UNIVERZITET U BEOGRADU

FILOZOFSKI FAKULTET

Ivana Ivković

MORALNE VREDNOSTI U DIZAJNU ARHITEKTURE INTERNETA

doktorska disertacija

Beograd, 2016

UNIVERSITY OF BELGRADE

FACULTY OF PHILOSOPHY

Ivana Ivković

MORAL VALUES IN THE INTERNET ARCHITECTURE DESIGN

Doctoral Dissertation

Belgrade, 2016

Комисија за одбрану докторског рада

Ментор:

Др Јован Бабић, редовни професор,
Филозофски факултет, Универзитет у Београду

Чланови комисије:

Др Мирјана Дракулић, редовни професор
Факултет организационих наука, Универзитет у Београду

Др Ненад Цекић, ванредни професор,
Филозофски факултет, Универзитет у Београду

Moralne vrednosti u dizajnu arhitekture interneta

Rezime

Filozofsko određenje interneta polazi od izbora pravog nivoa tehnološke apstrakcije na kome se može govoriti o njemu kao promenljivom tehnološkom sistemu, a isto tako i od izbora arhitekture kao objekta analize dizajna interneta. Arhitektura je sinonim za tumačenje interneta od strane inžinjera tj. mrežnih dizajnera, tokom koga su se oni upustili u kreiranje šireg viđenja o tome kako vide ili žele da vide, izgrade ili regulišu taj sistem. U originalnu arhitekturu interneta založene su vrednosti libertarijanske kulture i principi koji vode računa pre svega o što široj interkonekciji putem jedinstvenog seta protokola. Vremenom je internet zajednica morala da odustane od arhitekture mreže u korist postavljanja u centar pažnje velikog broja aplikacija. U toj post-arhitekturalnoj fazi, do filozofskog određenja interneta se dolazi kroz razmatranje pitanja vezanih za upravljanje internetom, njegovu materijalno-prostornu realizaciju i njegovu interakciju sa komercijalnom sferom. Upravljanje internetom, ma kako funkcionalno, nije sprečilo da se pojavi neupravljani internet tzv. tamni internet iliti mračna strana javnog interneta. Tamni internet je moguć zahvaljujući kriptografiji, i inherentna mu je subverzivnost. Iz tamnog interneta stiže ne samo ozloglašeni sajber kriminal, već i prodor istine zarad opšteg dobra tj. raskrinkavanje nadzora nad javnim internetom. Mapiranje interneta na planeti ukazuje da jedan mali broj lokacija prima, razmenjuje i transmituje veliki deo internet saobraćaja i komunikacija na planeti. Te lokacije jesu tu gde jesu iz razloga geografije, istorije i novca, dok s druge strane opstaje metafora sajber spejsa i zamagljuje potrebu običnog korisnika da obrati pažnju na mnoštvo načina za konceptualizovanje obrazaca i tokova informacija kroz internet. Internet industrija je direktno čedo inovativnih preduzetnika i dobro raspoloženih finansijskih tržišta i investicionih fondova. Najnoviji trend u internet industriji je internet stvari, u kome na mrežu dolaze kao krajevi najrazličitiji senzori (od kućnih senzora do narukvica za fitnes) i skoro sve se pretvara u uređaj koji proizvodi podatke. Ono što spaja ova tri post-arhitekturalna ugla sagledavanja interneta je to da upućuju na običnog korisnika interneta. G. i gđa Obični korisnik su ostvarili brojne dobitke od interneta, no u budućnosti moraju preuzeti punu odgovornost za pravce razvoja interneta. Oni su ti koji su nadzirani, i treba da učine nešto povodom toga. Oni su ti koji

umesto metafore sajber spejsa treba da konceptualizuje internet kao prostor koji počiva na interakcijama i u koji se preslikavaju sve oflajn strukture, uključujući nejednakosti. Oni su ti koji treba da se izjasne da li će prihvatiti internet stvari ili ga odbaciti. Pred običnog korisnika se postavljaju i drugi izazovi, primerice da odredi kakvu zaštitu ličnih podataka želi da poseduje na internetu. Tu se ponekad dešava dilema prodati ili čuvati svoje lične podatke. Bez obzira na ovu dilemu, barem u Evropi, zaštita privatnosti se ostvaruje kroz pravni okvir koji štiti lične podatke. Moć pravnog sistema je za sada jača od onih koji imaju interes da napadaju privatnost. Zbog toga i nastaje optimizam da se nadzor nad običnim korisnicima na internetu može zaustaviti i da će pitanje zaštite ličnih podataka i zaštite privatnosti biti prevaziđeno za 5 ili 10 godina. Metod primenjen u istraživanju obuhvatio je: istraživanje relevantne literature, ali i empirijsko istraživanje odnosno lični uvid u stvarno stanje interneta / na internetu, uključujući i studiju slučaja o platformama za onlajn učenje.

Ključne reči: internet, principi, upravljanje, onlajn učenje, digitalni aktivizam, nadzor, privatnost, korisnik.

Naučna oblast: Filozofija

Uža naučna oblast: Etika, politika interneta

UDK broj i klasifikaciona oznaka za datu oblast

Moral Values in the Internet Architecture Design

Abstract

Philosophical view of the internet starts with the choice of adequate level of technological abstraction, whereof one can speak of the internet as changeable technological system. This choice is paralleled with the choice of architecture as an object of analysis in relation to the internet design. The architecture is synonymous with the interpretation of the internet by the engineers or network designers, with which they have entered into creating larger picture of how they see or wish to see, build or regulate that system. Values of libertarian culture are vested in the original internet architecture, as well as principles fostering the widest interconnection based on the unique set of protocols. In the course of time, the internet community had to give up the architecture considerations in favor of putting the applications in the center of interest. Therefore in the post-architecture phase, philosophical view of the internet raises from the discussion of issues related to internet governance, its material-spatial realization and its interaction with economy and commercial sphere. No matter how functional and well ordered the internet governance is, it could not impede the formation of non-governed internet or dark internet, which is a dark side of the public internet. Dark internet is possible due to cryptography and the potential for subversion is inherent to it. Among the things coming from the dark internet are not only infamous cyber criminal incidents, but also truth checks for the common good – discovery of the surveillance of public internet. Mapping the internet on the planet shows that one small number of locations receive, exchange and transmit the huge portion of internet traffic and communications on the planet. These locations are where they are as the consequence of the reasons of geography, history and money. In the same time, we find the cyber space metaphor, obscuring the average user's need to direct attention to multiplicity of ways of conceptualizing the patterns and flows of information trough the internet. The internet industry is a direct intersection of innovative entrepreneurs, from one side, and „feeling lucky" financial markets and investment funds, from the other. The newest trend in the internet industry is internet of things, in which variety of sensors (from home sensors to fitness trackers) become the networks' ends turning almost everything in data producing machine. The common feature in these three post-architecture angles on internet is that they all refer

to an average internet user. An average user has achieved numerous gains from the internet, but in the future he/she has to take full responsibility for the direction of internet development. He/she is surveilled and has to do something about it. He/she is expected to leave behind the old cyber space metaphor and to conceptualize the internet as a space stemming from the interactions and mirroring all the off-line structures including the real world inequalities. He/she must determine for or against the acceptability of the internet of things, beginning with his/her most private life. An average user confronts some additional challenges too, for example to set boundaries on which kind of protection of private data is to be possessed on the internet. Here sometimes one witnesses the user's dilemma: to sell or to keep the private data. Regardless of this dilemma, at least in Europe, the privacy protection is implemented by the legal framework committed to keep control over data in the hands of average users. The power of that legal system is heavier so far than one of interest-driven privacy attackers. Therefore optimism can be well grounded and coupled with the confidence that "wild" internet users' surveillance as of today would soon be averted. It is a tentative view that private data protection issues will be overcome in 5 or 10 years time. The method used in this research covers: research of the relevant literature as well as empirical research and personal insight in the real situation on the internet, including the case study dealing with the on-line platforms for learning.

Key words: Internet, principles, governance, online learning, digital activism, surveillance, privacy, user

Discipline: Philosophy
Specific discipline: Ethics, Internet Policy

UKD number and clasification mark

Sadržaj

UVOD

Internet i filozofija

Ukoliko živite u stanu u bilo kom većem naseljenom mestu, mesečno vam stižu računi za potrošnju određenih dobara i usluga: računi na ime troškova struje, vode, daljinskog grejanja, odnošenja smeća, telefona i – interneta. Iako je ta pojava postala uobičajena možda tek zadnjih 10 ili 20 godina, na nju se navikavamo, a navikavamo se i na misao da je internet jedna od tih stvari, sličan struji, vodi, grejanju, odnošenju smeća, telefonu – nešto potrebno i podrazumevano u takvom načinu života. Jasno je da se sve to bazira na nekoj infrastrukturi i da njenu realnu ili beneficiranu cenu treba platiti. Prosečnog stanara jednako ne zanima kako voda stiže do njegove česme – sve dok je ispravna za piće - kao i kako se njegovi kućni uređaji povezuju na internet – sve dok je veza dovoljno brza. Da li bi onda filozofiju trebalo da zanima išta od toga? O vodi odgovor možemo prepustiti nekom drugom, a u slučaju interneta taj odgovor je potvrdan.

Filozofi se u prošlosti nisu bavili internetom, što nije ni čudno ako je tačno da internet relativno nov fenomen koji nema preteču ni pandana u čitavoj ljudskoj istoriji. Ali filozofija se uvek bavila i bavi onim što je bitno za ljudski život. Zbog odnosa koji je uspostavljen između čoveka i interneta, filozofija se okreće ka ovom novom fenomenu. Danas razumevanje interneta predstavlja ovladavanje pojmom jednog fenomena koji je u relativno kratkom periodu od nekih 40ak godina osvojio i promenio svet. Ne samo da se radi o fenomenu koji je ovaploćenje savremenog trenutka, nego je to fenomen koji je u stalnoj promeni. Sa tim promenama, i mi koji smo sve više i više, i vremenski i prostorno i mentalno na internetu, mi koji smo korisnici interneta, takođe se preoblikujemo kroz neke promene. Filozofija koja prati čoveka neminovno posvećuje pažnju i internetu.

U svojoj dugoj istoriji filozofija je nadilazila površno poimanje i saznavanje sveta i čoveka, tražeći uvide koji su intelektualno složeniji i dublji u shvatanju dešavanja, karakteristika, vrednovanja. Taj isti tretman potrebno je primeniti i kad je u pitanju internet, i to počev od samog izbora pristupa ovom fenomenu, o čemu će uskoro biti više rečeno.

Jasno je da značaj interneta još uvek nije do kraja demonstriran niti ispitan. Dosadašnje posledice interneta su multidimenzionalne; transformacije koje se vrše u

ovom ili onom pravcu odlukom raznih aktera su dinamične i teške za kontekstualizovanje; konačno, internet sadrži i potencijale, od kojih neki još uvek nisu do kraja uočeni, a koji se mogu razviti na mnogo načina, pri čemu svest o njima može uticati na pravac razvoja u budućnosti. Bilo da se veruje da pravac razvoja interneta određuje neka nevidljiva ruka, bilo da se to fiksira kroz delovanja dominantnih aktera, filozofija treba i može pratiti regulaciju interneta i tematizovati redistribuciju moći, kapacitet kontrole, očuvanje ljudske slobode, jačanje jednakosti šansi. Kakva regulacija je poželjna ili ispravna ili najbolja je interdisciplinarno (međunardno, pravno, ekonomsko, tehničko itd.) te delimično i filozofsko pitanje.

Smatram da filozofija treba da što je moguće više dozna o internetu kao tehnološkom izumu odnosno uspešno komercijalizovanoj tehnologiji koja je ostvarila globalni domet, po mnogima čak sveprisutnost, i stigla do naše kuće, pa čak i do naše odeće i kože. Filozofija ima zadatak da pomogne nama, korisnicima interneta, da se bolje snalazimo u svojim ulogama učesnika, kreatora, žrtava ili odlučioca o promenama interneta. Filozofija je čak jedinstveno pogodna da u ovoj temi (kao što radi sa svim temama) rasvetli i objasni ono podrazumevano, mit, racionalno saznanje, vrednosti, očekivanja i dr.

O naslovu

Termin „moralne vrednosti“ u ovom radu nije tehnički termin. Stipuliraćemo da se odnosi na ljudsku slobodu i jednakost šansi u kontrapoziciji sa društveno-ekonomskom-političkom-tehnološkom moći i kontrolom. Termin „moralno“ se inače tiče određivanja ispravnog i pogrešnog u ljudskom ponašanju. Stanovište od kog se u ovom radu polazi jeste da je jačanje slobode i jednakosti ono ispravno, ono što treba podržati. Treba napomenuti da je to vrednosni sud, i da kao takav on ima svoju suprotnost, suprotni vrednosni sud, po kome je jačanje kontrole i nejednakosti odnosa snaga ono ispravno, ono što treba podržati. Izbor između jednog i drugog vrednosnog suda nije predmet ovog istraživanja; strana je izabrana i uzima se ovde kao aksiom.

Termin „dizajn“ se odnosi na način kako je nešto napravljeno, i odabran je zato što već ima ustaljenu primenu u govoru koji se tiče tehničkih proizvoda.

Termin „arhitektura interneta“ predstavlja glavnu specifičnost ovog rada. On je odabran sa namerom da se zaobiđe površno poimanje i ostvari filozofsko saznavanje,

tražeći uvide koji su intelektualno složeniji i dublji u razumevanju dešavanja, karakteristika, vrednovanja. To je ovde primenjeno već i samim izborom pristupa internetu. Internetu će se pristupati polazeći od njegove arhitekture, a ne od sadržaja prisutnih na njemu, niti od korisnika i njihovih iskustava. Pristup preko arhitekture interneta obezbediće za početak filozofski ugao gledanja na ovaj fenomen, pristup koji omogućava dublji uvid u dešavanja, karakteristike i vrednosti implicirane u ovom tehnološkom sistemu.

Arhitektura interneta, kao i sam internet, je tehnički termin koji će kasnije u radu biti preciziran. Ovde možemo napomenuti da je internet mreža odnosno međupovezanost komjuterskih mreža, a arhitektura interneta je celina samorazumevanja interneta od strane njegovih tvoraca i rezultat najšire debate o njegovom karakteru. Arhitektura interneta je drugo ime za (pisanu i nepisanu) kompilaciju razmatranja suštinskih pitanja interneta. Ona nastaje time što se iskristališu preovlađujuća mišljenja internet zajednice o onom šta, kako i zašto treba uraditi sa tim tehničkim sistemom. Internet zajednicu čine naučnici iz domena kompjuterskih nauka i svi oni kojima je do interneta stalo. Gledišta i stavovi naučnika iz domena kompjuterskih nauka i ostalih zainteresovanih nisu samo tehničke sadržine već tu nalazimo i reference na druge discipline, uključujući i filozofiju. Arhitektura interneta je prva, mada ne i jedina, podloga razmatranjima o tzv. vrednosnoj obojenosti interneta, o kojoj će kasnije biti reči. Arhitektura interneta nije koncipirana u stilu „od inžinjera za inžinjere“ nego „od inžinjera za sve (koji su sposobni i voljni da se zainteresuju)“.

