

Biró Gabriella¹

A katonai és civil infrastruktúrák összefonódása az orosz–ukrán háború kiberműveleteiben

The Co-mingling of Military and Civilian Infrastructure in the Cyber Operations of the Russia–Ukraine War

Absztrakt

A 21. századi fegyveres konfliktusokban a kibertér domináns hadszínterré vált, ahol a kinetikus csapások és a kiberműveletek szoros szimbiózisban, valós időben támogatják egymást. Jelen tanulmány az orosz–ukrán háború tapasztalataira építve elemzi a katonai és a polgári kritikus infrastruktúrák technológiai és funkcionális összefonódását. A szerző rámutat, hogy a kettős felhasználású rendszerek – különösen az energiaellátás és a távközlés – elleni támadások során elmosódik a határ a katonai és civil célpontok között, ami súlyos társadalmi következményekkel és nemzetközi tovagyrúzó hatásokkal jár. A cikk konkrét esettanulmányokon keresztül (Viasat, Kyivstar, energetikai hálózatok elleni támadások) vizsgálja a hibrid hadviselés gyakorlatát, bizonyítva, hogy a civil rendszerek megbénítása a modern hadműveletek szerves részévé vált. Az elemzés kiemelt figyelmet szentel a védekezés paradigmaváltásának: bemutatja, hogyan váltak a globális technológiai magánvállalatok és a civil társadalom Ukrajna digitális védelmének kulcsszereplőivé. A tanulmány konklúziója szerint a jövőbeni nemzeti ellenálló képesség már nem garantálható kizárólag állami monopóliumként, a hatékony védelem alapfeltétele a civil szféra, a magánszektor és a védelmi szervek integrált, bizalmi alapú együttműködése.

Kulcsszavak: kibervédelem, kettős felhasználás, kritikus infrastruktúra, interdependencia

¹ Doktori hallgató, Nemzeti Köszolgálati Egyetem Katonai Műszaki Doktori Iskola; tanársegéd, Nemzeti Köszolgálati Egyetem ÁNTK Kiberbiztonsági és e-Közigazgatási Tanszék, e-mail: biro.gabriella@uni-nke.hu

Abstract

In 21st-century armed conflicts, cyberspace has become a dominant theater of war, where kinetic strikes and cyber operations support one another in close symbiosis and in real time. Building on the lessons learned from the Russia–Ukraine war, this study analyses the technological and functional interdependence of military and civilian critical infrastructure. The author points out that during attacks on dual-use systems – particularly energy supply and telecommunications – the line between military and civilian targets becomes blurred, leading to serious social consequences and international ripple effects. Through specific case studies (Viasat, Kyivstar, and attacks on energy grids), the article examines the practice of hybrid warfare, demonstrating that the disruption of civilian systems has become an integral part of modern military operations. The analysis devotes particular attention to the paradigm shift in defence: it illustrates how global private technology companies and civil society have become key players in Ukraine's digital defence. The study concludes that future national resilience can no longer be guaranteed solely through a state monopoly; rather, effective defence requires integrated, trust-based cooperation among the civil sector, the private sector, and defence agencies.

Keywords: cyber defence, dual-use, critical infrastructure, interdependence

Bevezetés

Problémafelvetés

A 21. századi konfliktusok természete alapvető átalakuláson ment keresztül; a hagyományos szárazföldi, vízi, légi és űrbéli hadszínterek mellé egyenrangú, sőt, sok esetben domináns tényezőként zárkózott fel a kibertér mint ötödik hadszíntér.² Ez a dimenzióváltás nagyon élesen megmutatkozik a jelenleg zajló orosz–ukrán háborúban, ahol a kinetikus csapások és a kiberműveletek szerves, valós idejű szimbiózisban valósulnak meg.³ A kiberműveletek így módon fel is erősíthetik a kinetikus támadások hatását és súlyosbíthatják a veszteségeket, például ha a védekező fél kommunikációjának akadályozásával megbénítják reagálóképességét.

A kinetikus és a kibertérben zajló támadások célpontjai általában a kritikus infrastruktúra elemei, amelyeket egymástól való függésük, fizikai interdependenciájuk gyakran még sérülékenyebbé tesz.⁴ Ezek a rendszerek azonban egy másik szempontból is összefüggenek: a katonai célpontokat és a polgári lakosságot kiszolgáló rendszereket sokszor ugyanaz az infrastruktúra látja el árammal és kommunikációs hálózatokkal. Ezért amikor az ilyen infrastruktúrák célkeresztbe kerülnek, a támadás következményei a hadsereget és a civil lakosságot egyaránt érintik. Ugyan az 1977-es, a genfi egyezményekhez fűzött I. Kiegészítő Jegyzőkönyv (AP I) 48. cikke (Alapvető szabály – Basic

² ORBÓK 2013.

³ MIRON–THORNTON 2024.

⁴ MUHA 2007.

Rule) kimondja, hogy a harcoló feleknek mindig meg kell különböztetniük a polgári lakosságot a harcosoktól és a polgári célpontokat a katonai célpontoktól, és műveleteiket csak katonai célpontok ellen irányíthatják a civil lakosság és célpontok védelme érdekében,⁵ a gyakorlatban mégsem ezt látjuk az orosz–ukrán háború során. Ennek nemzetközi jogi aspektusaival jelen cikk nem foglalkozik, azonban fontos megjegyezni, hogy a katonai parancsnokoknak tisztában kell lenniük a genfi egyezmény alapelveivel, amikor döntéseket hoznak a támadásokkal kapcsolatban, tehát a civil lakosságot is érintő következmények tudatos döntés eredményei. A kritikus infrastruktúra elemeit érintő kibertámadások meghatározásával és nemzetközi jogi megítélésével a *Tallinni Kézikönyv 2.0*⁶ foglalkozik behatóbban.

Jelen tanulmány célja annak részletes bemutatása, hogyan válnak a kettős felhasználású (*dual-use*) infrastruktúrák – mint a távközlés, az energiaellátás vagy a logisztikai hálózatok – a kiberműveletek elsődleges célpontjaivá akár önálló műveletek keretében, akár kinetikus műveletek támogató műveletei során. Az elemzés megmutatja, hogy ez az infrastrukturális interdependencia milyen komplex kihívások elé állítja a nemzeti ellenálló képességet, kiberrezilienciát. (A magyar nyelvre fordított európai uniós joganyagokban az angol *resilience* kifejezés fordítása „reziliencia”, azonban az angol szó köznapi értelemben ellenálló képességet jelent.) A kritikus feladatellátás biztonsága a jövőben már nem garantálható izolált védelmi stratégiákkal; ehelyett a polgári szféra, a katonai vezetés és a rendvédelmi szervek minden eddigénél szorosabb, integrált együttműködésére van szükség. A tanulmány arra a kutatási kérdésre keresi a választ, hogyan változtatja meg a kritikus infrastruktúrák technológiai és funkcionális interdependenciája a hadviselő felek célkiválasztási mechanizmusát, és ez milyen kényszerpályára állítja a nemzeti rezilienciaépítést a 21. századi hibrid konfliktusokban. A szerző hipotézise szerint a modern hadviselésben a kritikus infrastruktúrák fizikai és logikai összefonódása miatt a civil szféra veszteségei többé nem tekinthetők véletlenszerűnek, a hadviselés rendszerszintű, kalkulált velejárójává váltak. Bár a nemzetközi szakirodalom széleskörűen tárgyalja a kritikus infrastruktúrák militarizálódását, jelen tanulmány azzal kíván hozzájárulni a témakör vizsgálatához, hogy a nyugati elméleti modelleket ütközteti az orosz–ukrán háború regionális és doktrinális valóságával.

