Biró Gabriella

A kiberbiztonsági és digitalizációs metrikák felhasználási lehetőségeinek vizsgálata a kiberképességek meghatározásához

A tanulmány azt vizsgálja, hogy mennyire jelezhetik előre az egyes kiberbiztonsági és digitalizációs metrikák, hogy egy fegyveres konfliktusban melyik oldalon lesz a fölény a kiberműveletek terén. Az orosz–ukrán háború vonatkozásában a jelenleg használt metrikák nem minden esetben adnak megbízható előrejelzést azzal kapcsolatban, hogy a célpont mennyire képes sikeresen ellenállni a kibertámadásoknak. Például a Nemzetközi Távközlési Egyesület (International Telecommunication Union) kiberbiztonsági indexének 2021-es kiadása alapján Oroszország az 5., míg Ukrajna a 78. helyen állt. A 2024-es kiadás már nem tartalmaz rangsort, de Ukrajna a T3-as csoportba került, míg az Oroszországi Föderáció a T2-be. A nyilvánosan elérhető forrásokból tájékozódva nem mutatkozik ekkora különbség a két fél felkészültsége között a gyakorlatban. A kutatás során a 2020-tól napjainkig elérhető kiberképességekre vonatkozó metrikák vizsgálatával összevetem a támadási és védekezési képességekről elérhető információkat, és ez alapján értékelem a metrikák megbízhatóságát.

Kulcsszavak: *kiberbiztonság, digitalizáció, kiberképesség, metrika, kiberműveletek*

Bevezetés

A modern hadviselésben egyre inkább teret nyernek a kibertérben zajló műveletek, akár önállóan, akár a hagyományos, kinetikus műveletekkel összehangolva. A fokozódó digitalizáció révén akár egy egész ország közigazgatását is meg lehet bénítani, ahogy a 2007-es Észtország elleni támadás során megfigyelhető volt (Haig–Kovács 2008). Ugyanakkor, míg az egyes országok kinetikus műveleti képességeivel kapcsolatban rendelkezésre állnak olyan mérőszámok, mint például a *Global Firepower Index* (globálistűzerő-index) vagy a *Military Balance+* adatbázis adatai, addig a kiberképességekre vonatkozóan nincsenek ilyen jól kidolgozott metrikák (*2025 Military Strength Ranking* 2025; *Military Balance+* [é. n.]).

Megtudható, mekkora adott ország hadserege, illetve mennyi és milyen haditechnikával rendelkezik, de a kiberképességek felmérése bonyolultabb feladat. Ez egyrészt abból adódik, hogy kevésbé kézzelfoghatók a kibertérben támadásra és védekezésre használt eszközök – hiszen nagy részük szoftver vagy kihasználható

https://doi.org/10.36250/01323_02 • https://orcid.org/0009-0004-5924-6694

sebezhetőség –, másrészt sokkal szorosabban összefonódnak a katonai és civil képességek. Elég a kritikus információs infrastruktúrák üzemeltetésére gondolni, amely jellemzően nem a hadsereg kezében van, és máris belátható, hogy egyedül a haderő vizsgálatával nehéz meghatározni a védelmi képességeket.

Az egyes országok kiberbiztonsági és digitalizációs fejlettségével kapcsolatos mutatók széles körben használatosak – de mennyire megbízhatók egy fegyveres konfliktus idején? A vizsgálat célja meghatározni, hogy mennyire jelezhetik előre ezek az egyébként más céllal született mérőszámok, hogy egy fegyveres konfliktusban melyik oldalon lesz a fölény a kiberműveletek terén. A kutatás az orosz–ukrán háború kibertérben zajló eseményeivel kapcsolatos nyílt forrásból elérhető információkat használta fel annak érdekében, hogy összevethető legyen a kiberbiztonsági és digitalizációs metrikák által mutatott kép a tapasztalt kibervédelmi képességekkel.

