Pregledni naučni članak UDC 327:316.48(004:32.019.5)

Miloš Vukelić*

Sukobi u sajber prostoru „ispod praga rata": sajber oružje u obaveštajnom nadmetanju država**

Apstrakt

Ovaj rad predstavlja pregled ključnih nalaza literature međunarodnih odnosa koja se bavi sukobima država u sajber prostoru. Glavni zaključci su da do sada u sajber sukobima nije pređen „prag rata". Potom, da umesto rata svedočimo „sivoj zoni" obaveštajnog, odnosno informacionog nadmetanja država u sajber prostoru koje se može videti na mnoštvu sabotaža, subverzija i špijunaža. Na kraju, u radu su izneseni konkretni primeri iskorišćavanja ranjivosti aktera u sajber domenu, kao i oružja koje se koristi u te svrhe. Takvoj vrsti oružja države su u prethodnim decenijama neretko pribegavale. Cilj rada je da se razume manir delovanja država u sajber prostoru u odnosu na širi kontekst međunarodnih odnosa.

Ključne reči:

sajber sukob, sajber prostor, sajber bezbednost, obaveštajno nadmetanje, međunarodni odnosi

* milos.vukelic@fpn.bg.a.rs

** Istraživanje sprovedeno uz pomoć Fonda za nauku Republike Srbije, br. projekta 7744512, Monitoring i indeksiranje mira i bezbednosti na Zapadnom Balkanu – MIND / This research was supported by the Science Fund of the Republic of Serbia, grant no. 7744512, Monitoring and Indexing Peace and Security in the Western Balkans – MIND". Takođe, zahvalio bih se Gregoriju Vingeru (Gregory Winger) sa Univerziteta u Sinsinatiju, brz čijih predavanja ovaj rad ne bi bio moguć.

HOĆE LI BITI SAJBER RATA?

„Neće biti sajber rata" i „Biće sajber rata" naslovi su dva članka iz 2012. i 2013. godine, u kojima autori naglašeno zastupaju jednu ili drugu opciju. Argument o odsustvu nekakvog budućeg rata u sajber prostoru počiva na pretpostavkama koje je postavio Klauzevic pre dvesta godina, i one podrazumevaju da svaki čin rata mora ispunjavati tri kriterijuma: potencijal smrtonosnosti; da je instrumentalan; i suštinski političan. Tomas Rid (Thomas Rid) tvrdi da do sada nismo imali primer sajber ofanzive koja po sebi predstavlja čin rata jer je nedostajao element smrtonosnosti. Takođe, sajber ofanzivna sredstva nisu bivala ni instrumentalna, jer neretko podrazumevaju špijunažu zato što se „ukazala prilika", bez jasnog strateškog cilja. Konačno, u sajber sferi ofanzive nekada nemaju ni obeležja političnosti, budući da im cilj zaista ne mora biti politički.[1]

Nema sumnje da u sajber prostoru akteri, uključujući i one državne, deluju i sa jasnim strateškim i političkim ciljevima. Stoga su i sajber ofanzive po sebi često političke, tj. nastavak političkog opštenja, kao što je i rat, po Klauzevicovom mišljenju, puki nastavak politike.[2] Politika je, po Klauzevicovom mišljenju, stvar kontinuuma koji može ići od „trgovine, diplomatije i svih drugih interakcija između ljudi i vlada" pa sve do rata.[3] Ipak, čak i kada imamo ispunjene elemente instrumentalnosti i političnosti, nedostatak smrtonosnih ishoda je za Rida bio dovoljan da zaključi da sajber rata nije bilo, a verovatno neće biti razloga da ga u budućnosti i bude.

S druge strane, kada nalazi da će „biti sajber rata" Džon Stoun (John Stone) ne koristi smrtonosnost prema ljudima kao ključni kriterijum u svojoj oceni, već tvrdi da je za rat dovoljna i činjenica da ofanzivne akcije u sajber prostoru mogu da „razbiju stvari". Klauzevic u svom dobu sigurno nije mogao da pojmi domete i brzinu umreženosti sveta dva veka kasnije, kao što nije mogao da predvidi da čin ukucavanja koda na jednom kraju planete gotovo instantno može da napravi štetu na drugom kraju. Takođe, reći da nečega do sada nije bilo ne znači da ga u budućnosti neće i biti, pogotovo ukoliko znamo da sajber ofanzive nose mogućnost smrtonosnosti. Zbog potencijala čitavog spektra sajber napada na kritičnu infrastrukturu, poput fabrika za preradu voda, energetskog sistema, kontrola letenja itd., nekadašnji sekretar odbrane

---

1 Thomas Rid, "Cyber War Will Not Take Place", *Journal of Strategic Studies*, Vol. 35, No. 1, 2012, pp. 5–32, pp. 6–15.

2 Carl von Clausewitz (Peter Paret, Michael Eliot Howard, and Carl von Clausewitz), *On War*, Princeton University Press, 2008, p. 87, 605.

3 P. W. Singer and Emerson T. Brooking, "What Clausewitz Can Teach Us About War on Social Media", *Foreign Affairs*, October 4, 2018. Available from: https://www.foreignaffairs.com/world/what-clausewitz-can-teach-us-about-war-social-media (Accessed September 4, 2023).

SAD, Leon Paneta (Leon Panetta) u jednom od svojih govora izjavio je da se samo čeka „sajber Perl Harbor".[4] Zaista, čini se da sa današnjim spektrom potencijalnih napada, rat, i to moguće vrlo smrtonosan, može biti dobijen korišćenjem samo informacione sfere.

Međutim, kako do sada još uvek nismo svedočili takvom fenomenu, postavljaju se dva međusobno povezana pitanja. Prvo, kako bismo onda klasifikovali dosadašnja ofanzivna dejstva u sajber prostoru, i drugo, koja oružja su korišćena pri takvim delatnostima? U nastavku rada ću napraviti pregled literature koja se bavi ovim pitanjima uz prihvatanje teze da smo do sada, kada je u pitanju delovanje država, svedočili sajber ofanzivama uglavnom u sklopu šireg konteksta obaveštajnog takmičenja. Takođe, uz navođenje konkretnih primera, navešću i o kakvoj vrsti obaveštajnih delatnosti se radi i, konačno, kakva vrsta sajber oružja je korišćena u njihovom sprovođenju. Ciljevi rada su pružanje pregleda i klasifikacije osnovnih koncepata za izučavanje nadmetanja u sajber prostoru između država, kao i kontekstualizacija sajber sukobljavanja u širem okruženju međunarodnih odnosa.

SIVA ZONA, HIBRIDNI RATOVI I SUKOBI ISPOD PRAGA RATA

Ukoliko bismo usvojili argument da zbog nedostatka smrtnosti do sada nismo svedočili ratovima, kako bismo onda opisali dosadašnje ofanzivne akcije država i drugih aktera u sajber prostoru? Najšire moguće određenje u literaturi jeste da se radi o nekakvoj „sivoj zoni". Ona ne podrazumeva potpuni „mir, niti oružane sukobe", već se „strateško takmičenje država (...) odvija ispod praga oružanog sukoba".[5] Usled odsustva vrhovne vlasti u međunarodnim odnosima države imaju podsticaje da se služe mnoštvom instrumenata koji nisu oružani kako bi oslabile svoje protivnike. Među tim instrumentima su svakako i: podrška političkom antiestablišmentu unutar države takmaca; plasiranje odgovarajuće propagande koja može da podrije postojeće dominantne narative protivnika; ekonomska prinuda; agresivne obaveštajne delatnosti; sajber napadi, ali i posrednički (proxy) ratovi itd.[6]

---

4 Leon Panetta, "Defense secretary warns of 'cyber Pearl Harbor'". *CBS News YouTube Channel,* October 13, 2012. Available from: https://www.youtube.com/watch?v=C2Qp59aQyu4 (Accessed September 4, 2023).

5 Javier Jordan, "International Competition Below the Threshold of War: Toward a Theory of Gray Zone Conflict", *Journal of Strategic Security*, Vol. 14, No. 1, 2020, pp. 1–24. p. 2.

6 *Ibid*., pp. 10–15.

