SAJBER BEZBEDNOST – NOVI IZAZOVI U KONTEKSTU SAVREMENIH SUKOBA / CYBERSECURITY - NEW CHALLENGES IN THE CONTEXT OF MODERN CONFLICTS

Doc. dr. Filip Petrovski[1], Prof. dr. Atanas Kozarev[1]
[1]Law Faculty, MIT University, Severna Makedonija
e-mail: petrovskifilip2007@gmail.com, kozarev.atanas@yahoo.com

Stručni članak
UDK / UDC 004.42:355.48: 327.5(477)

Sažetak
Sajber bezbednost se suočava sa neviđenim izazovima, dodatno pojačanim naprednim tehnologijama i savremenim geopolitičkim sukobima, poput rata u Ukrajini. Sajber operacije postale su sastavni deo ratovanja, usmerene na kritičnu infrastrukturu, širenje dezinformacija i destabilizaciju komunikacionih mreža. Ovaj sukob je pokazao sve veću ulogu napada koje podržavaju države, uključujući ransomware i napredne uporne pretnje (APTs), brišući granice između sajber i kinetičkih operacija. Pojava tehnologija poput veštačke inteligencije (AI), kvantnog računarstva i Interneta stvari (IoT) uvela je nove ranjivosti i povećala složenost sajber pretnji. Rad se takođe bavi pravnim i etičkim dilemama sajber ratovanja, naglašavajući potrebu za međunarodnom saradnjom i snažnim regulatornim okvirima. Analizom ukrajinskog sukoba, ovo istraživanje ističe strateški značaj sajber bezbednosti u savremenim sukobima i zagovara inovativna, multidisciplinarna rešenja za jačanje globalne otpornosti u sve digitalizovanijem svetu.
Ključne riječi: *Sajber bezbednost, sajber ratovanje, sukob u Ukrajini, kritična infrastruktura i napredne uporne pretnje (APTs)*
JEL klasifikacija: H56, K33, O33, D74

Abstract
The cybersecurity landscape faces unprecedented challenges, amplified by advanced technologies and modern geopolitical conflicts like the war in Ukraine. Cyber operations have become integral to warfare, targeting critical infrastructure, spreading misinformation, and destabilizing communication networks. This conflict has revealed the growing role of state-sponsored attacks, including ransomware and Advanced Persistent Threats (APTs), blurring the lines between cyber and kinetic operations. Emerging technologies, such as artificial intelligence (AI), quantum computing, and the Internet of Things (IoT), have introduced new vulnerabilities and escalated the complexity of cyber threats. The paper also addresses the legal and ethical dilemmas of cyber warfare, emphasizing the need for international collaboration and robust policy frameworks. By examining the Ukrainian conflict, this study highlights cybersecurity's strategic importance in modern conflicts and advocates for innovative, multidisciplinary solutions to enhance global resilience in an increasingly digital battlefield.
Keywords: *Cybersecurity, cyber warfare, Ukraine conflict, critical infrastructure, and advanced persistent threats (APTs)*
JEL classification: *H56, K33, O33, D74*

UVOD U NOVE SAJBER IZAZOVE

U 21. veku, sajber prostor se pojavio kao kritični domen sukoba, koji utiče na nacionalnu bezbednost, ekonomsku stabilnost i globalnu politiku. Sve veće oslanjanje na digitalnu infrastrukturu učinilo je nacije, korporacije i pojedince ranjivim na sofisticirane sajber prijetnje, od špijunaže i sabotaže do dezinformacija i hibridnog ratovanja. Incidenti visokog profila, kao što su sajber napadi na Estoniju 2007. i ekstenzivna upotreba sajber operacija tokom rusko-ukrajinskog rata, naglasili su potrebu za snažnim mjerama kibernetičke sigurnosti i međunarodnom saradnjom.

Ovaj rad istražuje evoluirajuću prirodu sajber prijetnji, fokusirajući se na njihov historijski razvoj, pouke iz modernih sukoba i etičke dileme koje postavljaju. Predlaže sveobuhvatan okvir koji integriše stratešku odbranu, intervencije u ponašanju i tehnološka dostignuća za rešavanje ovih izazova. Ističući ulogu međunarodnih institucija, posebno Ujedinjenih naroda, naglašava hitnu potrebu za globalnim djelovanjem kako bi se osigurala sigurna i stabilna digitalna budućnost.