A támadóképességeket nagyon nehéz objektíven megítélni, hiszen gyakran még a nyilvánosságra hozott, jól dokumentált támadások esetében is csak feltételezésekre hagyatkozhatunk a támadó személyét illetően (attribúció). Ezért elsősorban a védekezési (kibervédelmi) képességek és a kiberbiztonsági metrikák kapcsolatát vizsgálja a tanulmány. A hipotézis szerint a jelenlegi mutatók nem jelzik megbízhatóan a fegyveres konfliktusokban a kibertámadásokkal szembeni ellenálló képességet. Másképp fogalmazva az egyes országok békeidőben felmért kiberbiztonsági tulajdonságai nem adnak megbízható előrejelzést azzal kapcsolatban, hogy mennyire képesek megbirkózni a kibertámadásokkal egy fegyveres konfliktus során.

Az elérhető metrikák vizsgálata

Számos különböző szempontú, digitalizációra és kiberbiztonságra vonatkozó mérőszám érhető el a világ különböző régióira vonatkozóan, amelyek közül 65 metrikát vizsgál Khudyntsev társaival (Khudyntsev et al. 2021: 117–126). Az országok digitalizációs szintje nem teljesen független kiberbiztonsági fejlettségüktől, azonban nem jelenthető ki egyértelműen, hogy a magas fokú digitalizáció minden esetben fejlett kiberbiztonsággal jár együtt (Kravets 2019). A kibervédelmi képességek szempontjából a kiberbiztonsági ellenálló képesség nagyobb relevanciával bír, mint a digitalizáció – amely inkább az adott ország digitális támadási felületének nagysága szempontjából releváns –, ezért elsődlegesen a kiberbiztonsággal kapcsolatos mérőszámokra kerül a fókusz, és a digitalizációval kapcsolatos indikátorokat csak kiegészítő információként használom fel.

Ahhoz, hogy egy pillanatképnél átfogóbb következtetéseket lehessen levonni a metrikákból, olyan mérőszámokat kell választani, amelyekre a következő feltételek teljesülnek:

- megbízhatók, azaz objektív szempontok alapján, jól dokumentált és megismerhető módszertannal készülnek;
- konzisztensek, azaz a módszertan megismételhető és lehetővé teszi az adott országra vonatkozó korábbi adatokkal, illetve más országokkal történő összevetést;
- rendszeresen frissülnek, tehát azonosíthatók belőlük az esetleges változások, fejlődési tendenciák.

Ezek a feltételek jelentősen leszűkítik azon metrikák körét, amelyek szóba jöhetnek a kiberképességek vizsgálata során. A továbbiakban Kravets tanulmánya nyomán három kiberbiztonsággal kapcsolatos metrikát vizsgálok közelebbről: a globális kiberbiztonsági indexet (*Global Cybersecurity Index,* GCI), a nemzeti kiberbiztonsági indexet (*National Cyber Security Index,* NCSI) és a kiberbiztonsági indexet (Index of Cyber Security, ICS) (Global Cybersecurity Index [é. n.]; *National Cyber Security Index* [é. n.]; *Index of Cybersecurity TAG Infosphere*). A 2.1. táblázat tartalmazza ezek összehasonlító elemzését.

A 2.1. táblázatban szereplő mutatószámok közül a harmadik, a kiberbiztonsági index nem alkalmas országok összehasonlítására, inkább a mindenkori szubjektív fenyegetettségi szintet jelzi. Az első két metrika közül csak az NCSI tartalmaz védelmi dimenziót, viszont az Oroszországi Föderáció értékelésére nem terjed ki, így nem alkalmas az orosz–ukrán háborúval kapcsolatos összevetés elvégzésére. A Nemzetközi Távközlési Egyesület (International Telecommunications Union, ITU), az ENSZ szakosított ügynöksége által készített *globális kiberbiztonsági index* viszont több szempontból is alkalmasnak látszik a további vizsgálatra.

