Pregledni naučni članak UDC 316.774(510)

Aleksandar Vranješ*
Fakultet političkih nauka
Univerzitet u Banjoj Luci

Internet suverenitet sa kineskim karakteristikama**

Apstrakt

Razvoj savremenih informaciono-komunikacionih tehnologija, kao i povećanje broja korisnika, pogodovalo je intenziviranju debate o upravljanju Internetom na međunarodnim forumima. S jedne strane, SAD insistiraju na "Multi-stakeholder Internet Governance" modelu, dok, s druge, Kina sve glasnije zagovara model „Internet suvereniteta" – multilateralni pristup u kojem bi sve države svijeta slobodno birale vlastiti put sajber razvoja, te nijedna država ne bi imala poziciju da primjenjuje sajber hegemoniju. Ovaj model je svakako naišao na kritiku na Zapadu, jer je označen kao platforma za jačanje kontrole i narušavanja građanskih sloboda. S druge strane, svjedoci smo da i određene zapadne države rade na uspostavljanju veće kontrole u vlastitom sajber prostoru, te je njihova kritika kineskog modela utoliko manje uvjerljiva. Sve u svemu, Kina kao prva „Internet suverena" država otišla je toliko daleko u domenu tehničkog i legislativnog unapređenja vlastitog sajber prostora, da je teško zamisliti da se postojeće stanje vrati na početne pozicije, posebno ako se uzme u obzir i rast političke i ekonomske moći ove mnogoljudne države. Skloniji smo zaključku da će u budućoj globalnoj debati o upravljanju Internetom argumenti biti sve više na kineskoj strani, te da je pred nama novo doba sajber suverenih država.

Ključne riječi:

Internet suverenitet, upravljanje Internetom, Kina, kontrola, nadzor

* aleksandar.vranjes@fpn.unibl.org

** Rad je proistekao iz autorove doktorske disertacije „Internet i razvoj ili ograničavanje slobode subjekata globalnog komuniciranja", odbranjene na Fakultetu političkih nauka Univerziteta u Beogradu.

UVOD

Razvojem savremenih informaciono-komunikacionih tehnologija (IKT) i povećanjem njihove dostupnosti širom svijeta došlo je do transformacije međunarodnog u globalno komuniciranje, a kao posebna karakteristika izdvaja se mogućnost da umreženi građani širom svijeta postanu subjekti ovog oblika komunikacione prakse. Akcenat se svakako stavlja na riječ „mogućnost" jer je važno naglasiti da nisu svi građani, kojima je Internet dostupan, ujedno i subjekti globalnog komuniciranja. Pored tehničko-tehnoloških pretpostavki i posjedovanja odgovarajućeg „gadžeta" za pristup Internetu, da bi se određeni umreženi građanin podrazumijevao kao subjekt ovog oblika komunikacione prakse, neophodno je da posjeduje i znanje, ideju, svijest, ali i potrebu odnosno motiv da komunicira u sajber prostoru, tj. preko granica svoje nacionalne države.[1] Ono što je takođe još jedna odlika globalnog komuniciranja jeste da države više nisu ekskluzivni subjekti koje uz transnacionalne kompanije, agencije i sl. jedino imaju mogućnost interakcije izvan vlastitih granica. Naravno, razvoj savremenih IKT i sve veći broj korisnika doprinijeli su ovakvom ishodu u kojem i građani dobijaju mogućnost da postanu globalni komunikatori. Ono što je važno za ovaj rad, spomenute transformacije u domenu međunarodnog/globalnog komuniciranja, možemo da objasnimo i kao posljedicu nestajanja komunikacionog suvereniteta, kojeg su moderne države izgubile mnogo prije pojave Interneta, da bi kasnije, pod uticajima globalizacijskih procesa, počele gubiti i ekonomski, vojni, finansijski, ekološki suverenitet.[2] Autori Stil i Štajn u tom kontekstu tvrde da je razvojem i dostupnošću novih IKT smanjena moć država, ali su zato njihovi stanovnici, kao i mediji, dobili mogućnost da dođu direktno i mnogo brže do traženih informacija.[3] Kada je riječ o sajber okruženju, savremene države doskora nisu ni imale prilike da uspostave komunikacioni suverenitet u ovom domenu, odnosno da ograniče vlastiti sajber prostor nad kojim će imati kontrolu. Ipak, razvoj i povećanje dostupnosti savremenih IKT, ali i sve većih rizika i izazova u sajber okruženju, dovelo je do toga da se ideja o Internet suverenitetu[4] sve jače čuje na međunarodnim forumima, pri čemu je Kina u tom daleko najglasnija.

---

1 Miroljub Radojković, Branimir Stojković, Aleksandar Vranješ, *Međunarodno komuniciranje u informacionom društvu*, Clio, Beograd, 2015, str. 141.

2 Isto.

3 Cherie Steele and Arthur A. Stein, "Communications Revolutions and International Relations" in: Juliann Emmons Allison (ed.), *Technology, Development and Democracy – International Conflict and Cooperation in the Information Age*, State University of New York Press, Albany, 2002, p. 35.

4 Kao sinonimi Internet suverenitetu, u literaturi se pronalaze još i varijacije: sajber, digitalni i virtuelni suverenitet, te će se i u ovom radu kao takvi koristiti.

UPRAVLJANJE INTERNETOM

Važno globalno pitanje koje se nametnulo u posljednjoj deceniji među vodećim državama svijeta jeste koji je budući najbolji model upravljanja Internetom. Svjetski samiti o informacionom društvu (WSIS), pod krovom Ujedinjenih nacija, pokazali su se neuspješni da odgovore na ovo pitanje, jer konsenzus nije postignut, a, u suštini, razlike među stavovima najvažnijih učesnika ove debate mogle bi se okarakterisati kao doktrinarne. Sjedinjene Američke Države, koje u određenom smislu smatraju da polažu pravo na Internet, zalažu se za tzv. "Multi-stakeholder Internet Governance" model ili, u slobodnom prevodu". Sistem upravljanja Internetom od strane više zainteresovanih strana"[5]. Osnovna odlika ovog koncepta jeste da se uspostavi sistem učestvovanja u dijalogu na osnovu kojeg bi se donosile odluke i rješenja u zajedničkom interesu, što je u suštini prihvatljivo državama Zapada. S druge strane, kritika navedenog modela upravljanja stigla je i od strane pojedinih autora sa Zapada koji smatraju da bi kroz ovaj model nekadašnji lobisti istih „zainteresovanih strana" sad bili učesnici u dijalogu sa pravom donošenja odluka, što svakako predstavlja manjkavost kompletnog koncepta.[6]

S druge strane, pored činjenice da je naklonjen interesima bivših klijenata, najveća kritika je došla od strane grupe država na čelu sa Kinom koje u ovom modelu vide dodatno uvećanje monopola SAD nad Internetom, koji bi se u konačnici trebalo posmatrati kao svjetsko opšte dobro. Kao alternativu predložili su koncept tzv. „Internet suvereniteta", posebno podstaknuti činjenicom da se čak i u preambuli Ustava Međunarodne telekomunikacione unije (ITU) navodi da se potpuno priznaje suvereno pravo svake države da reguliše vlastite telekomunikacije na svojoj teritoriji.[7] Takođe, dodatni argument za jačanje „Internet suvereniteta" pronašli su i u činjenici da je globalnoj javnosti postalo poznato da SAD imaju monopol i tehnička dostignuća pomoću kojih mogu da kontrolišu i nadziru kompletan Internet, što, na osnovu informacija Edvarda Snoudena, Džulijena Asanža i ostalih globalnih uzbunjivača, to i čine, te da je na taj način "Multi-stakeholder Internet Governance" model u suštini samo maska da najmoćnija država svijeta nastavi sa tom praksom.

---

5 Predstavnici vlada, privatni sektor, tehnička i akademska zajednica, civilno društvo itd.

6 Mike Gurstein, *Multistakeholderism vs. Democracy: My Adventures in 'Stakeholderland'*, Web blog post, 2013. Available from: https://gurstein.wordpress.com/2013/03/20/multistakeholderism-vs-democracy-my-adventures-in-stakeholderland (Accessed 8 December 2017).

7 International Telecommunication Union, *Collection of the basic texts adopted by the Plenipotentiary Conference*, 2015. Available from: http://search.itu.int/history/HistoryDigitalCollectionDocLibrary/5.21.61.en.100.pdf (Accessed 8 December 2017).

