HADMÉRNÖK
VÉDELEMINFORMATIKA

19. évfolyam (2024) 3. szám 183–200.
DOI: 10.32567/hm.2024.3.11

Kiss Adrienn[1]

Az orosz–ukrán háború hatása a kritikus infrastruktúrákra – fókuszban az energiaszektor[2]

The Impact of the Russian–Ukranian War on Critical Infrastructure – Focus on the Energy Sector

Absztrakt

Az orosz–ukrán háború során is megjelent a kibertér mint hadszíntér, ez pedig jelentősen hozzájárul a modern konfliktusok természetének folyamatos átalakulásához. A tanulmány célja az orosz–ukrán háború során végrehajtott kibertámadások empirikus elemzése, kitekintéssel az energiaszektorra. A kutatás a 2022-es és a 2023-as adatokat vizsgálja, feldolgozva az ismert kibertámadások időbeli trendjeit, földrajzi eloszlását és típusait. A tanulmány rámutat a kibervédelem felépítésének, fejlesztésének és fenntartásának, valamint a támadások elemzésének és a megfelelő tanulságok levonásának fontosságára. A kutatásban idősorelemzést, trendelemzést és hőtérképes megjelenítést alkalmaztam. Az eredmények rámutatnak arra, hogy mely szektor vált különösen kiemelt célponttá a kibertámadások során. Ezen felül bemutatja a kritikusinfrastruktúra-szektorok támadottságának mértékét a háború kapcsán, illetve a kibertámadások során alkalmazott technikákat.

Kulcsszavak: kritikus infrastruktúra, orosz–ukrán háború, kibertámadás

[1] Doktori hallgató, Nemzeti Közszolgálati Egyetem Katonai Műszaki Doktori Iskola, e-mail: adriennk73@gmail.com
[2] Az Innovációs és Technológiai Minisztérium ÚNKP-23-3-I-NKE-114 kódszámú Új Nemzeti Kiválóság Programjának a Nemzeti Kutatási, Fejlesztési és Innovációs Alapból finanszírozott szakmai támogatásával készült.

Abstract

During the Russia-Ukraine war, cyberspace also emerged as a theatre of war, contributing significantly to transforming the nature of modern conflicts. This study aims to provide an empirical analysis of cyber-attacks during the Russian-Ukrainian war, focusing on the energy sector. The research examines data from 2022 to 2023, analyzing the temporal trends, geographical distribution, and types of attacks. The study highlights the importance of building, developing, and maintaining cyber defenses, analyzing attacks, and drawing lessons learned. The research used time series analysis, trend analysis, and heat map visualization as scientific methods. The results show which sector has become a particular target of cyber-attacks. In addition, it shows how critical infrastructure sectors have been attacked in the context of the war and the techniques used in the attacks.

Keywords: critical infrastructure, Russian-Ukranian war, cyber attack

Bevezetés

Napjaink egyik meghatározó kihívásainak tekintendők a kibertérben zajló konfliktusok, illetve ezen konfliktusoknak a globális hatásai. Az információs technológia fejlődése és a digitális infrastruktúra térhódítása alapjaiban változtatta meg a hadviselés fogalmát, így ki kell emelni az államok közötti fegyveres konfliktusokra vonatkozó aspektusát is. A 2022-ben kirobbant orosz–ukrán háború példátlan mértékű kibertámadások sorozatát indította el, amelyek célpontjai között szerepelnek többek között a kritikus infrastruktúrák, valamint magán- és közszolgáltatók is. Ezen támadások hatása messze túlmutat a harcmezőkön, hiszen ezek képesek a gazdasági, társadalmi és politikai stabilitás megingatására is.

A 2022-ben kezdődött orosz–ukrán háború idején végrehajtott kibertámadások rávilágítottak arra, hogy az államok közötti konfliktusok során a kibertérben zajló műveletek szerves részévé váltak a hadviselésnek. A háború jelentős mértékben érintette Ukrajna kritikus infrastruktúráit, jelentős károkat okozva a különféle kommunikációs rendszerekben, energiarendszerekben és egyéb technológiai rendszerekben is.[3] Az energiaszektort célzó támadások különösen nagy veszélyt jelentenek, hiszen ezek az ellátás megszakításával vagy a rendszerek megbénításával akár egész régiók működését is veszélyeztethetik. Az ilyen támadások hatásainak vizsgálata elengedhetetlen ahhoz, hogy megértsük, milyen kockázatokkal és kihívásokkal kell szembenézni a jövőben. A kritikus infrastruktúrák – kiemelendő az energiaszektor – rendkívül sebezhetővé váltak a kibertámadásokkal szemben. Ezek a támadások nem csupán a célpontként szolgáló államok működését zavarhatják meg, hanem közvetetten más-más országokat is érintve világszintű fenyegetéseket hordoznak magukban.[4] Számos támadó csoport célzott kibertámadásokkal próbálta megbénítani Ukrajna egyes kritikus infrastruktúráit,

[3] Singla et al. 2023: 18.
[4] Aviv–Ferri 2023.

ezzel is gyengítve az ország védekezőképességét és társadalmi stabilitását.[5] Már 2013 óta Oroszország számos alkalommal hajtott végre különböző kiberműveleteket Ukrajna ellen,[6] a háborút illetően pedig a kibertámadások nemcsak a katonai célpontokat, hanem a civil infrastruktúrákat is sújtották, ami a lakossági ellátást tekintve súlyosbította a háborúban felmerülő kockázatokat és a háború következményeit.[7] Mivel az ipari technológiák alkalmazása során egyre inkább az összekapcsolt és egymásra ható rendszerekről beszélhetünk, így ez a tény is újfajta biztonsági kihívásokkal – például a kibertámadásokkal szembeni védelmi megoldások alkalmazásának nehézségével – erősíti a kritikus infrastruktúrák védelmének akadályait.[8] A digitális térben zajló hadviselés új kihívásokat hoz a nemzetközi jog és kapcsolatok számára, mivel a kibertámadások hatásai nemzetközi szinten is érezhetők.[9] Az orosz–ukrán háború során végrehajtott kibertámadások nemcsak Ukrajnát, hanem a háborúban érintett más országokat is sújtották, amelyek jelenleg is a gazdasági, politikai és társadalmi stabilitást veszélyeztetik.[10]

A kutatás céljai kettősek voltak. Egyrészről, az érintett szektorokat – kitekintéssel az energiaszektorra – érintő kibertámadások részletes feltérképezése és elemzése volt, az orosz–ukrán háború során. A célkitűzés lényege, hogy átfogó képet nyújtson a kritikus infrastruktúrák körébe tartozó szektorokat – kitekintéssel az energiaszektorra – érintő kibertámadásokról, feltárva azok gyakoriságát. Másrészről a kutatás célja volt a támadók leginkább alkalmazott stratégiáinak és módszereinek azonosítása. Ez alapján a kutatás során célom, hogy azonosítsam a leggyakrabban alkalmazott támadási technikákat.

A kutatás során, a következő kutatási kérdéseket határoztam meg:

- Milyen mértékben és milyen típusú kibertámadások érték az energiaszektort az orosz–ukrán háború során?
- Milyen stratégiákat és módszereket alkalmaztak a támadók, az egyes szektorok elleni kibertámadások folyamán?

Ezek alapján a kutatás során a következő hipotéziseket állítottam fel:

H1: A kibertámadások mértékét tekintve az energia mint ágazat a leginkább támadott kritikusinfrastruktúra-szektor.

H2: A DDoS-t mint támadási technikát alkalmazták a támadók a leggyakrabban a kritikusinfrastruktúra-szektorok ellen.

[5] Chukhua 2023.
[6] Lunn 2023.
[7] Cyberpeace Institute 2022.
[8] Bhaiyat–Sithungu 2022: 48.
[9] Feledy–Virág 2022.
[10] Givens–Gorbachevsky–Biernat 2023: 12.