2.1. táblázat. *A kiberbiztonsági mutatók összehasonlító elemzése*

A metrika neve	**Globális kiberbiztonsági index (Global Cybersecurity Index, GCI)**	**Nemzeti kiberbiztonsági index (National Cyber Security Index, NCSI)**	**Kiberbiztonsági index (Index of Cyber Security, ICS)**
Mit mér?	A központi kormányok kiberbiztonsági kötelezettségvállalásainak végrehajtása	Az országok felkészültsége a kiberfenyegetések megelőzésére és a kiberincidensek kezelésére	A vállalati, ipari és kormányzati információs infrastruktúrát érintő, a kiberbiztonsági fenyegetések széles spektrumából eredő kockázat
Alkalmazás	Nemzetközi kiberbiztonsági rendszer és nemzeti politikák kialakítása a kiberbiztonság területén	Információk nyújtása a naprakész nemzeti kiberbiztonsági rendszerekről, a nemzeti kiberbiztonsági rendszerek és politikák fejlesztéséről	Kiberfenyegetések kockázatkezelése adott szervezet számára
Célok	Segít az országoknak a fejlesztendő területek azonosításában; motiválja a cselekvést a relatív GCI-rangsor javítására; a kiberbiztonság szintjének emelése világszerte; segít a legjobb gyakorlatok azonosításában és népszerűsítésében; a kiberbiztonság globális kultúrájának előmozdítása	A korszerű nemzeti kiberbiztonsági rendszerek fejlettségi szintjének tudatosítása; a kiberbiztonsági rendszerek saját fejlettségi szintjének összehasonlítása más országok rangsorával; a legjobb gyakorlatokra vonatkozó információk megosztása	A kockázati szint értékelése iparági szakemberek által; a kiberbiztonsággal kapcsolatos általános vélekedések megosztása több célközönséggel; a saját tapasztalatok és a kiberbiztonsági értékelés összevetése az általános értékeléssel; a szervezet kiberbiztonsági szintjének havi szintű javítása
Frissítés	2015, 2017, 2019, 2021, 2024	2016 óta, naprakész	Havonta
Módszerek	Szakértői értékelés, többkritériumos elemzés (MCA), a tényezők súlyozása	Szakértői értékelés, lineáris függvény	Szentimentelemzés, szakértői értékelés, a tényezők súlyozása, idősorelemzés
Fő kategóriák	Jogi intézkedések; technikai intézkedések; szervezeti intézkedések; kapacitásépítés; együttműködés	Általános kiberbiztonsági mutatók (kiberbiztonsági politika kidolgozása, a kiberfenyegetések elemzése és információcsere, oktatás és szakmai fejlődés, hozzájárulás a globális kiberbiztonsághoz); kiberbiztonsági alapmutatók (a digitális szolgáltatások védelme, az alapvető szolgáltatások védelme, e-azonosítás és bizalmi szolgáltatások, a személyes adatok védelme); incidens- és válságkezelési mutatók (a kiberincidensekre való reagálás, kiberválság-kezelés, a kiberbűnözés elleni küzdelem, katonai kiberműveletek)	Támadó aktorok; kiberfegyverek; a támadók által kívánt hatás; támadási célpontok; a rendelkezésre álló védelmi eszközök sebezhetősége; általános értékelés
Az indikátorok száma	GCIv1: 17 mutató, 17 kérdés; GCIv2: 25 mutató, 157 kérdés; GCIv3: 25 mutató, 50 kérdés; GCIv4: 20 mutató, 82 kérdés; GCIv5: 20 mutató, 82 + 1 kérdés	46 mutató	25 mutató

A metrika neve	Globális kiberbiztonsági index (Global Cybersecurity Index, GCI)	Nemzeti kiberbiztonsági index (National Cyber Security Index, NCSI)	Kiberbiztonsági index (Index of Cyber Security, ICS)
Válaszadók	Az értékelt ország állami intézményeinek és kereskedelmi vállalatainak szakértői, állami szervezetei; nemzetközi szervezetek szakértői	Az értékelt ország tisztviselői, állami szervezetek, akadémikusok, az NCSI-csapat tagjai	A fejlesztők által kiválasztott iparági szakemberek (a lista nem nyilvános)
Az országok száma	194	126	–
Ellenőrzés	A partnerszervezetek szakértői végzik	Legalább két NCSI-csapattag végzi	Nem történik
Fejlesztők	Az ITU, nemzetközi partnerekkel	Az e-Kormányzati Akadémia (Tallinn) észt partnerekkel	Dan Geer és Mukul Pareek; TAG Infosphere-szakértők

