UNIVERZITET U SARAJEVU
FAKULTET POLITIČKIH NAUKA
ODSJEK POLITOLOGIJA

UTJECAJ CYBER TEHNOLOGIJE NA MEĐUDRŽAVNE SUKOBE

-magistarski rad-

Kandidat
Begić Melisa
Broj indeksa: 1211/II-PIR

Mentor
prof. dr. Nerzuk Ćurak

Sarajevo, 2024.

2024

Begić Melisa

Utjecaj cyber tehnologije na međudržavne sukobe

UNIVERZITET U SARAJEVU
FAKULTET POLITIČKIH NAUKA
ODSJEK POLITOLOGIJA

UTJECAJ CYBER TEHNOLOGIJE NA MEĐUDRŽAVNE SUKOBE
-magistarski rad-

Kandidat:
Melisa Begić
Broj indeksa: 1211/II-PIR

Mentor:
prof. dr. Nerzuk Ćurak

Sarajevo, *septembar* 2024.

SADRŽAJ

SKRAĆENICE 0
POPIS TABELA I SLIKA 0
UVOD 1
1. TEORIJSKE OSNOVE RADA 2
2. METODOLOŠKI OKVIR RADA 3
2.1. Problem istraživanja 3
2.2. Predmet istraživanja 3
2.2.1. Kategorijalno pojmovni sistem 3
2.3. Ciljevi istraživanja 5
2.3.1. Naučni cilj 6
2.3.2. Društveni cilj 6
2.4. Sistem hipoteza 6
2.4.1. Generalna hipoteza 6
2.4.2. Posebne hipoteze 6
2.5. Način istraživanja 7
2.5.1. Deskriptivna analiza 7
2.5.2. Analiza (sadržaja) dokumenata 7
2.5.3. Analiza slučaja/ case study 7
2.6. Naučna i društvena opravdanost istraživanja 8
2.6.1. Naučna opravdanost istraživanja 8
2.6.2. Društvena opravdanost istraživanja 8
2.7. Vremensko i prostorno određenje istraživanja 8
3. CYBER TEHNOLOGIJA 10
3.1. Historija cyber tehnologije 10
3.2. Cyber tehnologija u savremenom društvu 14
3.3. Identifikacija ranjivosti 16
3.4. Uloga cyber tehnologije u međunarodnim odnosima 21
3.4.1. Tehnološki i prostorni uticaji – promjena paradigme 24
3.5. Cyber ratovanje 26
3.5.1. Vrste i metode cyber ratovanja 28
3.5.2. Akteri u cyber prostoru 30
3.6. Strateška teorija cyber ratovanja 31
3.7. Dinamika cyber moći u međunarodnom sistemu 34
4. RUSIJA I UKRAJINA: HISTORIJA, DINAMIKA I IMPLIKACIJE 37
4.1. Međudržavni sukobi: nastanak i uzroci 37
4.2. Korijeni i dinamika sukoba 42
4.2.1. Pozadina sukoba 42
4.2.2. Trenutno stanje sukoba 45

4.3. Implikacije za međunarodnu sigurnost 49
4.4. Geopolitički aspekti sukoba 52
4.5. Uloga cyber tehnologije 55
5. STUDIJE SLUČAJA 65
Studija slučaja 1: Sputnik 65
Studija slučaja 2: AcidRain 67
DISKUSIJA 70
ZAKLJUČAK 72
BIBLIOGRAFIJA 75

SKRAĆENICE

BBS – Bulletin board system

CNA- Computer Network Attack

CND – Computer Network Defense

DARPA – Defense Advanced Resarch Projects Agency

ENIAC – The Electronic Numerical Integrator and Computer

EU – the European Union

IBM – The International Business Machines Corporation

ICANN - Internet Corporation for Assigned Names and Numbers

NATO – the North Atlantic Treaty Organization

NSF – The U.S. National Science Foundation

POPIS TABELA I SLIKA

Slika 1: Grafički prikaz globalnih trendova u međudržavnim sukobima i teritorijalnim sporovima, 1980-2020. .. 40
Slika 2: : Dominantne prijetnje uočene u kontekstu rata. Izvor:https://cyberconflicts.cyberpeaceinstitute.org/threats 59
Slika 3: Početna aproksimacija fizičkog naspram cyber napada. Izvor: https://cyberforumkyiv.org/A_Decade_in_the_Trenches_of_Cyberwarfare.pdf 61

UVOD

U međunarodnim odnosima, tehnološki napredak često ima dubok i kompleksan utjecaj na dinamiku sukoba i moći među državama. Suvremeno društvo sve više oslanja na cyber tehnologiju u gotovo svim aspektima života, što rezultira transformacijama u načinu na koji države komuniciraju, surađuju i suprotstavljaju se jedna drugoj. U ovom kontekstu, uloga cyber tehnologije u međunarodnim sukobima postaje sve značajnija, budući da je cyber prostor postao novo bojište za borbu za moć i utjecaj. Ovaj rad istražuje kako je duboka integracija cyber tehnologije u društvo i funkcije država transformirala međunarodne sukobe, donoseći sa sobom nove izazove i mogućnosti.

Prva hipoteza istražuje duboku globalnu integraciju cyber tehnologije u društvo i funkcije država. Tradicionalni oblici sukoba, poput ratovanja na kopnu, moru ili zraku, sada su nadopunjeni virtualnim sukobima u cyber prostoru. Ova transformacija omogućila je vanjskim subjektima, poput država, organizacija ili kriminalnih grupa, da iskoriste ranjivosti u digitalnoj infrastrukturi kako bi ostvarili svoje ciljeve. Time su se promijenili tradicionalni obrasci sukoba i moći, jer se borba sada odvija i na nevidljivim cyber frontovima, gdje se informacije i podaci mogu koristiti kao oružje.

Druga hipoteza istražuje evoluciju koncepta moći i utjecaja u kontekstu razvoja cyber tehnologije. Dok je ranije moć bila često mjerena kroz vojne resurse, teritorijalnu kontrolu ili ekonomske pokazatelje, danas se pojam moći širi na područje informacija, komunikacija i tehnološke dominacije. Cyber prostor omogućuje državama i drugim akterima da ostvare svoje ciljeve na suptilan i nekonvencionalan način, koristeći se taktikama poput hakerskih napada, dezinformacija i sabotiranja digitalne infrastrukture. Ova nova dinamika moći zahtijeva promjene u percepciji i strategiji država, jer se borba za utjecaj sve više seli iz tradicionalnih vojnih okvira u virtualni svijet.

Fokus istraživanja usmjeren je na konkretne primjere sukoba između Rusije i Ukrajine, koji su postali simboličan sukob između tradicionalnih i cyber tehnologija. Od izbijanja sukoba 2014. godine, cyber napadi postali su integralni dio ukrajinske krize, s obe strane koristeći cyber sredstva kako bi ostvarili svoje ciljeve. Ovaj sukob pruža bogat poligon za analizu utjecaja cyber tehnologije na međunarodne sukobe i geopolitičke dinamike. Kroz analizu historije cyber tehnologije, geopolitičkih faktora i konkretnih primjera sukoba, ovaj rad nastoji osvijetliti kompleksnu interakciju između tehnologije, moći i međunarodnih sukoba.

1. TEORIJSKE OSNOVE RADA

U današnjem sve više povezanom svijetu, cyber tehnologija je postala ključni faktor koji oblikuje dinamiku međudržavnih odnosa i sukoba. Ovaj magistarski rad istražuje duboko prožimanje cyber tehnologije s međunarodnom politikom i sigurnošću te kako je ta integracija utjecala na moćne dinamike među državama u međunarodnom sustavu. S obzirom na brzi razvoj cyber tehnologije i njezinu sveprisutnost u društvu i državnim strukturama, postavlja se ključno pitanje o utjecaju ove globalne digitalne transformacije na tradicionalne oblike sukoba i moći među državama. Kroz analizu suvremenih sukoba, kao i kroz proučavanje strategija korištenja cyber tehnologije u međunarodnim odnosima, ovaj rad će doprinijeti dubljem razumijevanju interakcije između cyber tehnologije i međudržavnih sukoba te njihovog utjecaja na globalnu sigurnost.

Prvi korak u istraživanju odnosi se na analizu historije cyber tehnologije, koja seže od pionirskih dana do današnjice. Proučavanje evolucije cyber tehnologije omogućuje razumijevanje njenog utjecaja na društvo i državne funkcije te kako je postala neizostavan dio suvremenog života. Poseban naglasak bit će stavljen na identifikaciju ranjivosti koje proizlaze iz sveprisutnosti cyber tehnologije u infrastrukturi modernih država. Analizom historijskih događaja i tehnoloških inovacija, rasvijetlit će se put kojim je cyber tehnologija prošla do svoje trenutne pozicije kao ključnog faktora u međunarodnim odnosima.

U drugom dijelu istraživanja fokus će biti usmjeren na konkretni sukob između Rusije i Ukrajine. Dubinska analiza povijesnih korijena ovog sukoba omogućit će razumijevanje dinamike sukoba te implikacija koje je ovaj sukob imao na međunarodnu sigurnost. Osim toga, istražit će se geopolitički aspekt sukoba, s posebnim naglaskom na ulogu cyber tehnologije u ovom kontekstu. Proučavanjem strategija koje su obje strane koristile u cyber domeni tijekom sukoba, bit će moguće sagledati kako cyber tehnologija mijenja tradicionalne obrasce međudržavnih sukoba.

Završni dio rada fokusirat će se na analizu konkretnih studija slučaja koje pružaju uvid u različite načine korištenja cyber tehnologije tijekom međunarodnih sukoba. Ovo će uključivati detaljne analize cyber napada, propagande i drugih oblika cyber aktivnosti koji su utjecali na tijek sukoba. Kroz proučavanje ovih studija slučaja, rad će dodatno produbiti razumijevanje specifičnih mehanizama i strategija koje se koriste u korištenju cyber tehnologije u međunarodnim sukobima te njihovog utjecaja na globalnu sigurnost.

2. METODOLOŠKI OKVIR RADA

2.1. Problem istraživanja

U ovom istraživanju se suočavamo s problemom duboke globalne integracije cyber tehnologije i njenog uticaja na dinamiku borbi za moć među državama u međunarodnom sistemu. Dok je cyber tehnologija postala neizostavan dio svakodnevnog života tokom proteklih trideset godina, njena sveprisutnost u društvu i državnim funkcijama donijela je brojne prednosti, ali i otvorila nove ranjivosti. Akteri poput obavještajnih organizacija, vojnih jedinica i sponzoriranih izvođača sve više koriste inherentne slabosti u cyber prostoru u svojim operacijama, koje sežu od krađe osjetljivih informacija do ciljanja infrastrukture i utjecanja na stanovništvo. Stoga, istraživanje se fokusira na analizu kako ova globalna digitalna transformacija utiče na dinamiku moći između država, istražujući kako se države koriste cyber tehnologijom u svojoj stalnoj potrazi za moći i utjecajem u međunarodnom sistemu, s posebnim fokusom na trenutačni sukob između Rusije i Ukrajine.

2.2. Predmet istraživanja

Predmet istraživanja se fokusira na sveprisutnost digitalne tehnologije i njezinu ulogu u međunarodnim sukobima. Cilj je razumjeti kako upotreba cyber tehnologije oblikuje dinamiku međunarodnih sukoba, posebno u vojne svrhe, kao i kako te tehnologije utječu na komunikaciju, obavještajne operacije, propagandu i druge aspekte međunarodnih sukoba. Dodatno, analizirat će se kako digitalna tehnologija mijenja tradicionalne obrasce međunarodnih sukoba te kako se mogu primijeniti strategije prevencije i rješavanja sukoba u digitalnom dobu. Elaborirajući, istraživanje će istražiti konkretne primjere cyber-napada, informativne operacije putem interneta, kao i međunarodne politike koje reguliraju upotrebu cyber-oružja i druge digitalne tehnologije u kontekstu međunarodnih sukoba.

2.2.1. Kategorijalno pojmovni sistem

Da bi se sadržaj ovog magistarskog rada što jasnije predočio, u nastavku su pobliže objašnjena značenja ključnih pojmova koji su inkorporirani u radu:

Cyber prostor – Globalno okruženje koje obuhvata sve međusobno povezane komunikacijske, informacijske tehnologije i druge elektroničke sustave, mreže i njihove podatke, uključujući one koji su odvojeni ili neovisni, a koji procesuiraju, skladište ili prenose podatke. Cyber prostor obuhvata mnogo više od samog Interneta ili zaštite informacijskih tehnoloških sistema. On je prostran i sveprisutan, obuhvatajući digitalne, informacijske tehnologije i operativne tehnologije, uključujući sisteme kontrole zračnog saobraćaja, medicinske sisteme za održavanje života, kontrolere fizičkih uređaja, industrijske kontrolne sisteme i nacionalne distribucijske mreže za vodu, plin i električnu energiju, često nazvane ključnom nacionalnom infrastrukturom (Ministry of Defence, 2022).

Cyber ratovanje – Vojni pokušaj postizanja strateške pobjede korištenjem skromnih sredstava za destabilizaciju infrastrukture države. Iako cyber rat ne uzrokuje nužno fizičku štetu, može privremeno zbuniti i frustrirati operatore vojnih sustava (Cartwright, 2010).

Cyber rizik – Rizik koji može biti definiran putem tri glavna faktora: utjecaj, koji ukazuje na potencijalnu štetu uzrokovanu određenim rizikom; prijetnja, koja ukazuje na vjerojatnost pojave određenog rizika; i ranjivost, koja ukazuje na prisutnost ili odsutnost slabosti koje bi mogle biti iskorištene (Biener, Eling i Wirfs, 2015).

Cyber tehnologija – Skup digitalnih tehnologija zasnovanih na novim medijima (uključujući virtualnu stvarnost, društvene mreže i multimediju), soft računarstvu[1], cloud računarstvu[2] i mobilnom računarstvu (Qu, 2011).

Geopolitika – Geopolitika se odnosi na proučavanje i praksu razumijevanja globalne politike kroz geografsku prizmu. Uključuje analizu geopolitičkog pejzaža svijeta koristeći geografske opise, metafore i obrasce, s ciljem stvaranja pojednostavljenih modela svijeta, koji se zatim koriste za informiranje o vanjskoj politici i sigurnosnom odlučivanju. Dodatno, geopolitika

[1] Soft računarstvo predstavlja najnoviji pristup tehnologijama računarstva koje su usmjerene na rješavanje problema koji su subjektivni, nesigurni ili kompleksni. Njegovi formalni modeli obuhvataju neuronske mreže, nejasnu logiku, genetske algoritme, među ostalima, čineći temeljne komponente umjetne inteligencije. Za razliku od hard računarstva, koje se oslanja na formalne logičke sustave poput predikatne ili propozicijske logike kako bi utvrdilo ishode unutar definiranih vremenskih okvira, soft računarstvo je sposobno rješavati probleme inherentno obdarene nepreciznošću, djelomičnom istinom i nesigurnošću. Osim toga, metodologije soft računarstva obično koriste induktivno zaključivanje, prioritizirajući prepoznavanje uzoraka i iterativne procese nad strogošću izračunavanja (Qu, 2011).

[2] Cloud computing je tehnološki napredak u isporuci računarskih funkcija gdje se potrebni resursi pružaju kao usluge od strane prodavatelja umjesto kao proizvodi. Korisnici pristupaju tim funkcijama putem pretplate na usluge koje nude pružatelji cloud računarstva, plaćajući samo za korištene resurse bez potrebe za detaljnim poznavanjem njihovih lokacija ili konfiguracija. Ova metoda omogućava efikasnu implementaciju različitih IT funkcija, slično kao korištenje električne mreže. Temeljne tehnologije uključene u cloud računarstvo su virtualizacija, usmjerena usluga, internet i centri podataka (Qu, 2011).

proučava kako oznake i koncepti oblikuju percepcije mjesta, zajednica i identiteta. Istražuje načine na koje se ove oznake koriste za definiranje političkih odnosa i dinamike moći na globalnoj razini, posebno tijekom razdoblja geopolitičkih rivaliteta poput Hladnog rata. Geopolitika nije samo domena država i vlada, također uključuje nevladine organizacije, privatne tvrtke i međunarodne institucije, kao i utjecaj novih medijskih tehnologija poput interneta na oblikovanje političkih narativa i mobiliziranje javne podrške (Dodds, 2007).

Geopolitička arhitektura - Pojam geopolitičke arhitekture koristi se kako bi opisao načine na koje države i organizacije izvan države pristupaju, upravljaju i reguliraju susret teritorija i tokova, uspostavljajući pri tome granice između unutrašnjosti/izvan, građanin/stranac i domaći/međunarodni. Na primjer, vlade ulažu velike napore u reguliranje granica jer one predstavljaju ulaznu/izlaznu tačku u nacionalni teritorij. Takve kontrole granica također postaju značajan element u demonstriranju efektivnog suvereniteta (Dodds, 2007).

Moć - Moć se odnosi na utjecaj koji se ostvaruje unutar društvenih interakcija, oblikujući sposobnost pojedinaca da određuju vlastite ishode. Ova ideja obuhvata dva osnovna aspekta: prvo, prirodu društvenih veza koje utječu na sposobnosti pojedinaca, i drugo, specifične karakteristike tih veza. Barnett i Duvall (2005) predstavljaju različite oblike moći unutar globalne arene. Predlažu sustav klasifikacije koji obuhvaća vrste poput obvezne moći koja uključuje izravnu dominaciju nad drugima, institucionalne moći koja podrazumijeva kontrolu nad udaljenim pojedincima, strukturne moći opisujući međusobno oblikovanje kapaciteta aktera, i produktivne moći koja se odnosi na stvaranje identiteta putem raspršenih društvenih interakcija (Barnett i Duvall, 2005).

2.3. Ciljevi istraživanja

Cilj ovog istraživanje jeste uvid u dinamiku između paradigme moći i sami utjecaj cyber tehnologije, kao sve više prisutnog domena u međudržavnim sukobima. Pored toga, analizom se nastoji doći do shvatanja implikacija cyber tehnologije i kako državne strukture mogu minimizirati utjecaj cyber tehnologije i cyber aktera.

2.3.1. Naučni cilj

Naučni ciljevi ovog istraživanja usredotočeni su na produbljivanje razumijevanja međusobne povezanosti između cyber tehnologije i međunarodnih sukoba. Kroz analizu historije, karakteristika i specifičnih primjera cyber aktivnosti, cilj je generirati nove spoznaje koje će unaprijediti teorijsko i empirijsko razumijevanje ovih fenomena. Ovim istraživanjem težimo razvoju teorijskih modela koji će pomoći u boljem razumijevanju dinamike cyber sukoba i pružiti osnovu za daljnje akademske analize i istraživanja.

2.3.2. Društveni cilj

Društveni ciljevi istraživanja fokusirani su na stvaranje temelja za razvoj informirane javne politike i strategija za prevenciju i rješavanje sukoba u digitalnom dobu. Očekuje se da će rezultati ovog istraživanja pružiti korisne uvide i preporuke za donositelje odluka, praktičare i političare u izradi politika i strategija koje će promicati sigurnost i stabilnost na globalnoj razini. Također, istraživanje će podržati razvoj novih pristupa i mehanizama za suočavanje s izazovima koje donosi sveprisutnost digitalne tehnologije u međunarodnim odnosima.

2.4. Sistem hipoteza

2.4.1. Generalna hipoteza

„Duboka globalna integracija cyber tehnologije u društvo i državne funkcije transformirala je međunarodne sukobe, pružajući vanjskim subjektima neviđenu sposobnost da se infiltriraju u procese donošenja odluka i implementacije strategija država.“

2.4.2. Posebne hipoteze

„Koncept moći evoluirao je s jednostavne materijalne mjere do kompleksne i izazovne za kvantifikaciju, reflektirajući utjecaj cyber tehnologije na dinamiku borbe za moć među državama.“

2.5. Način istraživanja

Metoda istraživanja koja će se primijeniti u ovom radu obuhvaća kombinaciju deskriptivne analize, analize slučaja i analize sadržaja kako bi se dublje istražio utjecaj cyber tehnologije na međunarodne sukobe. Kombinacija ovih metoda omogućit će sveobuhvatno istraživanje utjecaja cyber tehnologije na međunarodne sukobe i pružiti dublje razumijevanje ovog sve važnijeg aspekta suvremenih međunarodnih odnosa.

2.5.1. Deskriptivna analiza

Deskriptivna analiza će proučavati historiju i ključne događaje u razvoju cyber tehnologije kako bi se stvorio temeljni kontekst za razumijevanje njezine uloge u međunarodnim sukobima. Osim toga, analizirat će se karakteristike cyber tehnologije koje su relevantne za međunarodne sukobe, poput sposobnosti širenja dezinformacija ili izvođenja cyber napada.

2.5.2. Analiza (sadržaja) dokumenata

Analiza sadržaja će se provesti kroz pregled znanstvenih članaka, knjiga i drugih relevantnih izvora kako bi se prikupili podaci o utjecaju cyber tehnologije na međunarodne sukobe. Osim toga, bit će analizirani izvještaji sigurnosnih agencija, stručna mišljenja i analize koje se odnose na upotrebu cyber tehnologije u međunarodnim sukobima, pružajući dodatne uvide i perspektive o ovoj temi.

2.5.3. Analiza slučaja/ case study

Analiza slučaja će se fokusirati na prirodu sukoba između Rusije i Ukrajine, istražujući dinamiku sukoba i implikacije na međunarodnu sigurnost. Posebna pažnja bit će posvećena ulozi cyber tehnologije u ovom sukobu, analizirajući konkretne slučajeve cyber napada ili propagande. Ovo će uključivati istraživanje ciljeva, strategija i utjecaja cyber aktivnosti na tijek sukoba i međunarodne odnose.

2.6. Naučna i društvena opravdanost istraživanja

Naučna i društvena opravdanost ovog istraživanja su izuzetno važne zbog višestrukih razloga. S obzirom na rapidan razvoj cyber tehnologije i njezin sve značajniji utjecaj na međunarodne sukobe, postoji potreba za dubljim razumijevanjem ovog fenomena kako u znanstvenom, tako i u praktičnom smislu.

2.6.1. Naučna opravdanost istraživanja

Naučna opravdanost ovog istraživanja leži u potrebi za generiranjem novih spoznaja i uvida o složenoj interakciji između digitalne tehnologije i međunarodnih sukoba. Analiza historije, karakteristika i konkretnih primjera cyber aktivnosti pružit će osnovu za razvoj teorijskih i empirijskih modela koji će olakšati bolje razumijevanje ove dinamike. Osim toga, istraživanje će doprinijeti širenju znanja o mogućnostima i izazovima koje donosi digitalna era u kontekstu međunarodnih odnosa.

2.6.2. Društvena opravdanost istraživanja

Društvena opravdanost istraživanja je vidljiva u potrebi za stvaranjem informirane javne politike i strategija za prevenciju i rješavanje sukoba u digitalnom dobu. Uzimajući u obzir sveprisutnost digitalne tehnologije i njezin potencijalni utjecaj na međunarodnu stabilnost i sigurnost, važno je razviti nove pristupe i mehanizme za suočavanje s tim izazovima. Ovo istraživanje može poslužiti kao osnova za oblikovanje politika i strategija koje će pomoći u sprječavanju eskalacije sukoba, zaštititi digitalnu infrastrukturu i promicati sigurnost i stabilnost na globalnoj razini.

2.7. Vremensko i prostorno određenje istraživanja

Vremensko i prostorno određenje ovog istraživanja usredotočeno je na period prije i tijekom invazije Rusije na Ukrajinu, koja je započela 24. februara 2022. godine. Istraživanje će se temeljiti na događajima, trendovima i dinamici sukoba između Rusije i Ukrajine u navedenom razdoblju. Fokus će biti na analizi cyber tehnologije i njezine uloge u ovom specifičnom međunarodnom sukobu. Dok će se posebna pažnja posvetiti cyber aktivnostima

koje su se događale prije invazije, kao i tijekom samog sukoba, istraživanje će se također proširiti na druge aspekte sukoba između Rusije i Ukrajine kako bi se pružila sveobuhvatna slika o njihovom odnosu i utjecaju na međunarodne odnose.

3. CYBER TEHNOLOGIJA

Revolucija u cyber tehnologiji imala je globalni utjecaj koji nije sličan nijednom drugom izumu u modernoj historiji. Rasprostranjena, brzo evoluirajuća, i sve više integrirana u naše svakodnevne živote, dramatično je promijenila način na koji ljudi obavljaju poslove, komuniciraju, formiraju odnose u društvu, te vode konflikte. U samom procesu razvoja, cyber tehnologija je donijela mnoga obećanja i rizike, te postavila temeljna i neodgovorena pitanja o tome kako mijenja moć, politiku i društvene odnose uopće.

Brown (2020) definiše cyber tehnologiju kao sve ono što obuhvata direktno ili indirektno povezano s internetom, uključujući i uređaje koji su navodno izolovani od njega, ali koriste povezane računarske tehnologije. Iako ovo pruža određeni uvid u to šta cyber space obuhvata, fizička infrastruktura predstavlja samo jedan dio. Osim žičanih, rutera, uređaja i drugih materijalnih elemenata, cyber space također sadrži virtualne, upravljačke i socijalne elemente. Svaki od ovih interaktivnih dijelova utiče na to kako je cyber space struktuiran, korišten i upravljan, te se stoga mora uzeti u obzir u analizi.

3.1. Historija cyber tehnologije

Ziavras (/) u svom radu History of computation navodi da kroz vrijeme, elektronski računari su evoluirali kroz pet različitih generacija, pri čemu su napredak u osnovnoj tehnologiji bili glavni pokretač napretka. Od rudimentarnih oblika koji se nalaze u telefonskim centralama, skenerima u supermarketima i bankomatima, do sofisticiranijih verzija koje se koriste u osobnim računarima, naprednim mrežama, dizajnu aviona i prognozi vremena, elektronsko računanje postalo je neizostavno za različite aspekte savremenog života.

Prva generacija računara, prema Ziavrasu (/), obuhvatila je razdoblje od 1945. do 1955. Međutim, ranije u 1938. godini, engleski inženjer Charles Babbage dizajnirao je prvi mehanički digitalni računar. Nazvao ga je računar razlike i koristio ga je za rješavanje matematičkih problema, uključujući jednostavne diferencijalne jednačine. U njegovom radu pomogla mu je matematičarka Ada grofica Lovelace, koja je bila kći poznatog Lorda Byrona. Njih dvoje su doprinijeli razvoju matematičke teorije mehaničkih računalnih tehnologija, što je Babbagea inspiriralo da osmisli još ambiciozniji analitički stroj. Iako taj stroj nikada nije bio izgrađen, obuhvatio je mnoge principe rada računala koji su kasnije ponovno otkriveni s novijim modelima (Dilys i Atsushi, 1996).

Kasnih 1930-ih i ranih 40-ih godina, Dilys i Atsushi (1996) navode da barem tri odvojena nastojanja su učinjena da se elektroničkim sklopovima riješe problemi računanja, John Atanasoff, Britanska obavještajna služba i IBM. Od 1937. do 1941. godine, John Atanasoff, koji je predavao fiziku na Iowa State Collegeu i imao interes za opći problem brzog računanja, krenuo je u dizajniranje specijaliziranog uređaja koji bi mogao rješavati složene sustave linearnih jednačina. Atanasoff-Berry računalo, razvijeno uz značajan doprinos njegovog diplomskog studenta Clifforda Berryja, bilo je blizu, ako ne i potpuno operativno do 1941. godine. Do te godine, IBM, čije je tadašnje ekspertno znanje bilo u opremi za kartično tabuliranje, također je dizajnirao elektronički množitelj. Kasnih 1930-ih IBM je počeo surađivati s Wallaceom Eckertom s Columbia Universityja kako bi istražio kako se njihova oprema može koristiti u različite znanstvene svrhe. Postalo je jasno da bi elektronički množitelj znatno ubrzao vrste računanja koje je Eckert koristio.

Početak moderne ere računarstva može se pratiti do razdoblja Drugog svjetskog rata, kada su se ključni razvoji događali i na istočnoj i na zapadnoj strani Atlantika, kako navode Wilson i Campbell-Kelly (2020). U Engleskoj, revolucionarni računar Colossus koristio se za dešifriranje njemačkih vojnih šifri, dok je u Sjedinjenim Američkim Državama značajnu ulogu imao ENIAC (Ziavras, /; Wilson i Campbell-Kelly, 2020). Prije toga, poljski razbijači šifri, predvođeni Marianom Rejewskim 1932. godine, uspjeli su provaliti u Enigma mašine koje su koristili Nijemci. No, s eskalacijom rata, Enigma šifre postale su sve složenije, što je rezultiralo značajnim gubicima. Tek je Alan Turing i njegov tim provalnika šifri u Bletchley Parku, Engleska, uz pomoć Bomba mašine, uspio provaliti te šifre. Nadalje, Lorenzova šifrirajuća mašina, koju je koristio Hitler i njemačke vojne vođe, predstavljala je još veći izazov. Kao odgovor na to, pokrenut je tajni razvoj računara Colossus u Bletchley Parku kako bi se riješio taj šifrirani kod. Naporima Turinga i njegovih kolega skratio se period rata za do dvije godine, naglašavajući monumentalni utjecaj ranih računalnih napredaka u vojnim obavještajnim operacijama (Wilson i Campbell-Kelly, 2020).

Presper Eckert i John Mauchly su slavljeni kao vizionarski umovi iza konstrukcije ENIAC-a, revolucionarnog Elektronskog Numeričkog Integratora i Računara. Njihova suradnja rezultirala je stvaranjem prvog digitalnog, općenito namijenjenog, elektroničkog računara, često nazivanog Divovski Mozak (McCartney, 1999). ENIAC je predstavljao monumentalni korak naprijed u tehnologiji računarstva, hvaleći neviđenu razinu veličine i složenosti za to doba. Sastavljen od četrdeset devet stopa visokih ormara ispunjenih gotovo 18,000

vakuumskih cijevi i složenih žica, ENIAC je bio tehničko čudo (Ziavras, /). Njegova ogromna veličina i računarska moć oduševila je znanstvenike i inženjere, potičući revoluciju u području računarstva (McCartney, 1999).

Inicialno osmišljen kao alat za vojne svrhe, primarni cilj ENIAC-a bio je izračunavanje putanja za artiljerijske topove tokom Drugog svjetskog rata. Međutim, do vremena kada je ENIAC završen, rat je već bio završen, čime je njegova originalna svrha postala zastarjela. Unatoč ovom neuspjehu, ENIAC je pronašao novu svrhu u području znanstvenih istraživanja i tehnološkog napretka. Njegove sposobnosti su brzo prepoznate kao imajući dalekosežni potencijal izvan njegove početne vojne primjene (McCartney, 1999).

Godine 1945. tijekom svojih prvih testnih vožnji, ENIAC je krenuo u novu misiju: provođenje milijuna diskretnih izračunavanja povezanih s tajnim studijama termonuklearnih lančanih reakcija. Predvodili su ga znanstvenici Nicholas Metropolis i Stan Frankel iz Los Alamos Scientific Laboratoryja, gdje je ENIAC-ova računarska sposobnost stavljena na test u pionirskom istraživanju razvoja vodonične bombe. To je označilo značajan preokret za ENIAC, pokazujući njegovu prilagodljivost i svestranost u rješavanju složenih znanstvenih izazova izvan njegovih prvotnih dizajnerskih specifikacija (Dilys i Atsushi, 1996).

