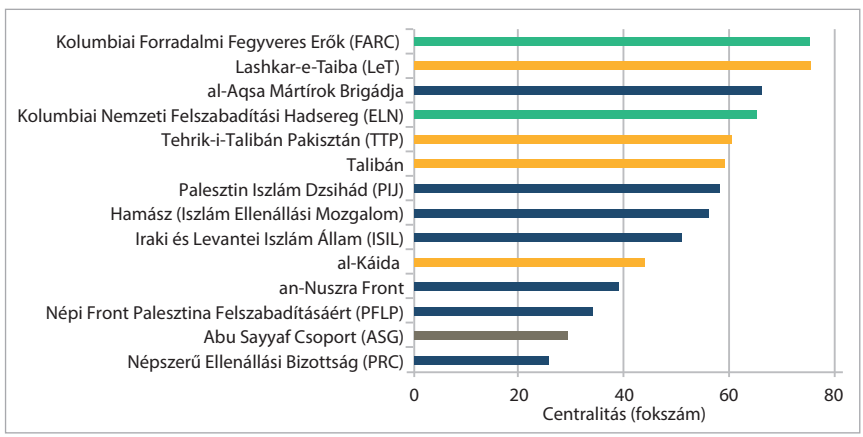


1. gráf: Az együttműködésben végrehajtott terrorista akciók globális hálózatának gráfja
Forrás: a szerző szerkesztése
Jelmagyarázat: az eltérő színek a regionális elhelyezkedésre utalnak.

A hálózat egymással kapcsolatban lévő szereplőiből létrejövő alrendszerben a geodézikus távolság 5,34 – ez alacsony szintű kompaktságot (0,040) és jelentős fragmentáltságot (0,96) eredményez. A hálózat központisága szintén alacsony (Freeman-féle fokszámközpontiság = 0,27%); a lehetséges kapcsolatoknak mindössze 0,27%-a létezik

[41] Jelen példában a terrorizmus operatív, akciók szintjén értelmezett formájával foglalkozunk, s nem fordítunk figyelmet a szervezetek közötti szövetségi rendszerekre. Utóbbi tágabb halmaz, és természetesen rendkívül érdekes szelete a globális terrorizmusnak, de célunk itt a konkrét, akciók szintjén megvalósuló együttműködések révén létrejövő, globálisan beágyazott terrorizmus hálózati rendszerének feltárása.
[42] Az elemzés tárgyát képező hálózat összesen 435 olyan szervezetet tartalmaz, amely az együttműködési struktúrában egyértelműen azonosítható, illetve megkülönböztethető, azaz ismert a szervezet neve.

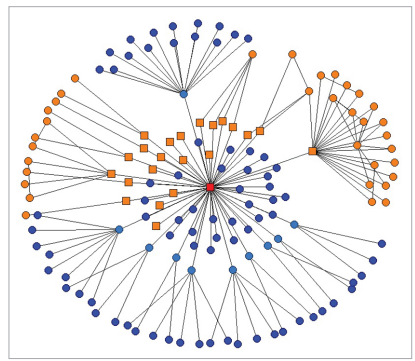
a hálózatban. A terrorszervezetek között jelentős eltérés van a kapcsolatok száma tekintetében: az átlagos fokszám 5,17 – vagyis átlagosan ennyi kötés jut egy szereplőre –, amelyhez magas szórás (10,16) társul. Az átlagos fokszám kétszórásnyival növelt értéke (25,49 kapcsolat) – azaz magasközpontiság – fölött *14 terrorszervezet* található (5. ábra), amelyek tehát a többi szervezethez képest *kiemelt súlyúak* a terroristák globális együttműködési hálózatában. Ezen szereplők a teljes hálózat kapcsolatainak egyharmadát (32,28%) fedik le, holott az összes szervezetnek csak töredékét (~3%) teszik ki. A terrorista csoportok ezen felső köre összetételét tekintve meglehetősen homogénnek bizonyul, amennyiben a hálózati elemek fele a közel-keleti és észak-afrikai régió terrorszervezetei közül való, további négy pedig a szintén kiterjedt dél-ázsiai térségben található. Az élmezőnyhöz tartozik még két dél-amerikai szervezet és egy délkelet-ázsiai szereplő.



