Patrik REBRICA, Vladimir PREBILIČ*

DOKTRINI KIBERNETSKEGA VOJSKOVANJA RUSIJE IN UKRAJINE**

Povzetek. *Kibernetsko vojskovanje je v sodobne konflikte uvedlo novo dimenzijo, pri čemer so nevarnosti večje kot kdaj prej, saj postajajo cilji kritična infrastruktura, finančni sistemi in osebni podatki. Meje med digitalnim in fizičnim svetom se brišejo, kar povečuje potrebo po učinkoviti kibernetski obrambi. Namen tega članka je preučiti vpliv kibernetskega vojskovanja v rusko-ukrajinski vojni. Razumevanje doktrin in taktik pripomore k boljši nacionalni varnosti, zaščiti civilistov in stabilnosti globalne digitalne infrastrukture, kar omogoča razvoj strategij za zmanjšanje tveganj v prihodnjih konfliktih.*
Ključni pojmi: *kibernetika, vojskovanje, vojna, doktrina, obramba.*

UVOD

Kibernetsko vojskovanje je v rusko-ukrajinski vojni odprlo novo fronto bojevanja, ki je ključnega 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 okrepile svojo kibernetsko obrambo. Države, predvsem članice NATA, so začele zaradi tega konflikta namenjati večjo pozornost svojim kibernetskim zmogljivostim (Willet 2022, 7–11).

Internet je spremenil naš pogled na svet in interakcijo z njim na veliko načinov, na žalost ta sprememba ni omejena le na mirnodobne dejavnosti. Ta razvoj vpliva tudi na način bojevanja v vojnah. Zdaj ko je vsaka država povezana in odvisna od interneta za novice, volitve in komuniciranje s svojimi državljani, je pomembno razumeti, kako kibernetsko vojskovanje deluje. Vojna v Ukrajini je idealen primer za analizo kibernetskega vojskovanja. V vojni med Rusijo in Ukrajino je imelo kibernetsko vojskovanje več različnih pomenov (za sodobne spopade). Kibernetski napadi niso le nova dimenzija vojskovanja, ampak so tudi dopolnili tradicionalne vojaške taktike, merijo lahko na digitalno in tudi na fizično infrastrukturo. Pred in med vojno so se ti napadi pogosto uporabljali za

* Patrik Rebrica, magister obramboslovja in varnostnih študij, Fakulteta za družbene vede, Univerza v Ljubljani, e-pošta: patrik.rebrica@gmail.com; Dr. Vladimir Prebilič, redni professor, Fakulteta za družbene vede, Univerza v Ljubljani, Slovenija.
** Pregledni znanstveni članek.
DOI: 10.51936/tip.62.1.171

ustvarjanje zmede, oslabili so poveljevanje in tudi moralo vojakov ali civilistov. Če ga primerjamo s konvencionalnim bojevanjem, je kibernetsko vojskovanje s finančnega in gospodarskega vidika enako uničujoče. Kibernetski napadi lahko destabilizirajo celotno gospodarstvo države in povzročijo dolgotrajne težave.

V članku bo analizirana doktrina kibernetskega vojskovanja Ukrajine in Rusije. Časovni okvir zajema obdobje pred invazijo in traja vse do leta 2024. Razloženi bodo posamezni načini delovanja kibernetskega vojskovanja v okviru doktrin. Raziskovalno vprašanje je: »Kako se ruska vojaška doktrina razlikuje od ukrajinske glede na ofenzivne in defenzivne strategije?«

Ta konflikt je za mednarodno skupnost jasen primer, zakaj je nujna potreba po močni kibernetski obrambi in zavarovani infrastrukturi. S tem se zmanjšujejo tveganja takšnih napadov. Posledice kibernetskih napadov niso omejene le na regijo, saj zahtevajo globalni odziv (Singer in Friedman 2022; Rid 2020).

OPREDELITEV KONCEPTOV KIBERNETSKEGA VOSKOVANJA

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 pomeni tveganje za nacionalno varnost, kibernetske vojne pa natančneje ne opredeljuje. 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 ogroziti cilje nasprotne države. Kljub temu do zdaj še ni univerzalne formalne opredelitve kibernetskega napada kot vojaškega dejanja (Clarke 2010).

V Talinskem priročniku (ang. *Tallinn Manual*), ki obravnava uporabo mednarodnega prava v kibernetskem prostoru, se izraz kibernetsko vojskovanje (ang. *cyber warfare*) uporablja za opisovanje sovražnih dejanj v kibernetskem prostoru, ki so primerljiva z oboroženimi napadi (Schmitt 2017).

V slovenščini še ni univerzalno sprejete definicije; uporabljajo se različni izrazi, kot so informacijsko bojevanje, informacijsko vojskovanje in kibernetsko vojskovanje. Poudarek je na tem, da informacijsko bojevanje ne zajema le vojaških operacij, ampak tudi vohunske, psihološke in gospodarske dejavnosti, ki jih izvajajo države, organizacije ali celo posamezniki. Kibernetsko vojskovanje se v tem kontekstu pogosto uporablja kot del informacijskega bojevanja, zlasti kadar gre za napade v digitalnem prostoru, vendar jasna razmejitev med izrazi še ni ustaljena (Bernik & Prislan 2011).

V tem članku bosta uporabljena naslednja termina:

Kibernetsko vojskovanje (ang. cyber warfare) označuje širši koncept uporabe kibernetskih operacij kot sredstva vojskovanja med državami ali oboroženimi akterji. Vključuje tako ofenzivne kot defenzivne strategije, kot so napadi na kritično infrastrukturo, vohunjenje, sabotaže in dezinformacije. To je strateški in politični vidik kibernetskega konflikta.

Kibernetsko bojevanje (ang. cyber combat ali cyber operations in combat) pa se nanaša na konkretne operacije v okviru kibernetskega vojskovanja. Gre za dejanske napade in obrambo v kibernetskem prostoru, ki se izvajajo v okviru oboroženih spopadov ali drugih sovražnih aktivnosti. Ta izraz se pogosteje uporablja v vojaškem in operativnem kontekstu.

Najpogostejše vrste kibernetskih napadov

Za razumevanje kibernetskega vojskovanja je treba najprej razumeti najpogostejše kibernetske napade.