Nakon završetka Drugog svjetskog rata i prekida mnogih vojnih projekata, ENIAC se suočio s neizvjesnom budućnošću. Međutim, njegov potencijal u visokobrzinskom računanju i neprocjenjiv doprinos znanstvenom istraživanju osigurali su daljnju podršku federalne vlade. Uloga ENIAC-a u unapređenju računarskih sposobnosti, posebno u kontekstu razvoja nuklearnog oružja, učvrstila je njegovo mjesto u povijesti kao pionirskog tehnološkog inovacijskog dostignuća. Nadalje, njegov je utjecaj prešao daleko izvan vojnih primjena, s njegovom vrijednošću prepoznatom u različitim sektorima za rješavanje složenih problema i poticanje inovacija (Dilys i Atsushi, 1996).

Druga generacija računarstva, koja se protezala od 1955. do 1965. godine, vidjela je revolucionarni prelazak s vakuumskih cijevi na tranzistore (Ziavras, /; Adda247, 2024). Ovaj napredak postao je moguć zahvaljujući izumu tranzistora 1947. godine od strane Johna Bardeena, Waltera Brattaina i Williama Shockleya. Tranzistori, za razliku od vakuumskih cijevi, bili su brži, efikasniji i manji po veličini, što je omogućilo stvaranje manjih, ali moćnijih računara. Proizvođači računara pedesetih godina proizvodili su prije svega mašine za obradu podataka, umjesto računara za matematičke zadatke. Međutim, značajni računari

poput IBM-a 7090, DEC PDP-1 i Control Data Corporation (CDC) 1604 bili su među prvima koji su uključili tranzistore (Ziavras, /).

Treća generacija, u periodu od 1965- 1974, je zabilježila značajanu prekretnicu u cyber tehnologiji (Ziavras, /). U kasnim 1960-ima, Ministarstvo odbrane Sjedinjenih Američkih Država predvodilo je revolucionarnu inicijativu koja je transformirala globalnu komunikaciju: program ARPANET (Brown, 2020). Finansiranje DARPA-e poguralo je projekt naprijed, vođeno potrebom za otpornom mrežom sposobnom za brzo širenje informacija preko ogromnih udaljenosti, čak i usred kaosa potencijalnog uništenja čvorova (Defense Advanced Research Projects Agency, 1981). Ovaj ambiciozni poduhvat, iako nastao iz vojne nužde, postavilo je temelje za ono što danas prepoznajemo kao internet, povezujući računare na različitim istraživačkim institucijama i postavljajući temelje za globalnu mrežu međusobno povezanih uređaja.

Ciljevi ARPANET-a bili su vizionarski i praktični, odražavajući duboko razumijevanje potencijala mrežnog računarstva (Defense Advanced Research Projects Agency, 1981). Dalje od samo povezivanja računara, program je težio poticanju suradnje i inovacija omogućavajući dijeljenje resursa među istraživačkim centrima. Kroz zajedničko iskorištavanje ekspertize i resursa, ARPANET je imao za cilj ubrzati razvoj tehnologija mreža, otvarajući put za buduće napretke u digitalnoj komunikaciji. Ovaj naglasak na suradnji i međusobnoj koristi naglašavao je značaj ARPANET-a ne samo kao tehnološkog čuda, već i kao katalizatora za interdisciplinarnu suradnju.

Posljedice ARPANET-a premašile su njegovo vojno podrijetlo, preoblikujući komunikacijske pejzaže u javnom i privatnom sektoru širom svijeta. Poput transformacijskih izuma ranijih razdoblja, poput telefona i tiskarskog stroja, ARPANET je otvorio novo doba međusobne povezanosti, temeljno mijenjajući način razmjene i pristupa informacijama. Njegovo trajno naslijeđe služi kao dokaz moći inovacija i suradnje u vođenju napretka i oblikovanju tijeka ljudske historije (Brown, 2020).

Period četvrte generacije računara trajao je od 1971. do 1980. godine. Računari četvrte generacije koristili su integrisane sklopove vrlo velike skale. Računari četvrte generacije postali su moćniji, kompaktniji, pouzdaniji i pristupačniji. Kao rezultat toga, došlo je do revolucije ličnih računara. U ovoj generaciji korištena su vremenska dijeljenja, mreže u realnom vremenu i distribuirani operativni sistemi (Business Bliss Consultants FZE, 2018).

Razvojem personalnih računara i osnivanjem ARPANET programa, koji je je služio kao primarni korisnički interfejs tijekom 1970-ih i 1980-ih, uspostavljen je temelj za nastanak Svjetske mreže, poznate kao *Web* ili *World Wide Web*. Tim Berners-Lee, krajem 1980-ih i početkom 1990-ih, je iskoristio infrastrukturu i protokole ARPANET-a kako bi stvorio sustav za pristup i dijeljenje informacija putem hiperlinkova, što je dovelo do rođenja Web-a kakav ga danas poznajemo (Brown, 2020).

Kako su oprema povezana s cyberom postajala brža, manja i jeftinija, internet se brzo proširio. Ovi napretci postavili su temelje za sljedeći korak naprijed: stvaranje korisničkog sadržaja. Ovaj korak, često nazvan Web 2.0, dao je cyber akterima moć da razvijaju i dijele vlastite informacije, slike, umjetnost i druge kreacije na načine koji su prije bili nemogući. Iako je stvaranje korisničkog sadržaja postojalo od vremena sistema za buletine 1980-ih, ti su sajtovi uglavnom bili domena računarskih naučnika i drugih tehnički vještih ljudi (Shah, 2016). Međutim, počevši od sredine 1990-ih, filozofski i tehnički razvoji kombinirali su se kako bi stvaranje korisničkog sadržaja učinili dostupnijim i privlačnijim drugima (Obar i Wildman, 2015). Kao rezultat toga, kolaborativne web aplikacije brzo su rasle u popularnosti i dostupnosti jer su ljudi bili privučeni prilikom da komuniciraju s drugima širom svijeta i pristupe globalnoj pozornici (Shah, 2016). Ovo je ubrzano još više s javnim uvođenjem Facebooka i Twittera 2006. Godine (Jenkins, 2013; Obar i Wildman, 2015).

3.2. Cyber tehnologija u savremenom društvu

Sve veće oslanjanje na cyber tehnologiju za svakodnevne funkcije postalo je važno ne samo u privatnom životu ljudi, već obuhvata gotovo svaki aspekt današnjeg društva. Iako pristup i korištenje cyber tehnologije ovise o socioekonomskim i političkim faktorima te nisu jednaki širom svijeta ili unutar država, tehnologija je ipak postala ključan dio života za većinu svjetske populacije u posljednjih četrdeset godina.

Različiti koncepti poput društva znanja, informacijskog društva, mrežnog društva i informacijskog kapitalizma predmet su intenzivnog istraživanja u suvremenoj sociologiji kao odraz promišljanja o suštini današnjeg društva i važnosti tehnologije, informacija, komunikacije i suradnje unutar njega (Sasvari, 2012). Sveprisutna upotreba pametnih telefona, razvoj umjetne inteligencije i mogućnost analize podataka doveli su do opsežne

primjene cyber tehnologije od strane malicioznih aktera koji koriste državne i globalne resurse za promicanje svojih ideologija i pokušaje narušavanja državnih infrastruktura.

U kontekstu gdje su podaci i informacije postali sve važniji, nije iznenađujuće što su razvoj i primjena vještačke inteligencije (AI) dobili zamah u različitim diskursima o međunarodnim sukobima u cyber prostoru. Tehnologije AI-a, poput mašinskog učenja, obrade prirodnog jezika, kvantnog računarstva i neuronskih mreža, pružaju vojnim i obavještajnim agencijama nove operativne alate za predviđanje i suzbijanje prijetnji, kao i za provođenje ofenzivnih operacija u cyber prostoru. Također, operativno preplitanje tehnologija AI-a u cyber prostoru dodatno zamagljuje već kontroverzne granice između obrane i napada u cyber prostoru, dok istovremeno izaziva razlikovanje između cyber sukoba i informacijskih operacija. Pored otvaranja novih operativnih sredina, usvajanje AI-enhanced cyber sposobnosti također predstavlja važnu stratešku imovinu za države, usklađujući se s širim geopolitičkim rivalitetima, naporima odvraćanja, strategijama sigurnosti i narativima o digitalnom suverenitetu u globalnoj utrci za usvajanje ovih tehnologija (Cristiano i sur., 2023)

Kedzie (1997) tvrdi da tehnologija stvara sukobe na različite načine i u različitim fazama; tokom početnih postupaka i planiranja, sporovi oko regulative, operativnih postupaka, pravila i normi te pitanja privatnosti i kontrole. Dodaje da se sa napretkom tehnologije koncept sukoba proširio izvan lokalnih lokacija ili osobnih interakcija licem u lice. Novi društveni sukobi pojavljuju se sa pojavom i napretkom nove tehnologije. Ti sukobi mogu biti, na primjer, zbog kršenja kolektivne svijesti, poput testiranja ili korištenja vojnih oružja u suprotnosti s ljudskim pravima i međunarodnim pravom (Kedzie, 1997). Adibifar (2016) smatra da neujednačeni razvoj tehnologije i razlike u tehnološkoj sofisticiranosti između nacija također će rezultirati sukobima. Na primjer, neke nacije mogu smatrati druge koloniziranom silom i tražiti moć da ih izazovu, ili tražiti moć kako bi se takmičile na svjetskoj sceni. Neke nacije opremaju se tehnologijom kako bi odbile bilo kakve vanjske i unutrašnje rizike koji bi mogli ugroziti njihov status quo. Promjene u tehnologiji i nejasnoće koje prate dovode do nesklada u odnosima među grupama u društvenoj strukturi. Jedan od efekata dijalektičke promjene u tehnologiji u našim savremenim društvima je ljudska otuđenost. Ovaj ozbiljan društveni trošak je primarni proizvod nepravednog ekonomskog sistema (Adibifar, 2016).

U svom zaključku, Bellasio i Silfversten (2020) naglašavaju da su duboka neizvjesnost i razvoj tehnoloških i cyber prijetnji ključne odlike budućeg geostrateškog okruženja. Ovi novi

izazovi stvaraju strukturalni nedostatak za profesionalce u cyber sigurnosti i odbrani, kao i za institucije i zajednice koje ih štite, dajući prednost napadačima nad odbrambenim mehanizmima. Povećanje svijesti o mogućem razvoju cyber prijetnji u sljedećoj deceniji moglo bi olakšati anticipaciju prijetnji i koordinaciju pravovremenih i efikasnih odgovora na buduće izazove. U nastavku ovog rada, istražićemo važnost cyber prostora, efekte i aktere cyber ratovanja, kao i geopolitičke implikacije, s ciljem boljeg razumijevanja navedenih neizvjesnosti prema perspektivi navedenih autora.

3.3. Identifikacija ranjivosti

Ustaljena integracija cyber tehnologije u savremene državne strukture otvorila je niz ranjivosti koje se mogu pripisati nekoliko inherentnih karakteristika ove tehnologije. Ove povezane karakteristike obuhvataju brzu evoluciju cyber tehnologije, inherentne teškoće u otkrivanju i pripisivanju upada, kao i sporost mehanizama odgovornosti (Brown, 2020). Sve zajedno, ovi elementi stvaraju okruženje koje obiluje prilikama za aktere koji posjeduju čak i rudimentarne sposobnosti da ostvare značajne efekte s minimalnom brigom o mogućim posljedicama.

Neprekidni napredak cyber tehnologije, zajedno sa ljudskom greškom, namjernim dizajnerskim nedostacima i složenom prirodom rezultirajućih sistema, stvara brojne ranjivosti, kako poznate tako i nepredvidive. Iako neki naučnici tvrde da se ove ranjivosti mogu efikasno upravljati, time postavljajući cyber prostor kao defanzivno dominantan domen, prevladavajući konsenzus naginje efikasnosti ofanzivnih akcija (Rinear, 2015: 686-687; Singer i Friedman, 2014). Imajući u vidu proširivanje opsega, raznovrsne primjene, dinamične karakteristike i konstantnu evoluciju cyber tehnologije, zajedno sa njenom otvorenom arhitekturom i infrastrukturom koja se oslanja na ljude, neizbježno je da će ranjivosti i dalje opstajati.

U sljedećem dijelu rada prikazat ćemo ključne ranjivosti, prouzrokovane sve većom integracijom cyber tehnologije, u sferama detekcije, društva, ekonomije, vlade i geopolitike.

a) Detekcija

Detekcija u cyber prostoru predstavlja značajan izazov, posebno zbog složenosti i širokog spektra upotrebe cyber tehnologije. Cyber prostor karakterizira brza evolucija tehnologije, što

omogućava zlonamjernim akterima da djeluju neprimjetno unutar kompleksnosti internet aktivnosti. Ovaj kontekst omogućava napadačima da neprimjetno provode različite zlonamjerne aktivnosti, uključujući krađu podataka, distribuciju virusa i ometanje normalnog funkcioniranja sistema (Kello, 2017). Tokom ovog perioda, oni mogu izvršavati razne zlonamjerne aktivnosti, uključujući krađu osjetljivih informacija, implementaciju virusa, nanos štete, ometanje operacija i nadgledanje povjerljivih aktivnosti koje su pretpostavljene sigurnim (Brown, 2020). Također, ranjivosti u lancu snabdijevanja cyber tehnologije pružaju dodatne mogućnosti za neovlaštene pristupe i zaobilazak tradicionalnih sigurnosnih mjera (The Economist, 2016). Čak i kada se otkriju takve intruzije, uklanjanje naprednih malicioznih programa može biti dugotrajan process (Fox-Brewster, 2017; Falliere i sur., 2011).

Poteškoće u detekciji dodatno se produbljuju kada se uzmu u obzir neopipljive posljedice cyber napada. Organizacije koje su meta cyber napada često se suočavaju s izazovom u procjeni stvarne štete, koja može uključivati gubitak reputacije, smanjenje produktivnosti i narušavanje poslovnih procesa (Council of Economic Advisors, 2018). Identifikacija i kažnjavanje zlonamjernih aktera također su kompleksni procesi. Iako su stručnjaci za cyber sigurnost sve bolji u atribuciji, zlonamjerni akteri koriste razne taktike kako bi izbjegli otkrivanje, često se koristeći lažnim tragovima i posrednicima (Symantec Corp., 2018; Rid i Buchanan, 2015). Čak i kada se identificiraju, pravni i jurisdikcijski izazovi otežavaju procese gonjenja i odgovornosti, često ostavljajući napadače nekažnjenima (Grimes, 2016).

Na međunarodnom nivou, nedostatak sveobuhvatnog pravnog okvira dodatno komplicira suočavanje s cyber prijetnjama. Iako se međunarodno pravo teoretski primjenjuje na cyber prostor, praktična primjena ostaje izazovna, s postojećim pravnim okvirima često nedovoljnim za suočavanje s novonastalim prijetnjama (Schmitt, 2015; UN GGE, 2013). Složenost međunarodnog prava stvara fragmentiran pravni okvir koji olakšava zloupotrebu cyber tehnologije od strane zlonamjernih aktera.

b) Društvo

Pored fizičkih rizika, cyber tehnologija ima značajne implikacije na društvo. Prvo, socijalno inženjerstvo iskorištava urođenu podložnost pojedinaca unutar cyber sistema za manipulaciju (Smith, 2019). Veliki broj aktera u cyber prostoru koriste različite tehnike poput ubjeđivanja, prijetnji i lažne bliskosti kako bi pristupili osjetljivim informacijama ili kompromitovali

sigurne sisteme. Ova manipulacija iskorištava ljudski element isprepletan s tehnološkom infrastrukturom, čineći je podložnom infiltraciji (Brown, 2020).

Drugo, sveprisutna prisutnost društvenih medija globalno pojačava dosega aktera koji žele manipulisati društvenim narativima. Iako društvene mreže podstiču povezanost, njihovi algoritmi nehotice olakšavaju širenje dezinformacija i propagande. Osim toga, nedostatak rigoroznih procesa provjere sadržaja na mrežama umanjuje vjerodostojnost tradicionalnih medija, pogoršavajući društvene podjele i podstičući nepovjerenje (Brown, 2020).

Treće, tenzije proizlaze iz kontrole i korištenja tehnologije od strane korporativnih i vladinih entiteta. Brige u vezi s praksama online prikupljanja podataka od strane kompanija i programa nadzora vlade podižu pitanja privatnosti i slobode govora (Steiner, 2018). Brown (2020) navodi da javna reakcija protiv ovih praksi, potaknuta dezinformacijama, može podrivati napore obavještajnih i pravnih organa, dodatno narušavajući društvenu koheziju.

Na samom kraju, integracija cyber tehnologije u ekonomiju utječe na finansijsko blagostanje pojedinaca i pogoršava postojeće društvene razlike (Muro i sur., 2019). Automatizacija i tehnološki progres izazivaju dislokaciju radne snage, što rezultira povećanom nezaposlenošću i ekonomskom nestabilnošću. Ove promjene na tržištu rada potiču političke podjele i društvene napetosti, posebno u kontekstu imigracije i obrazovne reforme, jer se određene segmente populacije percipira kao marginalizirane i isključene iz ekonomskih prilika (Muro i sur., 2019).

c) Ekonomija

U ekonomskoj sferi, jedna od glavnih zabrinutosti i ranjivosti leži u oblasti cyber napada i krađe podataka, koje predstavljaju značajne prijetnje ekonomskoj stabilnosti i rastu (Brown, 2020). Prema Lewisu (2018), ekonomska šteta cyber napada se kreće od desetina milijardi do triliona dolara godišnje, s tendencijom rasta tokom vremena. Posljedice se protežu izvan samih finansijskih gubitaka, budući da ovi incidenti imaju potencijal da poremete kritične infrastrukture i izazovu krize slične finansijskom padu 2008. godine. Osim toga, špijunaža i krađa intelektualne svojine dodatno kompliciraju ekonomske posljedice korištenja cyber tehnologije. Međutim, potpuna procjena ekonomskog utjecaja ovih aktivnosti izaziva izazove, uključujući nedovoljno prijavljivanje, tajnu prirodu takvih operacija i složenost u izračunavanju neizravnih troškova. Unatoč inherentnim poteškoćama u kvantifikaciji, jasno

je da ovi troškovi imaju značajnu težinu i pridonose općoj ekonomskoj ranjivosti koju stvara korištenje cyber tehnologije (Mee i Schuermann, 2018).

Još jedna dimenzija ekonomske ranjivosti, naglašena od strane Brown (2020) proizlazi iz direktnih troškova povezanih s nacionalnim i korporativnim ulaganjima u cyber sigurnost. Bez obzira na značajne troškove za jačanje odbrane od cyber napada i usklađivanje s regulatornim zahtjevima, upornost cyber prijetnji ostaje nepromijenjena. Ovaj postojani pejzaž prijetnji zahtijeva stalna ulaganja u mjere cyber sigurnosti, dodatno opterećujući ekonomske resurse i otpornost (Brown, 2020).

Ove ranjivosti se manifestiraju u različitim sektorima koji su ključni za ekonomski prosperitet razvijenih zemalja, uključujući berze, finansijske institucije, industriju i rastuću ekonomiju dijeljenja (Brown, 2020). Međusobna povezanost ovih sektora pojačava potencijalne ripple efekte cyber incidenata, naglašavajući imperativ za proaktivne mjere radi ublažavanja ekonomskih rizika povezanih s cyber tehnologijom (Council on Foreign Relations, 2018).

d) Vladin sektor

Vlade imaju ključnu ulogu u suočavanju s višeslojnim izazovima koje postavljaju cyber ranjivosti kako na domaćem tako i na međunarodnom nivou. Na nacionalnom nivou, vlade su zadužene za zaštitu kritične infrastrukture, osiguravanje ekonomske stabilnosti i zaštitu društvenog blagostanja usred pejzaža stalno evoluirajućih cyber prijetnji (Brown, 2020). Ova odgovornost obuhvata ne samo vanjske izazove već i interne ranjivosti inherentne u vladinim strukturama. Na primjer, simulacija vježbe usmjerene na cyber napad na električnu mrežu u Baltimoreu otkrila je složenost prevazilaženja pravnih, regulatornih, operativnih i proceduralnih prepreka, ističući važnost efikasnih upravljačkih okvira (Intelligence and National Security Alliance, 2018). Saradnja između vlada i privatnog sektora je ključna u suočavanju sa cyber ranjivostima, uz neophodnost povjerenja i dijeljenja informacija radi efikasnog reagovanja i oporavka, pri čemu birokratski procesi i regulatorni okviri značajno utiču na sposobnost vlade u suočavanju sa cyber prijetnjama (Brown, 2020).

Na međunarodnom nivou, cyber ranjivosti su postavile fundamentalna pitanja o mjerenju moći. Cyberspace predstavlja domen gdje tradicionalne vojne metrike možda ne mogu adekvatno uhvatiti sposobnosti, što otežava objektivnu procjenu i upravljanje dinamikom moći (Eriksson, 2007; Inkster, 2018; Venables, Shaikh i Shuttleworth, 2017). Osim toga, međusobno povezan karakter cyberspacea sa različitim komponentama država pojačava

uticaj cyber prijetnji na ekonomske, društvene, infrastrukturne i vladine sektore, rezultirajući u ekonomskim rizicima, ubrzavanju tehnološkog napretka zlonamjernih aktera, te postaje značajan izazov za donosioce politika. Proliferacija dezinformacija dodatno kompleksira procese donošenja odluka za vladine lidere, budući da je sve izazovnije razgraničiti istinu od fikcije, posebno imajući u vidu mogućnost da lideri budu pod utjecajem vlastitih izvora informacija i pristranosti. Naprotiv, umjesto da smanji prisustvo lažnih informacija, birokratski procesi nehotice mogu pojačati dezinformacije, čime se narušava efikasnost upravljanja (Brown, 2020).

e) Geopolitika

Geopolitički problemi u cyber prostoru sve više se prepoznaju kao ključni dijelovi modernih dinamika moći, uključujući ne samo države već i pojedince te različite subjekte poput poslovnih poduzeća, neprofitnih organizacija, kao i zlonamjernih aktera poput kriminalaca i terorista. Diskusija o geopolitičkim pitanjima sada je prešla s fizičkog područja na cyberspace. Sheldon (2014) opisao je promjenu geopolitičkih problema kao rezultat prioritetizacije nacionalnih interesa u državama u cyberspaceu kao dijelu njenog teritorija. Sheldon, s druge strane, tvrdi da, osim nevidljivog virtualnog svijeta, sukobi u virtualnom prostoru imaju posljedice i u fizičkom svijetu (Sheldon, 2014). Geopolitička pitanja sada se moraju tumačiti ne samo fizički, već i digitalno. Geopolitika više ne raspravlja samo o odnosima između regija, politike i ekonomskih instrumenata u razvoju regionalnih investicija. Geopolitička osporavanja i takmičenja za hegemoniju u nekom području, s druge strane, i dalje igraju važnu ulogu u geopolitičkim studijama (Ramadhan, 2021). Geopolitički problem države je što je cyberspace region bez granica (Sheldon, 2014). Kao rezultat toga, geopolitička stabilnost države u cyber prostoru mora uzeti u obzir kakav oblik upravljanja može održati njene sigurnosne interese u svijetu bez granica (Ramadhan, 2021).

Franklin D. Kramer (2009) smatra da je ključno da se razmatra da li se cyber prostor može kvalificirati kao domen, slično kao kopno, more, zrak i svemir, koji su redovno analizirani u geopolitičkom diskursu. Uspoređivanje cyber prostora s globalnim zajedničkim resursima sugerira njegovu analogiju s uspostavljenim domenima te ističe njihove sličnosti. Međutim, važno je da politički akteri shvate da sama klasifikacija kao domena ne donosi inherentna prava ili obaveze, jer sami status cyber prostora kao domena mora biti jasno definiran i propisan (Kramer, 2009).

Također, Kramer (2009) navodi da se istražuje tema postizanja dominacije u cyber prostoru. Za razliku od domena kao što su mora, zrak i svemir, gdje se vojna prevlast može tražiti, postizanje dominacije u cyber prostoru izgleda kao izazovan zadatak. Cyber prostor dijeli karakteristike s kopnenim ratovanjem, uključujući raznolikost aktera, niske prepreke za ulazak i obilne mogućnosti za prikrivanje. Dok najmoćnije svjetske mornarice posjeduju ograničen broj brodova i satelita, cyber prostor je domaćin milijardama korisnika s nebrojenim mrežnim vezama. Relativno niski troškovi ulaska u cyber prostor dodatno otežavaju napore ka postizanju dominacije (Kramer, 2009).

U zaključku, Emily B. Bordelon (2016) implicira da pojava cyber prostora kao nove arene zahtijeva pažnju donositelja politika, što zahtijeva integraciju cyber aktivnosti u geopolitičke okvire, naposljetku služeći kao osnovni okvir za sveobuhvatno razumijevanje prijetnji i izradu strategija koje mogu adresirati i fizičke i virtualne aspekte cyber prijetnji. Nakon toga, države bi trebale primijeniti dvostruku strategiju odvraćanja koja uključuje kažnjavanje i negiranje, adresirajući prijetnje od državnih i nedržavnih aktera putem ofenzivnih i defanzivnih mjera. Ovaj lokalni pristup je ključan za sve države, uz međunarodnu strategiju koja će unaprijediti legitimnost domaćih sistema i ojačati istrage nakon napada. Suradnja među državama u razumijevanju cyber prijetnji i suradnja nakon napada pomaže u hvatanju počinitelja, čime se na kraju jačaju cyber sigurnosne strategije država (Bordelon, 2016).

3.4. Uloga cyber tehnologije u međunarodnim odnosima

Kao što smo već spomenuli, cyber tehnologija je zastupljena u svakom aspektu savremenog društva, a međunarodni odnosi nisu nikakav izuzetak. Ova tehnološka revolucija temeljno je promijenila načine komunikacije između država, olakšavajući širenje ideja i informacija, te doprinoseći protoku kapitala, roba i ljudi preko granica. Kroz povijest, cyber tehnologija kontinuirano je imala značajan utjecaj na globalne geopolitičke strategije, ekonomske strukture, sigurnosne paradigme i kulturne razmjene, kontinuirano oblikujući operativni okvir globalnog sistema, uključene aktere i njihove međusobne interakcije (Albakjaji i Almarzoqi, 2023). Također, Monika Szkarłat i Katarzyna Mojska (2016) naglašavaju da tehnološki napredak dovodi do redistribucije moći u međunarodnom okruženju, promoviše promjene u njegovoj strukturi, oblikuje veze među ključnim učesnicima međunarodnih odnosa i predstavlja izvor povećanog opsega, intenziteta i efikasnosti transgraničnih aktivnosti. Utjecaj tehnološkog faktora na savremene međunarodne odnose manifestuje se u različitim

sferama društvenog života, kao i u operativnim mehanizmima međunarodnih odnosa, uključujući: „procese institucionalizacije i upravljanja međunarodnim okruženjem, komunikaciju, saradnju i sukobe između nacija“ (Szkarłat i Mojska, 2016:10).

Korištenje cyber tehnologije igra ključnu ulogu u oblikovanju dinamike ravnoteže moći među suverenim državama. Pružajući alternativne kanale za interakciju između zemalja s različitim političkim stavovima, time značajno efektuje na ravnotežu moći među njima (Malik, 2016). Napredak u tehnologiji doprinosi preoblikovanju moći unutar globalnog okvira, obuhvaćajući njezinu prirodu, distribuciju, porijeklo i manifestacije. Znanstvene i tehnološke sposobnosti, zajedno s rezervoarom znanja i informacija koji čini intelektualni kapital, čiji kvalitet se ogleda u razini inovacija, izranjaju kao ključni elementi moći. Važno je napomenuti da su ovi resursi sve više u vlasništvu entiteta izvan nacionalnih vlada, što dovodi do toga da ne-državni akteri postaju nositelji moći u međunarodnoj areni, izazivajući tradicionalnu dominaciju država u ovom području (Szkarłat i Mojska, 2016). Nadovezujući se na ovu tvrdnju, Amitav Mallik (2016) ukazuje na činjenicu da je eksponencijalni tehnološki napredak omogućio čak i pojedincima ili malim grupama da predstavljaju značajne prijetnje potpuno razvijenim državnim aparatima, predstavljajući odstupanje od strukturiranog, vladom kontroliranog međunarodnog okruženja.

Jedan od ključnih aspekata koji ističe vezu između tehnologije i državne moći leži u području informacijske tehnologije i njenog utjecaja na komunikaciju između država. Albakjaji i Almarzoqi (2023) ističu značaj stilova vođenja, domaćih političkih agendi i tehnoloških sposobnosti u oblikovanju globalnih poslova. Informacijska tehnologija omogućila je bezprijekornu komunikaciju između zemalja, pojačavajući njihovu sposobnost međusobnog djelovanja i utjecaja, u cilju afirmisanja svojih interesa unutar globalne arene. Osim toga, tehnologija služi kao ključni odrednik moći unutar kalkulacije međunarodnih odnosa. Mallik (2016) tvrdi da je tehnološko znanje postalo neophodno za održavanje diplomatske učinkovitosti i snalaženje u globalnim izazovima. Dok se diplomtija prilagođava zahtjevima elektronskog medija, karakteriziranog trenutnom komunikacijom i difuzijom informacija, tehnologija preuzima središnju ulogu u državništvu.

Pored promjena u tradicionalnim dinamikama moći, tehnologija također utječe na kapacitete soft moći nacija. Mallik (2016) istražuje kako upravljanje globalnim javnim dobrima, primjerice Svjetskom mrežom (World Wide Web), postaje ključni alat soft moći u 21. stoljeću. Nye (2010) navodi da u cyber prostoru, informacijski alati djeluju kao moćni

sredstva za generiranje soft moći putem različitih mehanizama kao što su oblikovanje dnevnog reda, privlačenje ili uvjeravanje. Također, širenje cyber informacija kroz cyber prostor može koristiti soft moć privlačenjem građana druge zemlje, što ilustrira kampanje javne diplomatije provođene putem interneta. Međutim, cyber informacije imaju potencijal da postanu resurs hard moći, sposoban nanijeti štetu fizičkim ciljevima u drugim zemljama. Na primjer, mnoge kritične infrastrukture i industrijski procesi ovise o računalno kontroliranim sistemima, kao što su sistemi za nadzor i prikupljanje podataka. Zlonamjerni softver infiltriran u ove sisteme mogao bi biti instruiran da izvrši radnje koje rezultiraju stvarnim fizičkim učincima, ilustrirajući transformaciju cyber informacija u alat za projiciranje hard moći (Nye, 2010).

Analiza Josepha Nyea o cyber moći pruža novi pogled na to kako se dinamikom moći mijenja u današnjem digitalnom dobu. Historijski, uspon i pad dominantnih država definirao je prijelaz moći, ali Nyeov koncept difuzije moći nudi novu perspektivu (Olender, 2015). Informatička revolucija, vođena napretkom u digitalnoj komunikaciji i smanjenjem troškova tehnologije, izjednačila je šanse u globalnoj politici, omogućujući i malim državama i nedržavnim akterima kao što su multinacionalne korporacije, pa čak i terorističke grupe da ostvare značajan uticaj (Olender, 2015:55). Nye tvrdi da pravi izazov sada nije hoće li države preživjeti, već kako će se prilagoditi i funkcionirati u ovom novom cyber okruženju. Razbijanjem starih barijera, digitalno doba je fundamentalno promijenilo način na koji se moć razumijeva i ostvaruje (Olender, 2015).