Forrás: Kravets 2019 nyomán, a szerző kiegészítéseivel

Az ITU globális kiberbiztonsági indexe

Az ITU *kiberbiztonsági indexe* (GCI) jelentős fejlődésen ment keresztül az elmúlt tíz év során. A munka 2013-ban kezdődött a módszertan kidolgozásával és az első adatgyűjtéssel, a felmérés eredményeit pedig 2015-ben tették közzé. Kezdetben jóval kevesebb kérdésből állt a felmérés, azonban maguk az értékelés alapját adó pillérek az első jelentés elkészítése óta változatlanok. A GCI pillérei és ezek indikátorai a következők:

- jogi intézkedések (kiberbűnözés, kiberbiztonság);
- technikai intézkedések (CSIRT/CERT, nemzeti keretrendszer);
- szervezeti intézkedések (stratégia, felelős intézmény, mérések/auditok, online gyermekvédelem);
- kapacitásfejlesztési intézkedések (biztonságtudatosság, oktatás, képzés);
- együttműködési intézkedések (nemzetközi együttműködések, jogsegély, köz- és magánszféra közötti partnerség, ügynökségek közötti partnerség).

A módszertannak állandó eleme az is, hogy az ITU által a nemzeti válaszokat koordináló hatóságoknak kiküldött kérdőíveket az ITU validálja, azaz megvizsgálja a válaszok megalapozottságát. Maga a validáció elsősorban dokumentációalapú, tehát a nemzeti válaszokban hivatkozott stratégiákat, jogszabályokat és egyéb iratokat ellenőrzik. Az indikátorok kiválasztásánál a kezdetektől szempont volt az adatok rendelkezésre állása és minősége, valamint a másodlagos adatokon

keresztül történő keresztellenőrzés lehetősége (Global Cybersecurity Index 2017). Ez a megközelítés viszonylag objektív eredményt ad, ugyanakkor a tényleges gyakorlati értékelés helyett inkább a *compliance* (jogszabályi megfelelés) irányába viszi el az értékelést.

2.2. táblázat. *A GCI időbeli alakulása*

Kiadvány	GCIv1	GCIv2	GCIv3	GCIv4	GCIv5
A kiadás éve	2015	2017	2019	2021	2024
Az adatgyűjtés éve(i)	2013–2014	2016	2017–2018	2020	2023–2024
Fókuszpontot adó országok	105	136	155	169	172
A kérdések típusa	Nyílt	Zárt, 2 választási lehetőség	Zárt, 2 választási lehetőség	Zárt, 3 választási lehetőség	Zárt, 3 választási lehetőség
Pontszámítási módszer	*Benchmark-pontszámok*	Rangsoralapú súlyozott pontszámok	Rangsoralapú súlyozott pontszámok	Összesített súlyozott átlagpontszám	Összesített súlyozott átlagpontszám
Az indikátorok száma	17	25	25	20	20
A kérdések száma	17	153 + 4 opcionális kérdés az online gyermekvédelemről	50	82	82 + 1 opcionális kérdés a mikro-, kis- és középvállalkozások képzéséről

Forrás: a szerző szerkesztése a GCIv5 nyomán (*Global Cybersecurity Index* 2024)

Az évek során a GCI módszertana nagyon nagy fejlődésen ment keresztül, amelynek összefoglalását a 2.2. táblázat tartalmazza. A globális kiberbiztonsági index kezdetben egyszerű átlagolással készült, majd a 2017-es kiadásban az ITU áttért a súlyozott értékelésre, ahol a súlyozás szorzóit szakértőkből álló munkacsoport állapítja meg (Global Cybersecurity Index 2017). A 2021-ben kiadott, 2020-ra vonatkozó adatok értékelését tartalmazó kiadás és a 2024-es kiadás 0–20 pont között értékeli az egyes kategóriákat összesen 100 pontig, míg a korábbi jelentések 0–1 közötti skálán pontoztak, és nem is tartalmazták az összes ország részletes pontszámát.