Tudományos módszer

Jelen cikkben szereplő adatok alapját az úgynevezett CyberPeace Institute (szervezet) nyújtotta. A szervezet jelenleg elsősorban, de nem kizárólagosan, az orosz–ukrán háború során történt kibertámadások felmérésére koncentrál. Tehát, bár a feljegyzett támadások száma bővülhet a jövőben, a cikk jelen formájában a hiteles információkra törekszik, így csak a szervezet által közölt és feljegyzett kibertámadásokkal foglalkozik. Érdemes tisztázni, hogy a szervezetnek saját metódusa van arra vonatkozóan, hogy mikor tekint incidensnek egy eseményt, így fontos, hogy adott feltételek valamelyike teljesüljön az incidensnek való minősítéshez.

Az adatgyűjtés során jelentős nehézségeket jelentett volna a dezinformáció, amely az orosz–ukrán háború információáramlására is jellemző. A hírfogyasztók és kutatók a háborúval kapcsolatos információkat számos esetben dezinformációként kezelik addig, amíg meg nem győződnek annak teljes hitelességéről. A háborúban előforduló információs torzítások általánosan megnehezítik, hogy a háború során bekövetkezett kibertámadásokat felmérjük és azonosítsuk és a hitelességüket ellenőrizzük.[11] Az elemzett adatok teljes mértékben ettől a szervezettől származnak, ugyanis hiteles módszerük van az események minősítésére. Az incidensek megerősítése, különösen Oroszországban és Fehéroroszországban, jelentős kihívást jelent. Az intézet az adatgyűjtést nyilvánosan elérhető információkra alapozza, beleértve médiaközleményeket, kormányzati és az egyes kiberbiztonsági jelentéseket. Minden azonosított incidenst legalább két belső elemző vizsgál meg, és ahol lehetséges, több forrással is megerősítik azt. A kibertámadások dokumentálása során az incidenseket az információforrások megbízhatósága alapján három kategóriába sorolják: megerősített, valószínű és lehetséges.

A kutatás három darab tudományos módszertant alkalmaz: idősorelemzést, trendelemzést és hőtérképes vizualizációt.

Eredmények

A kibertámadások gyakoriságának és módszereinek vizsgálata fontos, hogy megértsük a támadói oldal szemszögét, indíttatásait és azt, hogy összességében milyen képességek rejlenek a támadások alkalmazásai mögött. Azt azért érdemes megemlíteni, hogy az egyes kibertámadások nem pusztán az infrastruktúrák megzavarását célozzák meg, hanem előfordul, hogy összehangolt módon különféle dezinformációs kampányokkal is párosulnak. Olyan célok társulnak ezekhez a kampányokhoz, mint a saját narratívák népszerűsítése, az ellenség demoralizálása, bizalmatlanság keltése, konfliktusok provokálása stb.[12]

[11] Hameleers et al. 2024: 1642–1645.
[12] Ináncsi et al. 2023: 120–121.

Az orosz–ukrán háború rendkívüli mértékben tematizálta az online platformokat, és a támadók célja, a belpolitika szempontjából a szemben álló ország lakosságát, külpolitikai szempontból pedig a világot és a világ közvéleményét befolyásolni a saját preferenciák alapján.[13] Bár a jelen cikk a dezinformáció témáját kapcsolatba hozza a kibertámadások lebonyolításának mikéntjével, mélyebben nem vizsgálatam, ugyanis a kutatás célja a fő támadási technikák feltérképezése és a gyakoriságának vizsgálata volt, a dezinformációs tevékenységek alkalmazása pusztán kiegészítő információként jelentős.

Az idősorelemzés során a kibertámadások havi gyakoriságát vizsgáltam 2022. január 1. és 2023. december 31. között. A támadások számának elemzésekor érdemes elválasztani az egyes hónapokat, hogy részletesebb képet kaphassunk a támadások intenzitásának alakulásáról. A támadások nem pusztán az orosz és ukrán erőkre vonatkoznak, azonban a különféle országokban működő támadási célpontok valamilyen formában köthetőek a háborúhoz és a két szemben álló fél valamelyikéhez. Az 1. ábrán látható, hogy miként alakultak a trendek a támadási események bekövetkezése kapcsán. Fontos az egyes kiemelkedőbb hónapokat megemlíteni, hiszen a támadások számának kiugrásait feltételezhetően előidézhette a háború eseményeinek alakulása:

- 2022. február, az invázió kezdete, az ismert kibertámadások száma: 42 darab volt.

Az orosz–ukrán háború 2022. február 24-én robbant ki, amikor Oroszország katonai inváziót indított Ukrajna ellen. Már 2022 januárjában is voltak kibertámadások, februárban a kibertámadások száma megnőtt, nagy valószínűséggel az inváziához köthetően.

- 2022. március, az invázió intenzitásának növekedése, az ismert kibertámadások száma: 82 darab volt.

Az orosz erők folytatták a nagyobb ukrán városok ostromát. A kibertámadások száma az előző hónaphoz képest jelentősen megugrott, a háború intenzitásának növekedésével egyidejűleg.

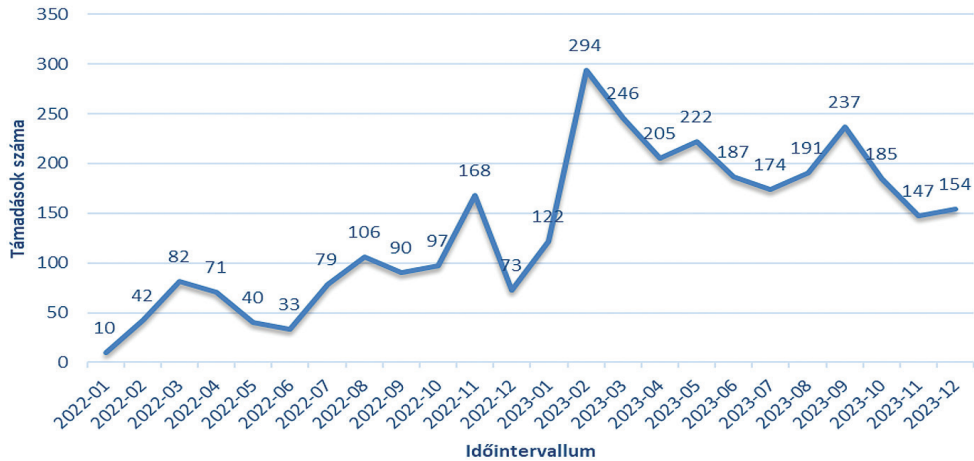
- 2022. november, a herszoni visszavonulás, az ismert kibertámadások száma: 168 darab volt.

2022 novemberében az orosz csapatok visszavonultak Herszonból, ami egyfajta katonai és stratégiai visszalépésnek minősült Oroszország szempontjából. A kibertámadások száma ebben a hónapban érte el a 2022-es év csúcsát. Ebből arra következtethetünk, hogy a visszavonulás hatására váltak intenzívebbé a kibertámadások.

- 2023. február, az egyéves évforduló, az ismert kibertámadások száma: 294 darab volt.

2023 februárjában volt a háború kezdetének egyéves évfordulója. A hónapban a kibertámadások száma jelentősen megugrott, ami feltételezhetően összefüggésbe hozható az évfordulóval kapcsolatos fokozott politikai és katonai feszültségekkel.

[13] Bányász et al. 2024: 56–57.