1. ISTORIJSKI RAZVOJ KIBERNETIČKE SIGURNOSTI I SAJBER RATOVANJA

Sajber napadi na Estoniju 2007 godine, poznati kao Bronzana noć, predstavljali su ključni trenutak u evoluciji sajber bezbednosti i razumevanju sajber ratovanja. Ovi napadi su izazvani odlukom estonske vlade da premjesti Bronzanog vojnika, ratnog spomenika iz sovjetskog doba, što je dovelo do nereda i vala sajber napada za koje se vjeruje da potiču od ruskih aktera. Napadi su prvenstveno bili usmjereni na vladine web stranice, banke i medijske kuće putem tehnika distribuiranog uskraćivanja usluge (DDoS)[164], efektivno paralizirajući ključne sektore kritične infrastrukture nacije sedmicama. Dok je neposredni tehnički uticaj napada bio ograničenog obima, njihov simbolički značaj je odjeknuo globalno, pokazujući ranjivosti međusobno povezanih digitalnih sistema i potencijal da sajber operacije služe kao oruđe geopolitičkog uticaja

Bronzana noć je naglasila sposobnost sajber napada da iskoriste ovisnost modernih društava o digitalnim mrežama, razotkrivajući kako takve operacije mogu poremetiti svakodnevni život, narušiti povjerenje javnosti i izvršiti politički pritisak bez tradicionalnog vojnog angažmana. Ovaj događaj je katalizirao prepoznavanje sajber prostora kao kritičnog domena nacionalne sigurnosti i podstakao promjenu paradigme u globalnoj sigurnosnoj politici. Odgovor Estonije, uključujući brze napore za ublažavanje i njeno zalaganje za međunarodnu saradnju u oblasti sajber bezbednosti, pozicionirao je zemlju kao globalnog lidera u sajber odbrani.

[164] DDoS (Distributed Denial of Service) napad ima za cilj da poremeti funkcionalnost servera, usluge ili mreže preplavljujući ih prekomjernim internet prometom. Koristi višestruke kompromitovane sisteme, često organizovane u botnetove, da preplavi cilj, čineći ga nedostupnim legitimnim korisnicima. „Distribuirana" priroda uključuje brojne uređaje, što ublažavanje čini izazovnim. "Odbijanje usluge" se fokusira na iscrpljivanje resursa cilja, kao što su propusni opseg ili procesorska snaga.
Vrste DDoS napada:
Zasnovano na volumenu: Nadvladavanje cilja velikim prometom (npr. UDP ili ICMP poplave).
Protokol: Iskorištavanje ranjivosti u mrežnim protokolima (npr. SYN poplave).
Sloj aplikacije: Ciljanje specifičnih aplikacija (npr. HTTP poplave).
DDoS napadi se koriste za ometanje organizacija ili službi iz ideoloških, političkih ili finansijskih motiva, što predstavlja značajne izazove za odbranu sajber bezbjednosti.

Jedan od značajnih ishoda ovog događaja bilo je uspostavljanje NATO-ovog Kooperativnog centra izvrsnosti za kibernetičku odbranu (CCDCOE)[165] u Talinu 2008 godine. CCDCOE je postao centar za istraživanje, obuku i razvoj politike u oblasti sajber-sigurnosti, nudeći državama članicama platformu za zajedničko baviti se složenošću sajber prijetnji. Napadi su također naglasili novi koncept hibridnog ratovanja, gdje državni i nedržavni akteri koriste sajber sposobnosti u sprezi s tradicionalnim oblicima sukoba za postizanje strateških ciljeva.

Geopolitičke posljedice Bronzane noći proširile su se i izvan Estonije, što je potaknulo šire rasprave o pripisivanju sajber napada, ulozi međunarodnog prava u sajber prostoru i potrebi za koordiniranim globalnim odgovorima na takve prijetnje. Ovaj događaj je poslužio kao opomena, ilustrirajući kako bi se sajber prostor mogao koristiti oružjem, čime se preoblikuje globalni sigurnosni krajolik i ubrzava institucionalizacija okvira kibernetičke sigurnosti u vojnim i civilnim domenima.

PRETNJE KOJE SE RAZVIJAJU:

Tokom protekle dvije decenije, priroda sajber ratovanja doživjela je značajnu evoluciju, prelazeći od izolovanih čina haktivizma i cyber kriminala na sofisticiranije, državno sponzorirane kampanje usmjerene na destabilizaciju političkih sistema, narušavanje ekonomije i vršenje geopolitičkog utjecaja. U početku su sajber napadi često bili povezani s pojedinačnim hakerima ili nedržavnim grupama koje su slijedile ideološke ciljeve ili finansijsku dobit. Međutim, sve veća digitalizacija kritične infrastrukture i oslanjanje na međusobno povezane sisteme transformisali su sajber prostor u strateško bojno polje za nacionalne države.