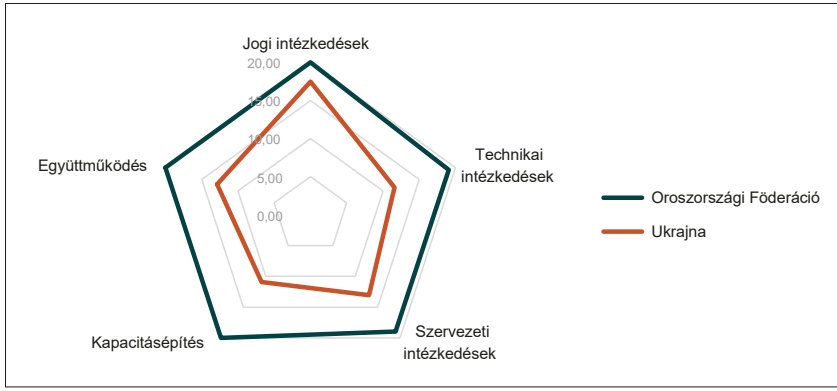
Az első négy kiadásban a GCI rangsort állított fel az országok között (hasonlóan ahhoz, ahogy a *Global Firepower Index* rangsorolja az országok haderejét), azonban a 2024-es kiadásban változtattak ezen a megközelítésen, és ötfokozatú skála szerinti pillércsoportokba sorolják az országokat anélkül, hogy összesített

pontszámukat megadnák (*Global Cybersecurity Index 2024* 2024). Ennek ellenére az összértékek könnyen kiszámíthatók, ha valaki mégis szeretne rangsort felállítani. A módszertani változások miatt részletesen csak a 2021-es és a 2024-es GCI-adatok vethetők össze, viszont azok megfelelnek a korábban leírt követelményeknek (megbízhatóság, konzisztencia, rendszeres frissítés).

A GCI készítői időről időre megvizsgálják a GCI-pontszámok és az egyéb digitalizációs indexek lehetséges összefüggéseit. 2017-ben így fogalmaztak: „A GCI-pontszámok és a jelentős IKT-fejlesztési indexek összehasonlítása nem mutat különösebben szoros összefüggést, mivel a tapasztalatok azt mutatják, hogy az IKT-fejlesztés terén magas pontszámot elérő országok nem feltétlenül fektetnek be ugyanolyan mértékben a kiberbiztonságba, és fordítva." (*Global Cybersecurity Index* 2017) 2018-ban az Egyesült Nemzetek Szövetsége (ENSZ) által kiadott e-kormányzati fejlesztési index *(E-Government Development Index)* kapcsán a következőket állapították meg: „A GCI és az e-kormányzati fejlesztési index összehasonlítása nem mutat különösebb összefüggéseket, és a tapasztalatok azt mutatják, hogy az e-kormányzati fejlesztés terén jól teljesítő országok nem feltétlenül fektetnek ugyanolyan mértékben a kiberbiztonságba, és fordítva." (*Global Cybersecurity Index* 2018) 2024-ben is hasonló következtetést vontak le: „A GCI-pontszámok és az általános információs és kommunikációs technológiák (IKT) fejlődésének összehasonlításakor figyelembe kell venni, hogy a pontszámok nem feltétlenül követik az ITU IKT-fejlesztési indexét (IDI), amely az univerzális és jelentős összekapcsoltságot méri." (*Global Cybersecurity Index 2024* 2024) Összességében tehát az ITU is arra a következtetésre jut, hogy a kiberbiztonsági és a digitalizációs metrikák között nem minden esetben van korreláció.

Az Oroszországi Föderáció és Ukrajna GCI-értékei és az orosz–ukrán háború

Ahhoz, hogy megvizsgálható legyen, mennyire használható a GCI-metrika az orosz–ukrán háború kibertérben zajló kimenetelének előrejelzéséhez, meg kell vizsgálni, hogy milyen értékeket mutatott a GCI az Oroszországi Föderációval és Ukrajnával kapcsolatban, ehhez képest pedig mi történt a valóságban. Az orosz–ukrán háború 2014-ben kezdődött a Krím félsziget orosz megszállásával, azonban a konfliktus jelentősen eszkalálódott a 2022. február 24-én indított orosz invázióval. Ezzel egyidőben a kibertérben is intenzívebbé váltak az Ukrajna elleni támadások, majd a válaszlépések sem várattak magukra sokáig.



