HADMÉRNÖK
VÉDELEMINFORMATIKA
20. évfolyam (2025) 2. szám 93–111.
DOI: 10.32567/hm.2025.2.6

Krasznay Csaba[1]

Az űr és a kibertér mint műveleti terek konvergenciája az orosz–ukrán háború tükrében[2]

The Convergence of Space and Cyberspace as Operational Domains in the Light of the Russian–Ukrainian War

Absztrakt

A világűr és a kibertér egyre szorosabb összefonódása jelentős kiberbiztonsági kihívásokat eredményez mind az állami, mind a magánszereplők számára. Jelen tanulmány 47 tudományos publikáció szisztematikus elemzésével azonosítja az űrkiberbiztonság fő tematikus klasztereit. A szövegalapú klaszterezés eredményeként hat meghatározó kutatási terület körvonalazódik: 1) kiberbiztonsági irányítás és stratégia; 2) jogi és szabályozási keretek; 3) az űr mint hadszíntér; 4) az orosz–ukrán háború tanulságai; 5) a magánszektor szerepe az űrkiberbiztonságban; valamint 6) technikai kiberfenyegetések és kiberreziliencia. Az elemzés rávilágít arra, hogy míg a nemzetközi kutatások száma növekszik, a témában magyar nyelven még nem jelent meg mélyreható tudományos publikáció. Tekintettel arra, hogy Magyarország és egyes magyar vállalatok deklaráltan rendelkeznek űrtechnológiai ambíciókkal, a jelen téma hazai kutatása indokolt. A tanulmány hozzájárul ennek a hiánynak a pótlásához, valamint rendszerezett áttekintést nyújt az űrkiberbiztonság kutatási trendjeiről és a további vizsgálatokat igénylő területekről.

Kulcsszavak: űrkiberbiztonság, orosz–ukrán háború, kiberműveletek, kiberreziliencia

[1] Egyetemi docens, Nemzeti Közszolgálati Egyetem ÁNTK Kiberbiztonsági és E-közigazgatási Tanszék, e-mail: krasznay.csaba@uni-nke.hu

[2] A tanulmány a Bolyai János Kutatási Ösztöndíj támogatásával készült.

Abstract

The increasing integration of space and cyberspace has led to significant cybersecurity challenges for both governmental and commercial actors. This study systematically analyses 47 academic publications to identify the key thematic clusters in space cybersecurity research. Through text-based clustering, six distinct research domains emerge: (1) cybersecurity governance and strategy, (2) legal and regulatory frameworks, (3) space as a theater of war, (4) cybersecurity lessons from the Russia–Ukraine war, (5) private sector involvement in space cybersecurity, and (6) technical cyber threats and resilience. The analysis highlights that while international research on space cybersecurity is growing, there is a notable absence of Hungarian-language academic publications on this topic. However, given the declared ambitions of Hungary and some Hungarian companies in space technology, domestic research on this topic is justified. The study contributes to bridging this gap by providing a structured overview of space cybersecurity research trends and identifying key areas for future investigations.

Keywords: space cybersecurity, Russia–Ukraine war, cyber operations, cyber resilience

Bevezetés

Az orosz–ukrán háború 2022. február 24-i nyílt fegyveres összecsapását számos kibertéri művelet előzte meg, illetve ezek a támadások azóta is folyamatosan megjelennek mindkét hadviselő fél oldalán. Az offenzív műveletek kiemelt célpontjai az egyes kritikus információs infrastruktúrák, amelyek közül az egyik példa az űrtávközlést megvalósító információs rendszerek, azaz a műholdak és az azokkal kommunikáló földi állomások, legyenek azok akár irányítóközpontok, akár végpontok. Habár az űreszközök kiemelt szerepe a hadviselésben nem újdonság, ez az első olyan háború, ahol az űreszközök biztonsága kiberbiztonsági szempontból kérdőjeleződik meg. A függés pedig kölcsönös, hiszen a harctéren használt informatikai eszközök működése igen gyakran az űrtávközlést megvalósító eszközöktől függ. Ez tehát azt jelenti, hogy a katonai kiberműveleteknek hatása van az űrben levő, katonai célokat is támogató eszközökre, példát mutatva a multidomén-műveletek egy, a magyar nyelvű szakirodalomban kevéssé tárgyalt esetére.

Míg a tengerészeti rendszerek (tehát a tenger mint műveleti tér) és a légi közlekedés (tehát a légtér mint műveleti tér) kiberfüggősége már évek óta vizsgált terület, az űr és a kibertér műveleti tér konvergenciájára aránylag kevés figyelmet fordítottak eddig a kutatók és a műveleti tervezők. Kutatási kérdésem, hogy a hadtudományban mérvadó szakirodalom milyen összefüggéseket állapított meg a két műveleti térrel kapcsolatban, mi a jelenlegi *state-of-the-art* ezen a területen az orosz–ukrán háború tapasztalatai alapján. Hipotézisem szerint a háborús tapasztalatok olyan új impulzusokat adtak a tudományos diskurzusnak, amelyek következtében új, jól körülhatárolható, korábban nem, vagy csak kevéssé kutatott tudományos tématerületek jöttek létre. Kutatásom során tudományos módszertanként szakirodalmi kutatást végzek, amelynek során feltárom a releváns tanulmányokat, és azok klaszterelemzésével támasztom alá a hipotézisemet.

Esettanulmányok az orosz–ukrán háborúból

Az űr és a kibertér konvergenciájának fontossága három jól dokumentált esettanulmányon keresztül mutatható be az orosz–ukrán háború kapcsán. Ezek a ViaSat műholdas szolgáltató elleni támadás, a Starlink műholdas távközlési rendszer felhasználása az ukrán védelmi műveletek során, illetve a GPS-jelek zavarása nemcsak a műveleti területen, hanem a Baltikum jelentős részén is.

A ViaSat szolgáltató elleni kibertámadást 2022. február 24-én, közvetlenül az orosz–ukrán háború kezdete előtt hajtották végre. A kiberművelet következtében jelentős hálózati kiesés történt, amely az ukrán katonai kommunikációt is érintette. A támadás célpontja a KA-SAT műholdhálózat földi szegmense volt, amelyet a támadók kompromittáltak. Az incidens több ezer, nem csak katonai védelmi rendszerben használt végfelhasználói modemet érintett, amelyek a támadás következtében használhatatlanná váltak. Az Európai Űrügynökség és az amerikai hírszerző ügynökségek vizsgálatai megállapították, hogy a támadás egy előre megtervezett kiberművelet része volt, amelyet az orosz összhaderőnemi támadás részeként kell értelmezni.

A támadás technikai aspektusait vizsgálva kiderült, hogy egy úgynevezett *wiper,* azaz adattörlő típusú rosszindulatú szoftvert használtak, amely a KA-SAT modemek memóriáját törölte, így azok újraindítás után sem tudtak csatlakozni a hálózathoz. A támadók a földi hálózati infrastruktúrát kompromittálták, és egy frissítési csatornán keresztül terjesztették a kártékony szoftvert. A támadás során nem közvetlenül a műholdakat vették célba, hanem azokat az eszközöket, amelyek a felhasználók és a műholdak közötti kapcsolatot biztosították.[3]

A támadás elsődleges tanulsága az volt, hogy noha közismert tény, hogy a műholdas kommunikáció kulcsfontosságú infrastruktúra, amely sérülékeny lehet kibertámadásokkal szemben, különösen katonai konfliktusok esetén, a szolgáltatók nem rendelkeznek megfelelő kibervédelemmel. Az incidens egyben rávilágított a műholdas rendszerek biztonságának és a beszállítói lánc védelmének fontosságára, rámutatva, hogy a saját űrképességekkel nem rendelkező országok mennyire kitettek a polgári űrtávközlésnek. A támadás után több szervezet, köztük a NATO, az EU és az amerikai kormány, fokozta a műholdas kommunikáció biztonságára vonatkozó intézkedéseit, hogy csökkentse a jövőbeni hasonló fenyegetések kockázatát, ezek megvalósítása azonban több évet vesz igénybe.

