Vladimir Prebilič,
Patrik Rebrica

DOI: 10.2478/cmc-2024-0030

KIBERNETSKO VOJSKOVANJE V RUSKO-UKRAJINSKI VOJNI

CYBER WARFARE IN THE RUSSO-UKRAINIAN WAR

Povzetek Kibernetsko vojskovanje je v sodobnih konfliktih odprlo novo dimenzijo vojskovanja. Nevarnosti so večje kot kdaj koli prej, saj kritična infrastruktura, finančni sistemi in osebni podatki postajajo tarče na tem digitalnem bojišču. Cilj prispevka je prikazati vpliv kibernetskega vojskovanja v rusko-ukrajinski vojni. Za razumevanje kibernetske vloge v vojskovanju je treba razumeti rusko, ukrajinsko in Natovo doktrino kibernetskega bojevanja ter aplikacijo le-teh na bojišču. Razumevanje teh taktik omogoča boljšo nacionalno obrambo držav, zaščito življenj civilistov in zagotavljanje stabilnosti globalne digitalne infrastrukture. Analiza kibernetske razsežnosti tega konflikta pomaga razviti strategije za ublažitev podobnih groženj v prihodnjih konfliktih.

Ključne besede ***Kibernetika, kibernetsko vojskovanje, vojna, doktrina, obramba, rusko-ukrajinska vojna.***

Abstract Cyber warfare has opened up a new dimension of warfare in modern conflicts. The dangers are greater than ever as critical infrastructure, financial systems and personal data become targets on this digital battlefield. The aim of this work is to show the impact of cyber warfare through the example of the Russian-Ukrainian war. To understand the role of cyber in warfare it is necessary to understand Russian, Ukrainian and NATO cyber warfare doctrine, and utilisation of these on the battlefield. Understanding these tactics allows for better national defence of states, protection of civilian lives and ensuring the stability of the global digital infrastructure. Analysing the cyber dimension of this conflict helps to develop strategies to mitigate similar threats in future conflicts.

Key words ***Cybernetics, cyber warfare, war, doctrine, defence, Russo-Ukrainian war.***

Uvod

Kibernetsko vojskovanje je v rusko-ukrajinski vojni odprlo novo fronto bojevanja, ki je bistvenega pomena za strokovnjake. Če gledamo ta konflikt zgolj z obrambnega vidika, je analiza uporabljenih taktik in doktrin v konfliktu dragocena lekcija za druge države, ki bi rade izboljšale svojo kibernetsko obrambo. Države, predvsem članice Nata, so začele zaradi tega konflikta namenjati večjo pozornost svojim kibernetskim zmogljivostim (Willet, 2022).

Internet je spremenil naš pogled na svet in interakcijo z njim na veliko načinov, na žalost pa ta sprememba ni omejena le na mirnodobne dejavnosti. Ta razvoj vpliva tudi na način bojevanja vojn. Zdaj, ko je vsaka država povezana z internetom in odvisna od njega za novice, volitve ter komuniciranje s svojimi državljani, je pomembno razumeti, kako kibernetsko vojskovanje deluje. Vojna v Ukrajini je dober primer za analizo kibernetskega vojskovanja. V vojni med Rusijo in Ukrajino je imelo kibernetsko vojskovanje več pomenov za sodobne spopade. Kibernetski napadi niso le nova dimenzija vojskovanja, temveč so tudi dopolnili tradicionalne vojaške taktike in lahko ciljajo na digitalno ter tudi fizično infrastrukturo. Pred in med vojno so se ti napadi pogosto uporabljali za ustvarjanje zmede in oslabili so poveljevanje ter tudi moralo vojakov ali civilistov. Če kibernetsko vojskovanje primerjamo s konvencionalnim bojevanjem, je s finančnega in gospodarskega vidika enako uničujoče. Kibernetski napadi lahko destabilizirajo gospodarstvo države in povzročijo dolgotrajne težave.

V tem prispevku je cilj razložiti, kaj je kibernetsko vojskovanje in kakšni doktrini kibernetskega vojskovanja imata državi. Hipoteza naloge je, da je ruska doktrina bolj osredotočena na ofenzivo, ukrajinska pa bolj na defenzivo. Za odgovor na hipotezo bodo analizirani trije kibernetski napadi, ki so se zgodili na začetku vojne.

Ta konflikt je jasen primer za mednarodno skupnost, v kateri je potreba po močni kibernetski obrambi in zavarovani infrastrukturi, saj se tako zmanjšujejo tveganja takih napadov. Posledice kibernetskih napadov niso omejene le na regijo, saj zahtevajo globalen odziv (Singer in Friedman, 2022; Rid, 2020).

1 OPREDELITEV KONCEPTOV KIBERNETSKEGA VOJSKOVANJA

Kibernetsko vojskovanje je opredeljeno kot kibernetski napad ali niz napadov na državo, ki povzročajo opustošenje infrastrukture in motijo delovanje kritičnih sistemov. Razprave med strokovnjaki o tem, kaj pomeni kibernetska vojna, še vedno potekajo.

Ameriško obrambno ministrstvo priznava, da internet predstavlja tveganje za nacionalno varnost, vendar ni natančne opredelitve kibernetske vojne. Leta 2010 je nekdanji ameriški nacionalni koordinator za varnost, zaščito infrastrukture in boj proti terorizmu Richard A. Clarke opredelil kibernetsko vojno kot: »dejanja države za vdor v računalnike ali omrežja druge države z namenom povzročitve škode ali motenj.« Običajno kibernetsko vojskovanje izvaja ena država proti drugi, včasih pa

tudi teroristične organizacije ali nedržavni akterji, ki želijo doseči cilje nasprotne države. Kljub temu do zdaj še ni univerzalne, formalne opredelitve, kako kibernetski napad pomeni vojaško dejanje (Clarke, 2010).

