Balogh Péter[♦]

Kibertérbeli műveletek 2016-ot követően – A kiberhadviselés mintázatai, trendjei, szereplői és kapcsolódásaik[*]

DOI 10.17047/Hadtud.2025.35.E.1

A kibertérbeli műveletek egyre meghatározóbb elemeivé válnak az új évezred különféle konfliktusainak, egyben sokrétűbbé, komplexebbé téve azokat. A tanulmányban arra vállalkozunk. hogy releváns koncepcionális értelmezési keretek segítségével áttekintsük a kibertérbeli műveletek és a biztonsági szektorok kölcsönkapcsolatát, s esettanulmányok alapján feltárjuk és illusztráljuk a kibertérbeli műveletek jellemzőit. Utóbbiakhoz lényeges vonatkoztatási pontot szolgáltat a NATO 2016. évi, Varsóban tartott csúcstalálkozója, amelyet követően a kibertér bekerül a műveleti területek közé, valamint a 2022 februárjában eszkalálódó orosz–ukrán konfliktus.
KULCSSZAVAK: kibertérbeli műveletek, biztonsági szektorok, esettanulmány, adatelemzés

Cyberspace Operations after 2016 – Some Patterns, Trends, Actors and Connections in Cyber Warfare

Cyberspace operations are becoming increasingly important elements of various conflicts of the new millennium, making them more diverse and complex. In this paper the interrelatedness between cyberspace operations and security sectors referring to relevant conceptual frameworks are reviewed, and the characteristics of cyberspace operations are explored and illustrated on the basis of case studies. An important reference point for the latter is the NATO summit held in Warsaw in 2016, after which cyberspace was recognized as one of the domains of operations, as well as the Russian-Ukrainian conflict having escalated in February 2022.
KEYWORDS: cyberspace operations, security sectors, case study, data analysis

Bevezetés és problémafelvetés

A kiberteret, mint a konfliktusok, biztonsági jellegű kihívások, kockázatok, fenyegetések[1] sajátos színterét több szempontból is kiemelt szakmai figyelem övezi. Egyrészt a biztonsági tanulmányokban az ún. koppenhágai iskola kutatói által kidolgozott, majd széles körben alkalmazott, a biztonság különféle aspektusainak elkülönítésére és elemzésére kidolgozott, szektorokra épülő megközelítésmód[2] továbbfejlesztett, az időközben változó biztonsági környezetre reflektáló, s ennek megfelelően kiegészített modelljében[3] külön területként

♦ Szegedi Tudományegyetem Bölcsészet- és Társadalomtudományi Kar, Szociológia Tanszék – *University of Szeged, Faculty of Humanities and Social Sciences, Department of Sociology;* e-mail: baloghp@socio.u-szeged.hu; https://orcid.org/0000-0001-8586-8308
[*] A tanulmány az MHTT 2023. évi cikkpályázatán harmadik helyezést ért el.
[1] Lásd ehhez pl. Resperger 2018; Farkas, Kelemen 2023.
[2] Buzan, Wæver, de Wilde 1998.
[3] Gazdag, Remek 2018, 24.

jelenik meg a – katonai, a politikai, a gazdasági, a társadalmi és a környezeti mellett – a biztonság *informatikai* dimenziója. Ezen aspektus a biztonság vizsgálatának, elemzésének során egy sokrétű, összetett és lényegében folyamatosan változásban lévő területet igyekszik megfoghatóvá tenni, ami önmagában is fontosnak tekinthető. Meglátásunk szerint azonban a biztonság informatikai – vagy ahogyan arra a szerzők szintén hivatkoznak, a kiberbiztonság[4] – szektora jelentősége mindenek előtt abban érhető tetten, hogy folyamatos fejlődésével és egyre szélesebb körű elterjedésével, alkalmazásával már nem csupán egy különálló szektoraként értelmezhető a biztonsági architektúráknak, hanem meglátásunk szerint úgy kell gondolnunk rá, mint olyan mezőre, mely egyre inkább áthatja a biztonság egyéb szektorait is. Ezáltal az informatikai vagy kibertérbeli biztonság nem egy, a többi szektor mellett azonosítható terület, hanem bizonyos tekintetben azok fölé lépve – vagy éppenséggel azokat mélységeiben átitatva – keresztbemetszi a többi biztonsági szektort, s ezáltal jelentős hatást gyakorol az abban zajló folyamatokra. Gondolhatunk itt például a biztonság politikai szektora tekintetében a választások tisztaságát megkérdőjelező, illetve a lakossági preferenciák módosításának, befolyásolásának szándékával zajló műveletekre[5] – utóbbi tekintetben a biztonság társadalmi aspektusa is relevánsnak tekinthető –, vagy éppen a gazdasági szektor vonatkozásában a tágabb működési feltételek[6] vagy a pénzügyi szektor online térből induló kihívásaira[7] is.

A *biztonság katonai dimenziója* – s hadtudományi szempontból ez tekinthető kiemelt jelentőségűnek – nyilvánvalóan ugyancsak jelentős mértékben összekapcsolódik az informatikai fejlődéssel, az információs társadalom kialakulásával,[8] s a kibertér egyre jelentősebb szerepével.[9] Ezek a változások egyaránt érintik az olyan, rendre előtérbe kerülő kérdéseket, mint például hogy az új info-kommunikációs körülmények között miként léphetnek fel a kihívásoknak és fenyegetéseknek újabb formái,[10] a korábban más technikai megoldásokkal kivitelezett műveletek hogyan bővülhetnek ki az újonnan megjelenő technológiai – online – bázison,[11] vagy éppen bizonyos régóta ismert fenyegetéseknek az új megjelenési formái.[12] A téma – s jelen tanulmány – szempontjából kiemelten fontos továbbá, hogy ezen folyamatok eredményeképpen – azok egyfajta betetőződéseként – a hadtudományi gondolkodásban kikristályosodott a kiberhadviselés koncepciója.[13] Ebben a tekintetben a fegyveres harc megvívásának ezen új formája, módja és eljárásai kettős szempont alapján is kiemelt szakmai, kutatási – és természetesen gyakorlati – problémává léptek elő.[14] Egyrészt az újabb és újabb informatikai megoldások és információs eljárások mind teljesebb

[4] Gazdag, Remek, 2018, 24. (lj. 3.)
[5] Lásd pl. Bányász 2019; Kovács, Krasznay 2017; NIC 2017.
[6] Lásd pl. Horváth 2013; Horváth, Erdősi, Kiss 2016.
[7] Lásd pl. MNB 2022; Terták, Kovács 2023.
[8] Lásd pl. Haig, Várhegyi 2005; Haig 2018 (különösen 54–76 és 84–88.)
[9] Lásd pl. Haig, Kovács 2008; Chwe 2016; Krasznay 2022.
[10] A közösségi média esetéhez lásd pl. Bányász 2012.
[11] Előbbihez kapcsolódóan említhető itt az információs műveletek kibertérben való megjelenése, ill. oda történő részleges áttelepülése, lásd pl. Haig 2021; Haig 2022.
[12] Amint az történt például a terrorizmus „ősi mestersége” esetében az új évezred viszonyai között, lásd ehhez Kovács 2013.
[13] Lásd pl. Joubert 2010; Robinson, Jones, Janicke 2015; Kovács 2018a; Kovács 2023.
[14] Lásd pl. Krasznay 2023.

megjelenése a védelmi erők működésében, a kiberképességek rendszerszintű beépülése új sebezhetőségekhez vezetett,[15] melyekkel szemben megfelelő védelmi ill. megelőző képességek kialakítása vált szükségessé.[16] Másrészt pedig felvetődött, illetve megindult a kiberképességek támadó céllal történő alkalmazásának fejlesztése, ami – a fegyverkezési verseny analógiájára – az elrettentés lehetőségét is felveti[17] – feltéve, hogy a szóban forgó képességek gyakorlati alkalmazásának esélye hitelesnek tekinthető.[18] A kiberhadviselés mint koncepció[19] és mint valós körülmények között zajló gyakorlat pályaívének kiteljesedése talán egyik mérföldkövének tekinthető a 2008-as esztendő a NATO Kooperatív Kibervédelmi Kiválósági Központ létrejötte okán,[20] de még inkább a 2016-os év, hiszen a NATO Varsóban tartott csúcstalálkozóján ekkor jelölik meg a kiberteret mint a hadviselés egy sajátos, elkülönülő területét.[21] Ily módon a fegyveres harc megvívásának mostanra öt területe különíthető el, előtérbe állítva az egyes dimenziókban párhuzamosan, koordináltan végrehajtott multi-domain műveletek szerepét.[22]

Kutatómunkánk jelen tanulmány keretei között bemutatott eredményei szempontjából az előbbi esemény tekinthető meghatározónak, amennyiben írásunkban arra vállalkozunk, hogy a 2016-ot követő időszak vonatkozásában feltárjuk és bemutassuk a kiberműveletek elemzésén keresztül a kiberhadviselés főbb mintázatait, tendenciáit, szereplőit és azok viselkedését. A vizsgált kutatási probléma kapcsán kérdésfelvetésünk arra irányul tehát, hogy miként lehet meghatározni a kibertérbeli műveletek összetételének, jellegzetességeinek mintázatait, illetve változását – különös tekintettel a szereplők közötti viszonyokra. Előzetes várakozásaink alapján a kiberhadviselés globális rendszere egyre strukturáltabb, kiforrottabb mintázattal jellemezhető, melyben a szereplők sajátos típusai és – egyre inkább interakciós jellegű, kölcsönösségre épülő – viselkedési formái mutathatók ki.

Módszertani háttér

A kutatási probléma gyakorlati keretek között történő vizsgálatához a kvantitatív esettanulmányok módszerét alkalmaztuk. Ennek megfelelően a kiberműveletek révén kialakuló struktúra feltárásának és jellemzésének empirikus hátterét két, eltérő jelleggel összeállított esettanulmányban vázoljuk fel a tanulmány elemző részeiben.

Az első esettanulmány keretében a kérdésfelvetés során megjelölt 2016-os esztendőtől indítva egy több éves időszakban vizsgáljuk meg az államok által támogatott kibertámadások jellemzőit, kiemelt hangsúlyt fektetve az időbeli változásra, trendek és tendenciák megjelenésére.[23] Ezen esettanulmány tehát az államok között a kiberműveletek révén kiépülő

[15] Bányi 2018.
[16] Lásd ehhez Kovács 2018a; Fekete, Karydis, Lázár 2020.
[17] Lásd ehhez pl. Lupovici 2011.
[18] Kovács 2021a; Kovács 2021b.
[19] Lásd ehhez pl. Liles 2010.
[20] Tóth 2018.
[21] Lásd pl. Wiedemar 2023, 2.
[22] Lásd ehhez pl. Mező 2021; Fazekas 2022.
[23] A korábbiak fényében az első esettanulmány keretében végzett kutatómunka által lefedett periódus kezdetének eszmei időpontja tehát a kibertérnek a NATO-ban történt hivatalos domain-né való előlépése alapján állt elő, az elemzett adatok időkeretének bezárása pedig a 2020-as évre esett, aminek alapvetően tartalmi-módszertani okai

szerkezet jellemzésén túl az abban megfigyelhető dinamikát is megfoghatóvá teheti. A második esettanulmány az előbbihez képest – szándékoltan – egy statikus, keresztmetszeti, rövid időszakra vonatkozó áttekintést – egyfajta pillanatképet – vázol fel a vizsgált témáról, azonban jóval tartalomgazdagabb formában foglalkozik a kiberhadviselés gyakorlati megnyilvánulásával, amennyiben új nézőponttal és részletesebb információs háttérrel kiegészülve készítettük el. A második kvantitatív esettanulmányban ugyanis az orosz–ukrán konfliktus 2022. február végén eszkalálódó fegyveres szakaszának első félévében zajló kiberműveleteket vizsgáljuk meg, egyaránt ismertetve az államilag támogatott, valamint az államokhoz közvetlenül nem kötődő szereplők, proxy csoportok[24] akcióit is.

Az esettanulmányok kidolgozásához a témával foglalkozó, a világhálón keresztül nyíltan elérhető weboldalakon megjelenítet információkat használtuk fel,[25] melyekből komplex adatbázisokat alakítottunk ki, mivel az adatelemzések során alapvető statisztikai eljárásokat, összevetéseket, valamint a hálózatelemzés néhány eljárását és grafikus megjelenítési módszereket alkalmaztunk.