A ViaSat-támadás után a Starlink műholdas internetrendszere kulcsszerepet játszott az ukrajnai háborúban, amikor 2022 februárjában, az orosz invázió kezdetén az ukrán kormány sürgős segítséget kért a kommunikációs infrastruktúra fenntartására. Elon Musk vállalata, a SpaceX rövid időn belül több ezer Starlink-terminált biztosított Ukrajna számára, lehetővé téve az ország katonai, kormányzati és civil szervezetei számára a folyamatos internet-hozzáférést. Az első egységek néhány napon belül megérkeztek, és a hálózat gyors telepítésével az ukrán hadsereg sikeresen fenntartotta a műveleti kommunikációt, miközben az orosz csapatok megsemmisítették vagy zavarták a hagyományos telekommunikációs infrastruktúrát.

[3] Boschetti–Gordon–Falco 2022.

A Starlink rendszere különösen a harctéren bizonyult nélkülözhetetlennek, mivel biztosította a drónműveletek vezérlését, a titkosított katonai kommunikációt és az ukrán erők koordinációját. A rendszer egyik előnye a hagyományos infrastruktúrával szemben az volt, hogy decentralizált és nehezebben támadható. Habár az orosz hadsereg több alkalommal is megpróbálta zavarni a Starlink műholdjeleit és kibertámadásokat indított a földi terminálok ellen, a SpaceX folyamatos frissítésekkel gyorsan reagált a fenyegetésekre. 2022 májusára több mint 10 000 Starlink-egységet használtak Ukrajnában, és ez a szám tovább növekedett a háború során.[4]

A Starlink katonai alkalmazása geopolitikai kérdéseket is felvetett, mivel egy magánvállalat közvetlen hatással volt egy háborús konfliktus menetére. 2023-ban Elon Musk elismerte, hogy a SpaceX korlátozott hozzáférést vezetett be a Starlink használatára bizonyos hadműveleteknél, például a Krím közelében végrehajtott támadások során. Ez rávilágított arra, hogy a kritikus kommunikációs infrastruktúra egy magánvállalat kezében stratégiai döntéseket befolyásolhat. Az ukrajnai eset tanulságai alapján egyre nagyobb figyelem irányul arra, hogy a modern hadviselésben milyen szerepet játszanak a magántulajdonban lévő technológiák, és milyen szabályozásokra lehet szükség a jövőben.

A GPS-jelek zavarása rendszeres problémává vált konfliktuszónákban, különösen az orosz–ukrán háborúban. Orosz egységek különböző elektronikai hadviselési eszközökkel bocsátanak ki elektromágneses impulzusokat, amelyek rontják a GPS-jel minőségét. Noha a GPS-alapú amerikai katonai műveletekre ez nem gyakorolt jelentős hatást, az Egyesült Államok dollármilliókat költött arra, hogy megvédje kommunikációs infrastruktúráját az orosz kibertámadásokkal és GPS-zavarásokkal szemben.

A GPS-alapú ukrán drónműveletek szintén kevéssé érintettek, mivel ezek képesek olyan területeken támadni, ahol nincsenek aktív orosz földi zavaróeszközök, illetve egyre jobban elterjednek a mesterséges intelligencia által vezérelt autonóm csapások, valamint sok esetben optikai szállal vezetik a drónokat. Az ukrán erők emellett a Starlink műholdrendszeren keresztül hatékonyan kommunikálnak és koordinálják csapásaikat. Ezzel szemben a polgári GPS-jelek zavara különösen nagy hatással érinti a légi közlekedést, és már előfordult, hogy repülőgépeket más repülőtérre kellett átirányítani, mert nem tudták biztonságosan végrehajtani a leszállást. Az Európai Repülésbiztonsági Ügynökség (EASA) 2022. március 17-én figyelmeztetést adott ki a műholdas navigációs zavarok miatt, és négy érintett régiót azonosított: Kalinyingrád, Kelet-Finnország, a Fekete-tenger és Észak-Irak.

A GPS-zavarás a régióban nem új jelenség, Oroszország már a 2014-es krími konfliktus óta alkalmazza ezt a taktikát, különösen kelet-ukrajnai területeken. 2017-ben a Fekete-tengeren 20 hajó fedélzeti rendszere mutatott hamis helyzetadatokat, és egy 2016 óta végzett elemzés szerint több mint 9800 esetben manipulálták a jeleket, érintve 1300 kereskedelmi hajót. Az ilyen beavatkozások nemcsak katonai műveleteket, hanem kereskedelmi és humanitárius feladatokat, például kutató-mentő műveleteket is akadályozhatnak. Az Egyesült Államok és

[4] Abels 2024.

az Európai Unió egyaránt aggódik a GPS-alapú rendszerek biztonsága miatt, különösen a Galileo rendszer 2019-es részleges leállása óta, ami rávilágított a műholdas infrastruktúra védelmének fontosságára.[5]

Szakirodalmi áttekintés és klaszterelemzés

A kiberbiztonság és az űrtevékenységek metszéspontja egyre nagyobb figyelmet kap a szakirodalomban. Annak érdekében, hogy látható legyen, milyen módon reagált a tudományos közösség az orosz–ukrán háború tapasztalataira, tematikus irodalomkutatást végeztem. Ennek során a célom az volt, hogy a mérvadó tudományos forrásokból felleljem a 2022 és 2025 közötti azon publikációkat, amelyek ezzel a témával foglalkoznak. Kulcsszavas keresés segítségével ezért átnéztem a Magyar Tudományos Művek Tárát, a Google Scholart, a ResearchGate-et, valamint a Nemzeti Közszolgálati Egyetem által előfizetett tudományos adatbázisok közül az IEEE, a Sage, a Scopus, a Springer és a Taylor & Francis listáit. Az adatbázisok kiválasztása során arra törekedtem, hogy a lehető legteljesebb merítést tudjam végezni az esetleges publikációk területén, így nagyobb listából szűrhettem le a mértékadó publikációkat. Ezek mellett az olyan mérvadó tudományos műhelyek kiadványait is átnéztem, mint a NATO Cooperative Cyber Defence Center of Excellence és az ETH Zürich. Keresőszavaim rendre a *cybersecurity, space, Ukraine-Russia, war, satellite* keresőszavak voltak. Emellett áttekintettem a fellelt források hivatkozási listáit is, bízva abban, hogy ezzel újabb, a kritériumoknak megfelelő szakirodalmat találok. A kiválasztás során minden esetben elolvastam az absztraktokat is, így ki tudtam zárni azokat a cikkeket, amelyek ugyan a keresőszavaknak megfeleltek, de tartalmukat tekintve nem voltak relevánsak. A kiterjedt keresés eredményeképp 47 releváns forrást találtam, amelyek teljesítik a tudományos publikációkkal kapcsolatos kritériumokat, tehát nem sajtóhírek vagy piaci cégek publikációi, valamint a kibertér és az űr konvergenciájának biztonsági vetületeiről szólnak. Elfogadtam viszont azokat a kiadványokat, amelyeket tudományos műhelyek, jellemzően egyetemek adtak ki jelentés formájában. A kiválasztott szakcikkek szerzői körét érdekes módon nem lehet klaszterezni, sem affiliációban, sem földrajzi értelemben nincsen meghatározó köre azoknak, akik a témában publikálnak. Ez is mutatja, hogy a választott téma egyelőre inkább csak partikuláris érdeklődésre tart számot.