Nye opisuje cyber moć kao sposobnost korištenja digitalnih resursa kao što su mreže, softver i infrastruktura za postizanje strateških ciljeva (Nye, 2011:123). Ova moć može se koristiti unutar samog cyber prostora ili za uticaj na druge oblasti. Njegova distinkcija između tvrde i meke moći u cyber svijetu je posebno zanimljiva. Tvrda moć uključuje korištenje cyber alata za agresivne svrhe, kao što su hakiranje sistema za krađu podataka ili ometanje usluga. S druge strane, meka moć u cyber prostoru može podržati pozitivne uzroke, poput pomaganja pokretima za ljudska prava putem digitalnih platformi. Ova dvostruka priroda cyber moći ističe i njen potencijal i rizike, naglašavajući potrebu za pažljivim navigiranjem kroz ovu kompleksnu teritoriju (Nye, 2011).

Ovi uvidi također otkrivaju paradoks za moćne države u cyber prostoru. Zemlje poput Sjedinjenih Američkih Država, Rusije i Kine, uprkos svojim naprednim tehnološkim sposobnostima, nisu imune na cyber prijetnje. Njihova velika zavisnost od povezanih sistema zapravo ih čini ranjivima na cyber napade (Nye, 2011). Ove ranjivosti mogu iskoristiti manji ili tehnološki manje razvijeni akteri, koji mogu nanijeti štetu uz relativno niske troškove (Olender, 2015). Nye ističe da velike prijetnje u cyber prostoru, uključujući ekonomsku špijunažu i cyber rat, pokazuju nerazmjernost na terenu. Nedostatak globalnog dogovora o cyber normama dodatno komplikuje situaciju, jer različite zemlje imaju vrlo različite stavove o pitanjima poput digitalnih sloboda. Na primjer, dok neki društvene mreže vide kao alat za lično izražavanje, drugi ih gledaju kao prijetnju (Nye, 2011). Ova podjela naglašava stalne izazove u razvoju učinkovitih međunarodnih cyber politika i održavanju otpornosti u stalno evoluirajućem digitalnom svijetu (Olender, 2015:56).

3.4.1. Tehnološki i prostorni uticaji – promjena paradigme

Razvoj cyber tehnologije, u kombinaciji s evoluirajućim konceptom prostora koji se koristi u geopolitičkim analizama, rezultirao je nastankom novih paradigmi koje reflektiraju promjene u socijalnim dinamikama, znanstvenim istraživačkim strukturama i geopolitičkim aranžmanima na razini koja se proteže od regionalnih do globalnih sfera (Mohamad Albakjaji and Reem Almarzoqi, 2023). Novonastali tehnološki paradigmi u analizi Soja (2009: 11-35) istražuju integraciju koncepta "prostora" putem njegovog evoluirajućeg dinamičkog koncepta kao procesa prostornosti i "prostornog." Koncept prostornog okreta ističe rastući značaj prostora u razumijevanju međunarodnih odnosa. Ovaj pomak odražava promjenjivu percepciju svijeta, gdje se prostor više ne smatra statičnim već dinamičnim i međusobno povezanim (Mohamad Albakjaji and Reem Almarzoqi, 2023). Ovu ideju podupiru Baylis, Smith i Owens (2020), koji ističu ključnu ulogu tehnološkog napretka u oblikovanju nove paradigme međunarodnih odnosa koja je karakterizirana umrežavanjem, međusobnom povezanošću i međusobnim interakcijama.

Tehnološki okret i nova prostornost povezani su s pitanjem o njihovom tehnološkom utjecaju na: „1) novu geografiju inovacija i 2) društvenu komunikaciju na globalnoj razini” (Stępień, 2016:5). U domeni društvene komunikacije i transfera podataka, proizlazi dilema vezana uz privatnost uslijed tehnološki posredovanih interakcija, što potiče na formiranje zajednica i sociopolitičkih pokreta kao novih oblika angažmana u društvenom i političkom kontekstu. U

oba scenarija, distribucija i korištenje informacija, zajedno s naknadnim tehnologijama komunikacije, postaju imperativni za uspješnu mobilizaciju društva. Dodatno, sfera međunarodnih odnosa sve više je oblikovana upotrebom ovih tehnologija (Stępień, 2016). Kao rezultat toga, tehnološki i prostorni obrati u geopolitiku uvode nove aktere, uz novi razumijevanje i razlikovanje tehnologija na korisne, vojne i zabavne domene s jedne strane, i konceptom tehnonauke u (post)konstruktivizmu koji ističe značaj "ne-ljudskih" elemenata u procesu razvoja s druge strane (Böhme, 2008; Latour, 2005: 63-86).

Jedan od ključnih aspekata prostornog preokreta izražava se kroz pojam cyber prostora. Rapidan razvoj digitalnih tehnologija omogućio je nastanak cyber ratovanja i informacijskog ratovanja, gdje jedan subjekt ima potencijalnu sposobnost poremetiti ili ugroziti cjelovite državne sisteme, što rezultira paradigmatskim pomicanjem međunarodnih odnosa iz tradicionalnog, reguliranog globalnog konteksta u digitalno okruženje (Stępień, 2016). U ovom kontekstu, naglasak se stavlja na potencijalne rizike razvoja cyber tehnologije. U tom smislu, Beckov model rizičnog društva ističe inherentne sistematske rizike koji proizlaze iz tehnonauke, zahtijevajući novi politički i normativni okvir za njeno upravljanje. Ovaj model zagovara kulturu participativnog odlučivanja u naučnim i tehnološkim pitanjima, naglašavajući javno učešće u debatama o tehnološkim inovacijama i njihovim društvenim uticajima (Beck, 1992). Latour (1993) proširuje ovu ideju naglašavajući inkluzivnu prirodu kolektivnog u teoriji mreže aktera, obuhvatajući i ljudske i ne-ljudske elemente tehnonauke. Umjesto tehnološkog determinizma, model tehnonauke promovira interakcionizam, prepoznajući međusobne odnose između naučnih, tehnoloških, društvenih i političkih procesa. Integriranjem ne-ljudskih elemenata u koncept društva, tehnonauka se pojavljuje kao okvir za upravljanje rizicima kako u društvenim tako i u međunarodnim kontekstima (Stępień, 2016).

Prostorni okret u geopolitičkim strategijama reflektira promjenjive karakteristike prostora. Tehnološki napredci, posebno u telekomunikacijama i satelitskoj tehnologiji, omogućili su globalnu suradnju i širenje informacija na globalnoj razini. Ovi razvoji nisu samo potaknuli suradnju, već su i iznjedrili nove oblike sukoba i natjecanja (Mohamad Albakjaji and Reem Almarzoqi, 2023). Antonio Missiroli (2021), u svom izvještaju *Geopolitics and strategies in cyberspace: Actors, actions, structures and responses*, navodi da proširenje geopolitičkog natjecanja u cyber prostor donosi jedinstvene dinamike, gdje teritorijalne granice nisu presudne, a moćne aktere ne čine samo države, već i globalni pružatelji digitalnih usluga, NVO-i te građanski akteri. Cyber moć djelomično se podudara s tradicionalnim

pokazateljima utjecaja i sposobnosti, kao što su veličina i međunarodni doseg, ističući rastući digitalni jaz između nacija, posebno u Globalnom Jugu, koji bi mogao postati poprište za geopolitički i tehnološki utjecaj. Naglasak na ofenzivnim cyber sposobnostima u posljednje vrijeme raste zbog eskalacije neprijateljskih aktivnosti. Unatoč različitim tumačenjima primjenjivosti međunarodnog prava na cyber prostor, većina stručnjaka se slaže s legitimnošću odmazde i mogućnošću ne-silovitih protumjera (Missiroli, 2021).

3.5. Cyber ratovanje

Rat je kompleksan čin koji se temelji na dinamičnim političkim, socio-kulturnim, ekonomskim i tehnološkim činiocima. Tokom vjekova, sredstva za vođenje rata evoluirala su od pješaka i pomorskih brodova do uključivanja najsavremenijih tehnologija poput nevidljivih aviona i bespilotnih letjelica (Dermer, 2013: 9). Ovaj trend evolucije ratovanja nastavio se u kasnom 20. stoljeću s pojavom novih tehnologija proizašlih iz pojave Interneta i mrežnih informacijskih sistema. Danas, vojske koriste umjetnički prostor cyberspacea kako bi povećale brzinu, agilnost i smrtonosnost rata (Dermer, 2013).

U proteklih dvadeset godina, percepcija mogućnosti međunarodnih sukoba prelaska u cyber prostor bila je značajno udaljena. Međutim, tijekom tog razdoblja, dogodile su se značajne promjene u percepciji i praksi. Sukobi u cyber prostoru danas nisu više neobična pojava, no i dalje postoji značajna neizvjesnost u vezi s njihovom „prirodom, opsegom i drugim karakteristikama“ (Gamero-Garrido, 2014: 1). Kako su godine prolazile, cyber prostor je postao ključno područje sukoba širom svijeta. Unatoč prvotnim strahovima od izbijanja otvorenih ratova isključivo u cyber prostoru, sukobi su se umjesto toga razvijali na načine koji ne odgovaraju jasno tradicionalnim definicijama rata i mira (Cristiano i sur., 2023).

Koncept cyber-ratovanja izaziva sliku vještih informatičkih ratnika koji pokreću agresivne napade na mreže suparnika, uzrokujući kaos i efikasno paralizirajući čitave nacije (Lewis, 2002). Međunarodni sukobi u cyber-prostoru uglavnom se odvijaju u takozvanoj sivoj zoni, fokusirajući se na manipulaciju informacija, podataka i srodnih aktivnosti poput špijunaže, sabotaže i subverzije. Kako brojni empirijski dokazi pokazuju, sukobi u cyber prostoru uglavnom obuhvataju aktivnosti niskog utjecaja poput hakiranja, špijunaže, širenja dezinformacija i nadzora (Cristiano i sur., 2023: 337).

Krepinevich (2012) u svom izvještaju *Cyber Warfare: A "Nuclear Option"?* daje generalnu definiciju koncepta cyber ratovanja navodeći da označava stratešku upotrebu cyber oružja od strane državnih aktera i entiteta izvan države radi infiltracije računarskih sistema ili mreža s višestrukim ciljevima. Ti ciljevi obuhvataju manipulaciju, korupciju ili fabrikaciju podataka, kao i poremećaj ili oštećenje računarske infrastrukture. Nadalje, cyber ratovanje obuhvata prikrivene aktivnosti, uključujući špijunažu, kriminalne radnje i manevre usmjerene na ekonomsku koerciju. Štoviše, obuhvata strateške inicijative prilagođene jačanju vojnih nastojanja na taktičkim, operativnim i strateškim razinama, čime se ostvaruju efekti na različitim nivoima sukoba (Krepnevich, 2012:8-9).

Ubrazan tempo tehnoloških napredaka, u kombinaciji sa sve nestabilnijim geopolitičkim okruženjem, sugeriše da trenutno razdoblje nosi značajan potencijal za bitne i transformacijske promjene u vojnoj dinamici, slične vojnoj revoluciji, poput perioda između dva svjetska rata (Krepinevich, 2012). Agresivne strategije i taktike u cyber ratovanju pružaju brojne prednosti potencijalnim akterima, pri čemu trenutni globalni događaji naglašavaju prevalenciju cyber sukoba. Stoga, lideri u nacionalnoj sigurnosti moraju unaprijediti svoje razumijevanje „tehnoloških, pravnih i etičkih dimenzija" cyber napada i odbrane kako bi efikasno integrirali razmatranja cyber ratovanja u sve aspekte planiranja nacionalne sigurnosti (Geers, 2008: 2).

Važno je naopomenuti da u domenu cyber ratovanja, postoje dvije ključne komponente – „*CNA/ Computer Network Attack* (Napad na računarske mreže) i *CND/ Computer Network Defens*e" (Odbrana računarskih mreža). (Dermer, 2013: 5) Konceptualno, CNA uključuje efekte koji se protežu od ometanja elektronskih sistema protivnika i operacija koje omogućavaju (komunikacija, sistemi vođenja, radarske sposobnosti, itd.) do izazivanja stvarne kinetičke štete korištenjem cyber alata za uzrokovane kvarove ili samouništenje u sistemima protivnika. Druga komponenta cyber ratovanja teži eliminaciji ili smanjenju rizika od prve. Uloga CND-a je odbrana mreža od napada putem pasivnih ili aktivnih mjera. Pasivne odbrane obuhvataju konvencionalne pristupe poput otkrivanja virusa i obuke korisnika o praksama osiguranja informacija. S druge strane, aktivna odbrana koristi senzore, softver i obavještajne podatke kako bi otkrila i zaustavila svaki zlonamjerni kod prije nego što može nanijeti štetu (Dermer, 2013).

Janczewski i Colarik (2008) su podijelili cyber napade u faze, usklađujući ih s konvencionalnim kriminalnim djelima. Prva faza uključuje istraživanje potencijalnih žrtava,

prikupljanje vrijednih informacija o operacijama cilja putem posmatranja i korištenja njihovih aplikacija i hardvera. Nakon toga, slijedi prodor, označavajući trenutak kada napadači dobijaju pristup sistemu, ograničavajući protumjere na ometanje pristupa uslugama cilja. Identifikacija i distribucija internih prilika slijede, pregledajući resurse sistema i prava pristupa ograničenim komponentama. Četvrta faza podrazumijeva stvarnu štetu na sistemu ili krađu podataka od strane napadača. Nadalje, tvrde da se savremeni cyber napadi pretežno manifestuju kao distribucija zlonamjernog softvera putem priloga u internet pregledaču, e-pošti ili ranjivosti sistema; odbijanje usluge (DoS) kako bi se otežala upotreba računarskih sistema i mreža; izmjena ili brisanje (uz poruke) vladinih i komercijalnih web stranica u svrhu propagande ili ometanja; i neovlašteni upadi u sisteme radi krađe povjerljivih i/ili vlasničkih informacija, kompromitacije podataka ili korištenja sistema za pokretanje napada na druge sisteme (Janczewski i Colarik, 2008). U okolnostima takve transformacije i različitih gledišta i shvaćanja sigurnosti općenito i međunarodne sigurnosti, cyber prijetnje svakako ponovno definiraju te pojmove. U skladu s naporima da se osigura sigurnost s jedne strane i specifičnostima cyber prijetnji i motivima aktera koji ih pokreću s druge strane, bit će potrebno uspostaviti novi međunarodni sigurnosni paradigmu cyber doba (Duić, Cvrtila i Ivanjko, 2017).

3.5.1. Vrste i metode cyber ratovanja

Cyber ratovanje koristi mnoge taktike, tehnike i postupke kako bi postiglo svoj cilj uključujući:

a. Špijunaža

U kontekstu cyber ratovanja, špijunaža se odnosi na tajno praćenje drugih zemalja ili entiteta radi krađe povjerljivih informacija. Ovo uključuje korištenje tehnika poput bot mreža ili napada ciljanih phishingom kako bi se inficirali ranjivi računarski sistemi, nakon čega se izvlače osjetljivi podaci. (Imperva, 2024) Vlade širom svijeta sve više izražavaju javne prigovore u vezi sa slučajevima cyber špijunaže. Na dnevnoj bazi, anonimni hakeri neovlašteno kopiraju značajne količine računarskih podataka i komunikacija putem mreže. Teoretski je moguće izvesti snažne operacije prikupljanja obavještajnih podataka, uključujući i one na visoko osjetljivim političkim i vojnim komunikacijama, iz bilo kojeg mjesta u svijetu (Geers, 2008: 4).

b. Propaganda

Jeftina, a ipak efikasna, propaganda često predstavlja jedan od najlakših i najmoćnijih oblika cyber napada. Digitalni sadržaj, bez obzira na istinitost, u tekstualnom ili slikovnom formatu, može se trenutno kopirati i poslati bilo gdje u svijetu, čak i duboko iza neprijateljskih linija. I provokativne informacije koje su uklonjene s interneta mogu se pojaviti na drugoj web stranici u sekundama (Geers, 2008). Koristeći kao pokušaj kontrole uma i mišljenja ljudi koji žive ili se bore za ciljnu zemlju, propaganda se može koristiti za izlaganje sramotnih istina, širenje laži kako bi ljudi izgubili povjerenje u svoju zemlju ili pristali na stranu svojih neprijatelja (Imperva, 2024).

c. Uskraćivanje usluga- Denial-of-Service (DoS)

DoS napadima je osnovna strategija ograničavanje korištenja računarskog resursa legitimnim korisnicima. Najčešća taktika je preplaviti ciljano mjesto tolikom količinom suvišnih podataka da ne može odgovoriti na stvarne zahtjeve za uslugama ili informacijama. Ostali DoS napadi uključuju fizičko uništavanje računarske opreme i upotrebu elektromagnetnog smetnji, namijenjenih uništavanju nezaštićene elektronike putem skokova u struji ili naponu (Geers, 2008).

d. Manipulacija podacima

Manipulacija podacima predstavlja izuzetnu opasnost jer uspješan napad može značiti da će legitimni korisnici (ljudi ili mašine) donijeti važne odluke na osnovu zlonamjerno izmijenjenih informacija. Takvi napadi variraju od defacementa web stranica (često nazivanog *elektronskim grafitima*, ali koji i dalje može nositi propagandu ili dezinformacije) do napada na baze podataka s ciljem korupcije oružja ili sistema za komandu i kontrolu (Geers, 2008). Ovi napadi manipulacije podacima namijenjeni su krađi ličnih, zdravstvenih, obrazovnih i finansijskih podataka. Pored toga, cilj im je i otimanje vrijednih imovinskih sredstava vodećih kompanija u obrambenoj, tehnološkoj i proizvodnoj industriji (Brooke, 2024).

e. Manipulacija infrastrukturom

Napadač iskorištava karakteristike infrastrukture mrežnog entiteta kako bi izveo napade ili prikupljao informacije o mrežnim objektima ili kako bi izmijenio uobičajeni tok informacija između mrežnih objekata. Najčešće, ovo uključuje manipulaciju usmjeravanja mrežnih poruka tako da umjesto da stignu na

odredište, budu usmjerene ka entitetu po izboru napadača, obično serveru koji je pod kontrolom napadača. Žrtva često nije svjesna da se njene poruke ne obrađuju kako treba. Na primjer, ciljani korisnik može pogrešno vjerovati da se povezuje sa svojom vlastitom bankom, dok zapravo pristupa web stranici kojom upravlja napadač. Nakon toga, napadač prikuplja korisničke podatke za prijavu s namjerom da neovlašteno pristupi stvarnom bankovnom računu (The MITRE Corporation, 2018).

3.5.2. Akteri u cyber prostoru

S malo prepreka za ulazak i visokom anonimnošću, cyber prostor je idealno tlo za države i nedržavne aktere da izvode činove neprijateljstva, agresije i ratovanja s malo ili nikakvih posljedica, čineći cyber prostor arenom za vođenje geopolitičkih i geoekonomskih rivalstava. Na primjer, trenutni sukob između Rusije i Ukrajine ima značajnu komponentu cyber ratovanja. Države teže dominaciji nad cyber prostorom, te u tom procesu koriste nedržavne aktere (Raman, 2023).

U cyber ratovanju, nedržavni akteri predstavljaju grupe ili entitete bez izravne povezanosti s vladama, koji se bave cyber operacijama iz različitih razloga, kao što su politički ili ideološki motivi, cyber kriminal ili promicanje ideoloških ili političkih ciljeva (Marasović, 2023). Takvi subjekti, koji nemaju fizički teritorij ili teritorijalni suverenitet, djeluju u cyber prostoru i mogu obuhvatiti pojedince, grupe ili organizacije koje djeluju neovisno ili u suradnji sa državnim akterima (Raman, 2023; Marasović, 2023).

Među tim akterima, Andress i Winterfeld (2014: 29) navode da su najvažnije hacktivističke grupe poput Anonymousa i LulzSeca, vođene političkim ili ideološkim agendama, koristeći tehnike hakiranja kako bi promovirale svoje ciljeve. Ove grupe su bile uključene u brojne cyber operacije i proteste, koristeći svoje vještine kako bi zagovarale svoja uvjerenja. S druge strane, kriminalne organizacije uglavnom teže financijskoj dobiti kroz cyber aktivnosti kriminala. Ove grupe, poput entiteta kao što su REvil i DarkTequila, bave se napadima ransomwarea, krađom podataka i krađom identiteta kako bi nezakonito stekli novčane nagrade (Andress i Winterfeld, 2014).

Osim toga, plaćeničke grupe nude usluge cyber ratovanja za najam, pružajući usluge vladama, korporacijama ili drugim entitetima koji traže specijalizirano znanje o ofenzivnim cyber operacijama. Poznati primjeri uključuju NSO Group, poznatu po razvoju alata prilagođenih scenarijima virtualnog ratovanja, dodatno zamagljujući granice između državnih i nedržavnih aktera u cyber prostoru (Andress i Winterfeld, 2014). Štoviše, terorističke organizacije poput Al-Qaede i ISIS-a sve više istražuju taktike cyber ratovanja kao sredstvo za ostvarenje svojih ciljeva, predstavljajući značajne prijetnje kritičnoj infrastrukturi i sigurnosti podataka širom svijeta. Napokon, međunarodne kriminalne organizacije, često bazirane u regijama poput istočne Europe, specijalizirane su za različite cyber kriminalne aktivnosti, uključujući prijevare s kreditnim karticama, krađu identiteta i online iznude, predstavljajući značajne financijske i sigurnosne prijetnje na globalnoj razini (Andress i Winterfeld, 2014:215).

3.6. Strateška teorija cyber ratovanja

Razvojem i integracijom moderne tehnologije u svakodnevni stil života te različite oblasti ljudskog djelovanja su za rezultate imale pojavu cyber ratovanja, koje je za najkraće vrijeme postalo značajno područje civilnog i vojnog sukoba. Pored činjenice da je cyber prostor postao ne samo polje za političke bitke velikih sila, već i za ekonomsku špijunažu i aktivnosti raznih terorističkih i drugih kriminalnih organizacija kao metod ratovanja, razvila se potreba za analizu i kontekstualizaciju strateške teorije cyber ratovanja i njenih implikacija na tradicionalan koncept ratovanja.

Dr. Jan Kallberg, stručnjak za cyber operacije kao alternative političkim strategijama, pružio je uvid u stratešku teoriju cyber ratovanja, argumentirajući da je njezina suština u tome da efikasnost cyber operacija zavisi o stepenu institucionalne stabilnosti u ciljanoj državi. Prema toj teoriji, sistematski cyber napadi na nacije s nekonsolidiranim institucionalnim osnovama mogu iskoristiti inherentne slabosti, što na kraju rezultira podređenošću vanjskim utjecajima. Ova promjena paradigme transformira percepciju cyber ratovanja, postavljajući ga ne samo kao podršku vojnim akcijama, već i kao strateško oruđe za kontrolu nad protivničkim društvima (Kallberg, 2016).

Koncept strateškog efekta u kontekstu cyber ratovanja predstavlja složenu temu koja nosi duboke implikacije za dinamiku odnosa među sukobljenim stranama. Colin Gray (2010), priznati stručnjak u oblasti strategije, pruža sveobuhvatno objašnjenje strateškog efekta, koji obuhvata posljedice djelovanja na neprijatelje i uključuje materijalne, psihološke ili kombinovane dimenzije. Ovi efekti imaju za cilj ograničiti sposobnost neprijatelja da pruži

otpor, utječući na njegovu spremnost za suprotstavljanje. Ove definicije posebno su relevantne u kontekstu cyber ratovanja, gdje posljedice često nadilaze samo fizičku štetu, prodireći u psihičku sferu ciljanih populacija (Dermer, 2013). Takvi ishodi, postignuti degradacijom vojnih sposobnosti ili destabilizacijom društvenih struktura, ključni su u izazivanju značajnih promjena u politici ili čak podčinjenosti ciljanog društva stranim nalogodavcima (Kallberg, 2016).

Collin S. Gray, u nastavku tematike strateška teorije cyber ratovanja, tvrdi da će „razumijevanje što znači cyber moć strategijski, donekle zadovoljno, nastati kada praksa cyber sukoba pruži dokaze o tome što je moguće, a što nije“ (2013:3). Shodno tome, nailazimo na činjenicu da cyber ratovanje, sa svojom jedinstvenom kombinacijom tehnološke sofisticiranosti i psihološke manipulacije, ima potencijal da oslobodi niz posljedica na neprijatelje. Na primjer, upotreba napada na računarske mreže (CNA) može ne samo nanijeti stvarnu štetu kritičnoj infrastrukturi, već i posijati sjeme sumnje i bespomoćnosti među civilnim populacijama. Ovaj dvostruki uticaj ističe transformacijsku prirodu cyber ratovanja, gdje se zamagljuju granice između fizičkog i psihičkog ratovanja, što zahtijeva detaljno razumijevanje njegovih strateških efekata. Nadalje, inherentno asimetrična priroda cyber operacija uvodi nove kompleksnosti, budući da čak i relativno mali napadi mogu rezultirati nesrazmjerno velikim strateškim ishodima, što pojačava značaj strateškog efekta u scenarijima cyber sukoba (Dermer, 2013).

U tradicionalnom aspektu ratovanja, postoji jasna granica između upotrebe oružja i zastupljenih aktera u sukobu. Međutim, takvo razgraničenje ne postoji u domenu cyber sigurnosti. Određeni aspekti cyber ratovanja uveliko liče na cyber napade koji imaju za cilj nanošenje teške štete. Na primjer, pokušaji da se infiltriraju u kompjutersku mrežu radi ekstrakcije podataka često liče na pokušaje koji imaju za cilj ubacivanje zlonamjernog koda ili izvođenje cyber napada, kao što su oštećenje podataka ili kompromitacija sistema. Ova sličnost predstavlja izazove u brzom prepoznavanju kada konkurent prelazi sa cyber špijunaže, kriminalnih aktivnosti ili ekonomskog ratovanja na ciljanje kritične infrastrukture protivnika (Krepinevich, 2012).

Dr. Jan Kallberg navodi četiri ključna izazova koja se pojavljuju u primjeni tradicionalne vojne teorije na cyber sukob – “anonimnost, postojanost objekta, mjerljivi rezultati i brzo digitalno izvršenje” (2016:103). Anonimnost predstavlja značajnu prepreku, budući da je pripisivanje cyber napada određenim akterima često neuhvatljivo. U tradicionalnom

ratovanju, jasna identifikacija neprijatelja ključna je za strateško planiranje i donošenje odluka. Međutim, u cyber prostoru napadači mogu sakriti svoje identitete kroz sofisticirane tehnike poput spoofinga i proxy servera, što otežava napore za pripisivanje i zamagljuje granice između državnih i nestalnih aktera (Kallberg, 2016:105). Ova anonimnost stvara osjećaj neodređenosti i neizvjesnosti, što otežava političarima i vojnim liderima formuliranje efikasnih strategija odgovora. Također, međusobno povezana priroda interneta omogućava protivnicima da djeluju s udaljenih lokacija, prevazilazeći geografske granice i pravne ograničenja nadležnosti, čime se dodatno komplicira pripisivanje napada određenim entitetima ili državama (Kallberg, 2016).

Dodatno, koncept trajnosti objekata, ključan za manevrisanje i pozicijske strategije, gubi relevantnost u cyber prostoru zbog njegove dinamične i prolazne prirode. Za razliku od fizičkih bojišta na kojima se terenske karakteristike relativno stabiliziraju, cyber pejzaž se neprestano mijenja, s digitalnim sredstvima i infrastrukturom podložnim brzim promjenama i prilagodbama. Stoga se tradicionalni vojni koncepti poput uspostavljanja i održavanja pozicijskih prednosti manje primjenjuju u fluidnom i promjenjivom okruženju cyber prostora. Protivnici mogu iskoristiti ovu fluidnost kako bi izveli prolazne i prilagodljive napade, iskorištavajući ranjivosti, a zatim se brzo povlače kako bi izbjegli otkrivanje ili odmazdu (Kallberg, 2016).

Mjerenje efikasnosti cyber operacija predstavlja još jedan izazov, budući da su tradicionalne metrike zasnovane na opipljivim rezultatima često nedovoljne u nematerijalnom prostoru cyber prostora. U konvencionalnom ratovanju, uspjeh se često mjeri u pogledu "osvojenog teritorija, zadanih neprijateljskih žrtava ili postignutih strateških ciljeva" (Kallberg, 2016: 113). Međutim, u cyber prostoru, utjecaj operacija može biti teže kvantificirati, jer efekti mogu biti suptilni, indirektni i teško se mogu direktno pripisati određenim radnjama. Osim toga, međusobno povezana priroda cyber prostora znači da efekti cyber operacija mogu proširiti se na više domena, utječući na socijalne, ekonomske i političke dinamike na načine koji izmiču tradicionalnim mjerilima uspjeha ili neuspjeha (Kallberg, 2016: 115).

Osim toga, brza tempo digitalne izvršbe nadmašuje sposobnosti tradicionalnih vojnih procesa donošenja odluka, zahtijevajući prilagodljivost i agilnost u cyber operacijama. Za razliku od namjernog i sekvencijalnog karaktera tradicionalnog vojnog planiranja i izvršbe, cyber operacije odvijaju se digitalnom brzinom, s napadima koji se pokreću i odbacuju u milisekundama umjesto satima ili danima. Ovaj ubrzani ritam operacija zahtijeva brzo

donošenje odluka, stvarno-vremensku svjesnost o situaciji i agilne sposobnosti odgovora kako bi se učinkovito angažirali protivnici u cyber prostoru (Kallberg, 2016). Nadalje, asimetrična priroda cyber sukoba znači da manji, manje resursni akteri potencijalno mogu nanijeti značajnu štetu većim, tehnološki naprednijim protivnicima, dodatno izazivajući tradicionalne pojmove vojne superiornosti i dominacije (Kallberg, 2016: 118).

Formiranjem strateške teorije cyber ratovanja postavio se fokus na prilagođavanje implikacijama i dinamikama cyber ratovanja, u cilju razumijevanja društvenih institucija i njihovih uloga i ranjivosti u ovom procesu. Teorija, zajedno s uspostavljenim praksama i znanjem fokusiranim na institucionalnu otpornost, formuliše strategije i pristupe u cilju destabilizacije protivničkih društava. Prema navodima Kallberga (2016) glavna tvrdnja strateške teorije podrazumijeva da će u budućnosti cyber sposobnosti služiti kao instrumentalni alati za postizanje geopolitičkih ciljeva putem podrivanja protivničkih nacija. Teorija strateškog cyber rata služi kao mehanizam za iskorištavanje ranjivosti unutar protivničkih država. Konačno, napredak cyber sposobnosti će prouzročiti stanje nereda ili kaosa, poznato kao entropija, unutar protivničkih zemalja, pružajući sistemski šok osnovnom institucionalnom okviru koji povezuje ove nacije. Kroz pristup strateške teorije, stavlja se imperativ na međunarodnu suradnju i djelovanje kao odgovor na prijetnje i izazove koji nam dolaze u cyber periodu i ratovanju (Kallberg, 2016: 122-125).