Esettanulmány I. Kiberhadviselés 2016–2020

A kiberműveletek hálózata

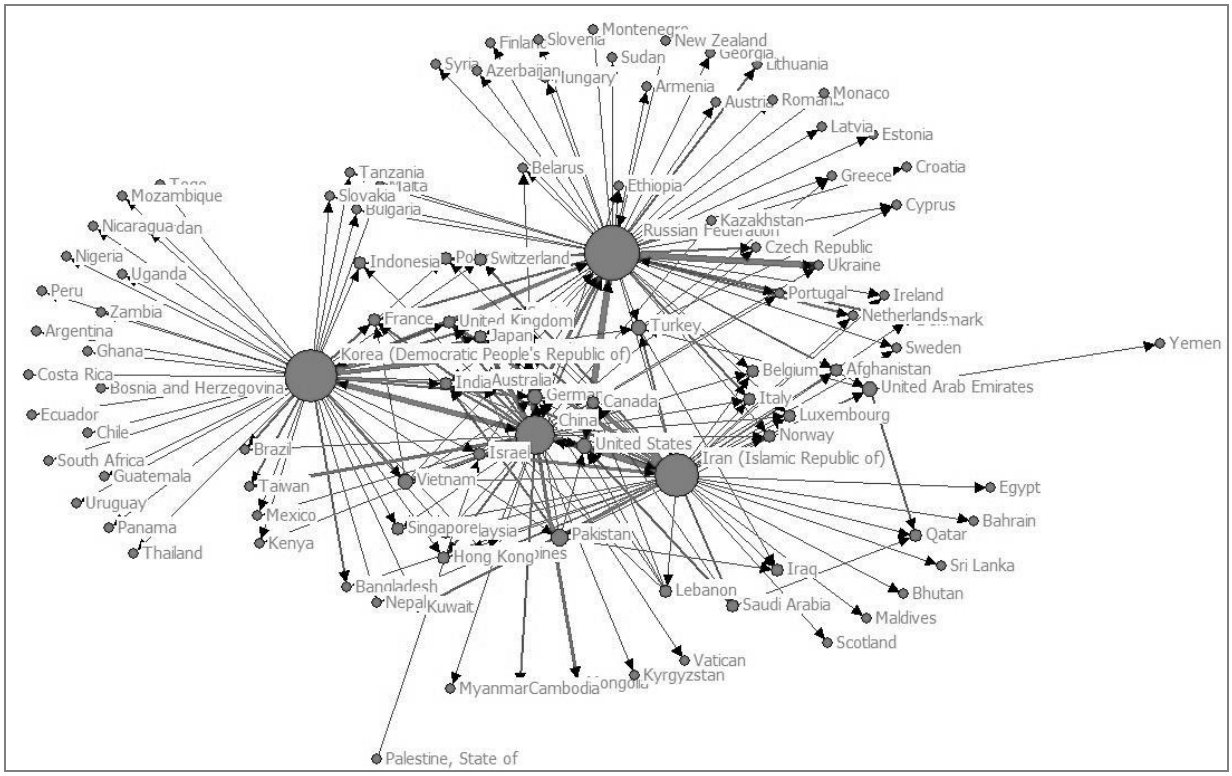
A 2016–2020. közötti időszak államokhoz köthető kiberműveleteinek hálózatában összesen 107 ország található, melyek között mindösszesen 534 kötés alakítja ki a hálózati struktúrát (*1. gráf*). A hálózatban jól kirajzolódnak a kibertámadások meghatározó szereplői – mindenek előtt ezek között találjuk Oroszországot, Észak-Koreát, valamint Iránt és Kínát is. Az előbbi két ország markánsan elkülönülő alhálózatot látszik kialakítani maga körül, melynek Oroszország és Észak-Korea központi, gravitációs pontjait képezik, körülöttük pedig számos olyan ország rendeződik el, amelyek az egyes államok kiberműveleteinek célpontjai. Vannak természetesen olyan országok is, melyek mindkét állam kibertámadásai által érintettek – például Szlovákia vagy Tanzánia –, ily módon egyfajta közös metszetet képeznek az orosz és észak-koreai kibertérbeli akciók kereszttüzében. Irán esetében részben hasonló, bár kisebb, kevésbé elkülönülő kibertérbeli csoportosulás tárható fel, s Irán jóval erőteljesebben be van ágyazódva a hálózat további jelentős országainak körében megjelenő, strukturálisan a hálózat középpontját alapvetően uraló csoportba. A hálózat ezen szegmensében találjuk mindenek előtt Kínát, mely amellett, hogy önmaga is a legmeghatározóbb szereplők között tűnik fel a vizsgált időszak kiberműveleti hálózatában, megannyi egyéb – nemzetközi, illetve európai

voltak: a 2020-ban globálisan meghatározóvá váló koronavírus-járvány alapvetően változtatta meg a kibertér állami és egyéb szereplőinek viselkedését, ezzel egyfajta új periódust képezve a kiberműveletek dinamikájában. Ezen időszak mintázatainak elemzése egy másik tanulmány tárgya lehet, jelen munka keretében azonban a kérdésfelvetés jellegéből fakadóan ettől eltekintünk.

[24] Lásd ehhez pl. Krasznay 2022, 57–71.

[25] Az adatbázisok kialakításához a Council for Foreign Relations. ill. a CyberPeace Institute tematikus oldalait használtuk fel. Fontos megjegyezni, hogy a kibertámadásokról nyilvánvalóan csak bizonyos mértékű – különösen attribúciós jellegű – bizonytalanság mellett lehet adatokat gyűjteni, hiszen a különféle szereplők – különösen az államok – ilyen jellegű tevékenységüket rejteni, fedni törekszenek, így az akciók látenciája feltételezhetően magas, adathiányok előfordulhatnak. Az adatgyűjtéshez használt források ezt a problémát oly módon igyekeznek kiküszöbölni, hogy több – alapvetően szakmai – forrás által megerősített műveletek esetében közölnek rekordokat, melyek révén a forrásadatok is transzparensek, visszakereshetők.

szinten kiemelt – országgal is összekapcsolódik. Mindenekelőtt utóbbiak között kell felismernünk Németországot, Kanadát, Ausztráliát és Indiát, de legfőképpen az Amerikai Egyesült Államokat. Ezen országok hálózati-strukturális fontosságát nem az esetükben mérhető kapcsolatszám kimagasló mértéke adja – mint az előzőekben bemutatott államoknál –, jelentőségük sokkal inkább pozicionális jellemzőjükből eredeztethető. Kanadát például a legaktívabb szereplők közül Oroszország, Észak-Korea és Irán kiberműveletei egyaránt érintik, ily módon az amerikai kontinens legészakibb állama ezen három támadó által kifeszített térben a hálózat centrális pozíciójába kerül. Ausztrália, Németország és az USA azonban mind a négy magas fokszámú ország kibertámadásainak célterületét jelentik, amennyiben az előzőek mellett jelentős mértékű kínai kibertevékenység is megjelenik esetükben, melynek következtében a hálózat meghatározó szereplőinek erőterében központi pozíciót foglalnak el.



1. gráf

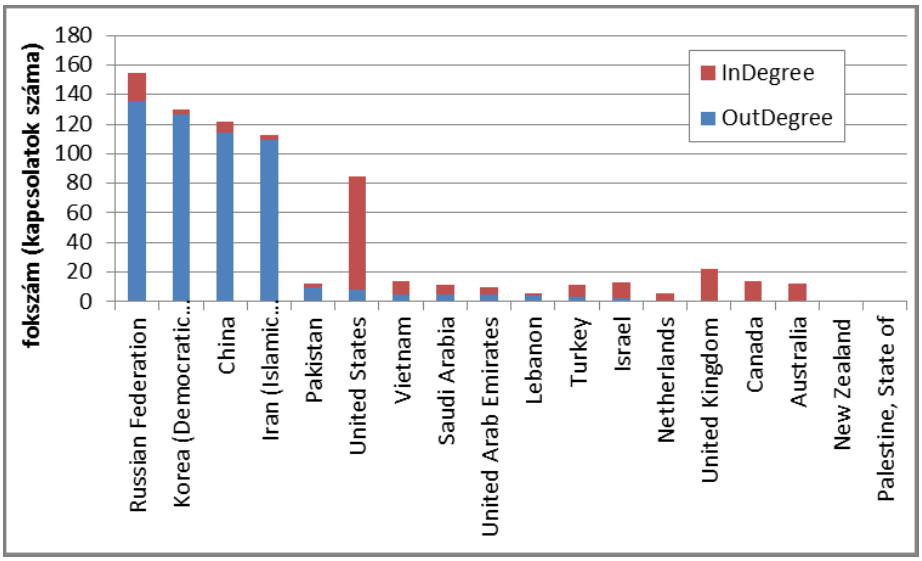
Az államok közötti kiberműveletek hálózata (2016–2020)

[Forrás: saját szerkesztés komplex adatbázis alapján. Megjegyzés*:* Az elemek mérete a fokszámot tükrözi.]

A hálózat további strukturális jellemzőjeként kiemelhető az egyes országok közötti kötések eloszlásának különbségei. A legmagasabb kifokszámmal – kifelé irányuló kötéssel, azaz ebben a tekintetben támadási relációval – bíró Oroszország és Ukrajna esetében például jelentősen magasabb kapcsolat mérhető, de hasonlóképpen jelentősebb az Észak-Korea által Dél-Korea ellen végrehajtott műveletek száma. A hálózatban szereplő országok közötti élek relatív jelentőségében, súlyaiban megmutatkozó különbségek egy bizonyos tekintetben sajátos kapcsolatforma, a kölcsönös kötések esetében szintén nagyon jól láthatók. Az Amerikai

Egyesült Államok Oroszországgal vagy Iránnal például kölcsönös viszonyban van, azaz mindkét ország hajtott végre a másik ellen – jóllehet eltérő mértékben – kibertámadásokat, de utóbbi ország ugyancsak ilyen kölcsönös kötéssel kapcsolódik Izraelhez, akárcsak Kína Vietnámhoz, de kiemelhető az is, hogy Észak-Korea és Oroszország viszonylatában is ilyen oda-vissza jellegű kapcsolat mutatható ki.

Összességében tehát megfogalmazható, hogy a kiberműveletek hálózatában egyrészt kiemelkednek azok az országok, melyek jelentős aktivitásukkal, magas támadási értékeikkel lényegében dominálják a hálózatot, illetve annak bizonyos szegmenseinek meghatározó szereplőiként azonosíthatók, másrészt pedig strukturálisan lényegesnek bizonyulnak azon országok, melyek annak köszönhetően foglalnak el központi pozíciót a hálózatban, hogy az előbbi domináns államok közül többen is célpontjukként tekintenek rájuk. A hálózat szereplőinek fokszám eloszlása (*1. ábra*) az előbbieket tükrözi vissza: az összes ország közül mindössze néhány olyan van, melynek magas a kifok értéke – összesen 18 állam rendelkezik kifelé mutató, azaz támadó kiberművelettel –, s jóval nagyobb azon országok száma, melyek mindössze elszenvedői a kibertérbeli akcióknak. Vagyis a kibertámadások csak az érintett országok egy szűkebb körét – kevesebb, mint egy ötödét (16,8%) érintik, a nagy többség mindössze elszenvedője a műveleteknek.



