UDK 327:004(73)
Biblid: 0025-8555, 76(2024)
Vol. LXXVI, br. 1, str. 55–86
DOI: https://doi.org/10.2298/MEDJP2401055V

Pregledni rad
Primljen 29. aprila 2023.
Odobren 25. oktobra 2023.

Karakteristike sajber prostora kao zasebnog domena sukoba na primeru strateškog delovanja SAD

Miloš VUKELIĆ[1]

Apstrakt: U radu se polazi od namere da se pruži doprinos sistematskom izučavanju sajber strategija i politika kroz sintezu ključnih događaja i nalaza o delovanju država u sajber prostoru nakon 2007. godine. Ovakva sinteza podrazumeva praćenje procesa koji su doprineli početku militarizacije sajber prostora u periodu od 2007. do 2013. godine. Potom, pri definisanju osnovnih karakteristika sajber prostora koje determinišu delovanje država, izdvajaju se demokratičnost, veliki potencijal ljudske greške, problem atribucije, tehničku volatilnost, i vremensku ograničenost i brzinu reagovanja. Konačno, sinteza podrazumeva i konkretan primer uticaja ključnih karakteristika na strateško delovanje SAD kao velike sile u tom domenu. Na osnovu analize strateških dokumenata SAD, ali i uvida u ranije ponašanje ove države, u radu se tvrdi da teorija „upornog angažmana", koja u izgradnji teorije uzima u obzir prethodno navedene karakteristike, ostaje okosnica delovanja SAD u sajber prostoru.

Ključne reči: sajber prostor, sajber strategija, sajber politika, sajber sukobi, SAD.

Od sajber utopije do sajber realizma[2]

Dugo je u tehnološkim, ali i političkim, ekonomskim, kulturnim i drugim elitnim krugovima vladalo oduševljenje zbog potencijala koji sa sobom nosi pojava interneta. Nastao 1969. godine kao projekat američke Agencije za

[1] Univerzitet u Beogradu – Fakultet političkih nauka, milos.vukelic@fpn.bg.ac.rs, https://orcid.org/0000-0002-0014-4122

[2] Autor se zahvaljuje profesoru Gregoriju Vingeru (Gregory Winger) sa Univerziteta u Sinsinatiju (University of Cincinnati), bez čijih predavanja ovaj rad ne bi bio moguć.

napredne istraživačke projekte (ARPA – Advanced Research Projects Agency)[3], internet je početkom 90-ih godina 20. veka doživeo ekspanziju kada je postao i masovni, ne samo elitni istraživački fenomen (Singer, Friedman 2014, 17-21).[4] Istovremeno se dogodila i ekspanzija utopijskih zamisli o tome šta sve može da nam donese umreženo društvo, pa se dugo verovalo u „sajber libertarijansku" viziju interneta koji će konačno uspeti da zaobiđe moć država. Prihvatana je poruka Džona Perija Barloua (John Perry Barlow) „vladama industrijalizovanog sveta" da su one „umorni divovi od mesa i čelika". Takođe, i poruka kako dolazi novo doba, doba sajber prostora, iliti „novog doma uma". Taj „novi dom uma", nastavlja Barlou, vodi ka prostoru koji je slobodan i „prirodno nezavisan od tiranija" (Barlow 1996). Ubrzo nakon toga i Bil Klinton (Bill Clinton), nekadašnji predsednik SAD, poručuje Kini da to što ta država pokušava da kontroliše internet, predstavlja nešto slično pokušajima da „žele ostane zalepljen za zid" – nemoguće (Clinton 2000). Dakle, i vlade su mislile da se radi o nezadrživom fenomenu, a u konkretnom slučaju, to je bilo i u interesu SAD.

„Tehno-optimizam" ili „tehno-euforija" (Fuchs 2012), koje se ogledaju u manifestu Džona Barloua, vide internet isključivo na jednodimenzionalan način. Odnosno, vide samo pozitivne uticaje interneta po društva. Takođe, sajber utopisti imaju tendenciju da razumevaju sajber prostor kao „prostor uma" – kao nešto potpuno nezavisno od okova fizičkog sveta.[5] Zanimljivo je i da sajber distopijske vizije, koje dolazak interneta posmatraju kao početak propasti, takođe govore o nekakvom prostoru uma. Vilijam Gibson (William Gibson), pisac

[3] Kasnije je dodavanjem slova D, koje označava odbranu (eng. defense), ova agencija dobila svoj krajnji i poznatiji akronim – DARPA.

[4] Omasovljenje korišćenja interneta je posledica dešavanja s kraja 80-ih godina, kada su američke vlasti dozvolile privatnim kompanijama da mogu da počnu sa uspostavljanjem infrastrukture koja će omogućiti korišćenje interneta i izvan istraživačkih centara (Singer, Friedman, 2014, 17-21).

[5] Iako u radu često koristim koncepte interneta i sajber prostora kao sinonime, radi se o dva srodna ali različita fenomena. U popularnoj kulturi je sajber prostor, kao znatno šira koncepcija, često poistovećivan sa internetom, pa ih je u naraciji teško odvojiti. Sajber prostor, dakle, nije samo prostor uma. On se sastoji od „stvari i ideja, strukture i sadržaja" (Deibert, Rohozhinski, 2010, 16), te podrazumeva „sve postojeće sisteme i mreže, uključujući i vazdušni prostor između sistema" (Kello, 2013, 17). Američki Nacionalni institut za standarde i tehnologiju (U.S. National Institute of Standards and Technology, 2012, B3) nalazi da je sajber prostor „globalni domen unutar informativnog okruženja koji se sastoji od nezavisnih mreža infrastrukture informacionih tehnologija, uključujući i internet, telekomunikacionih mreža, kompjuterskih sistema, i ugrađenih procesora i kontrolera". Kao što vidimo, postoji puno fizičkih i logičkih tačaka na koje je moguće uticati i koje je eventualno moguće kontrolisati.

distopijske naučne fantastike, koji je i skovao termin „sajber prostor“, govori o tome da je sajber mesto u kom ljudi pristaju na halucinacije (prema: Dunn Cavelty 2013, 107).

Ipak, niti je internet nužno emancipatorski, niti je sajber isključivo dom uma. Vremenom se sve više ukazivala vizija koja podrazumeva da je itekako moguća kontrola sajber prostora od strane država ili velikih tehnoloških korporacija. Takođe, da ta kontrola obuhvata kako manipulaciju uma, tako i uticaj na fizičku infrastrukturu od koje taj um nužno zavisi. Na kraju, da internet, kao značajan deo sajber prostora, uopšte ne mora voditi slobodi od tiranije, već može biti i oruđe u rukama tirana. Jevgenij Morozov (Евге́ний Моро́зов) zato govori o tome kako je sajber utopizam počeo da se poistovećuje sa naivnošću jer je gajio „uverenje u emancipatorsku prirodu onlajn komunikacija“ (Morozov 2011, xiii).

Veliki potencijal kontrole, mogućnost uvećanja tiranije i zavisnost od fizičke infrastrukture doprineli su stvaranju realističnijeg gledišta prema celokupnom sajber prostoru. Danas države sve više teže njegovoj kontroli. Rusija, Kina, Iran i Turska prednjače po odvajanju „svojih“ nacionalnih interneta od globalnog (Singer, Warren, Brookings 2018, 86-101). Istovremeno, i veliki broj drugih država pokušava da upravlja, manipuliše i koristi sajber prostor na strateški način, u čemu svakako prednjače SAD. Države formiraju „sajber trupe“ koje pokušavaju da iskoriste postojeće karakteristike sajber prostora zarad svojih ciljeva (Bradshaw, Howard 2018, 25). Zbog toga, postavlja se pitanje: koja su to strateška ograničenja ili strateški podsticaji koji utiču na ponašanje država u sajber prostoru?

Namera autora ovog rada jeste da taksativno predstavi karakteristike kojima se države vode pri strateškom delovanju u sajber prostoru. Na primeru SAD, pokazaću kako karakteristike oblikuju i konkretnu strategiju ove velike sile. Cilj rada jeste postavljanje osnova za sistemsko izučavanje sajber strategija i politika u Srbiji. Rad je podeljen na nekoliko celina. U prvom delu bavim se početkom vidljivije militarizacije i promene javnih paradigmi država prema sajber prostoru. Opisujem kako se i javno napušta utopistička iluzija da je sajber prostor samo dom uma, i to oslobođen od vlada industrijalizovanog sveta. Nakon utvrđivanja da je sajber prostor sve više polje kontrole država, u drugom delu predstavljam raspravu o tome da li zaista možemo da govorimo o sajberu kao petom i zasebnom domenu ratovanja. U trećem delu taksativno iznosim glavne odlike sajber prostora kao posebnog domena sukoba. U četvrtom iznosim teoriju „upornog angažmana“, koja je naglavačke izvrnula klasično razumevanje međusobnog obuzdavanja država i postavila osnov za novo strateško promišljanje koje direktno zavisi od prethodno opisanih glavnih odlika sajber prostora. Konačno, u petom delu iznosim evoluciju sajber strategije SAD, gde

naglašavam veliku podudarnost teorije „upornog angažmana" sa aktuelnim delovanjem i zalaganjem SAD.

Ubrzanje militarizacije sajber prostora

U periodu od 2007. do 2013. godine, bili smo svedoci nekoliko događaja koji su na suštinski način promenili odnos država prema sajber prostoru. Ukratko, radi se o: sajber napadima Rusije na Estoniju i Gruziju; sajber napadu SAD i Izraela na iransko nuklearno postrojenje; osnivanju komandi koje se izričito bave sajber prostorom; revoluciji preko društvenih mreža ili „Arapskom proleću; i o otkrivanju tajnog programa špijunaže saveznika ali i sopstvenih građana koji su sprovodile SAD i UK do 2013. godine.

Prvo, Estonija je krajem aprila 2007. godine iz centra Talina uklonila statuu bronzanog vojnika. Radilo se o simbolu sovjetske borbe protiv nacizma, a koji je u novoj estonskoj nacionalnoj interpretaciji viđen kao simbol sovjetske represije. Kao reakciju, pored protesta nezadovoljnih građana Talina, Rusija je lansirala sajber napad velikih razmera koji je trajao nekoliko nedelja i koji je potpuno blokirao izuzetno napredan i umrežen estonski javni sektor. Estonija je tada tražila da se aktivira Član 5. NATO, koji podrazumeva odmazdu Saveza u slučaju agresije na neku od zemalja članica. Iako do aktivacije ovog člana tada nije došlo, pre svega zbog nemogućnosti dogovora da li sajber napad predstavlja agresiju ili ne, Estonija će postati centar strateškog razmišljanja o delovanju NATO u sajber prostoru. Takođe, ruski napad će biti promovisan na Zapadu kao prvi veliki javni primer ofanzivnog korišćenja sajber prostora zarad ostvarenja nekog spoljnopolitičkog cilja (više o celom slučaju: Davis, 2007). Rusija je 2008. godine izvela sličan napad na Gruziju, preopterećenjem gruzijskih servera, nekoliko nedelja pre nego što je izvršila i intervenciju na terenu (Markoff 2008).

Drugo, 2010. godine je obelodanjen do tada najmoćniji maliciozni softver (malver, eng. malware) koji je, ispostaviće se (iako nikada zvanično), proizvod američkih i izraelskih obaveštajnih službi. Nazvan „Staksnet" (*Stuxnet*), softver je ciljao iranski nuklearni pogon u Natanzu. Preciznije, Staksnet je manipulisao centrifugama koje su mogle služiti za obogaćivanje uranijuma, menjajući frekvencije struji koja je pružala energiju centrifugama. Brzo menjanje sa izuzetno visokih na izuzetno niske nivoe okretanja, bez mogućnosti operatera da jasno vide u čemu je problem, dovelo je do kvarenja centrifuga i automatskog usporavanja iranskog nuklearnog programa. Tada smo saznali da je Staksnet prvi sajber napad koji je imao direktne fizičke posledice. Dodatno smo saznali i da je

ovaj malver deo šireg programa saradnje SAD i Izraela, nazvan Olimpijske igre (*Olympic games*), koji je pored pomenute sabotaže, podrazumevao i špijunski softver „Flejm“ (*Flame*), instaliran širom država Bliskog istoka (više o Staksnetu i Flejmu: Farwell, Rohozhinski, 2011; Zetter, 2012; Lindsay, 2013).