- Zlonamerna programska oprema je virus, ki napada informacijske sisteme (Malware, Ransomware, Wiper). Primeri zlonamerne programske opreme so izsiljevalni, vohunski in trojanski programi. Odvisno od vrste zlonamerne kode lahko hekerji zlonamerno programsko opremo uporabijo za krajo ali za skrito kopiranje občutljivih podatkov, blokirajo dostop do datotek, povzročajo motnje delovanja sistema ali onemogočijo delovanje sistemov (Pratt 2024).
- *Phishing* je vrsta kibernetskega napada, pri katerem se napadalci predstavljajo kot legitimni subjekti, da bi posameznike prevarali in dosegli, da jim posredujejo občutljive podatke, kot so uporabniška imena, gesla in številke kreditnih kartic. Ti podatki se nato uporabijo za škodljive namene, kot sta kraja identitete ali finančna goljufija (CISA 2024).
- *SMiShing*, imenovan tudi SMS phishing ali smishing, je razvoj metodologije lažnega predstavljanja prek besedila (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 prejemajo propagandna sporočila na svoje mobilne telefone (Pratt 2024).
- DDoS (distributed denial-of-service) se zgodi, ko hekerji bombardirajo strežnike organizacije z velikimi količinami podatkovnih zahtev hkrati, zaradi česar strežniki ne morejo obravnavati nobenih legitimnih zahtev. Ti napadi so prevladovali v začetnih dneh vojne v Ukrajini (Pratt 2024).
- »Tuneliranje« sistema domenskih imen (ang. *Domain name system – DNS*) je sofisticiran napad, pri katerem napadalci vzpostavijo in nato uporabljajo stalno razpoložljiv dostop ali predor/tunel v sisteme, na katere merijo (Pratt 2024).

Taktika kibernetskega bojevanja

Taktika se osredini na kratkoročne ukrepe in konkretne bojne operacije, medtem ko strategija določa dolgoročne cilje in splošno usmeritev vojne ali kampanje. Taktika obravnava, »kako« izvesti spopad, strategija pa »kaj« je njegov končni cilj in kako ga doseči (Clausewitz 1984).

Dezinformacije in propaganda – ruske dezinformacijske kampanje temeljijo na družbenih omrežjih. Glavni cilj je širiti nezaupanje v družbene in tradicionalne medije ter omajati zaupanje v poštenost volitev prek botnet sistemov.

Kibernetsko vohunjenje – to ni vojskovanje kot tako, ampak stalna dejavnost držav, da ugotovijo prednosti in slabosti ne samo sovražnikov, ampak tudi drugih držav, prijateljskih ali neopredeljenih. Obstaja veliko dokumentiranih primerov kibernetskega vohunjenja organizacij, ki jih je sponzorirala država. Država je lahko osumljena ali razkrita, da je nadzorovala druge države za namene kibernetskega vohunjenja. Ameriška agencija za nacionalno varnost je na primer posnela skoraj vsak pogovor z mobilnim telefonom na Bahamih, ne da bi bahamska vlada to dovolila.

Kibernetski terorizem – to 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, nezaupanje; destabilizirati ali degradirati vlado ali politično pomembne dejavnosti in infrastrukturo.

Kibernetska sabotaža – gre za kibernetsko operacijo, pri kateri nastane fizična škoda, oz. za sabotažo. To pomeni namerno uničiti, poškodovati ali ovirati delovanje infrastrukture znotraj države, zlasti zaradi politične ali vojaške koristi. Med sabotaže spada kibernetični napad na Viasat, pri katerem je bila povzročena ogromna škoda (A10 2022)

RUSKA DOKTRINA KIBERNETSKEGA VOJSKOVANJA

Rusija na kibernetiko oziroma kibernetsko vojskovanje gleda zelo drugače kot zahodne države. Ruski teoretiki opredeljujejo kibernetsko vojskovanje glede na to, kako Kremelj uporablja svoje kibernetske zmogljivosti. Članek izpostavlja značilnosti ruske doktrine kibernetskih napadov ter kako je bila ta doktrina uporabljena v vojni z Ukrajino (Connel in Volger 2017, 1–2).

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 prost pretok informacij, ki jih ustvarja, se pri tem obravnavata kot grožnja in tudi kot priložnost.

Ruska definicija kibernetskih napadov

Rusi na splošno ne uporabljajo izrazov, kot je kibernetsko vojskovanje (rus. *kibervoyna*), razen ko se sklicujejo na zahodne ali druge tuje zapise o tej temi. Namesto tega se nagibajo k uporabi besede informatizacija. To pomeni, da konceptualizirajo kibernetske operacije znotraj širše kategorije informacijske vojne. Izraz, kot ga uporabljajo ruski vojaški teoretiki, je celosten koncept, ki vključuje delovanje računalniških omrežij, elektronsko bojevanje, psihološke operacije in informacijske operacije. Z drugimi besedami, kibernetsko vojskovanje je treba razumeti kot mehanizem, ki državi omogoča prevlado v informacijski pokrajini, ki velja za samostojno področje novodobnega vojskovanja. Idealno bi moral biti ta koncept kibernetskega bojevanja del celotnega vladnega prizadevanja, skupaj z drugimi, bolj tradicionalnimi metodami. Že vse od časov sovjetske vojaške doktrine se država ukvarja z dezinformacijskimi operacijami oz. tako imenovanimi *PsyOps*, vohunjenjem in politično subverzijo. Razvejanost tega pojmovnega razlikovanja je velika. Po navedbah Vojaške doktrine Ruske federacije iz leta 2010 je ena od značilnosti sodobnih vojaških konfliktov predhodna izvedba operacij informacijskega bojevanja – z namenom doseči politične cilje brez uporabe vojaške sile in nato v interesu oblikovanja ugodnega odziva mednarodne skupnosti. Tako informacijska vojna in posledično kibernetska vojna postaneta legitimno orodje države v miru in tudi v vojnem času (Connel in Volger 2017, 3–6).

General Valerij Gerasimov, načelnik generalštaba Ruske federacije, je v svojem zdaj slavnem članku »Vrednost znanosti pri napovedovanju« bolj splošno namigoval na mirnodobno uporabo informacijskih operacij; zapisal je, da se v 21. stoletju brišejo meje med stanjem vojne in miru. Vojne niso več napovedane. Izkušnje vojaških spopadov, vključno s tistimi, ki so povezani s tako imenovano barvno revolucijo v severni Afriki in na Bližnjem vzhodu, so potrdile, da se lahko popolnoma uspešna država v nekaj mesecih oz. tednih spremeni v areno hudih oboroženih spopadov. Države postanejo žrtev tuje intervencije in se potopijo v mrežo kaosa, humanitarnih katastrof in državljanskih vojn (Connel in Volger 2017, 7–8).

