Hadtudományi Szemle
19. évfolyam (2026) 2. szám 171–189. • DOI: 10.32563/hsz.2026.2.12

Biró Gabriella[1]

A politika folytatása más eszközökkel?

Stratégiai aszimmetriák a Geraszimov-doktrína és az EU Cyber Diplomacy Toolbox között

Continuing the Same Policy with Different Tools?

Strategic Asymmetries between the Gerasimov Doctrine and the EU Cyber Diplomacy Toolbox

Absztrakt

A tanulmány azt vizsgálja, hogyan viszonyul egymáshoz a két domináns, de jellegében eltérő keretrendszer, az orosz és az európai megközelítés a kibertérben zajló konfliktusokhoz. Ennek érdekében a szerző összehasonlítja az Oroszországi Föderáció részéről Geraszimov-doktrína néven elhíresült cikk és az Európai Unió Kiberdiplomáciai eszköztára (Cyber Diplomacy Toolbox) által képviselt megközelítéseket. Míg az oroszok proaktívan ötvözik a konfliktus során a különböző katonai és nem katonai műveleteket, addig az Európai Unió reaktív megközelítést alkalmaz. A két rendszer teljesen eltérő időtávon működik, a tanulmány példákon keresztül bemutatja, hogy a kibertérben zajló orosz műveletek napok alatt megvalósulhatnak, ezzel szemben az EU-eszközkészlet tényleges alkalmazása a gyakorlatban több évet is igénybe vehet. A két megközelítés találkozása a kibertérben ezért a stratégiai egyensúly hiányát eredményezi, ami hosszú távon mindenképp megoldandó kérdés az Európai Unió számára. A tanulmány végül javaslatokat fogalmaz meg az EU-s eszközkészlet és válaszmechanizmus fejlesztésére.

Kulcsszavak: kiberdiplomácia, Európai Unió, Oroszországi Föderáció, Geraszimov-doktrína

[1] Doktori hallgató, Nemzeti Közszolgálati Egyetem Katonai Műszaki Doktori Iskola.

Abstract

In the article the relationship between the two dominant but different frameworks, the Russian and European approaches to conflicts in cyberspace, are examined. To this end, the approaches represented by the article known as the Gerasimov Doctrine on the part of the Russian Federation and the European Union's Cyber Diplomacy Toolbox are compared. While the Russians proactively combine various military and non-military operations during conflicts, the European Union takes a reactive approach. The two systems operate on completely different time scales: the article demonstrates through examples that Russian operations in cyberspace can be carried out in a matter of days, whereas the actual implementation of the EU's toolkit may take several years in practice. The convergence of the two approaches in cyberspace therefore results in a lack of strategic balance, which is an issue that the European Union will have to resolve in the long term. Finally, the article makes recommendations for improving the EU's toolkit and response mechanism.

Keywords: cyber diplomacy, European Union, Russian Federation, Gerasimov doctrine

Bevezetés

Az elmúlt évtizedekben a kibertér szerepe radikálisan növekedett az államközi konfliktusokban. Elég csak a 2007-es Észtország elleni orosz kibertámadásra, a 2008-as grúz–orosz háború kiberműveleteire[2] vagy a 2010-ben azonosított, iráni nukleáris létesítményeket célzó Stuxnetre gondolni.[3] A 2022-es Ukrajna elleni teljes körű orosz inváziót is átfogó kiberműveletek előzték meg és kísérik a cikk írásakor is.[4] Ugyanakkor a kibertérben folytatott műveletek a hadviselés kockázatkerülő megközelítését jelentik,[5] mivel nem okvetlenül járnak fizikai konfrontációval, tényleges harctéri találkozással. Ennek megfelelően a 21. századi konfliktusok jellege is megváltozott; a hagyományos háború és béke bináris logikája már nem alkalmas a valóság leírására.

Jelen tanulmány azt vizsgálja, hogyan viszonyul egymáshoz két domináns, de jellegében eltérő stratégiai keretrendszer: az orosz offenzív hibrid megközelítés és az európai defenzív normatív eszköztár. Az orosz stratégiai gondolkodást a Geraszimov-doktrína néven elhíresült, Valerij Geraszimov vezérkari főnök által jegyzett cikk[6] alapján vizsgáljuk, míg az Európai Unió megközelítését a kiberkonfliktusok kezelésére kifejlesztett EU Cyber Diplomacy Toolbox (CDT) (kiberdiplomáciai eszközkészlet) képviseli. Bár mind a Geraszimov-doktrína, mind az EU Cyber Diplomacy Toolbox elszakad a hagyományos kinetikus hadviseléstől, alapvető stratégiai aszimmetria feszül köztük: az orosz megközelítés a konfliktust állandósult állapotként és eszközként (proaktív), míg az EU a kibertér stabilitását védendő értékként, a fellépést pedig válaszlépésként (reaktív) kezeli. A tanulmányban arra a kutatási kérdésre keressük a választ, hogy milyen strukturális

[2] Krasznay 2023: 29.
[3] Kovács 2023.
[4] Cyber Diia 2024.
[5] Boda 2024.
[6] Герасимов 2013.

különbségek azonosíthatók a Geraszimov által összegzett orosz hibrid hadviselés és az EU kiberdiplomáciai eszközkészlete között, és ezek az eltérések milyen gyakorlati következményekkel járhatnak, ha a két megközelítés szembekerül egymással.

A tanulmányban először áttekintjük az elméleti hadtudományi kereteket és előzményeket, amelyek kontextusában megjelennek a kiberműveletek a 21. században. Ezután bemutatjuk az elemzés módszertanát és a vizsgált hivatkozások kiválasztásának szempontrendszerét. Az orosz és EU-s megközelítések azonos szerkezetben történő bemutatása után következik a két vizsgált rendszer összehasonlítása, majd a tanulmány lezárásaként összegezzük a következtetéseket, és javaslatokat fogalmazunk meg az EU eszközkészletének és reagálóképességének fejlesztésére.

A politika folytatása az ötödik dimenzióban: Clausewitz a 21. században

Carl von Clausewitz gyakran emlegetett klasszikus tétele szerint „a háború a politika folytatása más eszközökkel". A vesztfáliai rendszerben[7] és a hagyományos kinetikus hadviselés korában ez a tétel egyfajta eszkalációt feltételezett: létezett a diplomácia ideje, és amikor az kudarcot vallott, akkor következnek a fegyverek. A béke és a háború jól elkülöníthető, bináris állapotok voltak, a felek mindig pontosan tudták, hogy éppen hadban állnak-e. A 21. század digitális forradalma, a kibertér önálló hadszíntérré válása és államközi konfliktusokban betöltött szerepének drasztikus növekedése azonban alapjaiban írta át ezt a képletet.[8]

A modern konfliktusokban a diplomácia eszköztára és a fegyveres konfliktus közötti éles határvonal elmosódott. A klasszikus értelmezésben van egy pont, ahol a diplomácia véget ér, és a fegyverek veszik át a szót. A modern konfliktusokban azonban ez a határvonal megszűnik. A diplomácia és az erőszak alkalmazása *(use of force)* a kiberműveletek révén egyszerre van jelen.[9] Egy kiberképességekkel rendelkező állam képes arra, hogy egyfelől diplomáciai tárgyalásokat folytasson, miközben a másik oldalon – a kibertér láthatatlanságába burkolózva – agresszív műveleteket hajtson végre partnere kritikus infrastruktúrája ellen, vagy intenzív dezinformációs kampányt folytasson. A kibertérben a „fegyver" fogalma is jelentősen kitágult:[10] már nem csupán fizikai pusztításra alkalmas eszközöket értünk alatta, hanem adatokat vagy kódokat is. Ezzel összhangban a nemzetközi jog kiberműveletekkel kapcsolatos alkalmazhatóságát leíró *Tallinn Manual 2.0* definíciója szerint a kiberfegyverek „olyan kiberhadviselési eszközök, amelyeket személyek sérülésének, illetve halálának, valamint tárgyak károsodásának, illetve megsemmisítésének érdekében használnak, arra hoztak létre vagy terveztek használni, azaz amelyek a kiberművelet támadásként való minősítéséhez szükséges következményekkel járnak".[11] Ez a definíció

[7] A vesztfáliai rendszer az a világrend, amelyben a világ egymástól független, szuverén nemzetállamokra oszlik, amelyek tiszteletben tartják egymás határait és jogi egyenlőségét.