Elméleti és fogalmi keretek

A modern államok stabilitása a kritikus infrastruktúrák zavartalan működésén alapul. Ezen rendszerek – mint az energiaellátás, a közlekedés, az infokommunikáció vagy a pénzügyi szektor – kiesése súlyos gazdasági és társadalmi károkat, valamint a közbizalom megrendülését okozhatja. Ahhoz azonban, hogy megértsük a jelenlegi konfliktusok hibrid fenyegetéseit, elsőként tisztáznunk kell a kritikus infrastruktúrákhoz kapcsolódó definíciókat és elméleti megközelítéseket.

⁵ Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977 1977.

⁶ SCHMITT – NATO Cooperative Cyber Defence Centre of Excellence 2017.

Több gondosan megfogalmazott definíció is elérhető a kritikus infrastruktúrák,⁷ illetve az ahhoz kapcsolódó fogalmak meghatározására. Az Európai Unióban a 2022-ben kiadott CER irányelv⁸ így határozza meg a kritikus infrastruktúrát: „olyan eszköz, létesítmény, berendezés, hálózat vagy rendszer, vagy valamely eszköz, létesítmény, berendezés, hálózat vagy rendszer része, amely szükséges az alapvető szolgáltatás nyújtásához.” Az alapvető szolgáltatás meghatározása pedig a következő: „az alapvetően fontos társadalmi funkciók, a gazdasági tevékenységek, a népegészségügy és a biztonság vagy a környezet fenntartásához elengedhetetlen szolgáltatás.”

Hagyományos megközelítésben a civil és a katonai infrastruktúrák élesen elkülönülnek egymástól. A polgári infrastruktúra elsődleges célja a társadalmi és gazdasági jólét biztosítása, míg a katonai infrastruktúra a honvédelem operatív képességeit szolgálja ki. A nemzeti szabályozásokban (így a magyar⁹ és az európai uniós¹⁰ joganyagban is) a védelmi létesítmények általában nem részei a klasszikus kritikus infrastruktúra definíciónak, hanem önálló kategóriát képeznek (például honvédelmi célú létesítmények).

A katonai infrastruktúrák csak ott jelennek meg a nemzeti kritikusinfrastruktúra-rendszerekben, ahol funkcionális függőség mutatható ki: például, ha egy katonai bázis energiaellátása az országos hálózatról történik, vagy a logisztikai utánpótlás a közösségi közlekedési útvonalakra támaszkodik. Formálisan tehát létezik egy határvonal, a valóságban azonban ez a határ gyakran elmosódott. A 21. századi hálózatok legfőbb jellemzője az interdependencia. Egyetlen szektor sem működhet elszigetelten: a távközlés áramot igényel, az energiaszektor irányítása pedig távközlési hálózatokon zajlik. A kritikus infrastruktúrák interdependenciájának dimenzióit Bakos és Kovács vizsgálja részletesen.¹¹ Ebben a kontextusban jelenik meg a kettős felhasználás problematikája, amely a katonai műveletek egyik legnagyobb sérülékenységevé vált, és ezzel párhuzamosan katonai célponttá tette a civil lakosság által használt infrastruktúrát.

A szakirodalom gyakran *co-mingling* vagy *commingling* (összefonódás) néven hivatkozik arra a jelenségre, amikor a polgári és katonai adatforgalom, illetve funkciók fizikailag és logikailag nem választhatók szét. Az orosz–ukrán háború tapasztalatai alapján ez leginkább két területre összpontosul:

- energiahálózatok: a katonai létesítmények áramellátása ritkán független a lakossági hálózattól;
- távközlési rendszerek: a katonai kommunikáció (bár titkosított) gyakran ugyanazon a gerinchálózatokon, optikai kábeleken és műholdas rendszereken fut keresztül, amelyeken a civil internetforgalom.

Mivel a kritikus infrastruktúrák jelentős része magántulajdonban vagy civil állami vállalatok kezében van, ezek védelme nem tekinthető tisztán katonai feladatnak.¹²

⁷ MUHA 2007; BOGNÁR–BONNYAI 2019.

⁸ Az Európai Parlament és a Tanács (EU) 2022/2557 irányelve (2022. december 14.) a kritikus szervezetek rezilienciájáról és a 2008/114/EK tanácsi irányelv hatályon kívül helyezéséről (EGT-vonatkozású szöveg) 2022.

⁹ 2024. évi LXXXIV. törvény a kritikus szervezetek ellenálló képességéről.

¹⁰ Az Európai Parlament és a Tanács (EU) 2022/2557 irányelve.

¹¹ BAKOS–KOVÁCS 2025.

¹² MUHA 2007.

A jogi és operatív kereteket szükségszerűen úgy alakítják ki az egyes országok, hogy együttműködést feltételeznek a polgári biztonsági, katasztrófavédelmi és honvédelmi területek közt. Ez a széttagoltság azonban lassítja az információáramlást és a reakcióidőt.

Ha a kritikus infrastruktúra kiberműveletek célpontjává válik, akkor ez az összefonódás többszörös kockázatot jelent:

- járulékos veszteség: egy katonai célpont (például vezetési pont) elleni kiber-támadás, amely a civil hálózaton keresztül történik, kommunikációs vagy energetikai szempontból megbéníthatja egy egész régió lakossági ellátását (kórházak, fűtés, távközlés);
- célponttévesztés: a kettős felhasználású eszközök miatt a támadó számára nehezen azonosítható, hogy egy adott szerver vagy hálózati csomópont kizárólag katonai célt szolgál-e, illetve ha bizonyítottan látja a katonai felhasználást, akkor esetleg nem törődik a civil veszteségekkel;
- védelmi aszimmetria: a katonai rendszerek általában megerősített védelemmel rendelkeznek, míg a hozzájuk kapcsolódó civil beszállítói hálózatok gyakran a „leggyengébb láncszemet” jelentik, könnyű behatolási pontot kínálva a támadóknak.

Az orosz–ukrán háború kiberdimenziója

Az orosz–ukrán háború műveleteinek elemzése során elengedhetetlen az orosz hadviselési koncepció megértése, amely a kiberműveleteket nem csupán támogató elemként, hanem a modern hadviselés szerves részeként kezeli.¹³ A műveletek dinamikája rávilágít arra, hogyan próbálta az orosz vezetés a digitális térben elért információs fölényt fizikai győzelemre váltani.

A kiberhadviselés természetéről szóló nemzetközi elméleti vitákban gyakori a stratégiai és az operacionális szintű kiberműveletek éles fogalmi szétválasztása. Míg a nyugati elméletirők egy része (például Thomas Rid¹⁴) a kiberfegyverek stratégiai, háborút eldöntő képességét szkeptikusan ítéli meg, addig az orosz hadviselési doktrína egyáltalán nem alkalmazza ezt a nyugati elemzési keretet. Ahogy arra a hazai hadtudományi szakirodalom (például Jójárt Krisztián¹⁵) és az orosz kibereszközöket vizsgáló nemzetközi kutatók (például Miron és Thornton¹⁶) is rámutatnak, az orosz és a posztszovjet katonai gondolkodásban – így a Valerij Geraszimov által is fémjelzett megközelítésben – az „információs küzdelem” (*информационное противоборство*) holisztikus fogalom. Ebből a perspektívából nézve irreleváns a stratégiai és operacionális hatások mesterséges szétválasztása: a kiberműveletek és a kinetikus csapások egyazon információs-pszichológiai cél alá rendelve, elválaszthatatlan szimbiózisban működnek. Jelen tanulmány esettanulmányai éppen azt bizonyítják, hogy a kettős felhasználású kritikus infrastruktúrák megbénítása (például a Viasat vagy a Kyivstar elleni csapások) a nyugati elméletek szerinti operacionális zavarkeltésen túlmutatva,

¹³ MIRON–THORNTON 2024.