1. ábra

A kapcsolatok száma a támadó kötésekkel bíró hálózati szereplőkre szűkítve

[Forrás: saját számítás és szerkesztés]

A már korábban is látott négy állam mindegyike legalább száz támadó kapcsolattal rendelkezik, s közülük Oroszország esetében mérhető a legmagasabb érték a befelé mutató kötések tekintetében, de utóbbi kapcsolat forma szempontjából az Amerikai Egyesült Államok emelkedik ki messze a többi ország közül, illetve az Egyesült Királyság, Kanada és Ausztrália esetében mérhető még relatíve magasabb érték.[26] A kibertámadások hálózatának

[26] A nyugati – s mindenek előtt az Amerikai Egyesült Államok offenzív kiberműveleteinek – elemzésére jelen keretek között mindössze részlegesen nyílik lehetőség, egyrészt az adatok hozzáférhetősége, elérhetősége – ill.

néhány leíró statisztikáját vizsgálva az is megfogalmazható (*1. táblázat*), hogy a hálózat centralizáltsága alacsonynak tekinthető, azaz a teljes hálózatot kevéssé dominálja egyetlen szereplő, jóllehet a kifok értékek szerinti hálózati centralizáltság magasabb (C_{kifok}=6,566%), mint a befok mutató esetében (C_{befok}=3,609%), azaz a kezdeményezett kiberműveletek esetében inkább kiemelkedik néhány meghatározó szereplő. A hálózat sűrűségére vonatkozó mutatószám ugyancsak arról árulkodik, hogy a hálózatban szereplő államok közötti lehetséges kötéseknek mindössze töredéke van jelen a valós struktúrában (S=0,0471), fontos azonban megjegyezni, hogy a sűrűségstatisztikához tartozó szórás értéke rendkívül magas (SZ_S=0,5336), azaz markáns különbségek jellemzők a hálózatban. A gráf jellemzésekor az előzőekben említett kölcsönös kötések vonatkozásában érdemes megemlíteni egy további mutatót, a reciprocitás mértékét, mely ugyancsak alacsony értéket mutat (R= 0,0524), vagyis a kapcsolatpárok csak elenyésző része bizonyul kölcsönös jellegű kötésnek, azaz oda-vissza jellegű támadásnak.

1. táblázat

A hálózat főbb mutatói

[Forrás: saját számítás és szerkesztés]

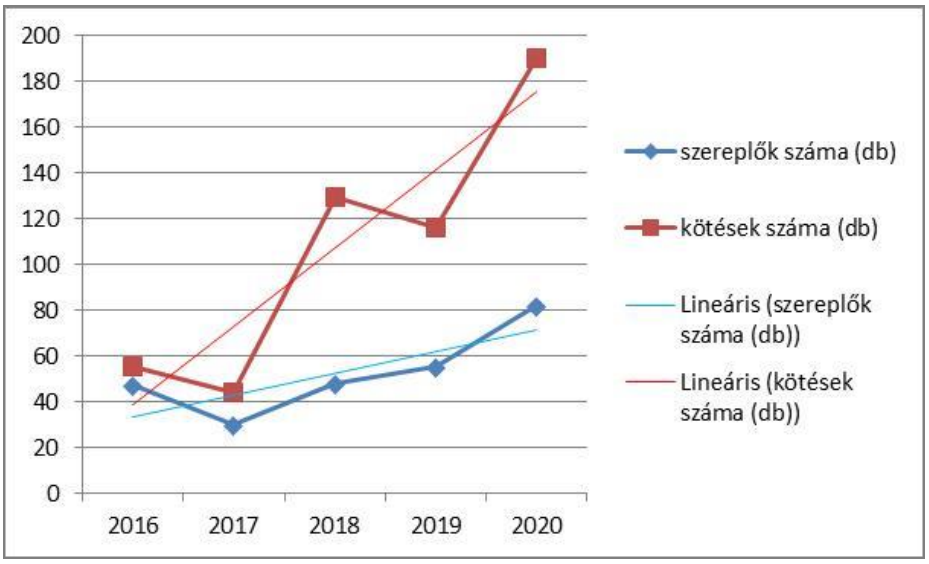
Hálózati szereplők száma	**107**
Hálózat centralizáció (kifok) (%)	**6,566**
Hálózat centralizáció (befok) (%)	**3,609**
Összes kapcsolat száma	**534**
Sűrűség (S, mátrix átlag)	**0,0471**
Szórás (S)	**0,5336**
Reciprocitás (diád alapú)	**0,0524**

A kiberműveleti hálózat időbeli dinamikája

Ahhoz, hogy képet alkothassunk a kiberműveletek hálózatának szerveződéséről, illetve az abban fontosabb szerepet játszó államok viselkedéséről, a fenti összevont mutatók mellett érdemes lehet megvizsgálni az elemzés által lefedett időszakban megmutatkozó esetleges tendenciákat és összefüggéseket.

A kibertámadások hálózatára dinamikus bővülés jellemző 2016 és 2020 között, amennyiben mind a szereplők, mind pedig a hálózatban mérhető kötések száma egyaránt növekedést mutat (*2. ábra*). Utóbbi esetében meredekebb a trend, de nyilvánvalóan a magasabb számú szereplők között jóval nagyobb a lehetősége a kapcsolatok kialakulásának.

esetlegesen az elemzett források jellege – okán, másrészt a vonatkozó államok különféle lehetséges műveleti biztonsági gyakorlatainak és a nemzetközi rendszerben való tevékenységükre vonatkozóan figyelembe vett normák és jogi követelmények folyományaképpen. Lásd ehhez pl. Kovács 2018b (különösen 141–161. ill. 163–293.), Bihaly 2022. Köszönettel tartozom a tanulmány korábbi verziójához fűzött lektori kritikáért, ill. hogy erre a problématerületre felhívta a figyelmemet és egyben iránymutatással is szolgált!

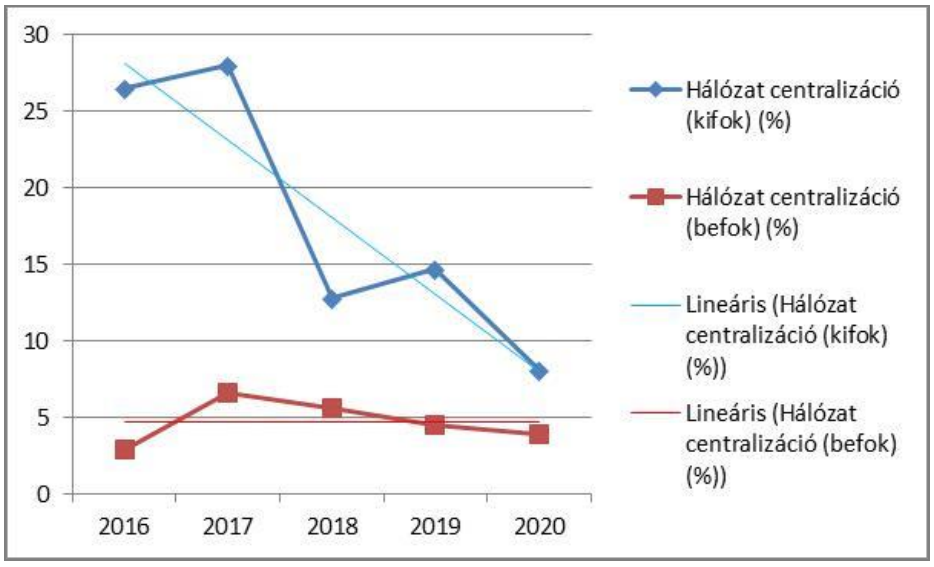


2. ábra

A hálózat dinamikája és összetétele

[Forrás: saját számítás és szerkesztés]

A hálózat központosítottsága tekintetében nem mutatható ki érdemi időbeli eltérés a befelé irányuló kapcsolatok vonatkozásában, azonban negatív trend jelenik meg a kifelé irányuló kötések vonatkozásában (*3. ábra*), azaz az idő előrehaladtával egyre kevésbé jellemző, hogy egyetlen – illetve néhány – ország kizárólagos jellemzője a kibertámadások kivitelezése, a kiberműveletek célpontjaiként szereplő országok kötései pedig egy diffúz mintázattal jellemezhetők.



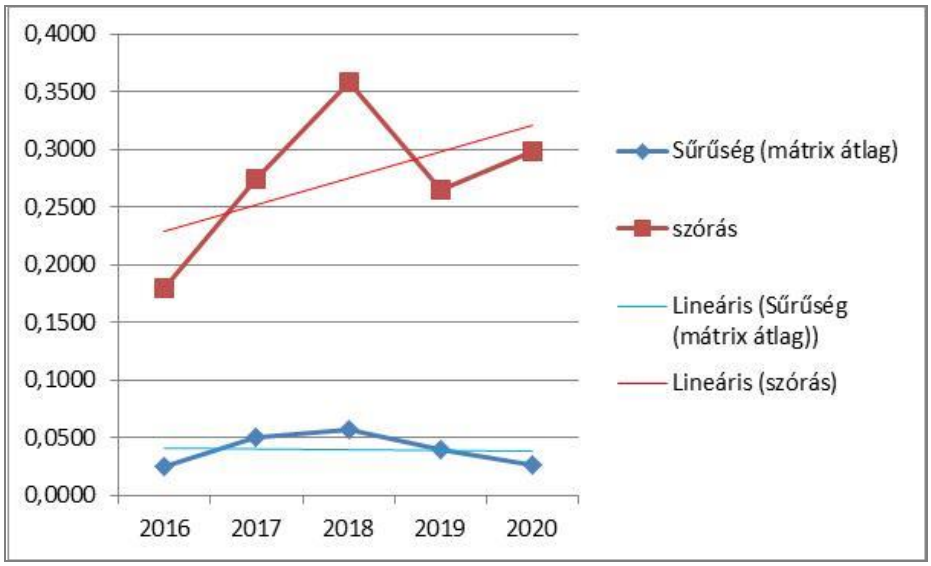
3. ábra

A hálózat központosítottságának időbeli változása és mintázatai

[Forrás: saját számítás és szerkesztés]

A hálózati centralizáció csökkenése mellett azonban nem beszélhetünk a sűrűség növekedésről, amennyiben a vizsgált időszakban lényegében nem változik a kiberműveletek hálózatának ezen mutatószáma (*4. ábra*). Ugyanakkor a sűrűség szórása emelkedő tendenciát

mutat, vagyis egyre markánsabb eltérések jellemzik a hálózatot az összevont statisztikaértékek mögött, ami – részben legalábbis – összefüggésben áll a hálózat méretével is.

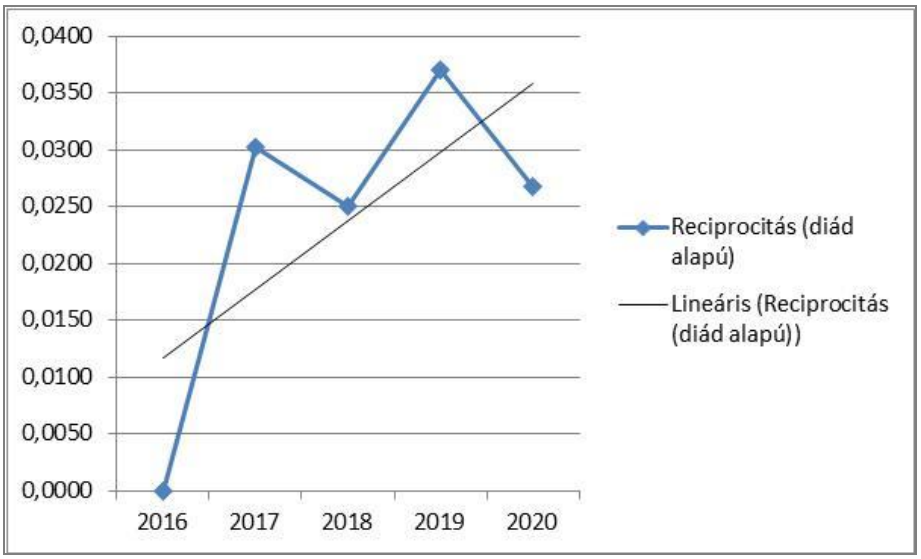


4. ábra

A hálózati sűrűség időbeli változása és mintázatai

[Forrás: saját számítás és szerkesztés]

A kölcsönös kapcsolatok előfordulása egyre jellemzőbbnek bizonyul az idő előrehaladtával (*5. ábra*), bár az erőteljes pozitív trend feltételezhetően nem kis részben annak is köszönhető, hogy a 2016-os évben nem fordult elő kölcsönös kötés.