[8] Nagy 2018.

[9] Schmitt – NATO Cooperative Cyber Defence Centre of Excellence 2017: fej. 14.

[10] Kovács 2023: 131–136.

[11] „cyber weapons are cyber means of warfare that are used, designed, or intended to be used to cause injury to, or death of, persons or damage to, or destruction of, objects, that is, that result in the consequences required for qualification of a cyber operation as an attack" (a magyar szöveg a szerző saját fordítása). Schmitt – NATO Cooperative Cyber Defence Centre of Excellence 2017: r. 103.

elég tág és technológiasemleges ahhoz, hogy a gyakorlatban jól használható legyen annak megítélésére, mikor történt fegyveres támadás a kibertérben.

A kiberfegyverek megjelenésének új realitása azt eredményezte, hogy a háború többé nem írható le egyszerű „van" vagy „nincs" (bináris) állapottal. Ehelyett folyamatos intenzitási spektrumról beszélhetünk, amelynek minden fokozatánál szerep jut a kiberműveleteknek, ahogy az 1. ábra szemlélteti. Boda Mihály a konfliktusspektrumot a következőképpen írja le:

> „Az állami konfliktusok típusai így egy spektrumon helyezhetők el. A direkt háború és a pozitív béke jelezte két véglet között található a pozitív békéhez közelebb a forró béke és a direkt háborúhoz közelebb a hidegháború. A hibrid háború a forró békére jellemző államközi konfliktus."[12]

Ezt a szemléletváltást tükrözi az orosz katonai gondolkodásban a Geraszimov által leírt eszkalációs folyamat vagy a nyugati stratégiákban és a CDT logikájában megjelenő fokozatosság elve is. A felek célja immár nem feltétlenül a nyílt hadüzenet, hanem a mozgástér maximalizálása ezen a skálán. A modern konfliktusok döntő többsége az úgynevezett „szürkezónában" zajlik, amelyben a műveletek intenzitása tudatosan a nyílt fegyveres konfliktus küszöbe alatt marad. A támadók gondosan adagolják az agressziót, ügyelve arra, hogy ne lépjék át azt a vörös vonalat, amely a NATO 5. cikkelyének[13] vagy az EU Lisszaboni Szerződése 42.7-es cikkelyének[14] aktiválását vonná maga után. Ugyanakkor megjelenik az attribúció (a támadó azonosítása) dilemmája is, mert a kibertérben nehezebb megfelelő bizonyossággal megállapítani, kinek tulajdonítható az adott támadás; ennek ellenére a politikai célok bizonyos esetekben akkor is megkívánják a nyilvános attribúciót, ha a bizonyítékok technikai elemzése nem nyújt százszázalékos bizonyítékot az elkövető kilétét illetően.

A jelenlegi nemzetközi gyakorlatban elválik egymástól a technikai, politikai és jogi attribúció. A Palgrave kiberdiplomáciáról szóló kézikönyve szerint:

> „A technikai felelősségre vonás egy eszközre vagy egy bizonyos rendszerre utalhat, de nem ad információt a szélesebb kontextusról vagy a gép mögött álló tényleges személyről. A politikai felelősségre vonás egy külpolitikai döntés, és itt lényegében azt jelenti, hogy nyilvánosan felelősségre vonnak valakit egy kiberműveletért (vagy annak elmulasztásáért). A jogi felelősségre vonás azonban, amely jogi célokat szolgál és nem feltétlenül jár együtt politikai felelősségre vonással vagy a bizonyítékok nyilvános közzétételével, magában foglalja az állam és a jogsértő cselekményt elkövető személy(ek) közötti kapcsolat jellemzését."[15]

[12] Boda 2023: 26.
[13] NATO 2025.
[14] European Union 2016.
[15] „Technical attribution may point to a device or a certain system, yet can be uninformative of the broader context or actual person behind the machine. Political attribution is a foreign policy decision and here essentially means publicly assigning blame for a cyber operation (or perhaps omission thereof). Legal attribution, however, which serves legal purposes and need not be accompanied by political attribution nor public disclosure of evidence, involves characterization of the link between the State and the person(s) performing the wrongful act" (a magyar szöveg a szerző saját fordítása). Christou et al. 2025: 93.

1. ábra: A konfliktus növekvő szintjei a nem erőszakostól a stratégiai fegyverekig
Forrás: a szerző szerkesztése a National Intelligence Council 2021: 104. alapján, Nano Banana Pro mesterséges intelligencia felhasználásával

A fogalmi keretek tisztázása elengedhetetlen ennek a komplexitásnak a megértéséhez, valamint az orosz és EU-s megközelítés leírásához és megértéséhez. A modern államközi konfliktusokban a hibrid hadviselés eszköztára (az információs hadviseléstől a kritikus infrastruktúrák megtámadásáig) keveredik a kiberdiplomácia új formáival. Ebben a környezetben az államok gyakran proxy (közvetítő) szereplőket – hacktivistákat, bűnözői csoportokat – alkalmaznak,[16] hogy fenntarthassák a „hihető tagadás" *(plausible deniability)* lehetőségét. Így a politika folytatása más eszközökkel ma már nem a harcmezőn, hanem a laptopokon és adatközpontokban, a béke és a háború közötti elmosódott határmezsgyén zajlik.

Módszertan és elemzési keretek

A tanulmány módszertani gerincét a kvalitatív összehasonlító szakpolitikai elemzés adja. A kutatás célja két, alapvetően eltérő logikára épülő stratégiai keretrendszer – az orosz „új generációs hadviselés" elméleti alapvetéseként kezelt Geraszimov-doktrína, illetve az Európai Unió normatív válaszlépéseit rögzítő Cyber Diplomacy Toolbox szisztematikus összevetése. Az elemzés a feltárt aszimmetriákat öt rögzített dimenzió mentén vizsgálja:

1. célok és eszközök;
2. intézményi keretek;
3. idősík: tempó és reakcióidő;
4. az attribúció követelményrendszere és
5. az eszkaláció kezelése.

[16] Krasznay 2023.

A fenti szempontrendszer minden egyes eleme külön-külön is alkalmas lenne arra, hogy önálló tanulmányban vizsgáljuk, mivel azonban a jelen tanulmány célja az átfogó összehasonlítás, ezért a fogalmak meghatározásával és vizsgálatával csak a szükséges mértékig foglalkozunk.

Mind az EU kiberbiztonsági és kibervédelmi eszközkészlete, mind az orosz katonai gondolkodás folyamatosan fejlődik, újabb és újabb publikációk és szabályozások születnek, azonban a jelen elemzés tudatosan csak az EU kiberdiplomáciai eszköztárára és a Geraszimov-doktrína által leírt eszközökre fókuszál. Ezek tágabb kontextusa és az EU, illetve az Oroszországi Föderáció további kibertérben alkalmazható eszközei és válaszintézkedései kívül esnek jelen tanulmány hatókörén.