1.1 Najpogostejše vrste kibernetskih napadov

Za razumevanje kibernetskega vojskovanja je treba najprej razumeti vrste kibernetskih napadov. Najbolj pogoste vrste napadov v ukrajinski vojni so:

- zlonamerna programska oprema je virus, ki napada informacijske sisteme. Primeri zlonamerne programske opreme so izsiljevalni, vohunski in trojanski programi. Odvisno od vrste zlonamerne kode lahko hekerji zlonamerno programsko opremo uporabijo za krajo ali skrito kopiranje občutljivih podatkov, blokirajo dostop do datotek, povzročajo motnje delovanja sistema ali onemogočanje delovanja sistemov (Pratt, posodobljeno 2024);
- *phishing* je vrsta kibernetskega napada, pri katerem se napadalci predstavljajo kot legitimni subjekti, da bi posameznike prevarali in bi jim ti posredovali občutljive podatke, kot so uporabniška imena, gesla in številke kreditnih kartic. Ti podatki se nato uporabijo za zlonamerne namene, kot je kraja identitete ali finančna goljufija (CISA, posodobljeno 2024);
- *SMiShing,* imenovan tudi *SMS phishing* ali *smishing*, pomeni razvoj metodologije lažnega predstavljanja prek besedila, in sicer storitev kratkih sporočil ali SMS. Hekerji pošiljajo družbeno oblikovana besedila, ki prenašajo zlonamerno programsko opremo, ko prejemniki kliknejo nanje. Te vrste napadov so zelo pogoste v ukrajinski vojni, saj vojaki z obeh strani dobivajo propagandna sporočila na svoje mobilne telefone (Pratt, posodobljeno 2024);
- DDoS (ang. *distributed denial-of-service*) se zgodi, ko hekerji bombardirajo strežnike organizacije z velikim številom hkratnih podatkovnih zahtev, zaradi česar strežniki ne morejo obravnavati nobenih legitimnih zahtev. Ti napadi so prevladovali v začetnih dneh vojne v Ukrajini (Pratt, posodobljeno 2024);
- tuneliranje sistema domenskih imen (ang. *Domain name system* – DNS) je sofisticiran napad, pri katerem napadalci vzpostavijo in nato uporabljajo stalno razpoložljiv dostop ali tunel v sistemih svojih ciljev (Pratt, posodobljeno 2024).

1.2 Taktika kibernetskega vojskovanja

Najpogostejše taktike kibernetskega vojskovanja so:

- dezinformacije in propaganda: ruske dezinformacijske kampanje temeljijo na družbenih omrežjih. Glavni cilj je širiti nezaupanje v družbene in tradicionalne medije ter zaupanje v poštenost volitev prek sistemov botnet;
- kibernetsko vohunjenje: to ni vojskovanje kot tako, temveč stalna dejavnost držav, da ugotovijo prednosti in slabosti ne samo sovražnikov, temveč tudi drugih prijateljskih ali drugačnih držav. Obstaja veliko dokumentiranih primerov kibernetskega vohunjenja organizacij, ki jih je sponzorirala država, ki je lahko osumljena ali odkrita, da je nadzorovala druge države zaradi kibernetskega

vohunjenja. Ameriška agencija za nacionalno varnost je na primer posnela skoraj vsak pogovor z mobilnim telefonom na Bahamih brez dovoljenja bahamske vlade;
– kibernetski terorizem: kibernetski terorizem je uporaba nedržavnih akterjev, ki jih financira državni akter za izvajanje kibernetskih napadov. Cilji so povzročiti fizično, politično, psihično, ekonomsko ali drugo škodo, ustvariti strah in nezaupanje ter destabilizirati ali degradirati vlado oziroma politično pomembne dejavnosti in infrastrukturo;
– kibernetska sabotaža: gre za kibernetsko operacijo, v kateri nastane fizična škoda oziroma sabotaža. To pomeni namerno uničiti, poškodovati ali ovirati infrastrukturo v državi zlasti zaradi politične ali vojaške koristi. K sabotaži spada kibernetični napad na Viasat, v katerem je bila povzročena zelo velika škoda (A10, 2022).

1.3 Dopolnjevanje tradicionalnih metod vojskovanja s kibernetskimi

Za lažje razumevanje učinkovitosti kibernetskega vojskovanja v rusko-ukrajinski vojni je treba razumeti, kako kibernetske operacije pripomorejo k tradicionalnim metodam vojskovanja oziroma jih dopolnijo. V tabeli 1 je predstavljeno, kako kibernetske metode dopolnijo tradicionalne metode (Bateman, 2022, str. 31).

Tabela 1: Prikaz dopolnjevanja tradicionalnih metod vojskovanja s kibernetskimi (Vir: prirejeno po Bateman, 2022, str. 31)

Področje delovanja	Tradicionalne metode	Kibernetske metode
Predvojno načrtovanje	Več kot 800 domnevnih virov HUMINT, vključno z nekaterimi višjimi častniki in opozicijskimi politiki. Obsežne raziskave o scenarijih invazije. Prosto dostopne informacije o ukrajinski politični in vojaški pripravljenosti na invazijo.	Telefonski nadzor. Poskus kibernetskih vdorov v telefone ukrajinski vojski, diplomatom, industrijski bazi, upravnim enotam in humanitarnim organizacijam.
Strateško ciljanje	Satelitski posnetki in posnetki UAV, radar lahko prepoznajo številne strateške tarče. Rusija tudi uporablja vire HUMINT, ki včasih posredujejo zastarele informacije.	Vsaj dva primera kibernetskih vdorov, v katerih je Rusija pridobila pomembne informacije o šibkostih na frontah, kar je prispevalo k bolj učinkovitemu ciljanju topništva.
Okupacija	Odprti viri lahko prepoznajo pomembne osebnosti, sovražne do ruskih interesov. Rusija je plačala številne kolaborante in saboterje po vsej državi. V okupiranih ukrajinskih mestih so vzpostavili začasno vodenje, sestavljeno iz ukrajinskih kolaborantov.	Dostop v upravne baze podatkov in telekomunikacije. S temi podatki si lahko okupacijske enote pomagajo pri prepoznavanju, sledenju in aretaciji upornikov. Kibernetska zbirka podatkov lahko pomaga preveriti podatke iz človeških virov. Lahko tudi dostopajo do podatkov, ki so jih Ukrajinci izbrisali pred izgubo ozemlja.
Propaganda	Nadzor nad mediji, javnostjo, informacijami, šolami in včasih televizijo, radiem in internetom na zasedenih območjih.	Rusija uporablja sisteme botnet, s katerimi širijo rusko državno propagando po družabnih omrežjih. Rusija je s pomočjo sistemov botnet poslala približno 5000 propagandnih sporočil ukrajinskim četam in organom kazenskega pregona.

2 RUSKA DOKTRINA KIBERNETSKEGA VOJSKOVANJA

Rusija na kibernetiko oziroma kibernetsko vojskovanje gleda drugače kot zahodne države. Ruski teoretiki opredeljujejo kibernetsko vojskovanje glede na to, kako Kremelj uporablja svoje kibernetske zmogljivosti. Rusko vojaško poveljstvo je prepričano, da je država zaklenjena v nenehnem eksistencialnem boju z notranjimi in zunanjimi silami, ki želijo ogroziti varnost na informacijskem področju. Internet in prosti pretok informacij, ki jih ustvarja, se pri tem obravnavata kot grožnja in tudi priložnost (Connel in Volger, 2017, str. 1–2).