2.1. ábra. *Az Oroszországi Föderáció és Ukrajna GCI-értékei 2020-ban*
Forrás: a szerző szerkesztése a 2020-as GCI-kiadás alapján (*Global Cybersecurity Index* 2021)

A 2022-es invázió idején a 2021-ben kiadott, 2020-as adatok alapján készült GCI-jelentés volt a legfrissebb elérhető metrika. Eszerint az Oroszországi Föderáció globális szinten (az értékelt 194 ország között) az 5. helyen állt 98,06 ponttal, míg Ukrajna a 78. helyen 65,93 ponttal, ami elég jelentős különbség. Hogy jobban kontextusba helyezhetők legyenek ezek az értékek, érdemes azt is megemlíteni, hogy ekkor Magyarország a 22. helyen állt 91,28 ponttal (*Global Cybersecurity Index* 2021). A számokat látva joggal feltételezhető, hogy Ukrajna kiberbiztonsági szempontból jelentősen elmaradt az Oroszországi Föderáció mögött. Ebből arra a következtetésre lehetne jutni, hogy a két ország közötti háborúban Oroszország gyorsan képes megszerezni a kibertérben a fölényt, a valós események azonban nem igazolják ezt a feltevést.

A 2022. február 24. utáni első 100 nap kibertérben zajló eseményeit sokan értékelték, és általában arra a következtetésre jutottak, hogy Ukrajna a támadások mértékéhez képest jól ellenállt a kibertámadásoknak (Smith 2022; Cyber Diia 2024). Az ukrán kritikus infrastruktúrák ugyan az orosz kiberműveletek célkeresztjébe kerültek, de a támadók nem arattak jelentős sikereket (Kiss 2024; Mueller et al. 2023).

Felvetődhet, hogy Ukrajna védekezőképességéhez jelentősen hozzájárult a kibertérben a NATO-tól és szövetségeseitől kapott segítség, azonban a nemzetközi együttműködés olyan tényező, amelyet az ITU GCI is figyelembe vesz. Ukrajna a 2020-as adatok alapján 12,87 pontos értékelést kapott az Együttműködés

kategóriában a lehetséges 20 pontból, tehát vagy nem voltak túl kiterjedt nemzetközi együttműködései, vagy az ITU-kérdőív rosszul mérte fel azokat. Ezzel szemben az Oroszországi Föderáció a maximális 20 pontot érte el az Együttműködés kategóriában, ami a 2024-es GCI-jelentésben már 16,77 pontra romlott. Ukrajna ugyanakkor 2024-ben 16,58-ra javított. Ebből úgy tűnik, hogy a GCI kellően érzékeny módon értékeli az együttműködéseket. Ukrajna védelmi képességeire pedig meggyőzőbb magyarázat, hogy a 2014 és 2016 között elszenvedett kibertámadások után a 2022-es események már nem érték teljesen felkészületlenül (Lewis 2022).

Érdemes megvizsgálni a GCI többi kategóriáját is, hogyan változtak a 2024-es felmérésben. Ukrajna pontszáma határozottan javult (65,93 pontról 83,93-ra), míg az Oroszországi Föderáció értékelése kisebb mértékben romlott (98,06 pontról 92,13 pontra). A részleteket a 2.3. táblázat tartalmazza. A jogi intézkedések értékelése Oroszország esetében változatlan, a maximális 20 pont. Ukrajna javuló értékelése tükrözi, hogy számos kiberbiztonsághoz kapcsolódó területen megújította és az Európai Unió szabályozásához közelíti jogszabályait. A technikai intézkedések értékelése erősen kötődik az incidenskezelési képességekhez, amelyeket mindkét országnak volt alkalma fejleszteni az elmúlt évek során, ugyanakkor míg Ukrajna javított, Oroszország romló értékelése azt tükrözi, hogy nem minden esetben sikerül eredményesen védekeznie az Ukrajnával együttérző hackerek támadásai ellen. A szervezeti intézkedések terén mindkét ország javított, de ez a pillér a stratégiák mellett olyan elemeket is tartalmaz, mint például az online gyermekvédelem, ezért a kibervédelmi képességek szempontjából kevésbé releváns. A kapacitásépítés pontszámai is a várakozásoknak megfelelően alakultak, az ukránok javítottak, míg Oroszországot nagyon sok jól képzett informatikus hagyta el a háború és a nagy technológiai cégek kivonulása miatt (AFP).