Internet je termin koji se u engleskom jeziku prvi put pojavio kao pridev (u dokumentu[1] RFC 675 „Specifikacija programa kontrole internet transmisije“ iz 1974. god.), da bi nekih 20ak godina kasnije postao i imenica. Kao pridev odnosio se na svojstva određenih kompjuterskih procesa da funkcionišu umreženo, (među)mrežno, u mreži kompjutera. Kao imenica odnosio se na mrežu kompjutera koji koriste jednu karakterističnu tehnologiju da komuniciraju međusobno. Takav je preuzet u srpski jezik.

[1] RFC 675 „Specification of internet transmission control program“ http://tools.ietf.org/html/rfc675 Objašnjenje pojma RFC biće dato u poglavlju 3. Na ovom mestu, u najkraćem, RFC označava zvaničan dokument koji je napisala i odobrila zajednica istraživača koji razvijaju internet.

Internet: medij ili tehnologija?

Zanimanje za internet često se usmerava na njegov aspekt medija koji ima svoje osobenosti u odnosu na druge medije (elektronske, štampane).[2] Takođe se u novjie vreme pridaje pažnja i njegovom aspektu sredstva kontrole i nadzora.[3] U ovom radu se internet tretira u smislu tehnološkog izuma, tehničkog sistema, inžinjerskog artefakta, tehničke infrastrukure koja je većim delom nevidljiva korisnicima. Ne tvrdimo da je pogrešno tretirati internet kao medij, niti kao sredstvo kontrole i nadzora, ali iz ugla autorke važnije je ono što predstavlja njegov opštiji pojam (ono što mu omogućava da bude mnogo toga, na primer medij, sredstvo kontrole, ...). To je upravo njegovo izjednačavanje sa tehnologijom koja ima mogućnost prožimanja mnogih oblasti života, kao i mogućnost inoviranja.

Tehnička infrastruktura interneta je nevidljiva ako se gleda samo sadržaj komunikacije na internetu, ako se pažnja usmeri na odnos medij-korisnik ili kontrolor-korisnik. Smatram da ona ne sme ostati nevidljiva, zato što predstavlja glavno mesto prelamanja interesa brojnih aktera koji žele da upravljaju internetom i dobrim delom stvara posledice interneta relevantne u moralnoj filozofiji.

Teoretičarka medija Sonja Livingston iznela je zapažanje: internet se tretira kao celovit zaokružen medij ali je to zapravo kolekcija različitih tehnologija, formi i servisa.[4] Iako ovde nećemo internet tretirati kao medij nego kao tehnički sistem, ovo zapažanje je dobar putokaz. Internet kao tehnički sistem je kolekcija raznih komponenti, nastalih u različitim vremenskim periodima i sa različitim namenama. Neke od komponenti postale su standardi, univerzalni i globalno primenjeni; druge se smatraju za najbolje prakse; treće su u raznim fazama istraživanja, primene ili

[2] Definicija medija iz člana 29. *Zakona o javnom informisanju i medijima Republike Srbije* („Sl. glasnik RS“, br. 83/2014 i 58/2015) glasi: „Medij je sredstvo javnog obaveštavanja koje rečima, slikom odnosno zvukom prenosi urednički oblikovane informacije, ideje i mišljenja i druge sadržaje namenjene javnoj distribuciji i neodređenom broju korisnika. Pod medijem se u smislu ovog zakona naročito podrazumevaju dnevne i periodične novine, servis novinske agencije, radio-program i televizijski program i elektronska izdanja tih medija, kao i samostalna elektronska izdanja (uređivački oblikovane internet stranice ili internet portali), a koji su registrovani u Registru medija, u skladu sa ovim zakonom.“ Član 30. istog zakona kaže: „Medij, u smislu ovog zakona nije: ...internet-pretraživači i agregatori. ... platforme, poput internet foruma, društvenih mreža i drugih platformi koje omogućavaju slobodnu razmenu informacija, ideja i mišljenja njenih članova, niti bilo koja druga samostalna elektronska publikacija, poput blogova, veb-prezentacija i sličnih elektronskih prezentacija, osim ao nisu registrovane u Registru medija, u skladu sa ovim zakonom.“ Zakon je dostpan na internet adresi http://www.paragraf.rs/propisi/zakon_o_javnom_informisanju_i_medijima.html

[3] O nadzoru nad internetom i njegovim korisnicima će biti više reči u poglavljima 5 i 8.

[4] Navedeno prema: Dragan Štavljanin. (2013). *Balkanizacija Interneta i smrt novinara*. Prag i Beograd: Radio Slobodna Evropa i Čigoja štampa. str. 58.

polemike. Ukupnost tih komponenti interneta može se proučavati u RFC-ima, kojih početkom 2016. god. ima 7772. Premda je jedan deo RFC-ova samo istorijskog značaja, prevaziđen i slično, a drugi deo se bavi istim predmetom kroz sukcesivne promene, i dalje imamo posla sa više hiljada validnih RFC-ova, koji sadrže brojne detalje ovog sistema. Tako veliki broj komponenti nije potrebno obraditi za potrebe ovog rada. Prvi korak će biti fokusiranje samo na najbitnije komponente interneta.

Tehnički sistem sagledan na „pravom" nivou apstrakcije

Zamka u koju ne treba pasti kod bilo koje analize interneta je baratanje mitom interneta a ne njegovom stvarnošću. O tome veoma strastveno piše Evgenij Morozov, jedan od kontroverznijih američkih kritičara moderne tehnologije. Njegova veoma polemički napisana knjiga *Da biste sačuvali sve, kliknite ovde. Ludost tehnološkog solucionizma*[5] iz 2013. god. budi oprez prema referiranju na internet kao jedinstven i stabilan objekt. Takav internet bi bio mit, dok je stvarnost interneta u specifičnim detaljima tehnologija koje se koriste u društvenom kontekstu.

> „On (Morozov – prim.aut.) poziva da dublje promislimo o tome kako interneti iz 1993., 2003. i 2013. godine uspevaju da budu osećani kao kontinuirani. A ne samo da su se dajl-ap modemi zamenili širokopojasnim vezama, nego je i broj korisnika globalno skočio sa 495 miliona 2001. god. na 2,3 milijarde 2011. god. Da li i dalje govorimo o istom entitetu (pod pretpostavkom da je 'entitet' prava reč)?"[6]

U jednom intervjuu datom povodom svoje knjige, Morozov odgovarajući na postavljeno pitanje ističe:

> „Problem koji ja vidim nije samo činjenica da imamo mnogo novih tehnologija koje su odjednom postale mnogo moćnije nego pre 10, 15, 100 godina; problem koji vidim je u tome kako su ove tehnologije stavljene zajedno pod kišobran 'Interneta' i kako se podrazumeva da imaju jedinstvenu autonomnu dinamiku kojom treba da budu shvaćene i upravljane."[7]

---

[5] Evgeny Morozov. (2013). *To Save Everything, Click Here: The Folly of Technological Solutionism*. New York Public Affairs. 2013.

[6] Kevin Driscoll. (17. mart 2013). "The God That Failed: Evgeny Morozov's 'To Save Everything, Click Here'" for *Los Angeles Review of Books*. Preuzeto sa https://lareviewofbooks.org/review/the-god-that-failed-evgeny-morozovs-to-save-everything-click-here

[7] Natasha Dow Schuell. (9. sep. 2013).„The Folly of Technological Solutionism: An Interview with Evgeny Morozov" *Public Books*. Preuzeto sa http://www.publicbooks.org/interviews/the-folly-of-technological-solutionism-an-interview-with-evgeny-morozov

Inače, treba dodati da je Morozov veoma kritičan prema „internet intelektualcima“ čiji je posao da objašnjavaju ideje i argumente široj javnosti, ali po njemu to ne čine. Praveći rečitu analogiju, Morozov delovanje ovih intelektualaca razvrstava na to da li misle da je internet više kao asteroid koji treba da bude objašnjen od strane astrofizičara ili više kao 'šarkando' – objekt koji svakako može da se objašnjava ali samo po cenu da ga činimo realnijim i uverljivijim nego što on treba da bude.[8] Reč šarkando je kovanica od engl. shark – ajkula i tornado – tornado, a odnosi se na zaplet nekog holivudskog naučnog fantastičnog filma. Jasna je aluzija na bavljenje nečim nerealnim, čega po Morozovu u akademskim i novinskim raspravama o internetu dosta ima. Nasuprot ključnim komponentama interneta postoje i brojni periferni detalji koji zamaglju glavnu stvar, a na žalost i pojmovi koji su „lansirani“ kao produkt nekog partikularnog interesa, mode, manipulacije i slično. Bavljenje ovim «lansiranim» pojmovima je prisutno u akademskoj javnosti koja se bavi internetom i posebno nervira Morozova. Morozov o tome daje oštru kritiku, nad kojom se treba zamisliti uopšte uzev, ali i konkretno u istraživanjima na temu interneta, kako ne bismo došli pod udar te kritike. Opomena glasi:

> „Možda je o tome reč u Hibridnom dobu: marketing maskiran kao teorija, šarlatani maskirani kao filozofi, kult Nju ejdža maskiran kao univerzitet, biznis maskiran kao iskupljenje, slogani maskirani kao istine.“[9]

U svetlu iznetog, osnovni preduslov za smislenost ovog istraživanja je odrediti pravi nivo apstrakcije na kome će se govoriti o internetu. To će se postići korektnim izdvajanjem glavnih sastavnih delova tehničkog sistema, da bi se kasnije sagledala njihova dinamika tj. kontinutiet ili diskontinuitet u dosadašnjem životu interneta.

Cilj istraživanja, metod istraživanja, osnovna pitanja

Iako internet ima istoriju kraću od 50 godina, svedoci smo da dizajn interneta kontinuirano prolazi kroz promene, čija priroda se odražava na ključne parametre ove mreže mreža. Cilj ovog istraživanja jeste rasvetljavanje dizajna interneta i implikacije

[8] Evgeny Morozov. (2. okt. 2013).„How to Stop a Sharkando“ *Die Zeit* Dostupan na http://www.zeit.de/digital/internet/2013-10/morozov-sharknado-chomsky-foucault

[9] Michael Meyer “Evgeny versus the Internet” *Columbia Journalism Review* January/February 2014. Dostupan na http://www.cjr.org/cover_story/evgeny_vs_the_internet.php?page=all\

koje iz ovog dizajna proizlaze na moralno, političko, pravno i, u meri u kojoj to ima filozofski ili etički značaj, ekonomsko stanje savremenog sveta. Implikacije dizajna interneta sadrže aspekte kao što su redistribucija moći, domet kontrole i ograničenje ljudske slobode, koje imaju potencijalno negativan moralni učinak, a takođe i aspekte koji se zbirno mogu podvesti pod kapacitet za dobro, koji načelno vodi unapređenju osnovnih moralnih vrednosti slobode, privatnosti i jednakosti šansi.

Saobraćaj u mreži kreće i zavisi od inputa učesnika, korisnika, „krajeva“, što podrazumeva značajnu etičku tezu da su „krajevi“ *prima facie* suvereni i imaju prioritet u dizajnu mreže, da je mreža tu zbog njih. No, činjenica je da sama infrastruktura mreže, „sredina“, vrši manji ili veći uticaj na saobraćaj i sudara se sa tom suverenošću „krajeva“. U „sredini“ mogu da se postave ili pojave barijere saobraćaju, prema odlukama provajdera, kontrolora, zaštitnika viših interesa, cenzora, razbojnika, lopova ili terorista; svaki od njih, svojim učešćem u distribuciji moći i u pretenzijama na opravdanost interesa koji stoje iza te moći, vrši dizajniranje mreže. Kako u slučaju „krajeva“, tako i u slučaju „sredine“ i „onih iz sredine“, treba ispitati kakva je moć u pitanju i kako ta moć može da se opravda (postoji li njen legitimitet).

Metod koji se koristi u istraživanju je prilaz sa više strana ovom višedimenzionom fenomenu. Metod istraživanja je složen, tako da obuhvata: istraživanje relevantne literature, filozofsku analizu argumenata nađenih u toj literaturi, pronalaženje relevantne veze sa klasičnim tekstovima iz istorije filozofije i velikim etičkim teorijama, istraživanje i lični uvid u stvarno stanje interneta / na internetu, kao i studiju slučaja za dodatno razvijanje argumenata na osnovi empirijskih nalaza.

U ovom istraživanju se traži odgovor na pitanje: kako filozofski odrediti i moralno vrednovati internet 2015. godine?

Ono se razlaže na sledeća potpitanja:

1. Koje su osnovne komponente interneta kao tehničkog sistema?
2. Šta je sadržavala i sadrži arhitektura interneta kao tehničkog sistema?
3. Šta se dešava kada (više) nema arhitekture interneta ali ima interneta?
4. Kakvo je upravljanje internetom danas?
5. Kako internet intereaguje sa prostornim fenomenima?
6. Kako internet intereaguje sa komercijalnom/ekonomskom sferom života?
7. Kakva je pozicija na internetu koja pripada običnom korisniku?

Svakom od ovih pitanja posvećeno je zasebno poglavlje rada. S obzirom na implikacije koje proizlaze iz pozicije običnog korisnika interneta, koje nisu samo

manifestovane kao dobici za njega kao moralno autonomog subjekta, građanina i učesnika političke javne sfere, kulturno biće i ekonomskog aktera, nego na žalost podrazumevaju i gubitke, prvenstveno gubitak privatnosti, bilo je potrebno, nakon poglavlja o korisnicima, još jedno zasebno poglavlje čiji fokus je na privatnosti korisnika i mogućim odnosima prema njoj. Tu je tražen odgovor na pitanje:

8. Kakva je zaštita ličnih podataka na internetu?

Pokazuje se da ne samo da države mogu preduzeti dosta toga da osiguraju zaštitu privatnosti, nego to može i individualni korisnik, ako to želi. Masovni nadzor na internetu može se zaustaviti pod uslovom da korisnik odluči da se bori protiv nadzora koji nad njim vrše države i kompanije. Ključ zaustavljanja masovnog nadzora na internetu nalazi se u preuzimanju odgovornosti za sebe od strane običnih korisnika interneta.