Ruska doktrina med kibernetskimi in informacijskimi operacijami ne razlikuje tako kot zahodna. Namesto tega ruski koncept prepleta fizične in psihološke značilnosti meddržavnega konflikta, ki je zdaj močno posredovan s tehnologijo v celotnem informacijskem prostoru. Dokument iz leta 2011, ki ga je objavilo rusko obrambno ministrstvo, je informacijsko vojno opredelil kot:

> *Konflikt med dvema ali več državami v informacijskem prostoru s ciljem povzročitve škode informacijskim sistemom, procesom in virom ter kritično pomembnim strukturam in drugim strukturam; spodkopavanje političnih, gospodarskih in družbenih sistemov; izvajanje množičnih psiholoških kampanj proti prebivalstvu države, da bi destabilizirali družbo in vlado; pa tudi prisiliti državo, da sprejema odločitve v interesu svojih nasprotnikov.*

Ta definicija je veliko širša od tistega, kar ameriški analitiki imenujejo »kibernetska vojna«. Pomaga tudi pri razlagi krepitve političnih ciljev države in potrebe po propagandi v ruskih operacijah. Posebnost »informacijske vojne« v Rusiji je povezanost njenih akterjev. Kdo je organizator teh akcij? Proti komu so v resnici uperjene? Ta dvoumnost, ne glede na akterje, služi tako kot zaščita za državo in možnost zanikanja informacijske vojne (Connel in Volger 2017, 7–10).

Rusija ne izvaja informacijske vojne le v tujih državah, ampak tudi nad svojim prebivalstvom. Ta zasnova tudi briše meje med tujimi in domačimi grožnjami, pri čemer se opira na leninistične teme nenehnega političnega boja. Na to nakazujejo kibernetsko podprta orodja spletnega nadzora in cenzure znotraj ruskih meja ter prizadevanja za izolacijo Rusije od svetovnega interneta. Zunanjepolitične bitke Kremlja pogosto ni mogoče ločiti od njegovega boja za stabilnost domačega režima (Connel in Volger 2017, 10–12).

Glavni pomen bojevanja v informacijskem soočenju izhaja iz ruskega koncepta »strateškega odvračanja«. Temelji na razumevanju, da jedrsko orožje ne odvrača dovolj oz. celotnega spektra sodobnih varnostnih groženj. Torej strateško odvračanje ne vključuje le jedrske in konvencionalne vojaške moči, temveč tudi vrsto nevojaških orodij, kot so ideološki, politični, diplomatski, gospodarski in osrednji informacijski in digitalni ukrepi. Zato je pomembno razumeti, da pri strateškem odvračanju, kljub njegovemu imenu, ne gre le za odvračanje v zahodnem razumevanju tega izraza, temveč za celovit pristop k doseganju strateških ciljev. Ruska vojska je priznala, da se poskušajo razvijati na tem področju, saj se hočejo izogniti usodi Sovjetske zveze in gospodarski stagnaciji sodobne Rusije (Hakala in Melnychuk 2021, 10–19).

Značilnosti ruske doktrine

Ruska doktrina kibernetskega vojskovanja zajema vrsto strategij in taktik za doseganje in 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, 33; Willett 2022, 22–23).

- Informacijsko vojskovanje in psihološko delovanje: Rusija daje velik poudarek uporabi kibernetskih orodij za informacijsko vojno, katere cilj je oblikovati javno mnenje in vplivati na politične rezultate. To vključuje širjenje dezinformacij, propagande in manipulacijo družbenih medijev za ustvarjanje razdora in nezaupanja v ciljnih družbah (Wilde 2022; Bateman 2022, 34–39).
- Vohunjenje in zbiranje obveščevalnih podatkov: ruske kibernetske operacije se pogosto osredotočajo na zbiranje obveščevalnih podatkov iz vladnih, vojaških in zasebnih omrežij. To dosegajo s prefinjenimi kibernetskimi vohunskimi kampanjami, ki izkoriščajo ranljivosti ciljnih sistemov za odliv občutljivih podatkov (Wilde 2022; Bateman 2022, 34–39).
- Napadi na ključno infrastrukturo: Rusija je dokazala, da je sposobna in da namerava napadati ključno infrastrukturo, vključno z energetskimi omrežji,

finančnimi sistemi in prometnimi omrežji. Eden od primerov takšnega napada je NotPetya. Ta napad je bil usmerjen na ukrajinsko električno omrežje in je povzročil obsežne motnje ter gospodarsko škodo. Glavni cilj napada je bil povzročiti prekinitev delovanja in škodo v omrežju. (Wilde 2022; Bateman 2022, 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 so to napadi DDoS. Cilj je ohromiti infrastrukturo, povzročiti finančno izgubo ali ukrasti občutljive informacije (Wilde 2022; Bateman 2022, 34–39).
- Usklajevanje z vojaškimi operacijami: ruske kibernetske zmogljivosti so trenutno vključene v konvencionalne vojaške operacije. S tem 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 strateško boljše ciljanje, obveščevalne podatke in lažjo okupacijo območja (Bartles 2016, 30–37; Bateman 2022, 34–39).

Informacijsko bojevanje in psihološko delovanje

Informacijsko bojevanje in psihološke operacije so osrednje sestavine ruske doktrine kibernetskega bojevanja. Cilj te strategije je vplivati na nasprotnika, ga ovirati in spodkopati njegovo politično, družbeno in gospodarsko stabilnost. Vključuje uporabo različnih tehnik za manipuliranje z javnim mnenjem, širjenje dezinformacij in ustvarjanje družbenega razdora.

Glavni cilj ruske informacijske vojne je ustvariti politične razmere, ki ustrezajo njihovim ciljem. To se naredi v treh fazah. Najprej je treba pridobiti celotno sliko situacije. Ugotoviti, kako ciljno prebivalstvo dojema realnost, zatem usmerjati politične in družbene danosti v korist Rusije. Druga faza je spodkopavanje zaupanja ljudstva v državne institucije, medije in demokratične procese v državi. Tretja in zadnja faza je sejati zmešnjavo – ustvarjanje kaosa v nasprotni državi, da bi oslabili enotnost in ustvarili ugodnejše okolje za ruske interese. Informacijsko bojevanje tudi pripomore k lažji okupaciji območja, ki ga je okupirala ruska stran (Atlantic Council 2024; Treyger in drugi 2022, 10–15).

Vohunjenje in zbiranje obveščevalnih podatkov

Zgodovinsko gledano sta bila vohunjenje in zbiranje obveščevalnih podatkov ključna vidika vojskovanja, prav tako tudi za kibernetsko vojskovanje. Gre za zbiranje občutljivih informacij vladnih, vojaških in zasebnih virov. Tovrstne operacije so namenjene zagotavljanju strateških prednosti, pri čemer lahko strategi potem informirano sprejemajo odločitve (Stiftung Wissenschaft und Politik 2023; Watts 2023).