¹⁴ RID 2013.

¹⁵ JÓJÁRT 2023.

¹⁶ MIRON–THORNTON 2024.

a társadalom működésének rendszerszintű megbénítását, ezáltal a védekezés stratégiai feltételeinek felszámolását célozza.

Az orosz katonai gondolkodásban az információs tér ellenőrzése kulcsfontosságú. A doktrína központi eleme a „káoszeremtés”, vagyis az ellenfél döntéshozatali ciklusának megbénítása. Ebben a koncepcióban a kibertámadások elsődleges célja az információs tér előkészítése a kinetikus műveletek támogatására: a célország társadalmi kohéziójának gyengítése, a bizalom aláásása és a védekező fél kommunikációs képességeinek kiiktatása még azelőtt, hogy az első lövés eldördülne.¹⁷

A 2022. február 24-i teljes körű orosz inváziót megelőző hónapokban, de különösen az utolsó hetekben a kibertevékenység jellege drasztikusan megváltozott. Míg korábban, 2014 után az orosz állami háttérű csoportok főként kémkedésre és adatszerzésre fókuszáltak, az 2022-es invázió előtt megjelentek a kifejezetten pusztításra tervezett, destruktív kódok (*wiperek*).¹⁸ Ukrajna és a világ többi része már 2017-ben találkozhatott a magát első ránézésre egyszerű zsarolóvírusnak álcázó NotPetya kártevővel, amely világszerte jelentős károkat okozott.¹⁹ 2022 januárjában jelent meg a WhisperGate, szintén zsarolóvírusnak álcázva magát, de valójában nem tartalmazott helyreállítási funkciót,²⁰ tehát a titkosított adat visszaszerzésére nem volt valószínűség. Közvetlenül az invázió előtt és alatt aktiválták a HermeticWiper és az IsaacWiper kódokat, amelyek ukrán kormányzati hálózatokat és pénzügyi rendszereket támadtak.²¹ Ezek a műveletek a felégetett föld taktikáját alkalmazták a digitális térben: céljuk a kritikus adatok megsemmisítése és a visszaállítás lehetetlenné tétele volt.

A destruktív vírusokkal párhuzamosan, a teljes körű orosz invázió előtti napokban (február 15-től kezdődően) és az első 48 órában Ukrajna történetének legintenzívebb elosztott szolgáltatásmegtagadás (*distributed denial of service, DDoS*) támadásai érték az országot.²² A célpontok tudatosan a civil szférából kerültek ki: a legnagyobb állami bankok, a védelmi minisztérium portáljai és a lakossági tájékoztatást szolgáló kormányzati weboldalak váltak elérhetetlenné. Ez a műveletsorozat szervesen illeszkedett az orosz hadászati elképzelésbe, amely a gyors siker feltételének tekinti az információs környezet destabilizálását. A banki szolgáltatások és kormányzati intézmények működésének akadozása a lakosság elbizonytalanítását, a pánikkeltést célozta, tehát pontosan a kritikus infrastruktúrák működésének/kiesésének társadalmi vetületére épült. A kormányzati kommunikációs csatornák elvágása (vagy azok megbízhatóságának megkérdőjelezése) megnehezítette a polgári védelem és a katonai vezetés koordinációját és gátolta a döntéshozatalt. A digitális vakság, a helyzetfelismerő képesség (*situational awareness*) elvesztése és a hátszárnyban eluralkodó káosz elméletben megkönnyítette volna az orosz előre nyomulást, előkészítve ezzel a kinetikus támadás sikerét és csökkentve a szervezett ellenállás esélyét.

¹⁷ HAIG 2018; KOVÁCS 2018.

¹⁸ *A Decade in the Trenches of Cyberwarfare* 2024.

¹⁹ KRASZNAV 2022.

²⁰ AMBRUS 2023.

²¹ ESET Research: *Ukraine hit by Destructive Attacks before and during the Russian Invasion with HermeticWiper and IsaacWiper* 2022.

²² *A Decade in the Trenches of Cyberwarfare* 2024.

Az orosz offenzíva nem ért el gyors sikert, de a kibertérben 2022 és 2023 közt nagyságrendi ugrás volt az orosz–ukrán háború során megfigyelt kibertámadások számában és a módszerek, célpontok is változatosabbak lettek.²³ A támadások adatait gyűjtő CyberPeace Institute pedig 2023 decemberével meg is szüntette az adatok publikálását,²⁴ de már 2023 során is látható volt, hogy nehezen birkóznak meg az egyre intenzívebb kibertevékenységek elemzésének feladatával.

Kutatási módszertan

Jelen tanulmány kutatási módszertana kvalitatív elemzésen alapul, keretében az elérhető szakirodalom, a technikai jelentések és a releváns események szisztematikus feldolgozása történt meg. A vizsgálat időbeli kereteit a 2022. február 24-én megindult orosz invázió kezdetétől napjainkig terjedő időszak határozza meg (néhány releváns korábbi esemény említésével), különös tekintettel a konfliktus azon szakaszaira, ahol a kiberműveletek és a kinetikus hadviselés koordinációja bizonyíthatóan megjelent.

Az elemzés esettanulmány-alapú megközelítést alkalmaz az elméleti megközelítések gyakorlati igazolására. A vizsgált incidensek – kiemelten a Viasat és a Kyivstar elleni támadások – kiválasztása során a célzott mintavétel elvét követtük, mivel ezek tekinthetők a leginkább reprezentatív példáknak a civil és katonai szféra összefonódásából fakadó kockázatok bemutatására. A Viasat-incidens a határokon átnyúló tovagyrúzó hatás (*spillover effect*), míg a Kyivstar-eset a társadalmi-katonai mély interdependencia miatt tekinthető paradigmateremtő példának – mindkettő alkalmas az elméleti hipotézis tesztelésére. Ezen esetek kiválasztását az is indokolta, hogy rajtuk keresztül szemléltethető legtisztábban a kettős felhasználású technológiák inherens sebezhetősége és a civil lakosságra gyakorolt súlyos következmények. Továbbá ezek az incidensek szolgáltatják a legkézzelfoghatóbb bizonyítékot arra, ahogyan egy lokális konfliktus kiberműveletei a fizikai határokon átnyúlva nemzetközi, tovagyrúzó hatásokat generálnak, veszélyeztetve ezzel harmadik felek kritikus infrastruktúráját is.

A kvalitatív kutatás adatgyűjtési protokollja a vizsgált jelenség – a zajló fegyveres konfliktus kiberdimenziója – dinamikusán változó természete miatt nem néhány, adott időpillanatban lefuttatott keresésre épült. A felhasznált források gyűjtése folyamatos forrásmonitorozáson és longitudinális szakirodalom-követésen alapult a 2022. február 24-től napjainkig terjedő időszakban. A szakirodalmi és technikai források felkutatása és kiválasztása szakértői célzott mintavétellel történt. A feldolgozott források köre elsődlegesen a kurált, referált folyóiratokat indexáló tudományos adatbázisokban (például Scopus, Web of Science) megjelent, kiberbiztonsággal és hadtudománnyal foglalkozó lektorált cikkekre terjedt ki. Ezt a szisztematikus szakirodalom-gyűjtést tudományos keresőmotorok (elsősorban a Google Scholar) találatai, valamint akadémiai kutatói közösségi platformok (ResearchGate, Academia.edu) használata egészítette ki. A téma sajátosságaiból fakadóan az elemzés támaszkodott továbbá releváns technikai és iparági jelentésekre (eseménykezelő központok és nagyvállalatok

²³ Kiss 2024.