U zaključku je konstatovano da internet treba koristiti, njegove dobre strane treba ugraditi u sopstvene životne izbore i životni stil, kao i u društvo čiji smo deo. Njegova loša strana, pretvaranje komunikacione tehnologije u tehnologiju za masovni nadzor, ne sme nas prepasti i zbuniti. Osnovna svrha ovog rada bila je davanje podloge za podizanje svesti o ulozi koju bi sami korisnici trebalo da odigraju u odnosu na nadzirani internet.

PRVO POGLAVLJE

Ključne komponente interneta kao tehničkog sistema

Internet je mreža kompjuterskih mreža, gde se u novije vreme umrežavaju i ostali uređaji. Interneta ne bi bilo bez kompjutera i razvoj interneta je tesno povezan sa razvojem kompjutera. Veoma dobra analiza o paralelnim tokovima evolucije interneta i evolucije kompjutera nalazi se u knjizi Džonatana Zitrejna *Budućnost interneta*.[10] No, kompjutere ćemo ostaviti po strani kad je reč o ključnim komponentama interneta. Internet ili mreža kompjuterskih mreža je kreiran za saobraćaj ili transfer digitalnih informacija spakovanih u tzv. pakete podataka. Suštinske komponente te mreže, koje srećemo u literaturi još i pod nazivom osnovna ili ključna infrastruktura interneta, koje možemo smatrati nužnim i dovoljnim uslovima interneta, su:

- Protokol kontrole transfera/internet protokol, skraćeno TCP/IP;[11]
- Sistem imena domena, skraćeno DNS;[12]
- Autonomni sistemi i protokol rutiranja, skraćeno AS i BGP[13].

Vidimo da se ponavlja reč protokol. Protokoli su kompjuterski kodovi tj. softverska uputstava koji služe izvršavanju funkcije za slanje podataka kroz mrežu. Kompjuterske mreže iz celog sveta međusobno komuniciraju na bazi ovih protokola koji su definisani, javni, besplatni, i dobrovoljno i univerzalno prihvaćeni. Umrežavanje kompjuterskih mreža (i samih kompjutera u mrežama) u vreme nastanka ovih kodova nije ni u kom smislu imalo u vidu epitet "globalno". Kao što ćemo videti, to se desilo tek nekih 20ak godina nakon stvaranja interneta. Međutim, može se smatrati da su protokoli od početka koncipirani tako da u principu tj. potencijalno daju jednu univerzalnu globalnu mrežu.[14]

---

[10] Jonathan Zittrain. (2008). *The Future of the Interne and How to Stop Itt*, New Haven & London, Yale University Press, Dostupno na http://futureoftheinternet.org/

[11] U daljem tekstu koristiće se skraćenica (od engl. Transfer control protocol/Inernet protocol).

[12] U daljem tekstu koristiće se skraćenica (od engl. Domain name system).

[13] U daljem tekstu koristiće se skraćenice (od engl. Autonomous systems, Border gate protocol).

[14] O prednostima TCP/IP može se reći da je on od samog početka bio otvoreni protokol dostupan svima, razvijen nezavisno od specifičnog operativnog sistema ili kompjuterske platforme, tako da može da radi na svim vrstama sistema i platformi. Druga prednost je bila to što je pogodan za transport podataka kroz mrežu bez obzira na heterogenost mreža. On je minimalan, pa je moguće prilagodi mu ostale slojeve. „Neinsistiranje na nekoj specifičnoj varijanti lokalnih mreža omogućilo je da se za potrebe formiranja interneta koriste najrazličitiji telekomunikacioni sistemi ... Izbegavanje prevelikog mešanja u prirodu podataka koji se prenose obezbedilo je veliku slobodu kreatorima aplikacija ...", a to je dovelo do stvaranja raznovrsnih aplikacija odnosno servisa, što je korišćenje interneta učinilo zanimljivim najrazličitijim korisnicima. Bojan Živković, „NJ.V.Internet" *Svet kompjutera* 4/12. Dostupno na http://www.sk.co.rs/2012/04/sksc01.html

Najkraće objašnjenje zašto je internet postao globalna mreža glasi da su tome doprinele aplikacije[15]. Pod aplikacijama se misli (kao i kod osnovnih protokola) na neke kodove tj. softverska uputstva koja međutim služe za izvršavanje funkcije za interakciju čoveka i kompjutera. Naročito uspešne aplikacije, kao što su www (HTML), elektronska pošta, transfer fajlova, pregledači (brauzeri), igrice, elektronska trgovina, internet telefonija i dr., su vremenom postale sinonim interneta. Međutim to izjednačavanje je pogrešno. Internet je u stvari temeljna infrastruktura zahvaljujući kojoj su aplikacije moguće. Broj aplikacija u momentu nastanka interneta je bio minimalan, da bi se danas izražavao stotinama hiljada. Stvaranje aplikacija odvijalo se slobodno, neograničeno i nedirigovano, tako da su neke aplikacije nastale kao ishod amaterske akcije, hobija, a neke kao komercijalno razvijen proizvod. Aplikacije su ono što je privuklo najrazličitije korisnike na Internet i tako posredno doprinele njegovoj ekspanziji i omogućile prednosti opšte umreženosti.

DNS najjednostavnije treba shvatiti kao telefonski imenik za internet. Da bi neka mreža mogla da postoji i razmenjuje saobraćaj sa drugim mrežama, i ona i oni moraju biti u DNS-u. Bez DNS-a paketi se ne bi mogli slati, jer im se ne bi znali ni pošiljalac ni primalac, a ne bi se mogla odrediti ni putanja kroz mrežu mreža.

Internet je globalna ali decentralizovana mreža mreža. Mreže koje čine internet nazivaju se precizno u tehničkom kontekstu autonomnim sistemima (AS), a to ime dolazi od njihove autonomnosti u politici rutiranja (koje se vrši protokolom tj. BGP). Politikom rutiranja mreža određuje koji paketi koji dolaze van nje će prolaziti kroz nju. Saobraćaj se obavlja tako što mreže sarađuju i jedne drugima prenose saobraćaj.

Uz ove tri ključne komponente interneta, treba dodati još dve, koje nisu postojale u najranijim fazama razvoja interneta već su se formirale zbog širenja interneta, njegove komercijalizacije i povećanja broja korisnika. One se najčešće ne navode kao osnovna infrastruktura, ali u ovom radu stojim na stanovištu da su i one danas nužni i dovoljni uslovi interneta. One su entiteti presudni za vezu između korisnika i interneta.To su:

- Pružaoci ili provajderi internet usluga, skraćeno ISP[16] i
- Regionalni internet registri, skraćeno RIR[17].

[15] Termin dolazi iz engleskog jezika, gde apply znači primeniti. U slobodnom tumačenju, aplikacije su ono što daje primenu kompjutera u svim za čoveka bitnim operacijama. Na pr. aplikacija za fotografije omogućava da korisnik formatira ili retuširа fotografiju na kompjuteru, aplikacija za e-banking omogućava da korisnik sa svog računa u banci obavi novčanu transakciju preko kompjutera bez odlaska u banku.

[16] U daljem tekstu koristiće se skraćenica (od engl. Internet service provider).

[17] U daljem tekstu koristiće se skraćenica (od engl. Regional internet registry).

ISP-ovi imaju ulogu posrednika preko koga korisnici ulaze na internet. Osim pružanja usluge priključenja na internet, mogu pružati i druge usluge kao što su registracija i hostovanje veb sajtova i dr. Jedan ISP može biti jedna mreža a može u sebi sadržati više mreža. ISP može biti identičan sa autonomnim sistemom, ali ne mora.

Regionalni internet registri ili RIR-ovi su udruženja velikih mreža tj. udruženja AS-ova ili ISP-ova na nivou kontinenata, i ima ih pet. Važni su jer se staraju za internet brojeve koje koriste AS-ovi, koji se tretiraju kao ograničeno javno dobro. Sami ISP-ovi ili AS-ovi ne bi mogli obaviti tu funkciju, niti bi to mogla da urade tela koja upravljaju internetom, tako da RIR-ovi moraju biti uključeni u ključnu tehničku infrastrukturu interneta.

Ovim se iscrpljuje lista ključnih tehničkih komponenti interneta. Čime branim tu tezu? Time da se ovaj rad odnosi na internet kao mrežu a sadejstvom ovih pet elemenata nastaje mreža. Internet nije nepromenljiv tehnički sistem. Svaki tehnički sistem (pa tako i internet) se može menjati u izvesnoj meri, i pri tome ostati ono što jeste. Ovde ćemo se baviti višestrukim promenama koje su se odgirale sa internetom tokom dosadašnjih 40-ak godina njegovog postojanja. Takođe ćemo pokuštati da tematizujemo količinu i prirodu promena koje internet može podneti a da ostane to što jeste, odnosno gde je krajnja granica iza koje internet postaje nešto drugo. U tom duhu, zamislivo je dodavanje šeste, sedme itd. ključne komponente interneta, ali trenutno one ne postoje. Fenomen globalne mreže mreže zasnovan je baš na ovih pet.

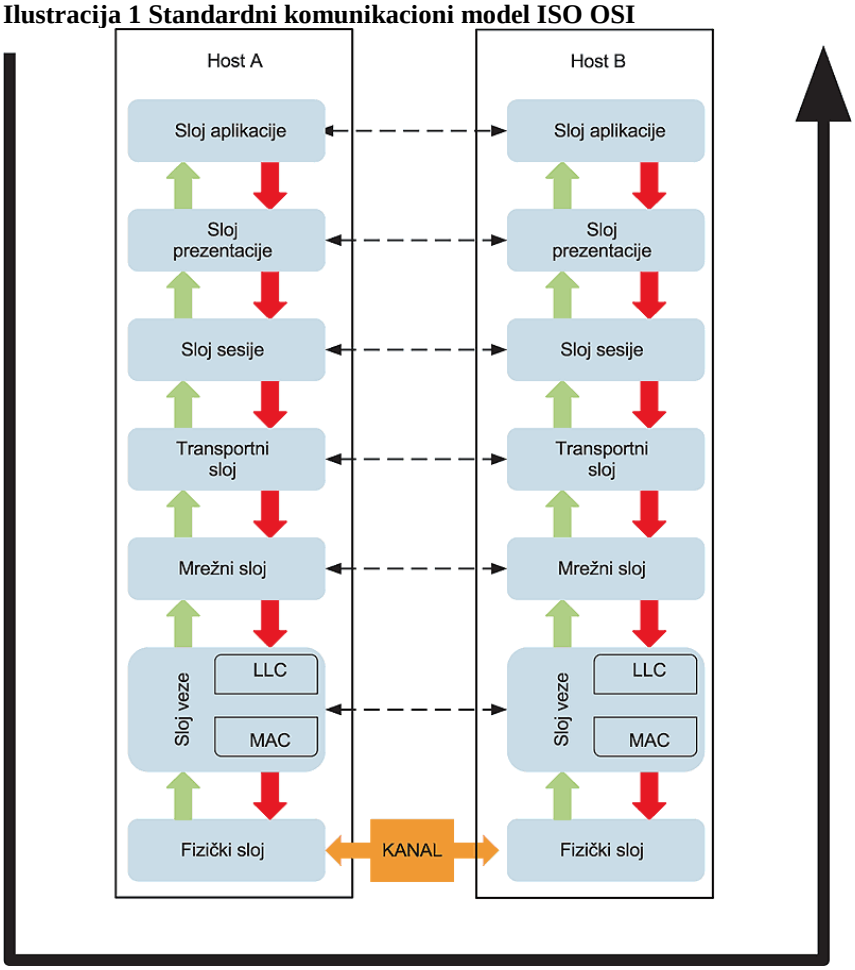
Internet kao komunikacioni sistem određuje se kao varijanta modela komunikacionog sistema koji je dala Međunarodna organizacija za standardizaciju ISO OSI (zvanično usvojenom 1988. god.). Odnos osnivača interneta prema ovom modelu izložen je u RFC 871[18] „Pogled na ARPANET referentni model“ iz 1982. godine. Detaljan prikaz ova dva modela izlazi iz okvira ovog rada, ali ono najkraće što se može reći je da model komunikacionog sistema služi opisu «principa po kojima se komunikacioni sistemi projektuju i načina na koji se sama komunikacija obavlja».[19] U komunikacionom modelu, komunikacija se analizira preko slojeva. «Sami slojevi ... predstavljaju aspekte sa kojih je potrebno posmatrati problem prenosa podataka kako bi se realizovao sistem koji će ga obavljati.»[20]

[18] RFC 871 “A Perspective on the ARPANET referene model” http://tools.ietf.org/html/rfc871
[19] Bojan Živković, „Raslojavanje“, *Svet kompjutera* 3/2012 http://www.sk.rs/2012/03/sksc01.html
[20] Živković, opus cit.

Po modelu ISO OSI, podatak se od jednog do drugog uređaja (nazovimo ih A i B) prenosi kroz 7 vertikalno poređanih slojeva. Svaki sloj može biti „svestan“ samo svog protokola i samo podataka koje sam proizvodi i interpretira. Podela na slojeve služi tome da se slojevi mogu izolovati odnosno sagledati akcije u svakom od njih. U ovom modelu se tok komunikacije razdvaja na horizontalnu i vertikalnu komponentu. Horizontalno komuniciranje označava da svaki sloj komunicira isključivo sa svojim parnjakom na drugom kraju kanala. Vertikalno komuniciranje označava da svaki sloj koristi usluge nižeg sloja i svaki sloj pruža uslugu višem sloju. Razmenu između slojeva omogućava princip enkapsulacije. Podaci višeg sloja predstavljaju „crnu kutiju“ koju treba zapakovati u format svog sloja i proslediti nižem sloju, bez ikakvog ispitivanja njenog sadržaja.

Standardni model ISO OSI prikazan je na ovom dijagramu:

Ilustracija 1 Standardni komunikacioni model ISO OSI



Preuzeto sa http://www.sk.rs/2012/03/sksc01.html

U modelu interneta najbitniji slojevi su mreža i transport, koji su rešeni sa TCP/IP. Sve iznad TCP/IP preuzima jedna sloj, popularno nazvan „debeli aplikacioni sloj“ (koji sadrži slojeve sesije, prezentacije i aplikacije). U aplikacionom sloju se smeštaju neki od najvažnijih protokola, kao što su oni za automatsku konfiguraciju hostova, razrešavanje imena hostova, upravljanje radom hostova. (Pod hostom se misli na host kompjuter, kompjuter primatelj.) U modelu interneta, autor aplikacije je taj koji nosi odgovornost za sve: od načina prezentacije, preko provere ispravnosti do obezbeđivanja perzistentnosti podataka između više sesija. [21]

Ilustracija 2 Razlike između slojeva kod modela interneta i modela OSI.