2.3. táblázat. *Az Oroszországi Föderáció és Ukrajna GCI-értékeinek változása 2020 és 2024 között*

Év	Ország	Jogi int.	Technikai int.	Szervezeti int.	Kapacitás-építés	Együtt-működés	Össz-pontszám
2024	*Oroszországi Föderáció*	20,00	↓16,59	↑20,00	↓18,77	↓16,77	*92,13*
	Ukrajna	↑19,42	↑17,35	↑15,97	↑14,61	↑16,58	*83,93*
2021	*Oroszországi Föderáció*	20,00	19,08	18,98	20,00	20,00	*98,06*
	Ukrajna	17,46	11,60	13,06	10,94	12,87	*65,93*

Forrás: a szerző szerkesztése

Következtetések

Összességében elmondható, hogy bár számos kiberbiztonsági és digitalizációs metrika létezik, jelenleg kevés olyan mérőszám van, amely megbízható, konzisztens, rendszeresen frissül, és kellően sok országot lefed. A vizsgált metrikák közül a Nemzetközi Távközlési Egyesület globális kiberbiztonsági indexe felel meg legjobban a fenti elvárásoknak, és mind Ukrajna, mind az Oroszországi Föderáció értékelésére kiterjed. Az orosz–ukrán háború valós kibertérben zajló eseményeivel összevetve azonban megfigyelhető, hogy az ITU GCI nagyon jelentős különbséget jelzett az orosz és ukrán kiberképességek között, míg a valóságban nem mutatkozott ekkora eltérés.

Ennek az egyik oka, hogy a GCI által használt indikátorok egy része egyáltalán nem releváns kibervédelmi szempontból. Például az online gyermekvédelem vagy a kiberbűnözés elleni fellépés fontos ugyan, de háborús helyzetben nem járul hozzá a kibervédelmi képességekhez. Ugyanakkor vannak olyan indikátorok is az ITU felmérésében, amelyek békeidőben is fontosak, de a háborúban felértékelődnek, mint például az incidenskezelés vagy a nemzetközi együttműködések. A GCI-ből emellett hiányoznak a kibervédelemmel kapcsolatos indikátorok, amelyek például a tallinni e-Kormányzati Akadémia által készített nemzeti kiberbiztonsági indexben szerepelnek. Az indikátorok megléte mellett a GCI-módszertanban fontos a súlyozásuk is (amely nem nyilvános), így előfordulhat, hogy bizonyos tényezőket felül- vagy alulértékel az ITU indexe. Az értékelés során a módszertan előnyben részesíti a dokumentumokkal alátámasztott adatokat, ezért a gyakorlatiasabb területeket nehezebben tudja pontosan feltérképezni.

A fentiek miatt a hipotézis, miszerint a jelenlegi mutatók nem jelzik megbízhatóan a fegyveres konfliktusokban a kibertámadásokkal szembeni ellenálló képességet, igazoltnak tekinthető. A kiberbiztonsági metrikák terén megfigyelhető egyfajta fejlődés és a valós eseményeket figyelembe vevő korrekció, ezért előfordulhat, hogy a jövőben ezek a békeidőben használt metrikák háborús körülmények közötti előrejelzésekre is alkalmasak lesznek, azonban jelenleg még nem ez a helyzet.

A jelenlegi kutatás továbbfejleszthető és kiterjeszthető a más országokkal kapcsolatos kibertéri események vizsgálatára. A jelenlegi metrikák hiányosságai alapján konkrét fejlesztési javaslatok (felmérési kérdések, értékelési szempontok) fogalmazhatók meg a GCI-vel vagy más mérőszámokkal kapcsolatban, azonban ez túlmutat jelen tanulmány keretein.