²⁴ *Cyber Attacks in Times of Conflict* [é. n.].

biztonsági jelentései, technikai elemzések), valamint elsődleges forrásokra (az érintettek Telegram- és blogbejegyzései). A kiberműveletekre vonatkozó források kiválasztásához és megbízhatóságának megítélésénél az ENISA (az Európai Unió Kiberbiztonsági Ügynöksége) fenyegetettségi térkép módszertanának szempontjait alkalmaztuk.²⁵ A tisztán kinetikus műveletekre fókuszáló forrásokat kizártam. Az azonosított források strukturálása, kódolása és rendszerezése egy dedikált referenciakezelő adatbázisban történt. A kutatás elméleti kereteit adó szakirodalom vizsgálatakor tudatosan nagy hangsúlyt kapott a magyar katonai és biztonságpolitikai szakirodalom, mivel a magyar kutatók nyelvi és regionális beágyazottságuk okán gyakran olyan primer orosz és ukrán forrásokat is feldolgoznak a konfliktus operatív szintű elemzésekor, amelyek az angol-szász elméleti irodalomban ritkábban jelennek meg.

Tekintettel a kutatás kvalitatív és esettanulmány-alapú jellegére, a vizsgálat megismételhetőségét és megbízhatóságát az analitikus transzparencia és a logikai konzisztencia garantálja. Az eredmények igazolhatóságát az események strukturált, előre rögzített analitikus mátrix – az interdependencia típusa, a járulékos kár és a további ürrítő hatás – mentén történő vizsgálata biztosítja. Ez a módszertani keret teszi lehetővé, hogy a vizsgált incidensek mint empirikus adatpontok, valamint a belőlük levont rendszerszintű, elméleti következtetések közötti összefüggés külső elemzők számára is egyértelműen visszakövethető és igazolható legyen bármilyen hiteles esetleírásból kiindulva.

Eredmények

Esettanulmányok: kritikus infrastruktúrák a célkeresztben

Az orosz–ukrán háború tapasztalatai azt mutatják, hogy a kinetikus hadműveletek sikeréhez ma már elengedhetetlen a hátszág kritikus rendszereinek megbénítása, mert a háború nem korlátozódik a frontvonalra. Az orosz támadók figyelme két szektor, az energia és a távközlés felé fordult, amelyek a modern információs társadalom és a hadsereg idegrendszerét és keringését jelentik, ezért stratégiai célpontok. Az energetikai hálózat elleni támadások, különösen az elosztóhálózatok és alállomások ipari vezérlőrendszerei (*industrial control systems* és *supervisory control and data acquisition*, ICS/SCADA) ellen azonnali, kaszkádszerű hatást váltanak ki. Áram nélkül megbénul a logisztika, leállnak a vízművek, és működésképtelenné válnak a kommunikációs tornyok. A távközlés és a kommunikációs csatornák elvágása pedig a védekező fél vakságát és süketségét eredményezi. Az orosz stratégia a fagyos tél taktikáját alkalmazta a kibertérben is: a polgári lakosság moráljának megtörése és a katonai vezetés kommunikációs csatornáinak elvágása egyszerre valósult meg ugyanazon infrastruktúrák támadásával.

A 2022-es teljes körű orosz invázió során látott kibertámadások nem voltak előzmény nélküliek, 2015 és 2016 során több nagyon súlyos kibertámadás is érte az ukrán villamosenergia-rendszert.²⁶ Az első nagyobb támadás során 2015. december 23-án

²⁵ European Union Agency for Cybersecurity 2025.

²⁶ KRASZNAY 2022.

mintegy 225 000 fogyasztó maradt ellátatlan a hideg ukrán télben.²⁷ A támadás egyértelműen Oroszországnak tulajdonítható, a közvetlenül karácsony előtti időzítés pedig erősen arra utal, hogy a lélektani hatás is szempont volt amellett, hogy az ünnepek alatt általában nehezebb a hibák elhárítása is. A vizsgált támadásokat és azok hatásait az 1. táblázat foglalja össze.

1. táblázat: A vizsgált incidensek összefoglalása

Vizsgált incidens	Elsődleges célpont	Érintett civil szféra	Interdependencia típusa	Tovagyűrűző hatás
Energetikai hálózatok elleni 2015-ös támadás	Ipari vezérlő-rendszerek (ICS/SCADA), elosztó-hálózatok	Lakossági áramellátás (több száz-ezer fogyasztó), fűtési kiesés	Fizikai és funkcionális (áramellátástól függő kritikus alrendszerek)	Szektorközi kaskádhatás (logisztika, vízművek, távközlési bázisállomások azonnali leállása)
Viasat KA-SAT (2022)	Viasat földi infrastruktúra, ukrán fegyveres erők C2 rendszere	Lakossági internetszolgáltatás, európai felhasználók	Technológiai (közös platform, kettős felhasználású műholdas hálózat)	Nemzetközi spillover (NATO-tagállam kritikus infrastruktúrája: német szélerőművek távvezérlésének elvesztése)
Kyivstar (2023)	Ukrán mobilszolgáltató maghálózata, katonai és polgári védelmi kommunikáció	Milliók mobil- és internetelérése, banki ATM-ek, légoltalmi szírnák	Szolgáltatói és logikai (azonos kereskedelmi hálózaton futó civil és védelmi adatforgalom)	Társadalmi-gazdasági sokk (pénzügyi tranzakciók és polgári védelmi rendszerek egyidejű megbénulása)

Forrás: a szerző szerkesztése

A Viasat KA-SAT-incidens

A Viasat KA-SAT-incidens a modern hadviselés történetének egyik legjelentősebb kiberbiztonsági eseménye 2022. február 24-én, az invázió megindulásának óráiban történt. A Viasat amerikai műholdas szolgáltató KA-SAT-műholdhoz kapcsolódó hálózata elleni támadás tökéletesen illusztrálja a kettős felhasználású technológiákból fakadó sebezhetőséget. Ez az eset tekinthető a civil–katonai összefonódás iskolapéldájának, ahol minden elméleti kockázat egyszerre vált kézzelfogható valósággá. Az offenzíva napján hajnalban, éppen akkor, amikor az orosz csapatok átlépték az ukrán határt, célzott kibertámadás érte a Viasat földi infrastruktúráját. A támadók egy menedzsmenthálózaton keresztül hibás *firmware* frissítést küldtek ki a felhasználói terminálokra (modemekre). A kártékony kód (amelyet később AcidRain néven azonosítottak) gyakorlatilag törölte a modemek memóriáját, használhatatlanná téve azokat és elvágyva a modemek által biztosított internetkapcsolatot.²⁸ A támadás elsődleges célpontja nem a civil lakosság volt, hanem az ukrán fegyveres erők. Ukrajna ugyanis – saját, dedikált katonai műholdas rendszer híján – nagymértékben támaszkodott a kereskedelmi

²⁷ GÖRGEY 2020.