Ruska doktrina kibernetskega vojskovanja obsega strategije in taktike za doseganje ter uresničitev ciljev v vojni. Ta doktrina vključuje tako ofenzivne kot defenzivne kibernetske zmogljivosti, zanjo pa je pogosto značilna uporaba kibernetskih orodij za vohunjenje, sabotažo in informacijsko bojevanje (Bateman, 2022, str. 33; Willett, 2022, str. 22–23):

- informacijsko vojskovanje in psihološko delovanje: Rusija namenja velik poudarek uporabi kibernetskih orodij za informacijsko vojno, katere cilja sta oblikovati javno mnenje in vplivati na politične rezultate. To vključuje širjenje dezinformacij in propagande ter manipulacijo družbenih medijev za ustvarjanje razdora in nezaupanja v ciljnih družbah (Wilde, 2022; Bateman, 2022, str. 34–39);
- vohunjenje in zbiranje obveščevalnih podatkov: ruske kibernetske operacije se pogosto osredotočajo na zbiranje obveščevalnih podatkov z vladnih, vojaških in zasebnih omrežij. To dosegajo s prefinjenimi kibernetskimi vohunskimi kampanjami, ki izkoriščajo ranljivosti v ciljnih sistemih za iznos občutljivih podatkov (Wilde, 2022; Bateman, 2022, str. 34–39);
- napadi na ključno infrastrukturo: Rusija je dokazala, da je sposobna in namerava napadati ključno infrastrukturo, vključno z energetskimi omrežji, finančnimi sistemi in prometnimi omrežji. Primer tega je napad NotPetya. To je bil napad na ukrajinsko električno omrežje, ki je povzročil obsežne motnje in gospodarsko škodo. Ta napad je bil izveden z glavnim namenom, da bi povzročil motnje in škodo v električnem omrežju (Wilde, 2022; Bateman, 2022, str. 34–39);
- kibernetska sabotaža: cilj ruskih kibernetskih napadov je tudi uničiti ali blokirati dostop do storitev. Zlonamerna programska oprema se namerno uporablja za oviranje ali uničenje delovanja državnih institucij, vlade ali vojske. Najpogostejše metode so okužbe z zlonamerno programsko opremo, pogosto pa so to napadi DDoS. Cilj je ohromiti infrastrukturo, povzročiti finančno izgubo ali ukrasti občutljive informacije (Wilde, 2022; Bateman, 2022, str. 34–39);
- usklajevanje z vojaškimi operacijami: ruske kibernetske zmogljivosti so trenutno vključene v konvencionalne vojaške operacije. Tako se poveča splošna učinkovitost vojaških kampanj. Kibernetske operacije se lahko uporabljajo za zbiranje obveščevalnih podatkov, motenje sovražnikovih komunikacij in podporo tradicionalnih vojaških operacij na bojišču. Vojska si s kibernetskimi operacijami zagotovi boljše strateško ciljanje, obveščevalne podatke in lažjo okupacijo območja (Bartles, 2016, str. 30–37; Bateman, 2022, str. 34–39).

3 UKRAJINSKA KIBERNETSKA DOKTRINA

Ukrajinska kibernetska doktrina je usmerjena h krepitvi kibernetskih zmogljivosti za obrambo kibernetske varnosti kot odziv na vse večje kibernetske grožnje, zlasti državnih akterjev. Doktrina, ki temelji na načelih nacionalne varnosti, daje prednost zaščiti kritične infrastrukture, vladnih sistemov in omrežij zasebnega sektorja pred kibernetskimi napadi. Glede na geopolitične razmere v Ukrajini, ki se spoprijema s trajnim kibernetskim napadom, vključno z zloglasnim napadom NotPetya leta 2017, doktrina poudarja pomen proaktivnega in sodelovalnega pristopa h kibernetski varnosti.

Strategija kibernetske varnosti temelji na treh načelih državne politike na področju nacionalne varnosti:

– odvračanje: razvoj varnostnih in obrambnih zmogljivosti za odvračanje oboroženega napada na Ukrajino;
– odpornost: sposobnost družbe in države, da se hitro prilagodita spremembam v varnostnem okolju ter ohranita trajnostno delovanje, zlasti z zmanjševanjem zunanje in notranje ranljivosti;
– interakcija: razvoj strateških odnosov s pomembnimi tujimi partnerji, predvsem z Evropsko unijo, Natom, njunimi državami članicami in Združenimi državami Amerike, ter pragmatično sodelovanje z drugimi državami in mednarodnimi organizacijami, ki temelji na nacionalnih interesih Ukrajine.

Strategija kibernetske varnosti si bo prizadevala zlasti za izboljšanje varnosti omrežnih in informacijskih sistemov ter uvedbo sistema upravljanja tveganj. Ureja tudi ustvarjanje pogojev za zagotavljanje virov, vključno s človeškimi viri za kibernetsko varnost, splošno pa izboljšuje operativno in kibernetsko varnost bistvene infrastrukture ter boj proti kibernetskemu kriminalu. Za to bo Ukrajina uporabila ne samo državne zmogljivosti, temveč tudi zmogljivosti zasebnega sektorja in zainteresiranih strani za reševanje vprašanj kibernetske varnosti in obrambe (Atkins, 2022; Spînu, 2020, str. 6–10).

Osrednje načelo doktrine je spodbujanje sodelovanja med vladnimi organi, zasebnimi podjetji in mednarodnimi zavezniki, da bi ustvarili skladen sistem kibernetske obrambe. Poudarja krepitev zmogljivosti z usposabljanjem, raziskavami in razvojem domačih rešitev na področju kibernetske varnosti. Doktrina spodbuja tudi ozaveščanje javnosti o tveganjih za kibernetsko varnost in odgovornost posameznikov pri vzdrževanju primernih digitalnih sledi. Cilj tega strateškega pristopa ni le zaščita ukrajinske digitalne suverenosti, temveč tudi prispevek h kolektivni varnosti svetovnega digitalnega ekosistema (Atkins, 2022; Spînu, 2020, str. 6–10).

4 UPORABA KIBERNETSKIH ZMOGLJIVOSTI MED VOJNO

Ruski kibernetski napadi na Ukrajino so dosegli vrhunec po kakovosti in številu v dnevih tik pred začetkom invazij in po njem. Rusija je na dan invazije izvedla znani kibernetski napad v Viasat. Glavna tarča napada naj bi bila ukrajinska vojska, ki se zelo zanaša na satelitske komunikacije, vendar je napad vplival tudi na internetne storitve za tisoče uporabnikov Viasata v Ukrajini in za več deset tisoč uporabnikov po vsej Evropi. Napad je prekinil tudi oddaljeni dostop do približno 5800 vetrnih turbin po vsej Nemčiji, saj so se za daljinsko spremljanje in nadzor vetrnic zanašali na usmerjevalnike Viasat. Po začetnih dnevih so se število, novosti in učinek ruskih kibernetskih napadov zmanjšali. Če bi bilo začetno načrtovanje boljše, bi bili mogoče zgodnji ruski kibernetski napadi le začetek, saj bi imela država med vojno manj zadržkov pri izvajanju kibernetskih napadov. Višji ukrajinski kibernetski uradnik Victor Zhora je aprila 2022 povedal, da so ruske ofenzivne kibernetske operacije verjetno že dosegle svoj polni potencial in se ne bodo razširile (Page, 2022; Bateman, 2022, str. 40–46).