Internet	vs.	OSI Model
Aplikacija	Sloj 7	Aplikacija
	Sloj 6	Prezentacija
	Sloj 5	Sesija
Transport	Sloj 4	Transport
Mreža	Sloj 3	Mreža
Pristup mreži	Sloj 2	Veza
	Sloj 1	Fizički kanal

Preuzeto sa http://www.sk.rs/2012/03/sksc01.html

Način nastanka suštinskih komponenata interneta (TCP/IP, DNS, AS i BGP, ISP, RIR)

Upotreba TCP/IP u projektovanju kompjuterskih mreža je počela da se širi u SAD sredinom 1980-tih godina (početak primene je zvanično 1.1.1983. god. u ARPANET[22] – prvoj mreži koja se smatra pretečom današnjeg interneta), i tokom samo jedne dekade je postao unverzalan do mere da su konkurentski protokoli prestali da se primenjuju. Ovaj set protokola je "opstao" delom i zato što je (odlukom proizvođača) bio ugrađen u operativne sisteme prvih kompjutera, tako da je kupac kompjutera već u startu mogao da ide na mrežu na taj način.

[21] Bojan Živković, „NJ.V. Internet“ *Svet kompjutera* 4/2012. Dostupno na http://www.sk.rs/2012/04/sksc01.html

[22] ARPANET – Advance Research Projects Agency's Network

Protokol TCP su kreirali američki naučnici Robert Kan i Vinton Cerf. Prvi put su svoju ideju izložili u naučnom članku "Protokol za interkonekciju paketnih mreža"[23] napisanom 1973. Njihova zamisao je bila da se poruke enkapsuliraju i dekapsuliraju i da postoje posebni kompjuteri tzv. ruteri (gateways) koji bi mogli da čitaju samo te kapsule, dok bi sadržaj poruke (ono što je u kapsuli) čitali kompjuteri primatelji (hosts). Taj sistem razmene poruka liči na sistem kontejnerskog transporta – kontejner može biti napunjen bilo čime, ali nosi standardni dokument u kome stoji adresa primatelja i druge za transport bitne informacije, dok se transport kontejnera može vršiti brodom, vozom, kamionom i sl. TCP je nakon prve specifikacije doživeo više promena.[24] Morao mu je 1978. god. biti dodat drugi protokol poznat kao IP, te je bila ustanovljena podela posla između dva protokola: IP brine za rutiranje paketa, a TCP za nastanak paketa, kontrolu greške, retransmisiju i asembliranje paketa. Danas se oba protokola smatraju celinom. Sam IP je doživeo više varijanti, a danas su paralelno u primeni verzija 4 i verzija 6, odnosno IPv4 i IPv6.

Kako je sam Cerf opisao,[25] do „otkrića" TCP/IP stiglo se kroz izvesnu predistoriju. Naime 1968. god. je Agencija za napredne istraživačke projekte Ministarstva odbrane SAD (DARPA) želela da isproba da li je moguća mreža bazirana na tehnologiji razmene paketa (packet switching) - za razliku od tada rasprostranjenih tehnologija vezivanja kola (circuit switching) i razmene poruka (message switching)[26] Na konkursu raspisanom za razvoj komunikacionog sistema na osnovama razmene paketa jedna mala firma BBN (Bolt Beranek and Newman) iz Masačuseca je dobila priliku da takav sistem napravi i isporuči, što je ona i uradila. Stručnjaci iz istraživačkih laboratorija velikih telefonskih kompanija u tom trenutku su smatrali da takav sistem praktički nije održiv. Testiranja mrežne komunikacije na osnovi razmene

[23] Vinton G. Cerf and Robert E. Kahn "Protocol for Packet Network Intercommunication" http://www.cs.princeton.edu/courses/archive/fall06/cos561/papers/cerf74.pdf (Reprinted with permission from IEEE Trans on comms, Vol Com-22, 5 May 1974)

[24] Lee A. Bygrave and Jon Bing, eds. (2009). *Internet Governance: Infrastructure and Institutions*, New York, Oxford University Press. Str. 26. (U daljem tekstu *Internet Governance*)

[25] Vinton G. Cerf, *Computer Networking: Global Infrastructure for the 21st Century*, dostupno na http://homes.cs.washington.edu/~lazowska/cra/networks.html

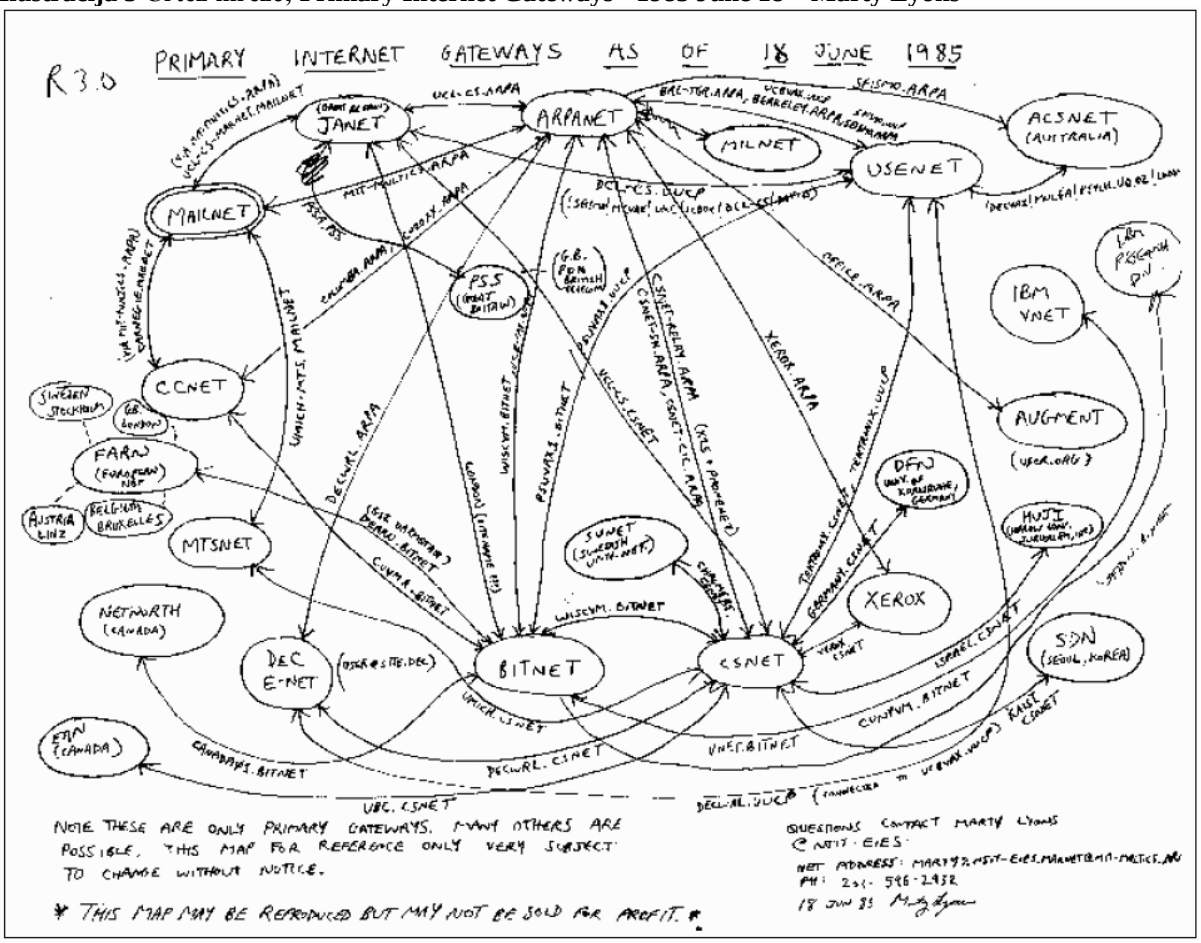
[26] Ideja o tehnologiji razmene paketa bila je poznata i pre 1968. god. ali tek je primena u praksi dovela do toga da na naučnici počnu da rade na njoj i da se dođe do više verzija TCP/IP, od kojih je najbolja zaživela. «U sistemu razmene paketa, podaci koje treba preneti razbijaju se u male delove kojima se stavlja nalepnica koja govori odkud dolaze i kuda treba da idu, prilično nalik poštanskim dopisnicama. Kao kod dopisnica, paketi imaju maksimalnu dužinu (1024 bita – prim. aut.) i nisu nužno pouzdani. Paketi se predaju od jednog kompjutera drugom dok ne stignu na svoje odredište. Ako se neki izgubi, pošiljalac ga ponovo šalje. Primalac potvrđuje prijem paketa da bi se eliminisale nepotrebne ponovne transmisije.» Cerf, opus cit.

paketa (i uređaja nazvnog IMP) izvršena su 1969. god. kada je najpre između kompjutera Univerziteta Kalifornija u Los Anđelesu i Istraživačkog instituta Stanford u Palo Altu razmenjena prva poruka, nakon čega su mreži dodati i Univerzitet Kalifornija u Santa Barbari i Univerzitet Juta. Sistem je prvi put javno (i uspešno) demonstriran na prvoj međunarodnoj konferenciji o kompjuterskim komunikacijama oktobra 1972. To je uverilo skeptike da ova tehnologija može biti održiva. Na javnoj demonstraciji sistema 1972. god. u ARPANET je bilo 24 kompjutera lociranih u raznim institucijama u SAD-u. Sama ARPANET mreža postojala je od 1969. do 1989. kada je ugašena jer su je zamenile druge mreže (NSFNET, UUCPNET itd.).

Od 1973. mreži su dodavani i računari izvan SAD-a, locirani na institucijama u Velikoj Britaniji, Norveškoj, Švajcarskoj, Japanu. Izgled mreže u 1985. god. - mreže koju tada već slobodno možemo zvati internetom - prikazuje mapa koju je nacrtao Marti Lajons[27] na jednom listu papira formata A4. Svaki krug na njegovom crtežu kao čvorište (primary gateway, danas bi se nazvalo ruter) označava jednu kompjutersku mrežu, pri čemu su vlasnici tih umreženih mreža, osim američke vojske i univerziteta, takođe i privatne firme, proizvođači hardvera i softvera, na primer IBM, XEROX, zatim ISP-ovi, na primer Bitnet itd. To je sam početak povezivanja u veliku javnu mrežu mreža, koje će se potom vrtoglavo ubrzati.

[27] Navedeno prema http://www.livinginternet.com/i/ii_arpanet_gateways.htm

Ilustracija 3 Crtež mreže; Primary Internet Gateways - 1985 June 18 – Marty Lyons



Preuzeto sa http://www.livinginternet.com/i/ii_arpanet_gateways.htm

Ovaj crtež govori da je već u to vreme internet privukao pažnju brojnih i raznolikih aktera, koji su uskoro uveliko tragali za načinima eksploatacije mogućnosti koje su se sa internetom ponudile.[28] U to prvo vreme bile su moguće dve vrste aktivnosti na

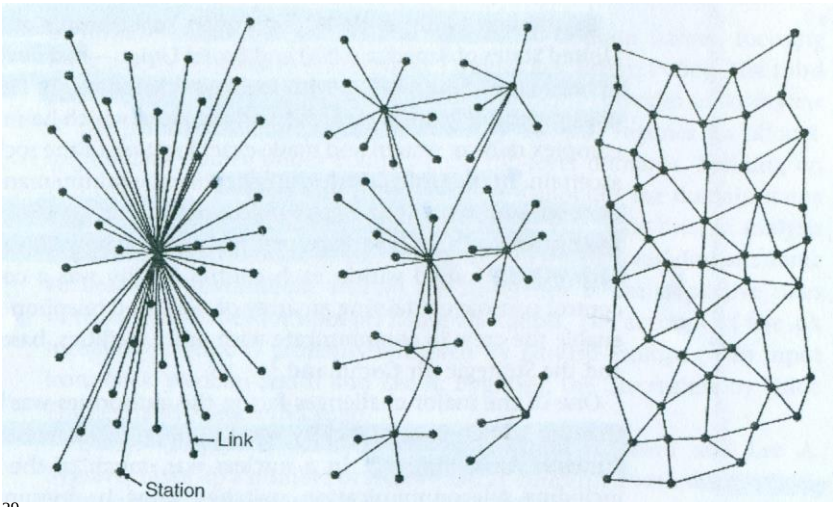
[28] Treba napomenuti da je prvobitna zamisao zbog koje se pošlo u ispitivanje mreže na bazi razmene paketa bila inspirisana primenom eventualne takve mreže u vojne svrhe. Pol Baran, Amerikanac poljskog porekla, zaposlen u RAND korporaciji radio je na problemu komunikacije između lansirnog mesta interkontinentalne rakete i centralne vojne komande u uslovima nuklearnog rata. Predložio je da je rešenje tog problema distribuirana mreža, razbijanje poruke u standardne blokove i algoritam za efikasno upućivanje blokova poruke kroz mrežu. Kasnije su se Baranovoj zamisli o mreži na bazi razmene paketa iz 1964. god. vratili naučnici okupljeni na kreiranju ARPANET-a. *Internet Governance*, str. 10-12. Ilustracija tri vrste mreža – centralizovane, decentralizovane i distribuirane, iz istog izvora, izgleda ovako:

mreži: telnet – mogućnost daljinskog obavljanja operacija (s jednog na drugom računaru) i transport fajlova (zahvaljajući protokolu transporta fajlova, skraćeno FTP[29]), što je bilo u skladu sa njenom osnovnom namenom, da se kompjuteri na univerzitetima racionalno koriste za naučna istraživanja (takozvano vremensko deljenje kompjutra). Međutim, naučnih istraživanja je manjkalo, pa je neko primetio: „Mreža je u to vreme bila opisivana kao jedna impresivna katedrala kojoj su falili vernici“.[30]

To se promenilo onog časa kada je Rej Tomilnson (iz firme BBN) napravio prvi program za elektronsku poštu. Ovaj program je u mrežu privukao mase koje su zavolele pisanje emailova. Još veći broj korisnika se priključio internetu sa primenom HTML-a, programskog jezika za kreiranje i prikazivanje materijala okačenog na internetu tzv. internet stranica (vebsajtova) kao i sa uvođenjim prvih „šunjača“ i pretraživača (crowlers, browsers) koji su stvorili lak pristup sadržaju postavljenom na internet stranicama. Tada je i reč šetnja intenetom – surfovanje internetom – počela da dobija smisao. Iz tih zametaka ubrzo je izrasla čitava internet industrija.