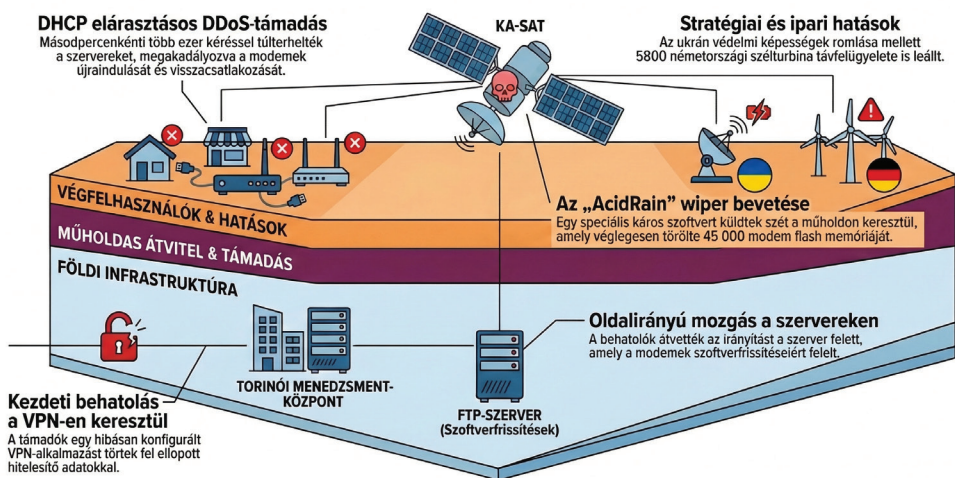
²⁸ BURGESS 2022.

Viasat hálózatra a katonai kommunikációban. A támadás következtében az invázió legkritikusabb első óráiban jelentős zavar keletkezett az ukrán parancsnoki és irányítási (C2) rendszerben, ami átmenetileg megnehezítette a védekező egységek koordinációját.

Amellett, hogy a támadás a katonai kommunikáción túl az ukrán civil lakosságot is jelentősen érintette, a Viasat-incidens rávilágított arra is, hogy a kibertérben nincsenek országhatárok. Mivel a KA-SAT-hálózat egész Európát lefedi, a támadás hatásai azonnal tovagyűrűztek, jelentős nemzetközi járulékos károkat okozva:

- civil felhasználók: Európa-szerte több tízezer lakossági internet-előfizető szolgáltatása szűnt meg hosszabb-rövidebb időre;
- kritikus infrastruktúra az EU-ban: a legmegdöbbentőbb hatás Németországban jelentkezett, ahol közel 5800 szélerőmű távvezérlése állt le.²⁹ Ezek a turbinák a Viasat hálózatán keresztül kommunikáltak a vezérlőközponttal. Bár az áramtermelés nem állt le, a rendszerek felügyelete megszűnt, ami rávilágít arra, hogy egy földrajzilag elkülöníthető konfliktus kiberműveletei hogyan veszélyeztethetik NATO-tagállamok kritikus infrastruktúráját is.

Ez az eset ékesen bizonyítja, hogy a katonai célú kibercsapások a közös technológiai platformok miatt elkerülhetetlenül érintik a civil szférát, a kibertér nemzetközi jellegéből adódóan potenciálisan globális biztonsági kockázatot teremtve. Az Európai Unió főképviselője közleményben ítélte el a Viasat elleni támadást, és kiemelte: „Az Ukrajnát célzó kibertámadások, beleértve a kritikus infrastruktúrát érintőket is, áttejedhetnek más országokra is, és rendszerszintű hatásokkal járhatnak, veszélyeztetve az európai polgárok biztonságát.”³⁰ Ez az eset empirikusan bizonyítja a kibertér területek feletti jellegét: egy lokális konfliktusban alkalmazott precíziós fegyver a közös technológiai platform miatt globálisan tovagyűrűző hatást váltott ki. A Viasat-incidens elemeit és hatásait az 1. ábra foglalja össze.



1. ábra: A Viasat-incidens elemei és hatásai

Forrás: a szerző szerkesztése a NotebookLM mesterséges intelligencia felhasználásával, a cikkben hivatkozott felhasznált irodalom alapján

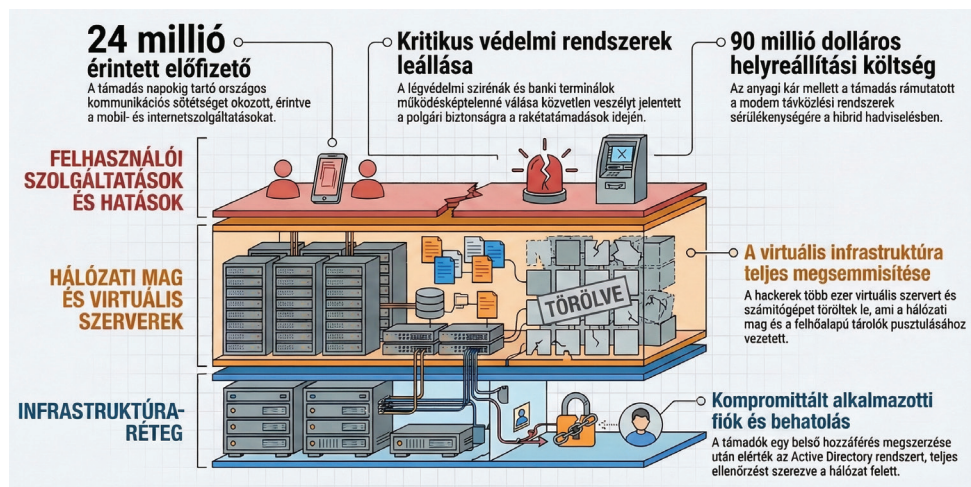
²⁹ Reuters 2022.

³⁰ European Council 2022.

A Kyivstar elleni támadás

2024. december 12-én történt egy másik nagyon jelentős, ukrán kommunikációs kritikus infrastruktúrát érintő támadás, amely a Kyivstar mobil- és internetszolgáltatását bénította meg napokra. A holland tulajdonú Kyivstar Ukrajna legnagyobb mobilszolgáltatója közel 24 millió előfizetéssel, így a szolgáltatáskiesés is több millió ügyfelet érintett Kijev és Szumi régióiban. A kommunikációs zavar nem csak lakossági ügyfelekre terjedt ki: a banki ATM-ek gyakran mobilhálózaton kommunikálnak (ha az elhelyezésük miatt nem praktikus vezetékes hálózatot kiépíteni), de a katasztrófavédelem kommunikációját és a két régió légoltalmazási-rendszereit is érintette a kiesés. A támadást technikai jellemzői alapján az ukrán eseménykezelő központ (CERT-UA) az orosz katonai hírszerzéshez, a GRU-hoz köthető Sandworm csoportnak tulajdonította. Egy szintén a Sandworm-egységhez köthető orosz hackercsoport pedig Telegram-közleményben vállalta magára a támadást. „A Kyivstar ellen azért indítottunk támadást, mert a vállalat kommunikációs szolgáltatásokat nyújt az ukrán fegyveres erőknek, valamint az ukrán kormányzati szerveknek és bűnüldöző szerveknek”, írták Telegram-csatornájukon.³¹ Mivel ez egy aktív információs hadviselési környezetben közzétett primer forrás, az abban foglalt állításokat a lehetséges stratégiai kommunikációs és dezinformációs célok miatt forráskritikával kell kezelni, azonban a közlés tartalma egybevág a más forrásokból ismert tényezőkkel (technikai attribúció, orosz hibrid hadműveletek módszertana).