Prekretnica u ovoj evoluciji bio je napad Stuxneta 2010[166] godine, vrlo sofisticirana operacija koja se pripisuje SAD-u. i Izrael. Stuxnet je ciljao iranska postrojenja za nuklearno obogaćivanje, koristeći zlonamjerni softver da fizički sabotira sisteme industrijske kontrole. Ovaj događaj je pokazao sposobnost sajber alata da se pomaknu dalje od digitalne špijunaže i precizno naruše fizičku infrastrukturu, označavajući pojavu sajber operacija kao oružja nacionalne sigurnosti.

Još jedan značajan slučaj bila je kampanja NotPetya iz 2017[167], pripisana ruskim hakerima. Prvobitno usmjeren na ukrajinske sisteme, ovaj sajber napad je brzo eskalirao u globalnu krizu, osakaćujući multinacionalne korporacije, pružaoce zdravstvenih usluga i vladine agencije u

[165] NATO Cooperative Cyber Defence Center of Excellence (CCDCOE) je multinacionalna institucija za istraživanje, obuku i razmjenu znanja usmjerena na poboljšanje sposobnosti sajber odbrane među NATO saveznicima i partnerima. Sa sjedištem u Talinu, Estonija, podržava NATO-ovu politiku kibernetičke odbrane tako što provodi istraživanja, organizira vježbe i nudi obuku u oblastima kao što su sajber sigurnost, pravo, strategija i tehnologija. CCDCOE je najpoznatiji po svom razvoju Talinskog priručnika, ključnog resursa o međunarodnom pravu primjenjivom na sajber ratovanje.

[166] Stuxnet (2010) je bio sofisticirano sajber oružje dizajnirano da poremeti iranski nuklearni program. Bio je to vrlo napredan kompjuterski crv koji je posebno ciljao industrijske upravljačke sisteme (ICS) koji koriste Siemens softver. Stuxnet je iskoristio višestruke ranjivosti nultog dana kako bi sabotirao centrifuge u iranskom postrojenju za obogaćivanje uranijuma Natanz, uzrokujući fizičku štetu dok je ostao neotkriven. Široko se pripisuje tajnoj operaciji SAD-a. i Izrael, označio je prvi poznati slučaj sajber napada koji je uzrokovao uništenje u stvarnom svijetu, naglašavajući potencijal sajber ratovanja.

[167] Napad NotPetya (2017) bio je destruktivni globalni sajber napad prerušen u ransomware, ali prvenstveno osmišljen da izazove široko rasprostranjene poremećaje. Poreklom iz Ukrajine putem kompromitovanog ažuriranja softvera za računovodstveni softver, brzo se proširio širom sveta. NotPetya je šifrirao podatke na zaraženim sistemima, čineći ih neoperativnim, ali nije imao funkcionalan mehanizam za dešifriranje datoteka čak i ako je plaćena otkupnina. Pripisan ruskim državnim akterima, ciljao je Ukrajinu, ali je prouzročio milijarde dolara štete na globalnom nivou, pogađajući preduzeća, infrastrukturu i vlade. Ostaje značajan primjer sajber ratovanja koje sponzorira država.

nekoliko zemalja. Za razliku od tradicionalnog zlonamjernog softvera, NotPetya nije dizajnirana da iznuđuje otkupninu, već da uništi podatke, pokazujući destruktivni potencijal sajber mogućnosti. Njegovi globalni efekti prelivanja naglasili su međusobno povezane ranjivosti modernih sistema, gdje napad usmjeren na jednu naciju može nenamjerno utjecati na druge na globalnoj razini.

Ovi primjeri ističu prirodu cyber sposobnosti dvostruke namjene, koje mogu poslužiti i kao alati za tajnu špijunažu i velike, otvorene poremećaje. Za državne aktere, sajber operacije nude jeftino, osporivo i skalabilno sredstvo za postizanje strateških ciljeva. Ovaj dualitet je proširio opseg sajber ratovanja, omogućavajući nacijama da projektuju moć bez prelaska tradicionalnih kinetičkih pragova koji bi mogli izazvati direktnu vojnu odmazdu.