Staksnet je samo privremeno usporio iranski nuklearni program, ali je dugoročno uticao na porast paranoje i militarizaciju sajber prostora, budući da je Iran ubrzo formirao svoje sajber snage i primenjivao odmazdu napadajući američke i mete američkih saveznika (Slayton 2016, 104-106). Kao jedan od destruktivnijih napada koji se pripisuju[6] Iranu navodi se „Šamun“ (*Shamoon*) malver iz 2012. godine, kada je naftni magnat Saudi Aramko (Saudi Aramco) tek nakon dve nedelje uspeo da uspostavi kontrolu nad svojom mrežom. U napadu ja zaraženo 30 000 radnih jedinica (kompjutera pre svega), sa kojih su, pre nego što su ukradeni, izbrisani svi fajlovi, a kompjuteri postali neupotrebljivi. Prekid kontrole sajber sistema kompanije kao što je Saudi Aramko podrazumeva ogromne finansijske gubitke, što je i razlog zašto je Šamun tada opisivan kao jedan od većih sajber napada u istoriji (Bronk, Tikk-Ringass 2013). Iran je 2014. godine naciljao i metu unutar SAD, kada je napadom (sličnim Šamunu) na sistem „Sends“ kazina (Sands) reagovao na izjavu direktora Sends korporacije, koji je 2013. godine smatrao da bi Iran trebalo napasti nuklearnim bombama. Šteta koja je tada prouzrokovana dostizala je cifru od najmanje 40 miliona dolara (Elgin, Riley, 2014). Međutim, pojavila se znatno važnija stvar od trenutne materijalne štete jednom sistemu kazina. Ukazano je da je strah od hakovanja koji su povezani sa nekom državom postao realan i znatno primetniji nakon Staksneta.

Obelodanjivanje Staksneta i ispunjenje obećanja Irana da će se osvetiti, doveli su i do širenja principa „katastrofiranja“ (eng. dooming). Sada se samo iščekivao veliki napad, razorniji od Staksneta, koji je mogao biti i „sledeći Perl Harbor“, kako je to upozoravao Leon Paneta (Leon Panetta 2012), nekadašnji državni sekretar odbrane SAD. Iako su ruski napadi na Estoniju i Gruziju u literaturi često navođeni kao primeri početaka ofanzivnog delovanja država u sajber prostoru, nisu ni približno doprineli paranoji u javnom prostoru u meri u kojoj je to otkrivanje napada na Natanz. Pre svega jer je postalo jasno da se radilo o prekretnici nakon koje države počinju znatno ofanzivnije da deluju u sajber prostoru. Paranoja je dodatno širena i zbog činjenice da niko nije mogao da predvidi šta bi mogao da bude cilj sledećeg napada. Da li sistemi za prenos električne energije, da li fabrike

[6] Videćemo kasnije da je problem atribucije, ili pripisivanja, jedan od najvećih strateških problema, a samim tim i karakteristika sajber prostora. Rusija nikada nije priznala napad na Estoniju, SAD i Izrael nikada nisu zvanično prisvojili napade na Natanz, niti je Iran priznao da su njegove sajber jedinice stvorile Šamun.

za prečišćavanje voda, grejni sistemi, sistemi kontrole leta, rafinerije, gasovodi, itd. Svi ovi sistemi deo su kritične infrastrukture koja se u većini država danas upravlja putem mreža za upravljanje i nadziranje (SCADA i DCS sistemi) (Peterson 2013, 121).[7] Sajber napadi na ove sisteme mogu ostaviti velike posledice ne samo po industrije država, već mogu dovesti i do smrti velikog broja ljudi. SAD su i same upale u pojačanu paranoju. To se dogodilo nakon što su i same, zajedno sa Izraelom, uticale na otvaranje „Pandorine kutije" sajber napadom na Iran.

Treće, otkrivanje Staksneta koincidiralo je sa stvaranjem sajber komande SAD (United States Cyber Command) 2010. godine. Zamenik sekretara odbrane u to vreme, Vilijem Lin III (William Lynn III), opisao je proces koji je doveo do stvaranja ove institucije. Prema njegovim rečima, nakon što je inficirani USB ubačen u kompjuter u jednoj od vojnih baza SAD na Bliskom istoku, došlo je do masovnog zaražavanja kompjutera Ministarstva odbrane SAD (U.S. Department od Defense). Malver je potom poverljive podatke slao na servere izvan kontrole SAD. Proces čišćenja je potrajao narednih 14 meseci, a taj incident (nejasno povezivan sa Kinom ili Rusijom), kao i primer velikog napora koje institucije moraju da ulože da bi potom otklonile negativne efekte incidenta, pružio je Amerikancima lekciju da moraju ozbiljnije da shvate sajber prostor. Krajnji proizvod tog shvatanja je stvaranje Sajber komande, koja je za početak bila zadužena za: „odbranu (…) i podršku vojnim i antiterorističkim misijama putem operacija u sajber prostoru"; redovno obučavanje za bezbedno delovanje vojnika u sajber prostoru; kao i koordinaciju sa svim drugim bezbednosnim agencijama SAD (Lynn 2010, 102). Osnivanje Komande u SAD dovelo je do toga da dva meseca kasnije Kinezi stave do znanja kako i oni imaju svoj sajber centar (McGuffin, Mitchell, 2014: 397). Do 2015. godine, Kinezi će taj centar razviti u Silu za stratešku podršku (SSF-Strategic Support Force) koja „centralizuje (…) sajber, elektronske i psihološke ratne sposobnosti" Narodnooslobodilačke armije Kine (Costello, McReynolds 2018, 1).

Četvrto, tokom 2011. godine, svedočili smo i „Arapskom proleću". Tada je vladalo oduševljenje među ljudima koji su percipirani kao sajber utopisti. Isticao se Manuel Kastels (Manuel Castells), kom je „Arapsko proleće" obnovilo veru u „svepovezano društvo" (Nagle 2017, 20-21). Obnavljanje vere je posledica činjenice da su revolucije na severu Afrike i Bliskom istoku podrazumevale krah

[7] Skraćenica SCADA proističe iz engleskog jezika – *Supervisory Control and Data Acquisition Networks* – kao i DCS, to jest *Distributed Control Systems*. Dok SCADA podrazumeva sistem nadzora i kontrole na velikim geografskim područjima (recimo elektroenergetske mreže na teritoriji Srbije), DCS podrazumeva upravljanje procesima na jednom mestu, recimo jednoj termoelektrani (Peterson, 2013, 120).

nekadašnjeg centralizovanog i cenzorskog informativnog sistema. Narod je pronašao način da decentralizovano širi nezadovoljstvo koristeći se društvenim mrežama, što je dovelo i do masovne mobilizacije i svrgavanja višedecenijskih režima u nekoliko arapskih zemalja (Khondker 2011). Čitav fenomen je išao pod ruku sa izjavom tadašnje državne sekretarke SAD, Hilari Klinton (Hillary Clinton), kada je 2010. godine izjavila da je strateško opredeljenje njene administracije da održava „slobodan internet" (Price 2017, 130-131). „Arapsko proleće", ali i protesti u Iranu 2009. godine, takođe nastalih na principu mobilizacije preko društvenih mreža zbog, kako se tada smatralo, „krađe izbora", pokazali su da strateško opredeljenje SAD da održava „slobodu interneta" jeste pre svega pitanje njihovog partikularnog interesa. Širen je njihov uticaj kako zbog svrgavanja nekooperativnih režima, tako i zbog toga što je sloboda interneta u tom trenutku direktno povezana sa američkim kompanijama za prikupljanje i širenje informacija. Na taj način je pored liberalizacije političkih sistema širena i platformska „liberalizovana ekonomija", a sve to pod dominacijom jedne države (ibid.). „Slobodan internet" nije nikakva egzogena varijabla na koju ne može da se utiče, već svesni politički izbor jedne velike sile. Nakon Arapskog proleća, Rusija i Kina znatno intenzivnije tumače internet kao jedan od mogućih izbora velike sile koji njima ne odgovara.

Vakuum moći nastao u arapskim zemljama nakon 2011. godine imao je izuzetno negativan neposredni uticaj na države poput Libije i Sirije. Međutim, još važnije za međunarodni sajber poredak, Kina i Rusija su ove događaje posmatrale kao prekretnicu. Recimo, Valerij Gerasimov (Вале́рий Васи́льевич Гера́симов), načelnik Generalštaba oružanih snaga Rusije, objavljuje 2013. godine nešto što će postati poznato kao „Gerasimovljeva doktrina". U njoj obrazlaže da je „Arapsko proleće" poslužilo Rusiji da razume nova pravila ratovanja. Ona sada uključuju „široku upotrebu političkih, ekonomskih, informacionih, humanitarnih i drugih ne-vojnih mera primenjenih u koordinaciji sa protestnim potencijalom populacije", ali i „simultano sukobljavanje u svim fizičkim okruženjima i informativnom prostoru" (Gerasimov 2016, 24).[8] Kina na „Arapsko proleće" reaguje automatskom cenzurom. Međutim, 2013. godine, dakle dve godine kasnije, samouvereno na primeru Libije i Sirije, putem interneta ali i tradicionalnih medija, svojim građanima širi sarkastičan narativ o tome kakav haos sledi državama koje pokušaju da primene model liberalne demokratije (Zeng, Stevens, Chen 2017, 437). Sveukupno, „Arapsko proleće" je zemljama koje su sumnjale u dobre i „neutralne" namere „slobodnog interneta" pokazalo da internet nije prostor koji je namenjen samo špijunažama i sabotažama.

[8] Ovde koristim engleski prevod „Doktrine".

Pokazalo im je da poseduje veliki potencijal za eroziju dotadašnjih institucija podrivanjem njihovog autoriteta u informativnoj sferi.

Peto, uzbunjivač Edvard Snouden (Edward Snowden) je 2013. godine doprineo otkrivanju tajnog američkog programa *PRISM*. SAD je zajedno sa UK koristila velike društvene platforme i pretraživače, poput Fejsbuka (Facebook) i Gugla (Google), kao i softvere Majkrosofta (Apple) i Epla (Apple), zarad prikupljanja podataka o suparnicima, poput Rusije i Kine, ali i zarad prikupljanja podataka o svojim građanima i državama saveznicima (ibid., 440). Kako saznajemo iz Snoudenovih dokumenata, SAD i UK su špijunirali 2009. godine lidere država G20 (Landau, 2013, 66). Takođe, UK je tokom 2010. i 2011. godine, najverovatnije uz pomoć ostalih službi anglosaksonskog sveta, špijunirala institucije EU u Briselu tako što je hakovala rutere belgijskog internet provajdera Belgakoma (Belgacom) (Smeets, 2022a). Objavljivanje ovakvih informacija značilo je i definitivno gubljenje poverenja u „slobodan internet" širom sveta. SAD više nisu viđene kao zaštitnik nekakvog slobodnog modela već neko ko zloupotrebljava poziciju dominacije u sajber sferi. Ta dominacija se možda najviše ogledala u tome što su SAD: pružile podsticaje za nastanak interneta; napravile osnov za omasovljenje njegove upotrebe u poslednjoj deceniji 20. veka; bile dom za osam od deset najvećih tehnoloških kompanija; profitirale i osnažile svoju ekonomsku dominaciju upravo na bazi internet dominacije (Goldsmith, Russel 2018). Nije zgoreg spomenuti i da se deset od trinaest servera koji pružaju nazive domena (*root servers*) nalaze u SAD, a dodatna tri u Holandiji, Švedskoj i Japanu (Nocetti 2015, 121). Radi se o serverima od esencijalne važnosti za operativnost globalnog interneta.