Kao što vidimo, radi se o mnoštvu političkih, ekonomskih, propagandnih, obaveštajnih i drugih sredstava koji mogu slabiti protivnika bez direktne oružane konfrontacije. Ovakav „paradoks stabilnosti–nestabilnosti" moguć je i zbog toga što velike sile nisu sklone direktnom sukobu, pre svega zbog posedovanja nuklearnog oružja.[7] Podstaknuto dokumentom iz 2013. godine načelnika Generalštaba oružanih snaga Rusije, Valerija Gerasimova (Вале́рий Васи́льевич Гера́симов), „siva zona" se u literaturi još naziva i „hibridnim ratovanjem". Gerasimov govori o „širokoj upotrebi političkih, ekonomskih, informacionih, humanitarnih i drugih nevojnih mera primenjenih u koordinaciji sa protestnim potencijalom populacije", kao i o „simultanom sukobljavanju u svim fizičkim okruženjima i informativnom prostoru".[8]

Kada govorimo o sivoj zoni ili hibridnom ratovanju, u literaturi koja se bavi sajber bezbednošću iz perspektive međunarodnih odnosa uvrežila se kovanica o „sukobima ispod praga rata" ili „ispod praga oružanog sukoba".[9] U svakom slučaju, dosadašnje ofanzivne delatnosti država u informacionom okruženju nisu dosegle nivo rata. Međutim, ofanzive su brojne, i to iz nekoliko razloga. Prvo, sajber prostor i njegova siva zona omogućavaju asimetrično ratovanje i gradualizam. Države mogu imati manju političku, vojnu ili ekonomsku moć, ali sajber prostor im pruža priliku nesrazmernog uticaja na snagu protivnika usled: demokratičnosti ulaska u sajber prostor (u smislu njegove anonimnosti, masovnosti i jeftinog pristupa);[10] problema teškog pripisivanja sajber napada (problema atribucije);[11] tehnološke volatilnosti ili čestih

---

7 Robert Jervis, *The meaning of the nuclear revolution: Statecraft and the prospect of Armageddon*, Cornell University Press, 1989, p. 20.

8 Valery Gerasimov, "The Value of Science in the Foresight", *Military Review*, January/February 2016. Available from: https://www.armyupress.army.mil/portals/7/military-review/archives/english/militaryreview_20160228_art008.pdf (Accessed September 4, 2023).

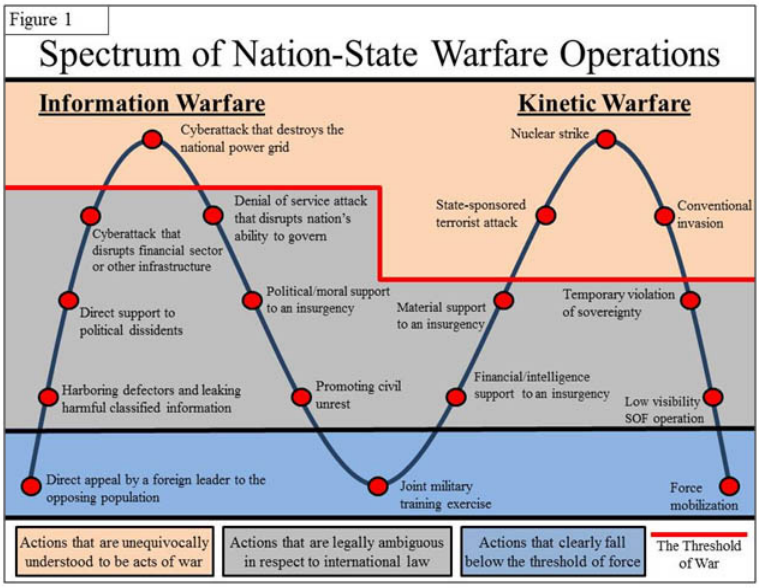
9 Michael P. Fischerkeller, and Richard J. Harknett, "Deterrence is not a credible strategy for cyberspace", *Orbis*, Vol. 61, No. 3, 2017, pp. 381–393.

10 Alex Wilner, "US cyber deterrence: Practice guiding theory", *Journal of Strategic Studies*, Vol. 43, No. 2, 2020, pp. 245–280.

11 Thomas Rid, and Ben Buchanan, "Attributing cyber attacks", *Journal of Strategic Studies*, Vol. 38, No. 1–2, 2015, pp. 4–37.

menjanja pravila igre,[12] velike verovatnoće ljudske greške pri sajber odbrani,[13] kao i brzine zbivanja u celokupnom sajber prostoru[14].

Figura 1. Spektrum ratnih operacija nacija–država[15]



Gradualizam podrazumeva da će mnoštvo malih operacija proći nezapaženo ukoliko se posmatraju individualno, ali će kumulativno doneti koristi onome koji ih sprovodi.[16] Višegodišnje umešno i strateško korišćenje sajber prostora,

---

12 Chris McGuffin, and Paul Mitchell. 2014. "On Domains: Cyber and the Practice of Warfare", *International Journal*, Vol. 69, No. 3, 2014, pp. 394–412.

13 George Platsis, "The human factor: Cyber security's greatest challenge". In *Cyber Law, Privacy, and Security: Concepts, Methodologies, Tools, and Applications*, IGI Global, 2019, pp. 1–19.

14 Will Goodman,. 2010. "Cyber deterrence: Tougher in theory than in practice?" *Strategic Studies Quarterly*, Vol. 4, No. 3, 2010, pp. 102–135.

15 Preuzeto iz: Jason Rivera, "Understanding and Countering Nation-State Use of Protracted Unconventional Warfare", *Small Wars Journal*. Available from: https://smallwarsjournal.com/jrnl/art/understanding-and-countering-nation-state-use-of-protracted-unconventional-warfare (Accessed September 4, 2023).

16 Javier Jordan, "International Competition Below the Threshold of War: Toward a Theory of Gray Zone Conflict", *Journal of Strategic Security*, Vol. 14, No. 1, 2020, pp. 1–24. p. 4.

stoga, može znatno unaprediti relativni položaj neke države, što bi bez takvih akcija bilo nedostižno. Međutim, zbog glavnih strateških karakteristika sajber domena, kao što su demokratičnost, problem atribucije itd., mnoštvom manjih operacija se ne služe samo mali, već i velike sile. U prevodu, tehniku „smrti sa hiljadu rezova"[17] usvajaju i velike sile kao glavnu državnu strategiju u informacionoj sredini.[18] Gledano sve zajedno, može se reći da je sukobljavanje ispod praga rata *modus operandi* odnosa između država takmaca u sajber prostoru, bez obzira na njihovu veličinu.

OBAVEŠTAJNA DELATNOST ILI NEŠTO VIŠE?

Neophodno je precizirati šta države postižu sukobljavanjem ispod praga rata da bi se jasnije odredilo pod kakvu delatnost država spadaju sajber ofanzive. U literaturi međunarodnih odnosa imamo viđenje da se radi o nadgradnji klasičnih obaveštajnih radnji.[19] Odnosno, da sajber prostor državama služi radi obaveštajnog nadmetanja ili „informacionog duela" u kojima se rivali takmiče u tome „ko će da ukrade informacije jedan od drugog, kako da zaštite ono što su pribavili, i kako da korumpiraju podatke i komunikacije druge strane".[20] Nesumnjivo je da su obim informacija i nepresušnost ofanzivnih prilika znatno veći u sajber prostoru u odnosu na klasične obaveštajne radnje. Ta razlika navela je pojedine istraživače da zaključe da je razlika u obimu sasvim dovoljna da konstatujemo da se ne može raditi o istom fenomenu i da obave-

---

17 Radi se o kineskom pristupu mučenju, gde bi žrtva bila predmet duge smrti sporim ispuštanjem krvi usled velikog broja rezova. Ova kovanica se koristi i za čest ofanzivni strateški pristup države sajber prostoru. Ryan C. Maness, 2021. "Death by a Thousand Cuts: Is Russia Winning the Information War with the West?" in (eds.) Mai'a K. Davis Cross and Ireneusz Paweł Karolewski, *European-Russian Power Relations in Turbulent Times*, The University of Michigan Press, Ann Arbout, Mi, 2021, pp. 160–186.

18 Za teorijsko obrazloženje strategije videti: Richard Harknett, and Max Smeets, "Cyber campaigns and strategic outcomes", *Journal of Strategic Studies*, Vol. 45, No. 4, 2020, pp. 534–567; Michael P. Fischerkeller, Emily O. Goldman, and Richard J. Harknett, *Cyber persistence theory: Redefining national security in cyberspace*, Oxford University Press, 2022. Za konkretnu strategiju koja je eksplicitno usvojila ovaj pristup „upornog angažmana" videti: "Department of Defense Cyber Strategy", *United States Department of Defense*, Washington DC, 2018.