Glavni cilji ruskega kibernetskega vohunjenja so pridobiti strateške informacije, spodkopavati sile nasprotnikov in podpirati vojaške in diplomatske cilje svoje države. Torej je glavni in najpogostejši cilj teh napadov pridobiti dragocene podatke, povezane z nacionalno varnostjo, vojaškimi zmogljivostmi, gospodarskimi strategijami in tehnološkimi inovacijami. Z natančnimi obveščevalnimi podatki si država priskrbi povečanje učinkovitosti vojaških operacij in diplomatskih pogajanj. S tem država tudi slabi zmogljivosti in moralo konkurenčnih držav z razkrivanjem ranljivosti in izkoriščanjem ukradenih informacij za propagando ali izsiljevanje (Stiftung Wissenschaft und Politik 2023; Watts 2023).

Socialni inženiring je znana taktika ruskega kibernetskega vojskovanja. To je manipulacijska taktika, ki se uporablja za pridobitev nadzora nad računalniškim sistemom ali krajo osebnih in finančnih podatkov. Napadalci uporabljajo psihološko manipulacijo, da zavajajo uporabnike in jih napeljejo k napakam ali razkritju občutljivih informacij. Napadi socialnega inženiringa se izvajajo v več korakih, pri čemer napadalec najprej razišče svojo žrtev in zbere potrebne informacije za izvedbo napada. Nato uporabi različne taktike, kot je pridobivanje zaupanja žrtve, da jo prepriča k nepremišljenim dejanjem, ki ogrozijo varnostne prakse, na primer razkritje občutljivih informacij ali odobritev dostopa do pomembnih virov (Watts 2023).

Kibernetske sabotaže in bojevanje proti ključni infrastrukturi

Kibernetski napadi na vladna omrežja in infrastrukturo lahko vplivajo na kulturo in javno mnenje, še posebej pred političnimi volitvami. Takšni napadi, ki vključujejo kibernetsko vohunjenje in dezinformacijske kampanje, lahko vplivajo na volivce in trajno poslabšajo demokratične procese. Hekerji, opremljeni s kibernetskim orodjem, kradejo denar, podatke in širijo laži, kar vpliva na zaupanje v vlado (legitimnost) in moti komunikacije. Nekateri režimi uporabljajo kibernetske operacije za vplivanje na notranje zadeve drugih držav in povzročanje političnih in družbenih nemirov. Zaščita agencij za nacionalno varnost in vladnih omrežij je zato nujna. Za boj proti kibernetskim grožnjam sta potrebna močna kibernetska varnost in mednarodno usklajevanje med zavezniki, saj imata lahko kibernetska vojna in vohunjenje resne posledice za mednarodne odnose in nacionalno varnost. Kibernetski napadi, kot so napadi na kreditna omrežja in plačilne sisteme, lahko povzročijo veliko gospodarsko škodo in ovirajo gospodarstvo v primeru motenj v energetskih sistemih in industrijskih dejavnostih. Obramba pred takšnimi napadi predstavlja operativne izzive. Poleg tega kibernetsko vohunjenje ogroža gospodarstva, saj lahko napadalci ukradejo občutljive podatke ali intelektualno lastnino, kar jim daje poslovne prednosti. Stroški, povezani s kibernetskimi napadi, vključujejo odzivanje na incidente in izdatke za varnost računalniških sistemov. Poleg tega lahko napadi povzročijo dolgoročne stroške, kot sta okrnjen ugled blagovne znamke in izguba zaupanja strank, kar lahko privede do izgub za podjetje. Vdori v vojaške sisteme lahko geopolitično vplivajo tudi na svetovne trge (Slonopas 2024).

Usklajevanje kibernetskega bojevanja z vojaškimi operacijami

Potem ko je februarja leta 2022 izvedla invazijo na Ukrajino, je Rusija – tako kot v vojni z Gruzijo – dopolnila tradicionalno vojskovanje s kibernetskim. Rusiji je uspelo tudi povečati učinkovitosti tradicionalnih vojaških sil z motenjem sovražnikovih komunikacij, logistike in sistemov poveljevanja in nadzora. Strokovnjaki ugotavljajo, da so kibernetske operacije v vojni uporabne tudi za napadanje logističnih sistemov, saj so ti pogosto civilni in manj zavarovani kot vojaški. Kljub temu mnogi ugotavljajo, da kibernetske zmogljivosti najbolje služijo obveščevalnim in izvidniškim funkcijam ter ne nadomeščajo konvencionalnega orožja. V mnogih primerih je hitreje, enostavneje in tudi ceneje nevtralizirati cilj z letalskimi napadi ali artilerijskim ognjem kot pa s kibernetsko operacijo (Schulze in Kerttunen 2023; Kerr 2023).

Kibernetsko bojevanje se dandanes ne obravnava več kot samostojna zmogljivost, ampak kot dodatek h konvencionalnim zmogljivostim. Kibernetske operacije lahko delujejo zelo učinkovito, če se uporabljajo na kombiniran način. Omogočajo pridobitev strateške prednosti z boljšim pridobivanjem informacij in motenjem sovražnikovih. Primer za to je zlonamerna programska oprema X-Agent, ki se infiltrira v opremo za ciljanje artilerije in posreduje geolokacijo artilerijskih položajev sovražnim silam, ki nato usmerjajo ogenj. Ta konceptualizacija kibernetskih zmogljivosti se odlično ujema z idejo manevrskega bojevanja in ohromitve sovražnika s kirurško natančnimi udarci. S tem se oslabi nasprotnikovo obrambo in infrastrukturo, s čimer se pripravi pot za učinkovitejše konvencionalne napade. Konstantno se tudi spodkopava sovražnikovo moralo in zaupanje civilistov z ustvarjanjem zmede in kaosa, kar vpliva na zmanjševanje odpora do prihodnjih vojaških ukrepov (Schulze in Kerttunen 2023; Kerr 2023).