Sveukupno, kulminirajući otkrićem *PRISM* programa, pokazalo se da internet sve više postaje mesto golog nadmetanja država. Razbijene su bilo kakve iluzije o „domenu uma", odsustvu tiranije ili o tehnološkoj neutralnosti, a sajber prostor je postao prilika za sopstveno jačanje ili slabljenje protivnika. Sukobljavanja su postala neprestana. Međutim, ona nikada nisu došla do nivoa eskalacije i rata. Sabotaža, opisana na primeru Estonije, Gruzije, Staksneta i drugih malvera, potom špijunaža, opisana na primeru Flejma i programa *PRISM*, ali i subverzija, kako je percipirano „Arapsko proleće" u očima kineskih i ruskih vlasti, tri su potencijalne ofanzivne akcije država u sajber prostoru koje ne podrazumevaju rat (Rid 2012, 16-22). Ove tri vrste akcija iskristalisale su se kod velikih sila u periodu od 2007. do 2013. godine. Daleko od toga da su države bile nesvesne ovakvih potencijala na internetu i ranije ili da i pre tog perioda nisu koristile sajber prostor zarad obaveštajnog rada.[9] Kina je još 90-ih godina počela sa uspostavljanjem „svog"

[9] Kina je recimo poznata kao država koja je težila ekonomskom hvatanju koraka sa najrazvijenijim državama Zapada putem konstantne industrijske špijunaže (Lindsay, Cheung, Reveron, 2015: 2-3).

interneta, najpre zbog toga što je verovala da je internet mesto odakle može doći „ideološka pretnja“ od „neprijateljskih stranih sila“, oličena u „subverzivnim univerzalnim vrednostima“ – dakle, slobodi interneta (Lindsay 2015, 15).[10] Međutim, serija događaja od 2007. do 2013. godine učinila je da se težnja država za povećanjem kontrole nad internetom, i posmatranjem sajbera kao prostora „obaveštajnog nadmetanja“ (Rovner 2020, 115), sve više pretvara u realnost. U tom periodu se i javno formiraju sajber trupe i centri odlučivanja za delovanje u sajber prostoru kao posebnom domenu sukobljavanja.

Sajber prostor kao zaseban domen sukoba

U SAD se prepričava jedna zanimljiva anegdota kako je ta država uopšte počela sa naglašavanjem značaja sajber prostora. SAD su 1983. godine dobile direktivu pod nazivom „Bezbednost nacionalne politike telekomunikacija i automatizovanih informacionih sistema“. Fred Kaplan opisuje da je direktiva proizvod spleta američke popularne kulture i slučajnosti. Naime, Ronald Regan (Ronald Reagan), tadašnji predsednik SAD, odgledao je jedno veče film „Ratne igre“ (*War Games*), u kom lik tinejdžera iz šale uspeva da hakuje američko Ministarstvo odbrane, i potom serijom događaja dovede svet na ivicu nuklearnog sukoba. Regan je idućeg dana prepričao radnju filma načelniku generalštaba, te ga upitao da li je takav scenario realističan. Nakon par dana raspitivanja, načelnik mu je saopštio da je „situacija mnogo gora“ (Kaplan 2016, 7-8). Međutim, u tom trenutku internet još uvek nije masovan, te se ni razumevanje sajber prostora ne može uporediti sa onim koji se razvija kasnije.

Do 1995. godine, postajalo je jasnije da internet potpuno menja i sama pravila ratovanja. Zbog toga je tadašnji načelnik generalštaba ratnog vazduhoplovstva SAD, Ronald Foglmen (Ronald Fogleman) konstatovao da možemo da pričamo o informacionoj dimenziji kao petoj zasebnoj dimenziji ratovanja. Svoju tezu je obrazložio kroz evoluciju drugih dimenzija. Opisuje kako smo do početka 20. veka kao jedine dimenzije ratovanja imali kopno i more. Potom pominje da je Drugi svetski rat ukazao na veliki značaj nove, vertikalne dimenzije – vazduha (iako je avijacija postojala već u Prvom svetskom ratu). U

[10] Zbog toga su kineski rukovodioci 1993. godine stvorili „Veliki kineski zaštitni zid“ (*The Great Chinese Firewall*) koji je znatno otežavao internet komunikaciju kineskih građana sa spoljnim svetom. Već 1998. godine, kreiran je i projekat „Zlatni štit“ (*Golden Shield*), kojim je otežavana i cenzurisana i unutrašnja komunikacija (Singer, Warren, Brooking, 2018, 96-101).

Zalivskom ratu 1991. godine u igru ulazi i značaj svemira kao četvrte dimenzije.[11] Konačno, smatra, Foglmen, dolazimo do pete, informacione dimenzije ratovanja, koja ima izuzetno veliki uticaj kako na društvo, tako i na vojsku, a „dominacija ovim informacionim spektrom biće od kritične važnosti za vojne uspehe u budućnosti" (Fogleman 1995, 1-3). Foglmen tada još uvek govori o informacionoj sferi, aludirajući pre svega na razvoj interneta. Skoro deceniju kasnije, 2004. godine, još jedan bivši načelnik ratnog vazduhoplovstva SAD, Leri Velč (Larry Welch), konstatuje da možemo govoriti o pet vojnih domena, gde je sajber prostor peti domen. Štaviše, pravi hijerarhiju među njima, opisujući kako je kopno okruženo morem, kopno i more vazduhom, čitava planeta zemlja svemirom, a sva ta četiri domena su direktno zavisna od sajber prostora koji ih prožima i bez kog je ratovanje postalo nezamislivo (Welch 2004: 3). Konačno, stvaranjem Sajber komande SAD 2010. godine je peti vojni domen institucionalizovan i formalizovan (The Economist, 2010). Uprkos naglašavanju da postoji nešto što se zove slobodan ili globalni internet, SAD su, kao što vidimo, vrlo rano postale svesne da se radi o prostoru međusobnog nadmetanja država i drugih aktera radi zaštite partikularnih interesa.

Ne postoji apsolutna saglasnost o tome da se zaista radi o zasebnom domenu. Recimo, pojavio se stav da ne možemo govoriti o odvojenom domenu sukoba zbog najmanje dve stvari: korišćenje reči „domen" jeste puki marketing i prenaglašavanje značaja, jer do sada nismo imali prilike da vidimo oružane napade na nivou rata u sajber prostoru; sajber prostor se ne odlikuje ni približno nekakvom doktrinarnom konzistentnošću kakvom se odlikuju „pravi" fizički domeni, i to pre svega zato što je uvek moguće izmeniti pejzaž sajber prostora kao proizvoda ljudske kreacije, naspram kopna, mora, vazduha i svemira koji imaju jasna fizička ograničenja (McGuffin, Mitchell 2014: 408). Može da deluje zbunjujuće konstatacija o nedostatku oružanih napada u sajber prostoru ukoliko smo prethodno naveli primere napada na Estoniju, Gruziju, Iran itd. Međutim, sve ove operacije se u literaturi koja povezuje sajber bezbednost i međunarodne odnose smatraju delovanjima „ispod nivoa oružanog napada" (Harknett, Smeets 2020, 7).

Do danas nismo imali zaseban sajber rat, smatra se u literaturi, budući da nismo imali ni glavno obeležje rata – a to je da neki napad bude smrtonosan – zbog čega svi napadi bivaju svrstavani u sabotaže, subverzije i špijunaže, dakle u obaveštajnu delatnost (Rid, 2012; Kollars, 2020; Lindsay, 2020; Rovner, 2020).

[11] Zalivski rat je prvi i poslednji put da samo jedna strana koristi tehnologiju navođenja iz svemira (*GPS*) (Cohen, 1994, 112).

Ovakvo shvatanje je podržano i u empirijskoj literaturi, koja se bavi konkretnom upotrebom sajber oružja na terenu. Analizirajući hiljade sajber incidenata u sukobima u Siriji i Ukrajini (u periodu od 2011. do 2016), Kostjuk i Žukov (Kostyuk, Zhukov 2019) nalaze da se pokazalo kako sajber nikako nije mogao do sada da bude supstitucija za kinetički rat. Takođe, pokazalo se da čak nije ni komplementaran sa ostalim domenima, te se često koristi nezavisno. Razlog odvojenog korišćenja, tvrde ovi autori, jeste što je mnogo teže koordinisati sajber napad sa kinetičkim napadom na način da se njihovom kumulativnom primenom postigne velika šteta. U prevodu, neophodna je izrazito precizna vremenska koordinacija efekata jednog sajber napada sa brzinom odvijanja stvari na terenu. Stoga, sajber sabotaže, subverzije i špijunaže se mahom odvijaju nezavisno, u svom mehuru.

U literaturi se često veruje da je ova teza potvrđena i na ratu u Ukrajini nakon ruske intervencije 2022. godine. Rusi su u periodu od 2014. do 2022. godine koristili Ukrajinu za testiranje svojih sajber kapaciteta, neretko stvarajući i štetu koja je imala globalne posledice. Oni su tada hakovali televizijske stanice, ukrajinsku izbornu komisiju (kada su manipulisali rezultatima predsedničkih izbora 2014. godine), ubacivali malvere u energetsku mrežu, brišući podatke i gaseći sisteme na po sat vremena kao upozorenje (Greenberg, 2017). U 2017. godini, Rusi su izvršili napad koji je opisivan kao „korišćenje nuklearne bombe da bi se postigla mala taktička pobeda“ (Greenberg, 2018). Tada je malver „NotPetja“ (*NotPetya*) proširen sa svoje mete u Ukrajini globalno, i pogodio je velike kompanije poput Maerska (Maersk) i Fedeksa (Fedex), brišući terabajte vrednih podataka i rezultujući u ukupnoj šteti od preko 10 milijardi dolara (ibid). Sveukupno, testiranja na Ukrajini, raniji događaji u Estoniji i Gruziji i pokušaj mešanja u politički sistem SAD 2016. godine (Mueller, 2019; Lipton, Sanger, Shane 2016), stvorili su uverenje da će Rusi poraziti Ukrajinu možda i samo sajber ratom.

Zaista, bilo je poprilično sajber napada na Ukrajinu od februara 2022. godine. Rusi su na samom početku intervencije blokadom komunikacija uspeli da stvore konfuziju u ukrajinskoj vojsci, administraciji, policiji i graničnim prelazima, ali su sabotirali i modeme koji su sa zemlje komunicirali sa satelitima. Sve ovo je bilo u skladu sa doktrinom munjevitog napada koji bi izazvao haos i doveo do brzog pada vlade u Kijevu (Cattler, Black 2022). Međutim, nedostajala je efikasna koordinacija uspešnog sajber napada sa situacijom na terenu. Kasnije, sajber nije pokazao pune kapacitete zbog toga što je postojala i izuzetno velika asistencija SAD u ukrajinskoj sajber odbrani (ibid.). Takođe postoji perspektiva da velikog samostalnog sajber napada nije bilo jer to Rusima nije bilo u interesu, pre svega zbog toga što im je bila namera da koriste komercijalne mreže za sopstvenu ratnu komunikaciju i

špijunažu (Kostyuk, Gartzke 2022). Ovo samo dodatno potvrđuje ideju da je sajber prostor prevashodno za sada područje obaveštajnog nadmetanja.

Međutim, to što do sada nismo videli veliki sajber napad koji bi rezultovao u smrti hiljada (npr. napad na kritičnu infrastrukturu), ne znači da se to ubuduće neće i dogoditi. Nema sumnje da je sajber prostor do sada služio za napredni obaveštajni rad, no to ne znači da će tako i ostati. Nisu ni putnički avioni do 2001. godine korišćeni kao oružje po sebi, jer to iz nekakve racionalne perspektive nikome nije bilo u interesu, pa je 11. septembar ipak promenio bezbednosnu arhitekturu sveta. Iako do sada nije došlo do velikog sajber rata, postoji izrazito veliki potencijal da do njega nekada i dođe. Zbog toga, u ovom radu zadržavam predstavu o tome da sajber prostor zaista jeste zaseban domen, ne radi marketinga, već radi pokušaja da se izoluju i razumeju njegove glavne odlike, koje čine da se on razlikuje od drugih domena, i što je važnije, koje determinišu strategije država u sajberu.