A Kyivstar és a hozzá hasonló kibertámadások civil lakosság által elszenvedett következményei miatt a Nemzetközi Büntetőbíróság is vizsgálatot indított.³² A bizonyítékokat, amelyek a vizsgálat elindításához vezettek, a Berkeley Human Rights Center kutatói gyűjtötték össze és nyújtották be. Az ő nyilatkozataiból tudjuk, hogy legalább öt ügyben zajlik vizsgálat: három, az ukrán energetikai hálózatot ért kibertámadás, a NotPetya és a Viasat-incidens esetében merült fel a háborús bűncselekmények, azaz a genfi egyezmények megsértésének gyanúja.³³ A Kyivstar elleni támadás elemeit és következményeit a 2. ábra foglalja össze.



2. ábra: A Kyivstar-incidens elemei és hatásai

Forrás: a szerző szerkesztése a NotebookLM mesterséges intelligencia felhasználásával, a cikkben hivatkozott felhasznált irodalom alapján

³¹ GREENBERG 2023.

³² DEUTSCH-BERG-PEARSON 2024.

³³ VERBRUGGEN 2023.

Következtetések

A védekezés új modellje: a magánszektor és a civil társadalom stratégiai szerepe

Az orosz–ukrán háború egyik legmeghatározóbb tanulsága, hogy a modern kibervédelem már nem kizárólag állami monopólium. Ukrajna digitális túlélése nagymértékben a globális technológiai óriások (*big tech* cégek) példátlan szerepvállalásának és a civil társadalom mozgósításának köszönhető. Ez a jelenség új működési modellt teremtett, elmosva a határokat az állami és a magánszereplők között, és az együttműködés már nemcsak a kiberbűnözés elleni harcra terjed ki,³⁴ hanem kifejezetten védelmi célokat is szolgál. A 2022-es teljes körű orosz invázió kezdetén egyfajta digitális védőernyő jött létre Ukrajna felett, amelyet nem a NATO, hanem magánvállalatok tartottak. A nagy felhőszolgáltatók (Microsoft, Google, Amazon), valamint a kiberbiztonsági cégek, mint az ESET és a Mandiant, proaktívan léptek fel az orosz fenyegetésekkel szemben. A Microsoft alelnöke és elnöke, Brad Smith emellett blogbejegyzésben fejezte ki aggodalmát a civil célpontok elleni kibertámadások miatt is.³⁵

Az Amazon Web Services (AWS), a Microsoft Azure és a Google Cloud segítségével Ukrajna a háború első napjaiban végrehajtotta a kormányzati rendszerek „digitális evakuációját”. A fizikai szervertermek, amelyek rakétatalálatnak voltak kitéve, virtuálissá váltak: az állami adatvagyon (nyilvántartások, banki adatok) biztonságos, külföldi felhő-infrastruktúrába költözött, garantálva az állam működőképességét. Míg korábban Ukrajna a magyar szabályozáshoz hasonlóan konzervatív módon tiltotta a nemzeti adatvagyon felhőbe költöztetését, a fizikai megsemmisülés fenyegetése miatt az ukránok újraértékelték a kockázatokat és kiadták a jogszabályt, amely lehetővé tette a felhő használatát.³⁶

Amikor a földi infrastruktúra a kinetikus támadások következtében sérült, a SpaceX Starlink műholdas rendszere biztosította a redundáns kommunikációt. Ez nemcsak a civil lakosság kapcsolattartását tette lehetővé, hanem a katonai egységek, tűzérési rendszerek és drónok irányításának gerincévé is vált, gyakorlatilag katonai képességgé konvertálva egy civil szolgáltatást.³⁷

A fentiek eredményeként a kormányzati és katonai műveletek támogatása egyre inkább privát kapacitásokra támaszkodik. A kettős felhasználású technológiák fogalma kiegészült a kapacitások „privatizálódásával”: a hadsereg olyan eszközöket használ, amelyeket nem ő birtokol, nem ő üzemeltet, és amelyek felett nincs teljes kontrollja. Ez a szimbiózis hatékony, de új függőségi viszonyokat és kockázatokat teremt, hiszen ezek a multinacionális cégek önálló geopolitikai aktorokká léptek elő, akiknek döntései (például szolgáltatás korlátozása egy adott régióban³⁸) közvetlen hatással vannak a katonai műveletek kimenetelére.

A technológiai óriások ezen szerepvállalása alátámasztja a civil–katonai viszonyokat vizsgáló korábbi nemzetközi kutatások (például Myriam Dunn Cavelty és Florian J.

³⁴ MOYNIHAN–WEBB–CLOONEY 2025.

³⁵ SMITH 2022.

³⁶ *Про хмарні послуги* [é. n.].

³⁷ BÍRÓ 2025a.

³⁸ ROULETTE – BRYAN–LOW – BALMFORTH 2025.

Egloff³⁹) azon megállapításait, miszerint a kibertérben a klasszikus állami erőszak-monopólium erodálódik. Kialakul a „digitális szuverenitás paradoxona”: az állam fizikai túlélése érdekében kénytelen védelmi funkcióinak és szuverenitásának egy részét önálló geopolitikai aktorokként fellépő magánvállalatokra delegálni. Bár ez a fejlődési irány megjósolható volt, a 2022. február 24. utáni események tökéletesen megmutatták, hogy a jelenség mennyire valós.

A technológia mellett az emberi tényező is átalakult. A kiberhadviselésben a frontvonal nem lövészárkokban, hanem szerverszobákban és nappalokban húzódik, a támadók és védekezők pedig gyakran civilek. A kritikus infrastruktúrák védelmében a magáncégek IT-szakemberei váltak az első védelmi vonallá. Amikor egy bankot vagy energiaszolgáltatót támadás ér, nem katonák, hanem civil mérnökök és rendszergazdák hárítják el a veszélyt. Ők azok, akik foltozzák a biztonsági réseket és helyreállítják a szolgáltatást, miközben munkájukkal közvetve kibervédelmi feladatot látnak el.

Egyedülálló jelenség az ukrán kormány által hivatalosan is támogatott, de önkéntes alapon szerveződő IT Army of Ukraine (ukrán IT hadsereg) létrejötte. Ez, a becslések szerint több százezer fős, globális hacktivisták közössége 2022 során koordinált DDoS-támadásokat intézett orosz célpontok ellen.⁴⁰ Bár rövid távon látványos sikereket tudtak felmutatni, és a kezdeményezés hatékony aszimmetrikus választ adott az orosz agresszióra, a jelenség súlyos etikai és jogi kérdéseket vet fel. Az IT Army of Ukraine-hez csatlakozó, Ukrajnán kívüli, nemzetközi önkéntesek az orosz rendszerek elleni támadásokkal valószínűleg bűncselekményt követnek el. Másfelől a nemzetközi hadijog (genfi egyezmények) értelmében a civilek védelmet élveznek, de ha közvetlenül részt vesznek a háborús cselekményekben (márpedig egy infrastruktúra elleni kibertámadás annak minősülhet), elveszíthetik védettségüket és legitim katonai célponttá válhatnak. Ugyanez fenyegeti azokat a civileket, akik az ukrán eVorog alkalmazás használatával segítik az orosz katonai célpontok azonosítását.⁴¹ Maga az eVorog szintén alapvetően civilek által használt komponensekből áll: a végfelhasználó mobiltelefonja, egy Telegram-csatorna és az ukrán elektronikus közszolgáltatásokhoz használt hitelesítési mechanizmus. Ezzel vissza is jutunk oda, hogy ha civil eszközöket használunk katonai célok megvalósítására, akkor a civil infrastruktúrák is katonai célponttá válnak.