Ruske sile so se trudile usklajevati delovanje na različnih področjih, kot so vojaška strategija, disciplina in operativni sektorji, ampak so ti primanjkljaji zelo ovirali vojno v Ukrajini. Ko ima vojska toliko resnih težav z usklajevanjem, tudi med osnovnimi tradicionalnimi vojaškimi vlogami, kot je na primer logistika, je uvajanje novejših vlog skoraj nemogoče. Kibernetsko vojskovanje je posledično predstavljalo velike izzive pri usklajevanju akcij s kinetičnimi silami. Boljše usklajevanje s kinetičnimi silami bi povečalo vojaško uporabnost kibernetskih operacij Rusije v vojni. Kibernetske operacije Rusije imajo največji strateški učinek, ko so najbolj povezane s kinetičnimi operacijami. Zgodnji ruski kibernetski uspeh ni bil odvisen le od kibernetičnega usklajevanja, temveč tudi od njegovega načrtovanja. V nekaj tednih po začetku vojne se je število ruskih kibernetskih napadov zelo zmanjšalo, ker se je izkazalo, da ruski hekerji ne morejo vzdrževati tako visokega tempa delovanja. Ko se je število ruskih kibernetskih napadov zmanjšalo, če jih primerjamo z obsegom vojne, se je usklajevanje s kinetičnimi operacijami prav tako poslabšalo. Če bi ruskim kibernetskim silam nekako uspelo ohraniti zgodovinski tempo pomembnih operacij, ki so bile vidne na začetku vojne, bi lahko sčasoma imele velik strateški vpliv, toda Rusija je po prvih nekaj tednih vojne doživela veliko zmanjšanje števila in kakovosti kibernetskih napadov. Ta neuspeh kaže tudi na omejene tehnične vire Ruske federacije (Bateman, 2022, str. 44–48).

Zaradi obsega ruskih kibernetskih napadov na Ukrajino je bolje analizirati tri najbolj kritične, ki so se zgodili tik pred invazijo in po njej:

– napad WhisperGate 14. januarja 2022 je bil uničujoč napad zlonamerne programske opreme, ki je ciljal na ukrajinska vladna spletna mesta in bistveno infrastrukturo. Napad je začasno onesposobil več vladnih spletnih strani in povzročil motnje v delovanju;

– satelitski napad na omrežja Viasat na dan invazije 24. februarja 2022 je bil usmerjen na satelitsko omrežje Viasat KA-SAT, ki ga je ukrajinska vojska uporabljala za komunikacijo. Ta napad je oviral komunikacijo v Ukrajini v kritičnih zgodnjih urah invazije;
– napad Industroyer2 na ukrajinsko električno omrežje aprila 2022 je bil namenjen motenju oskrbe z električno energijo v državi. Napad je ciljal na električne transformatorske postaje in bi lahko povzročil obsežne izpade električne energije. Čeprav je ukrajinskim ekipam za kibernetsko varnost uspelo preprečiti ta napad, je povzročil veliko škode.

4.1 Napad WhisperGate

Napad se je začel 14. januarja 2022, v ukrajinskih medijih pa so o njem prvič poročali komaj dan za tem. Ta napad je bil imenovan WhisperGate. Po podatkih naj bi kibernetski napad obsegal zlonamerni nalagalnik, ki poškoduje lokalne diske, program za prenos datotek in brisalec datotek.

Napad se je zgodil približno v istem času, ko je bilo napadenih več spletnih mest ukrajinske vlade. Zlonamerna programska oprema WhisperGate bootloader je na prvi pogled videti kot izsiljevalska programska oprema, vendar je v resnici program za brisanje datotek. Namenjena je nepovratnemu poškodovanju podatkov okuženih gostiteljev, vendar se z odkupnino 10.000 dolarjev prekrije kot izsiljevalska programska oprema. Program ni imel mehanizma za dešifriranje ali obnovitev podatkov in ni skladen z zlonamerno programsko opremo, ki se običajno uporablja v operacijah izsiljevalske programske opreme. To pomeni, da so se podatki izbrisali, čeprav je žrtev plačala odkupnino. Napad je bil prefinjen, saj je za povzročitev škode uporabil dve stopnji. Prva stopnja je poškodovala glavni zagonski zapis (MBR), zaradi česar sistemi niso mogli delovati, druga stopnja pa je bila usmerjena na datoteke z različnimi končnicami in jih je prepisala z odkupnino, čeprav obnovitev podatkov ni bila mogoča (Microsoft, 2022; Crowdstrike, 2022).

Napad je povzročil nepopravljivo škodo in izgubo datotek, kar je pomenilo večje motnje v delovanju pomembne infrastrukture. Napad je bil izveden sinhronizirano z drugimi napadi DDoS na spletne strani v Ukrajini. Po vsej verjetnosti so bili cilji napada ustvarjanje kaosa, uničenje zaupanja v vlado in splošna demoralizacija prebivalstva ter vojske, izveden pa je bil pred invazijo na Ukrajino. Glede na čas je mogoče predvidevati, da je bil glavni namen pripraviti podlago za invazijo države s strani Rusije. Napad je zaradi svoje usklajenosti z invazijo pomemben korak v taktiki kibernetskega vojskovanja, katerega cilj ni le povzročiti takojšnje škode, temveč tudi zasejati dolgoročno nestabilnost, ki bo pripomogla k tradicionalnemu vojskovanju (Crowdstrike, 2022; Lyons 2022).

Ukrajina je pokazala razmeroma visoko pripravljenost na napad in se je tudi učinkovito odzvala nanj. Ukrajinska kibernetska policija je sodelovala z drugimi agencijami za kibernetsko varnost in mednarodnimi podjetji, kot sta CISA ter Microsoft. Kibernetski napad so hitro prepoznali in posledično se je poskušal omejiti

mogoč doseg virusa. Zlonamerno programsko opremo so analizirali in preučili strokovnjaki na tem področju. CERT-UA (ang. Computer Emergency Response Team of Ukraine) je izdal navodila za zmanjšanje širjenja zlonamerne programske opreme in zaščito morebitnih drugih ciljev. Kljub začetnim uspehom je ukrajinskim kibernetskim silam uspelo obnoviti prizadete sisteme, s čimer so ohranile operativno celovitost pomembne državne infrastrukture. Hiter in učinkovit odziv je zelo omejil učinkovitost kibernetskega napada ter zagotovil hitro popravilo prizadetih strani. Ta kibernetski napad je tudi poudaril pomembnost sodelovanja državnih in nedržavnih akterjev, predvsem med CERT-UA ter podjetjem Microsoft (Microsoft, 2022; Lyons 2022).