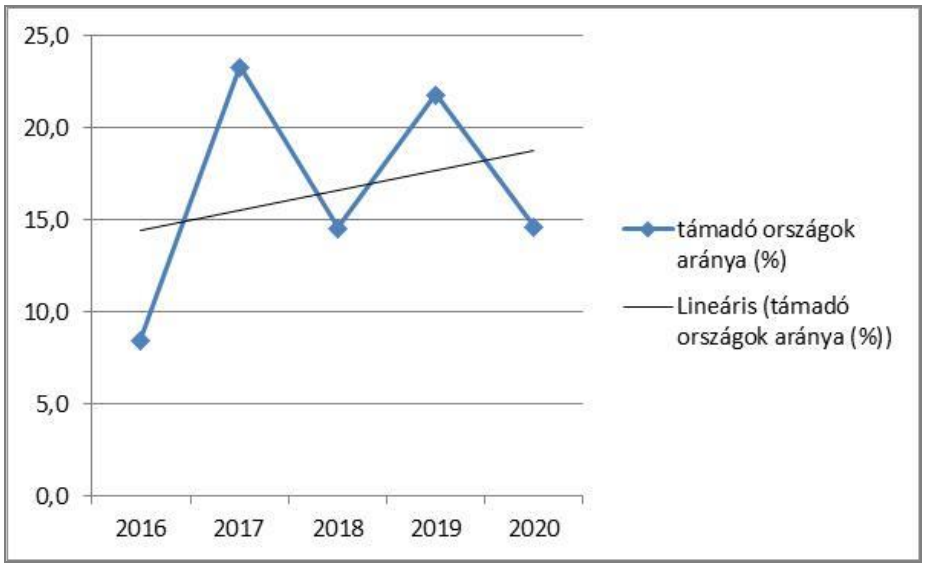
5. ábra

A kölcsönös kötések időbeli változása és mintázatai

[Forrás: saját számítás és szerkesztés]

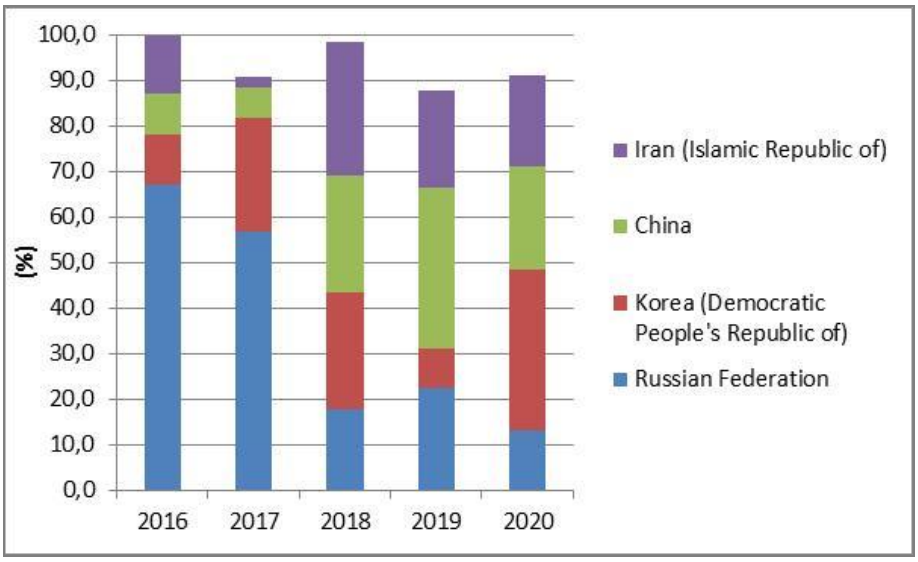
A statisztikai mutatószámok időbeli tendenciái áttekintésének zárásaként fókuszáljuk, illetve leszűkítjük az elemzést a kiberműveletek hálózatának aktív szereplőre, azaz azon országokra, melyek kibertámadások kezdeményezőiként (is) vannak jelen a struktúrában, hiszen ily módon képet kaphatunk arról, hogy milyen összetételű a hálózat bővülése ebben a

tekintetben. A támadó országok arányában pozitív trend mutatható ki (*6. ábra*), azaz az idő előrehaladtával növekszik a kiberképességeiket aktívan alkalmazó országok száma.



6. ábra
A támadó államok időbeli változása és mintázatai
[Forrás: saját számítás és szerkesztés]

Amennyiben arra is szűrjük az adatokat, hogy a teljes hálózatban kiemelkedő aktivitással bíró négy ország („Big4") milyen részesedést – milyen összetételi arányban – fed le a támadó kiberműveletek kötéseiből, akkor egy markáns átrendeződést, kicserélődést tárhatunk fel (*7. ábra*). A vizsgált időszak kezdetén domináns Oroszország részesedési aránya az összes kifelé mutató, azaz támadó kötésből először mérsékelten, majd 2018-ra radikálisan lecsökken, miközben Észak-Korea jelentős részarány növekményt realizál már 2017-ben is. Kína és Irán ugyancsak részt vesz az Oroszország relatív visszaszorulása keretében keletkező űr kitöltésében, amennyiben lényegében 2018-tól válnak igazán markáns szereplőkké. A négy kiemelkedő országnak az adott év támadó jellegű kötéseiben kitett összesített részaránya mindvégig kilencven százalék körül mozog, ami arra is utal, hogy az előzőekben vizsgált tendencia; azaz a támadó országok aránybeli bővülése mellett a „Big4" országok lényegében megőrzik kibertérbeli aktivitásuk dominanciáját.



7. ábra

A négy legjelentősebb támadó ország időbeli trendjei és mintázatai

[Forrás: saját számítás és szerkesztés]

Esettanulmány II. Kiberműveletek az orosz–ukrán háborúban

A 2022 februárjában eszkalálódó orosz–ukrán konfliktus talán leginkább kézzelfoghatónak, leglátványosabbnak tekinthető elemei a fizikai térben kibontakozó műveletek, fejlemények, sikerek és kudarcok, továbbá az Ukrajnát fegyveres harcában megsegíteni célzó nemzetközi összefogás, melyeket nagyfokú szakmai és média figyelem övezte. Emellett azonban az orosz–ukrán háború az online szféra kevéssé látható színterén, a kibertérben ugyancsak rendkívül érdekes és – jelen tanulmány tekintetében különösképpen – vizsgálatra érdemes folyamatokat és mintázatokat mutatott. Előbbiek fényében a tanulmány jelen, második esettanulmányának keretében arra vállalkozunk, hogy feltárjuk az orosz–ukrán konfliktus kibertérben zajló műveleteinek bizonyos aspektusait,[27] s némileg közelebb hozzuk a sokféle résztvevő tevékenységét, illetve az általuk végrehajtott műveletek sajátosságait és szerkezetét.[28]

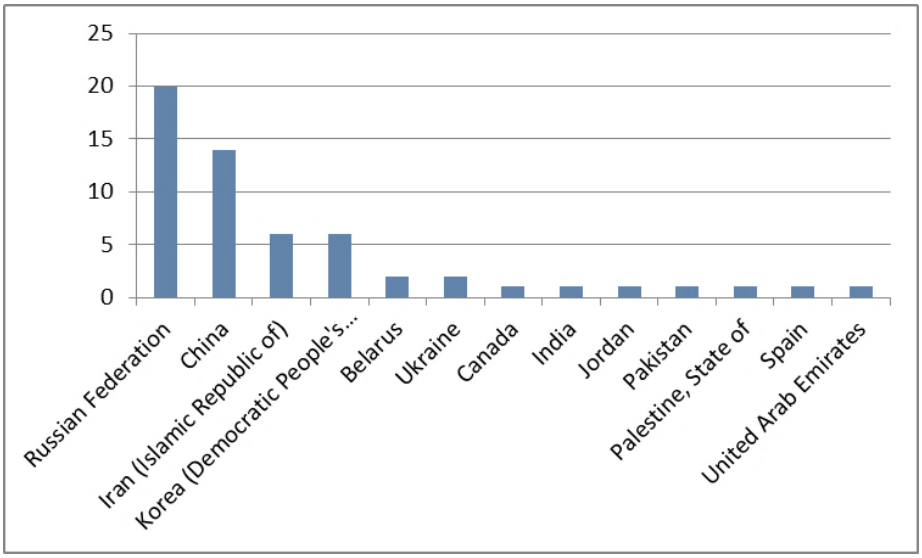
Az esettanulmány keretében vizsgált kibertébeli műveletek két részre bonthatók, melyek közül elsőként azzal foglalkozunk, melyet a tanulmány első esetbemutatása során dinamikus megközelítésben már vizsgáltunk, azaz az állami szereplők által végrehajtott támadásokat elemezzük, majd az államokhoz közvetlenül nem kötődő szereplőket vizsgáljuk.

Államok által támogatott kibertámadások

Az orosz–ukrán háború itt keresztmetszeti megközelítésmód alapján vizsgált szűk időkeretében – azaz a konfliktus 2022. február 24-én eszkalálódó első fél évében – az államokhoz köthető kibertámadások száma mindösszesen 57 műveletet jelentett. Ezen támadások legnagyobb része Oroszországhoz, valamint Kínához köthető – rendre 20. illetve 14 művelet –, ami az összes

[27] Hasonló megközelítést alkalmaz pl. White 2018.
[28] Az orosz–ukrán konfliktus kibertérbeli aspektusaihoz kapcsolódóan lásd pl. Lewis 2022; Mueller et. al. 2023; Balogh 2024.

kibertámadás közel hatvan százalékát jelenti (*8. ábra*). Az előbbi két meghatározónak tekinthető szereplőhöz további, relatíve magasabb részesedéssel jellemezhető, ugyancsak alapvetően lator államok kapcsolhatók, amennyiben Irán és Észak-Korea esetében a támadások aránya még a teljes műveletekre számított tíz százalékos szinten mozog. A fennmaradó kilenc ország legfeljebb két művelettel jelenik meg az itt vizsgált adatok alapján.

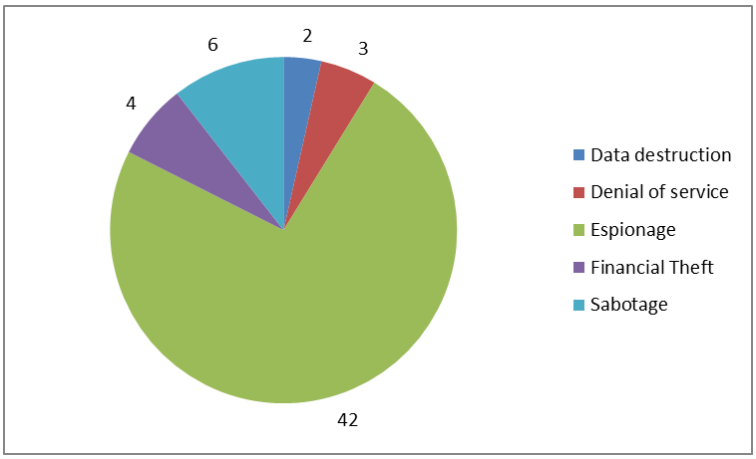


8. ábra

Az állami szereplők tevékenységének különbségei (esetszám)

[Forrás: saját számítás és szerkesztés]

A fenti államok által a kibertérben végrehajtott műveletek típus szerinti megoszlását vizsgálva (*9. ábra*) a kémtevékenység bizonyul dominánsnak: a támadások közel három negyede (42 eset) a kibertérbeli képességek előbbi, rejtett információszerzést célzó tevékenységeket fedi. A kibertér ezen hírszerzési jellegű felhasználása mellett említésre érdemesnek tekinthető még az online keretek mentén megvalósított szabotázsakciók előfordulás (6 eset), a többi művelet típus – pénzügyi célú behatolás, adatmegsemmisítés, DoS támadás – mérhető részarányban megjelenik, de ebben a metszetben nem tekinthetők meghatározónak.