1. ábra: A kibertámadások számának alakulása a vizsgált időszakban
Forrás: a szerző szerkesztése a CyberPeace Institute adatai alapján

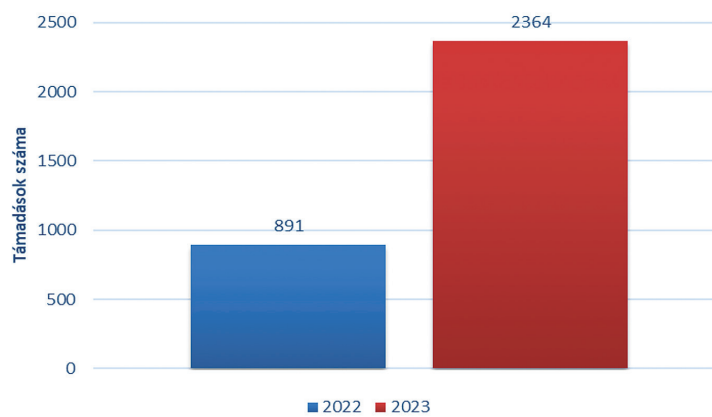
- 2023. szeptember, az őszi hadjáratok és ukrán ellentámadások, az ismert kibertámadások száma: 237 darab volt.

2023 szeptemberében az ukrán erők folytatták az ellentámadásokat Dél-Ukrajna és Kelet-Ukrajna területén. A kibertámadások száma ebben a hónapban ismét kiugróan magas volt, ami valószínűleg összeköthető az ellentámadások intenzitásával.

- 2023. december – év vége, az ismert kibertámadások száma: 154 darab volt.

Decemberben a támadások száma kismértékű növekedést mutat novemberhez képest, ami arra utalhat, hogy a felek az ünnepi időszakot is kihasználták a támadások számának fokozására. Azonban jelentős változást az év végének ténye sem okozott a kibertámadások számában.

A 2. ábrán látható a 2022-es és 2023-as kibertámadások száma, amely jelentős növekedést mutatott a 2023-as évben, a 2022-es évhez képest.



2. ábra: A kibertámadások évenkénti megoszlása az orosz–ukrán háborúban
Forrás: a szerző szerkesztése a CyberPeace Institute adatai alapján

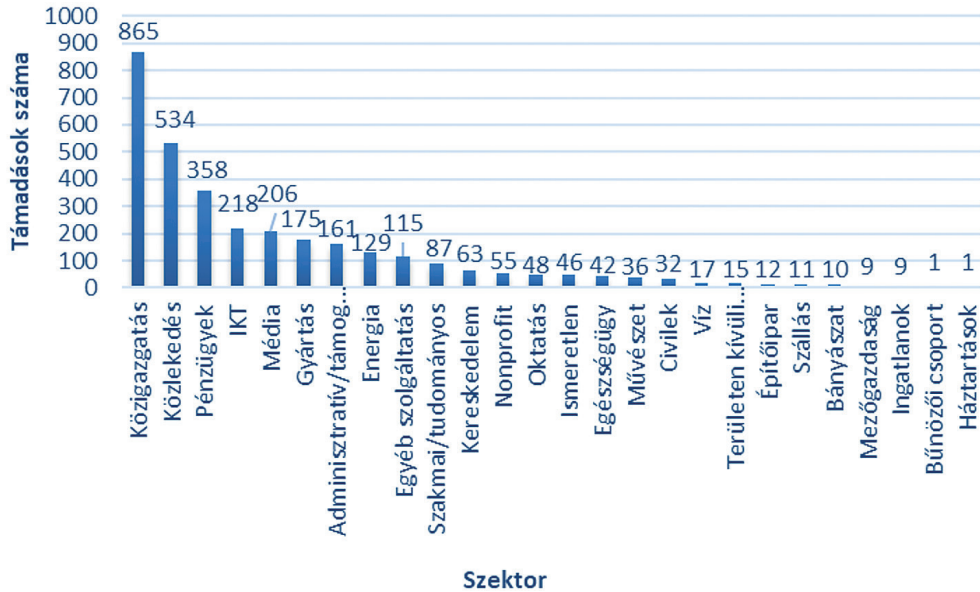
Az ismert támadások száma alapján 2022-ben 891 darab rögzített támadás volt, míg 2023-ra ez a szám 2364 darabra emelkedett. A növekedést, a támadók tapasztalatszerzésén túl az is okozhatja, hogy egyre többen csatlakoznak a különböző támadó csoportokhoz. Továbbá, a növekvő támadások száma nagy valószínűséggel összefüggésben áll a háború eszkalálódásával.

A támadások mennyiségének növekedése mellett a támadási módszerek és a célpontok is diverzifikálódtak 2023-ban. A háború során folyamatosan, egyre több szektor vált célponttá és a támadók újabb technikákat alkalmaztak. A támadások számának ilyen fokú növekedése azt is jelezheti, hogy a kibertámadások egy-egy konfliktusban vagy háborúban való alkalmazásának komplexitása nőtt, a kibertámadások lebonyolításához egyre több erőforrást lehet felhasználni mind a támadói, mind a védelmi oldalon. A számadatok arra is utalhatnak, hogy a jövőben a kibertámadások száma még tovább növekedhet, különösen akkor, ha a politikai feszültségek fennmaradnak vagy tovább fokozódnak.

A támadások számának növekedésével együtt érdemes megemlíteni azt a tényezőt is, hogy a 2022-ben kirobbant háború során nem ment végbe olyan kiberművelet, amely kiterjedt módon megbénította volna Ukrajna kritikus nemzeti infrastruktúráját. A háború előrehaladtával számos, eltérő nézőpont alakult ki arról, hogy a háború kiberműveleti oldala mennyire jelentős. Oroszország már évek óta fejleszti és alkalmazza a kiberműveleti képességeit, és ahogyan a későbbi ábrákon is meg lehet figyelni, a különféle műveletek nem pusztán az infrastruktúrák megzavarását célozzák, hanem a propaganda és a dezinformáció célzatával is alkalmazzák őket.[14] Továbbá Oroszország – a Geraszimov-doktrína értelmében – a közösségi médiát is egy szélesebb hadszíntér részének tekinti. A háború közösségimédia-megjelenését és a két szemben álló fél egymáshoz való viszonyát vizsgáló tanulmány alapján, a háború kitörése után, a másik ország iránt az ukránok 2%-a és az oroszok 23%-a mutatott pozitív hozzáállást. Ugyanezek a számok a tanulmány alapján 83% és 74%-os mutatók voltak 2012-ben.[15] Ez a példa a jelen cikk szempontjából azért is lényeges, mert a közösségi média potenciálisan hozzájárulhat ahhoz, hogy egy amúgy is ellenséges hangulatot felerősítsen, és feltételezhetően ahhoz is hozzájárulhat, hogy ösztönözze a támadói egyének és csoportok tevékenykedéseit.

Összességében a kibertámadások évenkénti megoszlása rávilágít a kibertér kihasználásának egyre növekvő jelentőségére napjaink modern konfliktusaiban. A kibertámadások intenzitásának növekedése égetővé teszi a kiberbiztonsági intézkedések megtételének fokozását, valamint a nemzetközi együttműködések erősítését ezen a téren.

[14] Willet 2022: 7–8.
[15] Kyrychenko et al. 2024: 1–3.