Ono što treba takođe uočiti na crtežu Martija Lajonsa je da su sva čvorišta imenovana. Drugačije se može reći da su akteri u mreži imali svoje jedinstvene domene. Kao što interneta ne bi bilo bez opšteg prihvatanja TCP/IP, tako ga ne bi bilo ni bez funkcionalne jednoznačnog sistema imena domena na nivou mreže mreža.

Vrlo rano je uočeno da je za razvoj mreže mreža nužno da svaki učesnik u mreži dobije svoju adresu i ime tj. domen. U tom cilju tri naučnika Jon Postel, Pol Mokapetris i Kreg Partridž kreirali su 1983. god. sistem imena domena (DNS) koji je



[29] U daljem tekstu koristiće se skraćenica (od engl. File transport protocol).
[30] *Internet Governanc*, str. 29.

bio u opštoj primeni od 1986. god. DNS povezuje međusobno imena domena i IP brojeve. Imena domena i internet protokol brojeve (IP brojeve) u jedinstvenu listu HOSTS.TXT ubacivao je sam Jon Postel na svom institutu gde je radio (Univerzitet Južna Kalifornija) i to u ime IANA, tela koje je tek neformalno postojalo. IANA je bilo neformalno telo koje se svodilo na jednu osobu – samog Postela. On je to radio do svoje smrti 1998. godine. Funkcije IANA preuzeo je 1998. godine ICANN[31] koji se i danas time bavi. Ažuriranje fajla HOSTS.TXT je jedna od centralnih funkcija za funkcionisanje interneta jer u ovom fajlu se sažima raspodela globalno jedinstvenih imena i brojeva korišćenih u internet protokolima.

Adresa internet protokola (IP adresa) ili internet broj služi za identifikaciju uređaja koji inicira komunikaciju i uređaja destinacije sa kojom želi da komunicira, omogućujući dvosmernu komunikaciju među njima. Ovaj broj (32-bitni broj u IPv4, odnosno 128 bitni broj u IPv6) se dodeljuje svakom uređaju koji učestvuje u kompjuterskoj mreži koja koristi internet protokol. Radi se o binarnim brojevima (nizovima cifara 0 i 1) koji se skladište u glavnom text fajlu i prikazuju u numeričkoj varijanti čitljivoj ljudima. Primeri IP adrese po IPv4 su 37.19.108.19 ili 178.254.184.67 (dakle, četiri broja u rasponu od 0 do 255 povezanih tačkom), a po IPv6 je 2001:0db8:85a3:0042:1000:8a2e:0370:7334 (dakle, osam grupa po četiri heksadecimalnih cifara[32] povezanih sa dve tačke).

Prema IPv4 može postojati oko 4,3 milijardi IP adresa, i budući da broj korisnika interneta sve više raste, moguće je da dostupne adrese budu iscrpljene. Stoga se javila potreba za prelaskom na IPv6, no do sada potpuni prelazak nije završen.[33] Do momenta punog prelaska na novi IPv6, oba protokola su u primeni tako što se novi «tunelira» u starom.

Sva imena domena su prevodi IP adresa iz numerčkog oblika u semantičku formu odnosno u označivač koji je ljudima lakše da zapamte. Još jedna prednost imena domena je u stabilnosti referencije, pošto IP adrese mogu da se menjaju. Međutim, imena domena nisu neophodna za saobraćaj na internetu, dok IP adrese jesu.

---

[31] ICANN će biti detaljno objašnjen u Pogljavlju 4.

[32] Heksadecimal je pozicioni numerički sistem koji koristi 16 različitih simbola i to: 0-9 i A, B, C, D, E, F koji označavaju vrednost od 10 do 15.

[33] Početak prelaska sa IPv4 na IPv6 bio je 6.6.2012. god. Međutim, do danas je tek manji procenat provajdera izvršio taj prelazak. Statistika je dostupna na http://www.ipv6actnow.org/info/statistics/ Razlog za slab odziv i interes za prelaskom nije samo taj što za sada IP adresa ima dovoljno u odnosu na potražnju već postoje i politički razlozi. To ne menja činjenicu da svaki uređaj mora imati IP broj da bi bio na internetu.

Kroz RFC 882 „Imena domena – pojmovi i ustanove“[34] iz 1983. godine (koji je kasnije zamenjen drugim RFC-om, uz čuvanje osnovnih ideja), Postel, Mokapetris i Partridž su predložili da imena domena:

- budu formirana po principu granjanja (polazeći s desna na levo od opšteg ka posebnom),
- moraju imati barem dva nivoa (primarni i sekundarni), koja se razdvajaju tačkom,
- budu formirana uz pomoć 37 karaktera, od čega 26 slova,[35] 10 cifara i simbola crtica „-„ koji ne može biti prvi niti zadnji u imenu domena i
- ne mogu biti sastavljena od samo jednog karaktera.

Takođe su ustanovili sedam primarnih domena (u daljem tekstu ćemo ih zvati: top level domeni), i to: .edu, .com, .gov, .mil, .net, .org i .int kao i primarne domene prema skraćenicama za imena država (u daljem tekstu ćemo ih zvati: domeni za zemlje). Svaki domen se svrstavao u jednu od ovih opštih kategorija odnosno završavao se jednim od ovih primarnih domena. (Jedan top level domen koji je specifičan i van ove podele je .arpa[36].) Broj primarnih domena se vremenom povećavao.

Sekundarni i ostali domeni su ostavljeni slobodi korisnika, tj. korisnici mogu birati naziv, dužinu domena tj. broj karaktera. Zavisno od broja karaktera u imenu, broj mogućih kombinacija karaktera (mogućih imena domena) se povećava, 37^2, 37^3, 37^4 – s tim da teorijski on nikada nije neograničen. Celokupan popis primarnih domena nalazi se na www.iana.org (Ovde dajemo primere nekih imena domena: www.mb.com ili www.b92.net ili www.osce.org ili www.mfa.gov.rs ili www.f.bg.ac.rs itd.)

Fajl HOSTS.TXT odnosno središnji fajl svih registara primarnih domena prema kome se svi korisnici interneta orijentišu, takozvani telefonski imenik za internet, od početka se fizički nalazio na Postelovom kompjuteru tj. serveru kao i na još nekoliko

[34] RFC 882 “Domain Names – Concepts and Facilities” http://tools.ietf.org/html/rfc882
[35] U vreme kreiranja DNS-a nije postojao interes za druge alfabete osim onog u engleskom jeziku. Međutim, od 1998. god. u primeni je aplikacija za internacionalizaciju imena domena. Ova aplikacija služi tome da se imena domena napisana alfabetima korišćenim u arapskom, persijskom, kineskom (starom i novom), ruskom, hindi, grčkom, korejskom, jidiš, japanskom i tamilskom jeziku prevedu na alfabet engleskog jezika.
[36] *Internet Governance*, str. 148.

drugih (to su bile kopije). Danas status glavnih servera ima 13 servera koji se nalaze širom sveta, i oni se nazivaju autoriteti ili rut serveri.[37]

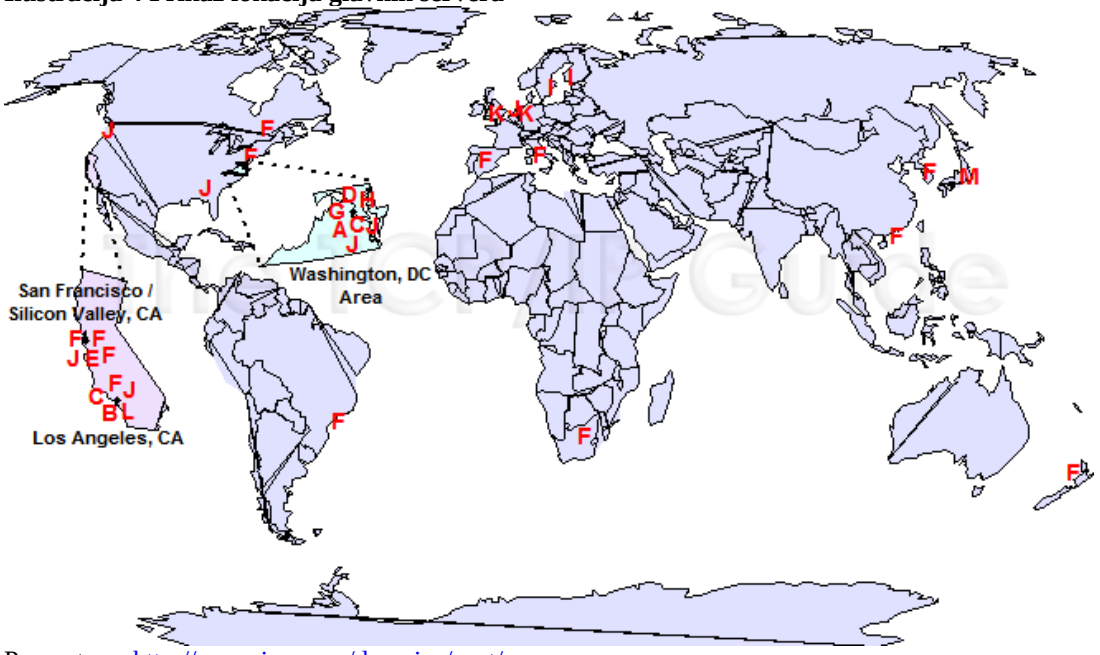
Tabela 1 Lista 13 glavnih servera

Ime kompjutera	IP adresa	Menadžer
a.root-servers.net	198.41.0.4, 2001:503:ba3e::2:30	VeriSign, Inc.
b.root-servers.net	192.228.79.201	University of Southern California (ISI)
c.root-servers.net	192.33.4.12, 2001:500:2::c	Cogent Communications
d.root-servers.net	199.7.91.13, 2001:500:2d::d	University of Maryland
e.root-servers.net	192.203.230.10	NASA (Ames Research Center)
f.root-servers.net	192.5.5.241, 2001:500:2f::f	Internet Systems Consortium, Inc.
g.root-servers.net	192.112.36.4	US Department of Defence (NIC)
h.root-servers.net	128.63.2.53, 2001:500:1::803f:235	US Army (Research Lab)
i.root-servers.net	192.36.148.17, 2001:7fe::53	Netnod
j.root-servers.net	192.58.128.30, 2001:503:c27::2:30	VeriSign, Inc.
k.root-servers.net	193.0.14.129, 2001:7fd::1	RIPE NCC
l.root-servers.net	199.7.83.42, 2001:500:3::42	ICANN
m.root-servers.net	202.12.27.33, 2001:dc3::35	WIDE Project

Preuzeto sa http://www.iana.org/domains/root/server

Kao što se vidi, samo tri glavna servera - i, k i m - ne nalaze se geografski u SAD već u drugim zemljama; glavni server i se nalazi u Švedskoj i Finskoj, glavni server k se nalazi u V.Britaniji i Holandiji i glavni server m se nalazi u Japanu. Glavni server f se nalazi u 9 zemalja od čega je jedna SAD.

Ilustracija 4 Prikaz lokacija glavnih servera



Preuzeto sa http://www.iana.org/domains/root/server

[37] Detalji preuzeti sa http://www.iana.org/domains/root/servers

Glavni serveri su međusobno nezavisni. Međutim, od 13 glavnih servera prvi među jednakima tj. prvi server, krajnji autoritet za internet (nekadašnji Postelov server) je u Los Anđelesu pod okriljem kompanije Verizajn (VeriSign). Za brigu o tom serveru ova kompanija ima ugovor sa Vladom SAD. Ovi autoritativni serveri se kopiraju na druge (iz praktičnih razloga, blizine korisnika i sl.) tako da je juna 2013. broj tih kopija glavnih servera dostigao blizu 400. Detalji za usmerenost svake zemlje ka nekom od servera mogu se naći na internet stranici http://root-servers.org/

Većina operatera glavnih servera se drži filozofije i tradicije distribuiranog autoriteta na internetu, tj. smatra da je nezavisnost operatera glavnih servera zdrava za internet. Operateri glavnih servera sebe definišu kao «različite profesionalne inžinjerske grupe» koje nisu uključene u kreiranje politika ili modifikacije podataka – oni samo objavljuju (bez uređivanja) fajl rut zone i odgovaraju na pitanja u vezi toga.[38] U tome su oni dosta različiti od ICANN, koji je u vršenju IANA funkcije, pretvoren u mesto susreta između tehničke koordinacije i javne politike.[39]

Internet je decentralizovana mreža mreža koje su međusobno (fizički) povezane. Mreže koje čine internet nazivaju se autonomni sistemi (AS). U 2012. god. bilo je preko 42.000 autonomnih sistema (1999. god. preko 5.000). Svaki AS ima svoj broj (prefiks)[40] i izvesnu količinu IP adresa koje su mu dodeljenje od strane ICANN. IP adresa nije vlasništvo AS-a već mu se samo ustupa na korišćenje. Ta dodela nije direktna već preko regionalnog internet registra u čijoj geografskoj oblasti se AS nalazi.

Kao što je već rečeno, AS nezavisno donosi odluke sa kojim AS-ovima će razmenjivati saobraćaj na internetu. Odluke moraju biti (tehnički) jasno definisane. AS se povezuje sa jednim ili više AS da bi krajnji korisnici unutar tog AS mogli

[38] John Mathiason (team leader), Milton Mueller, Hans Klein, Marc Holitscher and Lee McKnight. (2004). *Internet Governance: The State of Play*, The Internet Governance Project, str. 20 Dostupno na http://www.internetgovernance.org/wordpress/wp-content/uploads/mainreport-final.pdf

[39] Zanimljiv je operater rut servera F, firma Internet System Consortium (ISC) koja je kreirala poseban inovativan softver (BIND) za upravljanje DNS i omogćila kopiranje (mirroring) rut servera širom sveta

[40] Prema 16-bitnom označavanju, AS brojeva ima 65.536, pri čemu su neki brojevi rezervisani, na pr. AS 0 rezervisan za nerutirane mreže, AS 23.456 za tehničke testove sistema, od AS 64.512 do AS 65.534 za privatnu upotrebu itd. U slučaju da u budućnosti skup AS brojeva bude iscrpljen, postoji 32-bitna verzija označavanja, koja omogućuje preko 4,2 milijarde AS brojeva. Međutim, od već dodeljenih AS brojeva više od 10.000 se ne koristi i nema ih u tabelama rutiranja. Prema http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_9-1/autonomous_system_numbers.html

komunicirati sa svim drugim korisnicima interneta tj. sa celim internetom. Povezivanje sa drugim AS je dobrovoljno, stvar dogovora između dve strane. Zavisno od relativne snage i interesa dve strane, njihovo povezivanje se dogovara kao ravnopravno (peering) ili kao neravnopravno (kupovina tranzita).