Karakteristike sajber prostora kao zasebnog domena sukoba

U literaturi koja se bavi sajber bezbednošću iz perspektive međunarodnih odnosa, možemo da pronađemo da se ponavljaju uvek slične karakteristike sajber prostora kao zasebnog domena. Te karakteristike određuju domete država i njihovo eventualno strateško postavljanje prema pomenutom domenu. Glavne odlike sajber prostora kao zasebnog domena sukobljavanja država su: demokratičnost; veliki potencijal ljudske greške; problem atribucije; tehnička volatilnost; i konačno, vremenska ograničenost i brzina reagovanja. Ove odlike određuju balans, ili nedostatak balansa između ofanzivnog i defanzivnog delovanja država u sajber prostoru, ali određuju i na koji način je moguće uspostaviti međusobno obuzdavanje država u smislu prevencije eskalacije sukoba. Ofanzivno-defanzivni balans i obuzdavanje su pitanja od ključne važnosti kako za ispunjenje strateških ciljeva država, tako i za eventualno razmišljanje o održanju mira i predvidivosti u međunarodnim odnosima.

Prvo, demokratičnost sajber prostora podrazumeva nekoliko stvari, a to je da je on: lako dostupan, da lako obezbeđuje anonimnost, i da stvara veliku međupovezanost i međuzavisnost svih aktera koji mu pristupaju (Wilner 2020, 252). U kontekstu sukobljavanja i strateškog delovanja država, to podrazumeva znatno uvećanje eventualnih opasnosti u smislu toga da napadač može biti bilo ko sa elementarnim pristupom mreži i ne toliko zahtevnim znanjima. Jasno je da i u drugim domenima postoji mogućnost anonimnih napada, ili da obični građani

naprasno mogu postati pretnja i opasnost – na primer tako što se pridruže terorističkim organizacijama ili tako što reše da izvrše pucnjavu na veliki broj ljudi, što nije redak slučaj u SAD. No, demokratičnost sajber prostora je i dalje neuporediva sa drugim prostorima. Broj sajber napada – bilo da se radi o malverima iznude (*ransomware*), malverima koji brišu sadržinu, koji kradu podatke, ili pak običnim ucenama, lažnim predstavljanjima itd., od strane državnih ali i nedržavnih aktera – neuporedivo je veći u odnosu na konvencionalne domene. Gotovo da su beskonačni potencijalni izvori i načini pretnji u sajber prostoru usled nivoa njegove demokratičnosti i gotovo nepostojeće barijere ulaska u domen sukobljavanja. Na konkretnim brojkama, Senat SAD je samo tokom 2017. godine morao da blokira oko 23 miliona mejlova na dnevnom nivou, pošto su stručnjaci za bezbednost zaključili da se iza ovih mejlova krije loša namera, a Pentagon je tokom 2019. godine u proseku morao da blokira 36 miliona mejlova dnevno, ili oko 13 milijardi na godišnjem nivou (Vishwanath 2022, 4). Pored pukih brojeva, međuzavisnost dovodi i do velikog potencijala širenja (*scalability*) virusa kada se on jednom nađe u opticaju (Goodman 2010). To smo mogli da vidimo na primeru NotPetja virusa, kada je, šire gledano, od napada na malu metu, stvoren globalni fenomen u smislu posledica. Takođe, Staksnet možda nikada i ne bi bio otkriven da se nije proširio na mete izvan Irana i obuhvatio kompanije u desetinama država.

Druga karakteristika koja je najtešnje povezana sa demokratičnošću jeste veliki potencijal ljudske greške. Uvreženo je laičko mišljenje kako su sajber napadi plod velikih tehničkih znanja i stručnosti. Međutim, najveći broj sajber napada počiva na pretpostavci da su ljudi skloni banalnim greškama. Nedostatak elementarne „sajber higijene“ zato jeste i uzrok najvećeg broja sajber napada. Teško je prenaglasiti značaj toga da je 95 procenata uspešnih sajber napada proizvod ljudske greške koje su mogle biti izbegnute uz elementarnu prevenciju (Platsis 2019, 24). Recimo, pomenuto zaražavanje kompjutera Ministarstva odbrane SAD 2008. godine, koje je dovelo do stvaranje Sajber komande, započelo je tako što je ubačen USB sa malverom u samo jedan kompjuter od desetine hiljada u sistemu. Pentagon je potom zabranio upotrebu USB-ova svim zaposlenima (Schachtman 2010). USB koji je prvobitno zarazio sistem je dospeo do zgrade tako što ga je jedan vojnik primetio na parkingu vojne baze, te iz čiste radoznalosti pokušao da proveri šta se na njemu nalazi (Singer, Friedman 2014: 64). Najobičnija radoznalost zaposlenog dovela je do najveće operacije čišćenja mreža u Pentagonu i na kraju do institucionalizacije petog domena ratovanja. Takođe, sajber pljačka Nacionalne banke Bangladeša 2016. godine, koja je pripisivana Severnoj Koreji, i u kojoj je ukradeno 81 milion dolara, posledica je jednog klika zaposlenog u banci na naizgled bezazlen link u jednom od hiljada

mejlova (White 2021). Dva navedena primera ilustruju da države u izuzetno dinamičnom sajber okruženju moraju da računaju na veliku verovatnoću ljudske greške. Države su sposobne da se brane od sajber napada u zavisnosti od stepena naivnosti najnaivnijeg zaposlenog kako u javnom sektoru, tako i u privatnom sektoru koji može biti od velikog značaja za bezbednost sistema.

Treća karakteristika sajber prostora jeste problem pripisivanja napada, ili problem atribucije. U konvencionalnim domenima napade je relativno lako pripisati u odnosu na sajber domen. Bilo da se radi o samostalnim izvođačima, ili da iza pojedinaca stoje moćniji igrači, u konvencionalnim domenima će sa visokim stepenom sigurnosti, i u velikoj većini slučaja, sajber napad na kraju biti pripisan pojedincu ili organizaciji. Međutim, zbog lakoće anonimnosti, hakovanja i upotrebe tuđih kredencijala i resursa, u sajber prostoru problem atribucije dolazi do izražaja. Recimo, opisani sajber napad Rusije na Estoniju se očigledno pripisuje Rusiji, ali je sam napad došao sa kompjutera širom Evrope i SAD. Sumnja na Rusiju je bačena kako zbog očiglednog postojanja motiva, tako i zbog odbijanja Rusije da sarađuje u istrazi i pronalasku počinitelja, budući da su neki od kompjutera u napadu bili povezivani direktno sa državnim institucijama (Davis 2007). Rusija zvanično nikada nije priznala ovaj napad, kao što SAD i Izrael nikada zvanično nisu priznali da stoje iza Staksneta. Severna Koreja, naravno, takođe nije priznala da stoji iza pljačke Nacionalne banke Bangladeša. Ni u jednom od ovih slučajeva nemamo jasne dokaze ko je počinilac, ali imamo izuzetno snažne indicije ko bi to mogao biti, zbog čega smo i svedočili javnoj atribuciji napada.

Atribucija postoji kao problem na tri nivoa (Rid, Buchannan 2015, 7): na tehničkom, budući da se radi o tome da je u pitanju „umetnost koliko i nauka“, te da „nema jasnog recepta kako izvršiti atribuciju“; na operativnom nivou, jer je zarad uspešne atribucije neophodno angažovati veliki broj stručnjaka različitih profila koji moraju da budu u međusobnoj koordinaciji; i na strateškom, pošto čak i u slučaju uspešne atribucije, državi možda ne bude u interesu da objavi počinioca, ili obrnuto, u slučaju neuspešne atribucije, ipak objavi počinioca zarad svojih strateških ciljeva. Država (bila atribucija uspešna ili ne) može imati različite razloge javnog pripisivanja napada nekom počiniocu, bez obzira na stepen poverenja u atribuciju. To može biti (Egloff, Smeets 2021, 5-8): kako bi insistirala na postavljanju normi u međunarodnim odnosima i skrenula pažnju na fer i nefer ponašanja; kako bi odvratila od napada, ili pak ucenila i prinudila nekog aktera na ustupke; da uspori eventualno neizbežan nadolazeći napad zbunjivanjem protivnika; da potpuno spreči napad; da bi podelila informacije svojim saveznicima i tako radila na „izgradnji zajednice“; konačno, kako bi povećala svoj međunarodni kredibilitet ukazivanjem da može da se nosi sa kompleksnim izazovima atribucije. Kao što vidimo, atribucija, sa svojom tehničkom i

operativnom kompleksnošću je jedna stvar, dok je javna atribucija kao pitanje strateškog izbora države potpuno odvojena stvar. Javno pripisivanje i dalje ne mora da znači da je država na tehničkom nivou zaista razotkrila počinioce, što u sajber prostoru i dalje ostaje kao izuzetno težak zadatak.

Valjalo bi još naznačiti i da to što je teško pripisati napad, ne znači da se radi i o nemogućem poduhvatu. Hakeri takođe prave greške i ostavljaju tragove, što se može razotkriti sajber forenzikom. Uzmimo jedan prost primer zarad ilustracije ove poente. Radi se o hakovanju mejlova centrale američkih demokrata u godini predsedničkih izbora u SAD 2016. godine. Tada je na površinu isplivao haker „Gucifer 2.0", koji je tvrdio da stoji iza hakovanja mejlova saradnika Hilari Klinton, i od koga je „Vikiliks" (Wikileaks) redovno dobijao ukradene informacije. „Gucifer 2.0" je odgovarao na pitanja medija i izjasnio se kao Rumun čiji je motiv slabljenje kampanje Klintonove kao stvar njegovog političkog izraza. U toj komunikaciji, među novinarima su se našli i oni koji su izveli trik gde su mu preko Gugl prevodioca (Google translate) postavili pitanje na rumunskom jeziku. Ispostavilo se da je „Gucifer 2.0" svoj odgovor takođe formulisao pomoću Gugl prevodioca, što je utvrđeno nakon konsultacije sa onima kojima je rumunski maternji jezik. Zaključak je bio da hakeru rumunski jezik ne može biti maternji. Takođe, dodatnom analizom je pronađeno i da je u gomili fajlova koje je haker objavljivao, korišćena ruska verzija programa Vord (Word) (Lipton, Sanger, Shane 2016). No, bez obzira na pojedinačne slučajeve uspešne forenzike, problem atribucije ostaje jedna od ključnih karakteristika koje definišu ponašanje država u sajber prostoru.

Četvrta karakteristika jeste volatilnost sajber prostora u odnosu na druge domene sukobljavanja. Volatilnost može biti tehnička, proceduralna i fizička (McGuffin, Mitchell 2014, 408-410). Na tehničkom nivou, čovek je taj koji stvara dizajn sajber prostora, to jest, stvara sajber geografiju. Njegova moć u smislu tehničkih mogućnosti je kao kada bi čovek mogao da prkosi zakonima fizike u ostalim domenima. On određuje elementarni tehnološki dizajn koji je od stvaranja interneta pa do skoro bio vezan za ideologiju „tehnološke neutralnosti" iliti „sistem sa minimalnim pravilima koji neće imati centralnu moć niti cenzora" (Dunn Cavelty, Wenger 2020, 10). Čovek može da premosti reku, da prokopa tunel, sravni brdo, dizajnira hipersonično navođeno oružje ili oružje sa balističkom putanjom, ali sve u skladu sa utvrđenim zakonima fizike. U sajber prostoru, zakoni su ono što utvrdi dominantna ideologija ili dominantna politička moć. „Tehnološka neutralnost" je posledica „filozofskih i političkih uverenja tehnološke zajednice" (ibid.), koja vrlo lako mogu biti promenjena ili podređena drugim silama.