UKRAJINSKA KIBERNETSKA DOKTRINA

Ukrajinska kibernetska doktrina je usmerjena k krepitvi kibernetskih zmogljivosti za obrambo kibernetske varnosti; s tem se odziva na vse večje kibernetske grožnje, zlasti s strani 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 sooča s trajno kibernetsko agresijo, 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 oborožene agresije na Ukrajino;
- odpornost – sposobnost družbe in države, da se hitro prilagodita spremembam v varnostnem okolju in ohranita trajnostno delovanje, zlasti z zmanjševanjem zunanje in notranje ranljivosti;

- interakcija – razvoj strateških odnosov s ključnimi tujimi partnerji, predvsem z Evropsko unijo in Natom ter njunimi državami članicami, Združenimi državami Amerike, in pragmatično sodelovanje z drugimi državami in mednarodnimi organizacijami; to temelji na nacionalnih interesih Ukrajine.

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 ter 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, 6–10).

Priznavanje kibernetskega prostora kot operativne domene

Strategija kibernetske varnosti Ukrajine, ki je bila sprejeta z odlokom predsednika leta 2016, opredeljuje grožnje kibernetski varnosti in ustrezne prednostne naloge za zagotavljanje kibernetske varnosti v Ukrajini. Ta dokument temelji na določbah Konvencije Sveta Evrope o kibernetski kriminaliteti in je namenjen ustvarjanju razmer za varno delovanje kibernetskega prostora in njegovo uporabo v interesu posameznika, družbe in države. Strategija kibernetske varnosti Ukrajine (2016) je bila prvi uradni dokument na področju kibernetske varnosti. Opisuje glavne grožnje na področju kibernetske varnosti in priznava »kibernetski prostor« kot ločeno področje sovražnosti, v katerem so vse bolj dejavne kibernetske enote drugih oboroženih sil vodilnih držav. Dokument opisuje tudi nacionalni sistem kibernetske varnosti in določa odgovornosti za glavne subjekte kibernetske varnosti. Druga različica Strategije nacionalne varnosti Ukrajine, ki je bila potrjena leta 2020, je postala podlaga za številne nove strategije na več področjih. Varnost in razvoj kibernetskega prostora, uvedba e-uprave, zagotavljanje varnosti in trajnostnega delovanja elektronskih komunikacij in nacionalnih elektronskih informacijskih virov morajo biti sestavni vidiki državne politike razvoja informacijskega prostora in razvoja informacijske družbe v Ukrajini (Atkins 2022; Spînu 2020, 5).

Kolektivna obramba in medsebojna pomoč

Doktrina Nata poudarja kolektivno obrambo, pri čemer se napad na eno članico šteje za napad na vse. Ukrajina, ki se sooča z nenehnimi kibernetskimi grožnjami, zlasti s strani akterjev, ki jih podpirajo tuje države, poudarja pomen mehanizmov kolektivne obrambe in mednarodnega sodelovanja. Ukrajina aktivno sodeluje z Natom in drugimi mednarodnimi partnerji, da bi okrepila svoje zmogljivosti kibernetske obrambe, ter si prizadeva za vzajemno pomoč in podporo. Ukrajinska strategija vključuje tudi partnerstva in sodelovanje z

mednarodnimi organi, da bi okrepila svojo kibernetsko obrambo (Atkins 2022; Spînu 2020, 7–11).

K uspehu ukrajinske kibernetske obrambe je verjetno prispevalo več dejavnikov, med njimi pa so najpomembnejša partnerstva z drugimi državami. Čeprav partnerstva na področju kibernetske varnosti niso novost, je uspeh pogosto izmuzljiv in omejen. V ukrajinskem primeru je Kijev na operativni ravni (kjer poteka večina kibernetske obrambe) učinkovito sodeloval s številnimi sposobnimi subjekti na mednarodni, industrijski in vladni ravni. Zato je Ukrajina lahko uporabila mrežo operativnega partnerstva, ki omogoča dinamično usklajevanje različnih tehničnih zmogljivosti, strokovnega znanja in pristojnosti za skupno prepoznavanje groženj in obrambno ukrepanje. Ločeno so bile pred invazijo napotene ekipe, sestavljene iz ameriških vojakov iz kibernetskega poveljstva ZDA in civilistov iz ameriških podjetij, ki so pomagali pri pripravi ukrajinske obrambe. Vzpostavili so delovne odnose z ukrajinskimi upravljavci infrastrukture, kar je pomagalo preprečiti napade na najpomembnejše sisteme, kot so železniška infrastruktura in omrežja za nadzor meje. V več primerih so izkoristili odnose z zasebnimi podjetji za kibernetsko varnost in drugimi vladnimi subjekti, da bi zagotovili obrambne rešitve, prilagojene grožnjam (Atkins 2022; Spînu 2020, 10–11).

Skupine za hitro odzivanje na kibernetske grožnje in odzivanje na incidente

Ekipe Nata za hitro odzivanje na kibernetske incidente (*ang. Cyber Rapid Reaction Teams – CRRT*) so namenjene zagotavljanju takojšnje podpore med večjimi kibernetskimi incidenti. Ukrajina je razvila podobne mehanizme hitrega odzivanja za takojšnje odzivanje na kibernetske grožnje. To vključuje vzpostavitev specializiranih enot v njenem varnostnem aparatu za hitro obravnavo kibernetskih incidentov in ublažitev njihovih posledic (Spînu 2020, 9–10).

Javno-zasebna partnerstva

Ukrajina je že imela določeni okvir za javno-zasebna partnerstva, ki so povezana s področjem kibernetske varnosti, vendar pa so vse bolj zahtevni izzivi zahtevali hitro in celovito revizijo ter izboljšanje tehničnih in operativnih vidikov kibernetske varnosti. V prvi strategiji kibernetske varnosti je leta 2016 ustvarila razmere za varno delovanje kibernetskega prostora v korist posameznika, družbe in države. Trenutno posodobljena različica je namenjena obravnavi in izboljšanju vprašanj komunikacije in usklajevanja med vladnimi agencijami. Ukrajina ne premore finančnih spodbud, s katerimi bi pritegnila najboljše strokovnjake k delu za vlado. Zato je toliko bolj pomembno povečati sodelovanje med javnim in zasebnim sektorjem, ki je ključno za uspeh na področju kibernetske varnosti. Velik del krepitve ukrajinske kibernetske obrambe ne bi bil mogoč, če zahodni partnerji ne bi finančno pomagali ter usposabljali strokovnjake. Da bi Ukrajina v državi dosegla močno kibernetsko varnost, bi morala zagotoviti enak obseg

razvoja med zasebnim sektorjem in kibernetsko infrastrukturo. Področje javno-zasebnega partnerstva je še v zgodnji fazi razvoja, vendar že ima ključen pomen (Spînu 2020, 10–12; Koyanagi 2022).