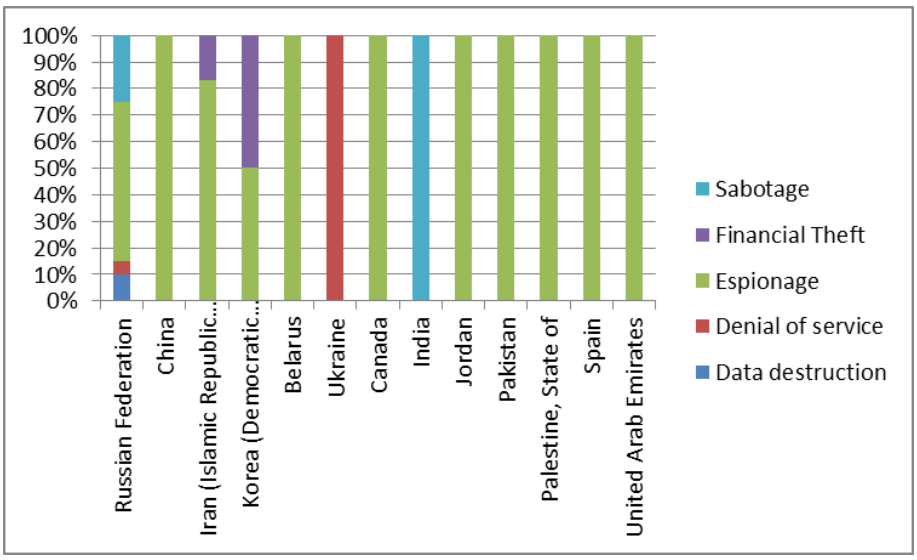


9. ábra

Az államokhoz köthető támadások jelleg szerinti eloszlása (esetszám)

[Forrás: saját számítás és szerkesztés]

Amennyiben az egyes országok tevékenységi területeit, kibertérbeli műveleti portfólióit vizsgáljuk (*10. ábra*) – itt azonban az alacsony elemszámok okán külön is fontos hangsúlyozni, hogy az adatok mindössze tájékoztató jellegűnek tekinthetők – egyrészt arra lehet rámutatni, hogy a két meghatározó szereplő eltérő stratégiát látszik alkalmazni kibertámadásai során. Míg Oroszország esetében egy meglehetősen összetett, sokrétű tevékenységi forma jelenik meg – amennyiben esetében szinte mindegyik támadási típus megjelenik, jóllehet eltérő súllyal –, addig Kína kizárólag – Irán pedig döntően – kémtevékenység vonatkozásában hasznosítja kiberképességeit. Ugyanezen mintázat jellemző a többi ország esetében is, jóllehet az esetek szórványos jellege ezt döntően érthetővé teszi.

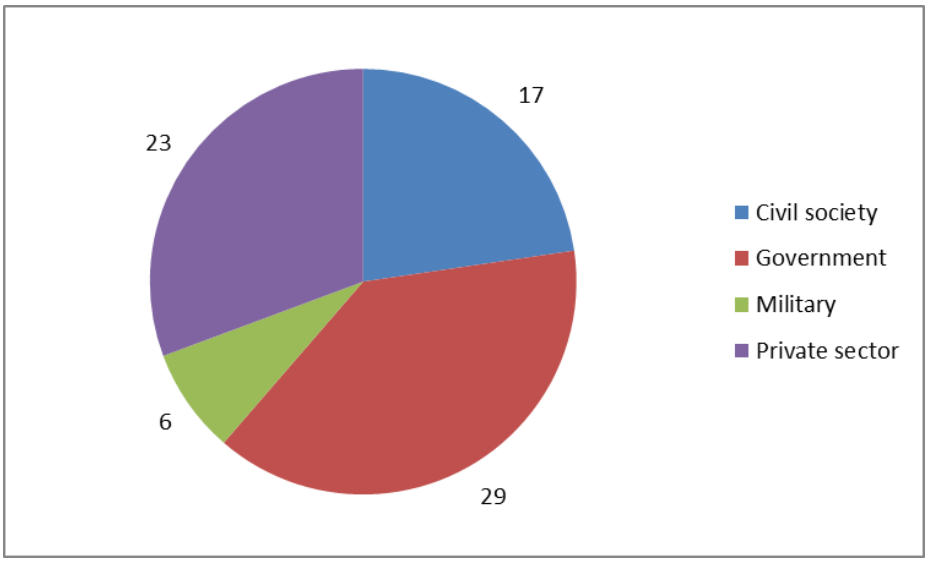


10. ábra

Az egyes állami szereplők tevékenységének összetétele

[Forrás: saját számítás és szerkesztés]

Az előbbi elemzési szemponthoz képest jóval kiegyensúlyozottabb, összetettebb kép rajzolódik ki a támadások által érintett terület vagy szektor jellege tekintetében (*11. ábra*). Mivel a kiberműveletek itt vizsgált nyilvántartása egy-egy esetben akár több terület együttes megjelenését is feltételezi, így összességében valamivel több; 75 említés mentén vizsgálható a kibertámadások ezen aspektusa. Talán nem meglepő módon a támadások legnagyobb arányban (29 említés) a kormányzati szektort érintették, amit nem különösebben jelentős lemaradással a gazdasági terület követ, továbbá a civil szektor ugyancsak nem elhanyagolható részesedét mutat. A legkevésbé jellemző terület a katonai szféra, ami – tekintve a támadási formák esetében kirajzolódó eloszlást – részben talán magyarázható ezen terület fokozott védelmével, illetve zárt jellegével, de lehetséges az a felvetés is, hogy a szembenálló fél nem a maradék elv alapján, hanem célzottan támadja a célpont állam más – jellemzően a hátországhoz kapcsolható – területeit.

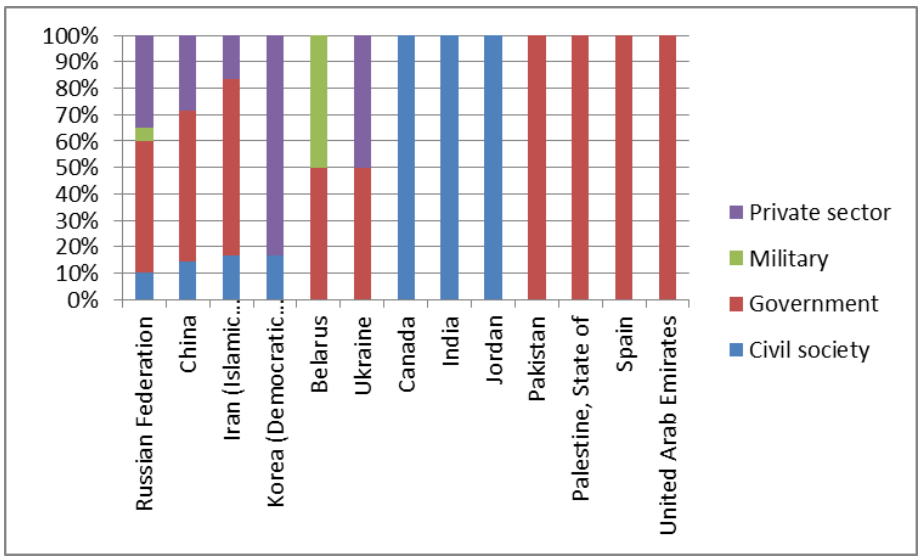


11. ábra

Az állami szereplők által támogatott kibertámadások által érintett szektorok (esetszám)

[Forrás: saját számítás és szerkesztés]

A kiberműveletek által érintett szektorok lefedettsége az egyes szereplők esetében ugyancsak szerteágazóbban megjelenik ebben az esetben (*12. ábra*). Oroszország mind a négy, de Kína és Irán is legalább három különféle területen tevékenykedett az adatok tanúsága szerint, míg a többi ország esetében a támadások szórványosságának megfelelően egy-egy terület jelenik meg.



12. ábra

Az egyes állami szereplők tevékenysége által lefedett területek (%)

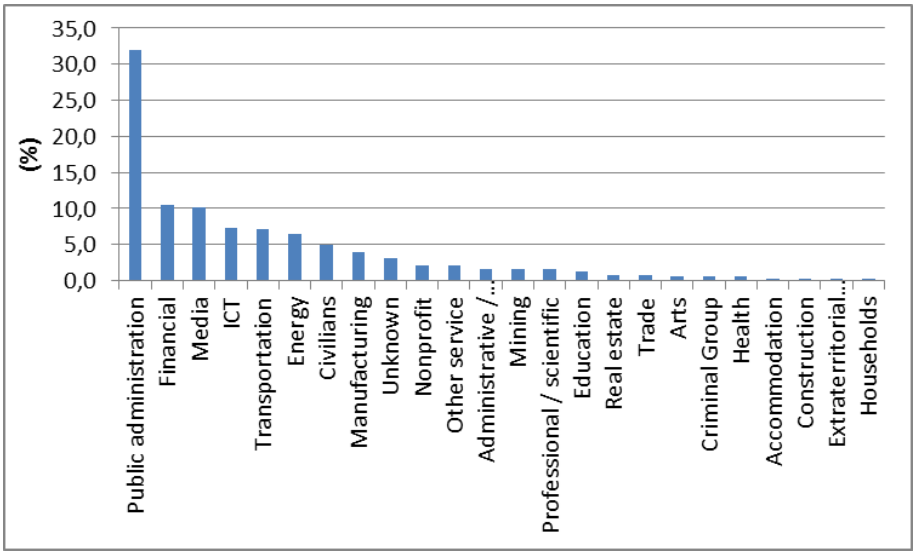
[Forrás: saját számítás és szerkesztés]

Nem közvetlenül állami kötődésű szereplők műveletei

Az orosz–ukrán konfliktus 2022. februári eszkalációs pontját követő itt vizsgált időszak nem közvetlenül állami irányítás alatt működő szereplői által megvalósított műveletek –

mindösszesen 382 művelet, melynek kezdeményezői között 54 csoportot, elkövetőt, illetve 29 megtámadott országot találhatunk – legnagyobb arányban a közigazgatás terület ellen irányultak – a támadások közel egy harmada (31,9%) ilyen célpontokhoz köthető (*13. ábra*). Előbbihez képest jelentősen elmaradva, de még az egy tizednyi részesedési arányt elérő mértékben fordulnak elő a pénzügyi szektort és a média területét érintő támadások, melyeket további – jellemzően kritikus infrastrukturális rendszerekhez kapcsolódó területek – követnek, amennyiben az info-kommunikációs technológiákhoz kapcsolódó célpontok, a szállítási-közlekedési elemek valamint az energetikai infrastruktúra területe hat-hét százalékos részarányt tesznek ki. Az állampolgárok elleni támadások öt százalékos arányát követően a műveletek támadási területek szerinti szétaprózódása figyelhető meg, hiszen a támadások fennmaradó, hozzávetőlegesen egy ötödnyi része (21,5%) mindösszesen tizenhét kategóriában elosztva található meg.

A támadási területek tehát döntően olyan szektorokat érintenek, melyek az érintett ország állami szintű működésének, működtetésének alapelemeit (közigazgatás, pénzügyi szektor, média), továbbá bizonyos kritikus infrastrukturális rendszereit jelentik.



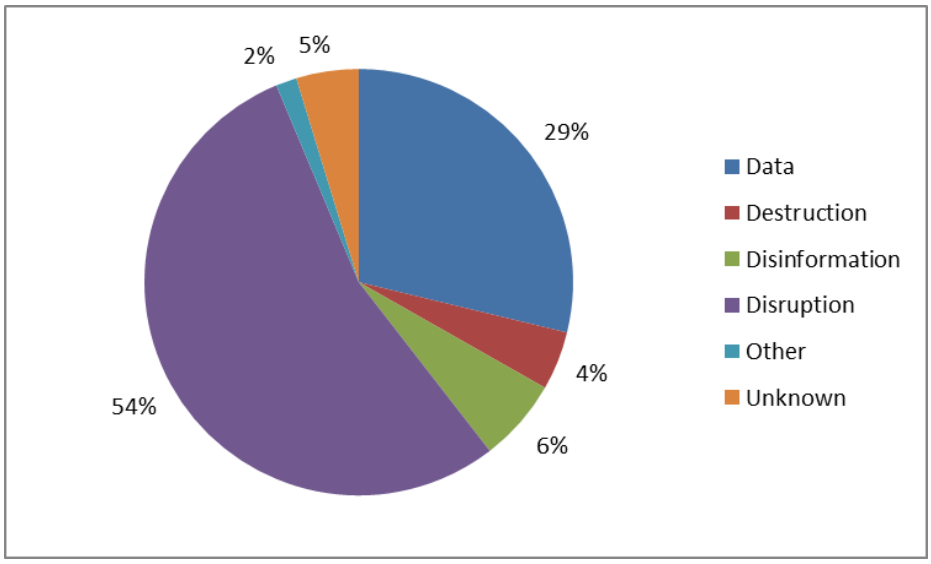
13. ábra

A proxy szereplők tevékenységi területei (%)

[Forrás: saját számítás és szerkesztés]

Az előbbiekben feltárt eredmények fényében nem tűnik meglepőnek, hogy az itt vizsgált kibertérbeli akciók legnagyobb része – több mint fele (54%) – a megtámadott ország működési feltételeinek akadályozására, gátolására, megzavarására irányul, emellett pedig ugyancsak relatíve jelentős arányban fordul még elő (29%) az adatokat érintő támadások, azokkal való visszaélések kategóriája (*14. ábra*). A támadási tevékenységek között a dezinformáció is megjelenik, bizonyos mértékben ugyancsak megtalálhatjuk a célpontba állított rendszerek elpusztításának, megsemmisítésének szándékát. A műveletek ezen aspektusában elenyésző arányban jelennek meg egyéb formák, s az esetek öt százaléka vonatkozásában nem áll rendelkezésre tartalmilag értelmezhető információ.