Na primer, dugo su algoritmi na društvenim mrežama Zapada bili uređeni na način da im jedini kriterijum uspeha bude što duže zadržavanje korisnika na društvenim mrežama, bez obzira na to koji sadržaj privlači korisnika. Vremenom,

pogotovo nakon 2014. godine, u ove sisteme postepeno bivaju ugrađivani cenzorski mehanizmi gde se određena vrsta sadržaja sankcioniše brisanjem ili smanjenom vidljivošću sadržaja (videti npr.: Cross, 2022; YouTube Help, 2023). Na taj način, može da se utiče na dominantan sadržaj na internetu, ili da se on makar usmerava. Takođe, može da se upravlja eventualnim pokušajima subverzija, ili ono što bi se moglo tretirati kao subverzivno delovanje. Kina je verovatno najpoznatiji primer drugačijeg tehnološkog dizajna, pošto na „svom" internetu već dugo primenjuje sistem filtracije ključnih reči (*keyword filtering*). Sistem podrazumeva da ukoliko je određena reč, ili kombinacija reči zabranjena na tlu Kine, njihovim ukucavanjem u pretraživač npr. nećemo dobiti nikakve rezultate, niti će naše poruke koje bi sadržale takve reči dostići svoju destinaciju. Jedan od poznatijih primera je zabrana kombinacije reči „Panama" i „papiri", pošto se u ovim dokumentima pominjao i zet kineskog predsednika (Singer, Warren, Brooking 2018, 97). Svako insistiranje na povezivanju sa korupcijom ili eventualnim iznošenjem novca iz države bi vlasti u konkretnom slučaju mogle da percipiraju kao pokušaje subverzije. Dakle, ultimativna ocena i procena šta je dozvoljeno u sajber prostoru, itekako može da zavisi od čoveka, a ne od više sile, kao što je to slučaj u drugim domenima. Volatilnost osnovnih pravila igre na tehničkom nivou u sajber prostoru je neuporediva sa stabilnošću fizičkih zakona u drugim domenima sukobljavanja.

U proceduralnom smislu, mnogo je lakše eliminisati pretnju u sajber prostoru, ako se ona otkrije na vreme, nego što je to slučaj sa recimo domenom vazduha ili svemira. Interkontinentalne balističke rakete ostaju strateška pretnja po države, uz veliku sigurnost da se u skorije vreme tu situacija neće drastično promeniti. U sajber prostoru se ranjivosti u slučaju pravovremenosti uglavnom jednostavno mogu ukloniti.

Konačno, sajber prostor uveliko zavisi i od volatilnosti na fizičkom nivou. S jedne strane, državama je izuzetno teško, a često im nije ni u interesu, da ograniče sadržaj u sajber prostoru na svojoj teritoriji. Za razliku od kopnenih granica, protočnost sajber granica je neuporediva. Ipak, postoje jasne tendencije da se stvaraju „nacionalni" interneti koji bi mogli po potrebi da se izoluju od spoljnog sveta.[12] Recimo, Rusija je među prvim zemljama koja tvrdi da je uspešno testirala ovu mogućnost 2021. godine (Reuters 2021), nakon što je 2019. godine

[12] Cilj država poput Kine i Rusije jeste da se uspostavi „sajber Vestfalija", po uzoru na ugovore u Minsteru i Osnabriku 1648. godine, kada su evropske sile dogovorile da se ne mešaju jedne drugima u unutrašnje poslove. Vestfalski princip nemešanja i suverenosti je nešto što u međunarodnim forumima Kina i Rusija pokušavaju da uspostave kao normu u sajber prostoru (videti: Deibert, Pauly 2019, 81-83).

donela „Zakon o suverenom internetu“. Jedan od glavnih ciljeva ovog Zakona jeste da država primora telekomunikacione kompanije da uspostave sistem „duboke inspekcije paketa“ (*Deep Packet Inspection – DPI*), kao i da državno nadzorno telo (Роскомнадзор) uspostavi ključne tačke kontrole saobraćaja na internetu (Sherman 2021). U prevodu, država će kontrolisati sav saobraćaj na internetu, i imaće mogućnost kontrole sadržaja samog saobraćaja (kada on nije šifrovan). Pandan tome bi bio da recimo država u svakom trenutku prilikom kontrole saobraćaja zna kakvi razgovori se odvijaju u automobilima na kolovozu. No, bez obzira na uspešne probe suverenog interneta, i činjenicu da država može da kontroliše većinu fizičke infrastrukture od koje i zavisi internet saobraćaj (poput optičkih kablova), uglavnom će ostajati makar neka konekcija sa spoljnim svetom koja može da se iskoristi za plasiranje malicioznog sadržaja.

Peta karakteristika se tiče vremenske ograničenosti i brzine reagovanja. Države uglavnom nemaju vremena, ili čak i ne znaju da se u njihovim sistemima nalazi potencijalna ranjivost. Recimo, 2017. godine, britanski zdravstveni sistem je bio pod udarom napada koji je iskoristio ranjivost Vindous (Windows) operativnih sistema. Maliciozni virus (*WannaCry)* iskoristio je poznatu ranjivost starih sistema i automatski zaključao sve podatke, a napadači su potom tražili otkup za otključavanje podataka. Situacija je razrešena relativno brzo, no posledice privremenog zaključavanja su da je hiljade pregleda pacijenata (pa i onih najugroženijih) širom zemlje otkazano (Ghafur et al. 2019). U slučaju *WannaCry* napada*,* ranjivost je bila poznata od ranije, a učinkovitost napada je posledica neažuriranja softvera – što nas opet vodi argumentu da je ljudska greška najveći izvor problema sajbera. Međutim, ukoliko bismo se vratili na virus Staksnet, videli bismo da je on u sebi sadržao nešto što se zove eksploatacija nultog dana (*zero days exploit*). Ova vrsta eksploatacije podrazumeva da napadač koristi ranjivost u sistemu koja nije poznata onome koji je napadan. To znači da nema vremena, tačnije, da postoji nula dana za pripremu odbrane, odakle i naziv toj vrsti eksploatacije (Smeets 2022b). Ako neko ni ne zna da njegov sistem ima ranjivost, i ako ta ranjivost može biti korišćena za tiho prisustvo u sistemima kao napad i reagovanje po potrebi, kako se onda zaštititi od ovakve vrste opasnosti? Upravo u odgovoru na ovo pitanje, pored uzimanja u obzir četiri ranije opisane karakteristike, leži i teorijska izgradnja strategije delovanja država u sajber prostoru koju predstavljam u narednom delu.

Odvraćanje u sajber prostoru i teorija „upornog angažmana“

Zamislimo da se nalazimo u poziciji donosioca odluke u nekoj moćnijoj državi i da razmatramo na koji način strateški delovati u sajber prostoru. Saznajemo da se sajber može koristiti za nanošenje štete našoj kritičnoj infrastrukturi, što pored značajnih ekonomskih gubitaka, može dovesti i do velikog broja smrtnih slučajeva. Istovremeno, zamišljamo da i u drugim državama postoje donosioci odluka koji se suočavaju sa istim dilemama. Stoga, pretpostavljajući da i oni dele našu racionalnost, priželjkujemo međusobno nenapadanje, tačnije, međusobno obuzdavanje. Kako se države međusobno obuzdavaju u sajber prostoru?

Odgovor na ovo pitanje u početku je bio definisan shvatanjem obuzdavanja iz drugih domena sukoba. Termin sajber obuzdavanje (*cyber-deterrence*) upotrebio je 1994. godine Džejms Der Derian (James Der Derian 1994) kako bi nakon posete jednoj sajber simulaciji bitke opisao ono što je video. Po njegovom mišljenju, simulacija je bila otvorena za javnost kako bi se svetu sajber signaliziralo da se ne isplati napadati SAD. Slično je i sa nuklearnim simulacijama. Obuzdavanje se ne stvara samim napadom, već uverenjem drugih da do napada može i doći. Uopšteno, da bi obuzdavanje bilo uspešno, nužno je da bude zadovoljeno nekoliko kriterijuma (Goodman 2010; Wilner 2020): da akteri dele istu racionalnu poziciju oko posledica napada; da ta racionalnost pretpostavlja da je nenasilje bolje rešenje; da strane jasno daju do znanja drugima da će pretnje u slučaju kršenja racionalnosti biti ostvarene i da će iracionalno ponašanje biti kažnjeno; da strane uverljivo imaju i kapacitete da kazne; konačno, obuzdavanje ima jedino smisla protiv jasnog i poznatog protivnika.

Der Derian je, stoga, poistovećivao sajber obuzdavanje sa ranije poznatim karakteristikama i oblicima obuzdavanja. Nije bilo neophodno izvršiti nuklearni napad da bi se obuzdala druga strana, već je bilo dovoljno vršiti probe i simulacije. Slično se mislilo i za sajber prostor u smislu da je on idealan kandidat za slanje signala o potencijalnim pretnjama i posledicama, što će dovesti do racionalnog ponašanja aktera i nenasilja. Međutim, sajber domen se drastično razlikuje po svojim karakteristikama od drugih domena. Demokratičnost, sklonost ka ljudskoj grešci, problem atribucije, volatilnost i brzina, čine da „stara“ pravila racionalnosti prestaju da važe. Ako znate da da svi imaju pristup sajberu, da mogu biti anonimni, brzi i neprimetni, odvraćanje kroz investiranje u odbranu i signaliziranje sopstvene snage postaje preskupo, i često besmisleno. Zbog toga se brzo pojavilo mišljenje da je u sajber prostoru odbrana daleko skuplja od napada i da bi napad morao da dominira u svakoj nacionalnoj sajber strategiji.

Ako se još prisetimo da se napadi događaju i bez toga da smo svesni naše ranjivosti, odbrana može delovati čak i nemoguće (Kello 2013, 27-28). Ravnoteža između napada i odbrane je u konvencionalnim strategijama obuzdavanja bila mahom na strani odbrane. Odnosno, investiranje u ofanzivne kapacitete, i uverljivost njihovih razornih posledica, bez iskorišćavanja tih kapaciteta, bili su dovoljni da se protivnici odvrate od pokušaja napada.

Sajber prostor, s druge strane, zbog njegovih navedenih karakteristika, podrazumeva konstantan kontakt suparnika, nasuprot pukom signaliziranju ili pretnji. Svedočimo konstantnom angažovanju i manjim ali upornim operacijama država, zbog čega obuzdavanje investiranjem u odbranu postaje nedovoljno, a država može imati koristi od sajber prostora samo ako i ona upornim ofanzivnim operacijama teži stvaranju taktičkih, operativnih i strateških prednosti (Fischerkeller, Harknett 2017, 399). Više manjih operacija može vremenom dovesti do kumulativnih koristi i ostvarivanja strateških ciljeva.[13] Recimo, strateški cilj Kine podrazumeva ubrzano sustizanje tehnološki najrazvijenijih zemalja, što je ova država u velikoj meri uspevala i korišćenjem sajber prostora, pre svega u domenu industrijske špijunaže. Međutim, ona to nije uradila jednom velikom, već hiljadama manjih, često i neprimetnih operacija. Onda kada su ove operacije i primećene, zbog odlika sajber prostora (atribucije i demokratičnosti) nisu proizvele osvetu ili neke značajnije posledice. Za razliku od drugih domena, dakle, strateška prednost u sajberu se često ostvaruje gomilom manjih operacija ispod nivoa sukoba, umesto nekakvim velikim i direktnim ratom (Harknett, Smeets 2020).