5. ábra: Az együttműködési hálózat jelentősebb szervezetei és a regionális hovatartozás
Forrás: a szerző számítása és szerkesztése

Az együttműködésben megvalósított terrortámadások sajátos formájának tekinthető azon eljárásmód, amikor a felek közötti aszimmetria úgy jelenik meg, hogy az együttműködésben érintettek nem is feltétlenül szervezeti formában végzik tevékenységüket, mindössze közvetett – például érdekegyezésen, ideológiai kapcsolódáson vagy szimpátián alapuló – viszony áll fenn az akció elkövetésében részt vevő felek között. Jó példa lehet erre a globális terrorizmus fenti hálózatában is meghatározó pozíciót betöltő, a felső szegmensben megtalálható Iszlám Állam (ISIL), amely meglehetősen sajátos működési mód révén igencsak összetett kooperációs hálót tudhat magáénak. Amellett ugyanis, hogy több másik terrorista vagy felkelőszervezettel hajtott végre együttműködésben műveleteket, számos olyan eset is kapcsolódik hozzá, amikor a támadás kivitelezői olyan személyek voltak, akik közvetlenül nem álltak kapcsolatban az ISIL központi vagy fiókszervezetével, tevékenységükkel mégis a hírhedt szervezet tevékenységének erősítéséhez, kiterjesztéséhez járultak hozzá. Az Iszlám Állam összetettsége alapján *komplexnek,* míg az elkövetők, illetve a támadások jellemzői tekintetében *kevertnek, hibridnek* tekinthető kooperációs hálózati gráfjának (2. gráf) egyik szegmense tehát azon terrorista csoportok közötti kapcsolódásokból épül fel, amelyek az Iszlám Állammal – illetve annak valamely

alegységével, tartományával, fiókszervezetével – közösen jegyeznek terrorista akciót.[43] A gráf ezen alhálózatának struktúrája meglehetően összetettnek bizonyul, amennyiben a szervezetek közötti többszörös kapcsolódásokból olyan szűkebb, összetartozó csoportosulások, klaszterek is kialakulnak, amelyek tagjai között a hálózati sűrűség magasabb, illetve amelyekben bizonyos szervezetek mint központi elemek emelkednek ki.[44]



2. gráf: Az Iszlám Állam globális együttműködési hálózatának gráfja
Forrás: a szerző szerkesztése

A komplex hálózat másik szegmensét az együttműködés előbbi, hagyományosnak tekinthető formáját meghaladó akciók személyi elkövetői adják.[45] Ezen hálózati elemek[46] (összesen 77 fő) strukturális megkülönböztető jellemzője – ugyancsak az előbbi, szervezeti szintű együttműködés mintázatával ellentétben – szükségszerűen egyfajta *izoláltság:* egymással jellemzően nem állnak kapcsolatban,[47] kizárólag az Iszlám Állammal mint a támadás eszmei indítékának forrásával.

[43] A gráf ezen csúcsait egységesen narancssárga színnel jelöltük, továbbá ezeken belül az Iszlám Államhoz kötődő szervezeteket, csoportosulásokat (alegységek, provinciák, fiókszervezetek) négyzet alakú jelölővel különböztettük meg. A gráf piros színnel jelölt csúcsa maga az Iszlám Állam mint a hálózat eszmei középpontja.

[44] Az Iraki és Levantei Iszlám Állam (ISIL) és az azzal több esetben is kooperációban (is) tevékenykedő an-Nuszra Front kapcsolódása által képzett alhálózat például további nyolc olyan szervezetet jelöl ki a gráfban, amely az előbbiek közül legalább az egyikkel, illetve – az esetek többségében – mindkettővel rendelkezik közös éllel (lásd a 2. ábra jobb oldalán lévő, részben különálló alhálózat belső kapcsolatait).

[45] Az itt feltüntetett eseményekre vonatkozó adatokat (elkövetők száma, személye, továbbá a támadások helye, ideje, az akcióban meghalt, illetve megsérült áldozatok száma) nyíltan elérhető internetes források felhasználásával gyűjtöttük össze, majd az adatok tisztítását és egységesítését követően közös adatbázisba rendeztük. Az alapkritérium minden esetben az volt, hogy az Iszlám Állam – jellemzően utólag – vállalta a felelősséget a támadásért, illetve az elkövető személy(eke)t – akiknek több esetben a nevük is ismert – mint a szervezet harcosait azonosította, illetve tüntette föl. Az adatok a 2014 májusa és 2018 februárja közötti időszakot fedik le.

[46] A személyi elkövetőket jelző csúcsokat a gráfban kék színnel jelöltük, továbbá azon esetek megjelenítéséhez, amikor a támadást több személy hajtotta végre (vagy a nyomozati munka során több gyanúsított személy is felmerült) – a könnyebb áttekinthetőség érdekében –, közbülső csúcsot iktattunk be (világoskék színnel jelölve), amely magát (a több személy által elkövetett) akciót jelöli, s ezen elem mögé soroltuk be az egyes személyeket (jelző csúcsokat).

[47] A több elkövető részvételével történt akciók támadói természetesen egymással kapcsolatban álló személyeket jelentenek, ezek között azonban a gráfon – a könnyebb átláthatóság érdekében – nem ábrázoltunk éleket, hanem az eseményt jelző csúcshoz kapcsoltuk azokat.