19 Thomas Rid, "Cyber War Will Not Take Place", *Journal of Strategic Studies*, Vol. 35, No. 1, 2012, pp. 5–32, p. 15.

20 Joshua Rovner, "What is an Intelligence Contest?", *Texas National Security Review*, Fall 2020, pp. 114–120, p. 115.

štajno nadmetanje nije adekvatan opis onoga što se dešava u informacionom okruženju.[21] Ipak, veći obim operacija i dalje ne znači da je promenjen njihov karakter, što čini da govorimo, makar za sada, o obaveštajnom nadmetanju.[22]

Informaciono ili obaveštajno nadmetanje podrazumeva u našem slučaju makar tri stvari: sabotaže, subverzije i špijunaže. Tomas Rid nalazi da je sabotaža „namerni pokušaj slabljenja ili uništavanja ekonomskog ili vojnog sistema". Potom, da je špijunaža „pokušaj penetracije protivničkog sistema radi izvlačenja osetljivih i zaštićenih informacija". Na kraju, subverzija podrazumeva namerni pokušaj da se potkopa autoritet, integritet i (...) uspostavljeni autoritet ili red". Sve tri stvari često moraju da podrazumevaju visok stepen tehničkih veština, ali neretko su omogućene društvenim interakcijama, tj. nisu moguće bez ljudskog faktora ili greške.[23]

SABOTAŽE

Do sada smo imali mnoštvo primera da države izdašno koriste sve tri vrste ovih delatnosti u sajber prostoru. Prvo, svrha sabotaže je da stvari rade drugačije u odnosu na ono što očekujemo, što može da nas zbuni, ili da dugoročno čini veliku štetu, a da i ne shvatamo da se neko „petlja" u naš sistem. Tipičan primer sabotaže jeste veliki sajber napad na iransko nuklearno postrojenje Natanz. Napad je otkriven 2010. godine, a vrlo brzo je pripisan SAD i Izraelu, iako ove države i dalje poriču direktnu umešanost. Napad je podrazumevao ubacivanje malicioznog programa (*malware*) u postrojenje (najverovatnije putem zaraženog USB-a). Program je zatim vrlo precizno sabotirao centrifuge koje služe za obogaćivanje uranijuma, tako što je kontrolerima zaduženim za njihov obrtni momenat davao signal za naglo ubrzavanje (preko granica mogućnosti), ili naglo usporavanje, što je u kratkom roku činilo da se centrifuge

---

21 Michael Warner, "The Character of Strategic Cyberspace Competition and the Role of Ideology" in (eds.) Robert Chesney and Max Smeets, *Deter, Disrupt, Or Deceive: Assessing Cyber Conflict as an Intelligence Contest*. Georgetown University Press, 2023.

22 Jedan od istraživača fenomena sajber bezbednosti smatra da pokušaji da se sajber operacije „rebrendiraju" u nešto drugo jesu neretko i marketinški trikovi bezbednosne zajednice kako bi se uvećali javni fondovi namenjeni odbrani. John Lindsay, "Hidden Dangers in the US Military Solution to a Large-Scale Intelligence Problem" in (eds.) Robert Chesney and Max Smeets, *Deter, Disrupt, Or Deceive: Assessing Cyber Conflict as an Intelligence Contest*. Georgetown University Press, 2023.

23 Thomas Rid, "Cyber War Will Not Take Place", *Journal of Strategic Studies*, Vol. 35, No. 1, 2012, pp. 5–32, p. 16–22.

kvare. Pritom, operateri ni u jednom trenutku nisu mogli da shvate zašto se kvari veliki broj centrifuga, budući da je malver, nazvan Staksnet (Stuxnet), signalizirao kompjuterima da je sa turbinama sve u redu. Ova sabotaža je zahtevala izuzetno visoka softverska i hardverska, dakle tehnička znanja, ali je podrazumevala i oslanjanje na ljudsku grešku. Recimo, tadašnji iranski predsednik je u jednom propagandnom videu prilikom posete postrojenju praktično omogućio celom svetu da vidi šta se dešava na kompjuterima koji kontrolišu turbine, zbog toga što su kamere slučajno (ili namerno) snimile ekrane računara. Staksnet napad nije neposredno doveo do ljudskih žrtava, ali jeste „polomio stvari".[24]

Iran nije dugo čekao na kontrasabotažu, ili, makar su SAD smatrale da Iran stoji iza jednog od kontranapada. U 2013. godini onemogućeno je daljinsko upravljanje Boumen Avenju branom (The Bowman Avenue Dam) u državi Njujork. Naime, infiltracijom u sistem upravljanja, napadači su onesposobili zatvaranje brane na daljinu. Radi se o izuzetno maloj brani, te su pretpostavke ili da su Iranci poslali signal kako i oni mogu da izvrše sofisticirane sabotaže služeći se sajber prostorom (u konkretnom slučaju infiltracija se dogodila preko mobilnog modema). Ili, postoji i opcija da su greškom napali manju od dve brane sa istim imenom, budući da se druga, dvanaest puta viša Boumen Avenju brana, nalazi u državi Oregon.[25]

Umešni ruski napadi na kritičnu infrastrukturu Ukrajine nakon 2014. godine postali su učestala pojava. Tako je Rusija npr. bila sposobna da „upali" ili „ugasi" ukrajinski energetski sistem po volji, kao što je učinjeno 2014. godine gašenjem mreže na sat vremena. Takođe, vrlo lako je sabotirala kablove koji spajaju Krim sa Ukrajinom.[26] Na početku invazije 2022. godine Rusi su sabotirali i komunikacije satelitskog internet provajdera KA-SAT, koji je uneo

---

24 Za opis napada i njegovih posledica videti: James Farwell, and Rafal Rohozinski, "Stuxnet and the Future of Cyber War", *Survival*, Vol. 53, No. 1, 2011, pp. 23–40; John Lindsay, "Stuxnet and the Limits of Cyber Warfare", *Security Studies,* Vol. 22, No. 3, 2013, pp. 365–404. Anonimna svedočenja američkih službenika i komentari zvaničnika SAD o ovom incidentu se mogu pogledati i u dokumentarnom filmu: Alex Gibney, *Zero days*, Showtime, USA, 2016.

25 Joseph Berger, "A dam, small and unsung, is caught up in an Iranian hacking case", *The New York Times*, March 26, 2016. Available from: https://www.nytimes.com/2016/03/26/nyregion/rye-brook-dam-caught-in-computer-hacking-case.html (Accessed September 4, 2023); Mark Thompson, "Iranian cyber attack on New York dam shows future of war", *Time*, March 24, 2016. Available from: https://time.com/4270728/iran-cyber-attack-dam-fbi/ (Accessed September 4, 2023).

26 Benjamin Jensen, Brandon Valeriano, and Ryan Maness, "Fancy bears and digital trolls: Cyber strategy with a Russian twist", *Journal of Strategic Studies,* Vol. 42, No. 2, 2019, pp. 212–234.

potpunu konfuziju u komunikaciji ukrajinskih policijskih, obaveštajnih i vojnih jedinica.[27] Sabotaža modema američke kompanije VIASAT, koja je poslovala u Ukrajini, dovela je do prelivanja napada na širu VIASAT infrastrukturu. Zbog toga ne samo da je nestao internet u drugim delovima Evrope, već je ugrožena i kontrola rada na daljinu 5.800 vetroturbina (uključujući i one u Nemačkoj).[28] Bilo kako bilo, dosadašnji primeri sabotaža pokazuju izuzetnu potentnost sajber prostora u smislu uticaja na kritičnu infrastrukturu, ali i potencijala širenja napada i njihovih (ne)nameravanih posledica. Ubrzanje broja sabotaža kritične infrastrukture od strane državnih aktera, pogotovo nakon Staksneta, govori nam da se radi o fenomenu na koji moramo da se naviknemo.

SUBVERZIJE

Subverzija, u smislu pokušaja potkopavanja autoriteta i integriteta ličnosti ili institucije, takođe je sveprisutna u sajber prostoru. Literatura na engleskom jeziku je sasvim logično pod dominacijom američke akademske i novinarske sfere, što dovodi da u primerima subverzija imamo prezastupljenost opisivanja ruskog pokušaja mešanja u američki izborni sistem manipulacijom društvenih mreža. Tako se u čuvenom Milerovom izveštaju (Mueller Report), ali i drugim svedočenjima pred Senatom SAD, navodi da je Agencija za istraživanje interneta (Internet Research Agency – IRA), pod kontrolom Jevgenija Prigožina (Евгений Пригожин), putem „farme trolova" pokušala da manipuliše predsedničkim izborima u SAD 2016. godine. Milerovo istraživanje, ali i drugi svedoci, uključujući i predstavnike društvene mreže Tviter (Twitter) i Fejsbuk (Facebook), konstatuju da je Prigožinova agencija svojim statusima na društvenim mrežama i putem neautentičnih naloga i grupa doprla do 126.000.000 ljudi tokom dve godine.[29] Tviter je početkom 2018. godine identifikovao 3.841 „Prigožinov" nalog i direktno obavestio 1.400.000 ljudi da su

---

27 David Cattler, and Daniel Black. *The Myth of the Missing Cyberwar*. Foreign Affairs, April 6, 2022. Available from: https://www.foreignaffairs.com/articles/ukraine/2022-04-06/myth-missing-cyberwar (Accessed September 4, 2023).

28 Matt Burges, "A Mysterious Satellite Hack Has Victims Far Beyond Ukraine", *Wired*, March 23, 2022. Available from: wired.com/story/viasat-internet-hack-ukraine-russia (Accessed September 4, 2023).