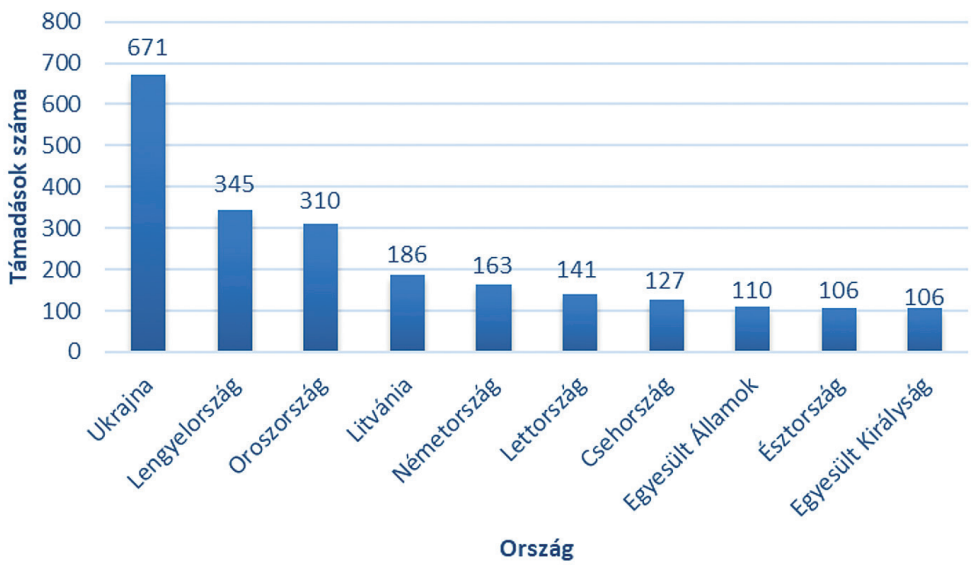
3. ábra: A kibertámadások számának megoszlása a célpontszektorok alapján
Forrás: a szerző szerkesztése a CyberPeace Institute adatai alapján

Megvizsgáltam a támadások ágazatspecifikus megoszlását, amely a 3. ábrán látható: az elemzett időszakban a közigazgatás, a közlekedés (amelybe a szállítmányozás, ellátási láncok is beletartoznak), a pénzügyi, az infokommunikációs technológiák (IKT), valamint a média ágazatot érte a legtöbb támadás. Az energiaszektor a kibertámadások számának tekintetében a 8. helyet foglalja el, az ismert kibertámadások száma 129 darab. Ez alapján elmondható, hogy a feldolgozott adatok szerint a kibertámadások mennyiségének szempontjából az energiaszektor – a többi kritikus szektorhoz viszonyítva – korántsem volt annyira érintett, mint például a közigazgatás, a közlekedés vagy a pénzügyi szektor.

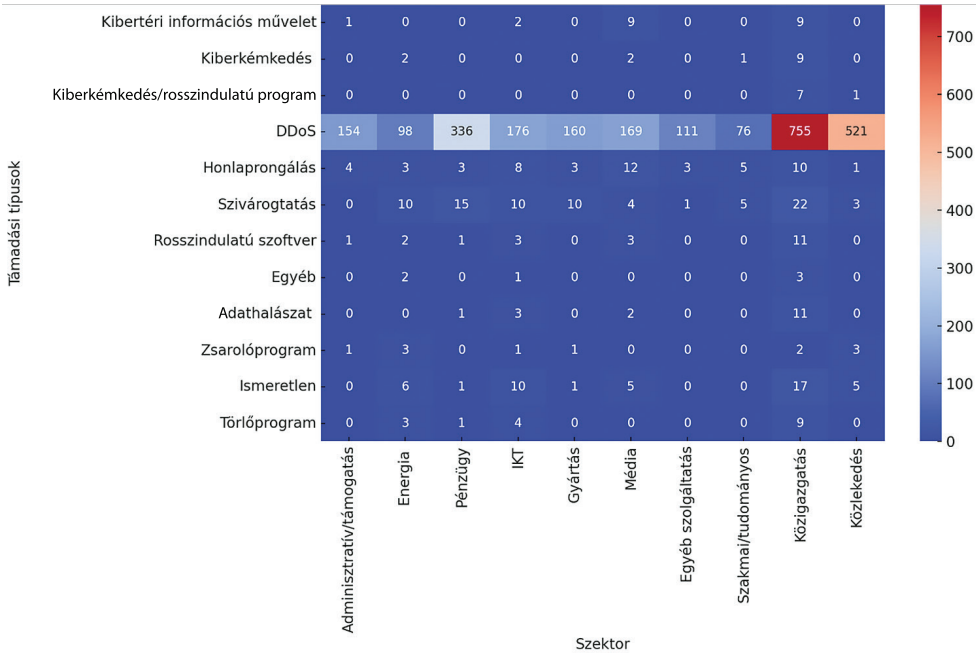
Az 4. ábra alapján elmondható, hogy a 2022-es és 2023-as évben a kibertámadásokban leginkább érintett ország Ukrajna, Lengyelország, Oroszország, Litvánia és Németország. Az ábrákon már nem látható, de a listán még számos más ország is szerepel, mint például Olaszország, Svédország, Spanyolország vagy éppen Szlovákia, Fehéroroszország vagy Horvátország. Az országonkénti kibertámadások számának megoszlása a vizsgált időszakban jelentős eltéréseket mutat, ami rávilágít a geopolitikai és a kibertérben fellelhető feszültségek összefüggéseire. Ukrajna messze a legtöbb kibertámadási incidenst szenvedte el, összesen 671 darab dokumentált támadással. Ukrajnának nagy valószínűséggel a háború alatt, illetve már az azt megelőző években is jelentős erőforrásokat kellett mozgósítania a kibervédelmi képességeinek a megerősítésére.

Ukrajnát a sorban Lengyelország követi 345 darab támadással, majd – Oroszországot, Németországot, Csehországot és az Egyesült Államokat leszámítva – a balti államok, különösen Litvánia (186 darab támadás), Lettország (141 darab támadás)

és Észtország (106 darab támadás), amely országoknál szintén viszonylag magas számú kibertámadási eseményt regisztráltak. Ezek az országok feltételezhetően stratégiai helyzetük miatt váltak célponttá, különösen az Oroszországgal való közelségük és NATO-tagságuk miatt. Az ilyen országokban megjelenő kibertámadások akár geopolitikai célokat is szolgálhatnak, például a NATO és az Európai Unió destabilizálását. Oroszországban 310 darab kibertámadást dokumentáltak, ami azt jelzi, hogy nemcsak támadóként, hanem célpontként is érintett az ország. A támadások egy része valószínűleg válaszlépésként érkezhetett a háborús tevékenységekre, illetve olyan célok is szolgálhattak a támadások hátterében, mint az orosz állam destabilizálása. Nyugat-európai országok, mint Németország (163 darab támadás) és az Egyesült Királyság (106 darab támadás) szintén gyakorta megjelenő célpontok voltak. Ezek az országok fontos gazdasági és politikai szereplők, így a támadások célja feltételezhetően lehetett a gazdasági zavarok okozása vagy politikai nyomásgyakorlás is. Az Egyesült Államok (110 darab támadás) szintén a 10 leggyakrabban támadott ország közé tartozik, különösen mint a globális hatalom egyik központja. Számos kisebb országban is dokumentáltak kibertámadásokat, bár ezek száma jelentősen alacsonyabb. Ezen országok, előfordul, hogy közvetett célpontokként jelennek meg, vagy más országokkal kapcsolatos konfliktusok miatt válnak célponttá.