Kettős strukturális jelleg rajzolódik ki tehát az Iszlám Állam hibrid kooperációs hálózatában: míg a *formális,* terrorszervezetek közötti együttműködésekből kialakuló alhálózatban bizonyos fokú egymásbaágyazottsággal, hídszerű beágyazottsággal[48] jellemezhető szerkezet alakul ki, addig az erőszakos akciókat az Iszlám Állam nevében elkövető személyek által megjelenített, egyfajta *informális* kooperáción alapuló alhálózat elemei jellemzően egyszeri kapcsolódások révén, a harmadlagos szerveződés mintázatával[49] kapnak helyet a gráfban. Mind a formális/szervezetek közötti, mind pedig az informális/harmadlagos szerveződésen alapuló együttműködések esetében felfedezhető azonban egy közös jellemző: a nem kooperatív támadásokhoz képest magasabb eredménymutatók.

3.2. II. Oroszország komplex érdekérvényesítési hálózata

Oroszország globális tekintetben meghatározó szereplőnek tekinthető,[50] bár gazdasági vagy éppen katonai tekintetben nem a legdominánsabb, talán éppen ezért jelenthet szemléletes példát arra, hogy esetében miként kerülhet előtérbe és válhat hatékonnyá a nemzetközi rendszerben történő érdekérvényesítés közvetett, áttételes formában, hálózati rendszerek kiépítésével, illetve működtetésével. Az alkalmazott eljárások ebben a tekintetben alapvetően azt teszik szükségessé, hogy az elérni szándékozott hatások minél inkább közvetett formában merüljenek fel. Érdekeinek érvényesítése érdekében Oroszország tehát *összetett,* a társadalmi élet *több szegmensét* is lefedő befolyásolási hálózatot tudhat magáénak (3. gráf).

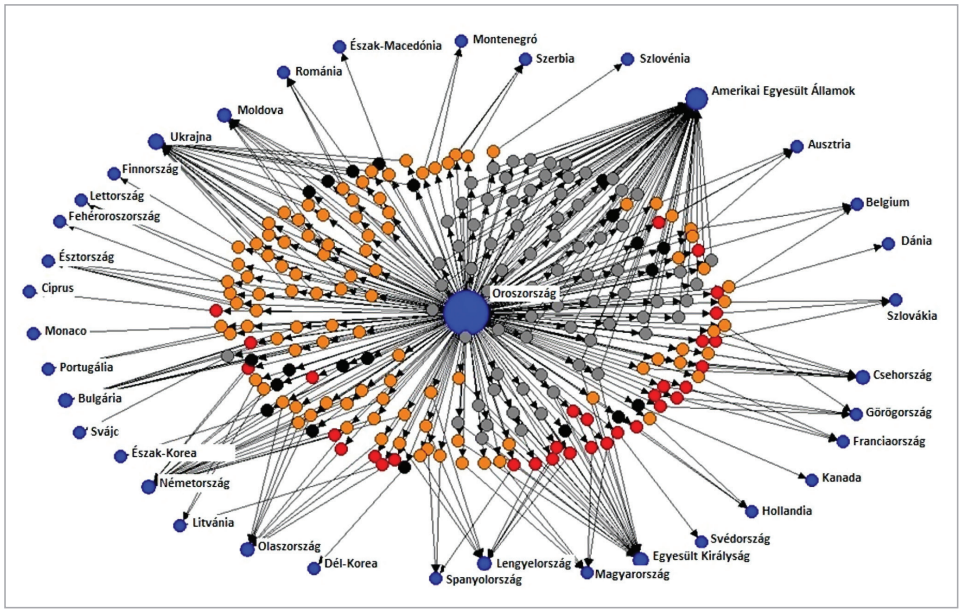
A kutatás jelenlegi készültségi fokán négy szegmensre tudunk adatok szintjén is reflektálni.[51] A *kulturális élet* – mint a *soft power,* kulturális diplomácia egyik eleme – tekintetében a kulturális intézmények, kulturális központok globális eloszlásának szerkezetét vettük figyelembe (4. gráf), amelyből kiderül, hogy Oroszország a kulturális diplomácia, illetve a *soft power* eme formája esetében – az élen található Kínához, Franciaországhoz és Egyesült Királysághoz képest „csak" – a középmezőnyben helyezkedik el a kulturális központok számát tekintve, ugyanakkor figyelemre méltó, hogy az ilyen jellegű orosz intézmények esetében jól kirajzolódik egy alapvetően eurázsiai dominancia a kulturális szervezetek elhelyezkedése s így az ország orientációja tekintetében.