Autorka Andrea Limbago ističe da rast broja inicijativa za sajber suverenitetom u 2016. godini nije ograničen samo na određene države, i to Kinu, Rusiju, Iran i Sjevernu Koreju, nego je u pitanju globalni fenomen, a kao primjere navodi[8]:

1) Turski predsjednik Redžep Tajip Erdogan pozvao je pristalice posredstvom društvenih mreža da izađu na ulice i protestuju zbog pokušaja puča u julu 2016. godine, što je interesantan primjer ako se uzme u obzir da je u Turskoj bila na snazi zabrana određenih društvenih mreža, kao i cenzura na Internetu;
2) Suočena sa jednom od najgorih suša u posljednjih 50 godina, vlada Etiopije je ugasila niz Internet servisa širom zemlje, kako bi time spriječila buduće proteste, ali i dijeljenje informacija tokom održanih protesta, kao što je bio u Oromiji;
3) Cenzure društvenih mreža u Jugoistočnoj Aziji – Vijetnam je blokirao Fejsbuk u maju 2016. godine, da bi mogao staviti pod kontrolu proteste zbog narušavanja životne sredine prouzrokovanih otpadom iz fabrike čelika. Indonezija je usvojila 2014. godine Zakon kojim promoviše „bezbjedno i zdravo korišćenje Interneta", a na osnovu kojeg je 2016. godine blokirala dva radikalna i teroristička veb sajta, ali i društvene mreže, kao što je Tambler i video servis Netfliks. Telekomunikaciona regulatorna komisija Bangladeša naredila je blokiranje 35 medijskih sajtova i društvenih mreža, što je dovelo do potpunog gašenja Interneta.

U tekstu „Sajber suverenitet mora da vlada globalnim Internetom" autor Vej Lu (Wei Lu), direktor kineske „Državne kancelarije za informacije o Internetu" koja je sastavni dio institucije „Uprava za sajber prostor Kine", navodi da je sajber suverenitet osnova budućih dobrih odnosa između Kine i SAD, jer nikada ranije ove dvije države nisu bile toliko usko povezane kao što su postale u sajber prostoru.[9] Navodeći ekonomske pokazatelje, Lu je naglasio da skoro sve vodeće američke Internet kompanije ostvaruju ogroman profit u Kini. Kao primjer navodi činjenicu da polovina svih novih korisnika Epl (Apple) proizvoda dolazi upravo iz Kine, na hiljade američkih investicionih fondova odredili su Kinu kao prioritet s ciljem da se dođe do svakog zapećka kineskog Internet tržišta. S druge strane, SAD su jedno od najvećih tržišta kineskih Internet

---

8 Andrea Limbago, *The global push for cyber sovereignty is the beginning of cyber fascism*, The Hill, 2016. Available from: http://thehill.com/blogs/congress-blog/technology/310382-the-global-push-for-cyber-sovereignty-is-the-beginning-of (Accessed 8 December 2017).

9 Wei Lu, *Cyber Sovereignty Must Rule Global Internet*, Huffington Post, 2014. Available from: http://www.huffingtonpost.com/lu-wei/china-cyber-sovereignty_b_6324060.html (Accessed 8 December 2017).

kompanija, sa kompletnim prometom od oko petstotina milijardi dolara. Upravo zbog produbljenih ekonomskih odnosa i bližih kontakata ovih Internet industrija, Lu ističe da je primjetan porast neslaganja između dvije države, posebno kada je riječ o pitanjima iz domena upravljanja sajber prostorom.[10]

POVRATAK KOMUNIKACIONOG SUVERENITETA?

Osnovna razlika između američkog i kineskog modela upravljanja Internetom je suštinski nepomirljiva jer proizlazi iz dva različita poimanja uloge tih država na globalnom planu. Kao što je već rečeno, SAD se zalažu za upravljanje Internetom po principu više zainteresovanih strana po kome bi, bar deklarativno, svi akteri na ravnopravnoj osnovi donosili pravila upravljanja „mrežom svih mreža". Dok Kina, s druge strane, zagovara multilateralni princip, po kome bi države donosile pravila zasnovana prvenstveno na svom suverenitetu jer predstavljaju svoje građane. Drugim riječima, ako su države ustavno odgovorne za svoje građane u realnom okruženju, taj isti model bi se morao primjeniti i u sajber prostoru.

Lu smatra da ova dva alternativna pristupa ipak nisu suštinski kontradiktorna, jer su međusobno prepletena. On smatra da bi povećanje nesuglasica između dvije države dalje štetilo i Kini i SAD, ali i razvoju Interneta. U daljem tekstu Lu ističe da je Kina svjesna da je Internet nastao u SAD, što je ogroman doprinos ljudskom razvoju, ali kako Kina danas predstavlja najveće Internet tržište, ona ima pravo da predloži jačanje međusobnog uvažavanja, a ne konfrontacije.[11] Isti autor ističe da bi sve zemlje svijeta, bile one velike ili male, trebalo da budu ravnopravne i da svaka treba da poštuje sajber suverenitet druge države.

S druge strane, bivši savjetnik pri Ujedinjenim nacijama Skot Malkomson (Scott Malcomson) vidi zalaganje za uspostavljanjem sajber suvereniteta isključivo kao napor Kine i Rusije da svoje građane drže podalje od stranih fondacija, ideologija i nezavisnog novinarstva.[12] Problem u ovom stanovištu je u tome što se kineska strategija razvoja sajber suvereniteta posmatra isključivo kroz prizmu američke političke doktrine „Internet slobode"[13]. Konačno, Kina

---

10 Wei Lu, *Cyber Sovereignty Must Rule Global Internet*, op. cit.

11 Ibid.

12 Scott Malcomson, *How Russia and China Are Cooperating to Dismantle America's Dominance of the Internet*, Huffington Post, 2016. Available from: http://www.huffingtonpost.com/scott-malcomson/russia-china-internet_b_9841670.html (Accessed 7 December 2017).

13 Doktrina 'Internet sloboda' se posmatrala kao jedan od prioriteta u američkoj spoljnoj politici 2010. godine, zagovarana od strane tadašnje državne sekretarke

ima pravo da zabrani sve onlajn aktivnosti na svojoj teritoriji koje bi mogle dovesti do potencijalne, fabrikovane „obojene revolucije" kao konkretan napad na državni suverenitet ove mnogoljudne države. Naposlijetku, postavlja se hipotetičko pitanje kako bi se SAD ili neka druga velika i razvijena država postavila po ovom pitanju da im putem Interneta prijete njihovom ustavnom poretku? Pretpostavljeni odgovor je da bi reagovale na sličan način, jer svaka država prvenstveno štiti svoje interese. Tako smo bili svjedoci da je koalicija razvijenih zapadnih država pokrenula ratove na Bliskom istoku zarad zaštite vlastitog suvereniteta i bezbijednosti svojih građana. Dakle, odgovor kako bi se ponašale u sajber prostoru da im ustavni poredak bude ugrožen od strane druge tehnološki visokorazvijene države je više nego logičan. Ono što se zanemaruje jeste da i određene države zapadnog bloka povećavaju svoje kapacitete i propise u domenu kontrole Internet aktivnosti, što bi se takođe moglo smatrati kao razvoj u pravcu sajber suvereniteta. Iako te države zvanično ne bi potvrdile našu konstataciju, ipak određene sprovedene mjere idu u prilog prethodnom zaključku.

Prvi primjer je Zakon o istražnim ovlašćenjima ("Investigatory Powers Act 2016 c. 25") u Velikoj Britaniji, koji je stupio na snagu 30. 12. 2016. godine, čime je omogućeno proširenje ovlašćenja britanske obavještajne zajednice. Novi zakon se odnosi na pravo istražnih organa da presreću komunikacije, te prikupljaju i zadržavaju podatke i ostale informacije.[14] Autor Glin Mudi (Glyn Moody) u tekstu pod nazivom „Zašto je 'Zakon o istražnim ovlašćenjima' katastrofa po privatnost koja tek treba da se desi" ističe da novi zakon omogućava pristup dokumentaciji o svim Internet aktivnostima korisnika.[15] Internet servis provajderi i telekom operatori na teritoriji Velike Britanije biće dužni da kreiraju evidenciju o korišćenju Interneta za sve svoje korisnike i biće u obavezi da te metapodatke čuvaju godinu dana. Takođe, odredbe ovog zakona omogućavaju bezbjedonosnim službama i policiji pristup računarima i mobilnim telefonima građana, da bi prikupili podatke.[16] Policijski službenici, prema ovom zakonu, neće imati obavezu da traže nalog od suda da bi imali

---

Hilari Klinton, kao napor da se onlajn komuniciranje promoviše kao alat za „otvaranje zatvorenih društava", što je podrazumijevalo i finansijska ulaganja u pomoć subjektima globalnog komuniciranja (blogerima, disidentima, aktivistima..) da se bore sa cenzurom u Kini, Iranu, Mjanmaru, itd.