Zbog svega toga, nastaje i teorija „upornog angažmana“ koja razmatra najbolji mogući način za delovanje država na osnovu specifičnih karakteristika sajber domena (Fisherkeller, Goldman, Harknett 2022). Teorija jasno stavlja naglasak na to da je ofanziva ne samo jeftinija, već da je i znatno delotvorniji vid ponašanja u sajber prostoru. Autori veruju da će se sve države pridružiti ovoj novoj racionalnosti koja je zasnovana na karakteristikama sajber prostora, te da će svaka od njih težiti strateškim dobitima stalnim kontaktom i stalnom prisutnošću. Vremenom će, tvrde, doći do toga da se razvije uverenje država da svaka od njih, zbog stalnih akcija i stalne prisutnosti u neprijateljskim sistemima, može itekako nauditi svom protivniku. Samo uverenje i strah od velike akcije

[13] „Smrt pomoću hiljadu rezova“ je stara tehnika mučenja do smrti koja se u Kini koristila makar hiljadu godina za najteže zločine poput izdaje. U literaturi o sajber bezbednosti i delovanju država, naziv ove tehnike biva usvajan radi opisivanja uspešne državne strategije (Maness, 2021)

suparnika, zbog znanja da smo i mi u mogućnosti da mu učinimo veliku štetu, dovešće do deeskalacije, ili do toga da se akcije velikog i smrtonosnog obima i ne koriste u sajber prostoru. Teorija je kontraintuitivna, u smislu da njeni autori veruju da je eskalacija u vidu akcija ispod nivoa sukobljavanja nužna zarad deeskalacije i obuzdavanja na nivou sukoba većeg obima (Fischerkeller, Harknett 2017, 389-391).

Međutim, jedno je konstatovati da je ofanziva plodotvoran način delovanja radi ostvarenja strateške dobiti, a sasvim druga koliko je teško takvu ofanzivu i ostvariti. Rebeka Slayton (Rebecca Slayton 2016, 82-91) obrazlaže da ravnoteža u sajberu između ofanzive i defanzive zavisi od nekoliko činjenica: pored toga što su neophodne i napredne tehnologije, izuzetno je teško i skupo za države da gaje raznovrsne talente koji su neophodni za ofanzivu; ofanziva i defanziva zavise od organizacionih sposobnosti i smanjivanja ljudske greške na minimum, što je opet izuzetno zahtevan i često nemoguć zadatak; konačno, vrlo je skupo da se napravi tehnologija koja može naneti nekakvu fizičku štetu. Maks Smits (Max Smeets) slično opisuje da je zarad organizacije sajber trupa neophodno uskladiti mnogo faktora. Neophodna je raznovrsnost talenata, ali i dostupnost različitih mogućnosti napada, alata, infrastrukture i organizacionih kapaciteta. Recimo, neophodni su pravnici, ljudi sa znanjem puno različitih jezika, sajber forenzičari, stratezi, operacioni konsultanti itd. Potom neophodno je platiti skupe napade, ali i gomilu manje skupih alatki za napade. Na kraju, neophodno je sve to organizovati, ali imati i infrastrukturu za stalne treninge i simulacije (Smeets 2022a). Pretpostavka je da samo najveće države mogu sebi da priušte postojanje sajber trupa. Međutim, to se pokazalo neistinitim, makar na primeru Izraela i Severne Koreje koje su uz rigidnu i fokusiranu organizovanost uspele da kreiraju itekako efektivne trupe sa globalnim dometima.

Sveukupno, teorija upornog angažmana je bazirana na stanovištu da različite karakteristike sajber prostora pružaju osnov za različito strateško razmišljanje u tom domenu. Demokratičnost, veliki potencijal greške, problem atribucije, volatilnost i brzina, čine da se potpuno menja strateška ravnoteža između napada i odbrane na koju smo navikli u konvencionalnim domenima. Stoga, menja se i strategija obuzdavanja i način na koji se ostvaruju strateški ciljevi. Države u sajber prostoru moraju biti uporne u svom angažmanu i moraju stalno ispitivati mogućnosti napada i kontakta sa suparnikom. Prema pomenutim teoretičarima, to nije stvar izbora, no pitanje nužnosti, ukoliko želite da održite relevantnost u međunarodnim odnosima.

Evolucija sajber strategija SAD

Evoluciju strateškog razmišljanja o sajber domenu u teoriji, pratila je i evolucija razvoja američkih strategija koje se vezuju za sajber prostor. Tako početne strategije, pa i tokom celokupne prve decenije 21. veka, oslikavaju naviknutost na odbranu i obuzdavanje kao najbolji način ostvarivanja strateških koristi SAD. Recimo, Bela kuća je 2003. godine objavila dokument koji je nazvan „Nacionalna strategija za obezbeđivanje sajber prostora". U njemu je jasan naglasak na odbrani u formulacijama da su ključni ciljevi SAD u tom domenu da „spreči sajber napade na američku kritičnu infrastrukturu", potom da „smanji ranjivost" na napade u sajber prostoru, i konačno, da „smanji štetu i vreme oporavka od napada koji su se već dogodili (White House, 2003, viii). Iako znamo da je već od 2007. godine sajber prostor trpeo velike promene u smislu njegove jasnije militarizacije, kao i da je Sajber komanda SAD osnovana 2010. godine, u doktrinarnom smislu do tada nismo imali nove i velike koncepte.

Međutim, stvari se menjaju 2011. godine. Tada Ministarstvo odbrane donosi „Strategiju za operacije u sajber prostoru". Najpreči cilj države prema ovom dokumentu jeste tretman sajber domena kao prostora za „organizaciju, obuku i opremanje, tako da Ministarstvo može u potpunosti da iskoristi potencijale sajber prostora" (United States Department of Defense, 2011, 5). Iskorišćavanje potencijala se drastično razlikuje od ranijih formulacija otpornosti i priprema za odbranu. Potencijali mogu podrazumevati i ofanzivne operacije i pružanje prilika za ostvarenje koristi koje ne bi postojale bez upotrebe sajbera. Ovde se već jasno ukazuje da bi tretman novog domena mogao biti drugačiji u odnosu na ostale. Paralelno sa ovom strategijom, administracija Baraka Obame (Barack Obama) 2012. godine donosi direktivu naziva *PPD-20*. Po toj direktivi, dozvoljava se ofanzivno delovanje Sajber komande izvan granica SAD. Takvo delovanje je još uvek ograničeno na niz odobrenja administracije, i prema direktivi, koristi se u nužnim slučajevima (Healey, 2019, 3). To znači da su SAD i formalizovale ofanzivne operacije, ali da su njihov obim i brzina još uvek zavisili od često sporih birokratija.

Direktiva *PPD-20* važi sve do 2018. godine, kada je zamenjena direktivom zasnovanoj na novoj „Sajber strategiji Ministarstva odbrane", objavljenoj iste godine. U toj Strategiji sada već imamo eksplicitno pominjanje aktera poput Kine i Rusije koji su označeni kao „strateški takmaci". Navode se i konkretne operacije ovih zemalja za koje se smatra da su ugrozili bezbednost SAD. U slučaju Kine, to je serija industrijskih špijunaža kako privatnog, tako i javnog sektora SAD, dok se u slučaju Rusije radi o pokušaju mešanja u politički sistem 2016. godine hakovanjem mejlova demokrata i podsticanjem polarizacije putem društvenih mreža. Sve zajedno, akcije Kine i Rusije su označene kao „uporne kampanje".

Takođe, SAD sada otvoreno konstatuju kako će preduzimati „akcije u sajber prostoru u svakodnevnom takmičenju kako bi sačuvale vojnu prednost i branile interese SAD“. Konačno, Strategija značajno povećava nivo asertivnosti u delu gde se Ministarstvo „usmerava ka ‘isturenoj odbrani’“, podstiče ka „oblikovanju svakodnevnog takmičenja“ i „priprema za rat gradeći smrtonosniju silu“ (United States Department of Defense, 2018, 1-7). Nova direktiva iz 2018. godine, označena kao *NSPM-13*, uklanja sva administrativna ograničenja stare, *PPD-20* direktive, i biva potpuno usaglašena sa ofanzivnim karakterom i rečnikom Strategije iz 2018. godine. Možda je najbolje formalnu i faktičku razliku između novih i ranijih dokumenata opisao Trampov savetnik za nacionalnu bezbednost, Džon Bolton (John Bolton). On je smatrao da zbog nove direktive, administraciji „nisu više vezane ruke kao što su bile za vreme Obamine administracije“, te da se sada ofanzivne akcije mogu vršiti bez ikakve zadrške (Healey 2019, 3-4).

Strategija iz 2018. dobila JE svoju konkretizaciju i u nastupima direktora Sajber komande SAD, Pola Nakasonea (Paul Nakasone)[14]. Nakasone obrazlaže kako Strategija omogućava administraciji da u svakom trenutku raspolaže vrlo širokim spektrom opcija za napad, pre svega zato što se njome favorizuje „uporno angažovanje“ sa „isturenom odbranom“ (Nakasone, 2019). Odnosno, Sajber komanda će težiti da penetrira sve kritične sisteme svojih takmaca, kako bi u presudnim momentima SAD imale na raspolaganju različit spektar opcija za napad. Konstantna prisutnost podrazumeva i konstantan kontakt i uporno angažovanje sajber trupa u ofanzivnim akcijama. Pretpostavka takvog mišljenja je da će uporni angažman služiti i obuzdavanju protivnika, pogotovo ako se povremenim akcijama signaliziraju ofanzivne mogućnosti. Međutim, karakteristike sajber prostora i delovanje drugih država, na šta je skrenuta pažnja u Strategiji iz 2018. godine, dovodi do toga da SAD veruju kako su i druge države već u njenim sistemima. Kada pogledamo rečnik strategije, ali i obrazloženje Nakasonea, vidimo da se obe ove stvari u potpunosti poklapaju sa teorijom upornog angažmana. Ovo ne bi trebalo da čudi, imajući u vidu da su kreatori te teorije povezani sa Sajber komandom ili kao predavači ili direktno kao njeni stratezi.[15]

Preterano bi bilo reći da je teorija upornog angažmana oblikovala asertivnije ponašanje SAD u sajber prostoru. Kao što smo videli još na primerima Staksneta

[14] Koji je istovremeno direktor Nacionalne bezbednosne agencije, NSA (National Security Agency).

[15] Napomenuo bih da sam tokom školske 2022-2023 godine bio gostujući istraživač na Univerzitetu u Sinsinatiju, gde je jedan od autora teorije, Ričard Harknet, redovni profesor i direktor Škole za javne i međunarodne poslove, kao i direktor Centra za sajber strategije i politike. Stoga, imao sam prilike i iz prve ruke da čujem i razumem evoluciju razmišljanja koje je postalo osnov za najvažniji strateški dokument SAD koji se tiče delovanja u sajber prostoru.

i Flejma, SAD su itekako imale istaknute ofanzivne operacije i pre 2010. godine. Pre bismo mogli da kažemo da je rečnik i konceptualizacija pratila američke akcije i da je kasnila za njima. „Sukobljavanje ispod nivoa rata“ je postala pravilnost sajber prostora i pre nego što se neko dosetio da na osnovu ove karakteristike kreira rečnik upornog angažmana ili isturene odbrane. Jakobsen (Jacobsen) piše, na primer, kako je potpuno nepotrebno usvajanje ofanzivnijih koncepata i rečnika. Jer, ukoliko su već uočene pravilnosti i način na koji funkcioniše kontakt u sajber prostoru, a koji kontraintuitivno omogućava deeskalaciju, zašto je neophodno dodatno opterećivati strategije ofanzivnim i često neprijateljskim rečnikom (Jacobsen 2021, 703-705)? Takođe, jasno isticanje ofanzivne terminologije šalje signal stranoj publici da su SAD predvodnik militarizacije sajber prostora i da će to uporno nastaviti da predstavljaju i u budućnosti (Healey 2019, 7).