[48] Mark Granovetter: A gyenge kötések ereje. A hálózatelmélet felülvizsgálata. In Angelusz Róbert – Tardos Róbert (szerk.): *Társadalmak rejtett hálózata.* Budapest, MKI, 1991.

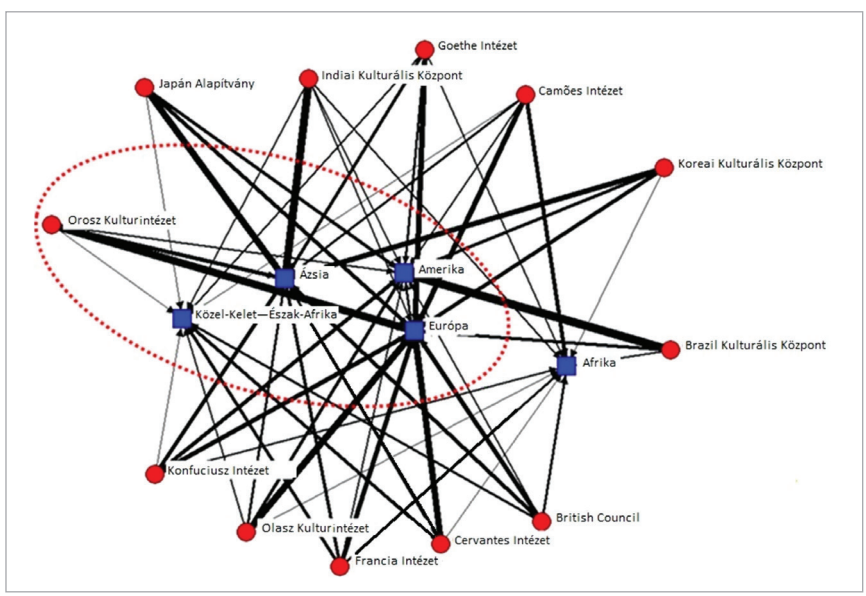
[49] Robert D. Putnam: *Bowling Alone. The Collapse and Revival of American Community.* New York, Simon and Schuster, 2000.

[50] Lásd ehhez például: Tömösváry Zsigmond: Oroszország mint globális szereplő? *Felderítő Szemle,* 17. (2018), 4. 57–70.; Steven A. Altman – Pankaj Ghemawat – Phillip Bastian: *DHL Global Connectedness Index 2018.* Bonn, Deutsche Post DHL, 2019.

[51] Nem maradhat szó nélkül, hogy ezen szegmensek között nem szerepel például a gazdasági szektor, amely a kutatás későbbi időszakában, az adatgyűjtés és -elemzés továbbfolytatásakor kiemelt pótolandó hiányosságként jut szerephez.

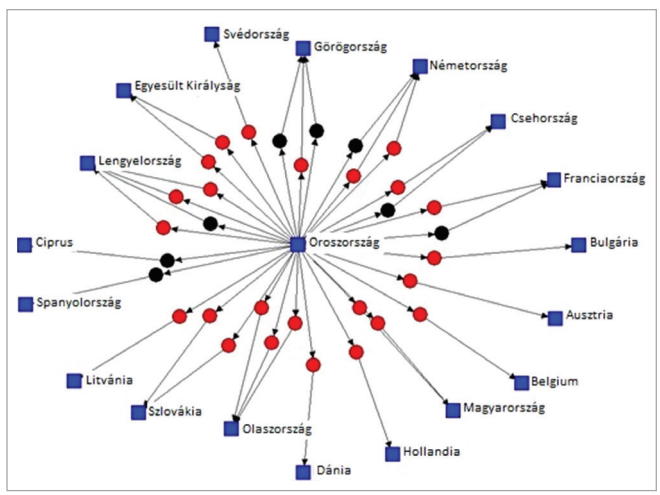


3. gráf: Oroszország komplex befolyásolási hálózatának áttekintő gráfja
Forrás: a szerző szerkesztése
Jelmagyarázat: kék kör: ország [középen: Oroszország]; narancssárga kör: kulturális központ; piros kör: politikai párt; szürke kör: internetes troll; fekete kör: APT



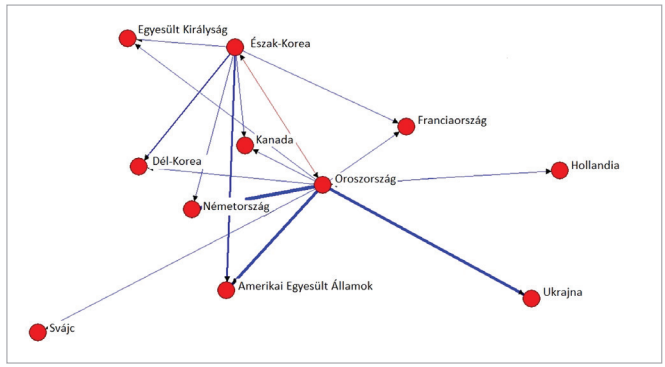
4. gráf: Az orosz kulturális diplomácia (soft power) globális orientációs hálózata
Forrás: a szerző szerkesztése
Jelmagyarázat: kék négyzet: régió; piros kör: kulturális intézet központja