A civil–katonai infrastruktúra kapcsolatának tanulságai a jövőre nézve

Az orosz–ukrán háború kiberdimenziója rámutatott a hagyományos védelmi doktrínák újragondolásának szükségességére. Korábban az állam szerepe kizárólagos vagy döntő volt a biztonság garantálásában, azonban a modern konfliktusokban – mint amilyen az orosz–ukrán háború is – ez a megközelítés már nem tartható. Az államnak ki kell alakítania a hatékony együttműködést a nem állami szférával (magánszektor, civil társadalom), mivel a biztonság szavatolása már nem tisztán állami feladat.⁴² Ugyanígy

³⁹ CAVELTY–EGLOFF 2019.

⁴⁰ SOESANTO 2022.

⁴¹ BIRÓ 2025b.

⁴² FARKAS–KELEMEN 2023.

a kritikus infrastruktúrák védelme is civil–katonai együttműködést igényel. A jövő konfliktusaiban a győzelem vagy vereség nem kizárólag a katonai képességeken múlik, hanem azon, hogy egy állam képes-e integrálni civil erőforrásait a védelmi rendszerbe. A konfliktus legfontosabb tanulságait az alábbi három pontban összegezhetjük:

- szervezeti és szabályozási paradigmaváltás;
- kiberreziliencia-építés és közös sérülékenységmentesítés;
- kritikus privát szereplők integrálása a védelmi tervezésbe.

A hibrid fenyegetések korában a polgári és katonai felelősségi körök szigorú szétválasztása biztonsági kockázatot jelent. A háború tapasztalatai alapján újra kell gondolni a védelmi struktúrákat. A védelem nem lehet kizárólag az állam feladata. Ukrajnában a decentralizáltan működő civil szervezetek (NGO-k) és szakmai közösségek sokszor gyorsabban reagáltak a kiberfenyegetésekre és az eszközhiányra, mint a központi bürokrácia. A jövő szabályozásának teret kell engednie az ellenőrzött, de rugalmas civil szakmai részvételnek. A békeidős jogszabályok gyakran akadályozzák az operatív együttműködést (például adatvédelmi korlátok a fenyegetési információk megosztásában). Olyan jogi keretekre van szükség, amelyek krízishelyzetben automatikusan lehetővé teszik a polgári infrastruktúra üzemeltetői és a honvédelmi szervek közötti közvetlen, kétirányú adatcserét.

Mivel a hadsereg a civil hálózatokon „utazik”, a katonai rendszerek biztonsága csak annyira erős, amennyire a civil infrastruktúra leggyengébb láncszeme. A felkészülés során fel kell térképezni a civil és katonai rendszerek közös metszeteit, leggyengébb láncszemeit (*single points of failure*). Nem elegendő a katonai hálózatot védeni; a hadsereg által használt polgári energiaszolgáltató vagy internetszolgáltató rendszerét is katonai szintű védelmi szabványokhoz kell közelíteni. A kettős felhasználású infrastruktúrák fejlesztésekor már a tervezési fázisban figyelembe kell venni a potenciális katonai felhasználásból eredő többletkockázatot.

A Starlink vagy a Microsoft szerepvállalása bizonyította, hogy a globális technológiai vállalatok *de facto* geopolitikai szereplőkké váltak. Az államoknak nem egyszerű beszállítóként, hanem stratégiai partnerként kell tekinteniük ezekre a cégekre. A védelmi tervezésbe be kell vonni a kritikus infrastruktúrát üzemeltető magáncégek képviselőit. A fenyegetésekről szóló hírszerzési információk (*threat intelligence*) megosztását ki kell terjeszteni a megbízható magánszereplőkre is, hiszen gyakran ők észlelik először a hálózataikon a rendellenes aktivitást, amely egy állami szintű támadás előjele lehet.

Az orosz–ukrán háború legátfogóbb tanulsága, hogy a civil infrastruktúrák sebezhetősége csökkenti az állam ellenálló képességét, mivel könnyű célpontot kínál az aszimmetrikus hadviseléshez. Ezzel szemben egy magas rezilienciájú, redundáns és a védelmi szektorral szorosan együttműködő civil infrastruktúra megnehezítheti a támadó dolgát. A jövőben a katonai erő nem értelmezhető a mögötte álló, ellenálló-képes digitális hátszázág nélkül.

Összegzés

Az orosz–ukrán háború elemzése rávilágított arra, hogy a 21. századi fegyveres konfliktusok természete visszafordíthatatlanul megváltozott. A tanulmányban bemutatott esettanulmányok és folyamatok igazolják, hogy a kinetikus és a kiberműveletek szinkronizációja a modern hadviselés alapmegközelítésévé vált. Ez a szoros összehangoltság a gyakorlatban megmutatta, hogy háborús helyzetben megszűnt az éles határvonal a civil és a katonai infrastruktúrák között, a civil szféra veszteségei pedig a hadviselés elkerülhetetlen következményévé váltak.

A technológiai fejlődés és a rendszerek mély integrációja miatt a katonai és civil infrastruktúrák szétválasztása ma már nem csupán elméleti, hanem súlyos gyakorlati nehézségekbe ütközik. A kettős felhasználású eszközök tömeges alkalmazása miatt a civil hálózatok (energia, távközlés) a hadműveletek szerves részévé és ezáltal legitimnek tekinthető célponttá váltak. Ebben a kontextusban a kritikus infrastruktúrák elleni támadások során a kiberműveletek stratégiai jelentősége megkérdőjelezhetetlen: képesek fizikai pusztítás nélkül is megbénítani egy állam védelmi képességeit és társadalmi működését.

A jövő kiberbiztonsági kihívásaira adható válasz kulcsa a szektorközi együttműködés. Az állami monopóliumra épülő védelem már nem elégséges; a nemzeti reziliencia csak a magánszektor, a technológiai szolgáltatók és a kormányzati szervek szoros, bizalmi alapú kooperációjával érhető el.

Végezetül, a hibrid fenyegetések komplexitása miatt felértékelődött a katasztrófavédelem szerepe. Mivel a kibertámadások a civil lakosságot is jelentősen érintő fizikai következményekkel járnak (például áramszünet, fűtés kiesés, ellátási láncok megszakadása), a katasztrófavédelem már nem csupán a természeti csapások kezelője, hanem a hibrid hadviselés okozta társadalmi sokkhatások első számú kezelője. A jövőben a kibervédelem és a polgári védelem (katasztrófavédelem) integrációja jelenti majd a nemzeti biztonság egyik legfontosabb pillérét.

Felhasznált irodalom

- A Decade in the Trenches of Cyberwarfare* (2024). Cyber Diia. Online: <https://nsarchive.gwu.edu/document/32135-30-cyber-diia-decade-trenches-cyberwarfare>
- AMBRUS Éva (2023): *Kiberhadviselési képességek a jelen tükrében*. Budapest: Nemzeti Közszolgálati Egyetem. Online: https://kmdi.uni-nke.hu/document/kdmi-uni-nke-hu/Ambrus_PhD_%C3%A9rtekez%C3%A9s.pdf
- BAKOS Tamás – KOVÁCS Ferenc (2025): Az interdependencia dimenziói és a kritikus szervezetek vizsgálata. *Hadtudomány*, 35(3), 106–119. Online: <https://doi.org/10.17047/HADTUD.2025.35.3.106>
- BÍRÓ Gabriella (2025a): Védelmi innováció az orosz–ukrán háború kiberműveleteiben. *Haditechnika*, 59(kisz.), 111–115.