AS ima svoju grupu rutera na koje primenjuje sopstvenu jedinstvenu politiku rutiranja.

Rutiranje je proces tokom kog se paketi podataka prosleđuju između autonomnih sistema[41] od jednog uređaja do drugog dok ne stignu na svoje destinacije. Na bazi adrese destinacije na koju paket treba da stigne, ruter određuje putanju kako da paket prosledi dalje tj. susednom ruteru. Da svaki ruter zna kuda da pošalje pakete zadužen je već pominjani BGP, protokol koji omogućava razmenu informacija o rutama i dostupnosti između autonomnih sistema.[42] Ovaj protokol nastao je naporom privatnih kompanija koje su proizvodile opremu za umrežavanje odnosno rutere (CISCO, IBM, UNIX itd.).

Informacije o putanjama se nalaze u tablici rutiranja (Routing Information Base) smeštenoj u svakom ruteru; ova tablica sadrži listu IP adresa drugih udaljenih rutera koji su programirani tako da prepoznaju dotični ruter. Ruter dobija tu tablicu rutiranja na dva načina: automatski kad se poveže sa drugim ruterima (dinamičko rutiranje) ili ručnim konfigurisnjem od strane vlasnika (statičko rutiranje). On konstantno razmenjuje sa drugim ruterima poruke o promenama u preporučenoj putanji za stizanje do date IP adrese. Dakle, BGP ruteri nemaju potpuni topološki pregled mreže, svaki ruter zna samo kako da dopre do svojih direktnih suseda i zna preko kojih suseda se konkretna destinacija može dostići.

U BGP ruteru odluka o prosleđivanju se donosi za svaki paket posebno, nezavisno u svakom čvoru. Po prijemu paketa, čvorovi pogledaju u svoje tablice rutiranja da utvrde izlaznu putanju za taj paket. Bilo koji paket može da koristi celu širinu veze na svakom izlazu, ali možda mora da čeka u redu ako su drugi paketi već zauzeli vezu. U tom čekanju paket može biti odbačen, zbog čega je usluga isporuke nepouzdana. Paketi mogu biti izgubljeni, duplirani, zadržani ili isporučeni pogrešnim redosledom.

[41] Za pakete koji se prosleđuju unutar jednog istog AS ili istog domena primenjuju se drugi protokoli. Na primer OSPF (Open Shortest Path First)

[42] Ovaj protokol razmatra se u brojnim RFC-ovima. Jedan od njih je RFC 4271 „Border gateway protool-4 (BGP-4)“ iz 2006. godine, nakon čega je imao još 5 izmena u narednim RFC-ovima. http://tools.ietf.org/html/rfc4271

Iako svi ruteri dele navedenu logiku, postoje ruteri različitih kapaciteta. Na primer, kućni ruter koristi malu tablicu rutiranja jer njegov zadatak je samo da prosleđuje odlazni saobraćaj kućnog računara ka serveru svog ISP-a. Njegova tablica može sadržati manje od deset unosa. Najveći ruteri u srcu interneta čuvaju potpunu tablicu rutiranja interneta koja prevazilazi 100.000 unosa. Ovi ruteri stalno ažuriraju putanje i broj unosa (dostupnih putanja) se povećava.

U RFC 4271[43] iz 2006. god. data je definicija AS koja stavlja akcenat na dešavanja unutar autonomnog sistema:

> «Klasična definicija AS je da je to set rutera pod upravom jedinstvene tehničke administracije, koja koristi jedan protokol unutrašnjih rutera (interior gateways protocol IGP- prim. aut.) i zajedničku metriku da odredi kako da rutira pakete unutar AS-a, i jedan protokol inter-AS rutiranja (BGP-prim. aut.) da odredi kako da rutira pakete drugim AS-ovima. Od nastanka klasične definicije, uobičajilo se da jedan AS koristi više IGP-ova a ponekad i nekoliko setova metrike unutar sebe. Upotreba termina AS naglašava činjenicu da, čak i kada se koristi više IGP-ova i metrika, administracija jednog AS-a deluje drugim AS-ovima kao da ima jedinstven koherentan interni plan rutiranja i predstavlja doslednu sliku o tome koje destinacije su dostupne preko njega.»[44]

AS može za svaku destinaciju da koristi samo jednu putanju kao osnovnu putanju, u principu to bi bila njegova najkraća putanja ili ona koja je u skladu sa njegovom politikom rutiranja.[45] On o toj osnovnoj putanji obaveštava druge rutere i njegovi susedi je mogu koristiti za svoje rutiranje odnosno tranzit svog saobraćaja. Pored osnovne putanje, ruter skladišti sve alternativne putanje koje vode do date destinacije, što se koristi kada osnovna putanja postane nedostupna.

Budući da AS propagiraju svojim susedima informaciju o putanji koju dobiju od suseda kome veruju, odnosno da postoji pretpostavka da su razmenjene informacije o putanjama tačne, propagacija je slična širenju glasina, pa se sreće izraz «rutiranje putem glasina» (na engl. routing by rumour). U ovome se ogleda ranjivost infrastrukture rutiranja prema slučajnim pogreškama i namenim napadima. O pretnjama po bezbednost infrastrukture rutiranja biće više reči u poglavlju 4.

---

[43] RFC 4271, str. 4-5.

[44] Prema http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_9-1/autonomous_system_numbers.html

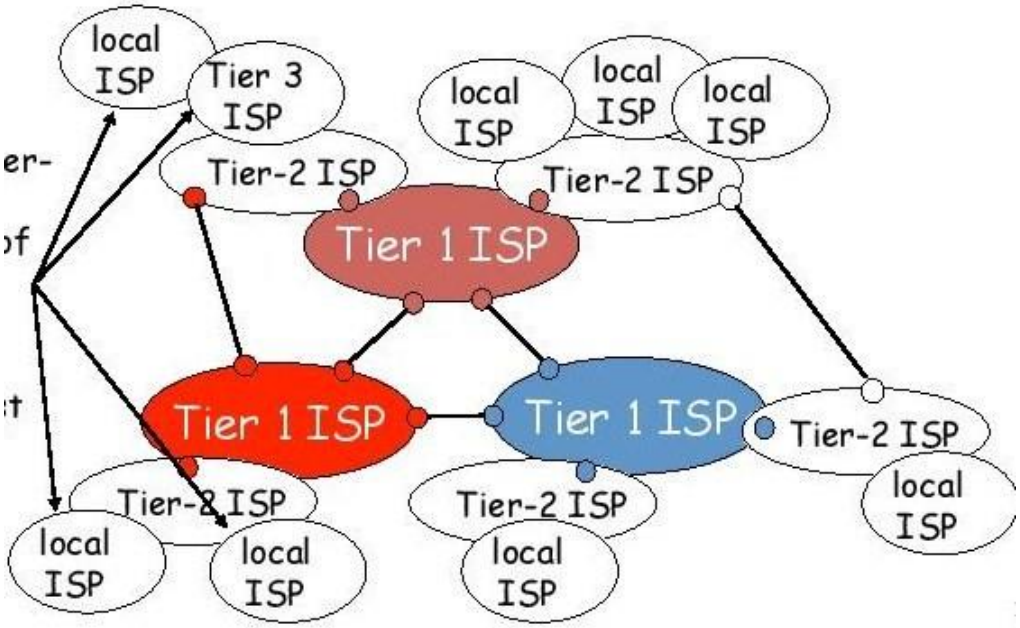
[45] Najkraća putanja se može različito meriti – po dužini u broju linkova, u fizičkoj udaljenosti, u sekundama itd. A isto tako se putanja može odabrati prema ceni. Stoga se čuju stavovi da se rutiranje između provajdera zapravo vrši na bazi novca a ne razdaljine ili da su putanje konzistentne sa ugovorima između ISP-ova.

AS-ovi sami biraju koju politiku rutiranja će primenjivati. Jedan popularan opis tipičnih politika rutiranje zove se «vruć krompir» i «hladan krompir». Rutiranje u stilu vrućeg krompira označava predaju saobraćaja drugom ruteru najranije moguće, a rutiranje u stilu hladnog krompira označava prenos vlastitog saobraćaja što je duže moguće preko svoje mreže pre puštanja u drugu mrežu. Na odluke o ovome utiče više faktora, na primer da li AS plaća tranzit (po količini saobraćaja), da li njegovi krajnji korisnici očekuju poseban kvalitet usluge i sl.

Među mrežama na internetu postoji istovremeno i ravnopravnost i hijerarhija. Ravnopravnost se ogleda u tome da je svaka mreža tehnička celina koja određuje svoj odnos sa drugim mrežama samostalno i nezavisno, imajući u vidu pre svega svoje mogućnosti i svoje interese odnosno svoj poslovni plan. Hijerarhija nastaje zbog razlika mređu mrežama - prema veličini, teritorijalnom obuhvatu, broju korisnika, ali pre svega prema kapacitetima za prenos paketa tj. fizičkoj infrastrukturi (kablovima, serverima) kojom raspolažu. Uobičajilo se rangiranje na mreže prvog, drugog i trećeg reda (na engl. tier 1, tier 2, tier 3) gledano od najmoćnije do najslabije.
Za mreže prvog reda ponekad se kaže da čine okosnicu interneta, mada taj pojam nije precizno definisan. Teritorijalno gledano mreže prvog reda obuhvataju čitave kontinente. Mreže prvog reda u sebi imaju mreže drugog reda, koje su najčešće na delu kontinenta, dok ove imaju u sebi mreže trećeg reda, prisutne na manjoj teritoriji, veličine države, grada i sl. Mreže prvog reda raspolažu prekookeanskim otpičkim kablovima, telekomunikacionim satelitima itd. Mreže trećeg reda su te koje organizuju pristup internetu za krajnje korisnike. One drže «zadnju milju» od interneta do korisnika.
Suštinska odlika mreža prvog reda je da ne kupuju tranzit od drugih mreža već to dobijaju besplatno, dok mreže drugog reda imaju osim besplatnih i (javno poznate) ugovore o tranzitu koji plaćaju. Ovde donosimo[46] dva grafička prikaza: dijagram odnosa u hijerarhiji mreža kao i dijagram moguće putanje određenog paketa podataka kroz ovu strukturu.

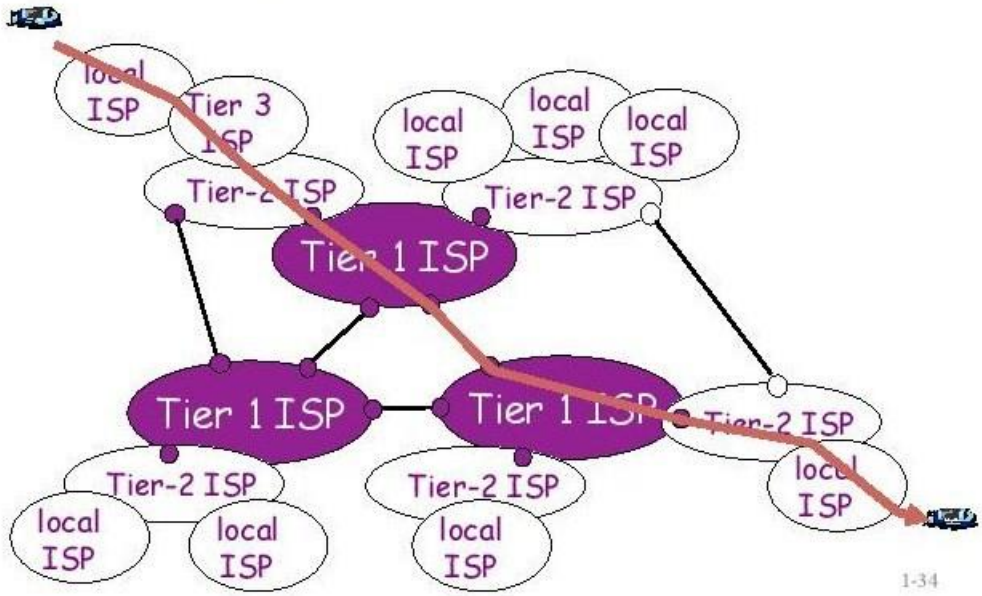
[46] Preuzeto sa http://www.cs.ccsu.edu/~stan/classes/CS490/Slides/Networks5-Ch1-1.pdf str.17.

Ilustracija 5 Dijagram- primer hijerarhije između ISP-ova



Preuzeto sa http://www.cs.ccsu.edu/~stan/classes/CS490/Slides/Networks5-Ch1-1.pdf

Ilustracija 6 Dijagram - primer kretanja internet saobraćaj između hijerarhizovanih ISP-ova



Preuzeto sa http://www.cs.ccsu.edu/~stan/classes/CS490/Slides/Networks5-Ch1-1.pdf

Sve ove mreže su pravno gledano privatne ili državne kompanije čiji je poslovni model baziran na pružanju raznih internet usluga raznim korisnicima. Ove kompanije su vlasnici ili najmoprimci samih fizičkih kanala veze kao i rutera.

Možda je ovo pravo mesto da se objasni pojam okosnica interneta (na engl. internet backbone). Okosnicu interneta čine glavne putanje između velikih strateški povezanih

mreža i glavnih servera u tim mrežama. To su linije za transmisiju podataka velike brzine, što podrazumeva širokopojasne veze i servere/rutere visokih performansi. Prva okosnica interneta se zvala Mreža Nacionalne fondacije za nauku, skraćeno NSFNET, i bila formirana od 1987. godine. Sadržavala je oko 170 manjih mreža, povezanih optičkim kablovima po brzini 1.544 Mbps.[47]

Još jedan pojam koji se mora uvesti je tačka internet povezivanja, skraćeno IX ili IXP.[48] Kada dva ISP-a odluče da se direktno povežu, obično moraju odrediti mesto na kome će se to fizički desiti, mesto koje odgovara obema stranama. Oni će na to mesto doneti svoju opremu i povezati je fizički. Od polovine 90-tih sve više su se razvijala ta posebna mesta povezivanja, IX-ovi.[49] U njima se okuplja veliki broj ISP-ova. Mesta su nešto poput berze internet konekcija. Vlasnik IX-a zarađuje od naknade koju plaćaju i kupci i prodavci za svoje prisustvo u toj tački. Za ISP-ove je postojanje IX-a značajno ekonomski, budući da direkna veza koju tu mogu uspostaviti snižava cene povezivanja sa većim ISP-ovima. Ovim mestima se ograničava ucenjivačka moć većih ISP-ova. IX-ovi se nalaze u većini svetskih gradova, između ostalog imamo jedan u Beogradu, o čemu će biti reči u poglavlju 6.