3.7. Dinamika cyber moći u međunarodnom sistemu

Max Weber definirao je moć kao „vjerovatnoću da će jedan akter unutar društvenog odnosa biti u poziciji da ostvari svoju volju uprkos otporu, bez obzira na osnovu na kojoj se ova vjerovatnoća temelji“ (Weber, 1978:53). U istom periodu kao i Weber, talijanski general Giulio Douhet povezao je zračnu moć s sposobnošću države da spriječi neprijatelja da leti dok istovremeno zadržava sposobnost letenja vlastitih snaga. Slično tome, britanski admiral Philip Howard Colomb opisao je kontrolu nad morem kao moć da se spriječi prolazak neprijatelja koji namjerava sletjeti na kopno (McCreanor, 2021).

Kako smatra Nye (2010), u svjetskoj politici, moć ovisi o kontekstu, a brzi rast cyber prostora predstavlja važan novi kontekst u tom smislu. Niska cijena ulaska, anonimnost i asimetrije u ranjivosti znače da manji akteri imaju veću sposobnost da iskoriste hard i soft moć u cyber prostoru nego u mnogim tradicionalnim domenima svjetske politike. Cyber prostor

predstavlja petu domenu, nakon zraka, kopna, mora i svemira, te se neprestano razvija i suprotstavlja ekonomskim, sigurnosnim i civilnim interesima (Wei, 2022). Promjene u informacijskim dinamikama uvijek su imale značajan utjecaj na moć, ali cyber domen je i novo i nestabilno okruženje. Karakteristike cyber prostora smanjuju neke od razlika u moći među akterima, čime pružaju dobar primjer difuzije moći koja je karakteristična za globalnu politiku u ovom stoljeću. Najveće sile vjerojatno neće moći dominirati ovim domenom koliko su to činile u drugim, poput morskih ili zračnih prostora. Ali cyber prostor također ilustrira činjenicu da difuzija moći ne znači jednakost moći ili zamjenu vlada kao najmoćnijih aktera u svjetskoj politici (Nye, 2010).

Proširujući prethodnu raspravu, cyber moć se pojavljuje kao višeslojna sila koja kombinuje karakteristike kopnene, morske i zračne moći, te istovremeno se razlikujući i koristeći paralele s ovim konvencionalnim oblicima vojne moći. Osim toga, inherentne sličnosti između cyber prostora i fizičkih domena omogućavaju teoriji cyber moći da koristi uvide iz prošlih ratnih iskustava, olakšavajući razvoj strateških okvira koji su informirani kako prošlim lekcijama, tako i suvremenim realnostima (Bonner, 2011). U skladu s tim, definicija Daniel T. Kuehla pruža uvid u sveukupni značaj cyber moći, tvrdeći da obuhvata sposobnost iskorištavanja cyber prostora radi sticanja strateških prednosti i izvršavanja utjecaja na različitim operativnim područjima i instrumentima moći, služeći kao sredstvo za postizanje političkih ciljeva aktera, bilo da su to pojedinci, organizacije ili države (Kuehl, 2009). Temeljno, cyber moć počiva na stvaranju, kontroli i komunikaciji digitalnih informacija putem interneta i drugih digitalnih kanala (Thong, 2016).

Cyber prostor i cyber moć predstavljaju neodvojive komponente informacionog aspekta moći. Strategijski, cilj je manipulirati percepcijama unutar strategijskog okruženja radi vlastite koristi, istovremeno smanjujući sposobnost protivnika da shvati isto to okruženje (Jansen van Vuuren i sur., 2016). Cyber moć, stoga, mjeri sposobnost manipulacije tim okruženjem putem pristupa cyber infrastrukturi cilja putem iskorištavanja i napada (Sheldon, 2011). Također, cyber moć može se posmatrati kao sposobnost upravljanja IT sistemima i mrežama unutar digitalnog ili cyber prostora, prožimajući se s ostalim elementima i instrumentima moći (Jansen van Vuuren i sur., 2016).

Cyber moć stvara sinergije među tim elementima, unaprijeđujući ih na transformacijski način (Zimet i Barry, 2009). Ova povezanost proširuje se na ljude i organizacije u modernom povezanom svijetu, gdje se tradicionalne granice mijenjaju (Sheldon, 2011). Odnosno, cyber

moć je sveprisutna prirode, djeluje neprimjetno, formirajući tri osnovne karakteristike ove moći uz njezin komplementarni karakter (Krekel i DeWeese, 2009; Sheldon, 2011). Iako kopnena, pomorska, zračna i svemirska moć mogu utjecati jedna na drugu strateški, trenutačna i opširna priroda cyber moći izdvaja je (Lonsdale, 2004). Prema Sheldonu (2011), cyber moć još nije dokazala svoju sposobnost prisile, čime je prvenstveno komplementarni instrument, iako je njena neprimjetnost čini atraktivnom opcijom za korištenje.

U zaključku, cyber moć predstavlja sposobnost države-nacije da uspostavi kontrolu i izvrši uticaj unutar i kroz cyber prostor, podržavajući se i usklađujući s drugim elementima nacionalne moći u različitim domenama. Postizanje cyber moći počiva na sposobnosti države da razvije resurse za operacije unutar cyber prostora. Slično kao i kopnena, pomorska, zračna ili svemirska moć, cyber moć se oslanja na umrežene računare, telekomunikacijsku infrastrukturu, softvere i pojedince s potrebnim vještinama, umjesto na tenkove, brodove ili avione (Spade, 2012). Cyber moć države-nacije obuhvata tri ključne dimenzije: „koordinaciju operativnih i političkih aspekata kroz vladine strukture, koherentnost politike putem međunarodnih saveza i pravnih okvira, te suradnju nevladinih aktera u cyber prostoru“ (Klimburg, 2011:43). Uzimajući u obzir da većinu onoga što nazivamo cyber prostorom posjeduje i upravlja privatni sektor, te kao posljedica ogromnih količina podataka koje kompanije za komunikacije kontroliraju kao dio svojih operacija, vlade su započele proces intenzivnijeg inkorporiranja interneta i telekomunikacijske kompanije u nadzor cyber prostora (Deibert, 2013). Bitna ideja iza stvaranja cyber moći proizlazi iz činjenice da se ona nalazi izvan neposredne kontrole vlade, već unutar domena poslovnih i civilnih društava. U ostvarivanju cjelovite nacionalne moći u cyber prostoru, ključno je poticati suradnju između vlasti i sektora civilnog društva, potičući motivaciju i aktivno uključivanje građana primjenjujući koncept soft moći usmjeren unutar zemlje.

4. RUSIJA I UKRAJINA: HISTORIJA, DINAMIKA I IMPLIKACIJE

4.1. Međudržavni sukobi: nastanak i uzroci

Nakon dugog perioda relativnog mira među državama, u proteklih petnaest godina zabilježen je značajan porast globalnih međudržavnih sukoba, uz sve veći broj sukoba između vojnih snaga suverenih nacija. U posljednje dvije godine, međunarodni odnosi su bili znatno pod utjecajem, prvo zbog ruske invazije na Ukrajinu, a zatim zbog izraelskih vojnih operacija u Palestini. Heidelberški institut za istraživanje međunarodnih sukoba definirao je sukobe kao "sukob interesa (različite pozicije) na nacionalnim vrijednostima određene trajnosti i veličine između najmanje dvije strane (organizirane grupe, države, grupe država, organizacije) koje su odlučne u namjeri da ostvare svoje interese i pobijede u svojim slučajevima" (Heidelberg Institute for International Conflict Research, 2005:1). Dok Juliet Kaarbo i James Lee Ray (2005) dijele međunarodni konflikt u dvije kategorije- međudržavni ratovi (ratovi između država) i unutrašnji ratovi (građanski ratovi unutar država).

U raspravi o međudržavnim sukobima, naučnici se i dalje bore da pronađu opću teoriju uzročnih faktora koja objašnjava pojavu smrtonosnih sukoba velikih razmjera među velikim grupama ljudi (ratova) u historiji čovječanstva (Bareis, 2018). Jedan opći konsenzus o ratu je da predstavlja izuzetno kompleksan fenomen koji proizlazi iz višeznačnog procesa koji obuhvata različite nivoe analize (Cashman, 2014). Juliet Kaarbo i James Lee Ray (2005) su argumentirali da izbor nivoa analize zavisi od toga da li je fokusiran na pojedinačne komponente ili na čitav sistem. U suštini, nivo analize određen je specifičnim društvenim entitetom koji se ispituje - bilo da su to pojedinačne države ili širi međunarodni sistem - koje analitičar pokušava objasniti u smislu ponašanja ili funkcionisanja.

Izgrađujući na ranijim radovima Babsta (1972), Rummela (1975–1981) i Doylea (1983a, 1983b), Maoz i Abdolali (1989) prvi su sistematski empirijski analizirali učestalost međudržavnih ratova između demokratskih parova država u poređenju s ratovanjem među mješovitim ili autokratskim parovima država tokom dužeg vremenskog perioda. Također su analizirali odnos između tipa režima i međudržavnog sukoba na nacionalnom i sistemskom nivou analize, ukazujući na različite odnose između demokratije i mira na svakom nivou. Na nacionalnom nivou, njihova istraživanja su pokazala da demokratske države, generalno, nisu manje sklone sukobima od drugih tipova država. Ipak, Maoz i Abdolali (1989: 21) su

izvijestili da demokratske države rijetko, ako ikada, ratuju jedna protiv druge na dijadičkom nivou[3]. Također su zaključili da "proporcija demokratija u sistemu pozitivno utiče na broj započetih i tekućih sukoba" (Maoz i Abdolali, 1989: 29). Maoz i Russett (1993) su prihvatili kontrast između nacionalnih i dijadičkih nivoa odnosa između demokratije i mira, videći ga kao istraživački problem. Ray (2001) zaključuje da empirijski odnosi između varijabli ne moraju biti konzistentni na različitim nivoima analize, jer odnosi na različitim nivoima (kao što su države, parovi država i međunarodni sistem) mogu biti nezavisni i značajno različiti. Stoga, moguće je imati kontrastne korelacije i uzročno-posljedične veze na različitim nivoima analize, što čini nelogičnim izvoditi zaključke o cjelokupnom međunarodnom sistemu iz odnosa na nacionalnom ili dijadičkom nivou.

Tradicionalno, proučavanje uzroka rata u političkim naukama bilo je dominirano realističkim teorijama koje pretpostavljaju da „suverene države (ili druge teritorijalno definirane skupine) djeluju racionalno kako bi unaprijedile svoju sigurnost, moć i bogatstvo u anarhičnom međunarodnom sistemu definiranom odsustvom legitimnog autoriteta za regulaciju sporova i sprovođenje sporazuma" (Levy, 2011:16). Realisti su podijeljeni oko toga koliko su anarhične strukture i sigurnosna dilema zapravo primoravajuće u primoravanju država u konfliktne odnose. Ofanzivni realisti tvrde da je međunarodni sistem toliko neprijateljski i neumoljiv da nesigurnost oko budućih namjera protivnika, u kombinaciji s ekstremnim analizama najgorih slučajeva, navodi velike sile da usvoje ofanzivne strategije i teže regionalnoj hegemoniji (Mearsheimer, 2001). Osnovna realistička tvrdnja je da varijacije u raspodjeli moći pomažu u objašnjavanju varijacija u učestalosti rata i drugih oblika međunarodnog ponašanja (Waltz, 1979, 1988; Mearsheimer, 2001).

Kao što smo već prikazali, Mearsheimerov ključni doprinos je njegova teorija ofanzivnog realizma, koja ima za cilj modificirati Waltzovu strukturalnu realističku teoriju kako bi objasnila visoke razine međunarodne agresije iz strukturalne perspective (Toft, 2005). Mearsheimer je stekao značajno priznanje u realističkoj tradiciji međunarodnih odnosa kroz svoje kontroverzne publikacije. Mearsheimerova teorija istražuje zašto su odnosi između velikih sila u modernom međunarodnom sistemu često obilježeni konfliktima, naglašavajući važnost strukture međunarodne politike. U svom istraživanju, identificira pet ključnih pretpostavki koje su općenito prihvaćene među suvremenim realistima i koje opisuju

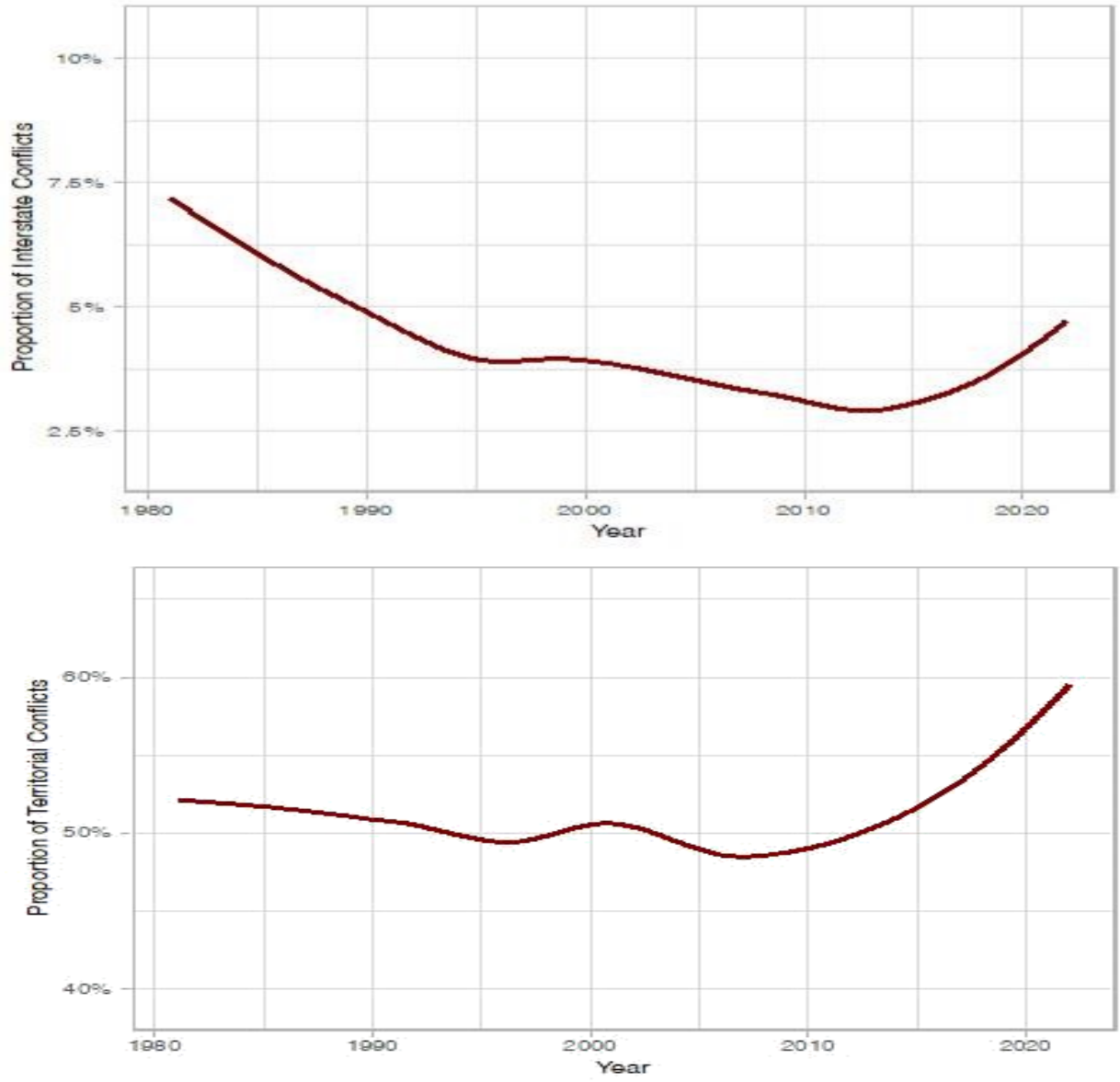
[3] Dijadički nivoi analize fokusiraju se na interakciju unutar 'agregata' umjesto na namjerne akcije pojedinačnih jedinica. Drugim riječima, čak i minimalni stepen agregacije koji uključuje tretiranje parova država kao jedinica analize prelazi važnu granicu između akcije i interakcije kao glavne tačke pažnje; analize strukturirane na ovaj način neizbježno vode do hipoteza o uključivanju u sukob nasuprot pokretanju sukoba

fundamentalne obilježja međunarodnih odnosa. Prva, međunarodni odnosi odvijaju se u okruženju bez centralne vlasti koja bi nametala pravila i sankcionirala prekršitelje. Druga, države su konstantno izložene neizvjesnosti o namjerama drugih država i mogućnosti upotrebe sile protiv njih, što dodatno kompliciraju nepotpune i promjenljive informacije. Treća, preživljavanje je glavni cilj svake države u međunarodnom sistemu jer je autonomija države ključna za ostvarivanje drugih ciljeva. Četvrta, države djeluju racionalno u smislu strategijskog procjenjivanja vanjskih okolnosti kako bi usvojile strategije koje maksimiziraju preživljavanje. Konačno, sve države posjeduju vojne kapacitete koji im omogućuju nanošenje štete i potencijalno uništavanje jedna drugoj. Integrirajući ove pretpostavke, Mearsheimer zaključuje da države prepoznaju povećanje svoje relativne moći kao najučinkovitiji način osiguranja preživljavanja u anarhičnom sistemu, s krajnjim ciljem postizanja hegemonijskog statusa. Ipak, s obzirom na nesposobnost svih država da istovremeno maksimiziraju svoju moć u odnosu na druge, neprestana sigurnosna konkurencija dominira unutar anarhičnog međunarodnog sistema (Mearsheimer, 2001).

Moć zauzima središnje mjesto u Mearsheimerovoj teoriji, definišući je kroz materijalne kapacitete, a ne ishode, jer smatra da su ishodi nepouzdani indikatori ravnoteže moći s obzirom na to da slabije države ponekad mogu nadvladati jače (Mearsheimer, 2001). Mearsheimer (2001) razlikuje sposobnosti država na latentnu moć (ekonomija i populacija) i stvarnu moć (vojska), pri čemu naglašava da je vojna moć ključna u međunarodnoj politici, jer predstavlja krajnji odrednik. Također, tvrdi da je kopnena moć od suštinskog značaja, jer kontrola teritorija, najvažnijeg resursa u svijetu teritorijalnih država, zahtijeva kopnene vojske (Mearsheimer, 2001). Prema Mearsheimeru, države teže maksimiziranju relativne moći radi postizanja hegemonije, definirane kao dominacija nad svim drugim državama u sistemu (Mearsheimer, 1995; 2001). Ovaj koncept se odnosi na globalnu i regionalnu dominaciju. Iako hegemonija obično znači globalnu dominaciju, može se koristiti i za opisivanje regionalne dominacije, na primjer u Evropi, Sjeveroistočnoj Aziji i Zapadnoj hemisferi (Mearsheimer, 1995). Regionalna hegemonija je glavni strateški cilj jer globalna hegemonija je gotovo nemoguća zbog izazova projektovanja moći preko okeana, osim u slučaju nuklearnog monopola, što je malo vjerovatno jer bi druge države razvile vlastite nuklearne snage (Mearsheimer, 2001).

Okupacija Ukrajine od strane Rusije u februaru 2022. godine predstavlja najintenzivniji međudržavni sukob od invazija Sjedinjenih Američkih Država na Irak 2003. i Afganistan

2001. godine (Bleng, 2022). Ovaj događaj nedvosmisleno ukazuje na značajnu promjenu ravnoteže moći i preusmjeravanje u savremenoj globalnoj politici. Prema navodima Amaan Charaniya (2024) detaljna analiza osnovnih uzroka sukoba između Rusije i Ukrajine otkriva da je glavni okidač spor oko granica i teritorija, koji u osnovi proizlazi iz nezadovoljstva država njihovim teritorijalnim rasporedom i željom za proširenjem domovine, što je ilustrovano ruskom invazijom na Ukrajinu osam godina nakon aneksije Krima u nastojanju da povrati izgubljenu zemlju.



Slika 1: Grafički prikaz globalnih trendova u međudržavnim sukobima i teritorijalnim sporovima, 1980-2020.

Izvor: https://saisreview.sais.jhu.edu/the-territorial-roots-of-interstate conflict/#:~:text=A%20close%20examination%20of%20the,desire%20to%20expand%20their%20homeland.

Empirijski nalazi prikazani na prvom grafiku ilustriraju prepoznatljiv uzorak. Od 1980. godine nadalje, postoji konzistentan pad udjela globalnih sukoba koji su kategorizirani kao međudržavni (u koje su uključene dvije države). Međutim, protekla decenija pokazuje obrnutu tendenciju, što ukazuje na porast sukoba između država. Istovremeno, drugi grafik pruža vizualnu reprezentaciju udjela globalnih sukoba koji su pod utjecajem teritorijalnih sporova. Kroz historiju, pitanja vezana za teritorij, zemlju i integritet granica kontinuirano su poticaj za sukobe. Ipak, od 2010. godine zabilježen je značajan porast učestalosti teritorijalnih sporova. Ovi dvostruki trendovi, analizirani od strane Amaana Charaniya (2024), zajedno sugeriraju oživljavanje dinamike međunarodnih sukoba, pri čemu teritorij postaje važan faktor koji motivira suvremene sporove.

Amaana Charaniya (2024) zaključuje da povratak međudržavnim sukobima, pri čemu je udio sukoba koji uključuju dvije ili više država, dostigao najvišu razinu u proteklih 15 godina. Međutim, okarakteriziranje tih ratova samo kao posljedica geopolitičkih rivaliteta ili etničkih tenzija zanemaruje temeljne uzroke sukoba. Kako bismo dublje razumjeli zašto države vode ratove i s nadom u smanjenje sukoba u budućnosti, važno je preispitati naš konceptualni okvir. Sukobi koji se pripisuju etno-religijskim razlikama ili neravnotežama moći često su manifestacije dubljih teritorijalnih sporova. Ti sporovi mogu obuhvatiti pitanja granica, zahtjeve za perifernim teritorijama ili veze s historijskim aspektima regionalnih odnosa (Charaniya, 2024).

Često teritorijalni sukobi mogu biti povezani s historijskim kontekstom i okolnostima pod kojima su granice povučene ili su definirane države. Historijski faktori i konkurentske ideje o teritoriji mogu izazvati izazove u suvremenim shvaćanjima države i dovesti do sukoba oko položaja granica ili prava na osporene zemlje. Bez obzira bila riječ o kolonijalnoj upravi ili natjecanju velikih sila, države često mogu navesti historijske nepravde kao motivaciju za svoju agresiju danas (Charaniya, 2024).

Kroz proteklo razdoblje, Rusija i Ukrajina održavale su bliske kulturne i historijske veze, proizašle iz njihove geografske blizine i trgovinskih veza (Kammer i sur., 2022; Lichterman, 2022). Unatoč ovoj vezi, Ukrajina je historijski priznata kao nezavisna država s vlastitim posebnim političkim sistemom odvojenim od Rusije. Međutim, dinamika se dramatično promijenila 24. februara 2022. godine, kada je ruska vlada odobrila ulazak vojnih snaga na teritorij Ukrajine (Ratten, 2023). Ovaj potez označio je početak potpunog vojnog napada na Ukrajinu, izazivajući značajnu globalnu zabrinutost ne samo zbog njegove smjelosti, već i

zbog posljedica na susjedne suverene države (Grossi i Vakulenko, 2022; Cai i sur., 2022). U sljedećem dijelu rada prikazat ćemo historijski aspekt i odnose između Rusije i Ukrajine koje se manifestiraju u suvremenoj dinamici sukoba.

4.2. Korijeni i dinamika sukoba

Početak trenutnog sukoba u Ukrajini dogodio se 24. februara 2022. godine, kada su ruske vojne snage ušle u zemlju iz Bjelorusije, Rusije i Krima. Ovaj događaj se odigrao usred osam godina prethodnog sukoba na istoku Ukrajine između snaga ukrajinske vlade i separatista koje podržava Rusija (Walker, 2023). Akcije koje je preduzela Ruska Federacija, predvođena Vladimirom Putinom, označavaju ponovni izlazak autoritarnih tendencija sličnih doba Staljinizma. Pokretanje sveobuhvatne vojne kampanje protiv susjedne države, Ukrajine, naglašava oslanjanje Rusije na fizičku prisilnu moć kao primarni instrument za proširenje svog uticaja i uspostavljanje dominacije (Hanappi, 2022). U nastavku ovog rada ćemo detaljno analizirati historiju i trenutni tijek sukoba između Rusije i Ukrajine, ističući posebno implikacije koje proizlaze iz ovog sukoba. Također, istražit ćemo geopolitičke aspekte ovog sukoba, kao i značajnu ulogu koju cyber tehnologija igra u njemu.

4.2.1. Pozadina sukoba

Od raspada Sovjetskog Saveza 1991. godine, odnos između Ukrajine i Rusije obilježavaju složene dinamike koje obuhvataju političke, ekonomske i sigurnosne dimenzije (Priyono, 2022; Demir, 2022). Ukrajinin put kao nezavisne države uglavnom se udaljio od usklađivanja s ruskim interesima, umjesto toga težeći bližim odnosima s Sjedinjenim Američkim Državama i Europskom unijom, što je doprinijelo napetostima između dvije zemlje, pri čemu Rusija često vidi Ukrajinu kao integralni dio svoje historijske, etničke i kulturne sfere (Demir, 2022). Opet, Rusija i Ukrajina su održavale bliske ekonomske veze. Rusija je ostala najveći trgovinski partner Ukrajine, a veći dio ukrajinske izvozne industrije bio je zasnovan na dobavi jeftine energije (plina) iz Rusije (Balmaceda, 2013). Demir (2022) dalje objašnjava da su države surađivale u aspektima koji se odnose na kontrolu nuklearnog oružja naslijeđenog od Sovjetskog Saveza, status Krimskog poluotoka, raspodjelu sredstava poput Crnomorske flote, sporazume o cijenama prirodnog plina i prava ruskih manjina koje žive na istoku Ukrajine.

Unatoč historijskim i kulturnim vezama između Ukrajine i Rusije, odnos je obilježen asimetrijom i sukobom, posebno u kontekstu natjecanja za geopolitičke aspiracije i različitih vizija za post-sovjetski prostor. Neriješeni sporovi i trajni sukobi naglašavaju složenost odnosa i izazove u postizanju stabilnosti i suradnje između dviju nacija (Demir, 2022). Jedan presudan događaj koji je značajno eskalirao napetosti bio je aneksija Krima od strane ruskih snaga u martu 2014. godine, nakon spornog lokalnog referenduma na kojem su Krimljani navodno izabrali da se pridruže Ruskoj Federaciji (Priyono, 2022).

Od samog početka postojanja nezavisne Ukrajine, nacionalni identitet bio je izgrađen na potpuno različitim društvenim stavovima. Osjećaj pripadnosti Ukrajini uglavnom su osjećali stanovnici zapadnih i centralnih regija (Demedziuk, 2017). Nacionalizam u Krimu ostao je skriven u populaciji sve do godina koje su prethodile izboru Victora Yanukovych 2010. godine, kada je političar pokrenuo opsežni projekt na poluotoku s ciljem mobilizacije etnički rusko i prorusko stanovništvo koje je naseljavalo regiju. Stoga je aktivirao političke segmente krimskog društva koji su imali smanjen utjecaj, koristeći složenu kombinaciju medijskih alata, političkih dogovora i drugih strategija, što je dovelo do promjene atmosfere među stanovnicima poluotoka u trenutku kada je ostvario uspjeh, a početak nove vlasti i usvajanje pomirljivog stava prema Rusiji bitno su izmijenili politički pejzaž Krima (Makio i Fuccille, 2023). Istovremeno, u Moskvi je kult ruske izuzetnosti i njezine manifestacije ojačan na poluotoku, te je porasla želja za ujedinjenjem s Ruskom Federacijom (Kuzio, 2014; Malinova, 2017). Identitet regije sve više se usklađivao s diskursom Kremlja o ruskoj izuzetnosti i postepeno se udaljavao od ukrajinskog identiteta. (Matsuzato, 2016) Stoga se godine demobilizacije separatističkih grupa mogu shvatiti kao početak događaja koji su rezultovali aneksijom 2014. godine (Makio i Fuccille, 2023).

Aneksija Krima predstavljala je akt opisan od strane Beblera (2015) kao hibridni rat, strateška kombinacija vojnih taktika i alternativnih sredstava s ciljem uspostavljanja dominacije, uključujući kontrolu medija, propagandu i širenje dezinformacija. Ruske akcije za stjecanje kontrole nad Krimom bile su potaknute izbijanjem antivladinih protesta poznatih kao Euromaidan[4] (Matzek, 2016). Bebler (2015) naglašava dugotrajne brige unutar Ukrajine zbog

[4] U novembru 2013. godine, Kijev je bio zauzet od strane demonstranata Euromajdana koji su izrazili nezadovoljstvo zbog obustave potpisivanja Sporazuma o asocijaciji s Europskom unijom (EU). Unatoč aktivnim naporima vlade da završi pregovore o sporazumu, Viktor Yanukovych (2010-2014) je naglo prekinuo pregovore. S obzirom na njegov pro-ruski politički stav, pojavile su se spekulacije o utjecaju Moskve na proces donošenja odluka. Kao rezultat toga, demonstranti su zagovarali jače veze s EU-om, s ciljem smanjenja ovisnosti Ukrajine o Rusiji (Makio i Fuccille, 2023).

mogućih napora Rusije za destabilizaciju, iako je primijetio period manjih napetosti nakon što je Victor Yanukovych izabran za predsjednika 2010. godine. Ipak, nakon što je Yanukovych pobjegao iz Ukrajine 22. februara 2014. godine, zemlja se našla u situaciji bez vlasti. Uslijedili su pro-ruski protesti u Simferopolu, glavnom gradu Krima, 26. februara. Sljedećeg dana, 27. februara, naoružane osobe nepoznatog identiteta preuzele su kontrolu nad vladinim zgradama na Krimu i postavile Sergeja Aksjonova, člana parlamenta i lidera partije Ruska Jedinstvo, za premijera. 28. februara, neoznačene vojne snage, kasnije prepoznate kao ruske (unatoč negiranju prisustva ruskih trupa od strane predsjednika Putina u više navrata, prema Bebleru (2015), zauzele su ključne lokacije na poluotoku, uključujući vojne objekte, aerodrome i medijske institucije, istovremeno blokirajući prometne rute koje povezuju Krim s Ukrajinom (Matzek, 2016).

Nakon aneksije Krima, održan je referendum 16. marta 2014 o njegovom odcjepljenju od Ukrajine i naknadnom uključivanju u Rusku Federaciju, u kojem je biračima bilo ponuđeno dvije opcije: podržati ponovno pripajanje Krima Rusiji kao subjektu Ruske Federacije ili podržati obnovu Ustava Republike Krima iz 1992. godine i zadržati status Krima kao dijela Ukrajine (Bebler, 2015). Međutim, legalitet referenduma bio je osporen, jer je kršio član 73 Ustava Ukrajine, koji propisuje da se pitanja o promjenama teritorije Ukrajine moraju rješavati isključivo putem sveukrajinskog referendum (FAO, 1996). Stoga je ukrajinska vlada odbila priznati njegovu pravnu valjanost. Unatoč kritikama vezanim uz tačnost odziva birača i rezultata, s prijavljenih 81,36% odaziva i podrškom od 96,77% birača za odcjepljenje, Krim je proglasio nezavisnost 17. marta 2014. godine i službeno je uključen u Rusiju sljedećeg dana, 18. marta 2014. godine (Matzek, 2016).