Pojava sajber kampanja koje sponzorira država također označava širi trend hibridnog ratovanja, gdje sajber operacije nadopunjuju tradicionalne vojne taktike za postizanje sveobuhvatnih strateških ciljeva. Primjeri uključuju rusko korištenje sajber alata u tandemu s vojnom agresijom tokom aneksije Krima 2014 i njenih kasnijih kampanja u Ukrajini. Ove operacije spajaju sajber napade s kampanjama dezinformacija, stvarajući višedomenski pristup sukobu koji komplikuje pripisivanje i odgovor.

Štaviše, kako se sajber sposobnosti razvijaju, tako se razvijaju i njihove implikacije na globalnu sigurnost. Proliferacija naprednih trajnih prijetnji (APT)[168], često sponzoriranih od strane države, izazvala je zabrinutost zbog eskalacije sukoba u sajber prostoru. Takve prijetnje ciljaju kritičnu infrastrukturu, uključujući električne mreže, zdravstvene sisteme i finansijske institucije, s potencijalom da izazovu kaskadne kvarove u međusobno povezanim sistemima. Tekući pomak sa oportunističkih napada na namjerne kampanje koje sponzorira država označava novu eru u sajber-ratu, gdje su ulozi veći, a posljedice dalekosežnije.

Ove evoluirajuće prijetnje naglašavaju hitnu potrebu za snažnim odbrambenim mjerama, međunarodnom saradnjom i adaptivnim strategijama za rješavanje rastuće složenosti sajber sukoba. Oni također naglašavaju važnost razumijevanja sajber sposobnosti ne samo kao remetilačkog alata, već i kao sastavnih komponenti modernih geopolitičkih strategija.

2. CYBER OPERACIJE U RUSKO-UKRAJINSKOM RATU TACTICAL VS. STRATEŠKI UTICAJ:

Uprkos početnim projekcijama da će sajber rat igrati odlučujuću ulogu u modernim sukobima, iskustvo ruskih sajber operacija tokom ukrajinskog rata otkrilo je njihov ograničeni samostalni uticaj. Cyber kampanje, uključujući phishing sheme i napade distribuiranog uskraćivanja usluge (DDoS), ciljale su kritične ukrajinske sisteme kao što su vladine web stranice, finansijske institucije i medijske platforme. Iako su ovi napori privremeno poremetili operacije, nisu uspjeli izazvati široko rasprostranjeni sistemski neuspjeh ili značajno degradirati sposobnost Ukrajine da

[168] APT je skraćenica od Advanced Persistent Threat, termin koji se široko koristi u sajber sigurnosti za opisivanje dugotrajnog i ciljanog cyber napada. Ove napade obično sprovode sofisticirane grupe sa dobrim resursima, često sponzorisane ili povezane sa državom, sa ciljem da se infiltriraju i održe pristup sistemima tokom dužeg perioda bez otkrivanja. Njihovi ciljevi mogu se kretati od špijunaže i krađe podataka do sabotaže i destabilizacije kritičnih sistema.

funkcionira. Ovaj ishod odražava inherentna ograničenja sajber operacija kada su raspoređene u izolaciji, naglašavajući njihovu komplementarnu, a ne primarnu ulogu u savremenom ratovanju.

Ključni izazov za ruske sajber snage bile su snažne odbrambene mjere koje je implementirala Ukrajina, uz podršku međunarodnih partnerstava s tehnološkim kompanijama iz privatnog sektora i savezničkim vladama. Napredna obavještajna informacija o prijetnjama, infrastruktura kibernetičke sigurnosti i timovi za brzu reakciju ublažili su utjecaj ovih napada. Na primjer, dok su ruske sajber kampanje nastojale da osakate ukrajinske električne mreže i komunikacije, otpornost ukrajinske sajber odbrane osigurala je da kritični sistemi ostanu operativni. Ovo naglašava novi trend u kojem su sajber operacije efikasnije kao pokretači konvencionalnih vojnih akcija, a ne kao odlučujuće, nezavisne strategije.

Međutim, strateški značaj sajber sposobnosti seže izvan bojnog polja. Ruske operacije su naglasile korisnost sajber prostora za psihološki rat, koristeći digitalne platforme za podrivanje ukrajinskog morala i narušavanje međunarodne podrške Kijevu. Kampanje dezinformacija, uključujući lažne narative koje se šire putem društvenih medija, imaju za cilj polarizaciju društava, podsticanje nepovjerenja u demokratske institucije i manipulaciju globalnim javnim mnijenjem. Na primjer, Rusija je koristila koordinirane mreže botova i farme trolova za širenje propagande koja dovodi u pitanje legitimitet ukrajinske vlade i optužuje njene vođe za ekstremizam. Ovi napori, iako manje direktni od kinetičkih operacija, pokazali su se efikasnim u oblikovanju percepcija i globalnom utjecaju na politički diskurs.