29 "Hearing Before the Senate Select Committee on Intelligence. Social Media Influence in the 2016 U.S. Election." *115th Cong. 13 (11/1/17) (testimony of Colin Stretch, General Counsel of Facebook)*, 2017; Robert Mueller, "Report On The Investigation Into Russian Interference In The 2016 Presidential Election", *Department of Justice Washington*, D.C. March 2019.

bili pod „stranim" uticajem.[30] Delatnosti IRA mogu se svesti pod subverziju koja podrazumeva eroziju poverenja u vidu plasiranja dezinformacija (disinformation) ili, pak, zloupotrebe istinitih informacija (malinformation) radi ostvarivanja zloćudne namere.[31] Cilj takve delatnosti jeste unošenje konfuzije, podsticanje nepoverenja u institucije, kao i snaženje društvene i političke polarizacije u širim društvenim okvirima.

Međutim, jedno je pitanje da li je postojao pokušaj ruskog mešanja u američki izborni sistem, a potpuno drugo da li je ta kampanja direktno zaslužna za porast međusobnog nepoverenja američkih republikanaca i demokrata. Istraživanja pokazuju da su stranice IRA na društvenim mrežama mahom reprodukovale sadržaj koji su već ranije proizveli sami Amerikanci, bilo da se radi o građanima, novinarima, ideolozima, političarima itd. Takođe, u relativnom odnosu, stranice IRA se mere promilima u odnosu na broj onih kojima su takođe upravljali Amerikanci, a koje su, ponovo, plasirale sadržaj sličan IRA.[32] U prevodu, američke stranice su znatno više doprinosile polarizaciji i međusobnom nepoverenju Amerikanaca, dok su stranice IRA zanemarljive u doprinošenju tom fenomenu. Ipak, mnogo je više buke dignuto zbog stranog mešanja nego zbog „domaće" generisanih podela. Bilo kakvo strano mešanje, nezavisno od njegovih stvarnih učinaka, vidljivije je u smislu pokušaja traženja krivca za domaću neslogu. Ovo se pogotovo odnosi na SAD koje su, zahvaljujući i svojoj geografskoj izolovanosti, istorijski mnogo manje bile podložne stranim uticajima na narative o dobrom i poželjnom društvu i narative o karakteru i kvalitetu unutrašnjih protivnika.

Takođe, kompletna arhitektura internet platformi jeste pogodna za društvenu i političku afektivnu polarizaciju. Možemo da kažemo da američki građani i političari, koji manipulišu informacijama u domaćem političkom i ideološkom sajber prostoru, vrše neku vrstu autosabotaže. Međutim, ukoliko žele da pobede u političkom takmičenju, a sve zbog postojeće arhitekture internet platformi, oni i nemaju drugu opciju nego da igraju na afekte svojih sledbenika

---

30 "Update on Twitter's review of the 2016 US election", *Twitter blog*, 2018. Available from: https://blog.twitter.com/en_us/topics/company/2018/2016-election-update (Accessed September 4, 2023).

31 Claire Wardle, and Hossein Derakhshan, "Information disorder: Toward an interdisciplinary framework for research and policymaking", *Council of Europe Report*, 2017.

32 Gregory Eady, Tom Paskhalis, Jan Zilinsky, Richard Bonneau, Jonathan Nagler, and Joshua A. Tucker, "Exposure to the Russian Internet Research Agency foreign influence campaign on Twitter in the 2016 US election and its relationship to attitudes and voting behavior", *Nature Communications*, Vol. 14, No. 1, 2023.

umesto pružanja pravovremenih i tačnih informacija.[33] Može se reći da firme sa Zapada istovremeno sa delovanjem IRA manipulišu izbornim sistemima sopstvenih, ali i drugih država, kao što je to činila npr. Kembridž analitika (Cambridge Analytica) u Trinidad i Tobagu već 2010. godine. Tada je cilj stranog mešanja i manipulacije bio obeshrabrivanje crne populacije sa tih ostrva da izađu na izbore.[34]

Ruski pokušaj mešanja u američke predsedničke izbore 2016. godine nije nikakav izuzetak, nego se radi o jednom od više slučajeva nove pravilnosti ili normalnosti. Ta pravilnost podrazumeva uspostavljanje obaveštajnog nadmetanja na osnovu podsticaja koji dolaze iz sajber prostora. Subverzije koje podrivaju autoritet stoga jesu nezaobilazni deo repertoara država (ili uticajnih kompanija) u sukobima ispod praga rata.

ŠPIJUNAŽE

Ako sajber prostor zaista jeste domen obaveštajnog nadmetanja država većeg obima, tom obimu u velikoj meri doprinosi špijunaža. Pre informacione ere, špijuniranje je zahtevalo vrlo obimne resurse, vreme i ljudski kapital specifičnog karaktera i obuke. Danas, uz negovanje sofisticiranih tehničkih sposobnosti profesionalaca, države ubiraju političke, ekonomske, obaveštajne i druge koristi ranije nepojmljive u smislu brzine i količine pribavljenih informacija.

Uzmimo za primer veliki sajber napad na Orion softver američke kompanije Solar Vinds (Solar Winds) tokom 2019. i 2020. godine, a koji je rastumačen tek 2021. i u detaljima postao rekonstruisan za širu javnost 2023. godine. Radi se o softveru koji su koristile velike tehnološke kompanije, poput Majkrosofta (Microsoft), Intela, Siska (Cisco) ili Mandianta, Gugl (Google) ćerke firme zadužene za sajber bezbednost. No, Orion su koristile i federalne institucije SAD, poput Ministarstva pravde (US Justice Department), Ministarstva odbrane (US Department of Defense), Ministarstva unutrašnje bezbednosti (Department of Homeland Security) itd. Radi se o najvećem hakovanju federalnih institucija SAD ikada. Svaki put kada bi neko u kompjuterima pomenutih institucija kliknuo ažuriranje Orion softvera napadači su uspevali da preusmere tok informacija ka sopstvenom komandnom centru, umesto ka serverima kompanije Solar Vinds. Time što je hakovan lanac snabdevanja (jedan od mnogih softvera koji koriste pomenute kompanije i institucije) u trenu je moglo biti

---

33 Miloš R. Vukelić, *Kulturni ratovi u Sjedinjenim Američkim Državama i Evropskoj uniji u periodu od 2014. do 2020. godine*, Doktorska disertacija, Univerzitet u Beogradu – Fakultet političkih nauka, 2023, str. 153–162.

34 Karim Amer and Jehane Noujaim, *The Great Hack*. Netflix, 2019.

zaraženo na milione kompjutera. Informacije koje su hakeri mogli da preuzmu tiču se npr. „detalja o planiranim sankcija protiv Rusije, o nuklearnim postrojenjima SAD i zalihama oružja, o bezbednosti izbornog sistema i druge kritične infrastrukture".[35] Kao što vidimo, pomenuti napad je sabotaža softvera, budući da je njegova funkcija naglo postala potpuno suprotna od očekivane, ali sve u svrhu špijunaže.

SAD su daleko od žrtve u špijunskim igrama informacione sfere. Edvard Snouden (Edward Snowden) je 2013. godine otkrio kako su, kroz program PRISM, SAD, zajedno sa Ujedinjenim Kraljevstvom, špijunirale takmace, ali i saveznike. PRISM je pokrivao primere koji se protežu od prisluškivanja lidera G7 država na sastanku 2009. godine,[36] preko korišćenja podataka pretraživača velikih tehnoloških kompanija poput Gugla,[37] pa do npr. hakovanja modema belgijskog operatera Belgacom, radi presretanja komunikacija unutar institucija Evropske unije.[38] Takođe, veruje se da su SAD, zajedno sa Izraelom, izradile Flejm (Flame) softver za špijunažu Irana, Egipta, Libana, Palestinske samouprave i drugih aktera na Bliskom istoku. Flejm je mogao da snima razgovore i uzima podatke sa zaraženih kompjutera. Recimo, jedna od funkcionalnosti tog malvera jeste da potpuno preuzme mikrofon zaražene jedinice, te snima razgovore u blizini ili preko tada popularnog Skajpa (Skype).[39]

Kina je po pitanju špijunaže sajber prostora među predvodnicima, u smislu obima i koristi od ove delatnosti po tu državu. Uzmimo za primer samo 2011. godinu, kada se pojavio izveštaj u kom se sumnja da je jedinica broj 61398 Narodnooslobodilačke armije Kine, stacionirana u Šangaju, izvršila napade na 70 različitih država i organizacija u periodu od nekoliko godina.[40]

---

35 Za detalje, tok i posledice napada videti: Kim Zetter, "The Untold Story of the Boldest Supply-Chain Hack Ever", *Wired*, May 2, 2023. Available from: https://www.wired.com/story/the-untold-story-of-solarwinds-the-boldest-supply-chain-hack-ever/ (Accessed September 4, 2023).