U periodu od 2015. do 2020. godine, na istoku Ukrajine, bili su česti smrtonosni sukobi između ukrajinskih snaga i proruskih separatista. Sukobi između ove dvije strane rezultirali su smrću više od 13.000 ljudi i raseljenjem 1,5 milijuna ljudi (Priyono, 2022). S ciljem suzbijanja sukoba, u aprilu 2016. godine NATO je poslao četiri bataljona u Istočnu Europu, rotirajući trupe kroz Estoniju, Latviju, Litvaniju i Poljsku kako bi odvratili moguću buduću rusku agresiju, posebno na Baltiku. Također, Sjedinjene Američke Države su u septembru 2017. godine poslale dvije oklopne brigade američke vojske u Poljsku kako bi ojačale prisustvo NATO-a u regionu. U januaru 2018. godine, Sjedinjene Američke Države su uvele nove sankcije pojedincima i kompanijama povezanim s sukobom na istoku Ukrajine, a u martu 2018. godine odobrile su prodaju protivtenkovskog naoružanja Ukrajini. Naknadno, u

oktobru 2018. godine, Ukrajina je sudjelovala u velikim vazdušnim vježbama s NATO zemljama na zapadu Ukrajine. Od oktobra 2021. godine, obavještajni podaci su ukazivali na nadolazeću rusku invaziju Ukrajine, što je navelo administraciju Joe Bidena da poboljša dijeljenje informacija s saveznicima, uključujući Ukrajinu, kako bi odvratila agresiju. Unatoč ruskom pozivu na prestanak vojnih aktivnosti u Istočnoj Europi i protivljenju proširenju NATO-a, Sjedinjene Američke Države i saveznici iz NATO-a ostali su čvrsti, prijeteći ozbiljnim sankcijama u odgovoru na bilo kakve agresivne akcije protiv Ukrajine (Center for Preventive Action, 2024).

Izbori za predsjednika Ukrajine 2019. godine označili su značajan trenutak s izborom Volodymyra Zelenskyya, čija je administracija stavila rješavanje trenutnog sukoba kao centralnu točku dnevnog reda. Kao rezultat toga, primjetni su bili značajni napretci: implementacija sporazuma o primirju 21. jula 2019. rezultirala je opipljivim smanjenjem nasilnih incidenata, što predstavlja odstupanje od prethodnih razina intenziteta sukoba. Također, uspješne inicijative o rasterećenju primijetile su se u tri ključne pilotske zone - Stanytsia Luhanska, Petrivske i Zolote - što označava značajan napredak prema naporima deeskalacije, te dopunske mjere koje su provedene 27. jula 2020. s ciljem jačanja primirja naglasile su kolektivnu posvećenost održavanju napora za izgradnju mira (France Diplomatie, 2022).

4.2.2. Trenutno stanje sukoba

Carl Von Clausewitz navodi da svako doba ima svoju "vrstu rata, svoje ograničavajuće uvjete i svoje posebne predrasude" (1976: 593). Alvin i Heidi Toffler (1993), u svojoj knjizi *War and anti-war: Making sense of today's global chaos*, predstavili su koncept tri vala civilizacije, koji direktno odgovaraju tri vala ratovanja. Njihova teorija razlikuje tri različite epohe u razvoju ljudskog društva: agrarno, industrijsko i doba informacija. Tvrdili su da je svaka epoha karakterizirana određenim skupom resursa koji potiču kako ekonomski prosperitet tako i vojne sukobe. U agrarnom dobu, životinje i rad su bili cijenjeni resursi, dok su strojevi i fosilna goriva postali ključni u industrijskom dobu. Prema Tofflerima, trenutno doba informacija stavlja naglasak na informacije kao primarni resurs. Stoga, ratovanje u ovoj eri nastojalo bi iskoristiti napredak u tehnologijama zasnovanim na informacijama kako bi se postigli politički i vojni ciljevi nacija (Toffler i Toffler, 1993).

U svom djelu *New dimension of war – conflict in Ukraine*, Sylvia Demedziuk (2017: 93) analizira karakteristike savremenih sukoba, često poznatih kao novi ratovi ili sukobi karakteristični za treći talas. Osnovne odlike ovih sukoba obuhvataju angažman ne-državnih aktera kao što su paravojne grupe i plaćenici pod kontrolom eksternih sila, što ukazuje na trend privatizacije ili denacionalizacije ratovanja. Uobičajeno je da ovi sukobi pokažu izraženu asimetriju, s neujednačenim snagama sukobljenih strana. Identifikacija protivnika, ciljeva i trajanja sukoba često predstavlja značajne izazove. Kulturni, etnički i vjerski faktori često su temeljni uzroci ovih sukoba. Ključni ciljevi u ovim sukobima često su strateška sredstva i institucije države, što može izazvati privremene ekonomske poremećaje poput fluktuacija u vrijednosti javnih kompanija. Civili često trpe najveće posljedice nasilja, a situacija se dodatno pogoršava nepovoljnim medijskim prikazima koji ciljaju na narušavanje međunarodnog ugleda neke zemlje. Nezakonite aktivnosti u cyber prostoru dodatno doprinose kompleksnosti ovih sukoba, koji često započinju kao unutrašnji sukobi prije nego što eskaliraju u međunarodne krize (Demedziuk, 2017: 94).

Shodno prema navedenim karakteristikama, možemo zaključiti da je sukob između Rusije i Ukrajine obilježen karakteristikama novog oblika ratovanja. Treći val rata dominiran je „psihološkim i informativnim propagandnim aspektima, kao i gerilskim snagama i operacijama koje vode male, specijalizirane grupe vojnika specijalnih snaga“ (Demedziuk, 2017:101).

Isto tako, možemo se vratiti na ukrajinsku krizu iz 2014. godine, kada je konflikt počeo pokazivati karakteristike hibridnog ratovanja koje obuhvata četiri ključna elementa: diplomatsko ratovanje usmjereno na razrješavanje postojećih državnih sporazuma i destabilizaciju saveza i država koje ne uživaju međunarodnu podršku; informacijsko ratovanje koje cilja kako na stanovništvo, tako i na međunarodnu zajednicu putem širenja lažnih narativa i dezinformacija; tajno i neatribuirano korištenje vojne sile za izvršavanje pritiska; te strategije ekonomskog ratovanja koje uključuju ucjene, sankcije i manipulaciju inflacijskim stopama (Jacuch, 2022: 157–180).

Ruska *posebna vojna operacija* je počela od 24. februara 2022. godine, iako su oružani sukobi trajali od 2014. godine (Ty, 2023). Ovaj konvencionalni pristup je predstavljao ofanzivnu operaciju sa naglaskom na kopnenu boru izvedenu u dvije faze — Faza I između 24. februara i 18. aprila, i Faza II od 18. aprila do današnjeg dana (Craisor-Constantin, 2023). Početkom 2023. godine, cilj posebne vojne operacije se promjeniosa osiguranja garantovane

zaštite suvereniteta i teritorijalnog integriteta Rusije na popularniju i konvencionalnu odbranu protiv mogućeg proširenja NATO-a na istok i suprotstavljanje takozvanom *Kolektivnom Zapadu* (Lupescu, 2023). Od početka invazije, konvencionalne operacije podržane su hibridnim akcijama, pojačane nuklearnom prijetnjom, cyber i informacijskim napadima, kao i iskorištavanjem, pojačavanjem i čak izazivanjem energetskih, humanitarnih i prehrambenih kriza (Craisor-Constantin, 2023).

Intenzitet sukoba se mijenjao na različitim prostornim područjima Ukrajine, pri čemu su početna tri mjeseca donijela široko rasprostranjeno uništavanje, a direktna oštećenja su brzo dostigla iznos od 97 milijardi američkih dolara (Himmelfarb, 2024; The World Bank, 2022). U drugoj polovini 2022. godine, Vlada Ukrajine je uspostavila kontrolu u spornim područjima, ograničila gubitak kontrole u drugim područjima te smanjila napredovanje ruskih snaga, čime je minimalizirala brzo eskaliranje šteta, iako su napadi na ključnu infrastrukturu u jesen i zimu 2022. godine rezultirali velikom štetom u sektoru energetike. Redovni intenzivni napadi na infrastrukturu nastavili su se tokom 2023. godine, sa nepredvidivim vazdušnim i dron napadima koji su se proširili izvan uspostavljenih i uglavnom nepomičnih zona sukoba, te su utjecali na gradove poput Kijeva, Odesa i Lviva. Uništavanje brane Kakhovka i hidroelektrane (HE) u junu 2023. godine rezultiralo je neizmjerivim uticajem na okoliš i pogoršalo izazove s kojima se već suočavaju ljudi koji se bore za pristup stanovanju, vodi, hrani i zdravstvenim uslugama, među ostalima. Također su zabeleženi ozbiljni napadi na luke, posebno u Odeskim i Mykolaivskim regijama i duž rijeke Dunav, kao i cyber napadi i intenzifikacija vazdušnih i dron napada u poslednjim mjesecima 2023. godine (Himmelfarb, 2024).

Početak invazije je obilježen cyber napadima usmjerenim na ukrajinsku vladinu administraciju i financijske sisteme, s ciljem smanjenja ili ograničavanja kapaciteta Ukrajine za efikasan odgovor i ometanje mobilizacije njenih snaga. Cyber-napadi su koristili osam različitih vrsta phishing softvera, koji su korišteni za blokiranje ključnih usluga i određenih vladinih web stranica (Lewis, 2022). Iako Rusija možda javno ne priznaje posjedovanje sposobnosti za cyber napade, aktivnosti u ovom operativnom području često su provođene od strane entiteta koji se često nazivaju nezavisni hakeri ili grupe hakera, često financirane od strane različitih ruskih sigurnosnih institucija. Ovi hakeri ili grupe su odgovorni za preko 2,000 takvih napada, uglavnom usmjerenih na jačanje Cyber Intelligence, s manjim brojem usmjerenih na podršku naporima ruske vojske (Bateman, 2022). Ovaj pristup proizlazi iz

perspektive Kremlja, koji smatra cyber napade kao olakšavajuće aktivnosti umjesto direktnih sredstava za postizanje strateških ciljeva (Craisor-Constantin, 2023).

Rastuća prisutnost ruskih cyber kriminalnih grupa evidentira iskorištavanje ratnog sukoba radi osobne financijske dobiti, uz istovremeno pružanje podrške ruskim političkim ciljevima. Ovaj angažman uključuje javno izražavanje podrške ruskom narodu i vladi, te širenje načina djelovanja na otvorene prijetnje izvođenja cyber operacija kao odgovor na percepirane napade na Rusiju ili kao reakciju na pružanje resursne podrške Ukrajini (Kaushik, 2023). Thomas Rid (2020) je izjavio da Rusija vodi drugačiju vrstu cyber ratovanja, s manje naglaska na rušenju ključne infrastrukture i više na ograničavanju koalicije koja podržava Ukrajinu, s ciljem zasijavanja kaosa i izazivanja sumnje i zabune na način koji je u skladu s naslijeđenim sovjetskim idejama o aktivnim mjerama i refleksivnoj kontroli. Ruski cyber operativci nastavljaju s izvođenjem manjih poremećaja protiv entiteta u njihovoj neposrednoj blizini, s fokusom na Ukrajinu i nacije koje su joj saveznici. Nedavni napad, organiziran od strane grupe Sandworm povezane s ruskom vojnom obavještajnom agencijom GRU, bio je usmjeren na Ukinform, nacionalnu novinsku agenciju Ukrajine, prelazeći na uklanjanje straha među civilnim stanovništvom u Ukrajini nakon što nisu uspjeli postići značajne rezultate kroz cyber operacije na bojnom polju (Vicens, 2023).

András Rácz, Ole Spillner and Guntram Wolff (2023) su naveli da stroge sankcije u tehnološkom sektoru, u kombinaciji s povlačenjem zapadnih visokotehnoloških kompanija, imale su konkretan utjecaj na ruske oružane snage. Rusija trenutno jedva može nadomjestiti gubitke vojnog materijala novoproizvedenim oružanim sistemima. Osim toga, na strukturnoj razini, sankcije koje su uvedene još 2014. oslabile su oružane snage. Od februara 2022. godine, sankcije protiv vojnih i dvojnih proizvoda značajno su pooštrene. I uprkos ponovljenim tvrdnjama o samodostatnosti, ruska odbrambena industrija ostaje snažno zavisna od dijelova i komponenti koje uvozi iz Zapada. Odlazak mnogih zapadnih visokotehnoloških kompanija stoga je zadavao veliki, do sada uglavnom nepopravljiv udarac ruskoj odbrambenoj industriji. Kao rezultat toga, od februara 2022. godine, Rusija se može osloniti samo na zapadne dijelove i komponente koje je unaprijed uskladištila, a ovi zalihi su ograničeni i opadaju (András, Ole i Guntram, 2023).

Philip Wasielewski (2023) smatra da je, trenutno, pažnja svijeta usmjerena na kontranutarni napad Ukrajine i njegov potencijal da promijeni strateški balans snaga u tekućem sukobu. Opservacije ukazuju da su ruske odbrambene strukture ometale napredovanje Ukrajine,

prvenstveno zbog njihove opsežne dubine, povoljne terene koji omogućavaju proširena polja vatre za vođene protuoklopne rakete, opsežnih minskih polja i relativno ograničenih resursa ukrajinskih borbenih inženjera. Ukrajinski vojni analitičari ističu da sposobnost Rusije da uspostavi ove odbrambene linije proizlazi iz ograničenih kapaciteta Ukrajine za udar na dugi rok, uključujući i sposobnosti raketa i zrakoplova, što otežava napore za rušenje ruskih utvrda. Strateška rasprava unutar ukrajinske vojske u prethodnoj zimi odnosila se na trenutak južnog napredovanja, raspravljajući o tome treba li promptno rasporediti dostupne snage ili pričekati uspostavu novih jedinica opremljenih zapadnom vojnom tehnologijom. Na kraju, odlučeno je da će se preferirati drugi pristup. Trenutno, ukrajinske vojne snage pokušavaju otkriti slabe točke u odbrambenim položajima i proboje sukcesivne linije, kako bi se mehaničke rezerve smjestile iza ruskih linija i prekinule komunikacijske veze prema Krimu (Wasielewski, 2023).

4.3. Implikacije za međunarodnu sigurnost

Sukob između Rusije i Ukrajine proizlazi iz percepcije Rusije o smanjenju njenog uticaja i statusa u globalnom geopolitičkom pejzažu, posebno zbog prijetnji od zapadnih sila, koje uključuju akcije poput proširenja NATO-a, smatrane od strane Rusija kao pokušaj podrivanja njenih ekonomskih, vojnih i diplomatskih sposobnosti. Taylor (2021) ovaj sukob karakteriše kao igru nulte sume, u kojoj svaki dobitak jedne strane dolazi direktno na štetu druge. Eskalacija vojnih akcija Rusije protiv Ukrajine pokazuje njen cilj da afirmiše dominaciju, iako uz značajan trošak. Kao rezultat toga, ova kriza ima dugoročne implikacije, utječući ne samo na političku i ekonomsku stabilnost uključenih zemalja, Rusije i Ukrajine, već postavlja i izazove za mirno suživot i međunarodne odnose širom svijeta (Taylor, 2021).

Nivedita Das Kundu i Taimur Khan (2023) navode da od početka ovog sukoba, svijet je svjedok ponovnog uspona blokovske politike, s velikom konkurencijom moćnih sila koja se manifestira na različitim dijelovima globusa, pri čemu su zemlje prisiljene odabrati jednu ili drugu stranu. Ova podijeljenost proizlazi iz činjenice da Rusija ucjenjuje svijet kroz mogućnost globalne gladi i nestašice energije, te otvoreno zastrašuje međunarodnu zajednicu prijetnjama eskalacije nuklearnog rata (Reznikov, 2022). Rozmeri A. Dikarlo je na Vijeću Sigurnosti UN-a izjavila da je sukob rezultirao humanitarnom katastrofom i kršenjem ljudskih prava, ubrzao globalne krize hrane i energije, te oslabio međunarodni sistem kolektivne sigurnosti na koji su se države članice obvezali održavati (The United Nations,

2023). Ipak, najalarmantnija posljedica sukoba između Rusije i Ukrajine leži u reorijentaciji globalnog sigurnosnog poretka prema tradicionalnom konceptu, koji je uspostavljen nakon Drugog svjetskog rata, a karakteriziraju ga vojne akcije, savezi, sporazumi, trke u naoružanju, masovna vojno-industrijska proizvodnja i značajni vojni budžeti (Nivedita i Taimur, 2023).

Nuklearno oružje ima značajnu ulogu u ovom sukobu, iako Rusija nije direktno koristila nuklearno oružje u borbama. Ipak, aktivno i javno je koristila svoje nuklearno oružje u kampanji uticaja s ciljem destabilizacije NATO saveza i prinude njegove lidere na pasivnost i prihvatanje novog statusa quo (Kehler, 2023). Edward A. Kolodziej je za intervju sa Phil Ciciora (2022) izjavio da Putinova invazija automatski podiže mogućnost eskalacije nuklearnog sukoba u vojni sukob između zapadnih saveznika i Rusije, pri čemu je uključeno nekoliko nuklearnih sila poput SAD-a, Rusije, Velike Britanije i Francuske. Shodno tome, možemo zaključiti da potencijalna nuklearna eskalacija se proširuje izvan granica Ukrajine i posljedično predstavlja sigurnosnu prijetnju na globalnom opsegu (Ciciora, 2022).

Ova kampanja uticaja započela je prije same invazije, te je obilježena je dugotrajnim ulaganjem Rusije u modernizaciju i razvoj novih nuklearnih sposobnosti, što je postalo prepoznatljivo obilježje Putinovog vladanja. Putin je osobno sudjelovao u visoko vidljivim nuklearnim vježbama, nadgledao je testiranja sistema za dostavu nuklearnog oružja te odobrio novu rusku nuklearnu doktrinu koja predviđa potencijalnu upotrebu, uključujući i moguće prvo korištenje, nuklearnog oružja kako bi se izdejstvovao ishod regionalnih sukoba u korist Rusije (Kehler, 2023). Hans M. Kristensen i suradnici (2023) u svom izvještaju *Russian nuclear weapons, 2023* navode da je ruski program modernizacije nuklearnog arsenala izgleda motiviran djelomično snažnom željom Kremlja da održi opću jednakost s Sjedinjenim Američkim Državama i da sačuva nacionalni prestiž, ali i da nadoknadi inferiornost konvencionalnih snaga, kao i uvjerenjem ruskih lidera da američki sistem protivraketne odbrane predstavlja stvarni budući rizik za vjerodostojnost Rusijeve osvete. Slaba izvedba ruskih konvencionalnih snaga u ratu protiv Ukrajine i iscrpljenost zaliha oružja vjerovatno će produbiti oslanjanje Rusije na nuklearno oružje za svoju nacionalnu odbranu (Krinstensen i sur., 2023).

Trenutni sukob između Rusije i Ukrajine je ponovno usmjerio pažnju na pitanja odbrane, što je dovelo do toga da NATO i Sjedinjene Američke Države ponovno preuzmu prominentne uloge kao garanti sigurnosti u regiji (Abrams, 2923). Prema podacima koje je pružio Stockholmski međunarodni institut za istraživanje mira/ *the Stockholm International Peace*

Research Institute (2024: para. 1), ukupna globalna vojna potrošnja dosegnula je 2443 milijarde dolara u 2023. godini, što predstavlja povećanje od 6,8 posto u stvarnim terminima u odnosu na 2022. godinu, s Sjedinjenim Američkim Državama na prvom mjestu. Iako Europska unija (EU) nije bila bez značaja, primjetno je doprinijela koordinacijom europskih reakcija i dodjelom financijske pomoći Ukrajini, ali povijesni trendovi od 1945. godine i dalje pokazuju ovisnost Zapadne Europe o podršci NATO-a i Američke odbrane (Abrams, 2023).

Pretežne argumentacije ukazuju na to da je američka intervencija bila ključna u sprječavanju neizbježnog poraza Ukrajine. Bez diplomatskog i vojnog angažmana, procjenjuje se da bi obrambena sposobnost Ukrajine trajala samo ograničeno vrijeme, procijenjeno na približno mjesec dana (Zadorožna, 2023). Krajem aprila 2024. godine, Zastupnički dom Sjedinjenih Američkih Država odobrio je paket strane pomoći u iznosu od 95 milijardi dolara, od čega je otprilike 61 milijarda dolara dodijeljena pomoći Ukrajini (Yang, 2024). Od ruske invazije na Ukrajinu u februaru 2022. godine, Sjedinjene Američke Države su zadržale status glavnog donatora pomoći Ukrajini, pružajući kumulativno 113 milijardi dolara, koje obuhvata financijsku pomoć, vojnu opremu, strojeve i humanitarnu pomoć (Kulakevich, 2024). Mark F. Cancian i Chris H. Park (2024) navode da paket u najvećem dijelu, u iznosu od 25,7 milijardi dolara, namijenjen je pružanju vojne opreme Ukrajini. To služi tri osnovne svrhe: zamjena opreme koja je prethodno ili trenutno opskrbljena putem predsjedničkog ovlasti smanjenja, pružanje financiranja putem programa Stranog vojnog finansiranja State Departmenta i unapređenje industrijske osnove odbrane radi povećanja proizvodnih sposobnosti i razvoja naprednog naoružanja (Cancian i Park, 2024).

Kao što smo već spomenuli, sukob u Ukrajini predstavlja razdvaja postojeći globalni poredak čime se narušava mogućnost održivog mirnog i kooperativnog globalnog uređenja. Ponovni uspon uskog nacionalnog sigurnosnog interesa i geopolitičkih aspiracija pojedinih država ističe primat ovih faktora nad globalnim mirom i sigurnošću (Greminger i Vestner, 2022). Podjela međunarodne zajednice na dva antagonistička politička bloka podsjeća na bipolarni svijet i mogući novi iron curtain između Evrope i Azije. Kao rezultat, stvorena su dva politička bloka, koji podržavaju različite frakcije u Ukrajini. Dok jedan blok obuhvata SAD, zapadne demokratije, NATO, EU, G7 članice i druge demokratije širom svijeta, drugi blok, kao produžetak BRICS-a, uključuje dodatne članice G20 koje nastoje uspostaviti azijski

NATO, konkurentsku monetarnu rezervu i moguću zajedničku crypto valutu (Craisor-Constantin, 2023).

4.4. Geopolitički aspekti sukoba

S geopolitičke perspektive, Heartland teorija Halforda Mackindera fokusira se na Heartland kao ključni korak prema potencijalnoj svjetskoj dominaciji, sugerirajući da bi, ako bi zemlja, federacija ili blok mogli dominirati ovom regijom i proširiti svoj utjecaj na obale Euroazije dok kontrolišu ključne trgovinske rute, moglo doći do nastanka globalnog carstva. Mackinder isto tako ističe značaj središnjih europskih zemalja i onih koje okružuju Baltičko i Crno more, tvrdeći da kontrola nad Istočnom Europom znači vladavinu nad Heartlandom, a vladavina nad Heartlandom vodi do dominacije nad svjetskim ostrvom. Konačno, ko god vlada svjetskim ostrvom, vlada svijetom(Ismailov i Papava, 2010). Prema navodima Al-Hasnawi (2022) zbog svoje lokacije u istočnoj Evropi i kao sastavni dijelovi Heartlanda, Ukrajina i ostale bivše sovjetske zemlje postale su žarišta geopolitičke konkurencije između glavnih sila, posebno Sjedinjenih Američkih Država na zapadu i Rusije na istoku, što je navelo Moskvu da odlučno reaguje na proširenje NATO-a u region i sukob u Ukrajini, s ciljem jačanja svoje vojne moći, što uključuje jačanje vojne prisutnosti, poput raspoređivanja flota na Crnom i Sredozemnom moru (Al-Hasnawi, 2022).

Prema teoriji pomorske moći Alfreda Thayera Mahana, status neke države kao globalne sile ovisi o snazi i adekvatnosti njenih pomorskih snaga, ključnih za projektovanje uticaja širom svijeta. Mahan tvrdi da bi pomorska moć trebala primarno težiti dominaciji nad morskim rutama (Iliopoulos, 2009). S aspekta Rusije, promjena u ukrajinskoj vladi od Janukoviča do Porošenka posmatra se kao napor da se ograniči Rusija u korištenju Crnomorske regije radi afirmacije svoje pomorske snage. Putinov odgovor na ukrajinska zbivanja bio je defanzivan umjesto ofanzivan, pokretan dugoročnim strateškim ciljem osiguravanja pristupa toplim morima. Prema ovoj interpretaciji od strane Al-Hasmawi (2022), Sjedinjene Američke Države nastoje ometati ruske ambicije podržavajući i anti-ruske i pro-ruske frakcije unutar Ukrajine kao dio šire strateške manevarske igre kako bi se opkolilo područje. Značaj ruske pomorske baze u Sevastopolju, na Krimu, kao oslonca za povezivanje ruskog Crnomorskog flote s Mediteranom, ističe odlučnost Putina u suprotstavljanju bilo kakvoj prozapadnoj ukrajinskoj vladi u Kijevu koja bi mogla ugroziti ruske vojne interese. Brza aneksija Krima 2014. godine služila je kao odlučno upozorenje ukrajinskoj vladi, ali kada je ocijenjeno kao

nedovoljno prisilno, Rusija je eskalirala svoj odgovor zagovarajući autonomiju Donbasa i Donjecka, što je dovelo do konačne invazije Ukrajine od strane ruskih vojnih jedinica 2022. godine (Al-Hasnawi, 2022).

Rusija analizira Ukrajinu iz različitih perspektiva, uključujući prvobitno kao strateško sredstvo, koje djeluje kao historijska prepreka protiv neprijateljskih napada. Ukrajina se percipira kao geopolitička granicu između zapadnih sila, koje predstavljaju Sjedinjene Američke Države i Europsku uniju, i istočnih sila, koje simbolizira Rusija. Ova geopolitička uloga kao prepreka sprječava direktni sukob između ovih ključnih aktera, odvajajući zapadni blok, uključujući NATO, od ruskih utjecaja (Al-Hasnawi, 2022). Također, prema navodima Demir (2022: 21) Rusija smatra da je proširenje NATO-a prema istoku egzistencijalna prijetnja, videći Ukrajinu kao ključnu zonu odvajanja između Zapada i sebe. Nakon odluke NATO-a o mogućem članstvu Gruzije i Ukrajine na summitu u Bukureštu 2008. godine, Rusija je shvatila ovaj korak kao uznemirujuću prijetnju svojoj nacionalnoj sigurnosti (Demir, 2022). Rutland (2015) navodi da Ukrajina djeluje kao posrednik u kulturi, olakšavajući tranzit ruskih energetskih resursa, posebno prirodnog plina, prema Europskoj uniji, koja ima velike energetske potrebe. Ova geoekonomska perspektiva, istaknuta od strane Al-Hasnawi (2022), naglašava ključnu ulogu Ukrajine u transportu vitalnih resursa kako na domaćem tako i na europskom tržištu, te eventualna integracija Ukrajine u Europsku uniju mogla bi predstavljati izazov za inicijativu Euroazijske ekonomske unije koju vodi predsjednik Putin. Također, Center for Strategic & Regional Studies (2022) navodi da je, uzajamno, Ukrajina djelovala kao odbrambeni bedem za Rusiju protiv zapadnih prodora, a ovaj položaj bi mogao biti ugrožen eventualnim pristupom Ukrajine NATO-u, kao što je bio slučaj s rušenjem Berlinskog zida. Na kraju, uzimajući u obzir predviđanja Huntingona (1993) o sukobu između zapadne i ruske civilizacije, postoji rasprava o civilizacijskoj pripadnosti Ukrajine i mogućnosti civilizacijskog raskola, što se manifestira u trenutnom sukobu.

Prije izbijanja sukoba u Ukrajini, bilo je očigledno da trenutni globalni sistem upravljanja teško uspijeva odgovoriti na izazove koje donosi povezani, međuzavisni i visoko digitalizirani svijet 21. Stoljeća (Lewis, 2022). Nedostatak jasno definiranih normi za odgovorno ponašanje oslabljuje vladavinu prava, dok nedostatak međunarodne suradnje, što je vidljivo u trenutnom konfliktu, doprinosi postupnom raskidanju regionalnih i globalnih saveza. (Lewis, 2022:3) Sukob u Ukrajini ne samo što predstavlja kulminaciju postupnog

pogoršanja odnosa između Zapada i Rusije, već također razotkriva konkurentne napetosti i različite interese unutar saveza poput NATO-a (Kraemer i Otarashvili, 2014). Iako europski dužnosnici općenito smatraju da je njihov odnos s Rusijom trajno narušen, umjesto da prihvate sveobuhvatni pristup poput Sjedinjenih Američkih Država, preferiraju osmisliti odgovor temeljen na budućim koracima Rusije (Pezard i sur., 2017). U proteklim godinama, Rusija se usmjerila na sprječavanje integracije zemalja koje su nekada bile pod sovjetskim utjecajem u EU i NATO, istovremeno jačajući svoju prisutnost u Srednjoj Aziji i razvijajući odnose s Kinom (Kraemer i Otarashvili, 2014). Invazija Ukrajine predstavlja odgovor na ovaj postupni promjenu statusa te zemlje – od zone pritiska do aspirantice za članstvo u EU i NATO-u – i služi kao upozorenje susjednim državama o ekonomskom, energetskom i geopolitičkom utjecaju Rusije na njih (Falk, 2022; BBC, 2022).

Eskalirajući sukobi između zapadnih zemalja i i Rusije i Kine uključuju nekoliko ključnih elemenata. Prvo, ekonomska borba ističe se kao primarni aspekt, ilustrirana nastojanjima Zapada da potkopa rusku ekonomiju kao odgovor na ukrajinsku invaziju, uključujući niz finansijskih mjera poput uvođenja sankcija protiv vladinih zvaničnika, zamrzavanje rezervi Ruske centralne banke, pokretanje širokih kampanja bojkota trgovine i investicija i izbacivanje Rusije iz SWIFT bankarskog sistema (Polyakova i sur., 2022; Al-Rodhan, 2022). Drugo, energetska sigurnost ističe se kao značajan problem, s obzirom na dugogodišnju zavisnost Evrope od ruskih energetskih izvora, što ju je učinilo ranjivom na manipulaciju i odmazdu sa obje strane (Polyakova i sur., 2022). Na primjer, Rusija je odgovorila na zapadne sankcije prekidom isporuke gasa određenim evropskim zemljama, što je navelo EU da obeća da će prestati uvoziti energiju iz Rusije (Al-Rodhan, 2022). Treće, ideologija i dezinformacije igraju ključnu ulogu u sukobu, u kojem i Rusija i Zapad se bave nacionalističkom propagandom i informacijskim ratom, prikazujući jedni druge kao ideološke protivnike (Polyakova i sur., 2022; Al-Rodhan, 2022; Al-Hasnawi, 2022).