A támadások összetételét tekintve tehát az állami-társadalmi keretek működésének megzavarását, korlátozását jelentő műveletek képezik a legfőbb megjelenési formát, ami kiegészülve az adatokat érintő akciókkal, az összes vizsgált támadás több mint négyötödét meg lehet ragadni.

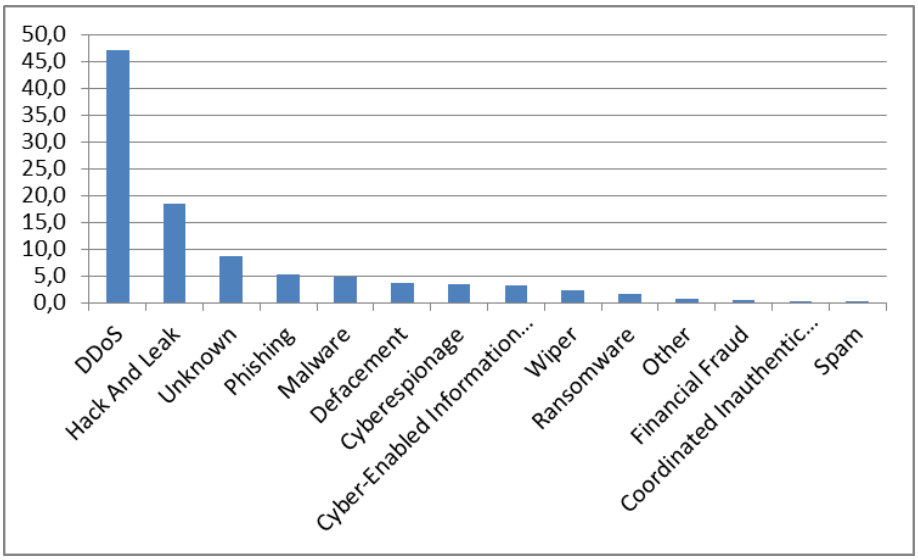


14. ábra

A nem közvetlenül állami kötődésű szereplők támadásainak jellege (%)

[Forrás: saját számítás és szerkesztés]

A társadalmi-állami élet megzavarása és az adatokat érintő támadások meghatározó jellege ugyancsak alapvetően érthetővé teszi, hogy az orosz–ukrán háború kiberdimenziójában zajló műveletek legnagyobb, kimagasló része túlterheléses támadás formájában valósult meg (*15. ábra*). Az alkalmazott eljárások közel felét (47,1%) kitevő DDoS támadások mellett – előbbitől jóval elmaradva bár, de – további relatíve jelentősnek tekinthető arányban (18,3%) fordul elő az információk, adatok megszerzése majd közzététele, kiszivárogtatása, s az is kiemelendő, hogy a műveletek közel egy tizede – pontosan 8,6 százaléka – esetében nem ismert, nem beazonosítható a támadás vektora. Az adathalászat és malware-ek alkalmazása még az öt százalékos arány körüli részesedési értékekkel jelenik meg a támadási formák között, s ezek mellett megtalálhatók a weboldalak feltörésével és megjelenésének megváltoztatásával járó defacement, a kiberkémkedés, az online csatornákon keresztül megvalósított befolyásolási műveletek, az adattörlésekre épülő wiper támadási mód, valamint a zsarolóprogramok alkalmazása, továbbá egy százalékos részesedési arányt nem meghaladó mértékben további egyéb formák. Megfogalmazható tehát, hogy – a támadások célterületével, céljával összhangban – az alkalmazott eljárások döntően túlterheléses támadásokat, továbbá kiszivárogtatásra épülő műveletformákat jelentenek.



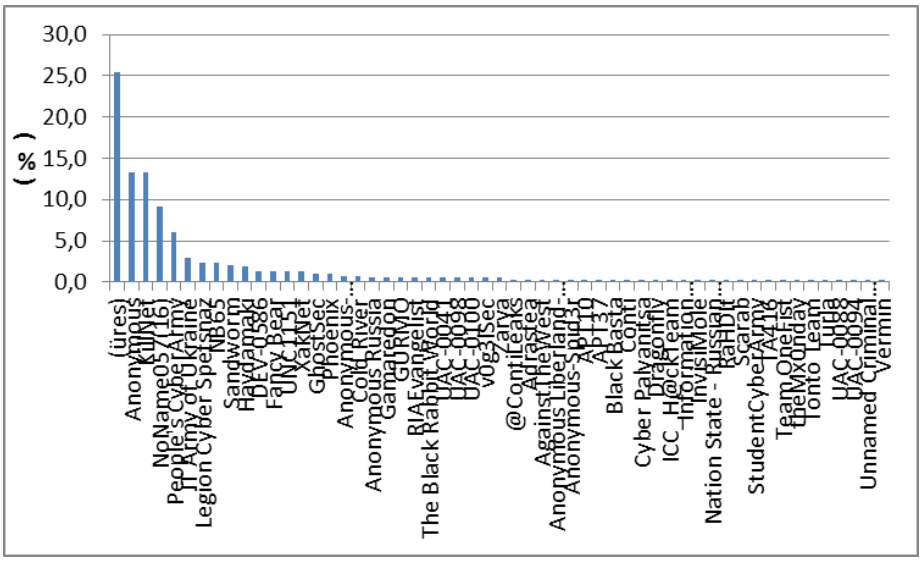
15. ábra

A proxy csoportok kibertámadási formái (%)

[Forrás: saját számítás és szerkesztés]

Az elemzés tárgyát képező kibertérbeli műveletek mögött összesen 54 – valamilyen mértékű bizonyossággal beazonosíthatónak tekinthető – különféle csoportot, illetve elkövetőt feltételezhetünk, melyek tevékenysége mindösszesen 29 ország ellen irányul. Fontos azonban elsőként kiemelni, hogy a támadások elkövetői az akciók legnagyobb része; 25,4 százaléka esetében nem ismertek, azaz valamivel több mint az esetek egy negyede (!) vonatkozásában nem beazonosítható a támadásért felelős csoport vagy elkövetői kör (*16. ábra*) – részben itt is fellép tehát a kibertámadások tekintetében jól ismert attribúciós kihívás. A beazonosítható támadások elkövetői vonatkozásában a közismertnek tekinthető Anonymous csoport, valamint az orosz kötődésűnek tekintett KillNet hackercsoport azonos részesedési aránnyal (13,4%) foglalják el a domináns pozíciót, melyeket az ugyancsak oroszbarát NoName057(16) hackercsoport követ a támadások közel egy tizedét kitevő aránnyal, valamint a szintén az Oroszország mellett tevékenykedő People's CyberArmy esetében mérhető még öt százalékot meghaladó részesedés. A fennmaradó mindösszesen 50 csoport, illetve elkövető a támadásoknak mindössze kevesebb mint egy harmadán osztozik összesen. Köztük kiemelhető az Ukrajnához kapcsolható IT Army of Ukraine, mely azonban összességében csak közel három százalékos arányt (2,9%) tudhat magáénak, továbbá a támadások ezen szempontból vett eloszlása tekintetében jellemzőnek tekinthető az is, hogy a beazonosítható elkövetők fele mindössze egy-egy támadás erejéig jelenik meg az itt vizsgált időkeret adatainak tanúsága szerint.

Egy erőteljes koncentráció mutatható ki tehát a támadásokért felelősnek tekinthető csoportok, elkövetők tekintetében, amennyiben az orosz-ukrán háború itt áttekintett időszakában a támadások jelentős része – több mint két ötöde – mindössze négy kollektívához köthető, melyek többsége a konfliktus oroszországi oldalán lép fel.



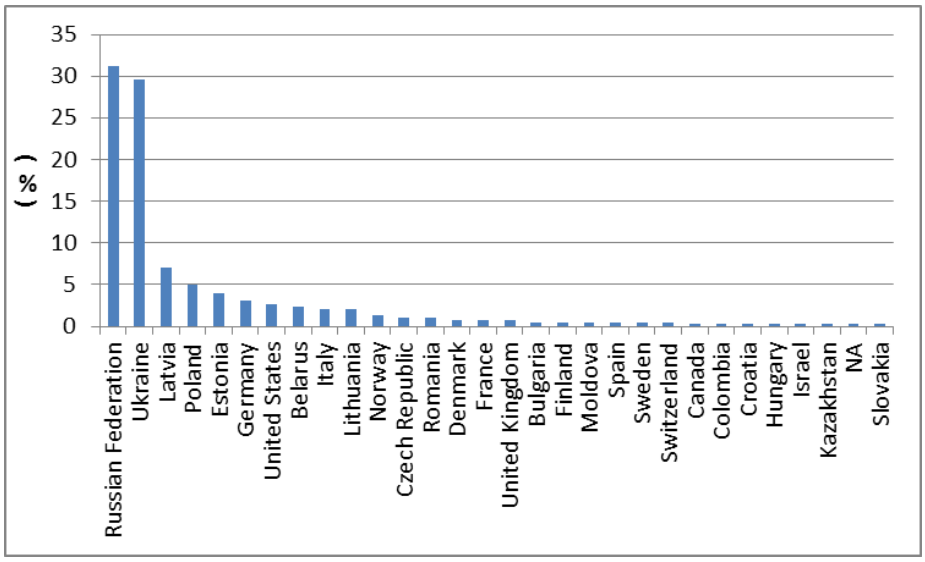
16. ábra

A nem közvetlenül állami kötődésű szereplőkköre

[Forrás: saját számítás és szerkesztés]

Ugyanakkor a kibertámadások célpontjaiként megjelenő országok között ugyancsak Oroszország kerül az első helyre, jóllehet mindössze néhány százalékpontos különbséggel megelőzve ellenségét, Ukrajnát (*17. ábra*). A konfliktus előbbi két főszereplője mindazonáltal a támadásoknak mindössze kevesebb mint két harmadát (60,7%) tudhatja magáénak, s a vizsgált kiberműveletek fennmaradó része huszonnyolc további egyéb országban oszlik meg különféle részesedések mentén. Ezen országok körében a leginkább érintettek között mindenek előtt Ukrajnával szolidáris államok találhatók – Lettország, Lengyelország, Észtország mellett Németország és Amerikai Egyesült Államok is –, bár az összes támadás valamivel több mint két százaléka a konfliktusban Oroszország szövetségesének tekinthető Fehéroroszország ellen irányul. Olaszország és Litvánia, Norvégia, valamint Csehország és Románia esetében még egy százalékot valamelyest meghaladó részarányok mérhetők, a fennmaradó államoknál pedig néhány akció fordul elő.

A kibertérbeli műveletek a két egymásnak feszülő ország mellett jelentős arányban irányulnak tehát további, a konfliktusnak közvetlenül részt nem vevő országok felé, melyek között többségben az Ukrajnának segítséget nyújtó államokat ismerhetjük fel, ami összhangban van azzal az előző megfigyeléssel, hogy a vizsgált kiberműveletek terén a legaktívabbnak bizonyuló csoportok, illetve elkövetői kör jellemzően a konfliktus oroszországi ágához köthető.