4. ábra: A 10 legtöbb kibertámadást elszenvedő ország a vizsgált időszakban
Forrás: a szerző szerkesztése a CyberPeace Institute adatai alapján



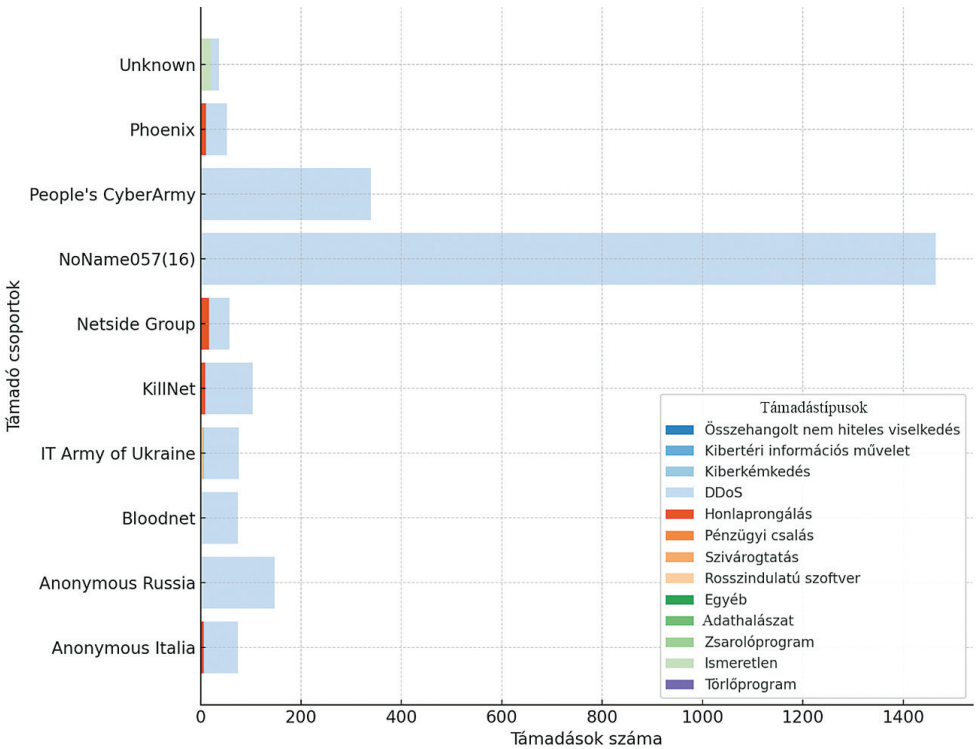
5. ábra: A 10 leginkább támadott ágazat hőtérképes mátrixa a támadástípusok szerint
Forrás: a szerző szerkesztése a CyberPeace Institute adatai alapján

Az 5. ábrán látható a tíz leginkább támadott szektorban előforduló különböző támadási típusok eloszlása összesítetten a vizsgált időszakban és az összes, vizsgált országra vonatkozóan. A rendelkezésre álló információk alapján – ahogy a 3. ábrán is megjelent – a közigazgatás, a közlekedés és a pénzügyi szektor voltak a legtöbbször érintett célpontok, különösen az elosztott túlterheléses (DDoS) támadások szempontjából. A 2022-es és 2023-as évet összesítve, a közigazgatási szektort érte a legtöbb DDoS-támadás, míg a közlekedési és pénzügyi szektort szintén jelentős mennyiségű DDoS-támadás érte, de látható, hogy más típusú kibertámadásokat is alkalmaztak a támadók, mint például a szivárogtatást *(hack and leak)*. Az energiaszektort is többfajta támadás érte, gyakori eset a szivárogtatás vagy a törlőprogramok alkalmazása, azonban itt is kiemelkedik ezek közül a DDoS mint támadási forma. Az ábra rávilágít arra, hogy a különböző szektorok számos, akár eltérő támadási módszerekkel néznek szembe. A DDoS-támadások a legtöbb szektorban dominálnak, különösen a közigazgatásban, közlekedésben és a pénzügyi szektorban, míg például a szivárogtatás a közigazgatás és pénzügyi szektoron kívül az energia- vagy az IKT-szektorban is megjelenik.

Az egyes rubrikákon belüli színtelítettség a támadások számának nagyságát jelzi, átlátható mátrixát nyújtva az érintett támadási technikáknak és szektoroknak. Az ábra alapján vélelmezhetően a közigazgatás, a közlekedés és a pénzügyi szektorban – az adatok alapján – adott mértékben magasabb szintű védelmi funkciókat szükséges kiépíteni, mint a többi szektorban a kiberbiztonsági kockázatok mérséklésének céljából. Azonban nem elhanyagolható a többi szektor, mint például az energiaszektor védelmének fejlesztése és fenntartása sem, bár vélelmezhetően az energiaszektor esetében magasabb

fizikai károkozásról lehet beszélni, mint kibertéri károkozásról. A közigazgatási szektor esetében feltételezhető, hogy a kibertérben zajló támadások nagyobb károkat tudnak okozni, mint a fizikai térben lévők.

A 6. ábra bemutatja a tíz legaktívabb támadó csoport által alkalmazott támadási típusok megoszlását. Látható, hogy a NoName057(16) csoport volt a legaktívabb, főként DDoS-támadások végrehajtásával. Ezt követi a People's CyberArmy, amely csoport szintén jelentős számú DDoS-támadást hajtott végre. A honlaprongálás mint támadási formában a Netside Group és a Phoenix, illetve a KillNet csoportok voltak a legaktívabbak, míg a szivárogtatás típusú támadásokban az IT Army of Ukraine 6 darab rögzített támadási eseménnyel és az Anonymous Russia 1 darab rögzített támadási eseménnyel voltak a legkiemelkedőbbek.



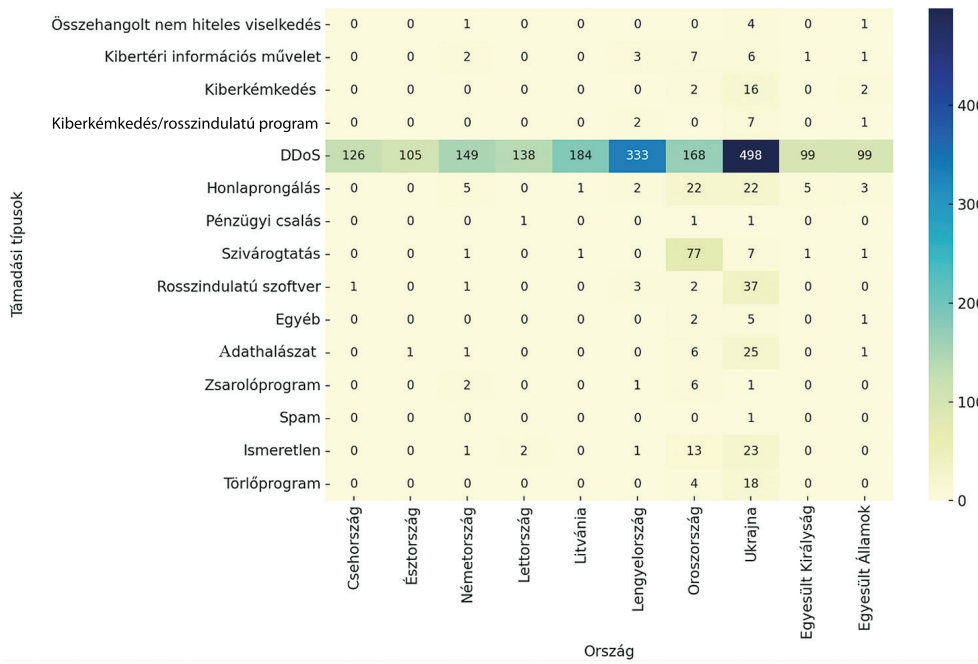
6. ábra: A különböző támadástípusok megoszlása a 10 legaktívabb támadó csoporthoz köthetően
Forrás: a szerző szerkesztése a CyberPeace Institute adatai alapján

A be nem azonosítható *(unknown)* kategóriába sorolt támadók számos különböző támadási módszert alkalmaztak, de leginkább az adathalászatot vetették be a célpontok ellen.

Ahogyan a korábbiakban is látható volt, a DDoS-támadások dominálják a legtöbb támadó csoport tevékenységét, különösen a NoName057(16) csoport és a People's CyberArmy esetében. Ezek a csoportok a támadások számában és intenzitásában is kiemelkednek a DDoS-támadás elkövetésének szempontjából. Összességében, bár

a támadó csoportok többféle támadási módszert alkalmaztak, azokat a DDoS-támadásokhoz képest csak elvétve alkalmazták, így az ábrán is alig-alig jelennek meg. Ezen felül – további kutatási szempontokból – még további elemzést érdemel azoknak a támadó csoportoknak a vizsgálata, amelyek a 6. ábrán nem jelennek meg, mert kevésbé minősültek aktív szereplőknek. Azonban ezek a csoportok változatosabb támadási formákat alkalmaztak.