Az elemzés alapját változatos források adják: a primer dokumentumok (hivatalos uniós kommunikáció és elemzések), valamint a releváns hazai és nemzetközi publikációk mellett a téma jellegéből adódóan megkerülhetetlenek az internetről származó források. Mostanra az internet, a szervezetek honlapjai és közösségimédia-csatornái a hivatalos kommunikáció széles körben elfogadott formáivá váltak, ezért bizonyos esetekben ezek a források vannak a legközelebb az információ eredetéhez, ugyanakkor a tanulmányban csak olyan internetes forrásokat használtunk, amelyek vagy az érintett szervezet/intézmény (például az EU vagy egyes kutatóintézetek) elsődleges kommunikációs csatornájának számítanak, vagy megbízhatónak számító hírportálok, akik elsőként, közvetlen forrásból számolnak be bejelentésekről, döntésekről.

A kutatás korlátjaként rögzítendő, hogy az elemzés kizárólag nyílt forrású adatokra támaszkodik; a kiberkonfliktusok természetéből adódóan a minősített információkhoz való hozzáférés hiánya miatt az esettanulmányokhoz kapcsolódó részletes technikai, jogi vagy politikai attribúció vizsgálata nem képezi a tanulmány tárgyát. Ugyanígy a kiberdiplomácia általános fogalmi meghatározása is túlmutat a jelen tanulmány keretein.

Az orosz megközelítés: a Geraszimov-doktrína

A modern konfliktusok orosz megközelítésének megértéséhez megkerülhetetlen Valerij Geraszimov orosz vezérkari főnök 2013-ban publikált, *A tudomány értéke az előrelátásban (Ценность науки в предвидении)*[17] című elhíresült cikke. Bár Geraszimov eredetileg a nyugati színes forradalmak működési mechanizmusát elemezte, írása nyugaton az orosz „új generációs hadviselés" (*new generation warfare,* NGW) alapvetésévé vált. A Geraszimov-doktrína fogalmát Mark Galeotti alkotta meg,[18] majd néhány év múlva blogbejegyzésben fejtette ki, hogy átértékelte a korábbi elemzését, és már bánja, hogy új fogalmat alkotott.[19] Ennek ellenére a Geraszimov-doktrína megmaradt a köztudatban, és bár az orosz katonai gondolkodásban nem volt előzmény nélküli,[20] olyan tömör és átfogó összefoglalást ad a modern orosz megközelítésről, hogy továbbra is a leggyakrabban idézett forrás maradt. Emellett Geraszimov cikke rendkívül jól „öregszik", az általa leírt módszerek az azóta eltelt több mint egy évtizedben

[17] Герасимов 2013.
[18] Galeotti 2014.
[19] Galeotti 2018.
[20] Jójárt 2024.

pontosan megfigyelhetők az orosz katonai műveletekben a Krím félszigeten, Donbaszban vagy Szíriában.

A Geraszimov-doktrína központi tézise szakít a hagyományos katonai gondolkodással: a stratégiai cél immár nem a fizikai területfoglalás, az ellenfél erőforrásainak megszerzése vagy az ellenséges haderő megsemmisítése a harcmezőn, hanem az ellenfél döntéshozatali mechanizmusának megbénítása és a célország belső társadalmi-politikai destabilizációja. Az információs hadviselés ilyetén alkalmazásának már korábban is voltak hagyományai az orosz katonai gondolkodásban,[21] de az internet és különösen a közösségi média és terjedése új lehetőségeket teremtett ezen a területen.

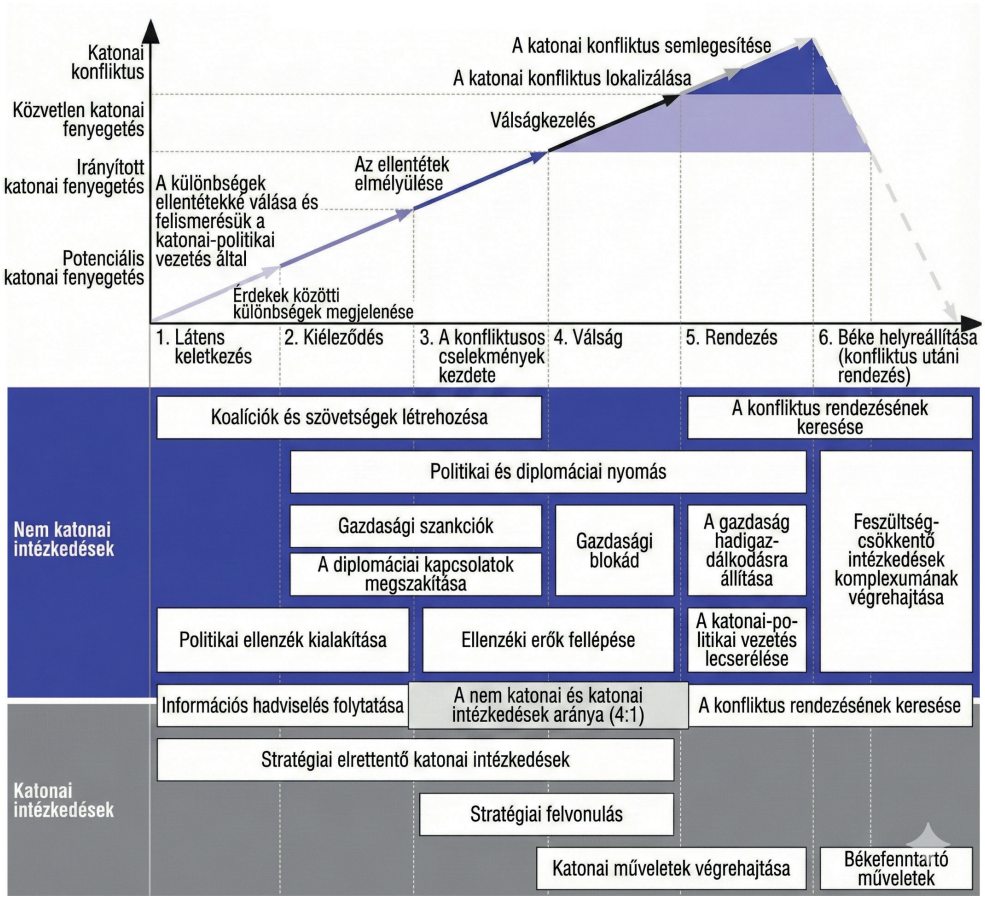
Ebben az aszimmetrikus megközelítésben a katonai és nem katonai eszközök aránya jelentősen eltolódott. Geraszimov híres képlete szerint a modern konfliktusokban 4:1 arányban dominálnak a nem katonai – kiber-, információs, gazdasági és diplomáciai – eszközök a hagyományos fegyverekkel szemben, ahogy cikkének központi eleme, a konfliktus kialakulásának fő szakaszait és az eszkaláció lépéseit összefoglaló ábra is szemlélteti (2. ábra).

Ebben a felállásban a kibertér már nem csupán a hírszerzés (kiberkémkedés) vagy dezinformáció terepe, hanem offenzív fegyverként jelenik meg. A stratégia legfontosabb eleme a béke és a háború közötti átmeneti állapot állandósítása. A cél a folyamatos nyomásgyakorlás fenntartása anélkül, hogy átlépnék a nyílt hadviselés küszöbét. Ennek kulcsa a „hihető tagadás" *(plausible deniability)* képessége: Oroszország hagyományosan a *maszkirovka* (megtévesztés) eszközeivel, proxy szereplők és függetlennek tűnő hackercsoportok mögé bújva hárítja el a felelősséget. Ezzel szemben az Európai Unió és a NATO válaszmechanizmusa a lassú és megalapozott technikai, jogi és politikai attribúcióra[22] (a támadó hivatalos azonosítására) épül, ami jelentős hátrányt jelent a gyorsan reagáló, anonimitásba burkolódzó támadóval szemben.