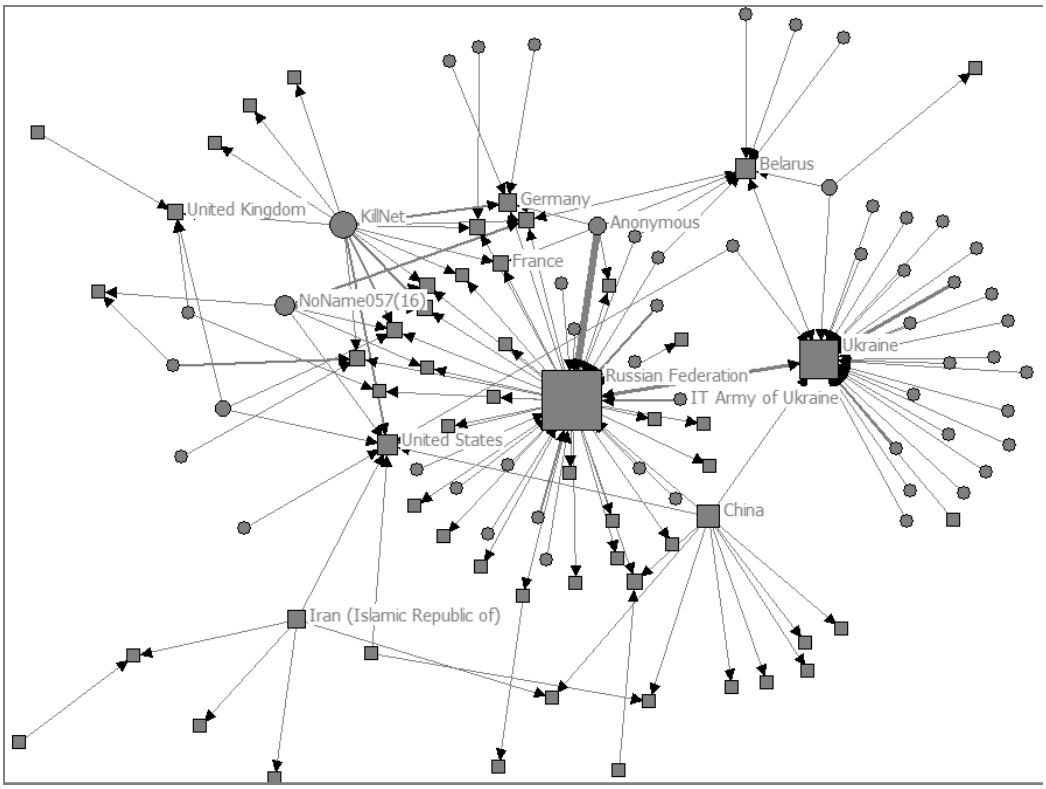


17. ábra

A proxy szereplők célpontjait jelentő országok

[Forrás: saját számítás és szerkesztés]

A konfliktus vizsgált időszakában a kibertér fentiekben bemutatott államai és államok által közvetlenül nem irányított szereplői által végrehajtott műveletek hálózata egy összefüggő struktúrában mutatkozik meg (*2. gráf*). A különféle – államtól állam felé közvetlenül mutató, illetve az előzőekben áttekintett kibercsoportok, elkövetők, kollektívák által megvalósított – kiberműveletek és támadások struktúrájában középponti helyzetben Oroszország található, mely centrális pozíciója mellett a legmagasabb kapcsolati számmal is jellemezhető. A 2022. február 24-én a fegyveres agressziót kezdeményező országot erős, kölcsönös él kapcsolja össze a hálózatban Ukrajnával, azaz a két ellenség közvetlenül (is) számos kibetérbeli műveletet hajtott végre egymás ellen. Ukrajna hasonlóképpen kölcsönös – bár az előbbihez képest kevésbé erős – kötéssel kapcsolódik Fehéroroszországhoz, ily módon képezve azt a triádot, mely lényegében a legmarkánsabb kapcsolatszámokkal jellemezhető az érintett országok között. Az vizsgált időszakban a kibertámadások tekintetében aktív országok között kiemelhető még Kína és Irán, valamint az Amerikai Egyesült Államok, mint a relatíve jelentősebb fokszámmal bíró állami szereplők, melyek azonban a hálózat egy külsőbb, illetve átmeneti vagy félperiférikusnak tekinthető szegmenségben kapnak helyet, s előbbi két ország jellemzően inkább egy-egy saját maga körül kialakított klaszter központi elemeként helyezkedik el, részleges kapcsolódásokkal a hálózat nagyobb, sűrűbben összefüggő tartományához. A jelentősebb nem állami szereplőkről részben hasonló megállapítások tehetők, amennyiben ezek jellemzően a lényegében egyfajta hálózati középpontot képező Oroszország körül koncentrikusan képezhető mező második szegmensében helyezkednek el, ami egy meglehetősen érdekes mintázattal magyarázható. Nevezetesen az tárható fel, hogy ezek a szereplők jellemzően egymástól eltérő országokkal szemben egyaránt végrehajtottak kibertérbeli akciókat. A KillNet csoport például tizenkettő államot ért el kibertevékenységével, többek között Németországot és Franciaországot, mely államok ellen – egyebek mellett – Oroszország közvetlenül is támadta a kibertérben.

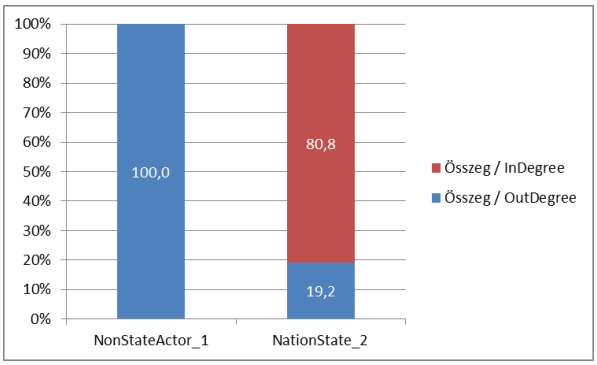


2. gráf
Az orosz–ukrán kiberháború első félévének hálózati térképe
[Forrás: saját szerkesztés komplex adatbázis alapján. Megjegyzés: négyzet: állam, kör: proxy szereplő.]

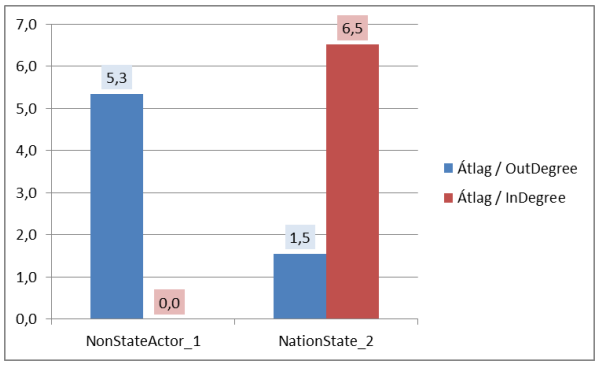
A hálózat ezen szegmenségben tehát olyan országokat találunk, melyek egyszerre bírnak állam-állam és nem állami szereplő-állam támadási relációval. A NoName057(16) csoport esetében hasonló a mintázat, jóllehet részben más országok felé irányulnak a műveletei. Fontos lehet felhívni a figyelmet arra is, hogy utóbbi két oroszországi kötődésű csoport *egyike sem* áll közvetlen támadási relációban Ukrajnával, sokkal inkább arról van szó, hogy egyfajta „ellenségem barátja az ellenségem” mintázat keretében az Ukrajnának támogatást nyújtó államok ellen tevékenykednek. Ugyancsak rendkívül sajátos hálózati pozícióban találjuk az Anonymus-t, mely amellett, hogy dominánsan Oroszország ellen fejti ki tevékenységét, emellett több más – Oroszország által ugyancsak közvetlenül támadott (!) – ország ellen fellépett – mindenek előtt itt érdemes példaként említeni Németországot és Franciaországot. Az alacsonyabb aktivitással jellemezhető szereplők alapvetően egy-egy állam ellen fejtik ki tevékenységüket – példaként említhető itt Ukrajna oldaláról az IT Army of Ukraine csoport –, ily módon képezve egy-egy többszereplős, de belsőleg nem összefűzött, kevéssé strukturált csoportosulásokat.

Az orosz–ukrán háború itt vizsgált félévek időszakában tehát a kibertérben működő állami és egyéb szereplők között egy összefüggő, integrált hálózat tárható fel a kiberműveletek mentén, mely hálózatban kiemelkedik néhány meghatározó szereplő a háló struktúrája szempontjából (is) mindkét szereplő típus tekintetében, egy meglehetősen sokszínű és összetett mintázatot eredményezve.

A hálózat irányított élei alapján kiszámítható fokszám eloszlás felhasználásával végzett számítások arra is lehetőséget adnak, hogy megvizsgáljuk a két szereplőtípus viselkedésében megmutatkozó esetleges különbségeket. Ennek kapcsán – mind a kapcsolati szám összegek, mind pedig az átlagot értékek vonatkozásában (*18A, 18B. ábrák*) – megállapítható, hogy a nem állami szereplők kizárólag kifelé mutató – azaz támadó jellegű – kötésekkel rendelkeznek a hálózatban. Az országok pedig – előbbinek megfelelően – döntően célpontként jelennek meg, jóllehet a támadások közel egy ötödét (19,2%) az állami szereplők tudhatják magukénak. Az egy szereplőre eső átlagos értékek viszonylatában pedig szintén jelentős többlet mutatkozik az államok tekintetében, amennyiben átlagosan több mint négyszeres mértékű a támadásoknak való kitettségük.



18A. ábra



18B. ábra

[Forrás: saját számítás és szerkesztés]

A konfliktus nem közvetlenül állami irányítás alatt működő kiberszereplői által megvalósított műveletek összességében tehát jellemzően a megtámadott ország működésének meggátolását, akadályozását szolgálták olyan területek célpontba helyezésével mint a közszolgáltatások, a pénzügyi szektor és média, amihez jellemzően túlterheléses támadási formát valamint kisziváro gtatásra épülő megoldásokat alkalmaztak. A dominánsnak tekinthető támadó felek köre részesedési arányuk alapján jól lehatárolható, a megtámadott országok köre pedig meglehetősen szélesnek tekinthető, amennyiben a két közvetlenül szembenálló fél mellett számos további – legalább két tucat – egyéb ország található meg. A szereplők közötti kiberműveletek eredményeképpen egy összetett, strukturált hálózat képe bontakozik ki, melyben ugyancsak felismerhetők a domináns szereplők, továbbá a közvetlen – akár kölcsönös – szembenállás mellett a közvetett kapcsolódások is feltárhatók.

Összegzés, értékelés, kitekintés

A tanulmányban arra vállalkoztunk, hogy feltárjuk és jellemezzük a NATO 2016-os döntése alapján hivatalosan is elfogadottá váló kiber domainben jellemző mintázatokat, az ott zajló folyamatokat és az abban található szereplőket, viselkedésüket. A kutatási téma szakirodalmi beágyazását és kérdésfelvetésének megjelölését követően kvantitatív esettanulmányok bemutatásán keresztül mind hosszabb időtartományban dinamikus, mind pedig keresztmetszeti, fókuszált formában vizsgáltuk a kiberműveleteken keresztül kirajzolódó

kiberhadviselési hálózatokat. Az esettanulmányok – fontosabbnak tekinthető – eredményei alapján (1) a kibertér állami szereplőinek tevékenységén keresztül egy *komplex* és *integrált*, ugyanakkor meglehetősen *strukturált hálózat* tárható fel, melyben kiemelkedik néhány meghatározó állam. Ezen államok, illetve az általuk a kibertérben támadott országok között (2) több esetben is *kölcsönös relációk* rajzolódnak ki, ami a hálózat beágyazottságát tovább növeli. A feltárt kiberhadviselési hálózatban (3) – mindenek előtt a kötések és szereplők száma tekintetében – kimutatható egy *bővülési, növekedési trend*, ami ugyanakkor csökkenő ill. stagnáló hálózati központosítottság, változatlan hálózati sűrűség, és egyre jelentősebb mértékű kölcsönösségi relációkkal zajlik. Megfogalmazható tehát, hogy a kiberhálózat az itt vizsgált időszakban egyre inkább egymás felé forduló kötések alapján látszik tagolódni, ami egyrészt (4) a *kibertámadásokban érintett országok növekedésé*vel magyarázható, másrészt a hagyományosan támadólag fellépő országokon *belül* is az átrendeződés jelei mutatkoznak – alapvetően Oroszország kárára nyer teret a többi állam. A kiberhadviselés globális hálózata tehát nem csak mennyiségileg bővül, hanem belső szerkezetét tekintve, minőségileg is az átrendeződés képét mutatja, melyben egyre gyakoribbá válik a *korábban támadások tekintetében nem meghatározó államok aktivizálódása*. A kibertérbeli összeütközések másik meghatározó aspektusának tekinthető a kibertér szereplőinek kibővülése – pontosabban a korábbról már ismert szereplők tevékenységének fókuszpontba kerülése, amit a második esettanulmányon keresztül igyekeztünk empirikusan megvilágítani. Az orosz-ukrán háború első időszakában kibontakozó kiberhadviselési hálózat feltárása lehetősége adott – egyebek mellett – annak illusztrálására, hogy (5) a rendkívül sokrétű tevékenységi területtel és tevékenységi formával jellemezhető, laza megszerveződésű, államokhoz közvetlenül nem kötődő csoportok, elkövetők (6) meghatározóbb részarányt és súlyt képviselnek a kiberhadviselési hálózatban az állami szereplőkhöz képest. A proxy csoportok ezen relatív jelentőssége – újfent – nem is elsősorban az általuk képviselt számbeli fölény és művelet mennyiségben jelölhető meg, hanem (7) az esetükben is megmutatkozó aránytalanságokban, de még inkább azon (8) sajátos kapcsolódási mintázatokban, melyek egy-egy meghatározó, közvetlen állami kapcsolódással nem bíró szereplő esetében kirajzolódott. Mindenek előtt érdemes lehet utalni itt (8) a háború irányában alapvetően közvetett formában történő beavatkozásra, ill. a némely esetben összetett, részben ellentmondásosnak tűnő műveleti hatósugárra.