14 *Investigatory Powers Act 2016*, Parliament UK, 2016. Available from: http://services.parliament.uk/bills/2015-16/investigatorypowers.html (Accessed 7 December 2017).

15 Glyn Moody, *Why the Investigatory Powers Act is a privacy disaster waiting to happen*, Ars Technica UK, 2016. Available from: https://arstechnica.co.uk/tech-policy/2016/11/investigatory-powers-act-privacy-disaster-waiting-to-happen (Accessed 8 December 2017).

16 Alan Travis, 'Snooper's charter' bill becomes law, extending UK state surveillance, The Guardian, 2016. Available from: https://www.theguardian.com/world/2016/

pristup podacima, nego samo odobrenje nadređenog lica u bezbjedonosnim službama.[17] Kao argument da ovim neće doći do zloupotreba, iz policije naglašavaju da bi složena birokratija u procesu dobijanja odobrenja za pristup podacima trebalo da spriječi eventualna prekoračenja ovlašćenja.[18]

Po pitanju novog britanskog zakona oglasio se i Amnesti Internešenel (Amnesty International), koji u svom izvještaju navodi da je ovaj zakon ozbiljna prijetnja za privatnost i ostala ljudska prava u Velikoj Britaniji ali i šire.[19] Kako se navodi, Zakon institucionalizuje veoma visoka ovlašćenja nadzora, počevši od presretanja gomile informacija, do samog pristupa ličnim podacima. Ono što takođe iz Amnesti Internešenela ističu, ovaj zakon ne zahtjeva postojanje razumne sumnje da je određena osoba počinilac ili tek planira da počini krivično djelo, da bi se izvršio nadzor ili pristup podacima, što je u protivnom sa ljudskim pravima, prvenstveno sa pretpostavkom nevinosti.[20]

Naredna aktivnost Velike Britanije koju možemo okarakterisati kao put ka učvršćivanju kontrole na Internetu jeste aktivnost parlamentarne Pravne komisije (engl. "Law Commission")[21], koju je angažovala britanska Vlada, čiji je zadatak da reformiše zakone o službenim tajnama.[22] Upravo ova Komisija je početkom 2017. godine objavila dokument, odnosno preporuke kojim se predlažu mjere za unapređenje postojećih zakona. U preporukama se navodi da je potrebno uvesti krivično gonjenje svakog pojedinca koji objavi tajnu obavještajnu ili spoljnopolitičku činjenicu zasnovanu na curenju informacija.[23]

---

nov/29/snoopers-charter-bill-becomes-law-extending-uk-state-surveillance (Accessed 8 December 2017).

17 Glyn Moody, *Why the Investigatory Powers Act is a privacy disaster waiting to happen*, op. cit.

18 Ibid.

19 *Dangerously disproportionate – The ever-expanding National Security State in Europe*, Amnesty International, 2017. Available from: https://www.amnesty.org/download/Documents/EUR0153422017ENGLISH.PDF (Accessed 8 December 2017).

20 Ibid.

21 U pitanju je nepolitičko nezavisno tjelo koje je 1965. godine osnovao britanski Parlament s ciljem da prate implementaciju zakona i da predlažu reforme. Od osnivanja do danas 73% predloženih preporuka od strane ove Komisije Vlada Velike Britanije je usvojila i implementirala u pravcu reformi, bilo u cjelini ili samo u dijelu.

22 Ljiljana Vujić, *Udar Londona na novinare i uzbunjivače*, Politika, Beograd. 2017. Dostupno preko: http://www.politika.rs/sr/clanak/374220/Udar-Londona-na-novinare-i-uzbunjivace (Pristupljeno 09. decembra 2017).

23 Ljiljana Vujić, *Udar Londona na novinare i uzbunjivače*, Politika, Beograd. 2017. Dostupno preko: http://www.politika.rs/sr/clanak/374220/Udar-Londona-na-novinare-i-uzbunjivace (Pristupljeno 09. decembra 2017).

Drugim riječima, svaki novinar ili uzbunjivač bi ubuduće mogao završiti u zatvoru kao špijun u slučaju da objavi dokumente, kao što je to učinio npr. Edvard Snouden u SAD. Prema ovom prijedlogu, obavještajci i državni službenici koji bi stavili tajne dokumente na dispoziciju javnosti mogli bi da dobiju četrnaest godina zatvorske kazne.[24]

U isto vrijeme i zvaničnici koji bi omogućili da „procure" osjetljive informacije, čime bi se narušila nacionalna bezbjednost, takođe bi mogli da završe u zatvoru. Ovaj prijedlog sadrži i mjere protiv stranaca koji bi u inostranstvu objavili informacije koje štete britanskoj nacionalnoj bezbjednosti, te bi se i njima sudilo pred britanskim sudovima, što je svakako novina.[25] Važno je istaći i da Komisija predlaže i da se iz zakona izbrišu anahronizmi koji opisuju tajne podatke kao što su: nacrti, planovi, modeli, lozinke, kodne riječi i da se zamjene jednim generičkim izrazom – informacija. Takođe, oni predlažu i da se stari Zakoni o službenim tajnama (The Official Secrets Acts) iz 1911, 1920. i 1939. godine zamjene modernizovanim Zakonom o špijunaži.

Na kraju, važno je istaći i da se ovim dokumentom predlaže da ubuduće tužioci nemaju potrebu da dokazuju postojanje i obim štete po nacionalnu bezbjednost koju je pojedinac počinio samim tim što je objavio ili omogućio da „procuri" tajna informacija.[26] Konačno, u kontekstu navedenih preporuka, pojedinac je počinio krivično djelo ako je znao ili imao razumne osnove da vjeruje da je njegovo postupanje omogućilo korist stranoj sili. Po ovom prijedlogu izjasnila se i britanska Vlada, koja je saopštila da podržavaju važan rad koji Komisija obavlja na zahtjev Vlade, te da taj posao još nije završen i ne mogu još uvijek dati svoj konačni sud po ovom pitanju. Kada Komisija završi posao tokom 2017. godine, na osnovu njihovih preporuka Vlada će sačiniti nacrt zakona kojeg će poslati u parlamentarnu proceduru.[27]

Za nas je važan ovaj primjer jer pokazuje da Velika Britanija korača prema jačanju svoje pozicije u domenu uređivanja vlastitog sajber prostora. Takođe, primjetno je i da ova država ostaje u određenom smislu van fokusa kritika kada je riječ o navedenim aktivnostima, ali i tajnim programima za

---

24 Christopher Hope, *Exclusive Spies and civil servants who leak secrets face 14 years in jail in first overhaul of the Official Secrets Act for 100 years*, The Telegraph, 2017. Available from: http://www.telegraph.co.uk/news/2017/02/02/exclusive-spies-civil-servants-leak-secrets-face-14-years-jail/ (Accessed 10 December 2017).

25 Ibid.

26 Ibid.

27 Ibid.

nadzor. Zaboravlja se da je i Britanija dio koalicije "Five Eyes"[28] koja vrši tajne operacije nadzora narušavajući time privatnost globalnih umreženih građana, a što je otkrio uzbunjivač Edvard Snouden. Dakle, zvanično, Velika Britanija je protiv kineskog modela „sajber suvereniteta", a nezvanično, u arkanskim sferama unutrašnje politike i te kako pojačava svoje kapacitete kada je riječ o kontroli i intervencijama države u sajber prostoru.