4.2 Satelitski napad na omrežje Viasat

Na dan ruske invazije v Ukrajini 24. februarja 2022 je kibernetski napad prekinil širokopasovni satelitski dostop do interneta. Ta napad je onesposobil modeme, ki komunicirajo s satelitskim omrežjem KA-SAT družbe Viasat. Satelitsko omrežje je zagotavljalo dostop do interneta več deset tisoč ljudem v Ukrajini in Evropi. Napad je bil izveden z novo zlonamerno programsko opremo za brisanje podatkov AcidRain. Zasnovan je bil za daljinsko brisanje ranljivih modemov in usmerjevalnikov. Podjetje Viasat trdi, da je bil glavni namen napada prekinitev storitev uporabnikom in ne pridobiti dostop do podatkov ali sistemov.

Po vsej verjetnosti je bil cilj kibernetskih napadov na komercialna satelitska komunikacijska omrežja, da bi med invazijo ovirali ukrajinsko poveljevanje in nadzor enot. Tako so povzročili kaos med invazijo in ovirali širjenje informacij. Ta kibernetski napad je imel posledice tudi v drugih evropskih državah (Cyber Peace Institute, 2022).

Satelit KA-SAT zagotavlja širokopasovni internet in satelitsko televizijo v Evropi ter delih Bližnjega vzhoda, izstreljen pa je bil leta 2010. V času napadov je satelitsko komunikacijsko omrežje uporabljalo od 110.000 do 120.000 modemov z mešanico komercialnih in vladnih strank ter tudi letalskih strank. Približno ob 18. uri 23. februarja 2022, torej dan pred invazijo, se je napadalec večkrat poskušal prijaviti v omrežje VPN, ki so ga administratorji podjetja Viasat uporabljali za dostop do strežnikov v severni Italiji. Ti strežniki so nadzorovali satelitsko internetno omrežje. Napadalcu najprej ni uspelo vdreti v omrežje, vendar je nekaj ur pozneje našel zadnja vrata (ang. backdoor), ki so delovala. Z dostopom do računalniškega sistema, ki se uporablja za komunikacijo z modemi, razpršenimi po Evropi in na Bližnjem vzhodu, je napadalec okužil modeme z zlonamerno programsko opremo Acid Rain, ki je onemogočila delovanje od 40.000 do 45.000 modemov. Ruski hekerji niso samo namestili zlonamerne programske opreme wiper, temveč so strežnike zasuli z zahtevami, ki so hitro preobremenile njihova omrežja. *S*trežniki so v petih minutah prejeli več kot 100.000 zahtev. To je pomenilo, da kadar koli je bil modem izključen iz omrežja, se ni mogel ponovno povezati, ker se strežnik ni mogel odzvati (Vasquez in Groll, 2023).

Cilj hekerjev so bili določeni terminali, vendar podjetje ni moglo natančno ugotoviti, kateri modemi so bili tarča napadov. Ta kibernetski napad je povzročil izgubo komunikacij. To je bil tudi namen, saj je bil usklajen z invazijo. Ruska taktika je bila narediti zmedo in to izkoristiti pri invaziji (Vasquez in Groll, 2023).

Napad je vplival na telekomunikacijske sisteme, zato ni ogrozil le vladnih ali vojaških objektov, temveč je vplival tudi na civilno prebivalstvo in civilne objekte v Ukrajini ter zunaj nje, ko so izgubili dostop do interneta in so bile mogoče motnje v sistemih v energetskem sektorju. Nekateri so poročali, da so bili brez dostopa do interneta več kot dva tedna. Napad na podjetje Viasat je vplival tudi na večje nemško energetsko podjetje, ki je izgubilo dostop do daljinskega nadzora več kot 5800 vetrnih turbin, v Franciji pa je skoraj 9000 naročnikov ponudnika satelitskih internetnih storitev doživelo izpad interneta. Poleg tega je bila prizadeta približno tretjina od 40.000 naročnikov drugega ponudnika satelitskih internetnih storitev v Evropi. Na splošno je ta napad vplival na več tisoč uporabnikov v Ukrajini in na več deset tisoč drugih fiksnih širokopasovnih uporabnikov po Evropi (Cyber Peace Institute, 2022).

V podjetju Viasat so takoj začeli izvajati ukrepe za stabilizacijo omrežja in ublažitev posledic virusa. Ukrajina se je lahko na napad odzvala le v omejenem obsegu, saj je bil satelit zunaj neposrednega nadzora ukrajinske infrastrukture za kibernetsko varnost. Napad je bil v bistvu napad na zunanjega ponudnika storitev. Ukrajini je to otežilo možnost neposredne obrambe ali ublažitve škode, vendar je ukrajinska vlada skupaj z mednarodnimi zavezniki tesno sodelovala s podjetjem Viasat in drugimi mednarodnimi partnerji, da bi hitro razumela obseg napada ter začela postopek ponovne vzpostavitve storitev. Podjetje je s pomočjo evropskih kibernetskih agencij zamenjalo napadene modeme, čeprav je ta postopek trajal dlje in je v kritičnem obdobju veliko uporabnikov ostalo brez povezave (Viasat, 2022).

Ukrajinska vojska in vlada sta se morali prilagodili tako, da sta prešli na alternativne načine komunikacije, s čimer sta pokazali odpornost ter prilagodljivost ob nepričakovani izgubi glavnega vira. Napad je tudi poudaril pomen načrtovanja kibernetske odpornosti. Kljub začetnemu šoku je Ukrajini in njenim partnerjem uspelo ohraniti določeno raven operativne komunikacije, čeprav po manj optimalnih kanalih (Sanger in Barnes, 2022).

4.3 Napad Industroyer2 na ukrajinsko električno omrežje

Izbruh konflikta v vzhodni Ukrajini leta 2014 je bil začetnik številnih kibernetskih napadov. Začeli so se takoj po tem, ko si je Rusija priključila Krim. Večina kibernetskih napadov je bila usmerjena na električno infrastrukturo Ukrajine.

Industroyer2 je naslednik zlonamerne programske opreme Industoyer, namenjene poseganju v procese industrijskih nadzornih sistemov, zlasti tistih, ki se uporabljajo na električnih postajah. Ta zlonamerna programska oprema je bila uporabljena v kibernetskem napadu na ukrajinsko električno omrežje leta 2016, ko je prekinil oskrbo z električno energijo v glavnem mestu. Pomembno je omeniti, da je to prva

znana zlonamerna programska oprema, zasnovana za napade na električna omrežja (HeadMind Partners, 2022).