A forrásokat ezután mélyelemzésnek vetettem alá, amelynek célja az volt, hogy tematikus klaszterelemzéssel feltárjam a megadott 47 publikáció főbb témacsoportjait a teljes szövegük alapján. A dokumentumklaszterezés lényege, hogy a hasonló tartalmú szövegeket közös csoportba rendezzük, így megkönnyítve a rejtett témák és mintázatok azonosítását. Ennek érdekében NLP-alapú szöveganalízist és gépi tanulási módszereket alkalmaztam a szövegek feldolgozására és a klaszterek kialakítására. Az optimális klaszterszámot előzetes elemzések alapján 5-6-ra becsültem, és végül hat tematikus klasztert azonosítottam. A tematikus klaszterelemzéshez mesterségesintelligencia-alapú megközelítést alkalmaztam, a ChatGPT mélyelemzés funkciójának

[5] Kolovos 2022.

segítségével azonosítva a fő témákat és strukturálva a besorolási folyamatot. Az NLP-alapú szövegelemzés lehetővé tette a dokumentumok tartalmi csoportosítását a TF–IDF vektorizáció és a *k-means* klaszterezési algoritmus alkalmazásával. Az alábbiakban részletesen bemutatom a klaszterezés módszertanát, majd ismertetem a kapott klasztereket azok főbb témái, jellemzői és egymáshoz fűződő szemantikai kapcsolatai szerint. Ennek az eszköznek a megbízhatóságát számos tanulmány vizsgálja,[6] amelyek alapján a ChatGPT megfelelő a feladat elvégzéséhez, de mint minden esetben, szakértői validációra van szükség. Ezt jelen esetben úgy tettem meg, hogy az alkalmazott elemzési módszereket részletesen dokumentáltattam a mesterséges intelligenciával, a kapott eredményeket pedig manuálisan visszaellenőriztem, azaz a cikkek teljes szövegének ismeretében meggyőződtem a klaszterezés megfelelőségéről.

Kutatási módszertan

Első lépésben a korábban említettek szerint elvégeztem az adatgyűjtést és előkészítettem a publikációkat a további vizsgálatra. A vizsgálatban szereplő 47 publikáció 2022–2025 között jelent meg, és mind az űr (világűr) és a kibertér metszetében felmerülő biztonsági kérdésekkel foglalkozik. A klaszterelemzéshez a cikkek teljes szövegét (vagy elérhetőség hiányában absztraktját és címét) használtam fel. A szövegeket az algoritmus előfeldolgozta: eltávolította a felesleges írásjeleket, *stopword*öket és normalizálta a szavakat (kisbetűs alakra hozva, szükség esetén szótövekre csonkolva). E lépések célja a nyelvtani alakulatok egységesítése és a zaj csökkentése, hogy a klaszterező algoritmus a tartalmi hasonlóságokra koncentrálhasson.

Második lépésben történt a szövegvektorizáció. Az előkészített dokumentumokat az algoritmus numerikus vektorként reprezentálta a tartalmuk alapján. Ehhez az elemzés TF–IDF *(Term Frequency – Inverse Document Frequency)* módszert alkalmazott, amely minden dokumentumhoz egy egyedi szóvektort rendel. A vektor elemei a szavak fontosságát tükrözik: magasabb érték jelzi, hogy az adott kifejezés gyakori az adott szövegben, de ritkább az összes dokumentum között, így jól jellemzi a tartalmat. Ez a megközelítés segít kiemelni az egyes cikkekre jellemző kulcsszavakat, és mérsékli az általános jelentésű szavak hatását. Alternatív megoldásként szóbeágyazási *(embedding)* technikák is szóba jöhetnek a szemantikai hasonlóság jobb megragadására – például egy pretrénelt nyelvi modell segítségével –, de a TF–IDF-alapú megközelítés is bevált a tematikus különbségek feltárására.

A harmadik lépés a klaszterező algoritmus futtatása volt. A dokumentumvektorok alapján az algoritmus *k-means* algoritmussal csoportosította a cikkeket. A *k-means* egy gyakran használt partícionáló klaszterezési eljárás, amelynek lényege, hogy előre meghatározott k klaszterközéppont köré rendezi a pontokat iteratív módon. Az algoritmus addig finomítja a klasztereket, amíg a dokumentumok a legközelebbi középpontjukhoz tartoznak. A *k-means* hatékony és jól skálázható módszer, amely elegendő információt ad a témák szétválasztásához. Emellett kísérletképpen az algoritmus a hierarchikus klaszterezést is megvizsgálta, amely fastruktúrát eredményez a dokumentumok között – ez részletesebb betekintést nyújthat a klaszterek alstruktúráiba, viszont nagyobb számítási igényű. Jelen elemzésben a *k-means* eredményeit

[6] Lásd például Natarajan–Verma–Kumar 2025.

használtam fel, mivel ezek jól értelmezhető, elkülönülő témacsoportokat adtak. Minden cikket egyetlen klaszterbe soroltam *(hard clustering),* így a klaszterek nem fedik át egymást, hanem diszjunkt tématerületeket reprezentálnak.

Ezután következett a klaszterszám meghatározása. Az optimális klaszterszámot több szempont figyelembevételével 5 és 6 közé állítottam be. Egyrészt a szakirodalmi témák ismeretében feltételeztem, hogy nagyjából öt-hat jól elkülöníthető tematikus csoport jelenhet meg (például jogi kérdések, katonai vonatkozások, technikai fenyegetések stb.). Másrészt kvantitatív módon is megvizsgáltam több klaszterszám mellett a modell kimenetét – például a sziluettmutató értékét –, illetve a klaszterek értelmezhetőségét. Az 5-6 klaszter közötti tartományban kaptam a legkoherensebb eredményeket. Végül a hatklaszteres megoldás bizonyult a legjobban értelmezhetőnek: ebben az esetben egyik klaszter sem volt túl kicsi vagy tartalmilag heterogén, és a csoportok jól leírható, összetartozó témákat fedtek le. Az alábbiakban a hat azonosított klasztert ismertetem, megnevezve fő témájukat és jellemzőiket. Ezen túl kitérek arra is, milyen szemantikai kapcsolatok fedezhetők fel a klaszterek között.

Eredmények: klaszterek és főbb témák

Az elemzés tehát hat tematikus klasztert eredményezett, amelyek az alábbi fő témakörökbe csoportosítják a publikációkat. Minden klaszternél megadom a jellemző tartalmi fókuszt, néhány kulcskifejezést és példaként egy-két idetartozó publikációt. Fontos megjegyezni, hogy noha a klaszterek különálló csoportokat alkotnak, közöttük vannak átfedések és kapcsolódási pontok is – ezeket a későbbiekben részletezem.

1. klaszter: Kiberbiztonsági irányítás (governance) és stratégia az űrben

Az első klaszter az űrbeli kiberbiztonság szabályozási, irányítási és stratégiai kérdéseire fókuszál. Idetartoznak azok a munkák, amelyek átfogóan tárgyalják, hogyan lehet biztosítani a kibertér biztonságát a világűrben, illetve milyen globális együttműködésre és szabványokra van szükség. Gyakoriak a *regulatory framework, governance, strategy* jellegű kulcsszavak, ami jelzi, hogy ez a klaszter a szabályozási kihívásokkal és megoldásokkal foglalkozik.

A publikációk ebben a klaszterben rendszerint rámutatnak, hogy az űr és a kibertér szorosan összefonódó globális közeg, amelyre egységes stratégiákat kell kidolgozni. Kiemelik a nemzetközi összefogás és terminológiai összehangolás fontosságát egy hatékony kiberbiztonsági szabvány vagy politika megalkotásához. Több munka hangsúlyozza a *final frontier* jellegű gondolatot, miszerint az űr a kibertér új határterülete, ahol a kihívások kezelése proaktív szabályozást igényel.

E klaszterbe tartozik például *Drafting a Cybersecurity Standard for Outer Space Missions: On Critical Infrastructure, China, and the Indispensability of a Global Inclusive Approach*[7] című cikk, amely egy globális, inkluzív kiberbiztonsági szabvány

[7] Segate 2024.

kidolgozásának szükségességét taglalja az űrmissziók számára. Szintén idesorolható az *Understanding Cybersecurity in Outer Space*[8] című publikáció, amely az alapvető kihívásokat és stratégiai megfontolásokat tekinti át az űrbéli kiberbiztonság területén. Ezen munkák közös nevezője, hogy átfogó képet adnak a kiberbiztonsági irányításról és stratégiai keretekről az űrtevékenységek kapcsán.