Regionalni internet registri (RIR) su udruženja nastala da okupe ISP-ove u određenom regionu. Oni od ICANN dobijaju blokove IP adresa i potom ih iznajmljuju na temelju zahteva koje prime od drugih organizacija (to mogu biti provajderi internet usluga ili druge organizacije) na svom geografskom području. U zahtevu tražioci IP adrese (najčešće vlasnici mreža) daju detaljno objašnjenje zašto su im potrebne IP adrese. RIR-ovi imaju set pravila i kriterijuma po kojima rešavaju zahteve tj. dodeljuju IP adrese. RIR-ovi tretiraju IP adrese kao zajednički javni resurs o kome su zaduženi da brinu. Oni neće izdavati ovaj resurs kriminalcima, špekulantima i sl. Najčešće se tražiocima dodeljuju kontinuirani blokovi adresa, jer to utiče na ekonomičniju tabelu rutiranja (kako bi bio što manji broj ruta u okosnici interneta). To je poznato pod nazivom hijerarhizovana agregacija ruta. Dodela adresa od strane RIR-a ne rukovodi se tržišnom logikom već tehničkom.

[47] Prema: https://www.techopedia.com/definition/20115/internet-backbone
[48] U daljem tekstu koristiće se skraćenica (od engl. Internet exchange point ili IXP)
[49] Osamdesetih u SAD su ova mesta imala drugačije nazive: CIX, FIX, NAP. Više o NAP u Poglavlju 7.

U ugovorima između RIR-ova i njihovih klijenata je izričito zabranjena preprodaja ili transferisanje adresa od strane klijenta drugim privatnim korisnicima.[50]

Registri koje vode RIR-ovi se priznaju kao merodavni i legitimni. Nosilac IP adrese uveden u registar ima legitimno i globalno priznato pravo na isključivo korišćenje te adrese.[51]

Detalji o RIR-ovima, sa detaljima njihove statistike, mogu se naći na stranici njihovog uduženja https://www.nro.net/about-the-nro (Udruženje je formirano 2003. godine).

Prvi je kreiran RIPE-NCC 1991. god. za Evropu i Bliski istok, potom APNIC 1995. god. za Aziju i Pacifik, a 1997. god. ARIN za Severnu Ameriku. Ova tri RIR-a su najuticajnija, ali postoje još i LACNIC za Latinsku Ameriku i AfriNIC za Afriku, koji su kreirani kasnije. Njihov prikaz na geografskoj mapi bi izgledao ovako:

Ilustracija 7 Mapa Regionalnih internet registara

Preuzeto sa https://www.nro.net/about-the-nro/regional-internet-registries

Svi RIR-ovi su privatne neprofitne organizacije. RIR-ovi se finansiraju od naknada za članstvo klijenata na svom području. Članovi određuju sudbinu RIR-ova. RIR-ovi izvlače svoj legitimitet i uticaj iz činjenice da provajderi internet usluga obraćaju pažnju na njh, odnosno poštuju i veruju njihovoj koordinaciji IP adresa. Oni (trenutno) nisu u odnosu prema bilo kojoj vladi kao što je ICANN prema vladi SAD.

[50] Postoje izuzeci, tj. kada firma ide kroz procese akvizicije i spajanja, dozvoljeno je da se transferišu i IP adrese zajedno sa vlasništvom nad firmom.

[51] Sve se pak dešava pod pretpostavkom da IP adresa ima dostupnih dovoljno tj. da ne postoji situacija nedostatka niti više zahteva za jednim blokom IP adresa.

RIR-ovi imaju sledeće funkcije:

1. registrovanje (ko je dobio koji blok IP adresa – podaci dostupni u WhoIs bazi podataka),
2. čuvanje resursa (briga šta se dešava sa napuštenim blokovima IP adresa i sl.),
3. distribuiranje blokova IP adresa na način koji agregira rute (štednja ograničenog prostora u tabelama rutiranja).

Međutim, postoje inicijative da se ovim funkcijama RIR-ova dodaju neke nove.[52] RIR-ovi ipak odbijaju da preuzimaju dodatne uloge, da poremete *status quo* u podeli moći. Posebno znajući da su IP adrese omiljeni mehanizam za praćenje korisnika interneta i sprovođenje državnih «intervencija» protiv njih, neke nove uloge RIR-ova bi zahtevale nošenje sa velikim temama, kao što je zaštita individualnih prava na privatnost, slobodu izražavanja ili sprovođenje zakona. Ove organizacije ostaju objekt a ne subjekt upravljanja, tj. nemaju težnju da se ubroje u tela koja upravljaju infrastrukturom interneta budući da jesu operativna infrastruktura.

[52] U nekom periodu razmatralo se da se RIR-ovima poveri uloga „sidra poverenja“ za RPKI, ali to nije ostvareno. Više reči o RPKI u poglavlju 4.

DRUGO POGLAVLJE

Arhitektura interneta - pojam

Arhitektura interneta će za potrebe ovog rada biti sinonim sa tumačenjem interneta od strane inžinjera tj. mrežnih dizajnera, tokom koga su se oni upustili u kreiranje šireg viđenja ovog tehničkog sistema. Arhitektura interneta je drugo ime za ishod procesa samorazumevanja mrežnog inžinjerstva, koje se osim imperativima efikasnog mrežnog dizajna rukovodi i drugim nameravanim posledicama, ciljevima i principima izgradnje sistema. Oni su pak delom inspirisani prihvaćenim vrednostima i ličnom filozofijom prvih tvoraca interneta.

Arhitektura interneta osim tehničkih stavova sadrži i druge stavove internet zajednice o tome kako ona vidi ili želi da vidi ili izgradi ili reguliše taj sistem. Stavovi su izraženi u formi RFC-a, o čemu će biti reči u posebnom poglavlju. RFC-i se mogu smatrati izvornim tekstovima za analizu arhitekture interneta. Međutim, u cilju objašnjenja korišćeni su i naučni članci merodavnih autora.

Treba reći da se arhitektura može sažeti i u samo jednoj rečenici. Dokaz toga nalazi se u RFC 1958 „Arhitektonski principi interneta“ iz 1996. god.[53] Tu je postojanje arhitekture sažeto je na sledeći način: „Mnogi članovi internet zajednice bi se složili da ne postoji arhitektura, nego samo tradicija, koja nije bila pisana u prvih 25 godina (barem ne od strane Odbora za arhitekturu interneta[54]). Ipak, uopšteno govoreći, zajednica smatra da je **cilj** konektivnost, **alat** internet protokol, a inteligencija s kraja na kraj umesto sakrivena u mreži.“[55]

Inicijalni ciljevi arhitekture interneta

Pogled na originlne ciljeve arhitekture interneta dat je u tekstu Dejvida Klarka „Filozofija dizajna internet protokola u DARPA“[56] iz 1988. god. Tu se navodi:

> „Vrhovni cilj arhitekture interneta u DARPA je bio razviti efektivnu tehniku multipleksne upotrebe postojećih međupovezanih mreža. ... Komponente interneta bile su mreže, koje je trebalo međupovezati da

[53] RFC 1958 “Architectural Principles of the Internet” https://www.ietf.org/rfc/rfc1958.txt
[54] Skraćeno IAB – Internet Architecture Board.
[55] RFC 1958, str. 2.
[56] David D. Clark “The Design Philosophy of the DARPA Internet Protocols” (Originally published in Proc. SIGCOM’88, Computer Communicatin Review Vol 18, No.4, August 1988, 106-114). Dostupno na http://ccr.sigcomm.org/archive/1995/jan95/ccr-9501-clark.pdf str. 106.

> bi dale neku širu uslugu. Originalni cilj je bio povezati originalni ARPANET sa ARPA paketnom radio mrežom ... U to vreme pretpostavljalo se da će biti i drugih vrsta mreža koje će trebati međupovezati, iako se u tom trenutku mreže lokalnog područja još nisu pojavile.“ [57]

Razmotrila se alternativa međupovezivanju postojećih mreža - da se na primer izgradi jedinstveni sistem koji bi uključio različite transmisione medije (multimedijalne mreže) i koji bi imao veći stepen integracje i bolju performansu. Ali ta alternativa odbačena jer su autori bili svesni da su date mreže u nadležnosti raznih entiteta (zasebnih administracija), pa integracija ne bi bila laka – entiteti bi se teško dogovorili. Opredeljenje da tehnika multipleksiranja bude razmena paketa došlo je otuda što je ona već bila isprobana u ARPANET. Tako je radna pretpostavka bila da će se mreže međupovezati slojem sa razmenjivačima internet paketa, koji su nazvani ruteri (gateways).

Tako se došlo do „osnovne strukture interneta: komunikacioni sistem na bazi razmene paketa u kome se više odvojenih mreža povezuje preko procesora razmene paketa nazvanih ruteri koji primenjuju algoritam za skladištenje i prosleđivanje paketa.“[58]

Polazeći od ovog vrhovnog cilja dolazi sledeći nivo ciljeva arhitekture interneta (ciljevi su izloženi po redosledu značaja):

1. Internet komunikacija mora da se nastavi uprkos gubitku mreža ili rutera.
2. Internet mora da podržava više vrsta komunikacionih usluga.
3. Arhitektura interneta mora da ugađa raznovrsnosti mreža.
4. Arhitektura interneta mora da dozvoli distribuirano upravljanje njegovim resursima.
5. Arhitektura interneta mora da bude troškovno efikasna.
6. Arhitektura interneta mora da dozvoli priključivanje hostova (kompjutera) uz male napore.
7. Resursi korišćeni u arhitekturi interneta moraju biti odgovorni (na engl. accountable).[59]

Konkretno objašnjenje zašto je cilj br. 1. značajniji od onih ispod sebe je to da je mreža dizajnirana da funkcioniše u vojnom kontekstu, a u ratu preživljavanje je preča briga od polaganja računa. Iz istog razloga je troškovna efikasnost niže kotirana od

[57] Ibid. str. 106.
[58] Ibid. str. 107.
[59] Ibid. str. 107.

raznovrsnosti mreža, jer se unapred ne zna koji tip mreže će biti značajan za preživaljavanje.

Protokol TCP je zadržan iako nije odgovarao nekim uslugama (na pr. isporuci digitalizovanog govora u realnom vremenu). Klark kaže da TCP nije bio pogodan za usluge kao što su pouzdana i sekvencirana isporuka, emitovanje iz mreže, prioritetno rangiranje trasportovanih paketa, podrška više vrsta usluga i interno znanje o neuspesima, brzinama i kašnjenjima, ali da je bio pogodniji u poređenju sa drugima s obzirom na heterogenost mreža – i to je presudilo u njegovu korist.

Klark je objasnio i opredeljenje da mreža bude distribuirana. Distribuirano upravljanje je pogodno (a i omogućeno) samim tim što svim ruterima (mrežama) ne upravlja jedno telo i što postoji način da ruteri raznih institucija razmenjuju tablice rutiranja iako ne veruju potpuno jedni drugima. Shodno tome, odluke o rutiranju donose se na bazi iskorišćenosti resursa, bez obzira na što taj mehanizam nije maksimalno efikasan. Iz opredeljenja za takvo rutiranje proizašla je recimo nedovoljna pouzdanost isporuke paketa (ostvarena pouzdanost je u stilu biće kako bude, Klarkovi termini su „deljenje sudbine“, „najbolji pokušaj“[60]).

Klark je ocenio: «U kontekstu svojih prioriteta, arhitektura interneta je bila vrlo uspešna.“[61] Međutim, ostavio je prostor da prioriteti dizajnera te arhitekture ne zadovoljavaju potrebe aktuelnih korisnika. Klarkov tekst je nastao 1988. god. A ciljevi o kojima je govorio negde 1969-1970. god.

Principi arhitekture interneta - definicija

Pod «principima dizajna»[62] podrazumevaju se dogovorena strukturalna i bihevioralna **pravila o tome kako dizajner/arhitekt** treba da strukturiše različite komponente i opiše fundamentalne i vremenski nepromenljive zakone koji rukovode funkcionisanjem inžinjerskog artefakta. Prinicipi dizajna pokreću većinu inžinjerskih **odluka na konceptualnom i operativnom nivou**. Iako se radi o inžinjerstvu,

[60] Ibid. str. 108.
[61] Ibid. str. 113.
[62] *Future Internet Design Principles*, Future Internet Architecture (FIArch) Group, coordinated by eight FP7 CSA projects supported by the DG Informatin Society and Media of the European Commission, January 2012. Dostupno na http://www.future-internet.eu/uploads/media/FIArch_Design_Principles_V1.0.pdf Str. 7.

prinicipi nisu formalno matematički definisani. Principi nastaju dogovaranjem inžinjera koji se bave razvojem interneta (princip kao stvar približnog koncenzusa). Poštovanje principa ogleda se tj daje svoj rezultat u načinu i formi specifikacija modela protokola i drugih inžinjerskih artefakta.

U RFC 1958 „Arhitektonski principi interneta“ iz 1996. god. istaknuto je da su od samog starta inžinjeri bili svesni konstantne promene koja se dešava vezano za principe arhitekture. „Principi koji su se činili neprekršivim pre nekoliko godina su danas pregaženi. Principi koji se danas čine svetim biće pregaženi sutra. Princip konstantne promene je možda jedini princip interneta koji će preživeti neograničeno.“[63] Ovaj odnos prema principima je prihvatljiv jer je posledica načina na koji se internet razvija: „Dobra analogija za razvoj interneta je ona sa konstantnim obnavljanjem pojedinačnih ulica i zgrada u nekom gradu, umesto sravnjivanja grada sa zemljom i ponovnog građenja.“[64] Osim toga, kao razlog za modifikaciju principa prihvata se «mišljenje sa terena» odnosno: «Inžinjersko mišljenje iz realne primene je važnije od bilo kog arhitektonskog principa.“[65]

Najstariji prinicip arhitekture interneta - princip E2E

Distinktivni princip arhitekture od samog nastanka interneta je čuveni princip na engleskom poznat kao end-to-end ili skraćeno E2E, što bi se u našem jeziku prevelo kao princip s-kraja-na-kraj. Da ovaj princip zauzima u dizajnu arhitekture interneta posebno mesto svedoči i naučni rad iz 1984. god. čiji su autori Salcer, Rid i Klark „End-to-end argumenti u dizajnu sistema“.[66]

Salzer, Rid i Klark su razmatrali smeštanje funkcija po modulima kompjuterskog sistema (iako ne sasvim tačno, radi lakšeg razumevanja uzećemo da bi moduli bili slojevi modela OSI i Interneta-prim. aut.) i došli do toga da funkcije koje se smeste na nižim nivoima sistema mogu biti redundantne ili od male vrednosti upoređeno sa troškom njihovog pružanja na tom niskom nivou. To su dokazali na primerima funkcija: ispravke greške, enkripcije, supresija duplikata poruka, podizanje nakon

[63] RFC 1958, str. 1.
[64] Ibid. str. 2.
[65] Ibid. str. 4.
[66] J.H.Saltzer, D.P.Reed and D.D.Clark. (November 1984). „End-to-End Arguments in System Design“ u ACM Transactions in Computer Systems Vol. 2, No 4, 277-288. Dostupno na http://web.mit.edu/Saltzer/www/publications/endtoend/endtoend.pdf

pada sistema i potvrda prijema, uz napomenu da se može primeniti i u širem kontekstu. Primer jednostavne funkcije obezbeđivanja integriteta podataka tj. provere greške u slanju podatka kaže: čak i kad bi mreža proveravala da li je izručivanje podataka prošlo bez greške, aplikacija bi ipak morala da to proveri ponovo, jer je greška mogla da nastupi pre ulaska podatka u mrežu. Dakle, sloj mreže bi to redundantno tj. nepotrebno radio. Suština argumenta je da implementaciju funkcija treba vršiti van mreže tj. na sloju aplikacije, izuzev kad se mogu vršiti na nižem nivou efikasno i uz minimalni trošak (neopterećujući druge aplikacije kojima ta funkcija nije potrebna a koriste isti niži nivo).