Primjer, ali u drugačijem kontekstu, imamo u SAD, u kojima savezne države pokušavaju da se „odbrane" od odluka višeg, federalnog nivoa. Tako, kao odgovor na Snoudenovo uzbunjivanje, imamo zanimljivu reakciju Kalifornije. Krajem 2015. godine guverner ove države Džeri Braun (Jerry Brown) potpisao je novi zakon pod nazivom „Zakon o privatnosti elektronskih komunikacija" (engl. "Electronic Communications Privacy Act"), koji je stupio na snagu 1. januara 2016. godine. Prema ovom zakonu, nijedna agencija niti lice koje vrši istragu na teritoriji Kalifornije ne mogu da vrše nadzor ili prikupljanje informacija koje nastaju posredstvom elektronskih komunikacija bez prethodno pribavljenog sudskog naloga. To uključuje i praćenje lokacija elektronskih uređaja kao što su mobilni telefoni i sl. Prema autorki Kim Zeter (Kim Zetter), ovo je najkompletniji zakon u ovom domenu u SAD i trebalo bi da bude uzor ostalim saveznim državama kada je reč o zaštiti ljudskih prava građana u sajber prostoru.[29] Pored Kalifornije, još pet saveznih država su donijele zakon koji se odnosi na obavezu da istražni organi pribave sudski nalog kada je riječ o prikupljanju sadržaja, dok još devet država imaju sličan zakon ali on se odnosi na zaštitu lociranja posredstvom satelita. Od svih ovih primjera jedino je kalifornijski zakon cjelovit i podrazumijeva pod elektronskim komunikacijama: lokacijske podatke, sadržaje, metapodatke i pretragu samih uređaja.[30] Ovaj primjer bi se mogao shvatiti kao otpor saveznih država SAD od aktivnosti federalnog nivoa u domenu nadzora, te bismo ga uslovno mogli označiti kao intenciju da savezne države u SAD ostvare izvjesan nivo sajber suverenosti, u odnosu na federalni nivo.

Dakle, bez obzira na negativne reakcije država Zapadnog bloka i kritike sa pozivanjem na ljudska prava, slobodu govora, razvoja civilnog društva, slobode protoka informacija i mnogih drugih, određen broj država se kreće u pravcu razvoja sajber suvereniteta, bez obzira što rizikuju da budu stavljene u „isti koš" sa Kinom, tj. označene kao države sa manjkom Internet sloboda odnosno, kolokvijalno rečeno, kao „sajber totalitarne" države.

---

28 Obavještajna koalicija koju, pored Velike Britanije, čine još i Australija, Novi Zeland, Kanada i, naravno, Sjedinjene Američke Države kao predvodnica.

29 Kim Zetter, *California Now Has the Nation's Best Digital Privacy Law*, The Wired, 2015. Available from: https://www.wired.com/2015/10/california-now-nations-best-digital-privacy-law (Accessed 10 December 2017).

30 Ibid.

Tako je npr. u Brazilu u novembru 2013. godine (neposredno nakon Snoudenovog uzbunjivanja), na prijedlog tadašnje predsednice Dilme Rusef (Dilma Vana Rousseff), podnesen amandman na brazilski okvirni Zakon o civilnim pravima na Internetu (Por. „Marco Civil da Internet"). Njime se zahtjeva da strani provajderi tzv. "klaud servisa" čuvaju sve informacije nastale, odnosno kreirane na teritoriji Brazila, isključivo na serverima koji su fizički smješteni u ovoj državi. Takođe, svi provajderi koji rade na teritoriji ove države dužni su da se pridržavaju brazilskog zakona.[31] Sličnu reakciju imamo i u Rusiji, gdje je u Državnoj dumi u julu 2014. godine usvojen zakon koji je inspirisan brazilskim zakonom o civilnim pravima na Internetu, u kome se takođe propisuje da se svi podaci prikupljeni sa teritorije Ruske Federacije moraju čuvati na serverima smještenim isključivo na teritoriji ove države.[32] Kao prvi primjer nepoštovanja navedenog ruskog zakona imamo slučaj društvene mreže *Linktin* („LinkedIn"), koja je blokirana u Rusiji krajem 2016. godine nakon što je utvrđeno da su prekršene odredbe zakona o čuvanju podataka.[33] Kako se mreža *Linktin* nije pridržavala odredbi ovog zakona, svim Internet provajderima u Rusiji naloženo je da ukinu pristup stranicama ove mreže koja u ovoj državi ima oko šest miliona korisnika.

Kada je riječ o Njemačkoj, Savezni parlament je usvojio zakon 2016. godine koji zahtjeva od telekomunikacionih kompanija da čuvaju privatne podatke korisnika do 10 nedelja, tj. da toliko dugo budu agencijama na dispoziciji nakon čega mogu da ih obrišu, bez obzira što je Evropski sud pravde ranije odbio sličnu direktivu Evropske unije.[34] Takođe, Savezno tužilaštvo Njemačke obavijestilo je uredništvo portala "Netzpolitik.org" da su njihova dva novinara bili pod istragom zbog izdaje jer su navodno objavili tekstove koji sadrže povjerljive državne informacije. Bez obzira što je slučaj brzo zatvoren, ipak

---

31 Dana Polatin-Reuben, Joss Wright, *An Internet with BRICS Characteristics: Data Sovereignty and the Balkanisation of the Internet*, 4th USENIX Workshop on Free and Open Communications on the Internet, 2014. Available from: https://www.usenix.org/system/files/conference/foci14/foci14-polatin-reuben.pdf (Accessed 10 December 2017), p.3.

32 Ibid.

33 Ankica Marinković, *Rusija blokirala društvenu mrežu „Linktin"*, Politika, 2016. Dostupno preko: http://www.politika.rs/sr/clanak/368039/Spektar/Digitalni-svet/Rusija-blokirala-drustvenu-mrezu-Linktin (Pristupljeno 10. decembra 2017).

34 Sanja Kelly, Mai Truong, Adrian Shahbaz and Madeline Earp, *Silencing the Messenger: Communication Apps under Pressure – Freedom on the Net 2016 – Annual report*, Freedomhouse, 2016. Available from: https://freedomhouse.org/report/freedom-net/freedom-net-2016 (Accessed 10 December 2017).

je privukao ogromnu pažnju ali i kritiku javnosti.[35] Kada je riječ o naporima Njemačke u pravcu učvršćivanja vlastitog sajber suvereniteta, nije zgoreg da napomenemo da se u aprilu 2017. godine pred Bundestagom našao prijedlog zakona koji bi trebalo da zabrani govor mržnje i izmišljene vijesti na Internetu, a društvene mreže koje ne otklone dovoljno brzo nedozvoljene sadržaje biće kažnjene kaznom i do pedeset miliona evra.[36] Kritičari ovog prijedloga zakona tvrde da se ovim ograničava sloboda govora i da se time preduzima kontrola sadržaja na društvenim mrežama, počevši od lažnih vijesti do anonimnih komentara.[37] U slučaju da se ovaj zakon usvoji, sve objave na društvenim mrežama koje sadrže lažne vijesti, govor mržnje, podsticanje na terorizam ili promociju dječije pornografije biće sankcionisane na teritoriji Njemačke. Na kraju, ovde se otvara pitanje da li ovaj zakon može da uspostavi granicu između potrebe za uklanjanjem spornih sadržaja i cenzure, odnosno da li će se društvene mreže na teritoriji Njemačke, u namjeri da izbjegnu velike kazne, pretvoriti u određen vid tajne državne policije, što dodatno zabrinjava kada posmatramo ovaj problem iz ugla ljudskih prava.

Na kraju, svi navedeni primjeri dokazi su da pojedine zapadne države jačaju svoj komunikacioni suverenitet posebno u sajber prostoru, a ako tome pridodamo i globalni nadzor na Internetu od strane SAD, koji je razotkrio Snouden, svakako možemo da zaključimo da ne stoje kritike sa Zapada na račun Kine i njenog koncepta Internet suvereniteta.

KINA KAO SAJBER-SUVERENA DRŽAVA

Ako uzmemo u obzir saznanja koja u ovom trenutku posjedujemo, slobodno možemo iskazati tvrdnju da je Kina danas jedina sajber-suverena država na svijetu. Ali prije nego što pređemo na razmatranje premisa na osnovu kojih smo izveli ovaj zaključak, osvrnućemo se na kratku istoriju razvoja Interneta u Kini.

Prva imejl poruka koja je prešla veliki Kineski zid u pravcu međunarodne akademske mreže davne 1987. godine napisana je preko prve kompjuterske

---

35 Sanja Kelly, Mai Truong, Adrian Shahbaz and Madeline Earp, *Silencing the Messenger: Communication Apps under Pressure – Freedom on the Net 2016 – Annual report*, Freedomhouse, 2016. Available from: https://freedomhouse.org/report/freedom-net/freedom-net-2016 (Accessed 10 December 2017).

36 *Bundestag zabranjuje govor mržnje i izmišljene vesti*, Politika, 2017. Dostupno preko: http://www.politika.rs/sr/clanak/377889/Bundestag-zabranjuje-govor-mrznje-i-izmisljene-vesti (Pristupljeno 10. decembra 2017).