A Geraszimov-féle modellben a különböző hibrid műveletek nem elszigetelten, hanem integráltan jelennek meg: az információs, pszichológiai, kiber-, politikai és rejtett katonai eszközök egységes műveleti terv részei. Ennek köszönhetően a modell intézményi háttere is összetett, a különböző civil és katonai szervezetek, médiumok összehangolt működését igényli, ami az Oroszországi Föderáció erősen központosított hatalmi struktúrájában megoldható feladat.

A doktrína egyik legfontosabb alapelve a proaktivitás. A konfliktusformálás nem a hadüzenettel kezdődik, a műveletek gyakran már évekkel a hivatalos ellenségeskedés (vagy annak látszata) előtt elindulnak, előkészítve a terepet azzal, hogy az ellenséget már a harc kezdete előtt cselekvésképtelenné teszik. Ebből a szempontból Geraszimov modelljének idősíkja összevethető az EU-eszköztár „tempójával", mivel ott is többéves időtávokról beszélhetünk. Az egyes kibertámadások időbeli megvalósíthatósága viszont nagyon eltérő: az egyszerű elosztott szolgáltatásmegtagadásra irányuló támadások (*distributed denial of service,* DDoS) gyorsan (akár órák alatt) kivitelezhetők, míg a szofisztikált, folyamatosan fennálló fejlett támadások (*advanced persistent threat,* APT) többnyire hónapokat vesznek igénybe, de akár évekig is elhúzódhatnak.

[21] Расторуев 1998; Biró 2025.
[22] Brunner 2025.



2. ábra: A konfliktus kialakulásának fő szakaszai és az eszkaláció lépései
Forrás: a szerző szerkesztése Герасимов 2013. eredeti ábrája alapján, Nano Banana Pro mesterséges intelligencia felhasználásával

A negyedik összehasonlítási dimenzió, az attribúció követelményrendszere csak korlátozottan releváns a Geraszimov-doktrína esetében a megközelítés proaktivitása miatt. Támadó félként nincs szükség attribúcióra, de ha mégis történik ilyen, az többnyire politikai attribúció, viszont nem korlátozódik a kibertér eseményeire. Például 2025. december 29-én Oroszország Putyin elnök Valdaiban lévő rezidenciája elleni dróntámadással vádolta meg Ukrajnát.[23]

A konfliktus eszkalációjának lépései és folyamata jól megfigyelhető a 2. ábra felső részében. A fegyveres konfliktus küszöbe ugyan explicit módon nem jelenik meg a Geraszimovtól származó feliratokban, de a színezés (amely megfelel az orosz eredetinek) kiemeli, hogy a 4., 5. és 6. szakaszban történnek aktív katonai (kinetikus)

[23] Russian Offensive Campaign Assessment 2025.

műveletek. Az ezekkel kapcsolatos döntéseket vélhetően a katonai vezetés hozza meg, bár erre nem tér ki Geraszimov cikke.

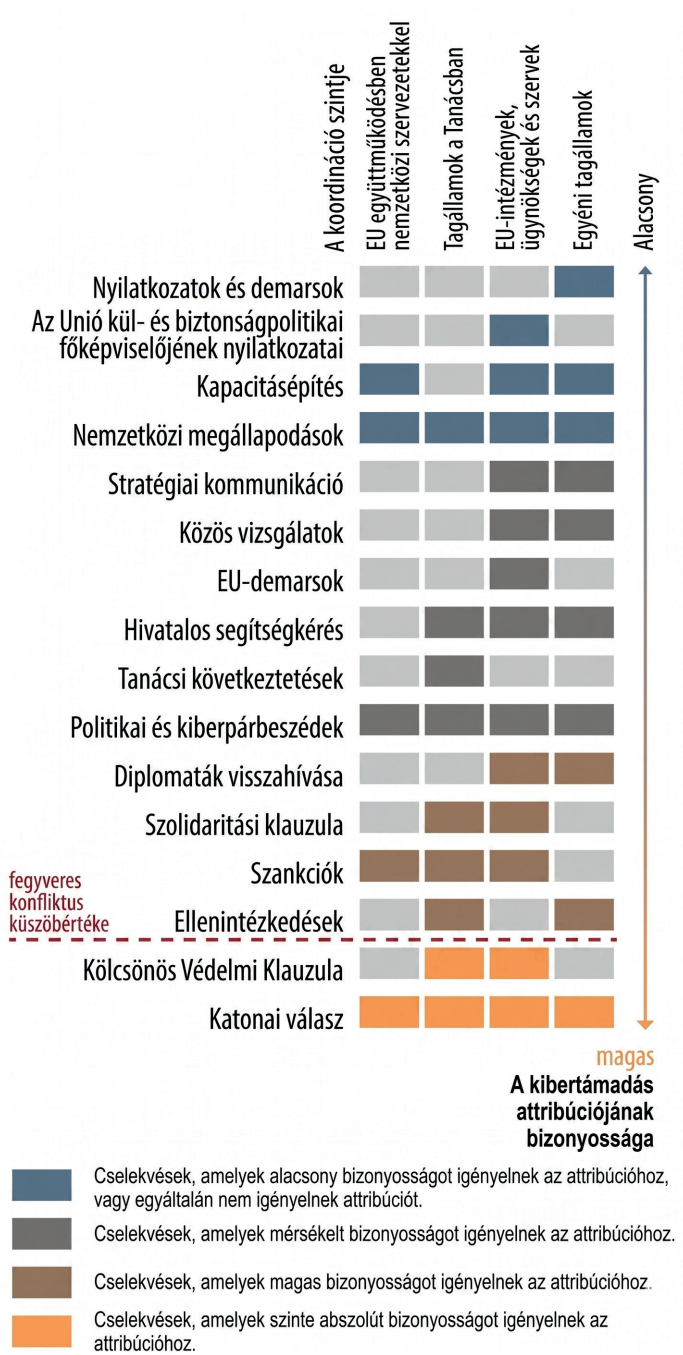
Az Európai Unió megközelítése: a Kiberdiplomáciai Eszköztár

Míg a Geraszimov-doktrína által fémjelzett orosz megközelítés a kiszámíthatatlanságra és a határok elmosására épít, az Európai Unió stratégiai válasza a rendteremtés igényéből fakad. Az EU a kibertérben is „normatív hatalomként" definiálja önmagát:[24] célja a szabályalapú nemzetközi rend kiterjesztése a digitális dimenzióra, a jogállamiság érvényesítése és a stabilitás megőrzése. Ennek a törekvésnek a kibertérben legfontosabb operatív keretrendszere az úgynevezett Kiberdiplomáciai Eszköztár (Cyber Diplomacy Toolbox, CDT).

Az Európai Unió 2017 júniusában hozott döntést a CDT-keretrendszer kidolgozásáról,[25] hogy egységes diplomáciai választ tudjon adni a rosszindulatú kibertevékenységekre, elmozdulva a pusztán technikai védekezéstől a koordinált politikai fellépés felé. Az eszköztár célja a konfliktusok megelőzése, az elrettentés és a stabilitás fenntartása a kibertérben különféle diplomáciai eszközökkel, a nyilatkozatoktól a szankciókig.[26] Az eszköztár fejlődésének következő fontos lépése 2019 májusa volt, amikor az EU 2019/796 rendelete[27] révén létrehozott egy célzott szankciórendszert, amely lehetővé tette korlátozó intézkedések bevezetését a támadások elkövetőivel szemben. Ennek keretében az Unió vagyoni eszközök befagyasztásával és beutazási tilalommal sújthatja a felelős egyéneket és szervezeteket. Az első éles alkalmazás 2020 júliusában volt, amikor az EU szankciókat (beutazási tilalmat és pénzeszközök befagyasztását) vetett ki hat személyre és három szervezetre a WannaCry, NotPetya és az Operation Cloud Hopper támadások miatt.[28] Az eszköztár azóta több bővítésen esett át, és az EU kiberbiztonsági stratégiájának alapkövévé vált, jelezve, hogy a kibertérben elkövetett agresszió nem marad következmények nélkül. 2023-ban felülvizsgálták, és az EU-tagállamok számára a CDT használatával kapcsolatos iránymutatást is kiadott az EU.[29]

A CDT alapvető célja nem a konfliktus eszkalálása, hanem a nemzetközi jog érvényesítése és a kibertér stabilitásának védelme kollektív diplomáciai válaszlehetőségek révén. Az eszköztár széles spektrumon mozog: a preventív intézkedésektől és a nem nyilvános diplomáciai figyelmeztetésektől *(demars)* kezdve a nyilvános elítélésen át egészen a korlátozó intézkedésekig, vagyis a célzott szankciókig terjed, ahogy azt a 3. ábra szemlélteti.