A 7. ábrán látható a vizsgált időszakban a 10 leginkább támadott ország és az ellenük alkalmazott különböző támadástípusok hőtérképes mátrixa. A DDoS támadási forma számosságát tekintve az összes ország esetében kiemelkedik. Ez különösen Ukrajna, Lengyelország és Litvánia esetében számottevő. A honlaprongálás, a rosszindulatú szoftver alkalmazása és a szivárogtatás legfőképpen Oroszország és Ukrajna esetében jelentős.



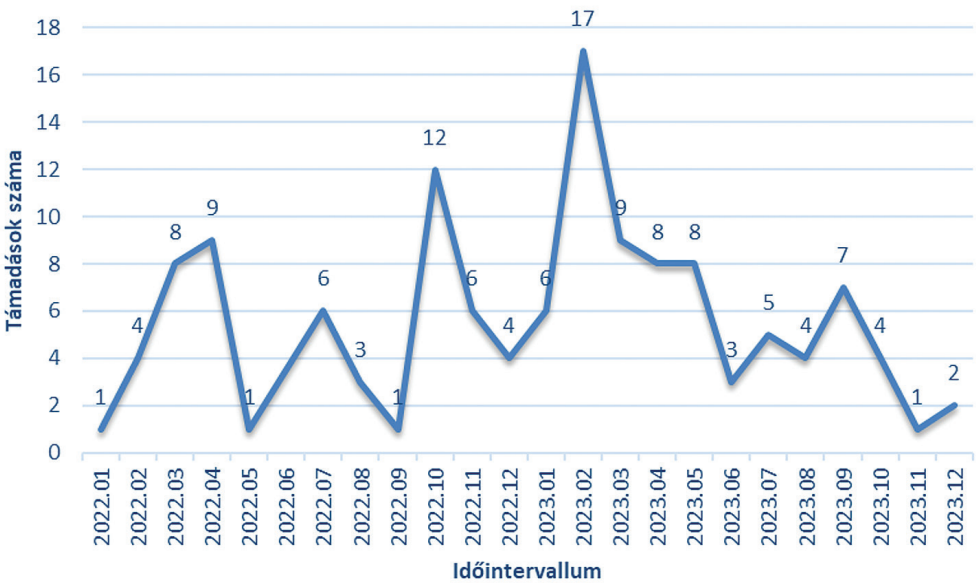
7. ábra: A 10 leginkább támadott ország és az őket ért támadási fajták hőtérképes mátrixa
Forrás: a szerző szerkesztése a CyberPeace Institute adatai alapján

A 6. ábrához hasonlóan a 7. ábrán is a támadások gyakoriságának nagysága látható, jelen esetben a támadási technikák és célpontországok mátrixaként. Látható, hogy az orosz–ukrán háborút illetően, bár Ukrajna a fő célpont, nem tekinthetünk el attól, hogy a háborús felek mellett más-más országok is célpontként szolgálnak. A feldolgozott adatok, ezzel együtt a támadások összessége az orosz–ukrán háborúhoz köthető valamilyen szempontból, tehát nem pusztán a szemben álló feleknek kell a kibervédelmükre – és annak a fejlesztésére – koncentrálni, hanem ez az érintett és egyébként minden más ország számára is fontos cél kell hogy legyen.

Energiaszektor

Az energiaszektor az egyik legkritikusabb iparág, így sokkal könnyebben válhat a kibertámadások célpontjává, mint más – ehhez az ágazathoz viszonyított – kritikus szektor, különösen olyan rendkívüli helyzetekben, mint az orosz–ukrán háború. Az energiaellátás megszakadása súlyos következményekkel járhat többek között a gazdaságra és a társadalom működésére is. Az alábbiakban több szempontból is vizsgálom az energiaszektort, beleértve az időbeli trendeket, a támadástípusok megoszlását, a támadó csoportok kapcsolatát a szektorral és az energiaszektort érintő kibertámadások földrajzi megoszlását.

Először azt vizsgálom, hogyan változott az energiaszektor elleni támadások száma a vizsgált időszakban:



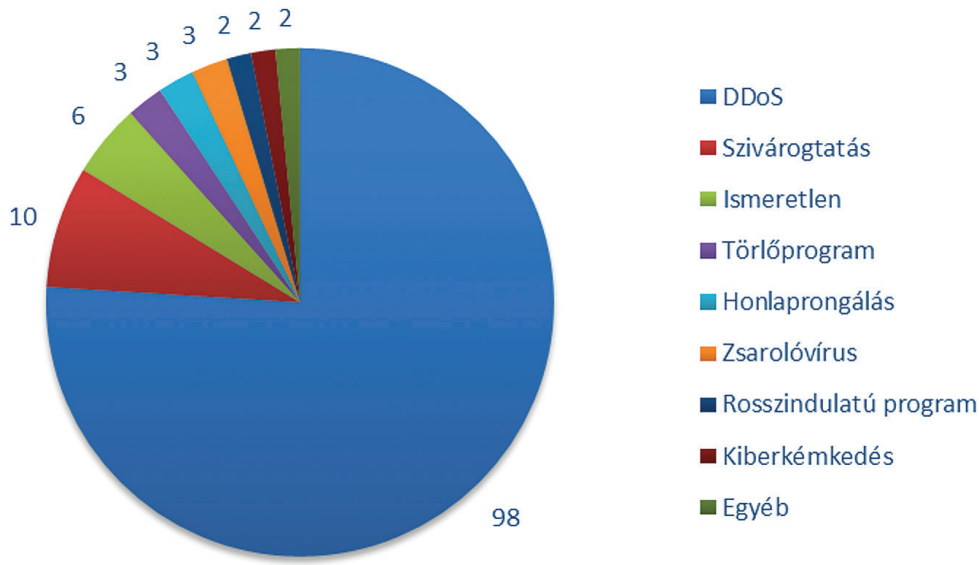
8. ábra: Energiaszektor elleni kibertámadások száma a vizsgált időszakban
Forrás: a szerző szerkesztése a CyberPeace Institute adatai alapján

A 8. ábrán az energiaszektor elleni kibertámadások (összesen: 129 darab) időbeli elemzése alapján megfigyelhető, hogy a támadások száma jelentős ingadozásokat mutatott a vizsgált időszakban. 2022 elején az energiaszektor elleni támadások száma fokozatosan növekedett, különösen a háború első hónapjaiban. Márciusban és áprilisban megvalósult az első csúcsosodás. Ez az időszak jelentős volt ebből a szempontból a háború kezdeti szakaszában, a támadók feltételezhetően arra törekedtek, hogy destabilizálják az energiaellátást.

A vizsgált időszak távlatában a támadások száma 2023 februárjában érte el a csúcsot, ekkor 17 darab kibertámadást regisztráltak. Ez valószínűleg összefügg a háború egyéves évfordulójával és az energiaellátás megbénítására irányuló törekvésekkel. A támadások száma az év hátralévő részében viszonylag ingadozó volt, és többet már

nem érte el a februári csúcsot. Feltételezhetően azért, mert a támadók stratégiája folyamatosan változó volt, és a támadások intenzitása a háború menetétől, a politikai történésektől függően alakult.

A támadási technikák elemzése során azt vizsgálom, hogy az energiaszektorban mely típusú kibertámadások voltak a leggyakoribbak. Ez segít megérteni, hogy milyen típusú fenyegetésekkel szembesül ez a szektor.