Odziv Ukrajine na napad Industroyer2 je bil uspešen in je pokazal, da je Ukrajina od prvotnega napada Industroyer leta 2016 bistveno izboljšala svoje zmogljivosti na področju kibernetske varnosti. Ukrajinski strokovnjaki za kibernetsko varnost, ki so sodelovali z mednarodnimi partnerji, kot sta ESET in CERT-UA, so zgodaj odkrili vdor ter hitro ukrepali, da bi omejili grožnjo. Hitra identifikacija in izolacija okuženih sistemov sta bili bistvenega pomena pri preprečevanju, da bi zlonamerna programska oprema v celoti izvedla svoje uničevalne cilje. (ESET, 2022).

Dva izmed bistvenih dejavnikov uspešne obrambe pred Industroyer2 sta bila boljše ozaveščanje in pripravljenost Ukrajine na kibernetske grožnje glede njene pomembne infrastrukture. Od leta 2016 je Ukrajina veliko vlagala v krepitev svoje kibernetske obrambe, predvsem z okrepljenim spremljanjem industrijskih nadzornih sistemov. Napadi na električno omrežje so lahko najbolj uničujoči, saj civilisti in prav tako vojska potrebujejo dostop do elektrike. Ukrajina je poskušala tudi izboljšati sodelovanje z mednarodnimi agencijami za kibernetsko varnost, ta prizadevanja pa so se obrestovala v tem kibernetskem napadu. Z novo vzpostavljenimi obrambnimi ukrepi jim je uspelo omejiti škodo in preprečiti ponovitev večjih izpadov elektrike, kot se je zgodilo v kibernetskem napadu leta 2016. Zaradi izkušenj je Ukrajina pridobila sposobnost, da hitro uporabi zunanje strokovno znanje in vire, kar je bilo zelo pomembno za ublažitev učinka tega napada. Incident je poudaril vrednost vzpostavljenih protokolov in partnerstev pred krizo, kar omogoča usklajen ter učinkovit odziv ob kibernetskem napadu (ESET, 2022; HeadMind Partners, 2022).

Na splošno je napad na Ukrajino z zlonamerno programsko opremo Industroyer2 dobra študija primera uspešne obrambe pred kibernetskimi napadi. Ponazarja tudi pomen integracije kibernetskih operacij s tradicionalnimi vojaškimi cilji.

Sklep

Doktrini kibernetskega vojskovanja Rusije in Ukrajine sta različni. Ruska doktrina je osredotočena na ofenzivo, ukrajinska pa na defenzivo. Rusija ima na voljo več zmogljivosti in strategij za ofenzivno bojevanje, poleg doktrine tudi več orodij ter dobro vzpostavljeno infrastrukturo v svojih vojaških in obveščevalnih agencijah. Od priključitve Krima leta 2014 je Rusija izvedla izbrane kibernetske napade na Ukrajino, s čimer je dokazala svojo ofenzivno kibernetsko moč. Del kibernetskih operacij je hibridno vojskovanje, v katerem združujejo kibernetske napade s tradicionalnimi vojaškimi taktikami, tako pa destabilizirajo nasprotnike in vplivajo na svetovne dogodke.

Ukrajinska kibernetska strategija je v nasprotju osredotočena na defenzivo, predvsem na zaščito svoje bistvene infrastrukture. Njena doktrina je oblikovana za odziv na ruski napad. Od ruske aneksije Krima leta 2014 je Ukrajina zelo izboljšala svojo kibernetsko obrambo s pomočjo zahodnih zaveznikov in zasebnih podjetij ter vzpostavila učinkovite ekipe (CERT-UA) za hiter odziv na kibernetske napade.

Tesno sodelovanje z zasebnimi podjetji, kot so Microsoft, Viasat in ESET, je zelo prispevalo h kibernetski obrambi države. Glavni cilj Ukrajine je bil zaščititi svojo glavno infrastrukturo, kar ji je uspelo. Posledično je hipoteza, da je ruska doktrina bolj osredotočena na ofenzivo, ukrajinska pa bolj na defenzivo, potrjena.

Rusija ima veliko več kibernetskih zmogljivosti kot Ukrajina, zato si lahko posledično privošči ofenzivno doktrino. Ukrajini primanjkuje strokovnega kadra, osebja, financiranja in drugega, lahko pa se osredotoča na obrambo, kar se kaže v njeni doktrini, zato tudi sodeluje z zasebnimi ter tujimi podjetji. Ukrajinska obrambna kibernetska doktrina izhaja iz potrebe po zaščiti kritične infrastrukture in nacionalne varnosti v času nenehnih kibernetskih napadov. Ta država je pogosta tarča kibernetskih operacij, ki jih sponzorira Rusija, zato daje prednost odpornosti in obrambi, da bi zaščitila svojo suverenost ter ublažila posledice teh napadov. Nasprotno je ruska ofenzivna kibernetska doktrina usklajena z njeno širšo geopolitično strategijo, saj kibernetske napade uporablja kot orodje za vpliv, motnje in asimetrično vojskovanje. Rusija uporablja kibernetske zmogljivosti za projekcijo moči, destabilizacijo nasprotnikov in doseganje strateških ciljev. Ta razlika kaže potrebo Ukrajine, da se zaščiti kot žrtev napada, Rusija pa uporablja kibernetske zmogljivosti kot orožje za vpliv.

Kibernetsko vojskovanje v rusko-ukrajinski vojni je poslabšalo humanitarne krize, saj je bilo usmerjeno na civilno infrastrukturo, kar je povzročilo motnje v osnovnih storitvah, kot so oskrba z elektriko, zdravstveno varstvo in voda. Zaradi kibernetskih napadov na ukrajinsko električno omrežje, kot so bili napadi WhisperGate in Industroyer, je pozimi leta 2022 na tisoče ljudi ostalo brez ogrevanja, kar je ogrozilo življenja. Dezinformacijske kampanje tudi krepijo paniko, zmanjšujejo zaupanje in otežujejo humanitarno odzivanje. Napadi, kot je bil WhisperGate, lahko vplivajo na zdravstvene sisteme, ogrožajo podatke o pacientih in zavlačujejo kritično oskrbo. Poleg tega se zaradi uporabe digitalnih platform širi propaganda, kar lahko zmanjšuje prizadevanja za mednarodno pomoč. Ta oblika vojskovanja nesorazmerno vpliva na ranljive skupine prebivalstva, kar povečuje njihovo trpljenje in poglablja humanitarne izzive v že tako nestabilnem konfliktu.