Az érdekérvényesítés nyilvánvaló, központi jelentőségű területének tekinthető a *politikai döntéshozás* szférája (5. gráf), amelynek vonatkozásában már sajátos hálózati ismérv jelenik meg: egyes viszonyok multiplex jellege, amely jelen vizsgálat szempontjából abban ölt testet, hogy több olyan ország (például Görögország, Németország) is található a hálózatban, amelyet nemcsak egy, hanem több szélsőséges(nek tekintett) politikai szervezet köt össze Oroszországgal. Vagyis utóbbi adott ország vonatkozásában több olyan, a politikai szférában működő szervezetet is támogat, amelyen keresztül (feltételezhetőleg) saját érdekeinek érvényesítésére találhat módot. Érdemes továbbá kiemelni, hogy ezen többszörös kötésekkel rendelkező országpárok esetében nem egy esetben fedezhető fel egyfajta vegyes mintázat abban a tekintetben, hogy az orosz fél a politikai spektrum két ellentétes pólusához tartozó formációkat is támogat, amiből következő előnyként merülhet fel, hogy ezáltal is növelhető a befolyásolási műveletek által lefedhető társadalmi csoportok köre, a megszólítható közvélemény szélessége.



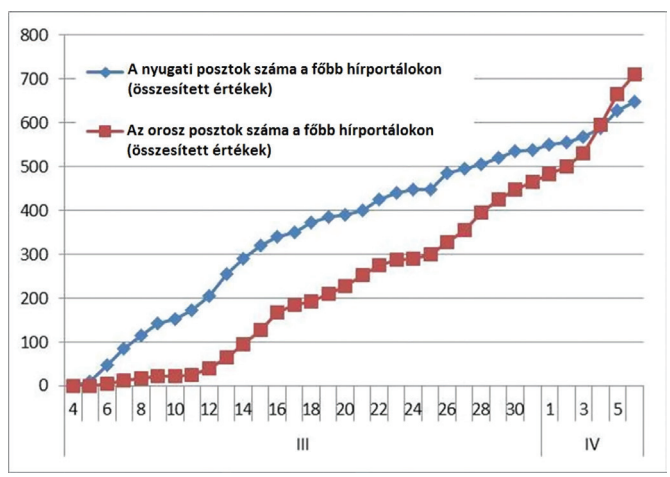
5. gráf: Oroszország által támogatott európai szélsőséges politikai formációk hálózata
Forrás: a szerző szerkesztése
Jelmagyarázat: kék négyzet: ország; piros/fekete kör: szélsőbal-/-jobboldali párt

A konfliktusok virtualizálódásának kétségtelenül egyik meghatározó eleme a *kibertér felértékelődése,* meghatározóvá válása. Ez a terület jelenti az itt vizsgált befolyásolási hálózat harmadik szegmensét: az Oroszország által a kibertérben végzett műveletek – amelyek sajátos közvetítőkön (APT-ken) keresztül valósultak meg – szerkezetére, összetételére (6. gráf) jellemző, hogy döntően az orosz kibertámadások németországi, ukrajnai és USA-beli célpontok ellen irányultak, de több további nyugat-európai ország esetében is megjelenik Oroszország ilyen jellegű tevékenysége, valamint egyes ázsiai országok is megtalálhatók az orosz kiberműveletek hálójában. Utóbbiak közül Dél-Korea esetében további érdekességként kiemelhető, hogy nem csupán orosz részről, hanem koreai részről is sor került kibertámadásra, így ezen államok viszonylatában kölcsönös kapcsolat jelenik meg a gráfban.



6. gráf: Oroszország pozíciója a kiberműveletek hálózatában
Forrás: a szerző szerkesztése
Jelmagyarázat: piros vonal: kölcsönös kapcsolat