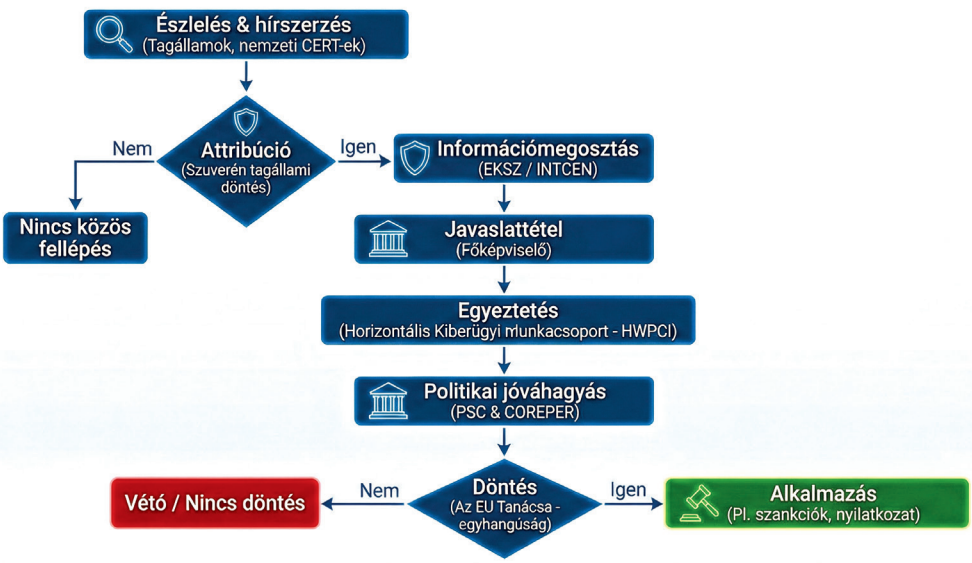
[24] Manners 2002.
[25] European Council 2017.
[26] Moret–Pawlak 2017.
[27] Council Regulation (EU) 2019/796 of 17 May 2019 Concerning Restrictive Measures against Cyber-Attacks Threatening the Union or Its Member States.
[28] European Council 2020a.
[29] General Secretariat of the Council 2023.



3. ábra: Kiberdiplomáciai eszközök és az attribúció bizonyossága
Forrás: a szerző szerkesztése Moret–Pawlak *2017 alapján, Nano Banana Pro mesterséges intelligencia használatával*

A CDT rendszerének logikája azonban alapvetően eltér az ellenfelekétől: reaktív természetű, nincsenek benne offenzív eszközök. Míg a hibrid hadviselés proaktívan formálja a konfliktust, az EU mechanizmusa csak akkor lép életbe, ha a normaszegés vélelmezhető vagy már megtörtént és igazolható. A stratégiai cél itt elsősorban az elrettentés *(deterrence),* nem pedig az ellenfél akaratának aktív megtörése vagy kényszerítése *(compellence).*[30] Ez a reaktív hozzáállás azonban komoly kihívásokkal szembesül az attribúció kérdésében, hiszen csak azzal a támadóval szemben alkalmazhatók az eszközök, akit sikerült megfelelő bizonyossággal azonosítani.

Az Európai Unióban a támadás forrásának megnevezése nem pusztán a támadás technikai részleteinek felderítése, hanem szuverén politikai döntés. A kiberbiztonsági szakértők hiába szolgáltatnak megdönthetetlen technikai bizonyítékokat *(forensics)* egy támadás eredetéről, ez önmagában nem elég a szankciók kivetéséhez. A tagállamoknak politikai szinten kell konszenzusra jutniuk arról, hogy nyilvánosan megvádoljanak egy másik államot (például Oroszországot vagy Kínát). Ez a politikai attribúció lassú és körülményes folyamat, amely éles ellentétben áll az autoriter ellenfelek parancsnoki láncának gyorsaságával és rugalmasságával.[31]



4. ábra: Az EU döntési mechanizmusa a CDT alkalmazása során
Forrás: a szerző szerkesztése Nano Banana Pro mesterséges intelligenciával

Az intézményi keretek szempontjából ezt a nehézkességet tovább fokozzák az Európai Unió strukturális korlátai. A 27 tagállam kiberképességei, fenyegetettség-érzékelése, jogi

[30] Míg az elrettentés *(deterrence)* célja a *status quo* fenntartása egy még meg nem történt, nemkívánatos cselekvés megakadályozásával, addig a kényszerítés *(compellence)* aktív nyomásgyakorlással igyekszik elérni a *status quo* megváltoztatását, rábírva a másik felet egy cselekvés végrehajtására vagy egy folyamatban lévő tevékenység beszüntetésére.
[31] Molnár–Molnár 2022.

és politikai kultúrája rendkívül eltérő. Ami Észtország vagy Lengyelország számára egyértelmű nemzetbiztonsági fenyegetés, az gyakran egy másik tagállam számára csupán távoli technikai incidens. A CDT alkalmazása a Közös Kül- és Biztonságpolitika (KKBP) (Common Foreign and Security Policy, CFSP) keretein belül történik. Ez meghatározza az intézményi szereplőket és a döntéshozatali mechanizmust is, amelyet a 4. ábra szemléltet. Az uniós intézményrendszer (az Európai Külügyi Szolgálat [EKSZ], European External Action Service [EEAS], az EKSZ-hez tartozó Hírszerzési Elemző Központ [INTCEN], az ENISA – az EU kiberbiztonsági ügynöksége – vagy a CERT-EU eseménykezelő központ) szolgáltatja a döntéshozatalhoz szükséges adatokat, elemzéseket és koordinálja az információmegosztást. Ha a Politikai és Biztonsági Bizottságban (Political and Security Committee, PSC) megvan az egyetértés, az ügy felmegy a nagyköveti szintre (COREPER), majd a Miniszterek Tanácsa elé.

1. táblázat: Az Uniót vagy annak tagállamait fenyegető kibertámadások elleni korlátozó intézkedésekről szóló határozatok

Döntés dátuma	Döntés hivatkozása	Szankcionáltak száma	Szankció tartalma	Szankció oka (kibertámadás neve/célpontja)
2020. július 30.	A Tanács (KKBP) 2020/1127 határozata[32]	6 személy 3 szervezet	Vagyoni eszközök befagyasztása, beutazási tilalom, pénzeszközök rendelkezésre bocsátásának tilalma	WannaCry, NotPetya, Operation Cloud Hopper (ipari kémkedés), OPCW elleni kísérlet (Hága)
2020. október 22.	A Tanács (KKBP) 2020/1537 határozata[33]	2 személy 1 szervezet	Vagyoni eszközök befagyasztása, beutazási tilalom	A Bundestag elleni támadás (a német szövetségi parlament informatikai rendszere ellen)
2024. június 24.	A Tanács (KKBP) 2024/1779 határozata[34]	6 személy	Vagyoni eszközök befagyasztása, beutazási tilalom	*Ransomware* kampányok (Conti, Trickbot), Wiper-támadások (WhisperGate) Ukrajna ellen, EU-s tagállamok elleni kémkedés/adathalászat
2025. január 27.	A Tanács (KKBP) 2025/171 határozata[35]	3 személy	Vagyoni eszközök befagyasztása, beutazási tilalom	Észtország elleni támadások (Gazdasági és Kommunikációs Minisztérium, Szociális Minisztérium, Külügyminisztérium ellen) – GRU 29155-ös egység tisztjei

Forrás: a szerző szerkesztése

[32] Council Decision (CFSP) 2020/1127 of 30 July 2020 Amending Decision (CFSP) 2019/797 Concerning Restrictive Measures against Cyber-Attacks Threatening the Union or Its Member States.