Az esettanulmányok keretében összefoglalt adatelemzések tanulságai megerősíteni látszanak tehát azon változási irányokat, tendenciákat, melyek alapján a kiberhadviselés, illetve. az állami érdekek kiberműveleteken keresztül történő érvényesítése stratégiai szinten is egyre hangsúlyosabb szerephez juthatnak az új évezredben,[29] a bemutatott kutatási eredmények emellett továbbá arra is rámutathatnak, hogy mindezen folyamatok egy rendkívül összetett, komplex módon szerveződő rendszerben zajlanak le. Ezen rendszer aktorai összetételüket tekintve is folyamatosan változnak, bővülnek, átalakulnak, viselkedésüket, illetve tevékenységüket tekintve pedig ugyancsak egyre finomabb, magasabb koordinációs szintet igénylő műveleti mintázatokat mutatnak fel. Előbbiek fényében kutatómunkánk

[29] Lásd ehhez pl. Kassai, Nagyszegi, Pozderka 2018; Krasznay 2022; Kovács 2023; Krasznay 2023.

további lehetséges irányaiként azonosíthatjuk be a szereplők közötti viszonyok mélyebb feltárását, az eltérő szereplőtípusok – különösen az állami és nem állami szereplők – közötti kapcsolódások és interakciók részleges vizsgálatát – beleértve a lehetséges motivációk és célok jellegzetességeit[30] –, valamint annak módszeres feltárását, illetve az elemzésbe való beemelését, hogy a kiberképességek fejlesztésének ill. alkalmazásának doktrinális háttere miként játszik szerepet az országok között kimutatható különbségekben.[31]

FELHASZNÁLT IRODALOM

Bányász Péter 2019. A közösségi média szerepe a választásokban. *Nemzetbiztonsági Szemle,* 7 (1): 85–105.

https://doi.org/10.32561/nsz.2019.1.7

Bányász Péter 2012. A közösségi média szerepe a 21. század hadseregeiben. *Hadtudomány,* 22 (1–2): 152–161.

Balogh Péter 2024. Államok kiberfenyegetettsége az új évezredben – az orosz–ukrán háború példájának vizsgálata. In Székely Zoltán – Zsezserán Anikó (szerk.): *Állam a krízisek árnyékában. Globális fenyegetettség és közigazgatás*. 26–55. Budapest: HM Zrínyi Nonprofit Kft. – Zrínyi Kiadó.

Bihaly Barbara 2022. Kibervédelem a NATO-ban és az EU-ban. *Hadtudományi Szemle,* 15. (4): 37–49.

https://doi.org/10.32563/hsz.2022.4.3

Brányi Bence 2018. Szemelvények a kiberhadviselés jelenéből. Az informatika uralta haderők sebezhetőségének érzékeltetése öt példán keresztül I. rész. *Haditechnika,* 52 (4): 14–18.

https://doi.org/10.23713/HT.52.4.03

Buzan, Barry, Wæver, Ole, de Wilde, Jaap 1998. *Security: A New Framework for Analysis*. London: Boulder, Lynne Rienner Publisher.

https://doi.org/10.1515/9781685853808

Chwe, Hanyu 2016. The Rise of Cyber Warfare: The Digital Age and American Decline. *Swarthmore International Relations Journal,* (1): 43–49.

https://doi.org/10.24968/2574-0113.1.11

Dévai Dóra 2022. A kiberképességek szervezeti integrációja az Amerikai Egyesült Államok haderejében – adaptációs lehetőségek a Magyar Honvédség számára. *Honvédségi Szemle,* 150 (1): 20–34.

https://doi.org/10.35926/HSZ.2022.1.2

[30] Lásd ehhez pl. Kovács 2018a; Kovács 2023.

[31] Lásd ehhez pl. Kovács 2018b., Kassai 2022., Dévai 2022. Köszönettel tartozom a tanulmány korábbi verziójához kapott vonatkozó lektori kritikáért, mely felhívta a figyelmemet ezen kérdéskörnek az elemzésbe való beemelése relevanciájára és fontosságára! A kutatómunka további szakaszában ezen aspektus kiemelt területként szerepel. Különösen érdekes lehet ez a kérdéskör az esetleges időbeli változások, oda-vissza hatások tekintetében, ami ugyancsak egy külön irányát jelentheti a további kutatómunkánknak.

Farkas Ádám – Kelemen Roland 2023. *Nemzeti biztonság és kibertér*. Budapest: Nemzeti Média- és Hírközlési Hatóság Médiatanács Médiatudományi Intézete.

Fazekas Ferenc 2022. A multitér (multi-domain) műveletek kialakulása és szükségessége. *Hadtudomány,* 32 (2): 59–73.

https://doi.org/10.17047/HADTUD.2022.32.2.59

Fekete-Karydis Klára, Lázár Bence 2020. A kibervédelem katonai dimenziói. *Honvédségi Szemle,* 148 (3): 44–54.

https://doi.org/10.35926/HSZ.2020.3.4

Gazdag Ferenc, Remek Éva 2018. *A biztonsági tanulmányok alapjai*. Budapest: Dialóg Campus Kiadó.

Haig Zsolt, Kovács László 2008. Fenyegetések a cybertérből. *Nemzet és Biztonság,* 2008. május. 61–69.

Haig Zsolt, Várhegyi István 2005. *Hadviselés az információs hadszíntéren*. Budapest: Zrínyi Kiadó, HM Zrínyi Kommunikációs és Szolgáltató Kht.

Haig Zsolt 2018. *Információs műveletek a kibertérben*. Budapest: Dialóg Campus Kiadó.

Haig, Zsolt 2021. Relationships between Cyberspace Operations and Information Operations. *Advances in Military Technology,* 16 (1): 91–105.

https://doi.org/10.3849/aimt.01466

Haig Zsolt 2022. Kibertéri kognitív befolyásolás az információs műveletekben. *Hadtudományi Szemle,* 15 (2): 115–130.

https://doi.org/10.32563/hsz.2022.2.7

Horváth Attila, Erdősi Péter Máté, Kiss Ferenc 2016. Az informatikai sérülékenységek gazdasági összefüggései – A kiberbiztonság megjelenése a makro- és mikroelemzésekben. In Horváth Attila – Kiss Ferenc (szerk.): *IT és hálózati sérülékenységek társadalmi-gazdasági hatásai.* 109–135. Budapest: Információs Társadalomért Alapítvány.

Horváth Attila 2013. Az ellátási láncok biztonsága. *Magyar Rendészet,* 2013 (Különszám): 45–53.

Joubert, Vincent 2010. Getting the essence of Cyberspace; a theoretical framework to face Cyber Issues. In Czosseck, Christian – Podins, Karlis (szerk.): *Conference on Cyber Conflict Proceedings 2010.* 111–126. Tallinn: Cooperative Cyber Defence Centre of Excellence Publications.

Kassai Károly, Nagyszegi Teréz, Pozderka Gábor 2018. Stratégiai szintű kibervédelmi áttekintés. *Szakmai Szemle,* 16 (3) 185–197.

Kassai Károly 2022. A kibertér műveleti képesség szerepének, jelentőségének és fókuszának evolúciója a NATO stratégiai dokumentumai alapján. *Military and Intelligence Cybersecurity Research Paper*, 2022/9. 1–38.

Kovács László, Krasznay Csaba 2017. Mert övék a hatalom: Az internet politikát (is) befolyásoló hatása a 2016-os amerikai elnökválasztás során. *Nemzet és Biztonság*, 10 (3): 3–15.

Kovács László 2013. Cyberterrorizmus: valós vagy túldimenzionált veszély? *Magyar Rendészet,* 2013 (Különszám): 85–94.

Kovács László 2018a. *A kibertér védelme*. Budapest: Dialóg Campus Kiadó.

Kovács László 2018b. *Kiberbiztonság és -stratégia*. Budapest: Dialóg Campus Kiadó.

Kovács László 2021a. Offenzív kiberműveletek 1.: Az offenzív kiberműveletek természete. *Hadmérnök,* 16 (2): 187–204.

https://doi.org/10.32567/hm.2021.2.13

Kovács László 2021b. Offenzív kiberműveletek II.: Kibererők és képességeik. *Hadmérnök,* 16 (3): 119–137.

https://doi.org/10.32567/hm.2021.3.7

Kovács László 2023. *Hadviselés a 21. században: kiberműveletek*. Ludovika Egyetemi Kiadó, Budapest.

Krasznay Csaba (szerk.) 2023. *Taktikák és stratégiák a kiberhadviselésben*. Budapest: Ludovika Egyetemi Kiadó.

Krasznay Csaba 2022. *Kiberbiztonság a XXI. században*. Budapest: Katonai Nemzetbiztonsági Szolgálat – Nemzeti Közszolgálati Egyetem.

Lewis, James A. 2022. Cyber War and Ukraine. *Center for Strategic and International Studies (CSIS),* June 16, 2022.

Liles, Samuel 2010. Cyber warfare: As a form of low-intensity conflict and insurgency. In Czosseck, Christian – Podins, Karlis (szerk.): *Conference on Cyber Conflict Proceedings 2010.* 47–57.Tallinn, Estonia: Cooperative Cyber Defence Centre of Excellence Publications.

Lupovici, Amir 2011. Cyber Warfare and Deterrence: Trends and Challenges in Research *Military and Strategic Affairs*, 3 (3): 49–62.

Mező András 2021. Multidomén műveletek vezetése és irányítása. *Hadtudomány* 31 (1): 3–21.

https://doi.org/10.17047/HADTUD.2021.31.1.3

MNB 2022. *A magyar pénzügyi szektor kiberfenyegetettségi térképe*. Budapest: Magyar Nemzeti Bank.

Mueller, Grace B., Jensen, Benjamin, Valeriano, Brandon, Maness, Ryan C. , Macias, Jose M. 2023. Cyber Operations during the Russo-Ukrainian War. From Strange Patterns to Alternative Futures. *Center for Strategic and International Studies (CSIS),* July 13, 2023.

NIC 2017. *Assessing Russian Activities and Intentions in Recent US Elections*. Intelligence Community Assessment, Office of Director of National Intelligence. 2017. január 6.

Resperger István 2018. A nemzetbiztonsági szolgálatok tevékenysége – biztonsági kihívások, kockázatok és fenyegetések. In Resperger István (szerk.): *Nemzetbiztonsági alapismeretek*. 29–93. Budapest: Dialóg Campus Kiadó.

Robinson, Michael, Jones, Kevin, Janicke, Helge 2015. Cyber warfare: Issues and challenges. *Computers & Security*, 49 (2015) 70–94.

https://doi.org/10.1016/j.cose.2014.11.007

Terták Elemér, Kovács Levente 2023. Fókuszban a pénzügyi biztonság kibertérben is – PÉNZ7. *Gazdaság és pénzügy*, 10 (1): 5–20.

https://doi.org/10.33926/GP.2023.1.1

Tóth Tamás 2018. A NATO Kibervédelmi Kiválósági Központ bemutatása. *Nemzetbiztonsági Szemle,* 2018/4. 48–62.

White, Sarah P. 2018. Understanding Cyberwarfare: Lessons from the Russia-Georgia War. *Modern War Institute at West Point*. United States Military Academy West Point. 2018. 03. 20.

Wiedemar, Sarah 2023. NATO and Article 5 in Cyberspace. *CSS Analyses in Security Policy* (323.). Center for Security Studies (CSS), ETH Zürich. 2023. május 2.