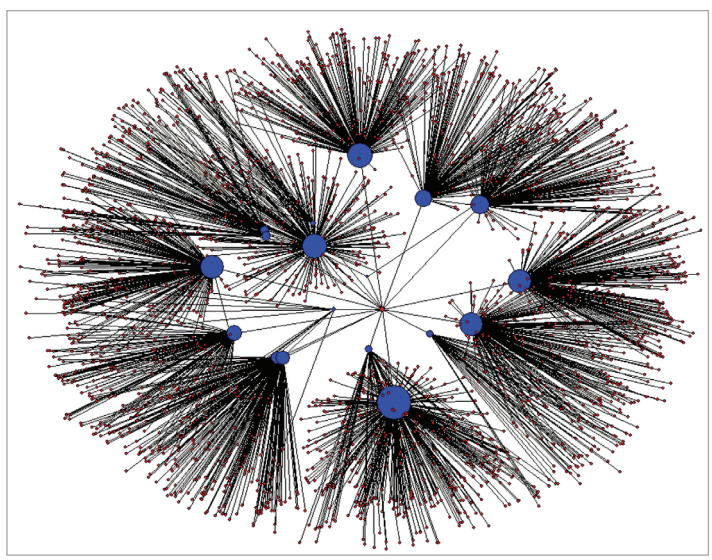
Részben a kibertérhez kapcsolódó, mégis érdemes elkülönülten is figyelembe venni egy negyedik szektort: a *közösségi média* területét, amelyből jelen munka keretében a (dez)információs szegmens emelhető ki. Ennek empirikus lehetőségéhez a 2018 márciusa elején Szergej Szkripal és lánya ellen elkövetett támadás biztosít kiinduló alapot, amennyiben a gyilkossági kísérlet rövid időn belül jelentős médiaversenyt indukált a virtuális térben. Az eseményt követő napon az arról beszámoló híradások keretében *(dez) információs versengés* indult meg, amelyet a nyugati források kezdeményezése és vezető szerepe jellemez. Az orosz sajtó több mint egy héten keresztül mindössze elenyésző mértékben tematizálta a problémát, és sokáig jelentős lemaradásban is volt – bár az orosz híradások időbeli eloszlásának trendvonala követi a másik oldal görbéjét (6. ábra).



6. ábra: A Szkripal-támadás kapcsán kibontakozó hírverseny
Forrás: a szerző számítása és szerkesztése
Megjegyzés: vízszintes tengely: a posztok időintervalluma (hónap, nap); függőleges tengely: posztok kumulatív száma

Hozzávetőlegesen három hét elteltével azonban az orosz kommunikáció mintha stratégiát váltott volna: markánsabb növekedés figyelhető meg, s az olló a két médiaforrás görbéje között záródni kezdett. Majd az orosz sajtó újabb trendváltással, a növekedési ütem még meredekebbé válásának köszönhetően, tulajdonképpen az esemény egy hónapos fordulójára a hírversenyben utolérte és meg is előzte a korábban domináns oldalt, ezzel a médiajelenlét ezen számszerűsíthető dimenziójában megnyerte a virtuális (dez)információs versenyfutást.

Valószínűsíthetően számos tényező együttes hatása állhat az online médiabeli hírverseny eredeti mintázatának sikeres megtörése, majd megfordítása mögött, amelyek között minden bizonnyal kiemelt jelentőségű a közösségi médiában működő – részben legalábbis – automatikus felhasználói felületek, trollok működése. Ezek a hírmegosztó felületek feltételezhetően rendkívül hatékonynak bizonyultak az Oroszország számára kedvező narratívák terjesztésében és hangsúlyozásában – különösen a számukat figyelembe véve. Egy vonatkozó tanulmány szerint[52] az előbb vizsgált esethez kapcsolódóan relatíve kevés (18 db) trollról van szó, amelyekről azonban elmondható egyrészt, hogy működésükre egyfajta *szórtság* jellemző, amennyiben nem kizárólag orosz területről működnek, hanem nyugat-európai országokbeli – jellemzően egyesült királyságbeli (4 db) – felhasználói felületek is megtalálhatók közöttük. A befolyásolási hálózat ezen online, közösségi médiához kötődő dimenziója (7. gráf) tehát – részben legalábbis – közvetlenül a célterület társadalmában működve fejti ki hatását.



7. gráf: Oroszországhoz köthető közösségi médiabeli trollok és követőik gráfja

Forrás: a szerző szerkesztése

Jelmagyarázat: kék kör: troll; piros kör: követő (középen Oroszország)

[52] Balogh Péter: Komplex befolyásolási hálózatok. Az érdekérvényesítés új évezredbeli formái Oroszország példáján keresztül. In Baráth Noémi Emőke – Mezei József (szerk.): *Rendészet–tudomány–aktualitások.* Budapest, DOSZ, 2020. 17.