37 Isto.

mreže u Kini pod nazivom „Kineska akademska mreža" (CANET)[38]. Ona je počela sa radom iste godine, omogućavajući korisnicima (istraživačima) da razmjenjuju podatke, imejl poruke i sl.[39] Kako ističe Dejvid Herold, Internet se u Kini razvijao paralelno sa Evropom i Amerikom, ali njegova struktura i način umrežavanja su se prilično razlikovali, iz razloga što su krajem osamdesetih i početkom devedesetih godina prvo povezane intranet mreže akademskih institucija Kine.[40]

Nakon CANET-a, osnivane su mreže kao što su Kineska obrazovna i istraživačka mreža (CERNET), mreža Instituta za visokoenergetsku fiziku (IHEP) i druge. Ali, one nisu imale „izlaz" na Internet kao globalnu mrežu.[41] Veza sa Internetom uspostavljena je onog trenutka kada se institucija doslovnog prevoda „Nacionalna računarska infrastruktura Kine" (NCFC) direktno povezala na Internet posredstvom strane telekom kompanije „Sprint korporacija" 1994. godine.[42] U maju 1995. godine „Kineska javna kompjuterska mreža" (Chinanet) počela je da izgrađuje mrežnu infrastrukturu širom države, da bi u januaru 1996. otvorila komercijalni Internet servis prema svim građanima. Od tada do danas, država i državna preduzeća su vlasnici fizičkih linkova koje obezbjeđuju Internet u Kini, a privatni provajderi imaju samo mogućnost da ih iznajme, nikako da obezbjede vlastite.[43] U tome je i glavna razlika u odnosu na evropske zemlje i SAD, jer, kako objašnjava Herold, zapadne vlade bi morale da donesu zakone kako bi stekle pravo kontrole Interneta, dok je, nasuprot tome, u Kini to bila polazna osnova.[44] Odnosno, država posjeduje infrastrukturu i daje je u najam, tako da automatski ima i kontrolu nad njom, što je svakako specifičnost Interneta u Kini.

---

38 Miroljub Radojković, Branimir Stojković, Aleksandar Vranješ, *Međunarodno komuniciranje u informacionom društvu*, nav. delo, str. 172.

39 Fengshu Liu, *Urban Youth in China: Modernity, the Internet and the Self*, Routledge, London, 2010, p. 35.

40 David Kurt Herold, "Noise, spectacle, politics: carnival in Chinese cyberspace" in: David Kurt Herold, Peter Marolt (ed.), *Online Society in China – Creating, celebrating, and instrumentalising the online carnival*, Routledge, London, 2011, p. 1.

41 Miroljub Radojković, Branimir Stojković, Aleksandar Vranješ, *Međunarodno komuniciranje u informacionom društvu*, nav. delo, str. 172.

42 Fengshu Liu, *Urban Youth in China: Modernity, the Internet and the Self*, op. cit.

43 Miroljub Radojković, Branimir Stojković, Aleksandar Vranješ, *Međunarodno komuniciranje u informacionom društvu*, nav. delo, str. 173.

44 David Kurt Herold, "Noise, spectacle, politics: carnival in Chinese cyberspace" in: David Kurt Herold, Peter Marolt (ed.), *Online Society in China – Creating, celebrating, and instrumentalising the online carnival*, op. cit., p. 2.

Prema statističkim podacima „Kineskog Internet informacijskog centra" (CNNIC), krajem 1997. godine Kina je imala oko 620.000 korisnika Interneta; do kraja naredne godine broj je porastao na 2.100.000; u 2005. godini bilo ih je oko 111.000.000, a tokom 2009. ovaj broj se popeo na 384.000.000 korisnika.[45] Čen tvrdi da je u 2014. godini preko šeststotina miliona Kineza imalo pristup Internetu posredstvom različitih digitalnih medija.[46] Prema autorima Fu i Čau, više od polovine kineskih građana u 2013. godini još uvijek nije koristilo Internet, a, analizirajući korisnike, autori navode da su u pitanju bolje obrazovani, finansijski obezbjeđeni građani iz urbanih krajeva koji pripadaju srednjoj klasi.[47] Prema posljednjim podacima kojim raspolažemo, u 2016. godini u Kini je registrovano 721.434.547 korisnika Interneta, što iznosi 52.2% ukupne populacije države, odnosno 21.1% od ukupnog broja svih korisnika Interneta na globalnom nivou.[48]

Prema Liu, već od 1995. godine, kada je Kina počela sa izgradnjom nacionalne mreže, usvojen je čitav niz veoma strogih pravila namenjenih provajderima, Internet kafeima, ali i samim korisnicima.[49] Kasnije je ozakonjena regulativa u vezi sa pitanjima državne tajne, onlajn biznisa, informacijskih i novinskih servisa, kao i bezbjednosti na Internetu.[50]

Sadržaji koji su zabranjeni na osnovu tadašnje Internet regulative su[51]:

1) Informacije usmjerene protiv osnovnih ustavnih načela;
2) One koje ugrožavaju nacionalnu bezbjednost, otkrivaju državne tajne, potkopavaju državni suverenitet i ugrožavaju nacionalno jedinstvo;
3) Informacije koje su usmjerene protiv nacionalnog digniteta i interesa;
4) One koje izazivaju mržnju i diskriminaciju između nacija i koje povređuju njihovu solidarnost;

---

45 Fengshu Liu, *Urban Youth in China: Modernity, the Internet and the Self*, op. cit., p. 36.

46 Wenhong Chen, "Taking stock, moving forward: the Internet, social networks and civic engagement in Chinese societies", *Information, Communication & Society*, 17:1. 1–6, Routledge, London, 2014, p. 1.

47 King-wa Fu, Michael Chau, *Reality check for the Chinese microblog space: A random sampling approach*, PloS One, Vol.8(3), 2013. Available from: http://www.plosone.org/article/info%3Adoi%2F10.1371%2Fjournal.pone.0058356, (Accessed 10 December 2017).

48 *China Internet Users*, Internet Live Stats, 2016. Available from: http://www.internetlivestats.com/internet-users/china/ (Accessed 10 December 2017).

49 Fengshu Liu, *Urban Youth in China: Modernity, the Internet and the Self*, op. cit., p. 38.

50 Miroljub Radojković, Branimir Stojković, Aleksandar Vranješ, *Međunarodno komuniciranje u informacionom društvu*, nav. delo, 173.

51 Yongming Zhou, *Historicizing online politics: Telegraphy, the Internet, and political participation in China*, Stanford University Press, Palo Alto, 2006, p. 142.

5) Informacije koje podrivaju državnu politiku o religiji i promovišu sekte i feudalno sujeverje;
6) One koje šire glasine, dovode u pitanje društveni poredak i ugrožavaju društvenu stabilnost;
7) Informacije koje su nepristojne i pornografske, ili promovišu kockanje, nasilje, ubistva i terorizam;
8) Zabranjene su klevete i informacije koje ugrožavaju prava drugih;
9) I sve ono što je inače zabranjeno zakonom i administrativnim propisima.[52]

Liu navodi da postoji najmanje dvanaest vladinih agencija širom zemlje koje formiraju nadzornu i kontrolnu piramidu, a koje su uključene u implementaciju Internet regulative u Kini.[53] Prema izvještaju kreiranom za potrebe američkog Kongresa, da bi se navedena Internet regulativa sprovela, Kina je osnovala tzv. „sajber policiju" u sklopu Ministarstva za javnu bezbjednost, koja, pored poslova istrage „onlajn krivičnih djela", nadzire sajtove, imejl poruke i uklanja nezakonite i subverzivne materijale.[54]

Čen smatra da se na Internet u Kini reflektuje veliki broj kontradikcija u društvu, od značajnog ekonomskog rasta koji izaziva socijalne nejednakosti, pa do navodne relativne ekonomske slobode koja živi uz striktnu političku kontrolu.[55] Herold opet tvrdi da kineska vlada nije toliko restriktivna i da dozvoljava dosta slobode korisnicima Interneta, ali ima mogućnost da ga ograniči, čak i zabrani.[56] Dobar primjer za to bili su nemiri muslimanskih Ujgura tokom ljeta 2009. godine. Tada je vlada Kine prvo ugasila Internet u provinciji Sinjang (Xinjiang) na sjeverozapadu Kine, da bi zatim dozvolila pristup njegovoj veoma ograničenoj verziji, prije vraćanja sistema u „normalu" u maju 2010. godine.[57]

S druge strane, zanimljivo je posmatrati kako razvijene zemlje zapadne civilizacije ocjenjuju praksu Kine kroz vlastite poglede koji uglavnom ističu demokratski potencijal Interneta, a da pri tom nisu dovoljno kritički preispitale

---

52 Yongming Zhou, *Historicizing online politics: Telegraphy, the Internet, and political participation in China*, Stanford University Press, Palo Alto, 2006, p. 142.