2. klaszter: Jogi és szabályozási keretek az űrkiberbiztonságban

A második klaszter középpontjában az űrtevékenységek kiberbiztonságának jogi vonatkozásai állnak. Idesoroltam azokat a publikációkat, amelyek nemzetközi és nemzeti jogi kereteket, szabályozásokat, illetve politikai irányelveket vizsgálnak a kibertér és a világűr metszetében. A klaszterre jellemző kulcsszavak: *international law, legal framework, policy, orbit,* utalva arra, hogy gyakran szó esik az űrszabályozás nemzetközi jogi aspektusairól és az orbitális rendszerek védelméről.

E klaszter publikációi részletesen elemzik, hogyan alkalmazhatók a meglévő nemzetközi jogszabályok (például az űrjog és a kiberhadviselés joganyaga) az olyan új kihívásokra, mint a műholdak elleni kibertámadások. Több tanulmány foglalkozik a jogi hézagokkal és dilemmákkal is – például hogy miként lehet felelősségre vonni egy államot vagy nem állami szereplőt egy műhold meghekkeléséért, illetve milyen önvédelemi lehetőségek (például *self-defence*) adottak egy kibertámadás esetén az űrben. Emellett felmerül a nemzeti szintű szabályozás kérdése is, például az EU és az USA eltérő megközelítéseinek összehasonlítása a műholdak kiberbiztonsági előírásaiban.

Ebbe a klaszterbe tartozik például a *Law in Orbit: International Legal Perspectives on Cyberattacks Targeting Space Systems*[9] című tanulmány, amely az űrrendszerek elleni kibertámadások nemzetközi jogi értelmezését tárgyalja. Szintén idesorolható a *Developing a Cybersecurity Policy for Low Earth Orbit Satellite Broadband – an International Law Perspective,*[10] amely az alacsony Föld körüli pályán működő műholdhálózatok (például műholdas internet) kiberbiztonsági szabályozását vizsgálja nemzetközi jogi szempontból. Továbbá az *Anti-Satellite Weapons and Self-Defence: Law and Limitations*[11] című munka is, amely a műholdak elleni fegyverek és a jogos önvédelem kérdését feszegeti. E klaszter minden munkája a szabályozási kihívások és jogértelmezések kérdéseit boncolgatja, biztosítandó az űrbeli rendszerek kiberbiztonságát.

3. klaszter: Az űr mint hadszíntér – kiberveszélyek és hadműveleti dimenzió

A harmadik klaszterbe azok a publikációk kerültek, amelyek az űr mint műveleti terület szerepét és az ott megjelenő kiberveszélyeket tárgyalják általános, nem egy konkrét konfliktusra korlátozódó módon. Idetartoznak a *warfighting domain, space warfare, threats in space* témájú munkák, amelyek azt vizsgálják, hogyan válik a világűr

[8] Poirier 2024a.
[9] Bace–Gökce–Tatar 2024.
[10] Kulesza – Akcali Gur 2023.
[11] O'meara 2024.

a hagyományos szárazföldi, tengeri, lég- és kibertér mellett a hadviselés egy új dimenziójává. A klaszter kulcsszavai közé tartozik a *domain* (domén vagy hadszíntér), *warfare, threats* és *security challenges.*

A klaszter publikációi arra mutatnak rá, hogy az űrbéli infrastruktúrák (műholdak, űreszközök) elleni kibertámadások és zavaró tevékenységek (például zavarás, APT-támadás) katonai szempontból stratégiai jelentőségűvé válnak. Több tanulmány foglalkozik a koncepcionális kérdésekkel, például hogy az űr- és kibertartomány mennyiben olvad össze *(space-cyber nexus),* és hogyan lehet kormányozni vagy szabályozni ezt az új hadszínteret. Idesorolhatók olyan munkák, amelyek a hatodik hadviselési domén gondolatát vetik fel – utalva arra, hogy a kibertér után az űr lehet a következő hadszíntér, vagy épp a kettő kombinációja. Emellett a klaszterbe tartozó cikkek érintik a fenyegetések típusait is (például *malicious cyber activities against space assets*) és ezek kezelésének elvi kérdéseit.

Ebben a klaszterben található az *On the Threshold of Space Warfare*[12] című publikáció, amely az űrháború küszöbén álló technológiai és stratégiai változásokat tekinti át. Szintén idesorolható a *The Sixth Warfighting Domain? Governing The Space-Cyber Nexus*[13] is, amely azt vizsgálja, miként lehet irányítani és szabályozni az űr-kiberhadműveleti területet. További példa a *Security Challenges When Space Merges with Cyberspace*[14] című cikk, amely a kibertér és a világűr összefonódásából eredő biztonsági kihívásokat térképezi fel. Összességében e klaszter anyagai az űrhadviselés általános elméleti és fenyegetésbeli aspektusait járják körül, megalapozva a konkrét konfliktusokra vonatkozó elemzéseket.

4. *klaszter: Az orosz–ukrán háború tanulságai és esetei az űr-kiberhadviselés*ben

A negyedik klaszter kifejezetten az orosz–ukrán háborúval és annak űrbeli kiberbiztonsági vonatkozásaival foglalkozik. Ez a klaszter gyűjti össze azokat a publikációkat, amelyek az Ukrajnában 2022-ben kirobbant háború során szerzett tapasztalatokat elemzik, különös tekintettel a műholdak és az űrinfrastruktúra szerepére, valamint a konfliktusban alkalmazott vagy észlelt kibertámadásokra. A klaszter leggyakoribb kulcsszavai: *War in Ukraine, Russian-Ukrainian conflict, military operations, space assets, satellites.* Ezek jól mutatják, hogy a csoport témája a valós háborús esetek és tapasztalatok feldolgozása.

Az idesorolt tanulmányok részletesen dokumentálják, hogyan jelentek meg a kibertérbeli műveletek a fizikai konfliktus részeként. Több publikáció hangsúlyozza, hogy az orosz–ukrán konfliktus volt az első, ahol a kereskedelmi műholdak (például Starlink) és a hozzájuk kapcsolódó kibervonatkozások kiemelt szerepet kaptak – egyesek „az első kereskedelmi űrháborúként" is hivatkoznak rá. E klaszter munkái sorra veszik a háború során tapasztalt kibertámadásokat, például a ViaSat műholdhálózat elleni támadást a konfliktus kezdetén, illetve azt, miként használták az űralapú

[12] Pražák 2022.
[13] Tepper et al. 2023.
[14] Varadharajan–Suri 2024.

szolgáltatásokat (navigáció, kommunikáció, felderítés) a harcoló felek. A tanulmányok elemeznek konkrét incidenseket és azok hatását a hadműveletekre, valamint levonják a stratégiai tanulságokat arról, hogyan kell felkészülni hasonló jövőbeni konfliktusokra.

Ebbe a klaszterbe tartozik a *Hacking the Cosmos: Cyber Operations Against the Space Sector – A Case Study From the War in Ukraine*[15] című tanulmány, amely konkrét esettanulmányként mutatja be, hogyan támadták meg a háború során az űrszektort (ilyen volt például a ViaSat műholdas hálózat elleni kibertámadás). Idesorolható a *The Space Domain and the Russia-Ukraine War*[16] is, amely átfogóan elemzi, hogyan vált a világűr a háború egyik hadszínterévé, és milyen műveletek történtek ebben a doménben. További példa a *Starlink's Role in Ukraine: Portent of a Space War?*[17] című publikáció, amely kifejezetten a Starlink műholdas internet szerepét vizsgálja a konfliktusban, felvetve, hogy ez előrevetíti-e az űrháborúk új korszakát. Ezek a publikációk mind az orosz–ukrán háború tapasztalatait dolgozzák fel, rávilágítva arra, hogy a modern fegyveres konfliktusokban az űrbéli kiberfaktor immár megkerülhetetlen.