A struktúra további jellemzője a *szegmentáltság,* illetve a lefedett közönség méretbeli eltérése, amely – egyebek mellett – a követők számának tükrében, az egyes trollok mögött található, eltérő nagyságú alhálózatokkal válik illusztrálhatóvá. E tekintetben tehát rendkívül lényeges különbség, *méretbeli hierarchia* rajzolódik ki az internetes felhasználói fiókok között. Az orosz befolyásolási műveletek ezen dimenziója az internetes hírportálok és az online közösségi média területén tehát arra enged következtetni, hogy a kívánatos tartalmak és célzott üzenetek továbbítására, illetve erősítésére meglehetősen hatékony struktúrát sikerült kialakítani, amely lehetővé tette rövid távon Oroszország számára, hogy felülkerekedjen. Mindezt jellemzően kevés közvetítő szereplőt magában foglaló, rugalmasan alakítható, az internetes lehetőségeket kihasználó, költséghatékony és adaptív struktúra kiépítésével.

Összegzés és kitekintés

A fentiekben kutatómunkánk keretében végzett vizsgálataink eredményeiből mutattunk be néhányat, amelyek az új évezred jellemző konfliktusformái, az aszimmetrikus kihívások és a hibrid hadviselés kérdésköréhez kapcsolódtak, hálózati megközelítésmód alkalmazásával. A koncepcionális keretek áttekintését követően két esettanulmányban összegeztük empirikus kutatásaink eredményeit. Az aszimmetrikus kihívások tekintetében a globális terrorizmus együttműködésben kivitelezett műveleteiből kialakuló hálózatát tártuk fel és jellemeztük, külön figyelmet fordítva az Iszlám Állam sajátos, hibrid kooperációs hálózatára. Az Oroszország példáját felhasználó esettanulmány a hibrid hadviselés vonatkozásában komplex, multiszektorális befolyásolási hálózat feltérképezését és elemzését eredményezte. Az esettanulmányok keretében törekedtünk arra, hogy a kijelölt kutatási problémák feldolgozása és elemzése során megfelelően illusztráljuk a hálózati szemléletmód alkalmazhatóságát.

Kutatómunkánk továbbfolytatásaként egyrészt a már meglévő kutatási eredmények kibővítésére és elmélyítésére – például a terrorista együttműködési hálózatok belső szerkezetének vizsgálatára vagy időbeli kiterjesztésére, illetve más országok hibrid hadviselési, befolyásolási hálózatainak feltérképezésére és összehasonlítására – teszünk kísérletet. Másrészt a megismert koncepcionális keretek fényében további tématerületeken – például kiberműveletek, szemantikai hálózatok és stratégiai kommunikáció – tervezünk empirikus kutatásokat.

Felhasznált irodalom

Altman, Steven A. – Pankaj Ghemawat – Phillip Bastian: *DHL Global Connectedness Index 2018.* Bonn, Deutsche Post DHL, 2019.

Balogh Péter: Komplex befolyásolási hálózatok. Az érdekérvényesítés új évezredbeli formái Oroszország példáján keresztül. In Baráth Noémi Emőke – Mezei József (szerk.):

Rendészet–tudomány–aktualitások. Budapest, DOSZ, 2020. 17. Online: https://dok.uni-nke.hu/document/dok-uni-nke-hu/Tanulma%CC%81nyko%CC%88tet.pdf

Beck, Ulrich: *Világkockázat-társadalom. Az elveszett biztonság nyomában.* Szeged, Belvedere Meridionale, 2008.

Brands, Hal: Paradoxes of the Gray Zone. *Fpri.org,* 2016. február 5.; Online: www.fpri.org/article/2016/02/paradoxes-gray-zone/

Buffaloe, David L.: Defining Asymmetric Warfare. *The Land Warfare Papers.* (2006), 58. Online: www.slideshare.net/alexpituba/defining-asymmetric-warfare

Castells, Manuel: *A hálózati társadalom kialakulása.* Budapest, Gondolat Kiadó – Infonia Kiadó, 2005.

Cohen, Raphael S. – Andrew Radin: *Russia's Hostile Measures in Europe. Understanding the Threat.* Santa Monica, RAND Corporation, 2019. Online: www.rand.org/pubs/research_reports/RR1793.html

Csermely Péter: *A rejtett hálózatok ereje. Mi segíti a világ stabilitását?* Budapest, Vince Kiadó, 2005.

Deák Veronika: Social engineering alapú információszerzés a kibertérben megvalósuló lélektani műveletek során. *Hadtudományi Szemle,* 12. (2019), 3. 95–111. Online: http://doi.org/10.32563/hsz.2019.3.6

Granovetter, Mark: A gyenge kötések ereje. A hálózatelmélet felülvizsgálata. In Angelusz Róbert – Tardos Róbert (szerk.): *Társadalmak rejtett hálózata.* Budapest, MKI, 1991.

Haig Zsolt – Várhegyi István: A cybertér és a cyberhadviselés értelmezése. *Hadtudomány,* 18. (2008), 1–12.

Horváth Pál: *A katonai nemzetbiztonsági szolgálatok helye, szerepe, feladatai a válságkezelő műveletek során.* PhD-értekezés. Budapest, ZMNE HDI, 2007.