53 Fengshu Liu, *Urban Youth in China: Modernity, the Internet and the Self*, op. cit., p. 39.

54 Thomas Lum, "Internet development and information control in the People's Republic of China", *CRS report for Congress*, Library of Congress, Washington, 2006.

55 Wenhong Chen, "Taking stock, moving forward: the Internet, social networks and civic engagement in Chinese societies", *Information, Communication & Society*, 17:1. 1–6, Routledge, London, 2014, p. 4.

56 David Kurt Herold, "Noise, spectacle, politics: carnival in Chinese cyberspace" in: David Kurt Herold, Peter Marolt (ed.), *Online Society in China – Creating, celebrating, and instrumentalising the online carnival*, op. cit., p. 2.

57 Ibid.

informacije o globalnom nadzoru i narušavanju ljudskih prava, koje su otkrili Edvard Snouden i Džulijen Asanž.

Zapadno orijentisani autori u svojim analizama korišćenja Interneta u Kini zaključuju da se, nasuprot pretpostavkama da će se pojavom komercijalnog Interneta na prostoru Kine ubrzati razvoj demokratije, najmnogoljudnija država na svijetu ipak odbranila od naleta novih tehnologija.[58] To su postigli izgradivši dva osnovna stuba budućeg Internet suvereniteta: „Veliki fajervol" (engl. "The Great Firewall") i Zlatni štit (engl. "Golden Shield").[59] Čen opisuje prvi stub kao ogroman lavirint zakona, regulativa i administrativnih praksi posredstvom kojih se nadgledaju i navodno cenzurišu Internet provajderi, ali i obični korisnici.[60] Sa tehničkog aspekta posmatrano, „Veliki fajervol" ima mogućnost da blokira adrese (serveri, sajtovi, društvene mreže) na Internetu koje ne ispunjavaju uslove iz Internet regulative Kine. Drugi stub kontrole, tzv. „Zlatni štit" – projekat Ministarstva za javnu bezbjednost vrijedan više milijardi dolara, posredstvom kojeg je Kina od 1998. godine do danas ušla u trag i navodno lišila slobode mnoge pojedince optužene da su kršili odredbe Internet regulative. Posredstvom ova dva „stuba" kineskog Internet suvereniteta, danas su zabranjene brojne društvene mreže na teritoriji Kine, kao što su Fejsbuk, Tviter, Instragram itd, zatim pretraživač Gugl, koji je funkcionisao četiri godine na teritoriji Kine, ali zbog nemogućnosti da ispuni sve propisane uslove povukao se 2010. godine. Interesantno je da danas na teritoriji Kine funkcioniše Majkrosoftov pretraživač Bing, naravno poštujući pravila koja postavlja kineska država.

Ipak, da ne bi potpuno uskratila korišćenje društvenih mreža, Kina je omogućila svojim građanima vlastite platforme kao što su Renren ("Renren" – pandan Fejsbuku sa preko 214.000.000 korisnika), Vaibo ("Sina Weibo" – mikroblogerski servis sličan Tviteru sa preko 361.000.000 korisnika), Vi-čet ("WeChat" – platforma za komunikaciju slična Vajberu i Vocapu sa oko 963.000.000 korisnika), Baidu ("Baidu Tieba" – zamjena za Google sa oko 300.000.000 korisnika)[61] itd. i time pokazala celom svijetu da u potpunosti može da funkcioniše bez najpopularnijih, globalnih, Internet servisa i društvenih mreža.

---

58 China's internet – A giant cage, The Economist, 2013. Available from: http://www.economist.com/news/special-report/21574628-internet-was-expected-help-democratise-china-instead-it-has-enabled (Accessed 10 December 2017).

59 Miroljub Radojković, Branimir Stojković, Aleksandar Vranješ, *Međunarodno komuniciranje u informacionom društvu*, nav. delo, 175.

60 Wenhong Chen, "Taking stock, moving forward: the Internet, social networks and civic engagement in Chinese societies", *Information, Communication & Society*, 17:1. 1–6, Routledge, London, 2014, p. 4.

61 *Most famous social network sites worldwide as of September 2017, ranked by number of active users (in millions)*, Statista, 2017. Available from: https://www.statista.com/

Bez obzira što sa Zapada stiže veliki broj kritika na račun građanskih sloboda u Kini, smatramo da je neophodno pogledati i drugu stranu medalje, posmatrajući kontrolu Interneta u Kini kao napor u odbrani vlastitog suvereniteta.

Ideja o „Internet suverenitetu u Kini" prvi put se spominje 2010. godine u tzv. „bijeloj knjizi" pod nazivom „Internet u Kini", objavljenoj u magazinu "People's Daily"[62]. U tekstu se objašnjava da je na teritoriji države Kine Internet pod jurisdikcijom kineskog zakonodavstva i da su svi ljudi i organizacije koji koriste Internet unutar teritorije Kine dužni da poštuju njihove zakone i regulaciju.[63] Tokom juna 2014. godine, bilten Komunističke partije Kine objavio je stav da bi svaka suverena država trebalo da ima apsolutnu moć da odredi koji Internet sadržaji mogu da uđu ili izađu sa njene teritorije.[64] Taj koncept koji je Kina ponudila nazvan je „Internet suverenitet" i zasniva se na ideji da svaka država treba da ima pravo da upravlja Internetom u okvirima svojih granica u skladu sa međunarodnim pravom, uz objašnjenje da SAD imaju preveliku moć kontrole sajber prostora i da je licemjerno promovisati ideje otvorenog i slobodnog Interneta, dok, s druge strane, upravo ta država nadzire strane vlade, kompanije i pojedince.[65] Drugim riječima, kontrola Interneta u Kini može se posmatrati i kao posljedica borbe za očuvanjem suvereniteta, kojom ova država želi da zaštiti svoje legitimne političke, ekonomske, bezbjednosne i kulturne interese.[66]

Iako određeni autori postupke Kine objašnjavaju kao uskraćivanje slobode širenja mišljenja, Radojković i dr. tvrde da neki radikalni primjeri potvrđuju da je možda i u Evropi trebalo zabraniti pojedine sadržaje, posebno kada su u pitanju recepti za kućnu izradu bombi, širenje antisemitizma, radikalizma, neonacizma, itd[67]. Naposlijetku, nameće se pitanje: koja je razlika, u kontekstu Internet sloboda, ako poredimo npr. kineski „Veliki fajervol" i globalni program za nadzor koalicije "Five Eyes" ili odnos prema uzbunjivačima

---

statistics/272014/global-social-networks-ranked-by-number-of-users/ (Accessed 10 December 2017).

62 *The Internet in China*, People's Daily Online, 2010. Available from: http://en.people.cn/90001/90776/90785/7017177.html (Accessed 10 December 2017).

63 Ibid.

64 Paul Mozur and Yang Jie, *China Argues for 'Internet Sovereignty' Is It a Good Idea?* Web blog post, 2014. Available from: https://blogs.wsj.com/chinarealtime/2014/06/23/chinas-lays-out-argument-for-internet-sovereignty-convinced/ (Accessed 10 December 2017).

65 Miroljub Radojković, Branimir Stojković, Aleksandar Vranješ, *Međunarodno komuniciranje u informacionom društvu*, nav. delo, 177.

66 Isto.

67 Isto.

kao što su Asanž i Snouden? Šta u tom kontekstu spriječava države da krenu u pravcu sajber suvereniteta i zaštite ustavom zagarantovanih prava vlastitih građana, kada su prema svim pokazateljima ljudska prava umreženih građana narušena na globalnom nivou.

ZAKLJUČAK

Konceptom sajber suvereniteta razvija se vizija Interneta koji ne bi bio više „mreža svih mreža", nego jednostavno Mreža svih nacionalnih intranetova i ostalih međunarodnih mreža u svijetu. Ekonomski nerazvijene zemlje koje ne mogu priuštiti „ograđivanje" svoje „sajber teritorije" ostale bi pod okriljem kontrole nekih od dominantnih „sajber sila" ili bi se možda stvorio tzv. „ničiji sajber prostor" koji bi ostao neregulisan i možda čak zloupotrebljen za razne nelegalne sadržaje. Iz svega napisanog možemo da izvedemo zaključak da je globalno komuniciranje već dobrim dijelom podvrgnuto kontroli, kako na Istoku tako i na Zapadu. Takođe, da se oblici te kontrole i dalje razvijaju kako tehnološki tako i administrativno, te da je stanje ljudskih prava umreženih građana, bez obzira iz koje države dolaze, i te kako ugroženo. Ako sve to stavimo u kontekstu pozicije nacionalne države, primjetne su aktivnosti na ojačavanju pozicija država unutar sajber prostora, što konačno identifikujemo kao trend rasta komunikacionog suvereniteta.