- BÍRÓ Gabriella (2025b): Az ukrán eVorog chatbot és a Delta rendszer. *Haditechnika*, 59(5), 18–21. Online: <https://honvedelem.hu/kiadvanyok/haditechnika-2025-5.html>
- BOGNÁR Balázs – BONNYAI Tünde szerk. (2019): *Kritikus infrastruktúrák védelme I.* Budapest: Dialóg Campus. Online: https://tudasportal.uni-nke.hu/xmlui/bitstream/handle/20.500.12944/12450/595_kritikus_infrastrukturak_vedelme.pdf?sequence=1
- BURGESS, Matt (2022): A Mysterious Satellite Hack Has Victims Far Beyond Ukraine. *Wired*, 2022. március 23. Online: www.wired.com/story/viasat-internet-hack-ukraine-russia/
- CAVELTY, Myriam Dunn – EGLOFF, Florian J. (2019): The Politics of Cybersecurity: Balancing Different Roles of the State. *St Antony's International Review*, 15(1), 37–57. Online: https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Dunn_Cavelty_Egloff_2019%20STAIR%20Issue%2015.1.pdf
- Cyber Attacks in Times of Conflict* [é. n.]. CyberPeace Institute. Online: <https://cyber-conflicts.cyberpeaceinstitute.org/>
- DEUTSCH, Anthony – BERG, Stephanie van den – PEARSON, James (2024): ICC Probes Cyberattacks in Ukraine as Possible War Crimes, Sources Say. *Reuters*, 2024. június 14. Online: www.reuters.com/world/europe/icc-probes-cyberattacks-ukraine-possible-war-crimes-sources-2024-06-14/
- ESET Research: *Ukraine hit by Destructive Attacks before and during the Russian Invasion with HermeticWiper and IsaacWiper* (2022). ESET. Online: www.eset.com/us/about/newsroom/research/eset-research-ukraine-hit-by-destructive-attacks-before-and-during-the-russian-invasion-with-hermet/?srsltid=AfmBOopiPjnyDqcsp-R5AVqX3bBaryP8zUjiQOXcLzF2OPfEOCRU0-dhd
- European Council (2022): *Russian Cyber Operations Against Ukraine: Declaration by the High Representative on Behalf of the European Union*. Online: www.consilium.europa.eu/en/press/press-releases/2022/05/10/russian-cyber-operations-against-ukraine-declaration-by-the-high-representative-on-behalf-of-the-european-union/
- European Union Agency for Cybersecurity (2025): *ENISA Cybersecurity Threat Landscape Methodology*. Luxembourg: Publications Office of the European Union. Online: <https://doi.org/10.2824/1888892>
- FARKAS Ádám – KELEMEN Roland (2023): *Nemzeti biztonság és kibertér*. Budapest: NMHH. Online: <https://mtmi.hu/files/7ddaa0c7-9a10-4123-af9c-e2d86c49cf30.pdf>
- GÖRGEY Péter (2020): Kibertámadások Ukrajnában: áramszünetek és tanulságok (I. rész). *Elektrotechnika*, 113(9–11), 9–11.
- GREENBERG, Andy (2023): Hacker Group Linked to Russian Military Claims Credit for Cyberattack on Ukrainian Telecom. *Wired*, 2023. december 13. Online: www.wired.com/story/ukraine-kyivstar-soltsepek-sandworm-gru/
- HAIG Zsolt (2018): *Információs műveletek a kibertérben*. Budapest: Dialóg Campus.
- JÓJÁRT Krisztián (2023): *Az orosz katonai gondolkodás 21. századi hadviselés-felfogásának értelmezése*. Budapest: Nemzeti Közszerológati Egyetem. Online: <https://doi.org/10.17625/NKE.2024.014>

- KISS Adrienn (2024): Az orosz–ukrán háború hatása a kritikus infrastruktúrákra – fókuszban az energiaszektor. *Hadmérnök*, 19(3), 183–200. Online: <https://doi.org/10.32567/hm.2024.3.11>
- KOVÁCS László (2018): *A kibertér védelme*. Budapest: Dialóg Campus. Online: www.uni-nke.hu/document/uni-nke-hu/Kov%C3%A1cs%20L%C3%A1szl%C3%B3.pdf
- KRASZNAY Csaba (2022): *Kiberbiztonság a XXI. században*. Budapest: Katonai Nemzetbiztonsági Szolgálat.
- MIRON, Marina – THORNTON, Rod (2024): The Use of Cyber Tools by the Russian Military: Lessons from the War against Ukraine and a Warning for NATO? *Applied Cybersecurity & Internet Governance*, 3(1), 147–169. Online: <https://doi.org/10.60097/ACIG/190142>
- MOYNIHAN, Harriet – WEBB, Philippa – CLOONEY, Amal (2025): *Legal Accountability for Malicious Cyber Operations*. Oxford Institute of Technology and Justice. Online: https://doi.org/10.35489/BSG-OITJ-PB-1_2025-01
- MUHA Lajos (2007): *A Magyar Köztársaság kritikus információs infrastruktúráinak védelme*. PhD-disszertáció. Budapest: Zrínyi Miklós Nemzetvédelmi Egyetem. Online: <https://real-phd.mtak.hu/74/1/1228916.pdf>
- ORBÓK Ákos (2013): A kibertér, mint hadszíntér. *Biztonságpolitika*, 2013, 101–108. Online: https://old.biztonsagpolitika.hu/documents/1375084295_Orbok_Akos_A_kibert%C3%A9r_mint_hadszinter_-_biztonsagpolitika.hu.pdf
- Reuters (2022): Satellite Outage Knocks out Thousands Of Enercon's Wind Turbines. *Reuters*, 2022. február 28. Online: www.reuters.com/business/energy/satellite-outage-knocks-out-control-enercon-wind-turbines-2022-02-28/
- RID, Thomas (2013): *Cyber War Will Not Take Place*. Oxford: Oxford University Press.
- ROULETTE, Joey – BRYAN-LOW, Cassell – BALMFORTH, Tom (2025): Musk Ordered Shutdown of Starlink Satellite Service as Ukraine Retook Territory from Russia. *Reuters*, 2025. július 25. Online: www.reuters.com/investigations/musk-ordered-shutdown-starlink-satellite-service-ukraine-retook-territory-russia-2025-07-25/
- SCHMITT, Michael N. szerk. (2017): *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge – New York: Cambridge University Press. Online: <https://doi.org/10.1017/9781316822524>
- SMITH, Brad (2022): *Digital Technology and the War in Ukraine*. Microsoft on the Issues. Online: <https://blogs.microsoft.com/on-the-issues/2022/02/28/ukraine-russia-digital-war-cyberattacks/>
- SOESANTO, Stefan (2022): *The IT Army of Ukraine. Structure, Tasking, and Eco-System*. Zürich: Center for Security Studies (CSS). Online: <https://doi.org/10.3929/ethz-b-000552293>
- VERBRUGGEN, Yola (2023): Cybercrimes under Consideration by the ICC. *International Bar Association*, 2023. október 13. Online: www.ibanet.org/cybercrimes-under-consideration-by-the-ICC

Jogi források

2024. évi LXXXIV. törvény a kritikus szervezetek ellenálló képességéről
Az Európai Parlament és a Tanács (EU) 2022/2557 irányelve (2022. december 14.)
a kritikus szervezetek rezilienciájáról és a 2008/114/EK tanácsi irányelv hatályon
kívül helyezéséről (EGT-vonatkozású szöveg). Online: <https://eur-lex.europa.eu/eli/dir/2022/2557/oj/hun>
Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to
the Protection of Victims of International Armed Conflicts (Protocol I), 8 June
1977. Online: <https://ihl-databases.icrc.org/en/ihl-treaties/api-1977>
Про хмарні послуги [é. n.]. Online: <https://zakon.rada.gov.ua/go/2075-20>