Tako asimetrično bojevanje je v nasprotju z mednarodnim humanitarnim pravom, saj je usmerjeno v civilno infrastrukturo, ki je bistvena za preživetje, kot so električna omrežja in zdravstveni sistemi. Humanitarno pravo zahteva ločevanje med civilnimi in vojaškimi cilji ter prepoveduje napade, ki povzročajo nesorazmerno škodo civilistom. Kibernetski napadi, ki motijo oskrbo z električno energijo ali vodo, kršijo ta načela, ogrožajo življenja in poslabšujejo humanitarne krize. Težave pri pripisovanju kibernetskih napadov otežujejo odgovornost in opozarjajo na pomanjkljivosti pri uporabi mednarodnega humanitarnega prava v digitalni vojni. Te kršitve poudarjajo, da je treba humanitarno pravo nujno prilagoditi za učinkovito obravnavo kibernetskih vplivov na civiliste.

S stopnjevanjem kibernetskih konfliktov se bo globalno varnostno okolje zelo spremenilo. Konflikti se bodo v prihodnosti stopnjevali, vedno bolj na tej novi fronti vojskovanja, ki bo postala čedalje bolj uničujoča. Glavna težava, ki se pojavlja, je pripisovanje krivde kibernetskim napadom. Država bo lahko »napadla« drugo državo, ne da se bo vedelo o krivdi in vpletenosti te države. Meje med akterji, ki jih podpira država, in neodvisnimi akterji bodo vedno bolj zabrisane. Pojavili se bodo tudi organizacije in zasebna podjetja, ki se bodo ukvarjali izključno s kibernetskim vojskovanjem, vključno s podjetji za kibernetsko varnost ter z najemniškimi hekerji oziroma hekerskimi plačanci. Tako bo postal mednarodni ekosistem še bolj zapleten.

Prihodnost kibernetskega vojskovanja bo zaznamovala večja integracija kibernetskih napadov s konvencionalnimi oziroma tradicionalnimi načini vojskovanja. Z napredovanjem tehnologije bodo države in tudi nedržavni akterji razvili še bolj zapletene vrste napadov, ki bodo lahko povzročili veliko škode. Meje med kibernetskim in kinetičnim bojevanjem se bodo izbrisale. Kibernetska orodja se v vojni uporabljajo kot topništvo, omehča se teren in pripravi okolje za tradicionalen kinetični napad. Kibernetsko vojskovanje je predvsem pomembno za predvojno načrtovanje, propagando in demoralizacijo, strateško ciljanje bistvene infrastrukture in drugih tarč ter nadziranje okupiranega območja. V kibernetskem vojskovanju je treba izpostaviti, da spada pod hibridno vojskovanje, saj poleg vojaških tarč cilja predvsem civiliste. Vojne bodo v prihodnosti še vedno potekale po istem načinu hibridnega vojskovanja (Duguin in Pavlova, 2023, str. 14–15).

Kibernetsko vojskovanje bo v prihodnosti sestavljeno iz novih tehnologij, kot je umetna inteligenca. Do zdaj so napade izvedli posamezniki, ki so morali dopolnjevati svoja orodja za napade. V prihodnosti bodo napadalci za izvajanje kibernetskih napadov uporabljali umetno inteligenco, s katero bi lahko avtonomna kibernetska orodja samodejno izvajala operacije in sproti dopolnjevala svojo programsko opremo, da bi se izognili varnostnim ukrepom. To prilagajanje obrambi bo potekalo brez neposrednega človeškega nadzora, kar bo povečalo hitrost in nevarnost kibernetskih konfliktov. Mogoče je tudi, da bo umetna inteligenca podivjala (ang. Rogue AI) in ušla izpod nadzora. Izraz Rogue AI se nanaša na sisteme umetne inteligence, ki delujejo v nasprotju z interesi svojih ustvarjalcev, uporabnikov ali človeštva na splošno. Čeprav so sedanji napadi, kot so goljufije in napadi na infrastrukturo, skrb vzbujajoči, niso edina vrsta grožnje umetne inteligence, na katero se moramo pripraviti. Napadalec bo namestil umetno inteligenco v drugi sistem, da bi ta dosegala njegove cilje, vendar bo ušla izpod nadzora. Ta vrsta umetne inteligence lahko nastane zaradi človeške napake ali tehnoloških omejitev. Zaradi napačne konfiguracije, nepravilnega testiranja modelov in slabega nadzora lahko napačno ravna z občutljivimi podatki ter povzroči veliko škode (AI Team, 2024).

Literatura

1. *A10, 2022. Cyber Warfare: Nation State Sponsored Cyber Attacks. https://www.a10networks.com/blog/cyber-warfare-nation-state-sponsored-cyber-attacks/, 10. december 2024.*
2. *AI Team, 2024. Rogue AI is the Future of Cyber Threats. TrendMicro. https://www.trendmicro.com/en_fi/research/24/h/rogue-ai-part-1.html, 10. december 2024.*
3. *Bartles, C. K., 2016. The Gerasimov Doctrine and Russian Non-Linear War. Military Review, 96(1), str. 30–37.*
4. *Bateman, J., 2022. Russia's Wartime Cyber Operations in Ukraine: Military Impacts, Influences, and Implications. Carnegie Endowment for International Peace, str. 31–49.* https://carnegieendowment.org/2022/12/16/russia-s-wartime-cyber-operations-in-ukraine--military-impacts-influences-and-implications-pub-88657*, 13. december 2024.*
5. *Clarke, R. A., 2010. Cyber War, HarperCollins.*
6. *Connel, M., in Vogler, S., 2017. Russia's Approach to Cyber Warfare. CNA Analysis and Solutions. https://www.cna.org/archive/CNA_Files/pdf/dop-2016-u-014231-1rev.pdf, 12. december 2024.*
7. *Corera, G., 2023. Ukraine war: Cyber-teams fight a high-tech war on front lines. BBC. https://www.bbc.com/news/world-europe-66686584, 17. december 2024.*
8. *CrowdStrike, 2022. Technical Analysis of the WhisperGate Malicious Bootloader. https://www.crowdstrike.com/blog/technical-analysis-of-whispergate-malware/, 22. november 2024.*
9. *Cyber Peace Institute, 2022. Case Study: Viasat. https://cyberconflicts.cyberpeaceinstitute.org/law-and-policy/cases/viasat, 17. december 2024.*
10. *Duguin, S., Pavlova, P., 2023. The role of cyber in the Russian war against Ukraine: Its impact and the consequences for the future of armed conflict. European Parliment.* https://www.europarl.europa.eu/RegData/etudes/BRIE/2023/702594/EXPO_BRI(2023)702594_EN.pdf*, 10. december 2024.*
11. *ESET, 2022. Industroyer2: Industroyer reloaded. https://www.welivesecurity.com/2022/04/12/industroyer2-industroyer-reloaded/, 1. december 2024.*
12. *HeadMind Partners, 2022. Industroyer 2 : the Russian Cyberattack on Ukraine Infrastructure. https://www.headmind.com/industroyer-2/, 3. november 2024.*
13. *Lyons, J., 2022. Data-wiper malware strains surge as Ukraine battles ongoing invasion. The Register. https://www.theregister.com/2022/04/29/wiper_attacks_jump_500_percent/, 22. november 2024.*
14. *Microsoft, 2022. Destructive malware targeting Ukrainian organizations. https://www.microsoft.com/en-us/security/blog/2022/01/15/destructive-malware-targeting-ukrainian--organizations/, 10. december 2024.*
15. *NATO 2030, 2020. United for the new Era. Analysis and Recommendations of the Reflection Group Appointed by the NATO Secretary General.* https://www.nato.int/nato_static_fl2014/assets/pdf/2020/12/pdf/201201-Reflection-Group-Final-Report-Uni.pdf*, 24. november 2024.*
16. *Page, C., 2022. US, UK and EU blame Russia for »unacceptable« Viasat cyberattack. Techcrunch. https://techcrunch.com/2022/05/10/russia=-viasat-cyberattack/?guccounter-1&guce_referrer=aHR0cHM6Ly93d3cucXdhbnQuY29tLw&guce_referrer_sig=AQAAAA5wODCUfzch8gg0n1XY6wQXOUYLUpxz8TEv1nO6nDGv_Je-w-NN-TGwxP3zqrN9JlT-FNDzMPit2knLXpwyIqzPyJuZ1a7jw75_hTnoW8wSJaJ4mSb5ieFGI-ZEyMkppcX37D5jOCcWoLuJnf80VSdOc-W1nj21wW8LOChfkQ1UFQ, 10. november 2024.*
17. *Pratt, M. K., posodobljeno 2022. Cyber attack. TechTarget. https://www.techtarget.com/searchsecurity/definition/cyber-attack, 10. december 2024.*
18. *Rid, T., 2020. Active Measures: The Secret History of Disinformation and Political Warfare. Farrar, Straus and Giroux.*