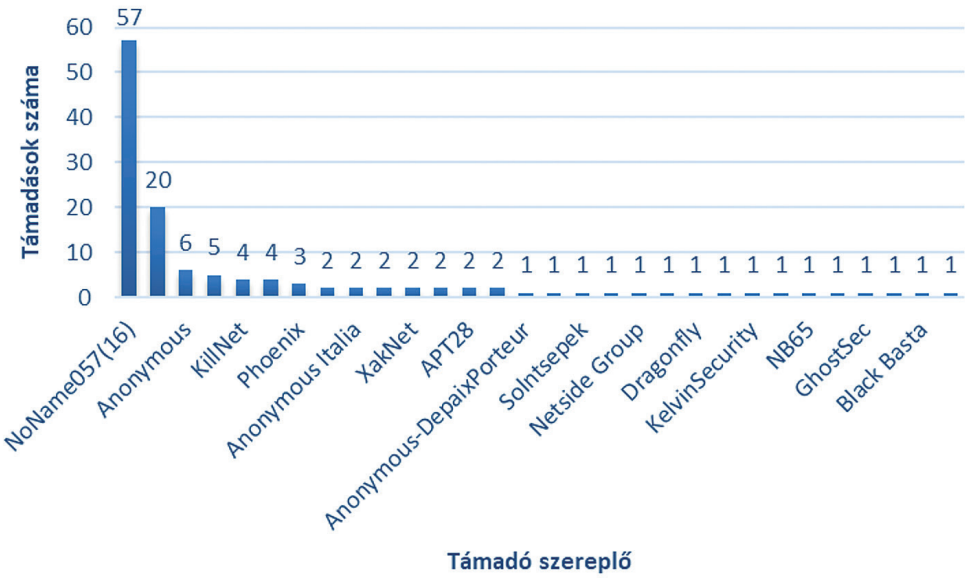


9. ábra: Energiaszektor elleni kibertámadások típusa
Forrás: a szerző szerkesztése a CyberPeace Institute adatai alapján

Ahogyan a 9. ábrán is látható, az energiaszektor elleni kibertámadások típusainak elemzése során a következő, főbb megállapításokat tehetjük: A DDoS-támadások voltak messze a leggyakoribbak az energiaszektorban is, összesen 98 darab ismert támadással. A támadások célja nagy valószínűséggel az volt, hogy túlterheljék az infrastruktúrát, ezzel megszakítva a szolgáltatások működését. A DDoS-támadások gyakorta minősülnek elsődleges választásnak a kritikus infrastruktúrák elleni támadások esetén, mivel gyorsan és viszonylag egyszerűen képesek jelentős zavarokat okozni.

A második leggyakoribb támadástípus a szivárogtatás volt, ahol a támadók olyan információkat szereztek meg, amelyeket a megszerzés után kiszivárogtatnak. Ez a fajta támadás 10 alkalommal fordult elő, potenciális célja a bizalom megrendítése vagy politikai célok elérése lehetett. A támadók ekkor érzékeny adatok kiszivárogtatásával próbálnak nyomást gyakorolni a támadásban érintett szervezetekre vagy országokra. Kismértékben ugyan, de jellemzők voltak még azok a támadási fajták is, amelyeket konkrétan nem lehetett behatárolni, hogy hova tartoznak, pusztán a kibertámadás tényét lehetett sejteni.

A következő elemzésben feltárom, hogy mely támadó csoportok voltak a legaktívabbak az energiaszektort érintő támadások okozása során. Az energiaszektor elleni támadásokat elemezve a következő főbb támadó csoportok emelkedtek ki:

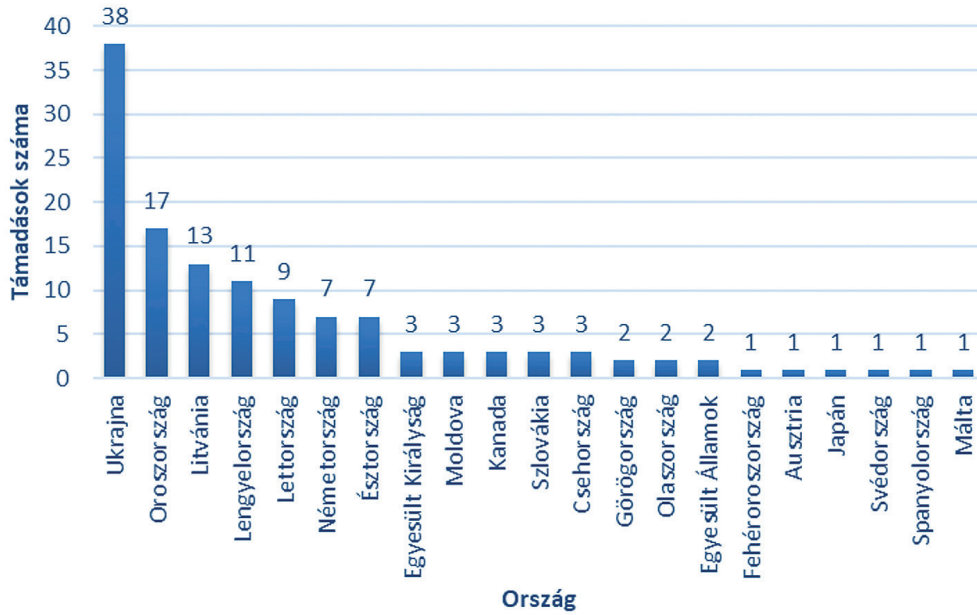


10. ábra: Az energiaszektort támadó csoportok és az általuk indított támadások számának megoszlása
Forrás: a szerző szerkesztése a CyberPeace Institute adatai alapján

A 10. ábrán látható, hogy a NoName057(16) volt a legaktívabb támadó csoport az energiaszektorban, összesen 57 darab támadással. Ez a csoport elsősorban DDoS-támadásokat hajtott végre, amely támadások célja az energiaellátás biztosításának akadályoztatása volt. Szintén az energiaszektor tekintetében a People's CyberArmy a második legaktívabb csoport, 20 darab támadás indításával. Ez a csoport szintén a DDoS-támadások alkalmazására fókuszált. Az energiaszektort érő támadások tekintetében az Anonymous és más hacktivista csoportok, mint például az Anonymous Italia és Anonymous-DepaixPorteur, szintén aktívak voltak, bár jóval kisebb mértékben, mint az első két helyen említett csoport. A Sandworm, az APT28 és az IT Army of Ukraine az energiaszektort kevésbé támadták más szektorokhoz képest.

Érdemes megemlíteni, hogy a különféle támadó csoportok tevékenysége gyakran része a szélesebb körű katonai stratégiáknak, ahol a kibertámadások a fizikai támadások kiegészítéseként szolgálnak.

Az energiaszektorra vonatkozó utolsó elemzési szempont során azt vizsgálom, hogy az energiaszektor mely országokban volt a leginkább érintett a kibertámadások által.



11. ábra: Az energiaszektort érő támadások földrajzi eloszlása
Forrás: a szerző szerkesztése a CyberPeace Institute adatai alapján

A 11. ábrán megfigyelhető az energiaszektor elleni kibertámadások földrajzi eloszlása, ami fontos információkat nyújt arról, hogy mely országok voltak a leginkább érintettek célpontként a vizsgált időszakban. Az energiaszektor elleni támadások többsége Ukrajna ellen irányult, ahol összesen 38 darab kibertámadást regisztráltak. Ez összhangban áll a háborús körülményekkel, ahol az energiaellátás megszakítása közvetlen hatással lehet a háborús erőfeszítésekre és a lakosság életére.

Ahogyan a 3. ábra kapcsán is említettük, Oroszország is célpont volt ebben a tekintetben, 17 darab támadás érte az országot. Ezen felül a balti államok, mint Litvánia (13 darab támadás), Lettország (9 darab támadás) és Észtország (7 darab támadás), szintén célpontoknak minősültek nemcsak összességében, de az energiaszektor tekintetében is. Az Egyesült Államokban és Kanadában is jelentek meg kibertámadási incidensek az energiaszektor ellen (2 és 3 darab támadás), ami arra utal, hogy a támadók globálisan is figyelembe veszik a stratégiai energiaforrásokat. Így az ezen országokat érintő támadások célja feltételezhetően az, hogy zavart keltsenek a nemzetközi energiaellátásban.