5. klaszter: Kereskedelmi és magánszereplők a digitális hadszíntéren

Az ötödik klaszter az űrbeli kiberbiztonság kereskedelmi és civil vonatkozásait emeli ki, különös tekintettel a magánszektor szereplőire (például kereskedelmi műhold-üzemeltetők) és a „digitális hadszíntér" koncepciójára. A klaszter kulcsszavai – mint *commercial, operators, digital battlefield, lessons learned* – arra utalnak, hogy ezek a munkák azt vizsgálják, miként vonódnak be a nem állami szereplők (vállalatok, magán-infrastruktúrák) a konfliktusokba, és milyen tanulságok adódnak ebből.

A publikációk rámutatnak, hogy napjaink fegyveres konfliktusaiban a magántulajdonú űreszközök és rendszerek (például kereskedelmi, távközlési vagy földmegfigyelő műholdak) is célpontokká, illetve stratégiai erőforrásokká válnak. Ez új kihívásokat hoz a nemzetbiztonság és a kibervédelem terén, hiszen a hadviselés immár kiterjed a kereskedelmi szolgáltatók hálózataira is. Több tanulmány ebben a klaszterben azt emeli ki, hogy a magánszektor bevonása miatt a hadszíntér „digitalizálódik", azaz az információs infrastruktúrák és a kibertámadások ugyanolyan fontossá váltak, mint a hagyományos fegyverek. Emellett szó esik a konfliktusokból levonható technikai és szervezeti tanulságokról is *(lessons learned),* amelyek segíthetnek a jövőbeni együttműködésben az állami és magánszereplők között.

A *Commercial Space Operators on the Digital Battlefield*[18] című tanulmány ebben a klaszterben azt vizsgálja, hogyan válnak a kereskedelmi űrcégek (például műholdas kommunikációt nyújtó vállalatok) a modern háborúk digitális hadszínterének részévé. Hasonló témát érint a *Russian-Ukraine Armed Conflict: Lessons Learned on the Digital Ecosystem,*[19] amely az orosz–ukrán háború kapcsán szerzett tapasztalatokat elemzi a digitális infrastruktúrák (beleértve a magánhálózatokat) vonatkozásában. Habár

[15] Poirier 2024b.
[16] Peperkamp–Bolder 2024.
[17] Ray–Selvamurthy 2023.
[18] Cesari 2023.
[19] Aviv–Ferri 2023.

tartalmilag átfedés van az előző klaszterrel a háborús kontextus miatt, ezek a művek kifejezetten a civil szféra és a katonai műveletek összefonódására koncentrálnak. Kiemelendő továbbá a *Cyber Orbits: The Digital Revolution of Space Security*[20] című cikk, amely átfogóbban tekint a digitális átalakulásra az űrbiztonság terén – ideértve a kereskedelmi és védelmi szféra kapcsolatát is. Ez a klaszter tehát rámutat a köz- és magánszféra közötti együttműködés szükségességére az űrkiberbiztonság területén.

6. klaszter: Technikai kiberfenyegetések és rendszerszintű ellenálló képesség

A hatodik klaszter központi témája az űrrendszerek elleni kiberfenyegetések technikai jellege és az ezekkel szembeni kibervédelmi mechanizmusok, reziliencia. Idesorolhatók azok a tanulmányok, amelyek konkrét technikai sebezhetőségeket, támadási módszereket, valamint a védekezés műszaki és szervezeti aspektusait taglalják. A klaszter kulcsszavai: *cyber attacks, critical infrastructure, resilience, communications, defence.* Ezek jelzik, hogy a csoport középpontjában a kritikus űrinfrastruktúrák (például műhold-kommunikációs rendszerek) védelme és a kibertámadások kezelése áll.

Az ebbe a klaszterbe tartozó publikációk részletesen bemutatják a fenyegetési képet: milyen jellegű kibertámadások érhetik az űreszközöket (például zavarás, adatlopás, szolgáltatásmegtagadás), és ezek milyen hatással lehetnek a rendszer működésére és a földi szolgáltatásokra. Több tanulmány foglalkozik a kiberreziliencia fogalmával, vagyis hogy az űrrendszerek tervezésénél és üzemeltetésénél miként lehet biztosítani a támadásokkal szembeni ellenálló képességet és a gyors helyreállítást. Idetartoznak továbbá olyan átfogó elemzések, amelyek rendszerszinten vizsgálják a sebezhetőségeket és a védekezési stratégiákat – például egyes munkák szakirodalmi felmérést nyújtanak az űrkiberbiztonság témájában, rávilágítva a technikai kihívásokra és a jelenlegi felkészültségi szintre. Emellett felmerül az interdiszciplináris megközelítés igénye: a műszaki megoldások mellett a stratégiai és szabályozási szempontok figyelembevétele is szükséges a hatékony védelemhez (ezt jelzi, hogy például egyes klaszterbeli dokumentumok az ESPI-jelentés[21] keretében tárgyalják a *space-cyberdefence* kihívásokat).

Példaként említhető a *Cyber Resilience Limitations in Space Systems Design Process: Insights from Space Designers*[22] című publikáció, amely űripari szakemberek bevonásával elemzi, hol vannak a tervezési folyamatban gyenge pontok a kiberreziliencia szempontjából. További idesorolható munka a *Cyber Attacks on Critical Infrastructures and Satellite Communications*[23] című elemzés, amely konkrétan a műholdas kommunikációs infrastruktúrák elleni támadások típusait és az azok elleni védekezés lehetőségeit tekinti át. Szintén érdekes az *ESPI Report – Space, Cyber and Defence: Navigating Interdisciplinary Challenges,* a már említett kiadvány, amely európai szemszögből, interdiszciplinárisan vizsgálja az űrkiberbiztonságot, beleértve a technikai és védelmi dimenziókat is. E klaszter tehát a technológiai kihívásokra és a védelmi válaszokra helyezi a hangsúlyt az űrkiberbiztonság területén.

[20] Botezatu–Vevera 2024.
[21] European Space Policy Institute 2023.
[22] Shahzad et al. 2024.
[23] Carlo–Obergfaell 2024.

Szemantikai kapcsolatok a klaszterek között

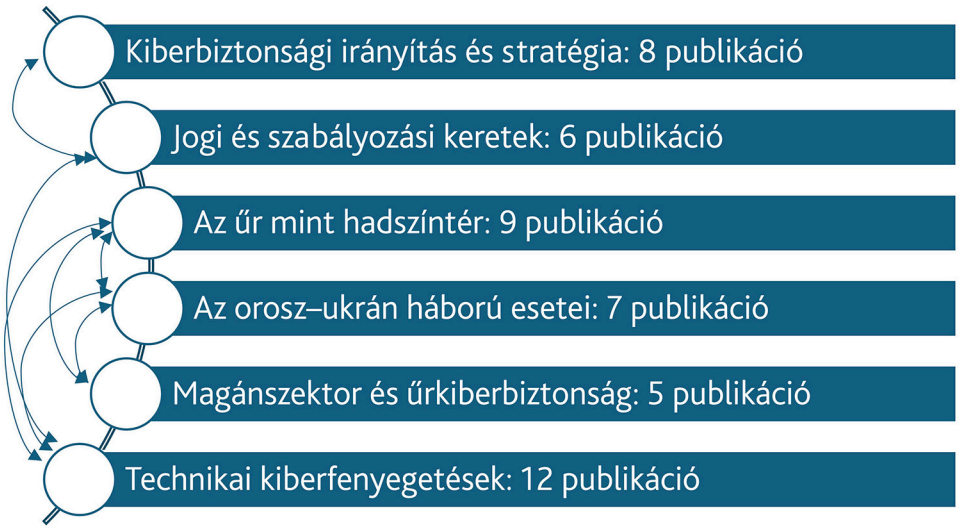
A már említett klaszterek jól elkülöníthető témaköröket jelölnek, ugyanakkor nem függetlenek teljesen egymástól (1. ábra). Figyelemre méltó, hogy több klaszter is a fegyveres konfliktusok köré szerveződik (különösen a 3., 4. és 5. klaszter), jelezve, hogy a katonai vonatkozás az űrkiberbiztonsági szakirodalomban kiemelt szerepet kap, nem függetlenül az orosz–ukrán háború tapasztalataitól. Ez a megállapítás egyben alátámasztja a hipotézisemet, és igazolja, hogy ezek a klaszterek új irányokat mutatnak a tudományos diskurzusban. A 3. klaszter az elméleti keretet adja meg ahhoz, hogy az űrt mint hadszínteret kezeljük, míg a 4. klaszter ennek a gyakorlati megnyilvánulását mutatja be az orosz–ukrán háború példáján. Az 5. klaszter ehhez kapcsolódva a konfliktusok egy speciális aspektusára, a magánszektor bevonására fókuszál, így szorosan kapcsolódik a 4. klaszterhez (hiszen az ukrán háborúban vizsgálja a Starlink és egyéb kereskedelmi infrastruktúrák szerepét). Valójában több publikáció is említhető lenne egyszerre a 4. és az 5. klaszterben – például a Starlinkről szóló tanulmány joggal illeszkedik a háborús és a kereskedelmi témájú klaszterbe is. Jelen tanulmányban azonban minden művet a fő fókusza alapján soroltam be egy klaszterbe.