Razvoj pravnih in normativnih okvirov

Zakon »O osnovnih načelih kibernetske varnosti Ukrajine« opredeljuje pravno in organizacijsko podlago za zaščito vitalnih interesov države v kibernetskem prostoru. Namen zakona je zagotoviti varnost človeka, družbe in države ter zaščititi nacionalne interese. Zakon določa cilje, usmeritve in načela državne politike na področju kibernetske varnosti ter pooblastila organov, podjetij, institucij, organizacij, posameznikov in državljanov na tem področju (Atkins 2022; Spînu 2020).

GLAVNE RAZLIKE MED DOKTRINAMI – PREGLED IN PRIMERJAVA

Primer ruske doktrine na napadu »WhisperGate«

Napad WhisperGate se je začel 14. januarja 2022, v ukrajinskih medijih pa so o njem poročali dan kasneje. Napad je vključeval tri komponente: zlonamerni nalagalnik, program za prenos datotek in brisalec datotek. Programska oprema je bila zasnovana tako, da je uničevala podatke okuženih sistemov, pri čemer se je prikazovala kot izsiljevalska programska oprema, čeprav ni omogočala obnovitve podatkov. Napad je poškodoval glavni zagonski zapis (MBR), s čimer je onemogočil delovanje sistemov, nato pa je prepisal datoteke z lažno zahtevo po odkupnini (Microsoft 2022; Crowdstrike 2022).

Napad je povzročil hude motnje v ključni infrastrukturi, potekal pa je sinhronizirano z napadi DDoS na ukrajinske spletne strani. Cilj je bil ustvariti kaos, zmanjšati zaupanje v vlado in demoralizirati prebivalstvo pred invazijo Rusije. Usklajenost napada z invazijo nakazuje, da je bil del širše strategije kibernetskega bojevanja za destabilizacijo države (Crowdstrike 2022; Lyons 2022).

Primer ukrajinske doktrine na napadu »Industroyer2«

Izbruh konflikta v vzhodni Ukrajini leta 2014 je sprožil številne kibernetske napade, predvsem na ukrajinsko električno infrastrukturo. Industroyer2 je nadgradnja zlonamerne programske opreme Industroyer, namenjena motenju industrijskih nadzornih sistemov v električnih postajah. Uporabljena je bila v napadu na ukrajinsko električno omrežje leta 2016, kar je povzročilo izpad elektrike v Kijevu (HeadMind Partners 2022).

Ukrajina je na napad Industroyer2 uspešno odgovorila, saj je od leta 2016 zelo izboljšala kibernetsko varnost. Sodelovanje z ESET in CERT-UA je omogočilo zgodnje odkrivanje napada in hitro izolacijo okuženih sistemov, s čimer so preprečili hujše posledice (ESET 2022).

Krepitev kibernetske obrambe, nadzor industrijskih sistemov ter sodelovanje z mednarodnimi agencijami so bili ključni za uspešno obrambo. Ta odziv

jasno odraža ukrajinsko doktrino kibernetskega vojskovanja, ki je primarno defenzivno usmerjena. Njena strategija temelji na odpornosti, hitrem odzivu ter sodelovanju s partnerji, kot so tehnološka podjetja in Nato. Namesto izvajanja agresivnih kibernetskih napadov Ukrajina krepi svojo obrambno infrastrukturo, kar je ključno za zaščito pred prihodnjimi grožnjami (ESET 2022; HeadMind Partners 2022).

Tabela 1: PRIMERJALNA TABELA DOKTRIN

Doktrina	Ruska doktrina	Ukrajinska doktrina
Osnovna usmeritev	Ofenzivna – usmerjena v napad in destabilizacijo	Defenzivna – usmerjena v zaščito in odpornost
Glavni cilji	Destabilizacija nasprotnikov, vpliv na politične procese, širjenje dezinformacij	Zaščita kritične infrastrukture, zagotavljanje nacionalne varnosti
Uporaba kibernetskih operacij	Vključuje informacijsko vojno, vohunjenje, sabotaže in psihološke operacije	Poudarek na obrambi pred napadi, izboljšanje kibernetske varnosti in odpornosti
Glavna taktika	Kibernetsko vohunjenje, dezinformacije, napadi na infrastrukturo, širjenje propagande	Hitra odzivnost na incidente, kibernetska odpornost, javno-zasebna partnerstva. Uporaba specializiranih enot za hitro odzivanje kibernetskim grožnjam
Sodelovanje s tujimi akterji	Povezava z državnim nadzorom in vojaškimi enotami, pogosto uporaba prikritih akterjev	Močno sodelovanje z Natom, EU, zasebnimi podjetji in organizacijami za kibernetsko varnost
Primeri napadov	Napad NotPetya, napadi DDoS, sabotaže ukrajinske infrastrukture	Obramba pred napadi na električno omrežje, finančne institucije, železniško infrastrukturo
Povezava s konvencionalnim vojskovanjem	Kibernetske operacije podpirajo vojaške akcije in destabilizacijo nasprotnikov	Kibernetske operacije kot dodatek h konvencionalni obrambi in zaščiti prebivalstva
Glavna slabost	Močna ofenziva, a težave pri prikrivanju sledi in mednarodni odziv	Odvisnost od zunanje podpore in omejeni lastni viri

Vir: Povzeto po Connel in Volger (2017), Bateman (2022), Wilde (2022), Spînu (2020).

SKLEP

Na zastavljeno raziskovalno vprašanje »Kako se ruska vojaška doktrina razlikuje od ukrajinske glede na ofenzivne in defenzivne strategije?« je mogoče odgovoriti. Doktrini kibernetskega vojskovanja Rusije in Ukrajine sta nesimetrični. Ruska doktrina se zanaša na ofenzivo, medtem ko se ukrajinska na defenzivo. Ruska strategija je izrazito ofenzivna, z močno osredotočenostjo na informacijsko vojskovanje, vohunjenje in sabotaže, medtem ko je ukrajinska doktrina primarno defenzivna, s poudarkom na zaščiti kritične infrastrukture in sodelovanju z mednarodnimi partnerji. Poleg tega ima Rusija zaradi močnejših virov in bolj

razvite infrastrukture večjo sposobnost izvajanja kibernetskih napadov, medtem ko je Ukrajina okrepila svojo odpornost predvsem z zavezništvi z zahodnimi državami in zasebnimi tehnološkimi podjetji. Ruska doktrina je zasnovana tako, da povzroči čim večji kaos ter škodo, finančno in človeško. Posledično je tovrstno hibridno bojevanje v nasprotju z mednarodnim humanitarnim pravom, saj je usmerjeno na civilno infrastrukturo, bistveno za preživetje, kot so električna omrežja in zdravstveni sistemi. Humanitarno pravo zahteva razlikovanje 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 zaostrujejo humanitarne krize. Težave z identifikacijo kibernetskih napadov zamegljujejo 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. Medtem pa je ukrajinska doktrina drugačna od ruske. Ukrajinska doktrina si prizadeva za hiter odziv na nove grožnje in minimiziranje škode napadov, vendar se močno zanaša na zunanjo pomoč, kar bi lahko v prihodnosti predstavljalo šibkost.