Tokom 2022. godine, SAD su donele i Nacionalne strategije bezbednosti i odbrane. Sajber prostor u njima igra značajnu ulogu sada već u jasno definisanom karakteru borbe protiv Kine i Rusije. Strategije opisuju maltene totalnu, integrisanu borbu na zemlji, u vodi, vazduhu, svemiru i sajberu, protiv Kine kao glavnog dugoročnog strateškog izazivača, koja jedina ima pretenziju promene celokupnog međunarodnog poretka, a opisuje i akutnu integrisanu borbu protiv Rusije (The White House 2022; United States Department of Defense 2022). „Nacionalna strategija za sajber bezbednost“ iz marta 2023. godine ponavlja neke od glavnih tačaka Strategija bezbednosti i odbrane. Među njima je svakako označavanje Kine i Rusije kao glavnih izvora pretnji po SAD, uz dodatak Irana i Severne Koreje. Svakom od ovih aktera posvećena je zasebna pažnja, gde se Rusija i Kina izdvajaju kao primeri „upornih pretnji“ (*persistent threats*), uz navođenje ruskog NotPetja virusa kao otelotvorenja toga kolika šteta može da se desi zbog ogromne međupovezanosti u sajber prostoru. Zanimljivo, reč „uporno“ se sada koristi isključivo kao epitet malicioznih aktera (strategija navedene države označava kao neprijatelje i maliciozne aktere) na tri mesta u Strategiji, bez ijednog korišćenja upornosti u kontekstu delovanja SAD (The White House 2023). Time vidimo da je napušten rečnik Strategije iz 2018. godine, i da je usvojena tadašnja kritika da se stiče utisak kako su SAD predvodnik militarizacije, upravo zbog definisanja svog „upornog angažmana“. Takođe, nova strategija ne koristi reč „obuzdavanje“ nigde, dok je ona u Strategiji iz 2018. godine upotrebljena 20 puta.[16]

U Strategiji iz 2023. godine se čak eksplicitno navodi kako se napušta ranija doktrina „isturene odbrane“ (*defend forward*) kojom je opisivana spremnost SAD

[16] Uporediti pretragom ključnih reči *persistent* i *deterrence*.

da konstantno budu u sistemima protivnika, te da na taj način pružaju opcije za napad donosiocima odluka. Sada je rečnik znatno zamućen. „Isturena odbrana" se menja novim pristupom „remećenja" (*disruption*) malicioznih aktivnosti, i ostaje nejasno kakva je zapravo razlika između dva procesa (ibid., 13-15). Uopšteno, remećenje, uključujući i preventivno sprečavanje malicioznih aktivnosti, ima izuzetno širok spektar. Ono u konceptualnom smislu može uključivati i ranije definisan „uporni angažman" kao i „isturenu odbranu". No, čini se da je usvojena kritika o ranijem militarizujućem rečniku, te da se koncepti upornosti i isturenosti sada vezuju samo za neprijatelje i maliciozne aktere. SAD promenom rečnika u novoj Strategiji nastoje da neguju imidž aktera koji se ponovo samo brani, budući da je defanziva dominantna u rečniku Strategije. Da ne bi došlo do zabune, to ne znači da defanziva u strateškom smislu ima prednost nad ofanzivom u sajber domenu, već se čini da su u SAD postali svesni negativnog marketinškog prizvuka pređašnjeg ofanzivnog rečnika, na šta je ukazivao jedan od kritičara američkih dokumenata (Healey 2019, 7).

Konačno, nije zgoreg pomenuti i da nova strategija skreće pažnju na veliki značaj privatnog sektora za odbranu i otpornost u sajber prostoru. Stavlja se fokus na činjenicu da se ne može očekivati od malih biznisa i pojedinaca da ne prave greške, ali da se od vladinih agencija i privatnih tehnoloških firmi očekuje da preuzmu odgovornost za sistemsku odbranu i bezbedno skladištenje podataka (ibid., 4-5). To bi u prevodu značilo da se od društvenih platformi i velikih softverskih kompanija očekuje da u potpunosti sarađuju sa federalnim vlastima u usklađivanju nacionalne politike bezbednosti u sajber prostoru. Posledica takvih konstrukcija jeste da će nekada globalne društvene mreže sve više biti percipirane kao nacionalne. SAD time same sebe stavljaju u paradoksalnu poziciju gde su one istovremeno promoter globalnog interneta (naspram „sajber Vestfalije" Kine i Rusije), uz strateško opredeljenje i potencijalna zakonska rešenja koja će primoravati sve domaće firme da se prilagode nacionalnoj bezbednosti SAD. Tipičan primer sprovođenja Strategije, ali i paradoksalne situacije, jeste saslušanje direktora kineske kompanije TikTok u martu mesecu 2023. godine u Kongresu SAD. Tokom više od 5 sati postavljanja pitanja i iznošenja stavova, jasno se vidi da su tehnološke kompanije viđene kao privatne i globalne samo ukoliko su upravljači i vlasnici unutar SAD (C-SPAN 2023). Time SAD doprinose „sajber Vestfaliji" makar u jednakoj meri kao Kina i Rusija, budući da šalju signal ostatku sveta da kada kažu „globalno", zapravo misle na „ekskluzivno rezervisano za interes SAD".

Sveukupno, najnovija Strategija koja se tiče delovanja SAD u sajber prostoru zamućuje i menja rečnik koji je od 2018. do 2023. godine bio znatno iskreniji i otvoreniji. Čini se da su SAD naučile lekciju prema kojoj sukobljavanje ispod nivoa

rata, uporni angažman i isturena odbrana nužno proističu iz karakteristika sajber prostora, ali da takve konstrukcije ne moraju da stoje i u Strategiji. Time se smanjuje značaj i same Strategije, budući da iz nje mnogo teže možemo da čitamo stvarne strateške postavke SAD. Ranije opisana teorija upornog angažmana je i dalje srž objašnjenja delovanja nominalno najbogatije države sveta u sajber prostoru, bez obzira što su ključni koncepti ove teorije izbačeni iz najnovije Strategije. To će tako ostati i u doglednoj budućnosti, pre svega zbog toga što se ključne karakteristike sajber domena svakako neće tek tako promeniti.

Zaključak

U radu je napravljen pregled postojeće literature koja se bavi sukobima i strategijama u sajber prostoru, s ciljem izdvajanja ključnih karakteristika sajber domena. Kao ključne karakteristike izdvajam: demokratičnost, koja se ogleda u lakoj dostupnosti sajbera, anonimnosti i velikoj međupovezanosti i međuzavisnosti aktera; veliki potencijal ljudske greške, uz naglasak da 95 procenata sajber napada imaju uzrok u jednostavnim ljudskim greškama; problem atribucije, koji se vidi u izuzetno teškom pripisivanju sajber napada određenom akteru; volatilnost, koja može biti na tehničkom, operativnom i fizičkom nivou, budući da čovek može promeniti i same zakone i osnovne postavke sajber prostora; konačno, vremenska ograničenost i brzina reagovanja, pošto sajber napadima možemo biti izloženi a da toga nismo ni svesni (što je često slučaj kod krađe podataka), ili ako i postanemo svesni, često ne možemo mnogo toga da učinimo u kratkom vremenskom roku. Opisane karakteristike su i osnov strateškog mišljenja teorije upornog angažmana, koja je potpuno promenila razumevanje obuzdavanja i ukazala na to da sajber prostor favorizuje ofanzivno naspram defanzivnog delovanja aktera.

Međutim, rad nije puki pregled literature, već se teorija upornog angažmana poredi sa evolucijom strateških dokumenata SAD koje se tiču sajber prostora u periodu od 2003. do 2023. godine. Početne strategije bile su odraz razmišljanja o tome kako obuzdati suparnika u drugim domenima, bez razmišljanja o specifičnostima sajber prostora. Takođe, novije strategije u svojoj srži imaju teoriju upornog angažmana, bez obzira što Strategija iz 2023. godine izbacuje rečnik ove teorije. Nešto zamućeniji rečnik ne odražava nameru, ali i ranije delovanje SAD, koje počiva na upornim ofanzivnim akcijama u sajber prostoru ispod nivoa rata. Ovo se najbolje može videti u činjenici da su SAD još u periodu od 2007. do 2013. godine razumele prednosti ofanzive u tom domenu. Stoga,

zaključak je da najnovija Strategija nema veliku saznajnu vrednost bez uporedne perspektive sa ranijim sličnim dokumentima, ali i konkretnim akcijama SAD u sajber domenu, koje su uporne, i vrlo često ofanzivne, a sve u skladu sa karakteristikama koje tu ofanzivnost i podstiču.

Neophodno je na kraju skrenuti pažnju na to da razumevanje karakteristika sajber prostora, ali i delovanje jedne moćne države poput SAD ima koristi i za eventualno strateško razmišljanje u malim državama poput Srbije. Države koje razumeju koristi ofanzivnog delovanja u sajber prostoru, vremenom će se sve više približavati kumulativnom koristima i postizanjima strateških ciljeva. Države koje propuste ovu priliku, biće izložene upornim operacijama drugih država, branile se one ili ne. Stoga, bez obzira koliko to bio težak i komplikovan zadatak u tehničkom, operativnom i fizičkom smislu, i manje države moraju pristupiti izgradnji sajber trupa ukoliko nameravaju da i dalje projektuju onoliko suverenosti koliko je to moguće. Dalja istraživanja na ovu temu bi zato morala biti usmerena na popisivanje različitih strategija koje države mogu usvojiti u sajber prostoru u zavisnosti od svog položaja, projekcije moći i stepena rizika sa kojima se suočavaju, što bi itekako koristilo i zemljama poput Srbije.

Bibliografija

Barlow, John Perry. 1996. "Declaration of Independence for Cyberspace." *Electronic Frontier Foundation*. https://www.eff.org/cyberspace-independence.

Bradshaw, Samantha, and Philip N. Howard. 2018. "The global organization of social media disinformation campaigns." *Journal of International Affairs* 71(1): 23-32.

Bronk, Christopher, and Eneken Tikk-Ringas. 2013. "The cyber attack on Saudi Aramco." *Survival* 55 (2): 81-96.

C-SPAN. 2023. "TikTok CEO Shou Zi Chew testifies before Congress." YouTube, March 2023. https://www.youtube.com/watch?v=_E-4jtTFsO4.

Cattler, David and Daniel Black. 2022. "The Myth of the Missing Cyberwar." *Foreign Affairs*, April 6. https://www.foreignaffairs.com/articles/ukraine/2022-04-06/myth missing-cyberwar.

Clinton, Bill. 2000. "Clinton's words on China: Trade is the smart thing." *The New York Times*, March 9. https://www.nytimes.com/2000/03/09/world/clinton-s-words-on-china-trade-is-the-smart-thing.html.

Cohen, A. Eliot. 1994. "The Mystique of U.S. Air Power." *Foreign Affairs* January-February: 109-124.

Costello, John, and Joe McReynolds. 2018. "China's strategic support force: A force for a new era." *China Strategic Perspectives 13*, Institute for National Strategic Studies.

Cross, Katherine. 2022. "The Transparency Theater of the Twitter Files." *The Wired*, December 12. https://www.wired.com/story/twitter-files-elon-musk-shadowbanning-censorship/.

Davis, Joshua. 2007. "Hackers take down the most wired country in Europe." *Wired magazine*, August 21. https://www.wired.com/2007/08/ff-estonia/

Deibert, Ronald J., and Louis W. Pauly. 2019. "Mutual entanglement and complex sovereignty in cyberspace." In: *Data Politics,* editors Didier Bigo, Engin Isin, and Evelyn Ruppert, 81-99. London: Routledge.

Deibert, Ronald, and Rafal Rohozinski. 2010. "Risking Security: Policies and Paradoxes of Cyberspace Security." *International Political Sociology* 4 (1): 15–32.

Der Derian, James. 1994. "Cyber-Deterrence." *Wired Magazine*. September 1. https://www.wired.com/1994/09/cyber-deter/.

Dunn Cavelty, Myriam, and Andreas Wenger. 2020. "Cyber security meets security politics: Complex technology, fragmented politics, and networked science." *Contemporary Security Policy*, 41 (1): 5-32.