36 Max Smeets, *No shortcuts: Why states struggle to develop a military cyber-force*, Oxford University Press, Oxford, 2023.

37 Jinghan Zeng, Tim Stevens, and Yaru Chen, "China's Solution to Global Cyber Governance: Unpacking the Domestic Discourse of 'Internet Sovereignty'", *Politics & Policy,* Vol. 45, No. 3, 2017, pp. 432–464.

38 Susan Landau, "Making sense from Snowden: What's significant in the NSA surveillance revelations", *IEEE Security & Privacy,* Vol. 11, No. 4, 2013, pp. 66–75.

39 Kim Zetter, "Meet 'Flame,' The Massive Spy Malware Infiltrating Iranian Computers", W*ired*, May 28, 2012, Available from: https://www.wired.com/2012/05/flame/ (Accessed September 4, 2023).

40 Richard J. Harknett & Max Smeets, "Cyber campaigns and strategic outcomes", *Journal of Strategic Studies*, Vol. 45, No. 4, 2022, pp. 534–567.

(Verovatno) Kinezi su hakovanjem rutera američkog Ministarstva odbrane uspeli da skinu 20 terabajta podataka. Potom (opet verovatno), Kina je hakovanjem Lokhid Martina (Lockheed Martin) uspela da učini zavidan skok u korišćenju stelt tehnologije i kopiranje najmodernijih borbenih aviona, poput F-35. Velika kineska špijunaža jeste i hakovanje američke federalne kancelarije koja prikuplja podatke miliona zaposlenih (Office of Personnel Management) 2014. godine. Podaci 22.000.000 ljudi mogli su biti korišćeni u razne svrhe. Između ostalog i za širenje špijunske mreže putem uspostavljanja sistema ucena, ukoliko su se uočili obrasci neprikladnog ponašanja ili finansijskih neprilika. Sve te informacije bile su deo formulara broj 86, koji je „savršen za ucene", budući da je skrojen na način da se u njemu uvek nađu potencijalno kompromitujuća saznanja.[41]

Uopšteno, kineska strategija je da, uz korišćenje tehnike smrti pomoću hiljada rezova u vidu konstantne industrijske špijunaže, sustiže nekada ekonomski dominantne države.[42] Ovakva praksa je dovela do toga da se 2019. godine dogodi nešto što je ranije bilo nezamislivo, i podrazumeva uvođenje sankcija od strane SAD Huaveju (Huawei) i ZTE-u, najvećim kineskim tehnološkim kompanijama, a sve zbog sumnje na krađu intelektualnog vlasništva. Naravno, ne bi trebalo smetnuti s uma da je to i jedan od načina SAD da održe stratešku prednost u tehnološkoj trci u odnosu na Kinu, a da krađa intelektualnog vlasništva može biti i izgovor. Sankcije su dovele do usporavanja kineskog tehnološkog snaženja pre svega zato što pomenute firme još uvek zavise kako od američkih softvera tako i od lanca snabdevanja najmoćnijih čipova, koji je pod suverenom kontrolom SAD.[43]

Sabotaže, subverzije i špijunaže nisu kršenje nekakvih normi sajber prostora. Takve pravne norme na međunarodnom nivou, uz sve dosadašnje pokušaje, maltene ni ne postoje. Zapravo, moglo bi se reći da ukoliko se neka država ne služi ovim vrstama obaveštajne delatnosti ona krši ustaljena pravila i ne ponaša se u skladu sa sopstvenim interesima. Te tri vrste delatnosti, makar do sada, i jesu uspostavljanje normi ponašanja. Ukoliko žele da održe korak u trci za tehnološki primat, pokazuje se, države moraju da učestvuju u „sivoj zoni", iliti u sukobima ispod nivoa rata i pokažu zube u obaveštajnom nadmetanju.

---

41 Za hakovanje Lokid Martina i federalne kancelarije videti: *Ibid*.

42 John R. Lindsay, Tai Ming Cheung, and Derek S. Reveron, *China and cybersecurity: Espionage, strategy, and politics in the digital domain*, Oxford University Press, pp. 2–3.

43 Chris Miller, *Chip War: The Fight For The World's Most Critical Technology*, Simon and Schuster, 2022.

DOPREMANJE ORUŽJA U SAJBER PROSTORU

Ukazano je da države vrše subverzije, sabotiraju i špijuniraju svoje protivnike, ali još uvek nije izloženo kako one to izvode u sajber prostoru, to jest kojim oružjem se služe u te svrhe. Kako bismo pronašli odgovor na tu nejasnoću postavlja se pitanje – kako države dopremaju oružje do svog cilja? U konvencionalnim sukobima i kinetičkom ratovanju stvari su dosta jasnije. Recimo, za uništenje protivnika ispaljuju se krstareće ili rakete sa balističkom putanjom s mora, kopna i iz vazduha, koriste se dronovi samoubice potpomognuti delovanjem veštačke inteligencije itd. U domenima kopna, mora, vazduha i svemira zakoni fizike su aksiomi od kog dalje polazi nauka kako bi smislila najefektniji način dopremanja oružja do cilja. Međutim, u sajber domenu aksiomi tog prostora mogu biti znatno volatilniji. Pravila ponašanja, moguće i nemoguće, izuzev u delu fizičke infrastrukture informacione sfere,[44] mogu se menjati izuzetnom brzinom i demokratični su. To je posledica činjenice da su ograničenja sajbera uglavnom proizvod čoveka, ne fizičkih sila prirode. Samim tim, postoji veliki, pa možda i beskonačan prostor za međusobno nadmudrivanje različitih programera, hakera i stručnjaka za informacionu bezbednost, ali zbog masovnosti upotrebe znatno se povećava i prostor manipulacije ljudima i oslanjanja na ljudsku grešku.

Stoga, dopremanje oružja zavisi od stepena ranjivosti protivnika koji u sajber prostoru zavisi od ljudskog ili tehničkog faktora. Opet, tehnički faktor možemo podeliti na hardverski ili softverski. Neretko, napadi mogu podrazumevati kombinaciju sve tri opcije. U svakom slučaju, bilo da se traže ljudske greške, softverske ili hardverske ranjivosti, napadači teže da ugroze nešto što se u literaturi sajber bezbednosti naziva CIA trijada. Poverljivost (confidentiality – C), integritet (integrity – I) i dostupnost (availability – A) predstavljaju tri osnovna elementa bezbednosne kontrole,[45] i ugroženost bilo koga od njih istovremeno znači i ugroženost celokupnog sistema.

Poverljivost se u velikoj meri poklapa sa pokušajima špijunaže. U svrhu zaštite sistema neophodno je sprečiti neovlašćen pristup informacijama na kompjuterima ili serverima neke organizacije, što se u velikoj većini slučajeva

---

44 Ovde pre svega mislim na to da sajber domen jeste i fizički domen, u delu gde zavisi od fizičke infrastrukture optičkih kablova, rutera, skretnika, servera itd. Te stvari se, pored softverske manipulacije, mogu i fizički uništiti, što opet može dovesti do značajnih posledica po mogućnost delovanja u onom delu sajber prostora koji možemo nazvati i „dom uma".

45 Spyridon Samonas, and David Coss, "The CIA strikes back: Redefining confidentiality, integrity and availability in security", *Journal of Information System Security*, Vol. 10, No. 3, 2014, pp. 21–45, pp. 21–22.

svodi na praćenje „neovlašćenog sadržaja" ili potrage za neovlašćenim korišćenjem određenog softvera. Integritet se poklapa sa sabotažom i subverzijom, budući da je neophodno odbraniti sistem od neovlašćenih promena na informacijama pohranjenim u sistemu. Konačno, napadač može pokušati da nam blokira pristup sistemu, te tako ugrozi dostupnost informacija, što ponovo jeste neka vrsta sabotaže. Danas se trijadi neretko dodaje i četvrti fenomen, a reč je o autentičnosti, te umesto CIA možda možemo govoriti o CIAA kvartetu. Autentičnost, šturo rečeno, predstavlja pitanje poverenja u informacije koje nam se plasiraju i uglavnom se tiče mogućnosti manipulacije informacijama putem društvenih mreža. Mada, nejasna je razlika između ugrožavanja integriteta i autentičnosti, pošto i jedno i drugo podrazumevaju alteraciju informacija, što dovodi do toga da CIA trijada ponovo pokriva sve eventualne slučajeve sajber napada.[46]

LJUDSKA GREŠKA

Kao što je ranije napomenuto, ugrožavanje poverljivosti, integriteta ili dostupnosti može biti proizvod ljudske ili tehničke ranjivosti. Ljudska ranjivost je gotovo nezaobilazna u svim sajber napadima. Do te mere da su istraživači zaključili kako je 95 procenata uspešnih napada proizvod iskorišćavanja ljudske greške.[47] Pomenuli smo primer Staksneta, gde je ranjivost došla od najviših zvaničnika države kada je propagandni video pružio previše informacija, dovoljnih za narušavanje integriteta Natanz sistema. Takođe, Solar Vinds hakovanje je, pored izuzetnog tehničkog nivoa napadača, uključivalo i neoprezno rukovođenje tokom izgradnje nove verzije Orion softvera. Hakovanje Nacionalne banke Bangladeša i izvlačenje preko 80.000.000 dolara 2016. godine proizvod je greške jednog od zaposlenih nakon klika na link u zloćudnom mejlu.[48] Virus *WannaCry* je 2017. godine onemogućio dostupnost informacija unutar britanske Nacionalne zdravstvene službe (National Health Service) i tako odgodio desetine hiljada pregleda, pa i onih najurgentnijih. To se nije dogodilo zbog izuzetnih tehničkih sposobnosti napadača, već zato što Majkrosoftov softver nije bio ažuriran na vreme na svim računarima, bez obzira što je do tada već naširoko postalo poznato kako hakeri zloupotrebljavaju

---

46 Za definicije i raspravu o evoluciji trijade videti: *Ibid*, p. 24, 30.

47 George Platsis, "The human factor: Cyber security's greatest challenge" in: *Cyber Law, Privacy, and Security: Concepts, Methodologies, Tools, and Applications*, IGI Global, 2019, pp. 1–19.