[33] Council Decision (CFSP) 2020/1537 of 22 October 2020 Amending Decision (CFSP) 2019/797 Concerning Restrictive Measures against Cyber-Attacks Threatening the Union or Its Member States.

[34] Council Decision (CFSP) 2024/1779 of 24 June 2024 Amending Decision (CFSP) 2019/797 Concerning Restrictive Measures against Cyberattacks Threatening the Union or Its Member States.

[35] Council Decision (CFSP) 2025/171 of 27 January 2025 Amending Decision (CFSP) 2019/797 Concerning Restrictive Measures against Cyber-Attacks Threatening the Union or Its Member States.

A hatáskörök töredezettsége és a döntéshozatal lassúsága miatt az EU gyakran lépéshátrányba kerül a proaktív, központosítottan irányított támadókkal szemben. Például a német Bundestagot ért 2015-ös kibertámadások kapcsán Németország 2020 júniusában kezdeményezett szankciókat,[36] amelyek végül 2020 októberében léptek életbe.[37] Az Észtország elleni 2020-as sorozatos kibertámadások miatt 2025 januárjában döntött az EU a CDT által definiált szankciók alkalmazásáról három orosz állampolgárral szemben.[38] Jelenleg 17 személy és 4 szervezet ellen vannak érvényben szankciók a CDT keretében hozott döntések alapján.[39] A szankciós döntések indokát szolgáltató eseményektől (kibertámadásoktól) jellemzően 2–5 év telt el a szankciós döntés megszületéséig. Az eddigi döntéseket az 1. táblázat foglalja össze.

Stratégiai aszimmetriák az orosz és az EU-s megközelítés között

Ha egymás mellé helyezzük az orosz Geraszimov-doktrína szerinti „új generációs hadviselést" és az Európai Unió kiberdiplomáciai megközelítését, sajátos stratégiai paradoxon rajzolódik ki. A felszínen a két szereplő helyzetértékelése meglepően hasonló, a választott megoldásaik azonban gyökeresen ellentétesek, ami mély strukturális aszimmetriához vezet.

A közös nevező a hadszíntér és az eszkalációs folyamat spektrumának felismerése. Az eltérő politikai kultúra dacára Moszkva és Brüsszel kiindulópontja azonos: mindkét fél elismeri a kibertér központi, megkerülhetetlen szerepét a modern államközi viszonyokban. Egyetértenek abban is, hogy a digitális tér a 21. század elsődleges stratégiai „ütközőzónája", ahol a kritikus infrastruktúrák egyszerre jelentenek védendő objektumot és támadási célpontot. A legfontosabb közös felismerés azonban a konfliktus természetére vonatkozik: mindkét fél elmozdult a bináris (béke/háború) szemlélettől a folytonos intenzitási spektrum felé. Oroszország és az EU is olyan eszközöket alkalmaz ebben a térben, amelyek tudatosan a nyílt fegyveres konfliktus jogi küszöbe alatt maradnak.

A hasonlóságok azonban itt véget is érnek. A két stratégia találkozása a proaktív környezetformáló és a normatív szabálykövető logikák ütközése. Az öt vizsgált dimenzió mentén a különbségeket a 2. táblázat foglalja össze.

Talán a legmélyebb filozófiai különbség a célok és eszközök viszonyában rejlik. Míg az EU a kiberteret elsősorban jogi és diplomáciai szempontokon keresztül nézi (a nemzetközi jog érvényesítése a cél), addig Oroszország tisztán műveleti és hatalmi (reálpolitikai) keretben gondolkodik. Oroszország számára érvényesül a klasszikus clausewitzi tétel: a kibertér csupán *eszköz* a szélesebb körű politikai célok (destabilizáció, befolyásszerzés) elérésére. Az EU számára viszont gyakran a kibertér biztonságának és integritásának megőrzése válik magává a *politikai céllá*.

[36] Pladson 2020.
[37] European Council 2020b.
[38] European Council 2025.
[39] European Council [é. n.].

2. táblázat: A Geraszimov-doktrína és az EU CDT összehasonlítása a módszertanban meghatározott öt dimenzió mentén

Összehasonlítási dimenzió	**Orosz megközelítés (Geraszimov-doktrína)**	**EU Cyber Diplomacy Toolbox (CDT)**	**Stratégiai aszimmetria jellege**
1. Célok és eszközök	Proaktív/Offenzív A cél az ellenfél döntéshozatali mechanizmusának megbénítása és belső destabilizáció. A katonai és nem katonai eszközök integráltan, 1:4 arányban dominálnak	Reaktív/Normatív A cél a szabályalapú rend védelme és a stabilitás megőrzése. Kizárólag defenzív, diplomáciai eszközöket (szankciók, nyilatkozatok) alkalmaz, offenzív képességek nélkül	Kezdeményezési aszimmetria Míg az orosz fél fegyverként használja a kiberteret, az EU védendő értékként kezeli, így az utóbbi gyakorlatilag folyamatos lépéskényszerben van
2. Intézményi keretek	Centralizált és hibrid Egységes hadműveleti vezetés, amely elmossa a határokat a reguláris erők, a hírszerzés és a proxy szereplők (bűnözői csoportok, hacktivisták) között	Összetett, szegmentált Töredezett hatáskörök (EEAS, ENISA, tagállamok). A védelem technikai, a válasz politikai szinten dől el, 27 tagállam eltérő fenyegetettségérzékelése mellett	Hatékonysági aszimmetria A központosított orosz parancsnoki lánc rugalmasabb és gyorsabb, mint az EU konszenzusigényes, többszereplős rendszere
3. Idősík: tempó és reakcióidő	Műveleti tempó A támadások végrehajtása jellemzően gyors (napok), a döntéshozatal azonnali. A konfliktus állandósult állapot, a műveletek gyakran már a nyílt konfrontáció előtt elindulnak	Diplomáciai tempó Lassú döntéshozatal. A technikai incidens és a politikai válasz (szankció) között évek telhetnek el	Időbeli aszimmetria A válaszintézkedés akkor érkezik meg, amikor a támadó már régen elérte a stratégiai céljait
4. Az attribúció követelménye	Hihető tagadás (plausible deniability) A cél az attribúció elkerülése, a felelősség szándékos elfedése *(maszkirovka),* álcázott infrastruktúra és proxyk használata a felelősségre vonás elkerülésére	Bizonyosságalapú Az intézkedések feltétele a jogilag és politikailag kikezdhetetlen attribúció. A technikai bizonyíték önmagában nem elég, politikai konszenzus szükséges	Felelősségi aszimmetria Az EU magas attribúciós bizonyítási küszöbe tág mozgásteret és sok esetben büntetlenséget biztosít az anonimitásba burkolózó támadónak
5. Az eszkaláció kezelése	Szürkezónás manőverezés Tudatosan a fegyveres konfliktus küszöbe alatt tartott, de folyamatos agresszió	Eszkalációkerülés Kockázatkerülő magatartás; a cél a konfliktus mérséklése (deeszkaláció). Az eszközök célja az elrettentés *(deterrence),* nem a kényszerítés *(compellence)*	Kockázati aszimmetria Az orosz fél bátrabban vállal kockázatot a határok feszegetésével, míg az EU önkorlátozó a konfliktus elkerülése érdekében

Forrás: a szerző szerkesztése

Ez a különbség a műveleti tér értelmezésében is megmutatkozik. Az orosz vezetés egyetlen, integrált térként kezeli a konfliktust, ahol a katonai, kiber- és információs eszközök összemosódnak. Az EU ezzel szemben intézményileg és fogalmilag is széttagolja a védekezést: külön silókban kezeli a kiberbiztonságot (technikai), a diplomáciát (politikai) és a védelmet (katonai).