Összegzés

Az orosz–ukrán háború kibertámadásai eddig kismértékben tapasztalt, újszerű kihívásokat hoztak magukkal a modern, technológián nyugvó kritikus infrastruktúrák számára. A kutatás célja az volt, hogy átfogóan elemezze az ismert kibertámadásokat, kitekintéssel az energiaszektorra. Az elmúlt években tapasztalt jelentős digitális fejlődés,

valamint a globális hálózati infrastruktúra növekvő függősége miatt a kibertámadások egyre komolyabb fenyegetést jelentenek. Ezen támadások nem csupán a katonai célpontokat érintik, hanem széles körben hatnak a civil infrastruktúrára, a pénzügyi rendszerekre és a kritikus ellátási láncokra is. Az energiaszektor különösen sebezhető, mivel a modern társadalmak energiafüggősége központi szerepet játszik a mindennapi élet fenntartásában és a gazdasági stabilitás megőrzésében. A kibertérben zajló harcok nemcsak a konfliktus közvetlen résztvevőire, hanem a globális közösségre is kihatnak, hiszen a digitális világ határok nélküli természetéből fakadóan a támadások könnyen érinthetnek más államokat is, illetve világszintű gazdasági és politikai következményekkel járhatnak. Az orosz–ukrán háború során alkalmazott kibertámadások nem pusztán az energiaszektorra irányuló támadások révén váltak jelentőssé, bár az energiaellátás zavarai közvetlen hatással vannak a lakosság életminőségére, az ipari termelésre és a nemzetbiztonságra. Az országonkénti megoszlás rávilágított arra, hogy a kibertámadások eloszlása szorosan összefügghet a geopolitikai helyzettel is. Azok az országok, amelyek közvetlenül érintettek háborúban – mint például Ukrajna – és a helyzet adta további konfliktusokban, vagy éppen stratégiai jelentőségűek, mint Lengyelország és a balti államok, vannak a legnagyobb fenyegetésnek kitéve.

Az energiaszektor nem a legnagyobb mértékben, de ugyanúgy célpont volt a 2022-es év és 2023-as év között vizsgált kibertámadások során, különösen a háborúban közvetlenül érintett régiókban. Az elemzés rámutatott, hogy az energiaellátás megszakítása a kibertámadások szempontjából nem a legfontosabb, de fókuszban lévő eleme volt a támadók stratégiájának. Továbbra is igaznak bizonyult, hogy az energiaszektor védelme fontos, különösen a jelenlegi, rendkívül feszült, globális helyzetben.

A kutatás célja egyrészről a kritikusinfrastruktúra-szektorokat érintő, az orosz–ukrán háború első két évében lezajlott kibertámadások elemzése volt, kitekintéssel az energiaszektorra, valamint a támadók stratégiáinak, leggyakrabban használt támadási technikáinak azonosítása.

A kutatás során a kutatási célkitűzések és kérdések megfogalmazása után két darab hipotézist állítottam fel. Ezeket három darab tudományos módszertannal vizsgáltam: végeztem trendelemzést, idősorelemzést és hőtérképes megjelenítést. A kutatás során a hipotézisekhez kapcsolódóan két darab megállapítás született:

T1: A kibertámadások mértékét tekintve nem az energiaágazat a leginkább támadott kritikusinfrastruktúra-szektor, hanem a közigazgatási szektor.

T2: A DDoS-t mint támadási technikát alkalmazták a támadók a leggyakrabban a kritikusinfrastruktúra-szektorok ellen.

A kibertámadások számának és a támadási technikáknak a fajtája változó volt, de általánosságban elmondható, hogy a DDoS-támadások és a zsarolóvírus-támadások voltak a leggyakrabban előforduló technikák. Ezek a támadások súlyos működési zavarokat tudnak okozni a szolgáltatások ideiglenes megállását, a rendszerek megbénulását eredményezve.

A jelen cikkben feldolgozott adatokat a jövőben szükséges lesz további szempontok alapján is feldolgozni és elemezni ahhoz, hogy a jövőben megfelelő következtetéseket lehessen levonni. A kutatási eredmények hasznosíthatók a jövőben az orosz–ukrán háború kibertámadásainak további elemzésére és a védelmi megoldások kialakításának megalapozásához.

Felhasznált irodalom

Aviv, Itzhak – Ferri, Uri (2023): Russian-Ukraine Armed Conflict: Lessons Learned on the Digital Ecosystem. *International Journal of Critical Infrastructure Protection,* 43, 1–31. Online: https://doi.org/10.1016/j.ijcip.2023.100637

Bányász, Péter et al. (2024): Empirical Studies of Russian–Ukrainian War Related Fake News – Part 2. *Hadmérnök,* 19(1), 55–83. Online: https://doi.org/10.32567/hm.2024.1.4

Bhaiyat, Humairaa – Sithungu, Siphesihle (2022): The Emergence of IIoT and its Cyber Security Issues in Critical Information Infrastructure. *European Conference on Cyber Warfare and Security,* (21)1, 46–51. Online: https://doi.org/10.34190/eccws.21.1.248

Chukhua, Ilona (2023): Russian Aggressive Cyber-Policy During Russia-Ukraine War. In Chitadze, Nika (szerk.): *Cyber Security Policies and Strategies of the World's Leading States.* Hershey, PA: IGI Global, 224–238. Online: https://doi.org/10.4018/978-1-6684-8846-1.ch014

CyberPeace Institute (2022): Cyber Attacks in Times of Conflict. Online: https://cyberconflicts.cyberpeaceinstitute.org/threats

Feledy, Botond – Csaba, Virág (2022): An Assessment of Cyber Volunteer Groups in Interstate Conflicts and Their Impact on Public Policies. *Scientia et Securitas,* 3(1), 1–7. Online: https://doi.org/10.1556/112.2022.00091

Givens, Austen – Gorbachevsky, Max – Biernat, Anita (2023): How Putin's Cyber-war Failed in Ukraine. *Journal of Strategic Security,* 16(2). Online: https://doi.org/10.5038/1944-0472.16.2.2099

Hameleers, Michael et al. (2024): Mistakenly Misinformed or Intentionally Deceived? Mis- and Disinformation Perceptions on the Russian War in Ukraine Among Citizens in 19 Countries. *European Journal of Political Research,* 63(4), 1642–1654. Online: https://doi.org/10.1111/1475-6765.12646

Ináncsi, Mátyás et al. (2023): Empirical Studies of Russian–Ukrainian War Related Fake News, Part 1. *Hadmérnök,* 18(4), 109–128. Online: https://doi.org/10.32567/hm.2023.4.8

Kyrychenko, Yara et al. (2024): Social Identity Correlates of Social Media Engagement Before and After the 2022 Russian Invasion of Ukraine. *Nature Communications,* 15(8127). Online: https://doi.org/10.1038/s41467-024-52179-8

Lunn, Stephen (2023): Human Security and the Digital Threat: Russia and Ukraine. In Reimer, L. E. – Standish, K. (szerk.): *Perspectives on Justice, Indigeneity, Gender, and Security in Human Rights Research.* Singapore: Palgrave Macmillan, 263–283. Online: https://doi.org/10.1007/978-981-99-1930-7_13

Singla, Rishabh et al. (2023): An Analysis of War Impact on Ukrainian Critical Infrastructure Through Network Measurements. In *Proceedings of the 2023 7th Network Traffic Measurement and Analysis Conference (TMA).* Naples, 1–10. Online: https://doi.org/10.23919/TMA58422.2023.10199005

Willett, Marcus (2022): The Cyber Dimension of the Russia–Ukraine War. *Survival: Global Politics and Strategy,* 64(5), 7–26. Online: https://doi.org/10.1080/00396338.2022.2126193