Kao što Velika Britanija pokušava da napravi zakonsku preventivu da se u njihovoj jurisprudenciji nikada ne pojavi neki Snouden ili Asanž, ili što Njemačka pokušava da smanji govor mržnje i dezinformacije uvođenjem jednog oblika cenzure, tako i Kina radi na jačanju Internet suvereniteta. U tom kontekstu važno je istaći da je početkom novembra 2016. godine Kina usvojila novi zakon o sajber bezbjednosti, kojeg su na Zapadu odmah nazvali „tehno-nacionalistički trojanski konj", jer navodno ulazi u domen poslovanja kako domaćih tako i stranih kompanija, a vezano za korišćenje informaciono-komunikacionih tehnologija. Zakon je stupio na snagu u junu 2017. godine i obavezuje strane kompanije koje posluju na teritoriji Kine i rade u „kritičnim" oblastima (energetika, transport, finansije, kompanije koje pružaju usluge u domenu informaciono-komunikacionih tehnologija i sl.) da podatke koje prikupljaju u procesu poslovanja obavezno čuvaju na serverima fizički smještenih na teritoriji Kine (već smo spomenuli sličnu legislativu u Brazilu i Rusiji) i da se ti podaci ne mogu slati van države bez prethodnog odobrenja. Takođe, zanimljiva odredba odnosi se i na obavezu dobijanja bezbjedonosnih sertifikata za mrežnu opremu i softver koji kompanije koriste na teritoriji Kine. To je posao državnog sertifikacionog tijela, što se odmah

protumačilo kao način da se favorizuje tehnologija proizvedena na teritoriji Kine, kao npr. mrežna oprema kompanije Huavej ili Lenovo. Naredna odredba odnosi se na obavezu Internet operatora da sarađuju u procesima istraga u vezi kriminala i nacionalne bezbjednosti. U tom kontekstu, kompanije će biti dužne da obezbijede vladinim agencijama koje sprovode istragu potpuni pristup svim podacima.[68]

S druge strane, iz institucije pod nazivom „Uprava za sajber prostor Kine" (engl. "Cyberspace Administration of China") navode da je novi zakon isključivo usmjeren u pravcu jačanja nacionalne bezbjednosti, odnosno jačanja sajber suvereniteta. U tom kontekstu zanimljive su i sljedeće odredbe navedenog zakona[69]:

1) Zakon o sajber bezbjednosti formulisan je tako da poveća bezbjednost na mreži, da očuva sajber suverenitet, nacionalnu bezbjednost i javni interes; da zaštiti prava i interese građana, pravnih lica i drugih organizacija i da promoviše zdrav razvoj ekonomske i društvene informatizacije;
2) Zakon se primjenjuje na izgradnju, upravljanje, održavanje i korišćenje računarskih mreža koje funkcionišu na teritoriji Narodne Republike Kine, što podrazumijeva i njihovu bezbjedonosnu superviziju i menadžment;
3) Država formuliše i kontinuirano unapređuje mrežnu bezbjedonosnu strategiju, preuzima mjere vezane za monitoring, prevenciju i rukovanje mrežnim bezbjedonosnim rizicima i prijetnjama, koje su nastale unutar ili van teritorije Kine. Takođe, država će štititi informacionu infrastrukturu od napada, upada, mješanja i razaranja, održavajući bezbjednost i red u sajber prostoru;
4) Svaka osoba ili organizacija koja koristi mreže pridržavaće se Ustava i zakona, poštujući javni red i društveni moral, te neće moći da ugrožava mrežnu bezbjednost i neće moći da koristi mreže zarad aktivnosti protivnih nacionalnoj bezbjednosti; nacionalnoj časti i interesu; za podrivanje državnog suvereniteta, smjenu socijalističkog sistema; podsticanje separatizma, potkopavanje nacionalnog jedinstva, zalaganje za terorizam i ekstremizam; za izazivanje nacionalne mržnje i etničke diskriminacije; širenje nasilja, nepristojnih ili pornografskih sadržaja; kreiranje i širenje lažnih informacija s namjerom da se de-

---

68 Christina Larson, Keith Zhai, David Ramli, Gao Yuan, *China Adopts Cybersecurity Law Despite Foreign Opposition*, Bloomberg Technology, 2016. Available from: https://www.bloomberg.com/news/articles/2016-11-07/china-passes-cybersecurity-law-despite-strong-foreign-opposition (Accessed 10 December 2017).

69 *2016 Cybersecurity Law*, 2016. Available from: http://www.chinalawtranslate.com/cybersecuritylaw/?lang=en (Accessed 10 December 2017).

stabilizuje ekonomski i društveni poredak; kao i za vrijeđanje ugleda, privatnosti, intelektualne svojine, kao i ostalih interesa drugih lica.

5) Država uspostavlja i unapređuje sistem standarda u domenu mrežne bezbjednosti.[70]

Dakle, bez obzira na sve kritike, Kina nastavlja u pravcu unapređenja svog sajber suvereniteta, što se može očitovati i iz stavova predsjednika Si Đinpinga. Naime, predsjednik Kine je u svom uvodnom obraćanju na ceremoniji otvaranja Druge svjetske Internet konferencije u Vudženu (Wuzhen) u Kini, 16. decembra 2015. godine, između ostalog zaključio da je princip suverene jednakosti, kako se navodi u Povelji Ujedinjenih nacija, jedna od osnovnih normi u savremenim međunarodnim odnosima i obuhvata sve aspekte međudržavnih odnosa, što takođe uključuje i sajber prostor. Trebalo bi poštovati pravo svake države da nezavisno izabere vlastiti put sajber razvoja, model sajber regulacije i Internet javnih politika, te da participira u upravljanju međunarodnim sajber prostorom na ravnopravnoj osnovi. Nijedna zemlja ne bi trebalo da primjenjuje sajber hegemoniju, da se miješa ili da se bavi unutrašnjim pitanjima drugih zemalja i da podržava sajber aktivnosti koje podrivaju nacionalnu bezbjednost drugih država.[71]

Na kraju, važno je da naglasimo da šira tema upravljanja globalnim Internetom sigurno nije završena, te će u narednom periodu sve više opterećivati odnose između SAD i Kine, a kojima se pridružuju i druge zemlje. Ipak, zabilježeni trend jačanja kontrole vlastitih sajber prostora kod pojedinih razvijenih zapadnih država govori nam da se američki model upravljanja Internetom ipak neće još dugo održati u međunarodnim forumima i da nam slijedi vrijeme jačanja komunikacionog suvereniteta u sajber prostoru.

BIBLIOGRAFIJA

[1] *Bundestag zabranjuje govor mržnje i izmišljene vesti*, Politika, 2017. Dostupno preko: http://www.politika.rs/sr/clanak/377889/Bundestag-zabranjuje-govor-mrznje-i-izmisljene-vesti (Pristupljeno 10. decembra 2017).

---

70 Ističemo da smo odredbe Zakona preuzeli iz neautorizovanog engleskog prevoda, te da se originalni tekst zakona na kineskom jeziku nalazi na linku: http://www.npc.gov.cn/npc/xinwen/2016-11/07/content_2001605.htm.

71 Jinping Xi, R*emarks by H.E. Xi Jinping President of the People's Republic of China At the Opening Ceremony of the Second World Internet Conference*, Ministry of Foreign Affairs of the People's Republic of China, 2015. Available from: http://www.fmprc.gov.cn/mfa_eng/wjdt_665385/zyjh_665391/t1327570.shtml (Accessed 10 December 2017).

[2] Chen, Wenhong, "Taking stock, moving forward: the Internet, social networks and civic engagement in Chinese societies", *Information, Communication & Society*, 17:1. 1–6, Routledge, London, 2014, p. 1.

[3] *China Internet Users, Internet Live Stats*, 2016. Available from: http://www.internetlivestats.com/internet-users/china/ (Accessed 10 December 2017).

[4] *China's internet – A giant cage*, The Economist, 2013. Available from: http://www.economist.com/news/special-report/21574628-internet-was-expected-help-democratise-china-instead-it-has-enabled (Accessed 10 December 2017).