A kibertérben folyó küzdelemben mindkét fél más-más erőforrásokra támaszkodik:

- Oroszország előnye a gyorsaságban, a hihető tagadhatóságban *(plausible deniability)* és az eszközök gátlástalan használatában rejlik.
- Az EU előnye a kiterjedt szövetségi hálókban, a kollektív diplomáciai nyomásgyakorlás lehetőségében és a hatalmas gazdasági súlyában keresendő, amely a szankciók révén válik fegyverré.

Következtetések

A következtetések célja a bevezetőben megfogalmazott kutatási kérdések megválaszolása, azaz hogy milyen strukturális különbségek azonosíthatók a Geraszimov által összegzett orosz hibrid hadviselés és az EU kiberdiplomáciai eszközkészlete között, és ezek az eltérések milyen gyakorlati következményekkel járhatnak, ha a két megközelítés szembekerül egymással. Az elvégzett összehasonlító elemzés alapján megállapítható, hogy a két keretrendszer találkozása a kibertérben strukturális stratégiai instabilitást eredményez. Míg az orosz megközelítés a konfliktust állandósult, integrált folyamatként kezeli, és proaktívan formálja a műveleti környezetet, addig az Európai Unió jogi-normatív alapállása és komplex, széttagolt intézményrendszere csak reaktív magatartást tesz lehetővé. Az elemzés rámutatott a „hatékonysági paradoxonra": az EU válaszmechanizmusa (politikai attribúció és konszenzusos döntéshozatal) jogilag megalapozott, de az idődimenzióban versenyképtelen a kibertérben rövid idő alatt végrehajtott offenzív műveletekkel szemben. A vizsgált példák (1. táblázat) igazolják, hogy a diplomáciai válasz késedelme miatt a büntetőintézkedések elveszítik közvetlen elrettentő erejüket. Emellett kérdéses, hogy például a GRU[40] három tisztjének szankcionálása[41] mennyire bír elrettentő erővel, azaz mennyiben tartja vissza az Oroszországi Föderációt a jövőbeli, Észtország elleni kibertámadásoktól. Ebben az esetben pont azt láthatjuk, hogy a Geraszimov-doktrína keretrendszerében értelmezhető, az orosz hadsereg által kivitelezett kiberműveletre az EU a Kiberdiplomáciai Eszköztár alkalmazásával bő négy év alatt adott választ, amelynek hatékonysága megkérdőjelezhető.

A tanulmány következtetése, hogy a jelenlegi, kizárólag defenzív és diplomáciai eszközökre építő uniós modell folyamatos stratégiai sebezhetőséget eredményez a „szürkezónás" agresszióval szemben. Ebből nem feltétlenül a kiberdiplomácia militarizálása következik, hanem a döntéshozatali ciklus szükségszerű gyorsítása. Az európai döntéshozók előtt álló stratégiai dilemma lényege, hogy a normatív hatalmi státusz megőrzése mellett miként növelhető az elrettentés *(deterrence)* hitelessége, illetve

[40] Oroszországi Föderáció Fegyveres Erői Vezérkarának Felderítő Főcsoportfőnöksége (Главное разведывательное управление Генерального штаба Вооружённых Сил Российской Федерации).

[41] Council Decision (CFSP) 2025/171 of 27 January 2025 Amending Decision (CFSP) 2019/797 Concerning Restrictive Measures against Cyber-Attacks Threatening the Union or Its Member States.

a jelenlegi diplomáciai eszköztár olyan szintre emelése, ahol a politikai és gazdasági ár megfizethetetlenné válik a támadó számára.

A tanulmányban feltárt stratégiai aszimmetriák alapján az EU Cyber Diplomacy Toolbox fejlesztésének logikus iránya a döntéshozatali ciklus radikális gyorsítása és a válaszlépések hitelességének növelése lehet. Mivel az elemzés kimutatta, hogy a jelenlegi teljes konszenzuson alapuló politikai attribúció jelentős időbeli hátrányt okoz a hibrid hadviselés műveleti tempójával szemben, a hatékony reagálás kulcsa olyan gyors döntési mechanizmusok kidolgozása lehet, amelyek lehetővé teszik a diplomáciai válaszok és szankciók kellő időben alkalmazását, még mielőtt a támadó stratégiai céljai megvalósulnának. A hatékonyság növelése érdekében elengedhetetlen a jelenleg elszigetelten működő technikai (incidenskezelés) és politikai (külügyi) szintek szorosabb együttműködése, ami csökkentheti az attribúciós eljárás átfutási idejét. Végezetül, a CDT által kínált válaszlépések palettájának bővítése is szóba jöhet, és a stratégiai egyensúly helyreállítása érdekében előbb-utóbb szükség lehet a kiberdiplomáciai eszköztár fajsúlyosabb intézkedéseinek bevetésére is.

Jelen kutatás korlátja, hogy a tanulmány kizárólag a nyilvánosan elérhető forrásokra és szövegekre támaszkodott, így nem vizsgálhatta a minősített attribúciós eljárások és döntési folyamatok idővonalát vagy belső dinamikáját. További kutatást igényel annak feltárása, hogy az egyes tagállamok eseménykezelési (incidensreagálási) és offenzív kiberképességei hogyan integrálhatók – vagy hogyan kerülhetnek konfliktusba – a közös uniós diplomáciai keretrendszerrel. Szintén vizsgálandó kérdés a jövőre nézve, hogy a kinetikus válaszcsapás lehetősége (amelyre az USA[42] vagy Izrael[43] esetében már van precedens) miként jelenhet meg az uniós biztonságpolitikai diskurzusban. Emellett további elemzésre érdemes, hogy a kiberdiplomáciai eszköztár mellett az Európai Unió más eszközei, mint például a kiberbiztonsági ellenálló képesség *(cyber resilience)* feljesztése vagy a hatékonyabb kiberkrízis-kezelés, hogyan erősíthetik és egészíthetik ki a CDT eszközkészletét.

Felhasznált irodalom

Biró Gabriella (2025): A kiberhadviselés fogalmának vizsgálata az orosz–ukrán háború kontextusában. In Molnár Dániel – Molnár Dóra (szerk.): *XXVIII. Tavaszi Szél Konferencia – Tanulmánykötet I.* Budapest: Doktoranduszok Országos Szövetsége, 189–200.

Boda Mihály (2023): Hibrid háború: konfliktusforma a harmonikus béke és a direkt háború között. A hibrid háború katonafilozófiai értelmezése. In Gőcze István – Padányi József (szerk.): *Lehelyezett kő. Tanulmányok M. Szabó Miklós nyugállományú altábornagy, a Magyar Tudományos Akadémia rendes tagja emlékére.* Budapest: Ludovika, 21–28. Online: https://doi.org/10.36250/01128_02

Boda Mihály (2024): A kockázatkerülő háború és a bátorság a 20–21. század fordulóján. *Honvédségi Szemle,* 152(3), 113–25. Online: https://doi.org/10.35926/HSZ.2024.3.9

[42] Starr 2015.
[43] Cimpanu 2019.