- Mednarodno pravo se bo seveda moralo prilagoditi novim oblikam vojaških konfliktov, saj se vojskovanje vse bolj premika v novo digitalno sfero ter združuje različne metode, kot sta kibernetsko in hibridno vojskovanje. Obstoječa pravila, kot so Ženevske konvencije, so bila zasnovana za tradicionalne konflikte, zato je nujno oblikovati jasnejše smernice o tem, kdaj kibernetski napad šteje za oborožen napad in kakšne so njegove pravne posledice. Prav tako bo treba urediti odgovornost držav in posameznikov za škodo, povzročeno s kibernetskimi operacijami, ter določiti, kdaj se država pred njimi brani. V prihodnosti bo mednarodna skupnost morala vzpostaviti jasnejša pravila glede uporabe kibernetskih napadov in umetne inteligence v vojaške namene. Eden od izzivov bo preprečevanje eskalacije konfliktov zaradi napačnega pripisovanja napadov.
- Talinski priročnik je orodje za razumevanje kibernetskega prava, saj predstavlja temeljito študijo o uporabi obstoječega mednarodnega prava v kibernetskih konfliktih. Nastal je pod okriljem Natovega centra odličnosti za kibernetsko obrambo (CCDCOE), pripravila ga je skupina mednarodnih strokovnjakov. Priročnik preučuje, kako se pravila, kot sta jus ad bellum (pravica do vojne) in mednarodno humanitarno pravo, uporabljajo v kibernetskih operacijah. Čeprav ni pravno zavezujoč, služi kot pomembna referenca za razumevanje mednarodnega prava v kibernetskem prostoru. Ker se kibernetske grožnje nenehno razvijajo, si mednarodna skupnost prizadeva prilagoditi pravne okvire tako, da uravnotežijo varnostne interese držav ter zaščito pravic posameznikov v digitalnem okolju. Države morajo spoštovati digitalno infrastrukturo drugih držav in se vzdržati vmešavanja v njihove notranje zadeve. Kibernetski napadi, ki povzročijo znatno škodo, primerljivo s fizičnimi napadi, se lahko po Ustanovni listini ZN štejejo za uporabo sile,

kar lahko upraviči samoobrambo. V oboroženih konfliktih morajo kibernetske operacije jasno ločevati med vojaškimi in civilnimi cilji ter se izogibati pretirani škodi. Poleg tega lahko vlade odgovarjajo za kibernetske napade, ki izvirajo z njihovega ozemlja, tudi če jih izvajajo nedržavni akterji. Kibernetske operacije tudi ne smejo kršiti temeljnih človekovih pravic, kot sta pravica do zasebnosti in svoboda izražanja (Schmitt 2017).

- Eden pomembnejših etičnih izzivov pri uporabi kibernetskih operacij v vojni je razmerje med učinkovitostjo in človeškimi pravicami. Kibernetsko orožje je večinoma uporabljeno za hibridno vojskovanje in lahko povzroči veliko škodo civilni infrastrukturi, kot so bolnišnice, električna omrežja ali vodovodni sistemi, kar pomeni neposredno ogrožanje življenj. Poleg tega je težko določiti odgovornost za kibernetske napade, saj jih lahko izvajajo tako države kot nedržavni akterji. Vse to zastavlja vprašanja o pravičnosti in odgovornosti v sodobnem vojskovanju.
- Ukrajinska kibernetska doktrina se osredini na obrambne ukrepe, mednarodno sodelovanje in usklajevanje s standardi kibernetske varnosti Nata in EU. Podpira načela suverenosti, nevmešavanja in zaščite kritične infrastrukture, pri čemer je v veliki meri v skladu z mednarodnimi normami, vključno s Talinskim priročnikom. Ukrajina prav tako poudarja boj proti dezinformacijam in kibernetskim grožnjam iz Rusije. Ruska kibernetska doktrina pa zavzema bolj agresivno držo in poudarja »informacijsko suverenost« in ofenzivne kibernetske zmogljivosti. Kibernetske operacije vključuje kot del hibridnega vojskovanja, pri čemer pogosto krši mednarodne norme. V primerjavi z mednarodnim pravom si Ukrajina v veliki meri prizadeva za skladnost, medtem ko Rusija pogosto izpodbija uveljavljene pravne okvire in uporablja kibernetska orodja za razširitev državne moči. Ta kontrast spodbuja nenehne geopolitične kibernetske napetosti.
- Prihodnost kibernetskega vojskovanja bo zaznamovala večja povezanost kibernetskih napadov s konvencionalnimi oz. tradicionalnimi načini vojskovanja. Z napredovanjem tehnologije bodo države (in tudi nedržavni akterji) razvile še bolj zapletene vrste napadov, ki bodo lahko povzročili ogromno škode, predvsem z orodji UI (ang. *AI*). Meje med kibernetskim in kinetičnim bojevanjem se bodo zabrisale. Kibernetska orodja se v vojni uporabljajo kot artilerija, da se omehča teren in pripravi območja za tradicionalni kinetični napad. Kibernetsko vojskovanje je predvsem pomembno za predvojno načrtovanje, propagando in demoralizacijo, strateško ciljanje ključne infrastrukture in drugih tarč in nadziranje okupiranega območja. V zvezi s kibernetskim vojskovanjem je treba izpostaviti, da sodi v okvir hibridnega vojskovanja, saj poleg vojaških tarč meri predvsem na civiliste. Najverjetneje bodo tudi prihodnje vojne še vedno temeljile na hibridnem vojskovanju. (Duguin in Pavlova 2023, 14–15).

LITERATURA

A10. 2022. »Cyber Warfare: Nation State Sponsored Cyber Attacks.« *a10networks*. https://www.a10networks.com/blog/cyber-warfare-nation-state-sponsored-cyber-attacks/.

AI Team. 2024. »Rogue AI is the Future of Cyber Threats.« *TrendMicro*, 25. avgust 2024. https://www.trendmicro.com/en_fi/research/24/h/rogue-ai-part-1.html.