[5] *Dangerously disproportionate – The ever-expanding National Security State in Europe*, Amnesty International, 2017. Available from: https://www.amnesty.org/download/Documents/EUR0153422017ENGLISH.PDF (Accessed 8 December 2017).

[6] Fu, King-wa and Chau, Michael, *Reality check for the Chinese microblog space: A random sampling approach*, PloS One, Vol.8(3), 2013. Available from: http://www.plosone.org/article/info%3Adoi%2F10.1371%2Fjournal.pone.0058356, (Accessed 10 December 2017).

[7] Gurstein, Mike, *Multistakeholderism vs. Democracy: My Adventures in "Stakeholderland"*, Web blog post, 2013. Available from: https://gurstein.wordpress.com/2013/03/20/multistakeholderism-vs-democracy-my-adventures-in-stakeholderland (Accessed 8 December 2017).

[8] Herold, David Kurt, "Noise, spectacle, politics: carnival in Chinese cyberspace" in: David Kurt Herold, Peter Marolt (ed.), *Online Society in China – Creating, celebrating, and instrumentalising the online carnival*, Routledge, London, 2011, p. 1.

[9] Hope, Christopher, *Exclusive Spies and civil servants who leak secrets face 14 years in jail in first overhaul of the Official Secrets Act for 100 years*, The Telegraph, 2017. Available from: http://www.telegraph.co.uk/news/2017/02/02/exclusive-spies-civil-servants-leak-secrets-face-14-years-jail/ (Accessed 10 December 2017).

[10] International Telecommunication Union, *Collection of the basic texts adopted by the Plenipotentiary Conference*, 2015. Available from: http://search.itu.int/history/HistoryDigitalCollectionDocLibrary/5.21.61.en.100.pdf (Accessed 8 December 2017).

[11] *Investigatory Powers Act 2016*, Parliament UK, 2016. Available from: http://services.parliament.uk/bills/2015-16/investigatorypowers.html (Accessed 7 December 2017).

[12] Kelly, Sanja, Truong, Mai, Shahbaz, Adrian and Earp, Madeline, *Silencing the Messenger: Communication Apps under Pressure – Freedom on the Net 2016 – Annual report*, Freedomhouse, 2016. Available from: https://freedomhouse.org/report/freedom-net/freedom-net-2016 (Accessed 10 December 2017).

[13] Larson, Christina, Zhai, Keith, Ramli, David and Yuan, Gao, *China Adopts Cybersecurity Law Despite Foreign Opposition*, Bloomberg Technology, 2016. Available from: https://www.bloomberg.com/news/articles/2016-11-07/china-passes-cybersecurity-law-despite-strong-foreign-opposition (Accessed 10 December 2017).

[14] Limbago, Andrea, *The global push for cyber sovereignty Is the beginning of cyber fascism*, The Hill, 2016. Available from: http://thehill.com/blogs/congress-blog/technology/310382-the-global-push-for-cyber-sovereignty-is-the-beginning-of (Accessed 8 December 2017).

[15] Liu, Fengshu, *Urban Youth in China: Modernity, the Internet and the Self*, Routledge, London, 2010, p. 35.

[16] Lu, Wei, *Cyber Sovereignty Must Rule Global Internet*, Huffington Post, 2014. Available from: http://www.huffingtonpost.com/lu-wei/china-cyber-sovereignty_b_6324060.html (Accessed 8 December 2017).

[17] Lum, Thomas, "Internet development and information control in the People's Republic of China", *CRS report for Congress*, Library of Congress, Washington, 2006.

[18] Malcomson, Scott, *How Russia and China Are Cooperating to Dismantle America's Dominance of the Internet*, Huffington Post, 2016. Available from: http://www.huffingtonpost.com/scott-malcomson/russia-china-internet_b_9841670.html (Accessed 7 December 2017).

[19] Marinković, Ankica, *Rusija blokirala društvenu mrežu 'Linktin'*, Politika, 2016. Dostupno preko: http://www.politika.rs/sr/clanak/368039/Spektar/Digitalni-svet/Rusija-blokirala-drustvenu-mrezu-Linktin (Pristupljeno 10. decembra 2017).

[20] Moody, Glyn, *Why the Investigatory Powers Act is a privacy disaster waiting to happen*, Ars Technica UK, 2016. Available from: https://arstechnica.co.uk/tech-policy/2016/11/investigatory-powers-act-privacy-disaster-waiting-to-happen (Accessed 8 December 2017).

[21] *Most famous social network sites worldwide as of September 2017, ranked by number of active users (in millions)*, Statista, 2017. Available from: https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/ (Accessed 10 December 2017).

[22] Mozur, Paul and Jie, Yang, *China Argues for 'Internet Sovereignty' Is It a Good Idea?* Web blog post, 2014. Available from: https://blogs.wsj.com/chinarealtime/2014/06/23/chinas-lays-out-argument-for-internet-sovereignty-convinced/ (Accessed 10 December 2017).

[23] Radojković, Miroljub, Stojković, Branimir i Vranješ, Aleksandar, *Međunarodno komuniciranje u informacionom društvu*, Clio, Beograd, 2015, str. 141.

[24] Polatin-Reuben, Dana and Wright, Joss, *An Internet with BRICS Characteristics: Data Sovereignty and the Balkanisation of the Internet*, 4th USENIX Workshop on Free and Open Communications on the Internet, 2014. Available from: https://www.usenix.org/system/files/conference/foci14/foci14-polatin-reuben.pdf (Accessed 10 December 2017), p. 3.

[25] Steele, Cherie and Stein, Arthur A. "Communications Revolutions and International Relations" in: Juliann Emmons Allison (ed.), *Technology, Development and Democracy – International Conflict and Cooperation in the Information Age*, State University of New York Press, Albany, 2002, p. 35.

[26] *The Internet in China*, People's Daily Online, 2010. Available from: http://en.people.cn/90001/90776/90785/7017177.html (Accessed 10 December 2017).

[27] Travis, Alan, *'Snooper's charter' bill becomes law, extending UK state surveillance,* The Guardian, 2016. Available from: https://www.theguardian.com/world/2016/nov/29/snoopers-charter-bill-becomes-law-extending-uk-state-surveillance (Accessed 8 December 2017).

[28] Vujić, Ljiljana, *Udar Londona na novinare i uzbunjivače*, Politika, Beograd, 2017. Dostupno preko: http://www.politika.rs/sr/clanak/374220/Udar-Londona-na-novinare-i-uzbunjivace (Pristupljeno 09. decembra 2017).

[29] Xi, Jinping, *Remarks by H.E. Xi Jinping President of the People's Republic of China At the Opening Ceremony of the Second World Internet Conference*, Ministry of Foreign Affairs of the People's Republic of China, 2015. Available from: http://www.fmprc.gov.cn/mfa_eng/wjdt_665385/zyjh_665391/t1327570.shtml (Accessed 10 December 2017).

[30] Zetter, Kim, *California Now Has the Nation's Best Digital Privacy Law*, The Wired, 2015. Available from: https://www.wired.com/2015/10/california-now-nations-best-digital-privacy-law (Accessed 10 December 2017).

[31] Zhou, Yongming, *Historicizing online politics: Telegraphy, the Internet, and political participation in China*, Stanford University Press, Palo Alto, 2006, p. 142.

[32] *2016 Cybersecurity Law*, 2016. Available from: http://www.chinalawtranslate.com/cybersecuritylaw/?lang=en (Accessed 10 December 2017).

Aleksandar Vranješ

INTERNET SOVEREIGNTY WITH CHINESE CHARACTERISTICS

Abstract

The development of the modern information and communication technologies, as well as the increase of the number of Internet users, has helped to intensify the debate on Internet governance at international forums. On the one hand, the United States insists on the Multi-stakeholder Internet Governance model, while on the other hand, China is more loudly advocating the "Internet sovereignty" model – a multilateral approach in which all countries of the world freely choose their own cyber-development way, with no state having a position to apply cyber hegemony. This model certainly came under criticism in the West, because it was designated as a platform for empowering control and violating civil liberties. But, on the other hand, we are witnessing that certain Western states are also working to establish greater control in their own cyber space, and therefor their critique of the Chinese model is less convincing. Finaly, China, as the first "Internet sovereign" state, has reach so far in the domain of technical and legislative improvement of its own cyber space, that it is difficult to imagine that the current situation will return to its initial position, especially if we consider the growth of political and economic power of this state. We have come to the conclusion that in the future global debate on Internet governance, the arguments will be increasingly on the Chinese side, and that a new era of cyber sovereign states is ahead of us.

Key words:

Internet sovereignty, Internet governance, China, control, surveillance.