Države Zapada sve više klize ka direktnom sukobu s Kinom, trend koji je naglašen trenutnim sukobom u Ukrajini, što je povećalo ekonomski i politički uticaj Kine (Albin, 2022). Ovaj trend je vidljiv i unutar BRICS okvira (koji se sastoji od Brazila, Rusije, Indije, Kine i Južne Afrike) i u pristupu Kine prema zapadnim nacijama. Osim toga, sukob je privremeno skrenuo pažnju s rastuće asertivnosti Kine u Indo-Pacifičkoj regiji (Albin, 2022; Al-Rodhan, 2022). Također, olakšao je širenje trgovinskih i energetskih saveza između Rusije i Kine, kao i između Kine i nekoliko srednjeazijskih zemalja, čime je ublažio negativne posljedice

ukrajinskog sukoba na sino-evropske odnose (Albin, 2022; Al-Rodhan, 2022). Iako Europska unija ostaje ključni trgovinski partner Kine, kinesko odbijanje podrške zapadnim sankcijama protiv Rusije dodatno je pojačalo tenzije između ova dva entiteta (Albin, 2022). Unutar kineskih intelektualnih krugova postoji općeniti konsenzus o percepciji Sjedinjenih Američkih Država kao primarnog izvora globalne nestabilnosti, pri čemu se američka vanjska politika prikazuje kao katalizator globalnog haosa (Bachulska i Leonard, 2023). Sukob u Ukrajini dodatno je konsolidirao i proširio ovu percepciju Sjedinjenih Američkih Država na aktere koji aktivno surađuju s Kinom.

4.5. Uloga cyber tehnologije

Cyber operacije koje se pripisuju Moskvi oblikovane su širim geopolitičkim razmatranjima i utjecajem ruskih vojnih, obavještajnih i političkih institucija. Ove operacije se uklapaju u evoluirajuću strategiju Moskve za asimetričnu međudržavnu konkurenciju, koja ima za cilj izbjegavanje sveobuhvatnog sukoba (Lilly i Cheravitch, 2020). Tokom posljednje dvije decenije, rusko rukovodstvo je fundamentalno revidiralo svoje razumijevanje ratovanja, sada uključujući kako oružano nasilje, tako i nemilitantne mjere (Chekinov i Bogdanov, 2015; Jonsson, 2019). Razumijevanje perspektive Rusije o ratovanju je ključno za shvatanje njene cyber strategije.

Ruski pristup cyber sigurnosti usko je povezan s njihovim evoluirajućim razumijevanjem ratovanja i pojmom informacijskog ratovanja. U ruskom diskursu, cyber sigurnost često se smatra zapadnom idejom, suprotstavljajući se ruskom pojmu informacijska sigurnost („informatsionnaya bezopastnost“) (Lilly i Cheravitch, 2020:133). Lily i Cheravitch (2020) navode da iako se definicije informacijskog ratovanja i informacijske sigurnosti malo razlikuju među vojnim stručnjacima i službenim dokumentima, općenito se slaže da informacijska sigurnost spada u područje informacijskog ratovanja. Ovaj koncept obuhvata kako tehničke tako i psihološke komponente. Informacijsko ratovanje teži postizanju informacijske dominacije nad protivnicima kroz tehničke i psihološke strategije, dok cyber operacije služe kao alati koje države koriste za kontrolu informacijskog okruženja, koje se prepoznaje kao domena ratovanja (Thomas, 2019; Connell i Vogler, 2017). Godine 2011., Ministarstvo odbrane Ruske Federacije definisalo je informacijsko ratovanje kao sukob između dvije ili više država u informacijskom prostoru, koje uključuje oštećenje informacionih sistema, procesa i resursa, kao i krucijalnih i drugih struktura. Cilj je

podrivanje političkih, ekonomskih i socijalnih sistema, psihološko manipulisanje populacijom radi destabilizacije države i društva te prisiljavanje države da donese odluke koje idu na korist suprotnoj strani (Ministry of Defense of the Russian Federation, 2011).

Područje informacija i koncept informacijskog ratovanja usklađeni su s evoluirajućim shvaćanjem rata u Rusiji. General Gerasimov istaknuo je da informacijsko područje, bez jasnih nacionalnih granica, omogućava daljinski i tajni utjecaj na ključnu infrastrukturu i populaciju, što direktno utječe na nacionalnu sigurnost. Istaknuo je važnost proučavanja pripreme i provođenja informacijskih aktivnosti kao ključnog zadatka vojne znanosti (Gerasimov, 2019). Zbog svoje raznovrsne i nekonvencionalne prirode, informacijsko ratovanje, uključujući i cyber operacije, može započeti prije službenog proglašenja rata i postići političke ciljeve bez uključivanja konvencionalne vojne sile (President of Russia, 2010).

Ruski vojni stručnjaci istakli su razorne sposobnosti i prilagodljivost cyber oružja, koje može ciljati civilne, vojne i vladine sektore. U skladu s ruskom doktrinarnom perspektivom informacijskog ratovanja, stručnjaci tvrde da cyber oružje utječe i na infrastrukturu i na psihologiju(Lilly i Cheravitch, 2020). Bazylev i suradnici (2012) ističu da cyber oružje može kritično utjecati na transportne i energetske objekte, potencijalno izazivajući financijske krize. Kiselev i Kostenko (2015) objašnjavaju da cyber oružje ugrožava ključne elemente infrastrukture poput SCADA[5] sistema i vojnih sistema. Tijekom sukoba, ovo oružje može onesposobiti infrastrukturu za kontrolu neprijatelja, a viši stupnjevi automatizacije povećavaju ranjivost i utjecaj (Starodubtsev i sur., 2012; Kuznetsov i sur., 2018). Osim tehnoloških učinaka, cyber oružje može poremetiti državnu i vojnu administraciju, demoralizirati populaciju i izazvati masovnu paniku Bazylev i sur., 2012). Još jedna percepcija cyber oružja koju ističu stručnjaci je relativno niska cijena u odnosu na tradicionalno oružje, uz postizanje usporedivih razina štete (Parshin i Bashkirov, 2019; Romashkina i Kildobskiy, 2015).

Implementacija cyber napada i operacija u mirnodopskim uvjetima i oružanim sukobima danas predstavlja stvarnost. Februarska invazija Ukrajine 2022. godine, izvedena od strane

[5] 5 Sistemi za nadzor i akviziciju podataka/ Supervisory Control and Data Acquisition (SCADA) koriste se za kontrolu, praćenje i analizu industrijskih uređaja i procesa. Ovaj sistem obuhvata softverske i hardverske komponente te omogućava prikupljanje podataka sa industrijske opreme na daljinu i na licu mjesta. SCADA sistem se sastoji od tri glavne komponente, koje zajedno osiguravaju prijenos podataka sa opreme koja se nadzire i kontrolira (senzori, motori, itd.) do sučelja gdje se podaci mogu analizirati i koristiti za izvještavanje (SCADA International, 2024).

ruskih oružanih snaga, bila je praćena destruktivnim cyber napadima, što jasno ilustrira ovaj trend. Firdini, Urbanus i Syaiful (2023) ukazuju na to da nakon neuspjelih pregovora između Rusije, Ukrajine, NATO-a i zemalja EU 13. januara 2022. godine, Rusija je pokrenula destruktivne napade koristeći wiper WhisperGate. Ovaj wiper je imao za cilj brisanje hard diskova i onesposobljavanje računara u vladi i privatnim IT sistemima (Urbanus i Syaiful, 2023). Također, Rusija je ciljala usluge web stranica ukrajinske vlade. Neposredno prije početka rata 23. februara 2022. godine, frakcija unutar ruske Agencije vojne obavještajne službe, poznate kao GRU, pokrenula je još jedan program nazvan FoxBlade[6] istovremeno na više mreža ukrajinske vlade i vojske (Orenstein, 2022).

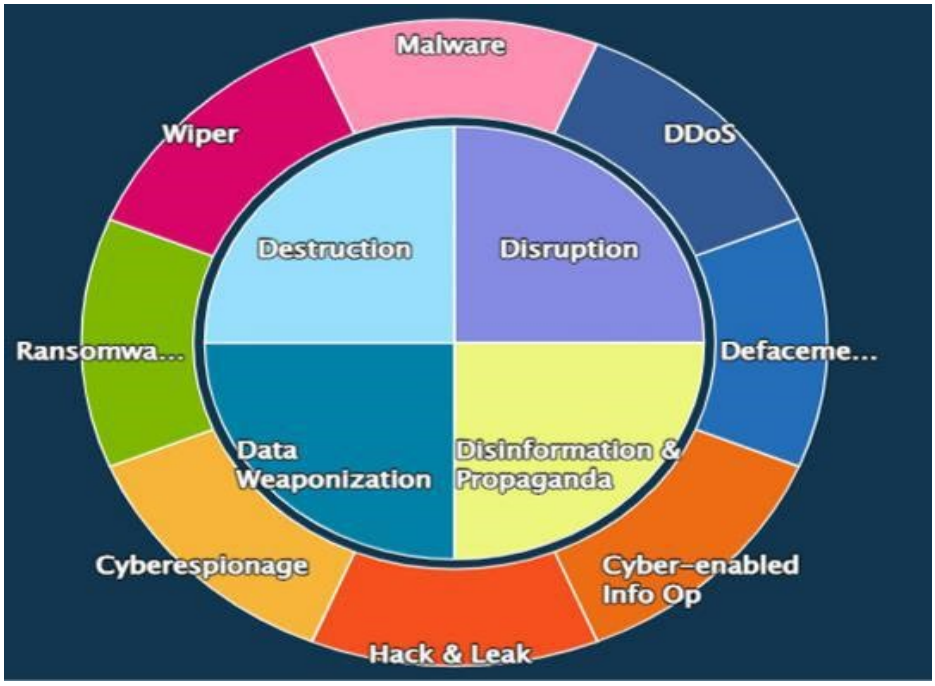
Korištenje cyber napada kao sredstva ratovanja zabilježeno je i ranije između država kao što su Ruska Federacija i Gruzija, Izrael i Iran, te Ruska Federacija i Ukrajina, pri čemu Rusija koristi cyber napade protiv Ukrajine od 2014. godine. CyberPeace Institut dokumentira cyber napade na kritičnu infrastrukturu i civilne objekte od početka ruskog agresorskog rata protiv Ukrajine, doprinoseći analizi upotrebe cyber sredstava u ratnim uvjetima. Do decembra 2023. godine, Institut je zabilježio „3255 cyber napada i operacija koje su izvršila 126 različita aktera“ (Cyber Peace Institute, 202:3). Ovi cyber incidenti su ciljali 23 različita sektora kritične infrastrukture, pogađajući Ukrajinu, Rusku Federaciju i otprilike 49 drugih zemalja (CyberPeace Institut, 2023:3).

Maschmeyer (2024) ukazuje na to da rat između Rusije i Ukrajine predstavlja prvi primjer cyber sukoba u velikom vojnom sukobu u kojem sudjeluje velika sila. Hakerske grupe sponzorisane od strane Rusije prilagodile su svoje metode ovom ratnom kontekstu. Iako je većina cyber operacija bila strateški nebitna, postoje značajni izuzeci kao što su operacija AcidRain, poremećaj UKRTelecoma, sabotaža elektroenergetske mreže u septembru 2022. godine i ozbiljan prekid rada Kyivstara 2023. godine, što ukazuje na to da hakerske grupe sve više kombiniraju cyber operacije s tradicionalnim subverzivnim metodama kako bi povećale svoju efikasnost (Maschmeyer, 2024). Nadovezujući se na argument, Pytlak (2024) je istakla cyber napad na KA-SAT satelit kompanije Viasat Inc. koji je poremetio mrežnu povezanost u Ukrajini, Francuskoj i Njemačkoj, što je izazvalo zabrinutost zbog cyber prelijevanja u zemlje koje nisu u sukobu i istaklo povezanost cyber sigurnosti i prostorne sigurnosti. Na

[6] 6 Malware spomenut u tekstu funkcioniše kao trojanac koji tajno iskorištava računare žrtava za učešće u napadima distribuirane uskraćenosti usluge (DDoS). Napadi uskraćenosti usluge (DoS) su zlonamjerni pokušaji gdje napadač ometa mrežno povezane hostove preplavljujući ih sa prekomjernim zahtjevima, s ciljem da onemogući pristup individualnim ili mrežnim resursima. DDoS napadi funkcionišu po sličnom principu, ali uključuju saobraćaj koji dolazi iz više izvora, što otežava napore za njihovo suzbijanje (Constantinescu, 2022).

početku sukoba, Ukrajina je mobilizirala globalnu IT vojsku, što je postavilo pravna pitanja o ulozi pojedinaca i privatnog sektora u ratovanju. Pored toga, otkrića o cyber operacijama povezanim s Rusijom protiv ukrajinskih ciljeva i saveznika prije invazije povećala su očekivanja o revoluciji u ratovanju vođenoj cyber tehnologijama i umjetnom inteligencijom (Pytlak, 2024).

Taylor Grossman, Monica Kaminska, James Shires i Max Smeets (2023:11) su u svom izvještaju *The Cyber Dimensions of the Russia-Ukraine War* identificirali nekoliko različitih faza cyber operacija u Ukrajini. U početku, prije nego što je Rusija započela svoju veliku invaziju 24. februara, Rusija se prvenstveno bavila cyber špijunažom kako bi strateški pozicionirala svoje snage za nadolazeće cyber napade. Tokom tog perioda, Rusija je rasporedila HermeticWiper protiv ukrajinskih vladinih agencija i banaka. Na dan invazije, cyber napad onesposobio je Viasat KA-SAT modeme u Ukrajini, što je dovelo do prelijevanja efekata koji su poremetili rad vjetroturbina u Njemačkoj i izazvali prekide u Velikoj Britaniji, Francuskoj i drugim zemljama. Na početku pune invazije, u ukrajinske mreže uvedeni su brojni wiper programi, što je ukazivalo na rusku namjeru da poremeti normalne vladine operacije, posebno ciljanjem energetske infrastrukture. Ova faza je uključivala raspoređivanje Industroyer2, ažurirane verzije malwarea koji je prethodno korišten protiv ukrajinske električne mreže 2016. Godine (Grossman i sur., 2023:11). Između maja i septembra, ruske cyber aktivnosti preusmjerile su se na špijunažu, s ciljem uspostavljanja pristupa strateški značajnim mrežama. Tokom ovog perioda, destruktivni napadi su bili relativno rijetki, pri čemu je CaddyWiper bio najčešće korišten wiper. CaddyWiper se odlikuje svojom lakoćom, jednostavnošću i lakom mogućnošću prilagođavanja, obično se širi putem Microsoft grupnih administrativnih postavki (Grossman i sur., 2023:11). Od oktobra do kraja 2022. godine, došlo je do ponovnog porasta destruktivnih cyber napada, s primjetnim povećanjem upotrebe wiper programa. Ove faze uglavnom odgovaraju širim fazama ruske cyber kampanje u Ukrajini, gdje su cyber operacije, cyber špijunaža i informacione operacije na različite načine podržavale cyber aktivnosti (Grossman i sur., 2023).



Slika 2: : Dominantne prijetnje uočene u kontekstu rata.
Izvor:**https://cyberconflicts.cyberpeaceinstitute.org/threats**

Prema analizi CyberPeace Institute (2023) u okviru ovog sukoba, ističe se osam glavnih cyber prijetnji koje su ponekad imale za cilj uništavanje, poremećaj, dezinformaciju i oružanje podacima. Malware obuhvata različite vrste invazivnog ili zlonamjernog softvera dizajniranog za oštećenje, uništavanje ili izobličavanje računalnih sistema, što uključuje wipere, ransomware i spyware. Napad distribuiranog uskraćivanja servisa (DDoS) podrazumijeva preplavljivanje mreže, usluge ili servera prekomjernim prometom kako bi se onemogućilo normalno funkcioniranje, a često je distribuiran od strane više računalnih sistema. U kontekstu oružanog sukoba, DDoS napadi su korišteni kako bi se poremetio pristup informacijama, financijama i čak humanitarnoj pomoći (Cyber Peace Institute, 2023:4). Defacement uključuje izmjenu sadržaja na internim ili javno dostupnim sistemima (obično web stranicama), posebno onih koje su u vlasništvu institucija vlade, kako bi se proširile dezinformacije ili propagandne poruke, utječući na javno mišljenje tijekom rata (Cyber Peace Institute, 2023:8). Hakiranje i curenje podataka podrazumijeva krađu i curenje podataka iz političkih ili ideoloških razloga, a često se ti procurjeni podaci manipuliraju kako bi se proširile dezinformacije. U kontekstu sukoba, krađa i curenje podataka (uključujući doxxing) često su izvršeni od strane takozvanih hakivističkih kolektiva, što dovodi do širenja nepovjerenja, pokazujući nesposobnost zaštite osjetljivih podataka i potencijalno dovodeći pojedince u opasnost (Cyber Peace Institute, 2023:16). Cyber špijunaža podrazumijeva prodiranje u sisteme i izvlačenje podataka kako bi se dobile povjerljive informacije o cilju, a

državni akteri su je koristili kao dio sukoba, primjerice kako bi navodno prikupili taktičke informacije prije napada. Ransomware je vrsta malware-a koja se koristi za enkripciju podataka ili sistema kako bi se iznudio otkup za dekripcijski ključ, što je postalo jedno od najdominantnijih i sofisticiranijih cyber kriminalnih prijetnji, često korišteno za poremećaj sistema suparnika. Wiper je druga vrsta malware-a koja trajno briše ili enkriptira podatke na zaraženim sistemima, uglavnom ciljajući ukrajinske entitete kako bi poremetio svakodnevni život i pristup važnim uslugama (CyberPeace Institut, 2023).

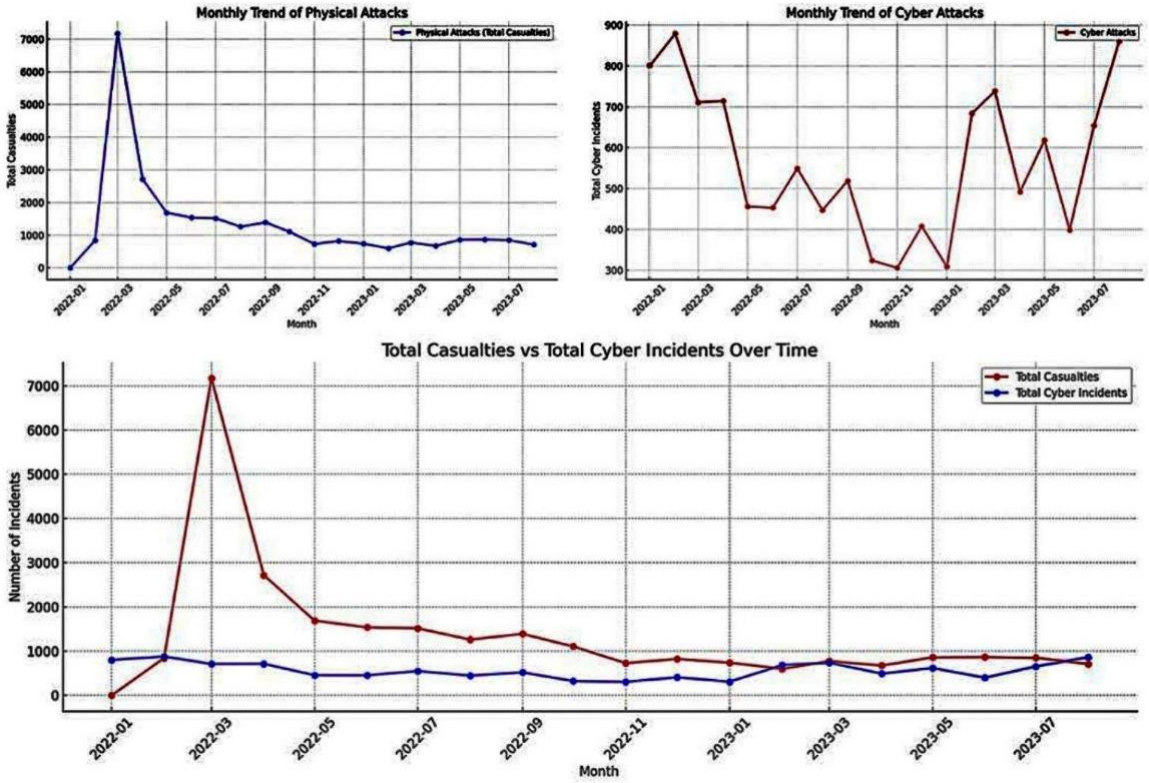
Benjamin Jensen i Elizabeth Hoffman (2024) u izvještaju za Center for Strategic and International Studies navode da u savremenoj Rusiji, stare strategije poput aktivnih mjera i refleksivne kontrole čine temelj cyber-omogućenog političkog ratovanja. Microsoftovi izvještaji otkrivaju da su, u prvoj godini sukoba s Ukrajinom, ruski hakeri ciljali preko 100 organizacija u više od 40 zemalja, koristeći napredne manipulativne timove za širenje lažnih narativa na društvenim mrežama. Novi projekti poput Maidan-3 imaju za cilj narušavanje povjerenja u Ukrajinu i njene zapadne saveznike (Smith, 2022: para 18). Kremlj je također pokušao koristiti prilagođene deepfake snimke kako bi pogoršao tenzije između ukrajinskog predsjednika Zelenskog i bivši vrhovni vojni zapovjednika, generala Valeriy Zaluzhny (Jensen i Hoffman, 2024).

Globalno, Rusija se bavi onim što Atlantski savet naziva ratom narativa, s ciljem destabilizacije povjerenja u Ukrajinu. Ova strategija se razlikuje od tradicionalnih cyber napada fokusirajući se na stvaranje haosa i oblikovanje javnog mnijenja kroz kompjutersku propagandu, koja uključuje lažne naloge na društvenim mrežama, botove i ciljani sadržaj. Ovaj napor je posebno primjetan izvan Evrope, gdje Rusija nastoji smanjiti međunarodnu podršku Ukrajini (Jensen i Hoffman, 2024). Studije Stanford Internet Observatory-a i BBC-a dokumentovale su značajne kampanje dezinformacija u Africi, s ciljem pridobijanja podrške za Rusiju, uključujući pružanje niskotarifnog pristupa ruskom propagandnom kanalu RT (Stanford Internet Observatory, 2019).

Pojavljuju se izvještaji koji sugeriraju da Rusija sve više cilja američku javnost. U aprilu 2024. Microsoft je identifikovao rusku kampanju uticaja koja je koristila kompjutersku propagandu i tradicionalne medije za širenje sadržaja putem sajtova poput D.C. Weekly i Miami Chronicle. Ova kampanja je uključivala kreiranje lažnih verzija legitimnih novinskih sajtova kako bi promovisala Kremljove narative i povezivala korisnike s web stranicama

kojima upravlja ruska obavještajna služba, fokusirajući se na podijeljene teme i sukob u Ukrajini (Reuters, 2024).

Pored toga, ruski operativci oživljavaju sovjetske taktike podmićivanja i manipulacije zvaničnicima širom svijeta. U martu 2024. godine otkrivena je ruska operacija uticaja kada je češka vlada sankcionisala "Voice of Europe," povezanu s pro-ruskom propagandom. U Belgiji su ruski agenti podmićivali članove Evropskog parlamenta da zagovaraju pro-ruske i anti-ukrajinske poruke. Ove prikrivene operacije, često finansirane putem kriptovaluta, imale su za cilj utjcati na evropske izbore i smanjiti podršku Ukrajini (Jensen i Hoffman, 2024).



Slika 3: Početna aproksimacija fizičkog naspram cyber napada. Izvor: https://cyberforumkyiv.org/A_Decade_in_the_Trenches_of_Cyberwarfare.pdf

Kako bismo bolje razumjeli dinamiku i korelaciju između fizičkih i cyber napada Rusije na Ukrajinu, Paziuk (2024) je analizirao mjesečne podatke, koji ukazuju na intenzitet oba tipa napada. U cilju procjene intenziteta fizičkih napada, koreliran je ukupan broj žrtava rata u Ukrajini s ukupnim brojem neprijateljskih incidenata za koje se sumnja da imaju ruski izvor. Pretpostavka je da žrtve pružaju grubu indikaciju intenziteta fizičkih napada. Slika prikazuje trendove u ukupnom broju žrtava od fizičkih napada (crvena boja) i ukupnim cyber incidentima (plava boja) tokom vremena. Iako postoje vrhunci i padovi i kod fizičkih i kod

cyber incidenata, nije odmah jasno postoji li jaka korelacija između njih. Na primjer, u martu 2022. godine, primjetan je značajan vrhunac u fizičkim žrtvama bez odgovarajućeg porasta cyber incidenata. Suprotno tome, august 2023. pokazuje veliki broj cyber incidenata bez sličnog porasta fizičkih žrtava (Paziuk, 2024).

Ruske cyber operacije ne potječu iz jedne jedinice ili agencije, već iz složene birokratske strukture. Učesnici su istakli različite pristupe koje Ruska federalna sigurnosna služba/ the Russian Federal Security Service (FSB) i Glavna direkcija Generalštaba Oružanih snaga/ the Main Directorate of the General Staff of the Armed Forces (GRU) primjenjuju prema cyber operacijama (Grossman i sur., 2023:6). Dr Tadas Jakstas (2024) u Izvještaju o ruskoj upotrebi ofanzivnih cyber sposobnosti u toku vojne agresije u Ukrajini navodi nekoliko glavnih aktera odgovornih za sprovođenje cyber aktivnosti uključujući Federalnu službu sigurnosti (FSB), Spoljna obavještajna služba (SVR), Glavna direkcija Generalštaba Oružanih snaga (GRU), te Grupe za cyber kriminal usklađene sa Rusijom (Jasaktas, 2024:7).

Federalna služba sigurnosti (FSB), nasljednica KGB-a, izvela je zlonamjerne cyber operacije koje su ciljale energetski sektor, uključujući energetske kompanije u UK i SAD, američke avijacione organizacije, američko vladino i vojno osoblje, privatne organizacije, kompanije za cyber sigurnost i novinare. Poznato je da FSB angažira kriminalne hakere za cyber aktivnosti usmjerene na špijunažu; ti isti hakeri su zasebno odgovorni za ometajuće ransomware i phishing kampanje. FSB Centar 16 odgovoran je za cyber operacije koje uključuju presretanje, dešifriranje i obradu elektronskih poruka, te tehničku penetraciju stranih meta. Njegov puni naziv je Centar za radio-elektronsku obavještajnu službu putem komunikacija i također je poznat kao Vojna jedinica 71330 (Jakstas, 2024:8).

Spoljna obavještajna služba (SVR) je glavna civilna obavještajna služba Rusije, koja je odgovorna za prikupljanje stranih obavještajnih podataka koristeći ljudske, signalne, elektronske i cyber metode (Jakstas, 2024:8). Većina posmatrača priznaje da SVR djeluje s jakim naglaskom na održavanju tajnosti i izbjegavanju otkrivanja. Većina cyber operacija koje se povezuju sa SVR-om fokusirana je na prikupljanje obavještajnih podataka. SVR je također poznat po visokom nivou tehničke stručnosti, često nastojeći da dobije i zadrži pristup unutar kompromitiranih mreža (Jakstas, 2024).

Glavna direkcija Generalštaba Oružanih snaga, poznata kao GRU, vojna je obavještajna agencija Rusije implicirana u neke od najpoznatijih i najštetnijih cyber operacija Rusije.

Medijska izvješća su identificirala dva glavna cyber odjela GRU-a, odnosno Odjel 26165 i Odjel 74455 (Jakstas, 2024:10).. Javni profil ovih odjela ističe visoki operativni tempo. GRU također kontrolira nekoliko istraživačkih instituta koji razvijaju alate za hakiranje i zlonamjerne programe. Opservatori su primijetili očitu spremnost cyber odjela GRU-a za provođenje smjelih i agresivnih operacija, ponekad s upitnim nivoima operativne sigurnosti i tajnosti. Cyber analitičari ovim odjelima zajedno daju nazive APT 28, Fancy Bear, Voodoo Bear, Sandworm i Tsar Team, naglašavajući njihovu odlučnost i ponekad nedovoljno skrivenu pristup (Jakstas, 2024:10). Nedavno je GRU preuzeo vodeću ulogu u cyber operacijama, investirajući značajne kapacitete u vojnu informacijsku operaciju (VIO) osnovanu u maju 2014. godine. Od invazije u februaru 2022. godine, GRU je održavao operativni tempo koji je znatno viši nego što je ikada prije viđeno. Prema mišljenju eksperata, GRU je uspio kombinirati tehničke efekte (sabotaža, uništavanje itd.) s operacijama utjecaja kako bi postigao psihološki utjecaj. Iako je teško mjeriti stvarni utjecaj ovih aktivnosti, autori su se složili da GRU djeluje na neviđenoj razini aktivnosti (Jakstas, 2024; Grossman i sur., 2023).

Grupe za cyber kriminal, motivisane finansijskim interesima, iskorištavaju ljudske i sigurnosne slabosti kako bi olakšale direktnu krađu ili iznudu od žrtava, posebno ciljajući kritičnu infrastrukturu širom svijeta (Jakstas, 2024:12). Nakon ruske invazije na Ukrajinu 2022. godine, određene frakcije kriminalnih internet grupa otvoreno su se opredijelile za podršku ruskoj vladi ili narodu. Prijetile su retaliacijskim cyber operacijama protiv percepiranih anti-ruskih akcija ili podrške Ukrajini. Ove grupe, povezane s Rusijom, prijete kritičnoj infrastrukturi prije svega kroz taktike poput korištenja ransomware-a za enkripciju podataka i značajno ometanje operacija. Također koriste napade Distribuirane uskraćivanje usluge (DDoS) kako bi preopteretile web stranice, često uz pokušaje iznude. Nedavni incidenti uključuju DDoS napade na obrambene entitete Ukrajine i tvrdnje o odgovornosti za poremećaje na američko m aerodromu koji je percipiran kao podrška Ukrajini (Jakstas, 2024: 12-13).

Raluca Csernatoni i Tim Maurer (2023) raspravljaju o zamagljivanju granica između rata i mira u cyber prostoru navodeći da sukob između Rusije i Ukrajine je istakao ključnu ulogu cyber operacija u modernom ratovanju, gdje države i nadržavni akteri koriste digitalne alate kako bi postigli strateške ciljeve. Cyber napadi usmjereni na kritičnu infrastrukturu, poput električnih mreža i komunikacijskih sustava, postali su moćni alati za prisilu i destabilizaciju.

Ti napadi ne samo da ometaju ključne usluge već i podrivaju javno povjerenje i oslabljuju strukture upravljanja, pojačavajući utjecaj konvencionalnih vojnih akcija. Štoviše, uključivanje privatnog sektora u cyber sigurnost unijelo je nove kompleksnosti u tradicionalnu dihotomiju između državnih i nadržavnih aktera. Privatne tvrtke, posebno one koje upravljaju kritičnom infrastrukturom, sve su ranjivije mete u cyber sukobima, što zahtijeva suradnju s vladama radi jačanja otpornosti i sposobnosti odgovora. Uspostavljena usklađenost tijekom rusko-ukrajinskog sukoba, gdje su privatne tvrtke dobrovoljno podržavale državne napore, ističe povezanu prirodu nacionalne sigurnosti i korporativnih interesa u cyber prostoru. (Csernatoni i Maurer, 2023)

Za razliku od konvencionalnog ratovanja, gdje odvraćanje često ovisi o vidljivim vojnim sposobnostima i savezima, cyber odvraćanje postavlja jedinstvene izazove. Pripisivanje cyber napada određenim akterima izuzetno je teško, što omogućava počiniteljima relativno bezbjedno djelovanje. Ova nejasnoća otežava uspostavu jasnih politika odvraćanja i eskalacijskih praga, potičući okruženje gdje cyber incidenti mogu brzo eskalirati bez jasnih granica ili pravila angažmana. Osim toga, pojava novih tehnologija, uključujući umjetnu inteligenciju (AI) i kvantno računarstvo, uvodi dodatne kompleksnosti u cyber prostor. Ove tehnologije nude neviđene mogućnosti kako za ofanzivne cyber operacije tako i za obrambene mjere, preoblikujući strateški račun cyber ratovanja. Kako države i nadržavni akteri koriste AI za cyber napade i obranu, potreba za međunarodnom suradnjom i regulacijom postaje sve hitnija kako bi se spriječila nekontrolirana eskalacija i osigurala globalna cyber sigurnost (Csernatoni i Maurer, 2023).