Brunner, Isabella (2025): Attributing Cyber Operations Under International Law: Political and Legal Aspects. *Questions of International Law,* 110, 27–43. Online: www.qil-qdi.org/wp-content/uploads/2025/06/03_Regulating-Activities_BRUNNER_FIN.pdf

Christou, George et al. szerk. (2025): *The Palgrave Handbook on Cyber Diplomacy*. Cham: Springer Nature Switzerland. Online: https://doi.org/10.1007/978-3-031-93385-1

Cimpanu, Catalin (2019): In a First, Israel Responds to Hamas Hackers with an Air Strike. *ZDNET,* 2019. május 5. Online: www.zdnet.com/article/in-a-first-israel-responds-to-hamas-hackers-with-an-air-strike/

Council Decision (CFSP) 2020/1127 of 30 July 2020 Amending Decision (CFSP) 2019/797 Concerning Restrictive Measures against Cyber-Attacks Threatening the Union or Its Member States. Online: http://data.europa.eu/eli/dec/2020/1127/oj

Council Decision (CFSP) 2020/1537 of 22 October 2020 Amending Decision (CFSP) 2019/797 Concerning Restrictive Measures against Cyber-Attacks Threatening the Union or Its Member States. Online: http://data.europa.eu/eli/dec/2020/1537/oj

Council Decision (CFSP) 2024/1779 of 24 June 2024 Amending Decision (CFSP) 2019/797 Concerning Restrictive Measures against Cyberattacks Threatening the Union or Its Member States. Online: http://data.europa.eu/eli/dec/2024/1779/oj

Council Decision (CFSP) 2025/171 of 27 January 2025 Amending Decision (CFSP) 2019/797 Concerning Restrictive Measures against Cyber-Attacks Threatening the Union or Its Member States. Online: http://data.europa.eu/eli/dec/2025/171/oj

Council Regulation (EU) 2019/796 of 17 May 2019 Concerning Restrictive Measures against Cyber-Attacks Threatening the Union or Its Member States. Online: http://data.europa.eu/eli/reg/2019/796/oj

Cyber Diia (2024): *A Decade in the Trenches of Cyberwarfare: Ukraine's Story of Resilience*. Online: https://nsarchive.gwu.edu/sites/default/files/documents/semon9-ryglx/2024-02-02-Cyber-Diia-A-Decade-in-the-Trenches-of-Cyberwarfare.pdf

European Council (2017): *Cyber Attacks: EU Ready to Respond with a Range of Measures, Including Sanctions*. Online: www.consilium.europa.eu/en/press/press-releases/2017/06/19/cyber-diplomacy-toolbox/

European Council (2020a): *EU Imposes the First Ever Sanctions against Cyber-Attacks*. Online: www.consilium.europa.eu/en/press/press-releases/2020/07/30/eu-imposes-the-first-ever-sanctions-against-cyber-attacks/

European Council (2020b): *Malicious Cyber-Attacks: EU Sanctions Two Individuals and One Body over 2015 Bundestag Hack*. Online: www.consilium.europa.eu/en/press/press-releases/2020/10/22/malicious-cyber-attacks-eu-sanctions-two-individuals-and-one-body-over-2015-bundestag-hack/

European Council (2025): *Cyber-Attacks: Three Individuals Added to EU Sanctions List for Malicious Cyber Activities against Estonia*. Online: www.consilium.europa.eu/en/press/press-releases/2025/01/27/cyber-attacks-three-individuals-added-to-eu-sanctions-list-for-malicious-cyber-activities-against-estonia/

European Council [é. n.]: *Sanctions against Cyber-Attacks*. Online: www.consilium.europa.eu/en/policies/sanctions-against-cyber-attacks/

European Union (2016): *Consolidated Version of the Treaty on European Union, Article 42, 202 OJ C*. Online: http://data.europa.eu/eli/treaty/teu_2016/art_42/oj

Galeotti, Mark (2014): The 'Gerasimov Doctrine' and Russian Non-Linear War. *War ont he Rocks,* 2014. július. Online: https://warontherocks.com/2014/07/the-gerasimov-doctrine-and-russian-non-linear-war/

Galeotti, Mark (2018): I'm Sorry for Creating the 'Gerasimov Doctrine'. *Foreign Policy,* 2018. március 5. Online: https://foreignpolicy.com/2018/03/05/im-sorry-for-creating-the-gerasimov-doctrine/

General Secretariat of the Council (2023): *Revised Implementing Guidelines of the Cyber Diplomacy Toolbox.* Online: https://data.consilium.europa.eu/doc/document/ST-10289-2023-INIT/en/pdf

Jójárt Krisztián (2024): *Az orosz katonai gondolkodás 21. századi hadviselés-felfogásának értelmezése.* PhD-disszertáció. Budapest: Nemzeti Közszolgálati Egyetem. Online: https://doi.org/10.17625/NKE.2024.014

Kovács László (2023): *Hadviselés a 21. században: kiberműveletek*. Budapest: Ludovika. Online: https://doi.org/10.36250/01057_00

Krasznay Csaba szerk. (2023): *Taktikák és stratégiák a kiberhadviselésben.* Budapest: Ludovika. Online: https://doi.org/10.36250/01079_00

Manners, Ian (2002): Normative Power Europe: A Contradiction in Terms? *JCMS: Journal of Common Market Studies,* 40(2), 235–258. Online: https://doi.org/10.1111/1468-5965.00353

Molnár Anna – Molnár Dóra szerk. (2022): *Kiberdiplomácia.* Budapest: Ludovika. Online: https://doi.org/10.36250/01008_00

Moret, Erica – Pawlak, Patryk (2017): *The EU Cyber Diplomacy Toolbox. Towards a Cyber Sanctions Regime?* European Union Institute for Security Studies. Online: https://data.europa.eu/doi/10.2815/399444

Nagy Bianka (2018): Az angolszász és az orosz hadviselési generációs elméletek elemzése és alkalmazhatósága a XXI században. *Szakmai Szemle,* 16(4), 39–58. Online: https://hhk.uni-nke.hu/document/hhk-uni-nke-hu/2018_4_szam.pdf

National Intelligence Council (2021): *Global Trends 2040: A More Contested World.* Online: www.dni.gov/index.php/gt2040-home

NATO (2025): *Collective Defence and Article 5.* Online: www.nato.int/en/what-we-do/introduction-to-nato/collective-defence-and-article-5

Pladson, Kristie (2020): Germany Demands EU Cyber Sanctions over Russia Hacking. *Deutsche Welle,* 2020. július 12. Online: www.dw.com/en/germany-proposes-first-ever-use-of-eu-cyber-sanctions-over-russia-hacking/a-54144559

Russian Offensive Campaign Assessment. *Institute for the Study of War,* 2025. december 29. Online: https://understandingwar.org/research/russia-ukraine/russian-offensive-campaign-assessment-december-29-2025/

Schmitt, Michael N. – NATO Cooperative Cyber Defence Centre of Excellence szerk. (2017): *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Second edition. Cambridge University Press. Online: https://assets.cambridge.org/97811071/77222/frontmatter/9781107177222_frontmatter.pdf

Starr, Barbara (2015): Prominent ISIS Recruiter Killed in Airstrike. *CNN,* 2015. augusztus 28. Online: www.cnn.com/2015/08/26/politics/isis-recruiter-targeted-in-airstrike

Герасимов, Валерий (2013): Ценность науки в предвидении. *Военно-промышленный курьер,* 2013. február 27. Online: https://vpk.name/news/85159_cennost_nauki_v_predvidenii.html

Расторгуев, С. П. (1998): *Информационная война*. Радио и связь. Online: https://sprotyvg7.com.ua/wp-content/uploads/2024/02/Rastorguev-Informacionnaja-Vojna.pdf