EXPLORING THE POTENTIAL USES OF CYBERSECURITY AND DIGITALIZATION METRICS TO DETERMINE CYBER CAPABILITIES

This study examines the extent to which individual cybersecurity and digitalization metrics can predict which side will have supremacy in cyber operations during an armed conflict. Specifically, in the context of the Russian–Ukrainian war, the metrics currently used do not always provide a reliable prediction of how successfully a target can resist cyberattacks. For example, based on the 2021 edition of the International Telecommunication Union Cybersecurity Index, Russia ranked 5th and Ukraine 78th, while the 2024 edition no longer includes a ranking, but Ukraine has been placed in the T3 group and the Russian Federation in T2. Based on publicly available sources, there does not appear to be such a large difference between the two sides' preparedness in practice. In this research, metrics on cyber capabilities available from 2020 to the present day are compared with information on attack and defense capabilities, and based on this comparison, the reliability of the metrics is assessed.

Keywords: *cybersecurity, digitalization, cyber capability, metrics, cyber operations*

Felhasznált irodalom

2025 Military Strength Ranking (2025). Global Firepower. Online: www.globalfirepower.com/countries-listing.php

AFP (2022): Moscow Says 100K IT Specialists Have Left Russia This Year. *The Moscow Times,* 2022. december 20. Online: www.themoscowtimes.com/2022/12/20/moscow-says-100k-it-specialists-have-left-russia-this-year-a79754

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

Global Cybersecurity Index [é. n.]. International Telecommunication Union. Online: www.itu.int/en/ITU-D/Cybersecurity/pages/global-cybersecurity-index.aspx

Global Cybersecurity Index (2017). International Telecommunication Union. Online: www.itu.int/pub/D-STR-GCI.01-2017

Global Cybersecurity Index (2018). International Telecommunication Union. Online: https://www.itu.int/pub/D-STR-GCI.01-2018

Global Cybersecurity Index (2021). International Telecommunication Union.

Global Cybersecurity Index 2024 (2024). [H. n.]: International Telecommunication Union. Online: www.itu.int/en/ITU-D/Cybersecurity/Documents/GCIv5/2401416_1b_Global-Cybersecurity-Index-E.pdf

Haig Zsolt – Kovács László (2008): Fenyegetések a cybertérből. *Nemzet és Biztonság,* 1(5), 61–69. Online: https://www.nemzetesbiztonsag.hu/cikkek/haig_zsolt__kovacs_laszlo-fenyegetesek_a_cyberterb__1.pdf

Index of Cybersecurity TAG Infosphere. Online: https://tag-infosphere.com/ccs

KHUDYNTSEV, Mykola et al. (2021): Cybersecurity Indices: Review and Classification. *CPITS II,* 3187, 117–126. Online: www.ceur-ws.org/Vol-3187/paper11.pdf

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

KRAVETS, Valentyna (2019): Comparative Analysis of the Cybersecurity Indices and Their Applications. *Theoretical and Applied Cybersecurity,* 1(1), 97–102. Online: https://doi.org/10.20535/tacs.2664-29132019.1.169090

LEWIS, James A. (2022): *Cyber War and Ukraine.* Washington, DC: Center for Strategic and International Studies. Online: www.jstor.org/stable/resrep41883

Military Balance+ [é. n.]. The International Institute for Strategic Studies. Online: www.iiss.org/the-military-balance-plus/

MUELLER, Grace B. et al. (2023): Cyber Operations during the Russo-Ukrainian War. *Center for Strategic and International Studies,* 2023. július 13. Online: www.csis.org/analysis/cyber-operations-during-russo-ukrainian-war

National Cyber Security Index [é. n.]. Online: www.ncsi.ega.ee/

SMITH, Brad (2022): Defending Ukraine: Early Lessons from the Cyber War. *Microsoft on the Issues*, 2022. június 22. Online: https://blogs.microsoft.com/on-the-issues/2022/06/22/defending-ukraine-early-lessons-from-the-cyber-war/