Atkins, Sean. 2022. »A web of partnerships: Ukraine, operational collaboration, and effective national defense in cyberspace.« *Atlantic Council,* 30. avgust 2022. https://www.atlanticcouncil.org/content-series/airpower-after-ukraine/a-web-of-partnerships-ukraine-operational-collaboration-and-effective-national-defense-in-cyberspace/.

Bartles, Charles. K. 2016. »The Gerasimov Doctrine and Russian Non-Linear War.« *Military Review* 96 (1): 30–37.

Bateman, Jon. 2022. »Russia's Wartime Cyber Operations in Ukraine: Military Impacts, Influences, and Implications.« *Carnegie Endowment for International Peace*, 31–49. https://carnegieendowment.org/2022/12/16/russia-s-wartime-cyber-operations-in-ukraine-military-impacts-influences-and-implications-pub-88657.

Bernik, Igor., & Kaja Prislan. 2011. »Informacijsko bojevanje v Sloveniji – od tradicionalno lokalnega v globalni kibernetski prostor.« *Varstvoslovje* 13 (3): 261–79.

CISA – The Cybersecurity and Infrastructure Security Agency. 2024. »Recognize and Report Phishing.« *Cisa.gov.* https://www.cisa.gov/secure-our-world/recognize-and-report-phishing.

Clarke, Richard. A. 2010. *Cyber War.* New York: HarperCollins.

Clausewitz, Carl von., Michael Howard, Peter Paret, eds. [1832]1984. *On war.* United States: Princeton University Press.

Connel, Michael in Sarah Vogler. 2017. »Russia's Approach to Cyber Warfare.« *CNA Analysis and* Solutions, 1–23. https://www.cna.org/archive/CNA_Files/pdf/dop-2016-u-014231-1rev.pdf.

Council of Europe. 2001. »Convention on Cybercrime (ETS No. 185).« *coe.int.* https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=185.

ESET. 2022. »Industroyer2: Industroyer reloaded.« *Welivesecurity,* 12. april 2022. https://www.welivesecurity.com/2022/04/12/industroyer2-industroyer-reloaded/.

Hakala, Janne, in Jazlyn Melnychuk. 2021. »Russia's strategy in cyberspace.« NATO Strategic Communications Centre of Excellence, 10–19. https://stratcomcoe.org/cuploads/pfiles/Nato-Cyber-Report_15-06-2021.pdf.

HeadMind Partners. 2022. »Industroyer 2: the Russian Cyberattack on Ukraine Infrastructure.« *Headmind,* 31. maj 2022. https://www.headmind.com/industroyer-2/.

Information Security Office. 2024. »Social Engineering.« *cmu.edu.* https://www.cmu.edu/iso/aware/dont-take-the-bait/social-engineering.html.

Kerr, Jaclyn. A. 2023. »Assessing Russian Cyber and Information Warfare in Ukraine: Expectations, Realities, and Lessons.« *cna.org.* https://www.cna.org/reports/2023/11/assessing-russian-cyber-and-information-warfare-in-ukraine.

Koyanagi, Ken. 2022. »Ukraine's cyber power shows value of public-private partnership.« *Nikkei Asia.* https://asia.nikkei.com/Politics/Ukraine-war/Ukraine-s-cyber-power-shows-value-of-public-private-partnership.

Lyons, Jessica. 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/.

Microsoft. 2022. »Destructive malware targeting Ukrainian organizations.« *microsoft.com* https://www.microsoft.com/en-us/security/blog/2022/01/15/destructive-malware-targeting-ukrainian-organizations/.

Pratt, Mary. K. 2022. »Cyber attack.« *TechTarget.* https://www.techtarget.com/searchsecurity/definition/cyber-attack.

Rid, Thomas. 2020. *Active Measures: The Secret History of Disinformation and Political Warfare*. New York: Farrar, Straus and Giroux.

Schmitt, Michael. N., ed. 2017. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations.* Cambridge: Cambridge University Press. https://doi.org/10.1017/9781316822524.

Schulze, Matthias, Mika Kerttunen. 2023. »Cyber Operations in Russia's War against Ukraine Uses, limitations, and lessons learned so far.« *Stiftung Wissenschaft und Politik,* 17. april 2023. https://www.swp-berlin.org/10.18449/2023C23/.

Singer Peter. W. in Allan Friedman. 2014. *Cybersecurity and cyberwar: What everyone needs to know.* Oxford: Oxford University Press.

Slonopas, Andre. 2024. »What Is Cyber Warfare? Various Strategies for Preventing It.« *Information Technology Blog – American Public University,* 14. april 2024. https://www.apu.apus.edu/area-of-study/information-technology/resources/what-is-cyber-warfare/.

Spînu, Natalia. 2020. »Ukraine Cybersecurity Governance Assessment.« Switzerland: Geneva Centre for Security Sector Governance, November 2020. https://www.dcaf.ch/sites/default/files/publications/documents/UkraineCybersecurityGovernanceAssessment.pdf.

Stiftung Wissenschaft und Politik. 2023. »Cyber Operations in Russia's War Against Ukraine.« *SWP-Berlin*. https://www.swp-berlin.org/10.18449/2023C23/.

Treyger, Elina, Joe Cheravitch & Raphael S. Cohen. 2022. »Russian disinformation efforts on social media.« Santa Monica, CA: RAND Corporation, 108–30. https://www.rand.org/pubs/research_reports/RR4373z2.html.

Watts, Clint. 2023. »Is Russia regrouping for renewed cyberwar?.« *Microsoft On the Issues,* 15. marec 2023. https://blogs.microsoft.com/on-the-issues/2023/03/15/russia-ukraine-cyber-warfare-threat-intelligence-center/.

Wilde, Gavin. 2022. »Cyber Operations in Ukraine: Russia's Unmet Expectations.« *Carnegie Endowment for International Peace,* december 2022. https://carnegieendowment.org/files/202212-Wilde_RussiaHypotheses-v2.pdf.

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

THE CYBER WARFARE DOCTRINES OF RUSSIA AND UKRAINE

Abstract. *Cyber warfare has introduced a new dimension to modern conflicts whereby the risks are greater than ever before as critical infrastructure, financial systems, and personal data become targets. The boundaries between the digital and physical worlds are becoming blurred, adding to the need for effective cybersecurity. The purpose of the work is to examine the impact of cyber warfare in the Russo-Ukrainian war. Understanding doctrines and tactics helps enhance national security, protect civilians, and maintain the stability of global digital infrastructure, and permits the development of strategies to mitigate risks in future conflicts.*

Keywords: *Cybernetics, warfare, war, doctrine, defence.*