19. *Sanger, D. E., in Barnes, J. E., 2022. The Russian cyberwar campaign in Ukraine is unfolding slowly, cautiously. The New York Times. https://www.nytimes.com/2022/02/27/us/politics/russia-cyberattacks-ukraine.html, 10. december 2024.*
20. *Singer, P. W., in Friedman, A., 2014. Cybersecurity and cyberwar : what everyone needs to know. Oxford University Press. https://www.worldcat.org/title/802324804, 15. december 2024.*
21. *Spînu, N., 2020. Ukraine Cybersecurity Governance Assessment. Geneva Centre for Securtiy Sector Governance. https://www.dcaf.ch/sites/default/files/publications/documents/UkraineCybersecurityGovernanceAssessment.pdf, 10. december 2024.*
22. *The BlackBerry Research and Intelligence Team, 2022. Threat Thursday: Malware Rebooted - How Industroyer2 Takes Aim at Ukraine Infrastructure. BlackBerry. https://blogs.blackberry.com/en/2022/05/threat-thursday-malware-rebooted-how-industroyer2-takes-aim-at-ukraine-infrastructure, 4. december 2024.*
23. *Vasquez, C., in Groll, E., 2023. Satellite hack on eve of Ukraine war was a coordinated, multi-pronged assault. Cyberscoop. https://cyberscoop.com/viasat-ka-sat-hack-black-hat/, 5. december 2024.*
24. *Viasat, 2022. KA-SAT Network cyber attack overview. https://news.viasat.com/blog/corporate/ka-sat-network-cyber-attack-overview, 7. november 2024.*
25. *Wilde, G., 2022. Cyber Operations in Ukraine: Russia's Unmet Expectations. Carnegie Endowment for International Peace https://carnegieendowment.org/files/202212-Wilde_RussiaHypotheses-v2.pdf, 10. december 2024.*
26. *Willett, M., 2022. The Cyber Dimension of the Russia–Ukraine War. Survival. https://www.researchgate.net/publication/364176417_The_Cyber_Dimension_of_the_Russia-Ukraine_War, 8. december 2024.*

e-mail: vladimir.prebilic@fdv.uni-lj.si
ORCID: 0000-0002-0576-4259

e-mail: patrik.rebrica@gmail.com

Dr. Vladimir Prebilič je izredni profesor na Katedri za obramboslovje Fakultete za družbene vede Univerze v Ljubljani. Na dodiplomskem študiju predava predmete Vojaška zgodovina, Obramboslovna geografija in Temelji EU ter na podiplomski stopnji Geopolitiko. Vodil je raziskovalne projekte za slovensko šolsko ministrstvo, obrambno ministrstvo, notranje ministrstvo in ministrstvo za javno upravo. Njegove raziskovalne teme so sodobno državljanstvo, patriotizem, vojaška zgodovina in lokalna samouprava. Njegova osebna bibliografija obsega 545 bibliografskih enot; med njimi je avtor več kot 70 člankov in sedmih knjig.

Vladimir Prebilič, PhD, is an Associate Professor at the Department of Defence Studies in the Faculty of Social Sciences of the University of Ljubljana. He lectures in Military History, Defence Geography and the Basics of the EU at the undergraduate level, and in Geopolitics at the postgraduate level. He has conducted research projects for the Slovenian Ministry of Education, the Ministry of Defence, the Ministry of the Interior and the Ministry of Public Administration. His research topics include contemporary citizenship, patriotism, military history and local self-government. His body of work comprises 545 items; among them he is the author of more than 70 articles and 7 books.

e-mail: vladimir.prebilic@fdv.uni-lj.si

ORCID: 0000-0002-0576-4259

Patrik Rebrica. je magistriral iz obramboslovje in varnostnih ved leta 2024. V svojem magistrskem delu se je poglobil v tehnično znanje in strateški vpogled v področje kibernetske varnosti ter obrambnih mehanizmov držav. Skozi študij in praktične izkušnje je pridobil znanja na področju analize groženj, digitalne forenzike in strategij kibernetske odpornosti. Njegov cilj je sodelovati z ekipami, usmerjenimi v inovacije na področju kibernetske varnosti in zaščite ključne informacijske infrastrukture.

Patrik Rebrica, MSc, . completed his master's degree in Defense and Security Studies in 2024. In his thesis, he delved into technical knowledge and strategic insights in the field of cybersecurity and state defense mechanisms. Through his studies and practical experience, he gained expertise in threat analysis, digital forensics, and cyber resilience strategies. His goal is to collaborate with teams focused on innovation in cybersecurity and the protection of critical information infrastructure.

e-mail: mark90.kogoj@gmail.com