Hasonló átfedés figyelhető meg a jogi-politikai (2. klaszter) és a stratégiai-irányítási (1. klaszter) témák között. Mindkettő a szabályozás és az irányítás kérdéskörével foglalkozik, csak eltérő szinten: az 1. klaszter általános stratégiai víziókat és koordinációs igényt fogalmaz meg, míg a 2. klaszter konkrét jogi kereteket és normákat elemez. E két klaszter együtt ad átfogó képet a kiberbiztonsági *governance*-ről: az egyik inkább politikai-stratégiai, a másik jogi végrehajtási nézőpontból. A közöttük lévő szemantikai kapcsolat abban rejlik, hogy a hatékony kiberbiztonsági stratégia kidolgozása (1. klaszter témája) megköveteli a megfelelő jogi háttér meglétét (2. klaszter témája), és *vice versa:* a jogi szabályozásnak igazodnia kell a stratégiai realitásokhoz. Ez a két kutatási területe semmiképpen sem nevezhető újdonságnak, több évtizedre visszamenő múltja van a témába vágó publikációknak. Az orosz–ukrán háború azonban olyan gyakorlati esettanulmány, amely miatt ennek a két klaszternek a finomhangolása szükséges.

A technikai kihívások klasztere (6. klaszter) szintén kapcsolódik a többiekhez, hiszen a műszaki sebezhetőségek és támadások ismerete alapozza meg mind a szabályozási/jogi válaszlépéseket, mind a katonai stratégiát. Például a 6. klaszterben tárgyalt sérülékenységek és védelmi mechanizmusok jelentik azt a valóságot, amelyre a 3. klaszterben vázolt hadműveleti stratégiáknak reagálniuk kell, és amelyeket a 2. klaszter jogi keretei szerint kell kezelni (például felelősség, nemzetközi együttműködés kérdése). Ugyanez igaz fordítva is: a 4. klaszter háborús esettanulmányai rávilágítanak olyan konkrét technikai problémákra (mint a ViaSat-incidens), amelyek a 6. klaszter általános technikai témái közé illeszkednek. A technikai aspektus vizsgálata szintén nem újdonság, azonban a konkrét támadások tapasztalatai alapján a műszaki védelem irányai tovább finomíthatók.

Összességében a klaszterek között erős szemantikai összefüggésrendszer bontakozik ki, ami természetes egy ilyen interdiszciplináris területen. Az űrkiberbiztonság témaköre komplex: magában foglalja a nemzetközi jogot és politikát, a katonai stratégiát, a technológiát és a gazdasági-kereskedelmi aspektusokat is. A klaszterelemzés eredményei azt tükrözik, hogy a szakirodalom fő áramlatai is e dimenziók mentén szerveződnek,

ugyanakkor együtt alkotnak egy koherens egészet. A külön klaszterekbe rendezett témák valójában egymásra épülnek és egymást kiegészítik: a háborús tapasztalatok informálják a jövőbeli szabályozást és technikai fejlesztéseket; a jogi keretek meghatározzák a katonai és kereskedelmi szereplők mozgásterét; a technikai újítások pedig új kihívásokat teremtenek a stratégák és a jogalkotók számára.



1. ábra: A megvizsgált publikációk száma klaszterenként és a klaszterek közötti szemantikai kapcsolat
Forrás: a szerző szerkesztése

Következtetések

A 47 publikáció tematikus klaszterelemzése révén öt-hat markáns tématerületet sikerült azonosítani az űrkiberbiztonság diskurzusában. Jelen esetben hat klaszter körvonalazódott: 1) kiberbiztonsági kormányzás és globális stratégia az űrben; 2) jogi és szabályozási keretek; 3) az űr mint új hadszíntér és a kiberveszélyek általános kérdései; 4) az orosz–ukrán konfliktus tapasztalatai és esettanulmányai; 5) a magánszektor és a digitális hadszíntér szerepe; valamint 6) technikai kihívások és rendszerszintű kiberbiztonsági ellenálló képesség. A klaszterek feltárása rávilágított, hogy a téma rendkívül szerteágazó, de az egyes almotívumok mentén jól strukturálható. Egyben alátámasztotta a hipotézisemet, és igazolta, hogy egyrészt vannak olyan tématerületek, amelyek korábban nem, vagy csak kis mértékben voltak kutatottak (2, 3, 4), míg a régóta kutatott területeken az orosz–ukrán háború tapasztalatai alapján finomhangolások történnek (1, 5, 6).

Az ilyen jellegű klaszterezés hasznos a kutatók számára, mert segít rendszerezni a tudásbázist, illetve azonosítani, hol koncentrálódik a kutatás. Látható például, hogy az orosz–ukrán háború témája kiemelt figyelmet kapott (számos publikáció tartozik ide), ami azt jelzi, hogy a valós események erősen formálták a diskurzust. Ugyanakkor a szabályozási és technikai klaszterek léte azt mutatja, hogy a hosszú távú kihívások – úgymint nemzetközi jogi mechanizmusok kialakítása, illetve a rendszerek biztonságos tervezése – szintén központi kérdések. A klaszterelemzés eredményei alapján a kutatásban esetlegesen hiányos vagy kevésbé feldolgozott területek is azonosíthatók. Ha például azt találtam volna, hogy alig van publikáció a kereskedelmi szereplők vonatkozásában, az egy lehetséges kutatási hézagra utalna – jelen esetben azonban minden fő aspektusra találtam több példát is.

Összefoglalva, a klaszterezés rámutatott az űrkiberbiztonsági szakirodalom fő sodorvonalaira. Az eredmények strukturáltan bemutatva segíthetnek egy készülő publikáció előkészítésében. A szerzők hivatkozhatnak arra, hogy mely fő témakörökbe csoportosul a téma irodalma, és hol helyezkedik el a saját kutatásuk ezen a térképen. Tekintettel arra, hogy a magyar űrambíciók hatására az űrrel kapcsolatos hazai tudományos kutatás a reneszánszát éli, klaszterelemzésem segítheti a témával foglalkozó kutatók orientációját. A részletes módszertani leírás pedig biztosítja az elemzés megismételhetőségét és átláthatóságát, ami a tudományos minőség szempontjából elengedhetetlen. A tematikus klaszterek bemutatása emellett összefoglaló képet nyújt az olvasóknak az űrkiberbiztonság jelenlegi tudásanyagának tagolódásáról és a különböző témák közötti kapcsolatokról.