48 Geoff White,. "The Lazarus heist: How North Korea almost pulled off a billion-dollar hack", *BBC News*, June 21, 2021. Available from: https://www.bbc.com/news/stories-57520169 (Accessed September 4, 2023).

ranjivosti ranijih verzija softvera. Da je bio potpuno uspešan, *WannaCry* napad bi podrazumevao vraćanje pristupa informacijama ali tek nakon plaćanja otkupa (*ransomware*). Srećom, malver je zaobiđen na drugi način.[49]

Naravno, informacije mogu biti i u potpunosti obrisane (*data wiping/bricking*). Iskorišćavanjem ljudske znatiželje i neopreznosti, iliti društvenim inženjeringom, napadači koriste i metode fišinga (phishing), kada odašilju maliciozne mejlove u etar očekujući da se makar neko u masi upeca, ili ciljanog i targetiranog fišinga (spear phishing), kada žele da izmanipulišu vrlo konkretnu osobu. Pored ove dve vrste ljudskih grešaka, ljudi su skloni ostavljanju privatnih informacija svuda po internetu, čime neretko i sami „pozovu" hakere na zloupotrebu.

SOFTVERSKE I HARDVERSKE RANJIVOSTI

Softverski napadi se uglavnom vezuju za tri vrste eksploatacija (*exploits*) ranjivosti: eksploataciju nultog dana (*zero-days exploit*); eksploataciju nezakrpljenosti N-tog dana (*unpatched N-day exploits*), kao i eksploataciju zakrpljenosti N-tog dana (*patched N-day exploits*).[50] U prevodu, kada ofanziva uključuje eksploataciju nultog dana (inače vrlo skupu na crnom tržištu) to znači da onaj koji je napadnut ne zna da njegov softver ima neku ranjivost, ili je to saznao tek nakon napada. U tom slučaju žrtva nema vremena da reaguje i ne može da se odbrani, tj. ima nula dana da se brani. U Staksnet napadu, SAD i Izrael su imali četiri eksploatacije nultog dana, za šta je bio neophodan ili veliki novac ili izuzetan stepen stručnog znanja većeg broja ljudi.[51] U druga dva slučaja žrtva je svesna da postoji ranjivost softvera i ima određeni (N) broj dana da reaguje pre nego što ranjivost bude eksploatisana. U slučaju nezakrpljenosti još uvek nije rešen problem ranjivosti, iako postoji svest o njoj. Kod zakrpljenosti N-tog dana kontrolor sistema jednostavno nije instalirao postojeći protivotrov, ali takođe ima određen broj dana da to učini, te ne može biti iznenađen ukoliko i dođe do ugrožavanja njegovog sistema. Upravo to se dogodilo sa *WannaCry* malverom. Pored ove tri vrste eksploatacija, ovde bi valjalo

---

49 Saira Ghafur, Soren Kristensen, Kate Honeyford, Guy Martin, Ara Darzi, and Paul Aylin, "A retrospective impact analysis of the WannaCry cyberattack on the NHS", *NPJ digital medicine,* Vol. 2, No. 1, 2019, p. 98.

50 Max Smeets, "The Risks of Managing a Purchased Cyber Arsenal". Blog Post by Max Smeets, Guest Contributor, *Council on Foreign Relations*, May 31, 2022. Available from: https://www.cfr.org/blog/risks-managing-purchased-cyber-arsenal (Accessed September 4, 2023).

51 James Farwell, and Rafal Rohozinski, "Stuxnet and the Future of Cyber War", *Survival*, Vol. 53, No. 1, 2011, pp. 23–40, p. 24.

napomenuti i DDoS (*Distributed Denial of Service*) napade, koji su česti i podrazumevaju ofanzivu putem opterećenja mreže do tačke da je ona neupotrebljiva za protok informacija. Jedan od poznatijih DDoS napada dogodio se 2007. godine, kada je Rusija opteretila saobraćaj estonskog interneta u znak odmazde, pošto je Estonija ranije odlučila da ukloni statuu sovjetskog vojnika iz centra Talina. Pri DDoS ofanzivama napadači često zloupotrebe tuđe računare i služe se njima kako bi preusmerili saobraćaj. Tako, bez obzira što je napad pripisivan Rusiji (pre svega zbog jasnog motiva), računari koji su napali Estoniju imaju poreklo svuda po Evropi i SAD. [52]

Konačno, pored društvenog inženjeringa, tj. oslanjanja na ljudsku grešku, potom softverskih ranjivosti, postoje i ranjivosti hardvera. Uzmimo za primer lanac snabdevanja čipovima. Samo jedna mašina koja služi za ultraljubičastu (EUV) litografiju slaže se od 457.329 delova sakupljenih iz svih delova sveta.[53] To bi značilo da postoji visok stepen rizika narušavanja integriteta konačnog proizvoda u kom učestvuje i EUV mašina. Rizik po integritet hardvera je jedan od razloga zašto su SAD donele Zakon o čipovima i nauci, kojim pokušavaju da smanje zavisnost od globalnih lanaca snabdevanja pri proizvodnji ključne tehnologije poput čipova.[54] Takođe, zbog straha od toga da se jednom instalirana oprema teško skida i da joj je lako narušiti integritet, SAD vode žestoku kampanju u celom svetu protiv instaliranja 5G Huavej i ZTE opreme.[55] Daleko od toga da se radi samo u običnom strahu od špijunaže, sabotaže ili subverzije, već sigurno možemo govoriti i o široj borbi za relativnu tehnološku dominaciju i održanje geopolitičke prednosti od koje direktno zavise i politička i ekonomska moć u međunarodnim odnosima.[56]

---

52 Joshua Davis, "Hackers take down the most wired country in Europe", *Wired magazine*, August 21, 2007. Available from: https://www.wired.com/2007/08/ff-estonia/ (Accessed September 4, 2023).

53 Radi se o tehnologiji koja omogućava proizvodnju čipova sa tranzistorima od 3 nanometra (milijardita dela metra). Trenutno kompanija ASML, stacionirana u Holandiji, ima monopol nad EUV tehnologijom i bez njene mašine je nemoguće proizvesti najnaprednije čipove velike računarske moći. Chris Miller, *Chip War: The Fight For The World's Most Critical Technology*, Simon and Schuster, 2022, p. 322.

54 "H.R.4346 – Chips and Science Act, 2022", *117th Congress (2021-2022)*, *U.S. Congress*, 2022. Available from: https://www.congress.gov/bill/117th-congress/house-bill/4346 (Accessed September 4, 2023).

55 Kadri Kaska, Henrik Beckvard, and Tomáš Minárik, "Huawei, 5G and China as a security threat", *NATO Cooperative Cyber Defence Center for Excellence (CCDCOE)*, Vol. 28, 2019, pp. 1–26, p. 4.

56 Min Tang, "Huawei versus the United States? The geopolitics of exterritorial internet infrastructure", *International Journal of Communication*, Vol. 14, 2020, pp. 4556–4577.

SAD nisu paranoične bez razloga, već zato što su, istorijski gledano, i same učestvovale u eksploataciji zavisnosti neke države od strane tehnologije. Recimo, do sada najveći napad, u smislu „razbijanja stvari", dogodio se 1982. godine u Sovjetskom Savezu. Naime, Sovjetima je bila neophodna nabavka SCADA softvera[57] radi kontrolisanja gasovoda koji bi spajao Sibir i evropska tržišta. CIA je, prema svedočenjima tadašnjih bezbednosnih zvaničnika SAD, sabotirala SCADA softver koji su Sovjeti kupili od Kanade tako da je neko vreme delovalo da sve funkcioniše savršeno. Međutim, slično kao i u slučaju Natanza, malver (trojanac) je čučao u sistemu i u jednom trenutku podesio pritisak u pumpama i ventilima sa ishodom „monumentalne" eksplozije koja je „mogla da se vidi iz svemira".[58] Ova sabotaža je iskorišćavanje softverske ranjivosti, ali nema razloga da verujemo da bi sabotaža mogla biti i hardverske prirode da se za tako nešto pružila mogućnost ili da se radilo o jednostavnijem načinu eksploatacije.