5. STUDIJE SLUČAJA

Ovaj rad istražuje dubok utjecaj cyber tehnologije na međunarodne sukobe, fokusirajući se na njezin transformacijski utjecaj na dinamiku državne moći i procese strateškog odlučivanja. Kako cyber sposobnosti nastavljaju evoluirati, one su zamaglile tradicionalne granice između rata i mira, nudeći neviđene prilike vanjskim akterima da infiltriraju procese odlučivanja i oblikuju strateške ishode. U istraživanju ovih dinamika, ovo istraživanje predlaže da se koncept moći razvio izvan konvencionalnih mjera kako bi uključio cyber sposobnosti kao jedan od ključnih faktora državnog utjecaja i otpornosti. U cilju prikaza ove hipoteze, ovaj dio rada predstavlja dvije ključne studije slučaja: cyber špijunsku kampanju 'Sputnik', cyber napad 'AcidRain' na satelitske komunikacije.

Studija slučaja 1: Sputnik

Cyber špijunaža postala je ključna za državne aktere, značajno mijenjajući međunarodne odnose i nacionalnu sigurnost. Primjer je kampanja Sputnik, pripisana ruskim hakerima koje podržava država, a koja cilja institucije vlade, vojne organizacije i kritičnu infrastrukturu širom svijeta. Povezana s ruskom vojnom obavještajnom agencijom (GRU), Sputnik je započeo početkom 2010-ih i nastavlja se i danas. Njegovi glavni ciljevi su izvlačenje osjetljivih informacija, ometanje operacija i prikupljanje obavještajnih podataka kako bi se utjecalo na geopolitičku dinamiku (Firdini, Urbanus i Syaiful, 2024: 121).

Sputnik koristi napredne taktike, tehnike i procedure (TTP) za infiltraciju ciljnih sustava. Uobičajene metode uključuju phishing i spear-phishing, gdje prilagođene e-pošte s zlonamjernim privicima ili poveznicama dobivaju početni pristup. Operacija također iskorištava ranjivosti zero-day - nepoznate softverske propuste - kako bi zaobišla sigurnosne odbrane. Unutar mreže, sofisticirani zlonamjerni softver, uključujući prilagođene Trojance za daljinski pristup (RATs), održava trajni pristup, izvlači podatke i prati komunikacije. Dodatno, operativci Sputnika koriste tehnike lateralnog kretanja za eskalaciju privilegija i pristup dodatnim sustavima i podacima. Operacija koristi snažnu infrastrukturu za upravljanje i kontrolu (C2) za komunikaciju s kompromitiranim sustavima, često putem šifriranih kanala kako bi izbjegla detekciju. (Computer Incident Response Center, 2023: para. 1) Nekoliko značajnih incidenata povezano je s operacijom Sputnik, uključujući interfiranje u američke izbore 2016. godine, te cyber napad NotPetya 2017. godine.

Ruska kampanja interfiranja imala je za cilj utjecati na predsjedničke izbore SAD-a 2016. godine s namjerom podrivanja vođenog liberalnog demokratskog poretka SAD-a. To uključuje napore za oslabljivanje očekivanog predsjedništva Hillary Clinton poticanjem nacionalne podjele i političke blokade od samog početka. Kampanja je također nastojala promovirati kampanje Donalda Trumpa i Bernieja Sandersa te podrivati povjerenje javnosti u izborni proces i validnost njegovih rezultata (Fisher, 2019:9). Također, Rusija je izvela cyber napad na američki izborni sustav rigoroznim testiranjem baza podataka za registraciju birača ili web stranica državnih tajnika u potrazi za mogućim ranjivostima u kodu, uspješno ili neuspješno pristupajući tim bazama podataka registracije birača (Fisher, 2019).

Ruski hakeri su ciljali kompaniju VR Systems u kampanji phishinga tri mjeseca prije izbora, pokušavajući dobiti korisničke podatke e-pošte kako od VR Systemsa tako i od nekih od njenih klijenata koji su bili uključeni u izborni proces. Također su istraživali web stranicu VR Systemsa u potrazi za ranjivostima, slično kao što su ranije radili na sistemima za registraciju birača savezne države Illinois (Zetter, 2019: para.5). Tokom izbora, ovi hakeri su pokušali interfirati se, ali su spriječeni da mijenjaju glasove ili direktno utječu na rezultate. Površno su istraživali web stranice povezane s izborima u 21 državi i provalili u nekoliko baza podataka registracije birača, ali nema dokaza da su mijenjali biračke zapise ili brojali glasove. Također su uspjeli provaliti u barem jednu kompaniju koja proizvodi softver za upravljanje popisima birača, instalirajući maliciozni softver na mreži te kompanije (Zetter, 2019).

U junu 2017. godine, kada se NotPetya malware prvi put pojavio na računarima širom svijeta, nije dugo trebalo vlastima u Ukrajini, gdje su primarno počele intruzije, da okrive Rusiju za razorni cyber napad koji će nanijeti štetu od 10 milijardi dolara na globalnom nivou (Wolff, 2021). U junu svijet je upoznao najrazorniji malware ikada upotrijebljen, koji je označio početak nove ere državom sponzorisanog cyber rata. NotPetya je bio dio tekućeg sukoba između Rusije i Ukrajine, ali iako je bio dizajniran da infiltrira računalne sisteme putem popularnog ukrajinskog računovodstvenog softvera, virus se proširio daleko izvan granica Ukrajine, na više od 60 zemalja, uništavajući računalne sisteme hiljada multinacionalnih kompanija (Wolff, 2021; Merchant, 2022).

Petya je vrsta ransomware-a koja je identificirana 2016. godine. Kao i druge vrste ransomware-a, Petya enkriptira datoteke i podatke na računaru žrtve. Operateri Petya-e zahtijevaju plaćanje u Bitcoinu prije nego što dekriptiraju datoteke i ponovno ih učine upotrebljivim. Za razliku od starijih varijanti ransomware-a koje su enkriptirale samo

određene važne datoteke radi iznude, Petya zaključava cijeli hard disk računara (Cloudfare, 2024). Iako se na početku činilo da je ransomware varijanta porodice Petya, istraživači su utvrdili da nisu povezani, te su sada ovaj malware nazvali NotPetya (Cloudfare, 2024; LogRythm Labs, 2017).

Ruski hakeri iz grupe Sandworm infiltrirali su servere kompanije Linkos Group, koja stoji iza popularnog ukrajinskog računovodstvenog softvera MeDoc. Kompromitiranjem MeDoc serverskog ažuriranja, uspjeli su zaraziti hiljade računara širom svijeta. Malware NotPetya, koristeći dvije ranjivosti – EternalBlue, ukradeni alat NSA-a, i Mimikatz, skriptu koja otkriva ranjivosti Windows lozinki – brzo se širio sa jedne mašine na drugu (VinciWorks Group, 2018: para. 3). NotPetya je također pogodio Maersk, globalnu brodarsku kompaniju, uzrokujući gašenje ekrana sa porukama o otkupnini ili porukama o popravci, čineći sisteme neupotrebljivim. Virus je brzo onesposobio Maerskove operacije, sprječavajući nove narudžbe i upravljanje flotom. IT sigurnost je bila paralizirana, a ključni sistemi uključujući servere, računare, rutere i telefone su bili kompromitirani (VinciWorks Group, 2018). Sedamnaest od 76 Maerskovih teretnih terminala širom svijeta je bilo poremećeno, zaustavljajući teretne operacije. Utjecaj NotPetye bio je katastrofalan, uzrokujući procijenjenu štetu od 10 milijardi dolara i paralizirajući velike multinacionalne kompanije kao što su TNT Express, Mondelez, Reckitt Benckiser, Rosneft i Merck (VinciWorks Group, 2018: para.7).

Studija slučaja 2: AcidRain

Satelitski komunikacijski sistemi su u posljednjih nekoliko godina postali ključni za globalnu povezanost, obuhvatajući širok spektar sektora poput vojne industrije, telekomunikacija i hitnih službi. Međutim, upravo ta ovisnost o satelitskim sistemima čini ih ranjivim metama za cyber napade, čiji je cilj poremećaj komunikacija i sticanje strateške prednosti. Jedan od najistaknutijih primjera je napad zlonamjernim softverom AcidRain, koji je odmah po početku sukoba između Rusije i Ukrajine onesposobio satelitske komunikacije koje je pružao Viasat-ov K-SAT servis širom Evrope. Među korisnicima K-SAT servisa bio je i vojni sektor Ukrajine (Maschmeyer, 2024: para. 10).

Operacija koja je implementirala AcidRain ističe se zbog svoje direktne povezanosti s vojnim ciljevima, ali i zbog potencijalne sposobnosti da ruskim trupama pruži taktičku, pa čak i stratešku prednost u ključnom trenutku. Posljedice napada bile su dalekosežne, uzrokujući široke smetnje u satelitskim komunikacijama, što je ozbiljno utjecalo na globalnu povezanost

i operativne sposobnosti u različitim sektorima. Vojne operacije su bile značajno otežane zbog kompromitacije sistema za komandu i kontrolu, dok su komercijalna preduzeća pretrpjela finansijske gubitke i prekide usluga (Maschmeyer, 2024).

Napad na telekomunikacijske sisteme nije pogodio samo vladine i vojne objekte, već je imao ozbiljan utjecaj i na civilno stanovništvo i infrastrukturu, kako u Ukrajini, tako i izvan nje. Gubitak pristupa internetu i mogući prekidi u energetskom sektoru bili su među najznačajnijim posljedicama za civilno društvo. Mnogi građani prijavili su da su ostali bez interneta više od dva tjedna, što je značajno otežalo svakodnevni život i komunikaciju. Napad na Viasat imao je dalekosežne posljedice i na šire područje Evrope. Velika njemačka energetska kompanija izgubila je mogućnost daljinskog praćenja više od 5.800 vjetrogeneratora, što je predstavljalo ozbiljan rizik za održavanje energetskog sistema. U Francuskoj je gotovo 9.000 pretplatnika jednog satelitskog internet provajdera doživjelo prekid internet usluge. Također, oko trećina od 40.000 pretplatnika drugog satelitskog internet provajdera u Europi, uključujući Njemačku, Francusku, Mađarsku, Grčku, Italiju i Poljsku, bila je pogođena ovim napadom (Cyber Peace Institute, 2022: para. 2). Sveukupno, ovaj cyber napad je utjecao na nekoliko hiljada korisnika u Ukrajini i desetine hiljada fiksnih širokopojasnih pretplatnika širom Evrope, čime je pokazao koliki razarajući potencijal imaju napadi na telekomunikacijske infrastrukture (CyberPeace Institute, 2022).

CyberPeace Intitute (2022) navodi da krajem marta 2022. godine, SentinelLabs javno je pripisao AcidRain razvojnim sličnostima s kampanjom VPNFilter iz 2018. godine, koju su prethodno povezali s ruskom vladom. Nakon toga, 10. maja, EU i zemlje (SAD, Velika Britanija, Australija, Novi Zeland, Kanada) službeno su pripisale AcidRain ruskoj vojnoj obavještajnoj službi (GRU), povezujući je s destruktivnim malverom poput WhisperGate koji cilja ukrajinske državne i privatne mreže (Cyber Peace Institut, 2022: para. 4). Ovaj atribut su podržale i nacionalne izjave Estonije, Danske, Irske, Nizozemske, Norveške, Austrije, Njemačke, Češke, Italije, Finske, Rumunije, Poljske i Francuske, što označava značajan korak u praksi političkog pripisivanja cyber napada. Ove izjave također su se referirale na navodne ruske povrede normi odgovornog ponašanja država u cyber prostoru, kako su utvrđene u izvještajima UN-ove Grupe eksperata vlada (UNGGE) i Otvorene radne grupe (OEWG). Izrazile su zabrinutost zbog napada na kritičnu infrastrukturu i njihovog utjecaja na civile koji nisu direktno uključeni u sukobe, doprinoseći raspravama o međunarodnom pravu i UN-ovim normama koje se odnose na cyber proctor (CyberPeace Institue, 2022: para. 5)

Pripisivanje odgovornosti za cyber napade određenim prijetnjama predstavlja stalni izazov, često zahtijevajući temeljnu forenzičku analizu i suradnju međunarodnih agencija za cyber sigurnost. Kao odgovor, pogođene organizacije i vlade jačaju mjere cyber sigurnosti, primjenjuju nadogradnje softvera i provode strože kontrole pristupa kako bi smanjili potencijalne buduće rizike (Cyber Peace Institute, 2022).

DISKUSIJA

Kako je navedeno u uvodnom poglavlju, hipoteza ovog rada temelji se na pretpostavci da revolucija u cyber tehnologiji značajno mijenja međudržavni sukob, pružajući eksternim akterima do sada neviđene sposobnosti za direktno prodiranje u države i podrivanje njihove moći putem inovativnih, brzo razvijajućih i globalno primjenjivih metoda koje je teško povezati s izvorom. Kao rezultat toga, koncept moći se pomjerio s tradicionalnog, centriranog na materijalne resurse, prema suptilnijem i teže mjerljivom pristupu.

Kako bi se procijenila hipoteza o transformacijskom utjecaju cyber tehnologije na međunarodne sukobe, neophodno je sistematski razmotriti ključne tvrdnje. Prvo, cyber tehnologija je omogućila eksternim akterima da manipulišu dinamikom državne moći na dosad neviđene načine. Strateška upotreba cyber operacija od strane Rusije, uključujući kampanje poput Sputnik i NotPetya, ističe ovu sposobnost. Kampanja Sputnik, pripisana ruskim hakerima podržanim od strane države, ciljala je institucije vlade, vojne organizacije i kritičnu infrastrukturu širom svijeta, demonstrirajući kako cyber špijunaža i taktike ometanja mogu utjecati na geopolitičke dinamike (Firdini, Urbanus i Syaiful, 2024). Slično tome, NotPetya, koja je započela djelovanjem ruskih hakera kroz kompromitaciju ukrajinskog softvera MeDoc, prouzrokovala je globalnu štetu, uključujući značajne ekonomske gubitke i operativne prekide u multinacionalnim kompanijama poput Maersk-a (Wolff, 2021; Merchant, 2022). Tokom 2010-ih godina, posebno za vrijeme geopolitičkih kriza kao što je bila invazija na Ukrajinu, cyber operacije su iskoristile višestruke ranjivosti infrastrukture protivnika. Za razliku od tradicionalnih metoda koje su često rizične i resursno zahtjevne, cyber operacije su se pokazale kao šire i manje rizične opcije za postizanje strateških ciljeva.

Drugo, utjecaj cyber tehnologije na međudržavnu moć je dubok, ali izuzetno kompleksan za preciznu kvantifikaciju. Kao što je ranije raspravljano, cyber sposobnosti nadilaze tradicionalne mjere moći, kao što su ekonomski pokazatelji i vojna oprema. One djeluju u sve evoluirajućem i nematerijalnom domenu, gdje su njihovi efekti moćni, ali ih je teško precizno mjeriti. Primjer cyber napada AcidRain na satelitske komunikacije, koji je značajno utjecao na vojne i civilne sektore u Ukrajini i širom Europe, pokazuje kako cyber ometanja mogu paralizirati ključnu infrastrukturu i operativne sposobnosti (Maschmeyer, 2024; CyberPeace Institute, 2022). Ovi incidenti naglašavaju ulogu cyber tehnologije u preoblikovanju strateških pejzaža, gdje kontrola nad informacijama i komunikacijskim kanalima postaje jednako važna kao i tradicionalna vojna dominacija. Iako se utjecaj cyber tehnologije

ponekad pokušava minimizirati, empirijski dokazi pokazuju suprotno. Cyber tehnologija nije samo omogućila značajne operativne prednosti, već se etablirala kao ključni domen modernih međunarodnih sukoba, pružajući državama neviđene prilike za iskorištavanje ranjivosti u protivničkim sistemima uz minimalne rizike pripisivanja.

U kontekstu realizma, teorijskog okvira koji tradicionalno naglašava opipljivu materijalnu moć kao centralnu u međunarodnim odnosima, rast cyber sposobnosti predstavlja značajan izazov (Baldwin, 2016). Za razliku od konvencionalnih vojnih ili ekonomskih pokazatelja, cyber sposobnosti unose složene i nijansirane dimenzije koje kompliciraju procjenu relativne moći. Informacijska i tehnološka moć sada stoje uz bok tradicionalnim elementima moći, proširujući strateške opcije država i preoblikujući dinamiku globalne konkurencije moći. U području politike moći, Rusija koristi različite tehnike za afirmaciju dominacije i utjecaja u međunarodnim odnosima. Teorija odvraćanja i suzbijanja ilustrira kako moćne države kroz vojne operacije i demonstracije snage odvraćaju slabije države. Asimetrični i simetrični ratni planovi naglašavaju upotrebu nekonvencionalnih taktika za iskorištavanje ranjivosti protivnika. Nagomilavanje vojnih jedinica duž granica, bilo radi stacioniranja ili vojnih vježbi, predstavlja vidljivu afirmaciju moći. Na kraju, propaganda igra ključnu ulogu, gdje države ili njihove agencije šire dezinformacije kako bi narušile reputaciju i međunarodnu sliku drugih (Fidelis i Ibrahim, 2023:220).

Zaključno, hipoteza o transformacijskom utjecaju cyber tehnologije na međunarodne sukobe ima validnost u svjetlu ovih analiza. Cyber tehnologija, kako je prikazano u studijama slučaja poput Sputnik, NotPetya i AcidRain, temeljno je preoblikovala dinamiku međunarodnih sukoba, pojačavajući sposobnosti država za iskorištavanje ranjivosti i ostvarivanje utjecaja na globalnim mrežama. Uvela je nove paradigme koje izazivaju tradicionalne pojmove moći, ističući važnost cyber sposobnosti u suvremenom državnom i sigurnosnom upravljanju.

ZAKLJUČAK

Generalna hipoteza postavljena u ovom radu glasi *da duboka globalna integracija cyber tehnologije u društvo i državne funkcije transformirala je međunarodne sukobe, pružajući vanjskim subjektima neviđenu sposobnost da se infiltriraju u procese donošenja odluka i implementacije strategija država.* Također, nadopunjujući generalnu hipotezu, posebna hipoteza predstavlja koncept moći koji je *evoluirao s jednostavne materijalne mjere do kompleksne i izazovne za kvantifikaciju, reflektirajući utjecaj cyber tehnologije na dinamiku borbe za moć među državama*. Kroz metodološki okvir kombinirane deskriptivne analize, analize sadržaja i analize slučaja, ovo istraživanje uspješno je potvrdilo postavljenu hipotezu o utjecaju cyber tehnologije na međunarodne sukobe. Deskriptivna analiza pružila je dublji uvid u historijski razvoj cyber tehnologije i ključne karakteristike relevantne za međunarodne sukobe, kao što su sposobnost širenja dezinformacija i izvođenja cyber napada. Analiza sadržaja, koja je uključivala pregled znanstvenih radova, knjiga i stručnih izvora, dodatno je potkrijepila hipotezu prikupljanjem empirijskih podataka o utjecaju cyber tehnologije na dinamiku međunarodnih sukoba. Analiza slučaja, fokusirana na sukobe između Rusije i Ukrajine, kao i na druge međunarodne konflikte, produbila je razumijevanje specifičnih implikacija cyber aktivnosti na međunarodnu sigurnost, demonstrirajući kako cyber tehnologija transformira strategije sukoba i međunarodne odnose.

Ovi nalazi jasno potvrđuju da duboka integracija cyber tehnologije u društvo i državne funkcije značajno mijenja međunarodne sukobe, omogućavajući vanjskim subjektima neviđenu sposobnost infiltracije u procese donošenja odluka i implementacije strategija država. Istraživanje također pruža temelje za oblikovanje informirane javne politike i strategija za prevenciju i rješavanje sukoba u digitalnom dobu, što će biti od ključne važnosti za buduće upravljanje globalnim sigurnosnim izazovima.

Cyber tehnologija nesumnjivo je omogućila vanjskim akterima da mijenjaju dinamiku državne moći na neviđene načine, što su pokazali incidenti poput Sputnik, NotPetya i AcidRain. Ove cyber operacije, koje se pripisuju državom sponzorisanim ruskim hakerima, ciljale su vladine institucije, vojne organizacije i kritičnu infrastrukturu širom svijeta. Ove akcije ilustriraju kako cyber špijunaža i taktike ometanja mogu direktno utjecati na geopolitičku dinamiku, pružajući državama alate za postizanje strateških ciljeva na načine koji su širi i manje rizični od tradicionalnih metoda.

Uticaj cyber tehnologije na mjere međudržavne moći je dubok, ali složen za kvantifikaciju. Za razliku od tradicionalnih metrika kao što su ekonomski indikatori i vojna oprema, cyber operacije djeluju u evoluirajućoj, nematerijalnoj domeni gdje su efekti snažni, ali teško mjerljivi. Napadi poput AcidRain, koji su ometali satelitske komunikacije u vojnim i civilnim sektorima širom Ukrajine i Evrope, pokazuju kako cyber ometanja mogu paralizirati kritičnu infrastrukturu i operativne sposobnosti. Ovi događaji naglašavaju ulogu cyber tehnologije u transformaciji strateških pejzaža, gdje kontrola nad informacijama i komunikacijskim kanalima postaje jednako vitalna kao i tradicionalna vojna dominacija.

Koncept moći i uloga cyber tehnologije u međunarodnim odnosima doživjeli su značajne transformacije uz sveprisutnu upotrebu digitalnih alata i tehnika. Raluca Csernatoni i Tim Maurer (2023) ističu da je sukob između Rusije i Ukrajine naglasio kritičnu ulogu cyber operacija u modernom ratovanju. Države i nedržavni akteri sve više koriste digitalne alate za postizanje strateških ciljeva, pri čemu cyber napadi ciljaju kritičnu infrastrukturu, kao što su električne mreže i komunikacioni sistemi, postajući moćni instrumenti prinude i destabilizacije. Ovi napadi ne samo da narušavaju osnovne usluge, već i potkopavaju povjerenje javnosti i slabe strukture upravljanja, čime se pojačava utjecaj konvencionalnih vojnih akcija.

Osim toga, uključenost privatnog sektora u cyber sigurnost unosi nove složenosti u tradicionalnu dihotomiju između državnih i nedržavnih aktera. Privatne kompanije, posebno one koje upravljaju kritičnom infrastrukturom, postaju sve ranjivije mete u cyber sukobima, zbog čega je neophodna saradnja s vladama kako bi se poboljšala otpornost i sposobnost odgovora. Saradnja uspostavljena tokom rusko-ukrajinskog sukoba, gdje su privatne kompanije dobrovoljno podržavale državne napore, naglašava međusobno povezanu prirodu nacionalne sigurnosti i korporativnih interesa u cyber prostoru.

Za razliku od konvencionalnog ratovanja, gdje se odvraćanje oslanja na vidljive vojne sposobnosti i saveze, cyber odvraćanje suočava se s jedinstvenim izazovima. Pripisivanje cyber napada određenim akterima izuzetno je teško, što počiniteljima omogućava da djeluju relativno nekažnjeno. Ova neizvjesnost komplikuje uspostavljanje jasnih politika odvraćanja i pragova eskalacije, stvarajući okruženje u kojem cyber incidenti mogu brzo eskalirati bez jasnih granica ili pravila angažmana. Poteškoće u atribuciji dodatno ometaju sposobnost država da efikasno reaguju, jer izvor napada često ostaje nepoznat ili neizvestan.

Pojava novih tehnologija, uključujući veštačku inteligenciju (AI) i kvantno računarstvo, unosi dodatne složenosti u cyber domen. Ove tehnologije nude neviđene mogućnosti kako za ofanzivne cyber operacije, tako i za odbrambene mjere, preoblikujući stratešku računicu cyber ratovanja. Kako države i nedržavni akteri sve više koriste AI za cyber napade i odbranu, potreba za međunarodnom saradnjom i regulativom postaje sve hitnija kako bi se spriječila nekontrolisana eskalacija i osigurala globalna cyber sigurnost. Ovi faktori jasno pokazuju kako cyber tehnologija redefinira koncept moći u međunarodnim odnosima, prelazeći iz tradicionalnih okvira vojne i ekonomske dominacije na složenu mrežu digitalnih kapaciteta i strategija.

Iz ovog istraživanja proizlazi nekoliko ključnih zaključaka- prvo, očigledno je da je moja hipoteza bila ograničena, jer je cyber tehnologija imala mnogo širi uticaj nego što se prvobitno pretpostavljalo. Konkretno, ona je omogućila državama da ostvaruju direktni i indirektni uticaj izvan svojih granica, dok je istovremeno stvorila efekte koji se protežu kroz sve elemente moći. Cyber tehnologija je značajno unaprijedila domet i preciznost oružja, poboljšala procese donošenja odluka i komunikacije, pružila obimne ekonomske prednosti, poslužila kao osnova za dramatične tehnološke napretke i promijenila navigaciju i komunikaciju na neviđene načine. Uticaj cyber tehnologije na međunarodne sukobe seže daleko izvan samih cyber napada, špijunaže i operacija uticaja, obuhvatajući praktično svaki aspekt nacionalne sigurnosti modernih država i povezanih resursa, organizacija i procesa.

Drugo, cyber tehnologija je stvorila novi domen sukoba koji je neuporediv s dosadašnjim. Kao rezultat toga, ciljevi za napade, krađu i uticaj sada se šire globalno, obuhvatajući ne samo fizičke i kognitivne sfere, već i virtualne elemente poput podataka i digitalnih okruženja. Ovaj novi domen je suštinski globalnog opsega i integrisan je u svaki element nacionalne moći. Za američku zajednicu nacionalne sigurnosti, koja je tradicionalno usmjerena geografski i ima stratešku kulturu usmjerenu na kvantitativne metrike, ovi razvoji postavljaju temeljna pitanja o procjeni prijetnji, prioritetizaciji resursa, razvoju odgovarajućih politika i potrebnim investicijama resursa.

Na kraju, jasno je da cyber tehnologija ne samo da transformira način na koji se vode sukobi, već i kako se nacionalna sigurnost shvata i upravlja. Ova nova stvarnost zahtijeva sveobuhvatan pristup koji uključuje saradnju među državama, inovacije u cyber sigurnosti i prilagođavanje postojećih strategija kako bi se odgovorilo na izazove koje donosi digitalna era.

BIBLIOGRAFIJA

KNJIGE

Al-Rodhan, Nayef, 2022, Implications for Geopolitics and Outer Space Security, u Greminger, Thomas i Vestner, Tobias (izdavači), The Russia-Ukraine War's Implications for Global Security: A First Multi-issue Analysis, Geneva Centre for Security Policy, Geneva.

Andress, Jason i Winterfield, Steve, 2014, Cyber Warfare: Techniques, Tactics and Tools for Security Practicioners. 2nd ed, Elsevier Inc., USA.

András Rácz, Ole, Spillner i Guntram, Wolff 7, 2023, Sanctions and the Russian war economy, u László, Andor i Uwe, Optenhögel (izdavači), Europe and the War in Ukraine from Russian Aggression to a New Eastern Policy, Foundation for European Progressive Studies Book, Brussels.

Balmaceda, Margarita M., 2013, Politics of Energy Dependency: Ukraine, Belarus, and Lithuania between Domestic Oligarchs and Russian Pressure, University of Toronto Press, Toronto.

Baylis, John, Smith, Steve i Owens, Patricia, 2020, The Globalization Of World Politics: An Introduction To International Relations, Oxford University Press, United Kingdom.
Beck, Ulrich, 1992, Risk Society: Towards a New Modernity, Sage Publications, London.

Bellasio, Jacopo i Silfversten, Erik, 2020, The Impact of New and Emerging Technologies on the Cyber Threat Landscape and Their Implications for NATO, u Ertan, A., Floyd, K. i Stevens, T. (Izdavači), Cyber Threats and NATO 2030: Horizon Scanning and Analysis, NATO CCDCOE Publications, Tallinn.

Böhme, Gernot, 2008, Invasive Technification: Critical Essays in the Philosophy of Technology, Graue Die Edition, Berlin.

Cashman, G, 2014, What causes war? An introduction to theories of international conflict, Rowman & Littlefield, Lanham.

Cavelty, Myriam Dunn i Wenger, Andreas, 2022, Cyber Security Politics Socio-Technological Transformations and Political Fragmentation, Routledge, New York.

Cristiano, Fabio, Broeders, Dennis, Delerue, François, Douzet, Frédérick i Géry, Aude, 2023, Artificial Intelligence and International Conflict in Cyberspace, Routledge, New York.

Connell, Michael i Vogler, Sarah, 2017, Russia's Approach to Cyber Warfare, Center for Naval Analysis: Arlington.

Ćurak, N. (2016). Rasprava o miru i nasilju: (geo)politika rata – (geo)politika mira – studije mira. Sarajevo/ Zagreb: Biblioteka Memorija

Dodds, Klaus, 2007, Geopolitics: A Very Short Introduction, Oxford University Press, New York.

Eriksson, Johan, 2007, Power Disparity in the Digital Age, u Knudsen, Olav F. (Ed.) Security Strategies, Power Disparity and Identity: The Baltic Sea Region, Routledge, London.

Ismailov, Eldar i Papava, Vladimer, 2010, Rethinking Central Eurasia, Central Asia-Caucasus Institute & Silk Road Studies Program, Washington, D.C.

Janczewski, Lech J. i Colarik, Andrew M, 2008, Cyber Warfare and Cyber Terrorism, Information Science Reference , New York.

Jonsson, Oscar, 2019, The Russian Understanding of War, Georgetown University Press: Washington.

Joseph S. Nye, Jr., 2011, The Future of Power, PublicAffairs, New York.

Kaarbo, Juliet i Ray, James Lee, 2005, Global politics, Houghton Mifflin Company, Estados Unidos.

Kedzie, Christopher R., 1997, A brave new world or a new world order?, u Kiesler, Sara (Ed.) Culture of the internet, Lawrence Eribaum Associates, New Jersey.

Kello, Lucas, 2017, The Virtual Weapon and International Order, Yale University Press, New Haven.

Kramer, Franklin D., 2009, Cyberpower and National Security: Policy Recommendations for a Strategic Framework, u Kramer, F. D., Starr, S. H., & Wentz, L. K. (Izdavači), Cyberpower and national security, National Defense University Press, Washington DC.

Krekel, Bryan A. i DeWeese, Steve, 2009, Capability of the People's Republic of China (PRC) to Conduct Cyber Warfare and Computer Network Exploitation, DIANE Publishing, Collingdale.