Sukob u Ukrajini također pokazuje kako sajber operacije mogu poslužiti kao oruđe za prisilu i ometanje bez prelaska tradicionalnih ratnih pragova. Na primjer, napadi Rusije na civilne sisteme, kao što su bankarske mreže i javni prevoz, imaju za cilj da unesu strah i nesigurnost među stanovništvo. Takve taktike pojačavaju psihološki danak fizičkog ratovanja, stvarajući okruženje nestabilnosti koje komplikuje upravljanje i otpornost. Ove operacije ističu dvostruku svrhu sajber kampanja: one funkcionišu i kao taktički pokretači i kao strateški instrumenti za postizanje širih geopolitičkih ciljeva.

Konačno, rat u Ukrajini ilustruje da, iako je malo vjerovatno da će sajber operacije zamijeniti konvencionalne vojne strategije, one su neophodne u modernom hibridnom ratovanju. Njihova uloga množitelja snaga, u kombinaciji sa njihovim potencijalom da utiču na globalne narative, osigurava da sajber sposobnosti ostanu kritična komponenta budućih strategija sukoba. Ovo naglašava potrebu za sveobuhvatnim pristupima koji integrišu sajber i kinetičke domene kako bi se maksimizirao njihov kombinovani uticaj uz minimiziranje ranjivosti.

OTPORNOST I ADAPTACIJA:

Sposobnost Ukrajine da izdrži sajber napade pripisuje se njenim proaktivnim strategijama sajber odbrane i međunarodnoj podršci. Javno-privatna saradnja sa tehnološkim kompanijama kao što su Microsoft i Google ojačala je kibernetičku sigurnost Ukrajine, pružajući kritičnu infrastrukturu otpornost na napade. Nadalje, sukob naglašava rastuću važnost sajber otpornosti kao prioriteta nacionalne sigurnosti, gdje odbrambene mjere po djelotvornosti često nadmašuju ofanzivne sposobnosti.

3. KONCEPTUALNE I ETIČKE DEBATE O SAJBER RATU

SAJBER RAT KAO SIVA ZONA:

Koncept "cyber rata" zauzima sporan prostor, uglavnom zato što prkosi tradicionalnim kategorizacijama sukoba. Za razliku od kinetičkog ratovanja, koje uključuje otvoreno fizičko nasilje, sajber rat spaja elemente špijunaže, kriminala i sabotaže, stvarajući maglovitu sivu zonu u kojoj je granica između rata i mira često zamagljena. Na primjer, ruski sajber napadi na električne mreže i komunikacijske mreže Ukrajine tokom sukoba usklađeni su s ciljevima konvencionalnog ratovanja, ali njihov relativno ograničen obim i nedostatak trajnog fizičkog uništenja ne uspijevaju zadovoljiti pragove koji se tipično povezuju s ratom. Ova dvosmislenost komplikuje zadatak definisanja "ratnih radnji" u sajber prostoru i postavlja izazove za uspostavljanje odgovarajućih pravnih i vojnih odgovora.

Dodatno usložnjavanje ove sive zone je izazov atribucije. Anonimna priroda sajber prostora bez granica omogućava napadačima da prikriju svoje porijeklo, što otežava definitivno pripisivanje napada određenim državnim ili nedržavnim akterima. Ovaj nedostatak jasnoće odlaže međunarodne odgovore i često rezultira fragmentiranim ili nedosljednim pristupom odvraćanju i odgovornosti. Pitanje da li značajan sajber napad predstavlja čin rata također stvara dileme za kreatore politike, budući da je prag odmazde u sajber prostoru i dalje nedefinisan prema međunarodnom pravu.

ETIČKE IMPLIKACIJE:

Etičke dimenzije sajber rata dodaju još jedan sloj složenosti. Sajber napadi često zamagljuju razliku između vojnih i civilnih ciljeva, što rezultira značajnom kolateralnom štetom. Na primjer, napadi ransomware-a na bolnice, općinske službe i javna preduzeća poremetili su osnovne usluge, ugrožavajući živote i dobrobit civila. Takvi incidenti pokazuju kako se sajber operacije, čak i kada su usmjerene na vojne ciljeve, mogu preliti na civilne domene. Ovo postavlja goruća etička pitanja o proporcionalnosti, nužnosti i legitimnosti takvih akcija u okviru međunarodnog humanitarnog prava.