Kao što vidimo na brojnim primerima, bezbednost sajber prostora uglavnom zavisi od kombinacije društvenog (ljudskog) i tehničkog (softverskog i hardverskog) faktora. To je razlog zašto se u literaturi sve više naglašava potreba za društveno (socio)-tehničkim rešenjima sajber bezbednosti. Tako imamo predloge holističkog pristupa koji za predmet imaju javne politike, i strategije sajber bezbednosti koje moraju biti u srži odbrane država, javnog i privatnog sektora. Takav pristup zahteva jasno definisane organizacione strukture, procedure, politike, regulacije, gajenje talenata, podizanje svesti, itd. [59] Sličnu poruku šalje nova NIS2 direktiva Evropske unije iz 2022. godine kada naglašava neophodnost uspostavljanja nacionalnih tela za upravljanje sajber prostorom, koja bi se, pored tehničkih aspekata, bavila i upravljanjem, kroz strategije, politike i efikasan organizacioni pristup ljudima i gajenju talenata. Takođe, uvodi obaveze i za srednja i velika preduzeća u smislu učestvovanja u koordinaciji sajber odbrane i praćenja pravila i procedura ponašanja i odgovornosti prema nacionalnom telu.[60] Na istom tragu je i nacrt novog „NIST okvira za sajber bezbednost 2.0" američkog Nacionalnog instituta za standarde i

---

57 Radi se o softveru pomoću kog se nadziru i kontrolišu veliki industrijski sistemi.

58 Thomas Rid, "Cyber War Will Not Take Place", *Journal of Strategic Studies*, Vol. 35, No. 1, 2012, pp. 5–32, p. 10.

59 Verena Zimmermann, and Karen Renaud, "Moving from a 'human-as-problem' to a 'human-as-solution' cybersecurity mindset", *International Journal of Human-Computer Studies*, Vol. 131, 2019, pp. 169–187.

60 "Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148, COM (2020) 823 final", *European Commission*. Available from: https://eur-lex.europa.eu/resource.html?uri=cellar:be0b5038-3fa8-11eb-b27b-01aa75ed71a1.0001.02/DOC_1&format=PDF (Accessed September 4, 2023).

tehnologiju (National Institute of Standards and Technology). Ključnim principima sajber odbrane (identifikuj, zaštiti, uoči, odgovori, oporavi se), koje preporučuje „organizacijama svih veličina i sektora", Institut dodaje i upravljanje (govern).[61] Upravljanje može biti izuzetno širok koncept, ali njegovim dodavanjem se naglašava složenost sajber odbrane i neophodnost posvećivanja pažnje ljudskom faktoru, na nivou pojedinaca i organizacije, u jednakoj meri kao i onom tehničkom.

ZAKLJUČAK

Rad predstavlja pregled literature koja se bavi specifičnostima sukoba u sajber domenu. Opšti zaključak je da do sada nismo prisustvovali sajber ratu, već isključivo sivoj zoni u vidu „sukoba ispod praga rata". Međutim, radi razumevanja kvaliteta i karaktera sukoba u sajber prostoru nije dovoljno da konstatujemo da nekakav prag do sada nije pređen, već i da preciziramo o kakvim konkretnim ofanzivnim aktivnostima i ponašanjima država se radi. Imali smo prilike da vidimo dominantan zaključak literature prema kom svedočimo obaveštajnom nadmetanju povećanog obima. Takva vrsta nadmetanja jeste nadogradnja ranijih obaveštajnih aktivnosti, tj. vrlo obimna nadogradnja u vidu različitih vrsta sajber sabotaža, subverzija i špijuniranja svojih takmaca, a neretko i saveznika.

Opisani su i vrlo specifični mehanizmi dopremanja oružja do svog cilja, koji, ugrubo rečeno, mogu zavisiti od ljudskih i tehničkih (softverskih i hardverskih) ranjivosti. Na konkretnim primerima sajber napada smo mogli da vidimo i kakve sve vrste sajber oružja su korišćene u ofanzivama država, ali i gde se u budućnosti nalazi veliki potencijal nanošenja štete suparnicima. Uopšteno, zaključak je da akademska literatura, predlozi praktičnih politika i konkretni savetodavni i zakonodavni akti usmeravaju svoje savete i naloge prema holističkom pristupu upravljanja sajber prostoru na način da odgovore na društveno-tehničke kompleksnosti izazova sajber odbrane.

---

61 "Public Draft: The NIST Cubersecurity Framework 2.0", *National Institute of Standards and Technology*, 2023. Available from: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.ipd.pdf (Accessed September 4, 2023).

BIBLIOGRAFIJA

[1] Amer, Karim and Jehane Noujaim, *The Great Hack*, Netflix, 2019

[2] Berger, Joseph, "A dam, small and unsung, is caught up in an Iranian hacking case", *The New York Times*, March 26, 2016. Available from: https://www.nytimes.com/2016/03/26/nyregion/rye-brook-dam-caught-in-computer-hacking-case.html (Accessed September 4, 2023)

[3] Burges, Matt, "A Mysterious Satellite Hack Has Victims Far Beyond Ukraine", *Wired*, March 23, 2022. Available from: wired.com/story/viasat-internet-hack-ukraine-russia (Accessed September 4, 2023).

[4] Cattler, David and Daniel Black. *The Myth of the Missing Cyberwar*. Foreign Affairs, April 6, 2022. Available from: https://www.foreignaffairs.com/articles/ukraine/2022-04-06/myth-missing-cyberwar (Accessed September 4, 2023).

[5] Davis, Joshua, "Hackers take down the most wired country in Europe", *Wired magazine*, August 21, 2007. Available from: https://www.wired.com/2007/08/ff-estonia/ (Accessed September 4, 2023).

[6] Eady, Gregory, Tom Paskhalis, Jan Zilinsky, Richard Bonneau, Jonathan Nagler, and Joshua A. Tucker, "Exposure to the Russian Internet Research Agency foreign influence campaign on Twitter in the 2016 US election and its relationship to attitudes and voting behavior", *Nature Communications*, Vol. 14, No. 1, 2023.

[7] Farwell, James, and Rafal Rohozinski, "Stuxnet and the Future of Cyber War", *Survival*, Vol. 53, No. 1, 2011, pp. 23–40.

[8] Fischerkeller, Michael P., Emily O. Goldman, and Richard J. Harknett, *Cyber persistence theory: Redefining national security in cyberspace*, Oxford University Press, 2022.

[9] Fischerkeller, Michael P., and Richard J. Harknett, "Deterrence is not a credible strategy for cyberspace", *Orbis*, Vol. 61, No. 3, 2017, pp. 381–393.

[10] Gerasimov, Valery, "The Value of Science in the Foresight", *Military Review*, January/February 2016. Available from: https://www.armyupress.army.mil/portals/7/military-review/archives/english/militaryreview_20160228_art008.pdf (Accessed September 4, 2023).

[11] Ghafur, Saira, Soren Kristensen, Kate Honeyford, Guy Martin, Ara Darzi, and Paul Aylin, "A retrospective impact analysis of the WannaCry cyberattack on the NHS", *NPJ digital medicine*, Vol. 2, No. 1, 2019.

[12] Gibney, Alex, *Zero days*, Showtime, USA, 2016.

[13] Goodman, Will, "Cyber deterrence: Tougher in theory than in practice?" *Strategic Studies Quarterly*, Vol. 4, No. 3, 2010, pp. 102–135.

[14] Harknett, Richard J. & Max Smeets, "Cyber campaigns and strategic outcomes", *Journal of Strategic Studies*, Vol. 45, No. 4, 2022, pp. 534–567.

[15] Jensen, Benjamin, Brandon Valeriano, and Ryan Maness, "Fancy bears and digital trolls: Cyber strategy with a Russian twist", *Journal of Strategic Studies*, Vol. 42, No. 2, 2019, pp. 212–234.

[16] Jervis, Robert, *The meaning of the nuclear revolution: Statecraft and the prospect of Armageddon*, Cornell University Press, 1989.

[17] Jordan, Javier, "International Competition Below the Threshold of War: Toward a Theory of Gray Zone Conflict", *Journal of Strategic Security*, Vol. 14, No. 1, 2020, pp. 1–24.

[18] Kaska, Kadri, Henrik Beckvard, and Tomáš Minárik, "Huawei, 5G and China as a security threat", *NATO Cooperative Cyber Defence Center for Excellence (CCDCOE)* Vol. 28, 2019, pp. 1–26.