Kersten, Lahl, 2023, Western weapons for Ukraine: road to escalation or end of the war?, u László, Andor i Uwe, Optenhögel (izdavači), Europe and the War in Ukraine from Russian Aggression to a New Eastern Policy, Foundation for European Progressive Studies Book, Brussels.

Kuehl, Daniel T., 2009, From Cyberspace to Cyberpower: Defining the Problem, u Kramer, Franklin D., Starr, Stuart H. i Wentz, Larry K. (Izdavači) Cyberpower and National Security, National Defense University Press: Potomac Books, Washington, DC.

Latour, Bruno, 1993, We Have Never Been Modern, Harvard University Press, Cambridge.

Latour, Bruno, 2005, Reassembling the Social: An Introduction to the Actor-Network Theory, Oxford University Press, New York.

Levy, Jack S.,2011, Theories and Causes of War. U Christopher J. Coyne and Rachel L. Mathers (Izdavači), The Handbook of the Political Economy of War, Edward Elgar: Cheltenham.

Levy, Jack S., 2013, Interstate War and Peace. U Walter Carlsnaes, Thomas Risse, and Beth A. Simmons (Izdavači), Handbook of International Relations, Sage: Los Angeles.
Lonsdale, David J., 2004, The nature of war in the information age: Clausewitzian Future, Psychology Press, Sussex.

Mallik, Amitav, 2016, Role of Technology in International Affairs, Institute for Defence Studies and Analyses, New Delhi.

Malinova, Olga, 2017, Political Uses of the Great Patriotic War in Post-Soviet Russia from Yeltsin to Putin, u Fedor, Julie, Kangaspuro, Markku, Lassila, Jussi i Zhurzhenko, Tatiana (Izdavači), War and Memory in Russia, Ukraine and Belarus, Palgrave Macmillan, London.

McCartney, Scott, 1999, ENIAC: The Triumphs and Tragedies of the World's First Computer, Walker Publishing Company, New York.

Mearsheimer, John J., 1995, Back to the Future: Instability in Europe after the Cold War. U Michael E. Brown, Sean M. Lynn-Jones, and Steven E. Miller (Izdavači), The Perils of Anarchy, Cambridge, MIT Press: Cambridge.

Mearsheimer, John J., 2001, The Tragedy of Great Power Politics, W. W. Norton: New York.

Mojska, Katarzyna, 2016, New Technologies as a Factor of the "Spatial Turn" in International Relations, u Szkarłat, Monika i Mojska, Katarzyna (Izdavači) New Technologies as a Factor of International Relations, Cambridge Scholars Publishing Lady, Newcastle upon Tyne.

Muro, Mark, Maxim, Robert i Whiton, Jacob, 2019, Automation and Artificial Intelligence:

How machines are affecting people and places, Brookings Institution, Washington, DC.

Rummel, R. J., 1975–81, Understanding Conflict and War, Vols I–V. Sage, Beverly Hills.

Thomas, Rid, 2020, Active Measures: The Secret History of Disinformation and Political Warfare, Macmillan, New York.

Singer, P.W. i Friedman, Allan, 2014, Cybersecurity and Cyberwar: What Everyone Needs to Know, Oxford University Press, New York.

Smith, Tony, 2019, Why Wilson Matters: The Origin of American Liberal Internationalism and Its Crisis Today, Princeton University Press, Princeton.

Soja, Edward W., 2009, Taking space personally, u Warf, Barney i Arias, Santa (Izdavači), The Spatial Turn: Interdisciplinary Perspectives, Routledge Studies in Human Geography, London.

Spade, Jayson M., 2012, Information as Power: China's Cyber Power and America's National Security, U.S. Army War College Carlisle Barracks, Pennsylvania.

Stępień, Tomasz, 2016, Technological Turn and the New Framework of International Relations, u Szkarłat, Monika i Mojska, Katarzyna (Izdavači) New Technologies as a Factor

of International Relations, Cambridge Scholars Publishing Lady, Newcastle upon Tyne.

Szkarłat, Monika i Mojska, Katarzyna, 2016, New Technologies as a Factor of International Relations, Cambridge Scholars Publishing, Newcastle upon Tyne.

Thomas, Timothy, 2019, Russian Military Thought: Concepts and Elements, The MITRE Corporation: Arlington.

Toffler, Alvin i Toffler, Heidi, 1993, War and anti-war: Making sense of today's global chaos, Warner Books, Inc., New York.

Turčalo, S. (2021). Međunarodna sigurnost (hrestomatija za internu upotrebu). Sarajevo: Fakultet političkih nauka.

Von Clausewitz, Carl, 1976, On War, Princeton University Press, New Jersey.

Zimet, Elihu i Barry, Charles L., 2009, Military Service Cyber Overview, u Wentz, Larry K., Barry, Charles L. i Starr, Stuart H. (Izdavači), Military Perspectives on Cyber power, Center for Technology and National Security Policy at the National Defense University, Washington, DC.

Waltz, Kenneth N., 1979, Theory of International Politics, Addison-Wesley: Boston.

Weber, Max, 1978, Economy and Society, University of California Press, Berkeley.

Williams, Paul D. (2021). Rat. U Turčalo, Sead (ed). Međunarodna sigurnost (Hrestomatija za internu upotrebu). Fakultet političkih nauka, Sarajevo.

ČLANCI

Adibifar, Karam 2016, „Technology and Alienation in Modern-Day Societies“, *International Journal of Social Science Studies*, Vol. 4, No. 9, str. 61-68.

Al-Hasnawi, Ahmed Hassan, 2022, “The Russian-Ukrainian war and its implications for international security: a geopolitical vision”, *Texas Journal of Multidisciplinary Studies*, Vol. 9, str. 177-192.

Babst, Dean V., 1972, „A Force for Peace“, *Industrial Research*, Vol. 14, str: 55–58.

Barnett, Michael & Duvall, Raymond, 2005, „Power in International Politics“, *International Organization*, Vol. 59, No. 1, str. 39-75.

Bazylev, S. I. i ostali, 2012, „Activities of the Armed Forces of the Russian Federation in the Information Space: Principles, Rules, Confidence Building Measures“*, Voennaya Mysl’*, No. 6, str:24–28.

Bebler, Anton, 2015, „The Russian-Ukrainian Conflict over Crimea“, *Teorija in Praksa*, Vol. 52, No. 1, str. 196-219.

Biener, Christian, Eling, Martin, Wirfs, Jan Hendrik, 2015, “Insurability of Cyber Risk: An Empirical Analysis“, *Geneva Papers on Risk and Insurance*, No. 40, str. 131–158.

Cai, Hong, Bai, Wei, Zheng, Yi, Zhang, Ling, Cheung, Teris, Su, Zhaohui, Jackson, Todd, Xiang, Yu T., 2022, „International collaboration for addressing mental health crisis among child and adolescent refugees during the Russia-Ukraine war“, *Asian Journal of Psychiatry*, Vol. 72.

Chekinov, Sergey i Bogdanov, Sergey, 2015, „Military art in the initial stage of the XXI century: problems and judgments“, *Voennaya Mysl, No.*1, str: 34–45.

Craisor-Constantin, Ionita, 2023, „Conventional and Hybrid Actions in the Russia's Invasion of Ukraine“, *Security and Defence Quarterly*, Vol. 44, No. 4, str. 5-20.

Demir, Sertif, 2022, „The 2022 Russia-Ukraine War: Reasons And Impacts“, *Mayıs*, Vol. 6, No. 1, str. 13-40.

Dilys, Winegrad i Atsushi, Akera, 1996, „A Short History of the Second American Revolution“, *Almanac*, Vol. 42, No. 18, str. 1-11.

Doyle, Michael, 1983a, „Kant, Liberal Legacies, and Foreign Affairs, Part 1“, *Philosophy and Public Affairs*, Vol. 12, str: 205–35.

Doyle, Michael, 1983b, „Kant, Liberal Legacies, and Foreign Affairs, Part 2“, *Philosophy and Public Affairs*, Vol. 12, str: 323–57.

Fidelis, Ikaade Ochim i Ibrahim, Ahmed, 2023, “Implications of Russia-Ukraine War on World Peace and Security”, *African Journal of Politics and Administrative Studies*, Vol. 16, No. 2, str. 216-230.

Firdini, Jeffri, Urbanus Panggabean i Syaiful, Anwar, 2024, “The Role of Russian Cyber Operations in The Russian–Ukraine War in Achieving Russia's Strategic Objectives”, *The Indonesian Journal of Development Planning*, Vol. 8, No. 1, str. 118-131.

Grossi, Giuseppe i Vakulenko, Veronika, 2022, „New development: accounting for human-made disasters – comparative analysis of the support to Ukraine in times of war“, *Public Money & Management*, Vol. 42, No. 6, str. 467-471.

Huntington, Samuel P., 1993, “The Clash of Civilizations?”, *Foreign Affairs*, Vol. 72, No. 3, str. 29-49.

Iliopoulos, Ilias. 2009, „Strategy and Geopolitics of Sea Power throughout History“, *Baltic Security & Defence Review*, Vol. 11, No. 2, str. 5-20.

Jenkins, Brian, 2013, „Keeping up With Zuck: A Brief History of Facebook Features“, *Techniques 88*, Vol. 88, No. 8, str. 60-61.

Jensen, Benjamin, 2017, „The Cyber Character of Political Warfare“, *The Brown Journal of World Affairs*, Vol. 24, No. 1, str. 159-172.

Kallberg, Jan, 2016, „Strategic Cyberwar Theory – A Foundation for Designing Decisive Strategic Cyber Operations“, *The Cyber Defense Review*, Vo. 1, No. 1, str. 113-128.

Kehler, Robert C., 2023, Observations on U.S. Nuclear Posture and the War in Ukraine, u Trachtenberg, David J, Lessons Learned from Russia's FullScale Invasion of Ukraine, *National Institute Press*, Vol. 3, No. 10.

Kiselev, V. i Kostenko, A., 2015, „Cyberwar as the Basis of Hybrid Operations“, *Armeiskii sbornik 257*, No. 11, str. 3–6.

Klimburg, Alexander 2011, „Mobilising Cyber Power“, *Survival*, Vol. 53, No. 1, str. 41-60.

Kristensen, Hans, Korda, Matt i Reynolds, Eliana, 2023, "Russian nuclear weapons", *Bulletin of the Atomic Scientists*, Vol. 79, No. 3, str. 174-199.

Kuzio, Taras, 2014, „Impediments to the Emergence of Political Parties in Ukraine“, *Politics*, Vol. 34, No. 4, str. 309-323.

Kuznetsov, Sergey, Anisimov, Vasily, Teslya, Sergey i Morozov, Igor, 2018, „Cyber Operations as a Kind of Mililtary Action“, *Zashchita i bezopasnost',* Vol.1, No. 84, str. 5.

Lichterman, Andrew, 2022, „The Peace Movement and the Ukraine War: Where to Now?“, *Journal for Peace and Nuclear Disarmament*, Vol. 5, No. 1, str. 185-197.

Makio, Danielle i Fuccille, Alexandre, 2023, „The 2014 Russian Invasion of Crimea: Identity and Geopolitics“, *Revista Brasileira de Política Internacional*, Vol. 66, No. 1, str. 1-20.

Maoz, Zeev i Bruce Russett, 1993, „Normative and Structural Causes of Democratic Peace, 1946–1986“, *American Political Science Review*, Vol. 87, str: 624–38.

Maoz, Zeev i Nasrin Abdolali, 1989, „Regime Types and International Conflict, 1817–1976“, *Journal of Conflict Resolution, Vol.* 33, str: 3–35.

Matsuzato, Kimitaka, 2016, „Domestic politics in Crimea, 2009-2015“, *Journal of Post-Soviet Democratization*, Vol. 24, No. 2, str. 225-256.

McCreanor, Kyle 2021, „The Theory, Pursuit, and Practice of Cyber power in Israel“, *Journal of Military and Strategic Studies*, Vo. 20, No. 4, str. 1-21.

Obar, Jonathan i Wildman, Steve, 2015, „Social media definition and the governance challenge: An introduction to the special issue“, *Telecommunications policy*, Vol. 39, No. 9, str. 745-750.

Olender, Michael, 2015, „Keeping Pace with Cyber Power, Defense, and Warfare“, Journal of International and Global Studies, Vol. 6, No. 2, str. 55-61.

Parshin, S. i N. Bashkirov, 2019, „Cyberthreats and International Stability“, *Zarubezhnoe voennoe obozrenie*, No. 11, str: 3–10.

Priyono, Ujang, 2022, „Cyber warfare as part of Russia and Ukraine conflict“, *Jurnal Diplomasi Pertahanan*, Vol. 8, No. 2, str. 44-59.

Ramadhan, Iqbal, 2021, „The Implication of Cyberspace Towards State Geopolitics“, *POLITICON*, Vol. 3, No. 2, str. 161-184.

Ratten, Vanessa, 2023, „The Ukraine/Russia conflict: Geopolitical and international business strategies“, *Thunderbird International Business Review*, Vol. 65, str. 265–271.

Ray, James Lee, 2001, „Integrating Levels Of Analysis In World Politics“, *Journal of Theoretical Politics*, Vol. 13, No. 4, str. 355-388.

Rid, Thomas i Ben Buchanan, Ben, 2015, „Attributing Cyber Attacks”, *Journal of Strategic Studies*, Vol. 38, str. 1-37.

Rinear, Matthew, 2015, „Armed with a Keyboard: Presidential Directive 20, Cyber-Warfare, and the International Laws of War“, *Capital University Law Review*, Vol. 43, str. 679-720.

Romashkina, N. P. i Kildobskiy, A. B., 2015, „New XXI Century Methods of Confrontation“, *Vestnik Akademii voennykh nauk*, No. 1, str: 134–139.

Rummel, R.J., 1983, „Libertarianism and Interstate Violence“, *Journal of Conflict Resolution*, Vol. 27, str: 27–71.

Sarkees, Meredith Reid, Wayman, Frank Whelon i Singer, David J., 2003, „Inter-State, Intra-State, and Extra-State Wars: A Comprehensive Look at Their Distribution over Time, 1816–1997“, *International Studies Quarterly*, Vol. 47, str: 49-70.

Starodubtsev, Y. I., Bukharin, V. V. i Semyonov, S. S., 2012, „Technosphere war“, *Voyennaya Mysl*', Vol. 7, str: 22–31.

Toft, Peter, 2005, „John J. Mearsheimer: an offensive realist between geopolitics and power“, *Journal of International Relations and Development*, Vol. 8, str. 381-408.

Zagare, Frank C., 2007, „Toward a Unified Theory of Interstate Conflict“, *International Interactions*, Vol. 33, str: 305–327.

Waltz, Kenneth N., 1988, „The Origins of War in Neorealist Theory“, *Journal of Interdisciplinary History*, Vol. 18, No. 4, str: 615-628.

ONLINE IZVORI

Abrams, Elliott, 2023, Implications of the Russia-Ukraine War, datum pristupa: 22.04.2024, dostupno na: https://www.cfr.org/blog/implications-russia-ukraine-war

Adda247, 2024, Generations of Computer 1st to 5th, datum pristupa: 14.03.2024, dostupno na: https://www.adda247.com/school/generation-of-computer/

AJ, Vicens, 2023, Russia's Sandworm hackers blamed in fresh Ukraine malware attack, datum pristupa: 29.04.2024, dostupno na: https://cyberscoop.com/sandworm-wiper-ukraine-russia-military-intel/

Albakjaji, Mohamad i Almarzoqi, Reem, 2023, The Impact Of Digital Technology On International Relations: The Case Of The War Between Russia And Ukraine, datum pristupa: 15.04.2024, dostupno na: https://ajee-journal.com/upload/attaches/att_1679412084.pdf

Albin, Thomas, 2022, The Russia-Ukraine Crisis and its Implications for China, datum pristupa: 22.04.2024, dostupno na: https://www.internationalaffairs.org.au/australianoutlook/the-russia-ukraine-crisis-and-its-implications-for-china/

Anne Himmelfarb, 2024, Ukraine: Third Rapid Damage and Needs Assessment (RDNA3) February 2022 – December 2023, datum pristupa: 03.05.2024, dostupno na: https://ukraine.un.org/sites/default/files/2024-02/UA%20RDNA3%20report%20EN.pdf

Bachulska, Alicja i Leonard, Mark, 2023, China and Ukraine: The Chinese debate about Russia's war and its meaning for the world, datum pristupa: 21.04.2024, dostupno na: https://ecfr.eu/wp-content/uploads/2023/07/China-and-Ukraine-The-Chinese-debate-about-Russias-war-and-its-meaning-for-the-world.pdf

Baldwin, David A., 2018, Realism, datum pristupa: 22.06.2024, dostupno na: https://doi.org/10.23943/princeton/9780691170381.003.0005

Bareis, Luka, 2018, Interstate Resource Conflicts: International Networks and the Realpolitik of Natural Resource Acquisition, datum pristupa: 04.06.2024, dostupno na: http://etheses.lse.ac.uk/3783/1/Bareis__interstate-resource-conflicts.pdf

Bateman, Jon, 2022, Russia's Wartime Cyber Operations in Ukraine: Military Impacts, Influences, and Implications, datum pristupa: 29.04.2024, dostupno na: https://carnegieendowment.org/research/2022/12/russias-wartime-cyber-operations-in-ukraine-military-impacts-influences-and-implications?lang=en

BBC, 2022, Ukraine War: Russia warns Sweden and Finland against Nato membership, datum pristupa: 22.04.2024, dostupno na: https://www.bbc.com/news/world-europe-61066503

Bleng, P. K., 2022, Ukraine-Russia War: A prelude to a post-Western international order?, datum pristupa: 11.06.2024, dostupno na: http://www.carnegieedownment.org https://www.isdp.eu/publication/ukraine-russia-war-a-prelude-to-a-post-western-international-order/

Charaniya, Amaan, 2024, The Territorial Roots of Interstate Conflict, datum pristupa. 10.06.2024, dostupno na: https://saisreview.sais.jhu.edu/the-territorial-roots-of-interstate-conflict/#:~:text=A%20close%20examination%20of%20the,desire%20to%20expand%20their%20homeland

Cloudflare, 2024, What are Petya and NotPetya, datum pristupa: 16.06.2024, dostupno na: https://www.cloudflare.com/learning/security/ransomware/petya-notpetya-ransomware/
Computer Incident Response Center, 2023, TR-10- Red october/ Sputnik malware, datum pristupa: 16.06.2024, dostupno na: https://www.circl.lu/pub/tr-10/

Constantinescu, Vlad, 2022. New FoxBlade Malware Hit Ukraine Hours Before Invasion, Microsoft Says, datum pristupa: 13.06.2024, dostupno na: https://www.bitdefender.com/blog/hotforsecurity/new-foxblade-malware-hit-ukraine-hours-before-invasion-microsoft-says/

Csernatoni, Raluca i Maurer, Tim, 2023, Is Russia Changing the Rules of Cyberspace?, datum pristupa: 06.06.2024, dostupno na: https://carnegieendowment.org/podcasts/europe-inside-out/is-russia-changing-the-rules-of-cyberspace?lang=en&center=europe

CyberPeace Institute, 2022, Case Study: Viasat, datum pristupa: 16.06.2024, dostupno na: https://cyberconflicts.cyberpeaceinstitute.org/law-and-policy/cases/viasat

Fisher, Kate, 2019, Russian Interference in the 2016 United States Presidential Election, datum pristupa: 16.06.2024, dostupno na: https://repositories.lib.utexas.edu/server/api/core/bitstreams/062bf524-f0b9-4ad6-af62-456bd588f39f/content

Gamero-Garrido, Alexander, 2014, Cyber Conflicts in International Relations: Framework and Case Studies, datum pristup: 11.03.2024, dostupno na: https://dx.doi.org/10.2139/ssrn.2427993

Gerasimov, Valery, 2019, Vectors for the Development of Military Strategy, datum pristupa: 18.06.2024, dostupno na: https://www.ndc.nato.int/research/research.php?icode=585

Geers, Kenneth, 2008, Cyberspace and the Changing Nature of Warfare, datum pristupa: 04.03.2024, dostupno na: https://ccdcoe.org/uploads/2018/10/Geers2008_CyberspaceAndTheChangingNatureOfWarfare.pdf

Giles, Keir, 2023, Russian cyber and information warfare in practice, datum pristupa: 06.06.2024, dostupno na: https://www.chathamhouse.org/2023/12/russian-cyber-and-information-warfare-practice/03-distinctive-features-war

Grossman, Taylor, Kaminska, Monica, Shires, James i Smeets, Max, 2023, The Cyber Dimensions of the Russia-Ukraine War, datum pristupa: 11.06.2024, dostupno na: https://nsarchive.gwu.edu/sites/default/files/documents/2023-04-00_ECCRI_REPORT_The-Cyber-Dimensions-of-the-Russia-Ukraine-War.pdf

Heidelberg Institute for International Conflict Research, 2022, Conflict Barometer 2022, datum pristupa: 07.06.2024, dostupno na: https://hiik.de/wp-content/uploads/2023/05/CoBa_2022_00_01.pdf

HIIK, 2005, Conflict barometer 2005: Crisis, wars, coups d'état, negotiations,mediations, peace settlements, datum pristupa: 07.06.2024, dostupno na:

https://www.calameo.com/read/0001911094a152d63478f

Jakstas, Tadas, 2022, Report on the Russian Use of Offensive Cyber Capabilities in the Course of the Military Aggression in Ukraine, datum pristupa: 12.06.2024, dostupno na: https://www.nksc.lt/doc/rkgc/Report_Russian_Use_of_Offensive_Cyber_Capabilities_in_UA.pdf

Jensen, Benjamin i Hoffman, Elizabeth, 2024, Victory in Ukraine Starts with Adressing Five Strategic Problems, datum pristupa: 09.06.2024, dostupno na: https://www.csis.org/analysis/victory-ukraine-starts-addressing-five-strategic-problems

Lewis, James A., 2022, Cyber War and Ukraine, datum pristupa: 14.03.2024, dostupno na: https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/220616_Lewis_Cyber_War.pdf?VersionId=S.iEKeom79InugnYWlcZL4r3Ljuq.ash

Lilly, Bilyana i Cheravitch, Joe, 2020, The Past, Present, and Future of Russia's Cyber Strategy and Forces, datum pristupa: 08.06.2024, dostupno na: https://ccdcoe.org/uploads/2020/05/CyCon_2020_8_Lilly_Cheravitch.pdf

LogRhythm Labs, 2017, NotPetya Technical Analysis, datum pristupa: 16.06.2024, dostupno na: https://gallery.logrhythm.com/threat-intelligence-reports/notpetya-technical-analysis-logrhythm-labs-threat-intelligence-report.pdf

Maschmeyer, Lennart, 2024, Cyber Conflict and Subversion in the Russia-Ukraine War, datum pristupa: 14.06.2024, dostupno na: https://www.lawfaremedia.org/article/cyber-conflict-in-the-russia-ukraine-war

Ministry of Defense of the Russian Federation, 2011, Conceptual Views on the Activities of the Armed Forces of the Russian Federation in the Information Space, datum pristupa: 18.06.2024, dostupno na: https://ccdcoe.org/uploads/2018/10/Russian_Federation_unofficial_translation.pdf

Orenstein, Mitchell, 2022, Russia's use of cyber-attacks: lessons from the second Ukraine war – analysis, datum pristupa: 16.06.2024, dostupno na: https://www.fpri.org/article/2022/06/russias-use-of-cyberattacks-lessons-from-the-second-ukraine-war/

Paziuk , Andrii, 2024, A Decade in the Trenches of Cyberwarfare: Ukraine's Story of Resilience, datum pristupa: 14.06.2024, dostupno na: https://cyberforumkyiv.org/A_Decade_in_the_Trenches_of_Cyberwarfare.pdf

President of Russia, 2010, Military Doctrine of the Russian Federation, datum pristupa: 18.06.2024, dostupno na: http://kremlin.ru/supplement/461

Pytlak, Allison, 2024, False Alarms: Reflecting on the role of Cyber Operations in the Russia-Ukraine War, datum pristupa: 13.06.2024, dostupno na: https://www.stimson.org/2024/false-alarms-role-of-cyber-operations-in-the-russia-ukraine-war/

Reuters, 2024, Microsoft finds Russian influence operations targeting U.S. election have begun, datum pristupa: 11.06.2024, dostupno na: https://www.reuters.com/world/us/microsoft-finds-russian-influence-operations-targeting-us-election-have-slowly-2024-04-17/

SCADA International, 2024, SCADA systems explained, datum pristupa: 08.06.2024, dostupno na: https://scada-international.com/what-is-scada/#:~:text=What%20does%20SCADA%20stand%20for,data%20from%20the%20industrial%20equipment

Smith, Brad, 2022, Defending Ukraine: Early Lessons from the Cyber War, datum pristupa: 11.06.2024, dostupno na: https://blogs.microsoft.com/on-the-issues/2022/06/22/defending-ukraine-early-lessons-from-the-cyber-war/

Stanford Internet Observatory, 2019, Evidence of Russia-Linked Influence Operations in Africa, datum pristupa: 11.06.2024, dostupno na: https://cyber.fsi.stanford.edu/io/news/prigozhin-africa

Taylor, Brain D., 2014, Putin's Own Goal: The Invasion of Crimea and Putin's Political Future, datum pristupa: 22.04.2024, dostupno na: https://www.foreignaffairs.com/articles/ukraine/2014-03-06/putins-own-goal

The Council of Economic Advisers, 2018, The Costs of Malicious Cyber Activity to the U.S. Economy, datum pristupa: 22.02.2024, dostupno na: https://trumpwhitehouse.archives.gov/articles/cea-report-cost-malicious-cyber-activity-u-s-economy/

The Economist, 2016, Vladimir Putin's unshakable popularity: The Russian president's approval ratings refuse to budge, datum pristupa: 11.03.2024, dostupno na: https://www.economist.com/graphic-detail/2016/02/04/vladimir-putins-unshakeable-popularity

The MITRE Corporation, 2018, CAPEC-161: Infrastructure Manipulation, datum pristupa: 09.03.2024, dostupno na: https://capec.mitre.org/data/definitions/161.html

The Stockholm International Peace Research Institute (2024), Global military spending surges amid war, rising tensions and insecurity, datum pristupa: 24.04.2024, dostupno na: https://www.sipri.org/media/press-release/2024/global-military-spending-surges-amid-war-rising-tensions-and-insecurity

The United Nations, 2023, Russia-Ukraine war has weakened international security, USG DiCarlo warns, datum pristupa: 24.04.2024, dostupno na: https://dppa.un.org/en/msg-usg-dicarlo-sc-9357-ukraine-23-jun-23

United Nations Group of Governmental Experts (UN GGE), 2013, Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, datum pristupa: 27.03.2024, dostupno na: https://dig.watch/resource/un-gge-report-2013-a6898

VinciWorks Group, 2018, NotPetya: The World's Worst Cyber Attack, datum pristupa: 16.06.2024, dostupno na: https://vinciworks.com/blog/notpetya-the-worlds-worst-cyber-attack/

Zaheer, Merchant, 2022, NotPetya: the cyberattack that shook the world, datum pristupa: 16.06.2024, dostupno na: https://economictimes.indiatimes.com/tech/newsletters/ettech-unwrapped/notpetya-the-cyberattack-that-shook-the-world/articleshow/89997076.cms?from=mdr

Zetter, Kim, 2019, How Close Did Russia Really Come to Hacking the 2016 Election?, datum pristupa: 16.06.2024, dostupno na: https://www.politico.com/news/magazine/2019/12/26/did-russia-really-hack-2016-election-088171

Ziavras, Sotirios G., /, History of computation, datum pristupa: 28.02.2024, dostupno na: https://web.njit.edu/~ziavras/Ziavras-history.pdf

Zydyk, Mariusz, 2005, bulletin boardsystem (BBS), datum pristupa: 28.02.2024, dostupno na: https://www.techtarget.com/whatis/definition/bulletin-board-system-BBS

Qu, Yanzhen, 2011, Cyber Technology's Impact to the Future Education, datum pristupa: 15.02.2024, dostupno na: https://www.researchgate.net/publication/271020214_Cyber_Technology's_Impact_to_the_Future_Education#:~:text=Cyber%20technology%20is%20a%20term,cloud%20computing%2C%20and%20mobile%20computing

Walker, Nigel, 2023, Conflict in Ukraine: A timeline (2014 - eve of 2022 invasion), datum pristupa: 16.04.2024, dostupno na: https://researchbriefings.files.parliament.uk/documents/CBP-9476/CBP-9476.pdf

Wasielewski, Philip, 2023, Fighting to Win: Ukraine, Russia, and the War for Survival, datum pristupa: 03.05.2024, dostupno na: https://www.fpri.org/article/2023/08/fighting-to-win-ukraine-russia-and-the-war-for-survival/

Wilson, Robin i Campbell-Kelly, Martin, 2020, Computing: the 1940s and 1950s, datum pristupa: 28.02.2024, dostupno na: https://link.springer.com/article/10.1007/s00283-020-10009-x

World Bank, 2022, Ukraine Rapid Damage and Needs Assessment, datum pristupa: 03.05.2024, dostupno na: https://documents.worldbank.org/en/publication/documents-reports/documentdetail/099445209072239810/p17884304837910630b9c6040ac12428d5c

Yang, Tian, 2024, House approves $61bn aid for Ukraine – what we know so far, and what happens next, datum pristupa: 26.04.2024, dostupno na: https://www.theguardian.com/world/2024/apr/21/house-approves-61bn-aid-for-ukraine-what-we-know-so-far-and-what-happens-next

Naziv odsjeka i/ili katedre:	Politologija – Međunarodni odnosi i diplomatija
Predmet:	Master teza

IZJAVA O AUTENTIČNOSTI RADOVA

Ime i prezime:	Melisa Begić
Naslov rada:	**UTJECAJ CYBER TEHNOLOGIJE NA MEĐUDRŽAVNE SUKOBE**
Vrsta rada:	Završni magistarski rad
Broj stranica:	93

Potvrđujem:

- da sam pročitao/la dokumente koji se odnose na plagijarizam, kako je to definirano Statutom Univerziteta u Sarajevu, Etičkim kodeksom Univerziteta u Sarajevu i pravilima studiranja koja se odnose na I i II ciklus studija, integrirani studijski program I i II ciklusa i III ciklus studija na Univerzitetu u Sarajevu, kao i uputama o plagijarizmu navedenim na web stranici Univerziteta u Sarajevu;
- da sam svjestan/na univerzitetskih disciplinskih pravila koja se tiču plagijarizma;
- da je rad koji predajem potpuno moj, samostalni rad, osim u dijelovima gdje je to naznačeno;
- da rad nije predat, u cjelini ili djelimično, za stjecanje zvanja na Univerzitetu u Sarajevu ili nekoj drugoj visokoškolskoj ustanovi;
- da sam jasno naznačio/la prisustvo citiranog ili parafraziranog materijala i da sam se referirao/la na sve izvore;
- da sam dosljedno naveo/la korištene i citirane izvore ili bibliografiju po nekom od preporučenih stilova citiranja, sa navođenjem potpune reference koja obuhvata potpuni bibliografski opis korištenog i citiranog izvora;
- da sam odgovarajuće naznačio/la svaku pomoć koju sam dobio/la pored pomoći mentora/ice i akademskih tutora/ica.

Mjesto, datum **Potpis**

_____ _____