Az űrkiberbiztonság tehát egy dinamikusan fejlődő kutatási terület, amely az űreszközök, a műholdak és a világűrben alkalmazott informatikai rendszerek sebezhetőségeit, valamint azok védelmi megoldásait vizsgálja. Noha a nemzetközi szakirodalomban az előző fejezetekben bemutatott módon egyre növekvő figyelem irányul az űrkiberbiztonság stratégiai, jogi és technikai aspektusaira, a magyar nyelvű tudományos diskurzusban ez a téma még feldolgozatlan. A 2022 utáni magyar nyelvű szakirodalom áttekintése során megállapítottam, hogy jelenleg nem áll rendelkezésre olyan magyar nyelvű tudományos publikáció, amely kifejezetten az űrkiberbiztonságot vizsgálná, és amely tematikus rendszerezéssel segítené a terület hazai kutatóinak és döntéshozóinak munkáját. A témával kapcsolatos magyar nyelvű anyagok jellemzően szakmai blogokban, híroldalakon és előadások formájában jelentek meg, amelyek ugyan fontos megállapításokat tartalmaznak, de nem biztosítanak mélyreható tudományos elemzést vagy rendszerezett módszertani megközelítést.

Jelen tanulmány segítségével lehetővé válik ennek a hiánynak a pótlása. Miután tudományos keretbe helyezve bemutattam az űrkiberbiztonság legfontosabb tématerületeit egy átfogó tematikus klaszterezési elemzés segítségével, az eredmények hozzájárulhatnak a magyar nyelvű szakirodalom bővítéséhez, valamint irányt mutathatnak a döntéshozók és a kutatók számára a jövőbeli űrbiztonsági kihívások megértéséhez és kezeléséhez.

Felhasznált irodalom

Abels, Joscha (2024): Private Infrastructure in Geopolitical Conflicts: The Case of Starlink and the War in Ukraine. *European Journal of International Relations,* 30(4), 842–866. Online: https://doi.org/10.1177/13540661241260653

Aviv, Itzhak – Ferri, Uri (2023): Russian-Ukraine Armed Conflict: Lessons Learned on the Digital Ecosystem. *International Journal of Critical Infrastructure Protection,* 43, 100637. Online: https://doi.org/10.1016/j.ijcip.2023.100637

Bace, Brianna – Gökce, Yasir – Tatar, Unal (2024): Law in Orbit: International Legal Perspectives on Cyberattacks Targeting Space Systems. *Telecommunications Policy,* 48(4), 102739. Online: https://doi.org/10.1016/j.telpol.2024.102739

Boschetti, Nicolò – Gordon, Nathaniel G. – Falco, Gregory (2022): Space Cybersecurity Lessons Learned from the ViaSat Cyberattack. *ASCEND 2022.* American Institute of Aeronautics and Astronautics. Online: https://doi.org/10.2514/6.2022-4380

Botezatu, Ulpia-Elena – Vevera, Adrian-Victor (2024): Cyber Orbits: The Digital Revolution of Space Security. In Burt, Sally: *National Security in the Digital and Information Age.* IntechOpen. Online: https://doi.org/10.5772/intechopen.1005235

Carlo, Antonio – Obergfaell, Kim (2024): Cyber Attacks on Critical Infrastructures and Satellite Communications. *International Journal of Critical Infrastructure Protection,* 46, 100701. Online: https://doi.org/10.1016/j.ijcip.2024.100701

Cesari, Laetitia (2023): *Commercial Space Operators on the Digital Battlefield. HAL Open Science. Online:* https://hal.science/hal-04491357/document

European Space Policy Institute (2023): *ESPI+ Report. Space, Cyber and Defence: Navigating Interdisciplinary Challenges.* Vienna: ESPI. Online: https://www.espi.or.at/wp-content/uploads/2023/11/ESPI-Report_-Space-Cyber-and-Defence-Navigating-Interdisciplinary-Challenges.pdf

Kolovos, Alexandros K. (2022): *Commercial Satellites in Crisis and War: The Case of the Russian-Ukrainian Conflict.* Online: https://kolydas.eu/wp-content/uploads/2023/05/CommercialSatellitesincrisisandwar.pdf

Kulesza, Joanna – Akcali Gur, Berna (2023): *Developing a Cybersecurity Policy for Low Earth Orbit Satellite Broadband – an International Law Perspective.* Online: https://doi.org/10.2139/ssrn.4424148

Natarajan, K. – Verma, Srikar – Kumar, Dheeraj (2025): Enhanced Interpretation of Novel Datasets by Summarizing Clustering Results Using Deep-Learning Based Linguistic Models. *Applied Intelligence,* 55, 317. Online: https://doi.org/10.1007/s10489-025-06250-6

O'Meara, Chris (2024): Anti-Satellite Weapons and Self-Defence: Law and Limitations. In Kwan, Claire et al.: *CyCon 2024: Over the Horizon. 16th International Conference on Cyber Conflict.* Tallinn: NATO CCDCOE, 249–262. Online: https://doi.org/10.23919/CyCon62501.2024.10685637

Peperkamp, Lonneke – Bolder, Patrick (2024): The Space Domain and the Russia-Ukraine War. In Rothman, Maarten – Peperkamp, Lonneke – Rietjens, Sebastiaan: *Reflections on the Russia-Ukraine War.* Leiden: Leiden University Press, 257–273. Online: https://doi.org/10.24415/9789400604742-014

Poirier, Clémence (2024a): Understanding Cybersecurity in Outer Space. *CSS Analyses in Security Policy,* 343, 1–4. Online: https://doi.org/10.3929/ETHZ-B-000675292
Poirier, Clémence (2024b): Hacking the Cosmos: Cyber Operations Against the Space Sector. A Case Study from the War in Ukraine. *CSS Cyberdefense Reports.* Online: https://doi.org/10.3929/ethz-b-000697348
Pražák, Jakub (2022): On the Threshold of Space Warfare. *Astropolitics,* 20(2–3), 175–191. Online: https://doi.org/10.1080/14777622.2022.2142351
Ray, Kaushik – Selvamurthy, William (2023): Starlink's Role in Ukraine. Portent of a Space War? *Journal of Defence Studies,* 17(1), 25–44. Online: https://www.idsa.in/publisher/journal-of-defence-studies/starlinks-role-in-ukraine-portent-of-a-space-war/
Segate, Riccardo Vecellio (2024): Drafting a Cybersecurity Standard for Outer Space Missions: On Critical Infrastructure, China, and the Indispensability of a Global Inclusive Approach. *Journal of Asian Security and International Affairs,* 11(3), 345–375. Online: https://doi.org/10.1177/23477970241261432
Shahzad, Syed et al. (2024): Cyber Resilience Limitations in Space Systems Design Process: Insights from Space Designers. *Systems,* 12(10), 434. Online: https://doi.org/10.3390/systems12100434
Tepper, Eytan et al. (2023): The Sixth Warfighting Domain? Governing The Space-Cyber Nexus. *Georgia Law Review,* 59. Online: https://ssrn.com/abstract=4791739
Varadharajan, Vijay – Suri, Neeraj (2024): Security Challenges when Space Merges with Cyberspace. *Space Policy*, 67, 101600. Online: https://doi.org/10.1016/j.spacepol.2023.101600

Függelék: Az elemzés során felhasznált források listája

Klaszter	Megjelenés éve	Szerzők	Cím
Az űr mint hadszíntér	2024	Ahumada, Abraham; Del Canto Viterale, Francisco	Securing the Final Frontier: United States Space Force Cybersecurity Capabilities
Az űr mint hadszíntér	2024	Botezatu, Ulpia-Elena	Cybersecurity in the Era of Space Domain Awareness
Az űr mint hadszíntér	2024	Botezatu, Ulpia-Elena; Vevera, Adrian-Victor	Cyber Orbits: The Digital Revolution of Space Security
Az űr mint hadszíntér	2023	Chabert, Valentina	The Outer-Space Dimension of the Ukraine Conflict: Toward a New Paradigm for Orbits as a War Domain?
Az űr mint hadszíntér	2024	de Zoysa, Sayonara; Siriwardana, Deemantha	Final Frontier of Strategic Information Warfare and Cybersecurity Challenges to Satellites and Space Infrastructure
Az űr mint hadszíntér	2023	Heinl, Caitríona	Outer Space as a Growing Security and Defence Domain: Strategic Lessons on Cyber Disruption