Dunn Cavelty, Myriam. 2013. "From cyber-bombs to political fallout: Threat representations with an impact in the cyber-security discourse." *International Studies Review* 15 (1): 105-122.

Egloff, Florian J., and Max Smeets. 2021. "Publicly attributing cyber attacks: a framework." *Journal of Strategic Studies*: 1-32.

Elgin, B., and M. Riley. 2014. "Now at the Sands Casino: An Iranian Hacker in Every Server." *Bloomberg,* December 12. https://www.bloomberg.com/news/articles/2014-12-11/iranian-hackers-hit-sheldon-adelsons-sands-casino-in-las-vegas.

Farwell, James and Rafal Rohozinski. 2011. "Stuxnet and the Future of Cyber War." *Survival*, 53 (1): 23-40.

Fischerkeller, Michael P., and Richard J. Harknett. 2017. "Deterrence is not a credible strategy for cyberspace." *Orbis* 61 (3): 381-393.

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

Fogleman, Ronald R. 1995. "Information operations: The fifth dimension of warfare." *Defense issues* 10 (47): 1-3.

Fuchs, Christian. 2012. "Some Reflections on Manuel Castells' Book 'Networks of Outrage and Hope. Social Movements in the Internet Age'." *tripleC: Communication, Capitalism & Critique. Open Access Journal for a Global Sustainable Information Society* 10 (2): 775-797.

Gerasimov, Valery. 2016. "The Value of Science in the Foresight." *Military Review*, January/February. https://www.armyupress.army.mil/portals/7/military-review/archives/english/militaryreview_20160228_art008.pdf.

Ghafur, Saira, Soren Kristensen, Kate Honeyford, Guy Martin, Ara Darzi, and Paul Aylin. 2019. "A retrospective impact analysis of the WannaCry cyberattack on the NHS." *NPJ digital medicine* 2 (1) (2019): 98.

Goldsmith, Jack, and Stuart Russell. 2018. "Strength Becomes Vulnerabilities." *Aegis Series Paper No. 1806*, The Hoover Institution.

Goodman, Will. 2010. "Cyber deterrence: Tougher in theory than in practice?" *Strategic Studies Quarterly* 4 (3): 102-135.

Greenberg, Andy. 2017. "How an entire nation became Russia's test lab for cyberwar." *Wired,* June 20. https://www.wired.com/story/russian-hackers-attack-ukraine/

Greenberg, Andy. 2018. "The untold story of NotPetya, the most devastating cyberattack in history." *Wired,* August 22. https://www.wired.com/story/notpetya-cyberattack ukraine-russia-code-crashed-the-world/.

Harknett, Richard, and Max Smeets. 2020. "Cyber campaigns and strategic outcomes." *Journal of Strategic Studies*, 45 (4): 534-567.

Healey, Jason. 2019. "The implications of persistent (and permanent) engagement in cyberspace." *Journal of Cybersecurity* 5 (1): 1-15.

Jacobsen, Jeppe T. "Cyber offense in NATO: challenges and opportunities." *International Affairs* 97, no. 3 (2021): 703-720.

Kaplan, Fred. 2016. *Dark territory: The secret history of cyber war*. New York: Simon and Schuster.

Kello, Lucas. 2013. "The meaning of the cyber revolution: Perils to theory and statecraft." *International Security* 38 (2): 7-40.

Khondker, Habibul Haque. 2011. “Role of the new media in the Arab Spring.” *Globalizations* 8 (5): 675-679.

Kollars, Nina. 2020. “Cyber Conflict as an Intelligence Competition in an Era of Open Innovation.” *Policy Roundtable: Cyber Conflict as an Intelligence Contest.* https://tnsr.org/roundtable/policy-roundtable-cyber-conflict-as-an-intelligence contest/.

Kostyuk, Nadiya, and Erik Gartzke. 2022. “Why Cyber Dogs Have Yet to Bark Loudly in Russia’s Invasion of Ukraine “ *Texas National Security Review*.

Kostyuk, Nadiya, and Yuri M. Zhukov. 2019. “Invisible digital front: Can cyber attacks shape battlefield events?” *Journal of Conflict Resolution* 63 (2): 317-347.

Landau, Susan. 2013. “Making sense from Snowden: What’s significant in the NSA surveillance revelations.” *IEEE Security & Privacy* 11 (4): 66-75.

Lindsay, John R. 2020. “Military Organizations, Intelligence Operations, and Information Technology.” *Policy Roundtable: Cyber Conflict as an Intelligence Contest*. https://tnsr.org/roundtable/policy-roundtable-cyber-conflict-as-an-intelligence-contest/

Lindsay, John R., Tai Ming Cheung, and Derek S. Reveron (eds). 2015. *China and cybersecurity: Espionage, strategy, and politics in the digital domain*. USA: Oxford University Press.

Lindsay, Jon. 2013. “Stuxnet and the Limits of Cyber Warfare.” *Security Studies,* 22(3): 365-404.

Lindsay, R. Jon. 2015. “The Impact of China on Cybersecurity: Fiction and Friction.” *International Security* 39 (3): 7-47.

Lipton, Eric, David E. Sanger, and Scott Shane. 2016. “The perfect weapon: How Russian cyberpower invaded the US.” *The New York Times*, December 13. https://www.nytimes.com/2016/12/13/us/politics/russia-hack-election-dnc.html.

Lynn III, William F. 2010. “Defending a new domain-the Pentagon’s cyberstrategy.” *Foreign Affairs* 89: 97-109.

Maness, Ryan C. 2021. “Death by a Thousand Cuts: Is Russia Winning the Information War with the West?” In: *European-Russian Power Relations in Turbulent Times*, edited by Mai’a K. Davis Cross and Ireneusz Paweł Karolewski, 160-186. Ann Arbour, Mi: the University of Michigan Press

Markoff, John. 2008. “Before the gunfire, cyberattacks.” *New York Times*, August 12. https://www.nytimes.com/2008/08/13/technology/13cyber.html.

McGuffin, Chris, and Paul Mitchell. 2014. "On Domains: Cyber and the Practice of Warfare." *International Journal* 69 (3): 394–412.

Morozov, Evgeny. 2011. *The dark side of Internet freedom: The net delusion*. New York: Public Affairs. 2011.

Mueller, Robert. 2019. *Report On The Investigation Into Russian Interference In The 2016 Presidential Election*. Washington, D.C.: Department of Justice.

Nagle, Angela. 2017. *Kill all normies: Online culture wars from 4chan and Tumblr to Trump and the alt-right*. UK: John Hunt Publishing.

Nakasone, Paul M. "A cyber force for persistent operations." *Joint force quarterly* 92 (1): 10-14.

Nocetti, Julien. 2015. "Contest and conquest: Russia and global internet governance." *International Affairs* 91 (1): 111-130.

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

Peterson, Dale. 2013. "Offensive Cyber Weapons: Construction, Development, and Employment." *Journal of Strategic Studies* 36 (1): 120-124.

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

Price, Monroe. 2017. "The global politics of Internet governance: A case study in closure and technological design." In: *Technology and World Politics,* edited by Daniel McCarthy, 126-145. London and New York: Routledge.

Reuters. 2021."Russia disconnects from internet in tests as it bolsters security - RBC daily." July 22. https://www.reuters.com/technology/russia-disconnected-global-internet-tests-rbc-daily-2021-07-22/.

Rid, Thomas, and Ben Buchanan. 2015. "Attributing cyber attacks." *Journal of Strategic Studies* 38 (1-2): 4-37.

Rovner, Joshua. 2020. "What is an Intelligence Contest?" *Texas National Security Review*, Fall: 114-120.

Shachtman, Noah. 2010. "Insiders Doubt 2008 Pentagon Hack Was Foreign Spy Attack (Updated)". *Wired,* August 25. https://www.wired.com/2010/08/insiders-doubt-2008-pentagon-hack-was-foreign-spy-attack/.

Sherman, Justin. 2021. "Reassessing RuNet: Russian Internet Isolation and Implications for Russian Cyber Behavior." *The Atlantic Council,* July 12. https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/

reassessing-runet-russian-internet-isolation-and-implications-for-russian-cyber-behavior/#executivesummary.

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

Singer, Peter Warren, and Emerson T. Brooking. *LikeWar: The weaponization of social media*. Boston: Eamon Dolan Books, 2018.

Slayton, Rebecca. 2016. "What is the cyber offense-defense balance? Conceptions, causes, and assessment." *International Security* 41 (3): 72-109.

Smeets, Max. 2022a. *No shortcuts: Why states struggle to develop a military cyber-force*. Oxford: Oxford University Press.

Smeets, Max. 2022b. "The Risks of Managing a Purchased Cyber Arsenal". *Blog Post by Max Smeets, Guest Contributor* May 31. https://www.cfr.org/blog/risks-managing-purchased-cyber-arsenal.

The Economist. 2010. "War in the fifth domain." July 3. https://www.economist.com/briefing/2010/07/01/war-in-the-fifth-domain.

The White House. 2003. *The national strategy to secure cyberspace*. Washington D.C.: The White House.

The White House. 2022. *National Security Strategy*. Washington D.C.: The White House.

The White House. 2023. *National Cybersecurity Strategy*. Washington D.C.: The White House.

Thomas Rid. 2012. "Cyber War Will Not Take Place." *Journal of Strategic Studies* 35 (1): 5-32.

U.S. National Institute of Standards and Technology. 2012. "*Information Security*." U.S. Department of Commerce. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf.

United States Department of Defense. 2011. *Department of Defense Strategy for Operating in Cyberspace*. Washington DC: DoD.

United States Department of Defense. 2018. *Department of Defense Cyber Strategy*. Washington DC: DoD.

United States Department of Defense. 2022. *National Defense Strategy*. Washington DC: DoD.

Vishwanath, Arun. 2022. *The Weakest Link: How to Diagnose, Detect, and Defend Users from Phishing*. Cambridge, MA: MIT Press.

Welch, Larry D. 2004. *Cyberspace-The fifth operational domain*. Alexandria, VA: Institute for Defense Analyses.

White, Geoff. 2021. "The Lazarus heist: How North Korea almost pulled off a billion-dollar hack." *BBC News*, June 21. https://www.bbc.com/news/stories-57520169.

Wilner, Alex. 2020. "US cyber deterrence: Practice guiding theory." *Journal of Strategic Studies* 43 (2): 245-280.

YouTube Help. 2023. "YouTube's Community Guidelines." *Google Support*. https://support.google.com/youtube/answer/9288567?hl=en.

Zeng, Jinghan, Tim Stevens, and Yaru Chen. 2017. "China's Solution to Global Cyber Governance: Unpacking the Domestic Discourse of 'Internet Sovereignty'." *Politics & Policy* 45 (3): 432-464.

Zetter, Kim. 2012. "Meet 'Flame,' The Massive Spy Malware Infiltrating Iranian Computers." W*ired*, May 28. https://www.wired.com/2012/05/flame/.

Miloš VUKELIĆ

CHARACTERISTICS OF CYBERSPACE AS A DISTINCT DOMAIN OF CONFLICT: A CASE STUDY OF U.S. STRATEGIC OPERATIONS

Abstract: In this paper, I intend to contribute to the systematic study of cyber strategies and policies by offering a synthesis of key events and findings on state actions in cyberspace after 2007. Such a synthesis implies tracing the processes that contributed to the beginning of the militarization of cyberspace from 2007 to 2013. Then, it implies defining the basic characteristics of cyberspace that determine the actions of states, among which are: the democratic character; high potential for human error; attribution problem; technical volatility; and time and speed constraints. Finally, the synthesis includes a concrete example of the influence of key characteristics on the strategic behavior of the USA. Based on the analysis of the strategic documents of the USA and the analysis of the previous behavior of this country, I argue that the theory of "persistent engagement", which in its construction considers the aforementioned characteristics, remains the backbone of the USA's behavior in cyberspace.

Keywords: Cyberspace, cyber domain, cyber strategy, cyber policy, cyber conflict, USA.