Nedostatak fizičkog uništenja u mnogim cyber napadima ne negira njihove etičke posljedice. Poremećaji u električnim mrežama, na primjer, mogu indirektno uzrokovati štetu zaustavljanjem kritičnih medicinskih tretmana, ometanjem odgovora na hitne slučajeve ili ugrožavanjem ugroženog stanovništva tokom ekstremnih vremenskih događaja. Slično, napadi usmjereni na komunikacijske mreže mogu prekinuti žičare tokom kriza, dodatno pogoršavajući štetu civilima. Ove etičke dileme osporavaju postojeće norme sukoba, koje su prvenstveno dizajnirane za fizičko ratovanje, i pozivaju na ažurirane okvire koji se bave jedinstvenim karakteristikama sajber operacija.

POTREBA ZA NORMAMA I UPRAVLJANJEM:

Da bi se odgovorilo na ove konceptualne i etičke izazove, postoji hitna potreba za razvojem međunarodnih normi i mehanizama upravljanja specifičnih za sajber prostor. Dok okviri poput

Talinskog priručnika pružaju smjernice o primjenjivosti međunarodnog humanitarnog prava u sajber prostoru, njihova primjena ostaje ograničena. Štaviše, decentralizovana i dinamična priroda sajber domena zahteva kolaborativni pristup koji uključuje ne samo države već i privatne subjekte, međunarodne organizacije i civilno društvo.

Napori da se uspostave sajber norme također moraju uzeti u obzir raznolikost uključenih aktera, od nacionalnih država do kriminalnih sindikata i haktivista. Ova raznolikost komplikuje stvaranje univerzalnih standarda, ali i naglašava važnost saradnje sa više zainteresovanih strana. Transparentni mehanizmi za pripisivanje, odgovornost i proporcionalnost su od suštinskog značaja za ublažavanje rizika od eskalacije i osiguravanje da se sajber operacije pridržavaju etičkih i pravnih standarda.

Konačno, tekuće debate oko sajber rata odražavaju širu borbu za prilagođavanje tradicionalnih koncepata rata i mira stvarnosti digitalnog doba. Kako granice između civilnih i vojnih domena nastavljaju da erodiraju u sajber prostoru, potreba za jasnim definicijama, čvrstim upravljanjem i etičkom odgovornošću postaje sve kritičnija.

ULOGA I STAV UN-A O SAJBER RATOVANJU:

Ujedinjene nacije (UN) su prepoznale sajber sigurnost kao kritično globalno pitanje, bavećи se rastućim rizicima sajber ratovanja kroz inicijative kao što su Grupa vladinih eksperata UN-a (GGE) i Otvorena radna grupa (OEWG). Ovi forumi naglašavaju da se postojeće međunarodno pravo, uključujući principe suvereniteta i neintervencije, primjenjuje na sajber prostor. GGE-ov izvještaj iz 2015. godine navodi dobrovoljne norme odgovornog ponašanja države, kao što je zaštita kritične infrastrukture i promoviranje inicijativa za izgradnju kapaciteta za pomoć zemljama u razvoju.

Uprkos ovim naporima, izazovi i dalje postoje. Poteškoće pri atribuciji ometaju odgovornost za sajber napade, a različiti prioriteti među državama članicama, kao što je fokus Rusije i Kine na državni suverenitet u odnosu na naglasak zapadnih zemalja na ljudskim pravima, komplikuju konsenzus. Štaviše, većina sporazuma ostaje neobavezujuća, što ograničava provedbu.

UN promovira izgradnju kapaciteta, s organizacijama poput Međunarodne unije za telekomunikacije (ITU) koje pomažu državama u jačanju njihovih strategija kibernetičke sigurnosti i podsticanju razmjene informacija. Međutim, nedostatak obavezujućeg globalnog ugovora specifičnog za sajber ratovanje naglašava potrebu za poboljšanim normama, mehanizmima odgovornosti i tehnološkim ulaganjima.

Budući napori moraju se fokusirati na stvaranje obavezujućih sporazuma, poboljšanje sposobnosti atribucije i rješavanje digitalnog jaza kako bi se osigurala globalna sajber otpornost. UN ostaje ključna platforma za podsticanje međunarodne saradnje u upravljanju sajber prostorom.