Klaszter	Megjelenés éve	Szerzők	Cím
Az űr mint hadszíntér	2022	Pražák, Jakub	On the Threshold of Space Warfare
Az űr mint hadszíntér	2023	Tepper, Eytan; Shackelford, Scott J.; Romano, James B.; Dmitriachev, Sergei	The Sixth Warfighting Domain? Governing The Space-Cyber Nexus
Az űr mint hadszíntér	2024	Blechová, Anna; Harašta, Jakub; Kasl, František	From Space Debris to Space Weaponry: A Legal Examination of Space Debris as a Weapon
Jogi és szabályozási keretek	2024	Bace, Brianna; Gökce, Yasir; Tatar, Unal	Law in Orbit: International Legal Perspectives on Cyberattacks Targeting Space Systems
Jogi és szabályozási keretek	2024	De Sousa, Bruno Reynaud	Cyber Operations Targeting Space Systems. Legal Questions and the Context of Privatisation
Jogi és szabályozási keretek	2023	Li, Du	Legal Dilemma for Combatting Malicious Cyber Activities Against Space Activities
Jogi és szabályozási keretek	2023	Martin, Anne-Sophie	Outer Space, the Final Frontier of Cyberspace: Regulating Cybersecurity Issues in Two Interwoven Domains
Jogi és szabályozási keretek	2024	O'Meara, Chris	Anti-Satellite Weapons and Self-Defence: Law and Limitations
Jogi és szabályozási keretek	2022	Omelyanenko, Vitaliy; Huts, Nataliia; Melnyk, Lina	Space Law in Ukraine: Current Status and Future Development
Kiberbiztonsági irányítás és stratégia	2022	Dilworth, Seth W.; Osborne, D. Daniel	Cyber Threats Against and in the Space Domain: Legal Remedies
Kiberbiztonsági irányítás és stratégia	2023	Febbraro, Daniella	The Need for Cyber Resilience of Space Assets: Law and Policy Considerations of Ensuring Cybersecurity in Outer Space
Kiberbiztonsági irányítás és stratégia	2023	Jacobs, Bas	A Comparative Study of EU and US Regulatory Approaches to Cybersecurity in Space
Kiberbiztonsági irányítás és stratégia	2024	Mattila, Juha Kai	Arranging the Defence of the Cyber Environment as a Part of Military Affairs: Tactical, Operational and Strategic Approach in Retrospect of The Russian-Ukrainian War 2022
Kiberbiztonsági irányítás és stratégia	2024	Poirier, Clémence	Understanding Cybersecurity in Outer Space

Klaszter	Megjelenés éve	Szerzők	Cím
Kiberbiztonsági irányítás és stratégia	2024	Racionero-Garcia, Juan; Shaikh, Siraj Ahmed	Space and Cybersecurity: Challenges and Opportunities Emerging from National Strategy Narratives
Kiberbiztonsági irányítás és stratégia	2024	Segate, Riccardo Vecellio	Drafting a Cybersecurity Standard for Outer Space Missions: On Critical Infrastructure, China, and the Indispensability of a Global Inclusive Approach
Kiberbiztonsági irányítás és stratégia	2024	Shahzad, Syed; Joiner, Keith; Qiao, Li; Deane, Felicity; Plested, Jo	Cyber Resilience Limitations in Space Systems Design Process: Insights from Space Designers
Magánszektor és űrkiberbiztonság	2023	Kulesza, Joanna; Akcali Gur, Berna	Developing a Cybersecurity Policy for Low Earth Orbit Satellite Broadband – an International Law Perspective
Magánszektor és űrkiberbiztonság	2024	Abels, Joscha	Private Infrastructure in Geopolitical Conflicts: The Case of Starlink and the War in Ukraine
Magánszektor és űrkiberbiztonság	2023	Cesari, Laetitia	Commercial Space Operators on the Digital Battlefield
Magánszektor és űrkiberbiztonság	2022	Kolovos, Alexandros K.	Commercial Satellites in Crisis and War: The Case of the Russian-Ukrainian Conflict
Magánszektor és űrkiberbiztonság	2023	Ray, Kaushik; Selvamurthy, William	Starlink's Role In Ukraine: Portent of a Space War?
Az orosz–ukrán háború esetei	2022	Sokiran, Maksym; Zubko, Oksana; Levchenko, Diana	Space Information and Technologies in the Military Activity of Ukraine: Legal Aspect
Az orosz–ukrán háború esetei	2023	Aoki, Setsuko	International Law of the Military Uses of Outer Space in Light of the War in Ukraine as the First Commercial Space War
Az orosz–ukrán háború esetei	2024	Bataille, Mathieu	The Impact and Consequences of the War in Ukraine on Military Space Policies and Operations
Az orosz–ukrán háború esetei	2024	Chadwick, Steven L.	Russia-Ukraine War Lessons for Multidomain Operations
Az orosz–ukrán háború esetei	2022	Choi, Seonghwan	Analysis and Aspects of Space Warfare in the Russia-Ukraine War (Russian Invasion of Ukraine) and Considerations for Space Technology Development
Az orosz–ukrán háború esetei	2024	Gurantz, Ron	Satellites in the Russia-Ukraine War

Klaszter	Megjelenés éve	Szerzők	Cím
Az orosz–ukrán háború esetei	2024	Peperkamp, Lonneke; Bolder, Patrick	The Space Domain and the Russia-Ukraine War
Technikai kiberfenyegetések	2024	Nichols, Randall K.; Mumm, Hans C.; Lonstein, Wayne D.; Ryan, Julie J. C. H.; Carter, Candice M.; Open Textbook Library	Cyber-Human Systems, Space Technologies, and Threats
Technikai kiberfenyegetések	2024	Poirier, Clémence	Hacking the Cosmos: Cyber Operations Against the Space Sector: A Case Study from the War in Ukraine
Technikai kiberfenyegetések	2023	Aviv, Itzhak; Ferri, Uri	Russian-Ukraine Armed Conflict: Lessons Learned on the Digital Ecosystem
Technikai kiberfenyegetések	2022	Boschetti, Nicolò; Gordon, Nathaniel G.; Falco, Gregory	Space Cybersecurity Lessons Learned from the ViaSat Cyberattack
Technikai kiberfenyegetések	2024	Carlo, Antonio; Obergfaell, Kim	Cyber Attacks on Critical Infrastructures and Satellite Communications
Technikai kiberfenyegetések	2024	Jones, Rachel C.	Survey of Space Professionals' Perception of Satellite Cybersecurity from 2012 to 2022: Decision-Makers' Thoughts on Satellite Cybersecurity Evolving
Technikai kiberfenyegetések	2023	Kavallieratos, Georgios; Katsikas, Sokratis	An Exploratory Analysis of the Last Frontier: A Systematic Literature Review of Cybersecurity in Space
Technikai kiberfenyegetések	2024	Khan, Shah Khalid; Shiwakoti, Nirajan; Diro, Abebe; Molla, Alemayehu; Gondal, Iqbal; Warren, Matthew	Space Cybersecurity Challenges, Mitigation Techniques, Anticipated Readiness, and Future Directions
Technikai kiberfenyegetések	2024	Lin, Patrick; Abney, Keith; DeBruhl, Bruce; Abercromby, Kira; Danielson, Henry; Jenkins, Ryan	Outer Space Cyberattacks: Generating Novel Scenarios to Avoid Surprise
Technikai kiberfenyegetések	2022	Thangavel, Kathiravan; Plotnek, Jordan Joseph; Gardi, Alessandro; Sabatini, Roberto	Understanding and Investigating Adversary Threats and Countermeasures in the Context of Space Cybersecurity
Technikai kiberfenyegetések	2024	Varadharajan, Vijay; Suri, Neeraj	Security Challenges when Space Merges with Cyberspace
Technikai kiberfenyegetések	2023	European Space Policy Institute (ESPI)	ESPI+ Report. Space, Cyber and Defence: Navigating Interdisciplinary Challenges