[19] Landau, Susan, "Making sense from Snowden: What's significant in the NSA surveillance revelations", *IEEE Security & Privacy,* Vol. 11, No. 4, 2013, pp. 66–75.

[20] Lindsay, John R, Tai Ming Cheung, and Derek S. Reveron, *China and cybersecurity: Espionage, strategy, and politics in the digital domain*, Oxford University Press.

[21] Lindsay, John, "Hidden Dangers in the US Military Solution to a Large-Scale Intelligence Problem" in (eds.) Robert Chesney and Max Smeets, *Deter, Disrupt, Or Deceive: Assessing Cyber Conflict as an Intelligence Contest*. Georgetown University Press, 2023.

[22] Lindsay, John, "Stuxnet and the Limits of Cyber Warfare", *Security Studies,* Vol. 22, No. 3, 2013, pp. 365–404.

[23] Maness, Ryan C, "Death by a Thousand Cuts: Is Russia Winning the Information War with the West?" in (eds.) Mai'a K. Davis Cross and Ireneusz Paweł Karolewski, *European-Russian Power Relations in Turbulent Times*, The University of Michigan Press, Ann Arbout, Mi, 2021, pp. 160–186.

[24] McGuffin, Chris, and Paul Mitchell, "On Domains: Cyber and the Practice of Warfare", *International Journal*, Vol. 69, No. 3, 2014, pp. 394–412.

[25] Miller, Chris *Chip War: The Fight For The World's Most Critical Technology*, Simon and Schuster, 2022.

[26] Mueller, Robert, "Report On The Investigation Into Russian Interference In The 2016 Presidential Election", *Department of Justice Washington*, D.C. March 2019.

[27] Panetta, Leon, "Defense secretary warns of 'cyber Pearl Harbor'", *CBS News YouTube Channel*, October 13, 2012. Available from: https://www.youtube.com/watch?v=C2Qp59aQyu4 (Accessed September 4, 2023).

[28] Platsis, George, "The human factor: Cyber security's greatest challenge" in: *Cyber Law, Privacy, and Security: Concepts, Methodologies, Tools, and Applications*, IGI Global, 2019, pp. 1–19.

[29] "Public Draft: The NIST Cubersecurity Framework 2.0", *National Institute of Standards and Technology,* 2023. Available from: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.ipd.pdf (Accessed September 4, 2023).

[30] Rid, Thomas, "Cyber War Will Not Take Place", *Journal of Strategic Studies*, Vol. 35, No. 1, 2012, pp. 5–32.

[31] Rid, Thomas, and Ben Buchanan, "Attributing cyber attacks", *Journal of Strategic Studies*, Vol. 38, No. 1–2, 2015, pp. 4–37.

[32] Rivera, Jason, "Understanding and Countering Nation-State Use of Protracted Unconventional Warfare", *Small Wars Journal*. Available from: https://smallwarsjournal.com/jrnl/art/understanding-and-countering-nation-state-use-of-protracted-unconventional-warfare (Accessed September 4, 2023).

[33] Rovner, Joshua, "What is an Intelligence Contest?", *Texas National Security Review*, Fall 2020, pp. 114–120.

[34] Samonas, Spyridon and David Coss, "The CIA strikes back: Redefining confidentiality, integrity and availability in security", *Journal of Information System Security*, Vol. 10, No. 3, 2014, pp. 21-45.

[35] Singer, P. W. and Emerson T. Brooking, "What Clausewitz Can Teach Us About War on Social Media", *Foreign Affairs*, October 4, 2018. Available from: https://www.foreignaffairs.com/world/what-clausewitz-can-teach-us-about-war-social-media (Accessed September 4, 2023).

[36] Smeets, Max, "The Risks of Managing a Purchased Cyber Arsenal", Blog Post by Max Smeets, Guest Contributor, *Council on Foreign Relations*, May 31, 2022. Available from: https://www.cfr.org/blog/risks-managing-purchased-cyber-arsenal (Accessed September 4, 2023).

[37] Smeets, Max, *No shortcuts: Why states struggle to develop a military cyber-force*, Oxford University Press, Oxford, 2023.

[38] Tang, Min, "Huawei versus the United States? The geopolitics of exterritorial internet infrastructure", *International Journal of Communication*, Vol. 14, 2020, pp. 4556–4577.

[39] Thompson, Mark, "Iranian cyber attack on New York dam shows future of war", *Time*, March 24, 2016. Available from: https://time.com/4270728/iran-cyber-attack-dam-fbi/ (Accessed September 4, 2023).

[40] Von Clausewitz, Carl, (Peter Paret, Michael Eliot Howard, and Carl von Clausewitz), *On War*, Princeton University Press, 2008.

[41] Vukelić, Miloš R., *Kulturni ratovi u Sjedinjenim Američkim Državama i Evropskoj uniji u periodu od 2014. do 2020. godine*, Doktorska disertacija, Univerzitet u Beogradu – Fakultet političkih nauka, 2023.

[42] Wardle, Claire, and Hossein Derakhshan, "Information disorder: Toward an interdisciplinary framework for research and policymaking", *Council of Europe Report*, 2017.

[43] Warner, Michael, "The Character of Strategic Cyberspace Competition and the Role of Ideology" in (eds.) Robert Chesney and Max Smeets, *Deter, Disrupt, Or Deceive: Assessing Cyber Conflict as an Intelligence Contest*. Georgetown University Press, 2023.

[44] White, Geoff, "The Lazarus heist: How North Korea almost pulled off a billion-dollar hack", *BBC News*, June 21, 2021. Available from: https://www.bbc.com/news/stories-57520169 (Accessed September 4, 2023).

[45] Wilner, Alex, "US cyber deterrence: Practice guiding theory", *Journal of Strategic Studies,* Vol. 43, No. 2, 2020, pp. 245–280.

[46] Zeng, Jinghan, Tim Stevens, and Yaru Chen, "China's Solution to Global Cyber Governance: Unpacking the Domestic Discourse of 'Internet Sovereignty'", *Politics & Policy*, Vol. 45, No. 3, 2017, pp. 432–464.

[47] Zetter, Kim, "Meet 'Flame,' The Massive Spy Malware Infiltrating Iranian Computers", *Wired*, May 28, 2012. Available from: https://www.wired.com/2012/05/flame/ (Accessed September 4, 2023).

[48] Zetter, Kim, "The Untold Story of the Boldest Supply-Chain Hack Ever", *Wired*, May 2, 2023. Available from: https://www.wired.com/story/the-untold-story-of-solarwinds-the-boldest-supply-chain-hack-ever/ (Accessed September 4, 2023).

[49] Zimmermann, Verena, and Karen Renaud, "Moving from a 'human-as-problem' to a 'human-as-solution' cybersecurity mindset", *International Journal of Human-Computer Studies*, Vol. 131, 2019, pp. 169–187.

[50] "Department of Defense Cyber Strategy", *United States Department of Defense*, Washington DC, 2018.

[51] "Hearing Before the Senate Select Committee on Intelligence. Social Media Influence in the 2016 U.S. Election", *115th Cong. 13 (11/1/17) (testimony of Colin Stretch, General Counsel of Facebook)*, 2017.

[52] "Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148, COM (2020) 823 final", *European Commission*. Available from: https://eur-lex.europa.eu/resource.html?uri=cellar:be0b5038-3fa8-11eb-b27b-01aa75ed71a1.0001.02/DOC_1&format=PDF (Accessed September 4, 2023).

[53] "Update on Twitter's review of the 2016 US election", *Twitter blog,* 2018. Available from: https://blog.twitter.com/en_us/topics/company/2018/2016-election-update (Accessed September 4, 2023).

[54] "H.R.4346 – Chips and Science Act, 2022", *117th Congress (2021-2022), U.S. Congress*, 2022. Available from: https://www.congress.gov/bill/117th-congress/house-bill/4346 (Accessed September 4, 2023).

Miloš Vukelić

CYBER CONFLICT BELOW THE "THRESHOLD OF WAR": CYBER WEAPONS IN INTELLIGENCE CONTEST

Abstract

This paper provides an overview of key findings in the international relations literature concerning conflicts between states in cyberspace. The main conclusions drawn from this literature suggest that, thus far, the "threshold of war" has not been crossed in cyber conflicts. Instead, what we are witnessing is a "gray zone," characterized by state intelligence contest in cyberspace, manifesting through a multitude of acts of sabotage, subversion, and espionage. Furthermore, the paper presents specific examples of vulnerabilities exploited by actors in the cyber domain and the weaponry employed for such purposes. States have frequently resorted to such forms of weaponry in the previous decades. The aim of this paper is to contextualize how states operate in cyberspace within the broader environment of international relations.

Keywords:

cyber conflict, cyberspace, cyber security, intelligence contest, international relations.