International Security Advisory Board: Report on Gray Zone Conflict. *2009-2017.state.gov*, 2017. január 3. Online: https://2009-2017.state.gov/documents/organization/266849.pdf

Kassai Károly: *A Magyar Honvédség információvédelmének – mint a biztonság részének – feladatrendszere.* PhD-értekezés. Budapest, ZMNE, 2007.

Kiss Álmos Péter: Generációk a hadviselésben – a negyedik generáció. In Resperger István – Kiss Álmos Péter – Somkuti Bálint (szerk.): *Aszimmetrikus hadviselés a modern korban. Kis háborúk nagy hatással.* Budapest, Zrínyi Kiadó, 2015. 66–80.

Kiss Álmos Péter: A hibrid hadviselés természetrajza. *Honvédségi Szemle,* 147. (2019), 4. 17–37.

Kovács László: *Biztonságpolitika: a kibertérben.* Budapest, NKE, 2019.

Krajnc Zoltán – Csengeri János: A légierő képességei a hibrid fenyegetésekkel szemben. *Hadtudományi Szemle,* 10. (2017), 4. 112–125.

Liang, Qiao – Wang Xiangsui: *Unrestricted Warfare.* Beijing, PLA Literature and Arts Publishing House, 1999.

Lind, William S.: Understanding Fourth Generation War. *Antiwar.com,* 2004. január 15. Online: www.antiwar.com/lind/?articleid=1702

Lőwi Ildikó: Információs hadviselés hatása az idegenellenességre. *Hadtudományi Szemle,* 9. (2016), 1. 249–259.

Nagy Bianka: Az orosz nem lineáris hadviselés és az ellene irányuló önvédelem lehetőségei. *Felderítő Szemle,* 17. (2018), 1. 143–150.

Neumann, Peter R.: Old and New Terrorism. *Socialeurope.eu,* 2009. Online: www.socialeurope.eu/2009/08/old-and-new-terrorism/#

Perl, Raphael F.: Asymmetric Warfare: A Doctrine to Fit the Times. In Álmos Péter Kiss (szerk.): *Asymmetric Warfare. Conflict of the Past, the Present and the Future. Proceedings of the*

Conference in Budapest, Hungary, 9–10 November 2016. Budapest, Dialóg Campus Kiadó, 2017. 43–47.
Pix Gábor: *A lélektani műveletek jellemzőinek vizsgálata.* PhD-értekezés. Budapest, NKE, 2005.
Putnam, Robert D.: *Bowling Alone. The Collapse and Revival of American Community.* New York, Simon and Schuster, 2000.
Resperger István: A XXI. század fegyveres konfliktusainak hatása a hadtudományra. In Resperger István – Kiss Álmos Péter – Somkuti Bálint (szerk.): *Aszimmetrikus hadviselés a modern korban. Kis háborúk nagy hatással.* Budapest, Zrínyi Kiadó, 2015. 13–47.
Resperger István: A nemzetbiztonsági szolgálatok tevékenysége – biztonsági kihívások, kockázatok és fenyegetések. In Resperger István (szerk.): *Nemzetbiztonsági alapismeretek.* Budapest, Dialóg Campus Kiadó, 2018. 29–93.
Resperger István – Somkuti Bálint: Hybrid Warfare or the Ever Changing Face of War. *Defence Review,* 144. (2016), 1. 73–79.
Rózsa Tibor: A befolyásolás művészete. *Hadtudományi Szemle,* 7. (2014), 2. 44–53.
Somkuti Bálint: A negyedik generációs hadviselés. In Resperger István – Kiss Álmos Péter – Somkuti Bálint (szerk.): *Aszimmetrikus hadviselés a modern korban. Kis háborúk nagy hatással.* Budapest, Zrínyi Kiadó, 2015. 48–65.
Szternák György: Gondolatok a hatásalapú- és a hálózatközpontú katonai műveletekről. *Hadtudományi Szemle,* 1. (2008), 3. 1–7.
Tóth András: *A hálózat nyújtotta képesség megvalósításának lehetőségei a Magyar Honvédség kommunikációs rendszerében.* PhD-értekezés. Budapest, NKE HDI, 2015.
Tömösváry Zsigmond: Oroszország mint globális szereplő? *Felderítő Szemle.* 17. (2018), 4. 57–70.
Tucker, David: Terrorism, Networks, and Strategy. Why the Conventional Wisdom is Wrong. *Homeland Security Affairs.* 4. (2008), 42. Online: www.hsaj.org/articles/122
United States Special Operations Command White Paper: The Gray Zone. *Publicintelligence.net,* 2015. szeptember 9. Online: https://publicintelligence.net/ussocom-gray-zones/