4. PREDLOŽENI OKVIR ZA BUDUĆU SAJBER SIGURNOST

STRATEŠKI UVIDI

Integrisana nacionalna sajber odbrana: Države moraju uspostaviti centralizovane jedinice za sajber odbranu da nadgledaju, otkrivaju i reaguju na sajber pretnje u realnom vremenu. Izvlačeći pouke iz estonskog CCDCOE-a i ukrajinske IT armije, ove jedinice bi trebale integrirati stručnost vlade, privatnog sektora i akademske zajednice. Takve jedinice moraju biti opremljene naprednim alatima za rješavanje višestrukih prijetnji, uključujući zlonamjerni softver, ransomware i špijunske kampanje. Međunarodna saradnja je neophodna; Čvrsta partnerstva mogu omogućiti razmjenu obavještajnih podataka, brzu koordinaciju odgovora i usklađene protokole. Na primjer, zajedničke vježbe i simulacije među savezničkim državama mogu poboljšati spremnost i izgraditi povjerenje, osiguravajući kolektivnu otpornost na sofisticirane protivnike.

Spremnost za hibridni rat: Rusko-ukrajinski rat naglašava neophodnost integracije sajber operacija sa konvencionalnom vojnom taktikom. Cyber alati bi trebali biti ugrađeni u šire operativne okvire kako bi se poremetila logistika neprijatelja, degradirala komunikacija i potkopao moral, čime bi se pojačao utjecaj kinetičkih operacija. Ova integracija zahtijeva vojne doktrine koje tretiraju sajber prostor kao domen jednak kopnu, zraku i moru. Osim toga, wargaming i planiranje scenarija mogu pripremiti snage da efikasno iskoriste sajber sposobnosti u hibridnim sukobima.

BIHEVIORALNE I OBRAZOVNE INTERVENCIJE

Programi kibernetičke higijene: Nacionalne kampanje trebale bi ciljati na specifične ranjivosti u individualnim i organizacijskim praksama sajber sigurnosti. Osim opšte svijesti, od suštinskog su značaja prilagođeni programi za vladine službenike, operatere kritične infrastrukture i privatni sektor. Na primjer, obavezne certifikacije za sajber sigurnost, redovne simulacije krađe identiteta i poticajno usvajanje sigurnih praksi mogu značajno smanjiti ljudsku grešku, koja ostaje vodeći uzrok kršenja. Ovi programi se također moraju baviti novim tehnologijama, kao što je IoT, kako bi se umanjili rizici povezani sa sve povezanijim sistemima.

Kampanje podizanja svijesti javnosti: sukob u Ukrajini pokazuje moćnu ulogu informacionog rata. Vlade se moraju proaktivno suprotstaviti dezinformacijama i dezinformacijama sarađujući sa tehnološkim platformama kako bi otkrile i uklonile lažne narative. Inicijative javnog obrazovanja trebale bi osnažiti građane u vještinama medijske pismenosti, omogućavajući im da prepoznaju i odole se propagandi. Nadalje, ulaganja u organizacije za provjeru činjenica i alate za verifikaciju sadržaja vođene umjetnom inteligencijom mogu poboljšati kredibilitet digitalnih ekosistema.

ULAGANJA U TEHNOLOGIJU I INFRASTRUKTURU

Otporna infrastruktura: Jačanje otpornosti infrastrukture ključno je za nacionalnu sigurnost. Ovo uključuje usvajanje redundantnih sistema kako bi se osigurao kontinuitet usluge, napredno šifriranje za osiguranje osjetljivih podataka i automatizirano otkrivanje prijetnji za identifikaciju kršenja u realnom vremenu. Pored toga, saradnja sa privatnim sektorom, koji posjeduje većinu kritične infrastrukture, je od vitalnog značaja za uspostavljanje jedinstvenih standarda i protokola odgovora. Redovno testiranje na stres i testiranje penetracije kritičnih sistema može dodatno poboljšati spremnost.

Napredne tehnologije: Ulaganja u umjetnu inteligenciju (AI) i kvantne tehnologije predstavljaju budućnost sajber sigurnosti. Sistemi vođeni umjetnom inteligencijom mogu predvidjeti, identificirati i ublažiti prijetnje brže od ljudskih analitičara, koristeći mašinsko učenje kako bi se prilagodili vektorima napada koji se razvijaju. Šifriranje otporno na kvantnost će zaštititi komunikaciju i podatke od novih prijetnji kvantnog računarstva, osiguravajući dugoročnu sigurnost. Vlade i privatne firme trebale bi uspostaviti centar za inovacije kako bi ubrzali istraživanje i razvoj u ovim oblastima, podstičući konkurentsku prednost u sajber odbrani.

ZAKLJUČAK

Pejzaž sajber prijetnji koji se brzo razvija zahtijeva proaktivan, kolaborativni i sveobuhvatan pristup kako bi se osigurala globalna sajber sigurnost. Nedavni sukobi, uključujući rusko-ukrajinski rat, pokazuju da je sajber prostor postao kritična domena u kojoj nacije moraju zaštititi svoju infrastrukturu, suprotstaviti se dezinformacijama i održati povjerenje javnosti. Sajber bezbjednost više nije tehničko pitanje ograničeno na IT odjele, već strateški imperativ koji utiče na nacionalnu sigurnost, ekonomsku stabilnost i geopolitičku dinamiku.

Ujedinjene nacije moraju preuzeti vodeću ulogu u rješavanju ovog hitnog pitanja. Omogućujući razvoj globalno obavezujućeg cyber ugovora, UN mogu uspostaviti jasne norme za odgovorno ponašanje države, mehanizme za pripisivanje i odgovornost, te protokole za reagovanje na sajber incidente. Ovaj sporazum bi trebao dati prioritet zaštiti kritične infrastrukture, regulisanju sajber oružja i zaštitnim mjerama za sprječavanje civilne štete tokom sajber operacija.

Da bi se to postiglo, UN također moraju pokrenuti Akcioni plan za kibernetičku sigurnost i mir, uključujući:

Globalne kampanje podizanja svijesti: Podižite svijest među nacijama, korporacijama i pojedincima o važnosti sajber sigurnosti i njenoj ulozi u održavanju globalne stabilnosti.

Inicijative za izgradnju kapaciteta: Pružati tehničku i finansijsku podršku zemljama u razvoju kako bi ojačale svoje sposobnosti za sajber bezbjednost.

Javno-privatna partnerstva: Angažirajte se sa tehnološkim kompanijama, akademicima i civilnim društvom kako biste podstakli inovacije i saradnju u praksi sajber bezbjednosti.

Podizanje svijesti i podsticanje međunarodne saradnje su ključni za rješavanje rastuće složenosti sajber prijetnji. Vrijeme za djelovanje je sada – nacije moraju prepoznati da je osiguranje cyber prostora fundamentalno za očuvanje mira i prosperiteta u 21. vijeku.

LITERATURA

[1] Bokil, R. (2023). Cyber Warfare: Taking War to Cyberspace and its Implications for International Humanitarian Law. International Journal for Multidisciplinary Research, 5(1), 1–12. https://doi.org/10.36948/ijfmr.2023.v05i01.1494

[2] Europol (2023). Europol sounds alarm about criminal use of ChatGPT, sees grim outlook. https://www.reuters.com/technology/europol-

[3] Lakomaa, E. (2017). The history of business and war: introduction. *Scandinavian Economic History Review*, *65*(3), 224–230. https://doi.org/10.1080/03585522.2017.1397314

[4] Lewis, J. Cyber Terror: Missing in action. *Know Techn Pol* **16**, 34–41 (2003). https://doi.org/10.1007/s12130-003-1024-6

[5] Mueller, G. B., Jensen, B., Valeriano, B., Maness, R. C., & Macias, J. M. (2023). *Cyber Operations during the Russo-Ukrainian War: From Strange Patterns to Alternative Futures*. Center for Strategic and International Studies (CSIS). http://www.jstor.org/stable/resrep52130

[6] von Wussow, P. (2019). "Cyberwar": Past and Present of a Contested Term. Conflict Zone Cyberspace: Prospects for Security and Peace Cyberspace as a Domain of Military Action 2 ETHICS AND ARMED FORCES 01/19.

[7] Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., & Basim, H. N. (2020). Cyber Security Awareness, Knowledge and Behavior: A Comparative Study. *Journal of Computer Information Systems*, *62*(1), 82–97. https://doi.org/10.1080/08874417.2020.1712269

[8] https://www.controlrisks.com/riskmap/top-risks?utm_referrer=https://core.ac.uk

[9] Unexpectedly, All UN Countries Agreed on a Cybersecurity Report. So What? https://translate.google.com/?sl=auto&tl=bs&text=Unexpectedly%2C%20All%20UN%20Countries%20Agreed%20on%20a%20Cybersecurity%20Report.%20So%20What%3F&op=translate

[10] Cybersecurity and New Technologies, https://www.un.org/counterterrorism/cybersecurity?utm_source=chatgpt.com