Ono što se naziva argument end-to-end je ovako tu predstavljeno:

> „U sistemu koji uključuje komunikacije ... postoji spisak funkcija od kojih svaka može biti implementirana na bilo koji od više načina ... U razmišljanju o tom izboru, ono što zahtevaju aplikacije daje osnovu za jednu klasu argumenata koji glase:
> funkcija o kojoj se radi može biti potpuno i pravilno implementirana samo uz znanje i pomoć aplikacije, koja se nalazi na krajevima komunikacionog sistema, i stoga nije moguće da funkcija bude data kao osobina samog komunikacionog sistema.
> Ovu liniju razmišljanja protiv implementiranja funkcija na niskom nivou nazivamo 'argument ent-to-end'.“[67]

Posledica ovog principa je to da niži nivoi ne moraju da pruže 'savršenu' pouzdanost. Napor koji se unosi u mere za pouzdanost u komunikacionom sistemu treba sagledati u odnosu sa drugim performansama a ne samo na bazi zahteva tačnosti.

U zaključku teksta je rečeno:

> „Argumenti end-to-end su jedna vrsta Okamovog brijača kad je reč o izboru koje će funkcije biti pružene u komunikacionom podsistemu. Pošto je komunikacioni podsistem često specifikovan pre nego što su poznate aplikacije koje će ga koristiti, dizajner može biti u iskušenju da 'pomogne' korisnicima preuzimajući više funkcije nego što je potrebno. Svest o argumentima end-to-end može da pomogne da se smanji to iskušenje.“[68]

Iako E2E na prvi pogled može delovati kao princip interesantan samo inžinjerima, radi se o izboru iz koga su proizašle izuzetno važne posledice za razvoj i domete interneta. Ovaj princip je uveo odustvo diskriminacije u mreži, prevashodno zato što je mreži ostavio samo funkcionalnost transporta paketa. Osnovna logika ovakve

[67] Ibid. str. 277-278.
[68] Ibid. str. 286.

arhitekture svodi se na sledeću jednačinu: ono što uđe (u mrežu) to i izađe (iz mreže). Mreža ne vrši interne transformacije na paketima. Paketi se samo analiziraju da bi se videla njihova destinacija (čak ne ni poreklo tj. pošiljalac) i da bi se prosledili dalje (rutirali). Redosled prolaska kroz čvorove je: prvi došao, prvi uslužen. Takvu mrežu definiše sloj protokola koji jednostavno ne sadrži u sebi funkcionalnost softvera koji bi pregledao pakete. Mreža zato „ne zna“ da li je neki paket podataka veb stranica, imejl, naučni članak ili muzički fajl, niti daje prioritet jednoj vrsti paketa podataka nad drugom. Drugim rečima, mreža je glupa,[69] a inteligencija nije u samoj mreži nego u aplikacijama koje su na krajevima mreže. Posao mreže je da prenosi datagrame onoliko efikasno i fleksibilno koliko je moguće. Sve drugo treba da se obavlja na krajevima.

Ova ista odlika interneta se naziva i transparentnost za aplikacije. Ona znači da mreža ne stoji na putu aplikacijama koje žele da isprobaju nešto novo. Zahvaljujući tome, milioni ljudi su u prilici da isprobavaju kreiranje najrazličitijih aplikacija bez velikih troškova skopčanih sa tim pokušajima, tj. kreatorima aplikacija data je mogućnost praktično neograničene inovacije i kreativne aktivnosti. Sve što oni rade tiče se samo sloja aplikacija, kojima rukuju krajevi mreže. Dakle, eksperimentisanje sa aplikacijama ne zahteva komplikove izmene nižih slojeva mreže (rekonfiguraciju cele mreže), pa samim tim ni visoke troškove usvajanja inovacije. Ni korisnici ni provajderi mrežnih usluga ne snose troškove inovacije, trošak inovacije pada samo na kreatora aplikacije. Imajući to u vidu, broj korisnika neke inovacije može brzo da raste, te raste i verovatnoća da se ostvari i efekat umrežavanja u prilog date inovacije. Iz toga proizilazi da ovakva arhitektura mreže olakšava inovacije na sloju aplikacija.

Opredeljenje za princip E2E je bilo prvenstveno motivisano praktičnošću i neznanjem koje bi se nove aplikacije mogle pojaviti u budućnosti. Ako bi se “središte” mreže optimizovalo za u datom momentu najrasprostranjenije aplikacije, time bi se napravile barijere kasnijim aplikacijama. Zato je odlučeno da se u protokole vezane za “središte” mreže ugradi što je manje moguće funkcija i da upravljanje paketima bude agnostičko prema aplikacijama. Neko iz miljea osnivača je to sažeo u rečenici: To je osobina, ne falinka. (na engl. This is a feature, not a bug.)

[69] David Isenberg *Rise of the Stupied Network.* Dostupno na http://www.hyperorg.com/misc/stupidnet.html

Ostali inicijalni principi arhitekture interneta

U pomenutom RFC 1958 „Arhitektonski principi interneta“ iz 1996. god. navedeno je (osim E2E) još 28 principa arhitekture interneta razdvojenih po temama (zavisno od toga da li se tiču dizajna generalno, internet imena i adresa, eksternih tema, poverljivosti i autentikacije). Za svrhe ovog rada, ukazaćemo samo na pojedine principe koji su interesantni za analizu iz ugla vrednosne obojenosti koja se pripisuje internetu.[70] Ti principi su formulisani na sledeći način[71]:

- Heterogenost je neizbežna i mora biti podržana dizajnom.
- Ako je prethodni dizajn, u kontekstu interneta ili drugde, uspešno rešio isti problem, izaberi isto rešenje, osim ako ne postoji dobar tehnički razlog da se to ne uradi.
- Sva rešenja dizajna moraju biti proširiva/skalabilna (primenljiva za veliki broj čvorova).
- Performanse i troškovi se moraju uzeti u obzir kao i funkcionalnost.
- Neka bude jednostavno. Kada si u sumnji oko dizajna, izaberi najjednostavnije rešenje.
- Modularnost je dobra. Ako možeš da držiš stvari razdvojene, uradi tako.
- U mnogim slučajevima je bolje usvojiti delimično završeno rešenje odmah nego čekati dok se ne nađe savršeno rešenje.
- Izbegavaj opcije i parametre gde god je to moguće. Opcije i parametri treba da se konfigurišu ili pregovaraju dinamički a ne ručno.
- Budi strog u slanju a tolerantan u primanju.[72] Implementacije moraju precizno slediti specifikacije kod slanja u mrežu, a tolerisati pogrešne ulaze iz mreže. Kada si u sumnji, tiho odbaci pograšan ulaz, bez slanja poruke o grešci osim ako se to ne zahteva specifikacijom.
- Budi škrt sa netraženim paketima.
- Objekti treba da budu samoopisujući (uključivo tip i veličinu) u razumnim granicama. Smeju da se koriste samo kodovi i drugi „magični“ brojevi koje dodeljuje IANA.
- Treba da se koristi jedna struktura imenovanja.

[70] Izostavljeno je ukupno 10 teza.
[71] Ovako sročeni principi su parafraze iz RFC 1958, str. 4-6.
[72] Ovaj princip se naziva princip robusnosti, i biće pojašnjen u nastavku poglavlja.

- Adrese moraju biti nedvosmislene (jedinstvene unutar područja u kome se javljaju).
- Daj prednost nepatentiranoj tehnologiji, ali ako je najbolja tehnologija patentirana i dostupna svima pod razumnim uslovima, tada je uključivanje patentirane tehnologije prihvatljivo.
- Postojanje izvoznih barijera za neke aspekte internet tehnologije je od sekundarnog značaja kod izbora koja će tehnologija biti usvojena kao standard. Sva tehnologija potrebna da bi se implementirali standardi interneta može biti izrađena u svakoj zemlji, tako da globalna upotreba internet tehnologije ne zavisi od toga da li je dozvoljen izvoz u pojedinu zemlju ili zemlje.
- Dizajn treba da bude potpuno internacionalan, sa podrškom za lokalizaciju (adapataciju za lokalni set karaktera).
- Sva rešenja moraju da se uklope u arhitekturu IP sigurnosti.
- Veoma je poželjno da nosači (na engl. carriers) internet saobraćaja štite privatnost i autentičnost celokupnog saobraćaja, ali to nije zahtev arhitekture. Poverljivost i autentikacija su odgovornost krajnjih korisnika i moraju se implementirati protokolima koje koriste krajnji korisnici. Krajevi ne treba da zavise od poverljivosti ili integriteta nosača. Nosači mogu izabrati da obezbeđuju neki nivo zaštite, ali to je sekundarno u odnosu na primarnu odgovornost krajnjih korisnika da sami sebe štite.

U ovim principima ogleda se vrednosna obojenost utoliko što traže da dizajn poštuje raznovrsnost (heterogenost), mogućnost proširenja, internacionalnost i globalnu dostupnost. Takođe je važan akcenat na toleranciji eventualnih (tuđih) grešaka i primarnoj odgovornosti krajeva mreže za sopstvenu privatnost i bezbednost.

Razrade principa jednostavnosti zbog rasta mreže

RFC 1958 doživeo je dopunu u RFC 3439 iz 2002. god. koji nosi naslov „Neke smernice i filozofija za arhitekturu interneta“.[73] To je svojevrsna razrada principa jednostavnosti, ali i principa proširivosti, modularnosti i sl. uz istovremeno dodavanje principa labavog uparivanja, otpornosti na pojačavanja i sl.

[73] RFC 3439 „Some Internet Architectural Guidance and Philosophy“ http://www.ietf.org/rfc/rfc3439.txt .

U RFC 3439 je obrazloženo zašto je potrebno očuvati jednostavnost u dizajnu interneta[74] i koje su posledice toga. U ovoj verziji princip jednostavnosti nam kaže da se složenost mora kontrolisati da bi mogao da se efikasno skalabilizuje složeni objekt. (Glavna svrha ovog RFC je pak da „podigne svest o složenosti u našoj sadašnjoj ahritekturi i da ispita efekat koji će takva složenost skoro izvesno imati na uspeh industrije IP nosača“. Jer „složenost je primarni mehanizam koji sprečava efikasnu proširivost/skalabilnost“.[75])

Osnovno polazište je da velike mreže, a internet je takav, pokazuju svojstvo nelinearnosti koga nema kod malih mreža. U teoriji sistema je dokazano da nelinearnost za sobom povlači princip pojačavanja.

> «Pojačavanje» (na engl. amplification-prim.aut.) znači da čak vrlo male promene mogu da izazovu i izazivaju velike promene u sistemu tzv. velike događaje. Male perturbacije u ulazu mogu da destabilizuju izlaz sistema, o čemu postoji mnogo primera – jedan primer je rušenje mosta Takoma Nerous 1940. god. zbog efekta pojačavanja malih naleta vetra. Kad je u velikoj mreži zbog složenosti na delu pojačavanje malih perturbacija, javiće se ozbiljne greške, pa arhitekt mreže mora da obezbedi da takve perturbacije budu izuzetno retke.“[76]

Deo nelinearnosti u velikim sistemima potiče i od uparivanja. Princip uparivanja kaže da kada se sistem uvećava, često ga odlikuje povećana međuzavisnost među komponentama. Što više događaja se dešava simultano, veća je verovatnoća da će dva ili više intereagovati i da će se desiti nepredviđena interakcija. Da bi se izbegle takve situacije a dobile jednostavne linearne interakcije, sistemi treba da imaju komponente u različitim i po mogućstvu udaljenim delovima sistema. U teoriji se smatra da labavo upareni sistemi imaju više fleksibilnosti i manju izloženost nepredviđenim padovima u odnosu na čvrsto uparene sisteme. Zato je to poželjan princip za arhitekturu interneta.

Međutim, ono zbog čega je ovaj RFC posebno zanimljiv je pominjanje Okamovog brijača u zaključku RFC-a.

> «Ideja da jednostavnost sama po sebi može da vodi nekoj formi optimalnosti je opšte mesto kroz čitavu istoriju i izrečena je na mnogo načina i u mnogim dimenzijama. Na primer, uzmimo maksimu koja je poznata kao Okamov brijač, koju je formulisao srednjevekovni

[74] Princip jednostavnosti u ovoj formulaciji glasi: Složenost je glavni mehanizam koji ometa efikasno skaliranje odnosno koji povećava kapitalne i operativne troškove, pa zbog toga, IP nosači moraju da usmeravaju arhitekturu mreže ka najjednostavnijim mogućim rešenjima. RFC 3439, str. 3.
[75] RFC 3439 str. 2.
[76] Ibid. str. 4.

> engleski filiozof i franciskanski monah Vilijam od Okama (oko 1285-1349.) i koja kaže 'Pluralitas non est ponenda sine neccesitate' ili 'mnoštvo ne treba stvarati bez nužnosti' (zato se Okamov brijač ponekad naziva princip nepotrebnog mnoštva i princip jednostavnosti)».[77]

U RFC 3439 se zaključuje da «da za mreže na bazi paketa koje su reda veličine današnjeg interneta ili veće, moramo težiti najjednostavnijim mogućim rešenjima ako se nadamo da izgradimo troškovno efikasnu infrastrukturu.»[78]

Princip robusnosti

Zanimljivo je da se ovaj RFC ukazuje i na povezanost principa složenosti i principa robusnosti koja čini moguću trgovinu između njih. Radi se o tome da

> „evolucija protokola može voditi spirali robusnost-složenost-krhkost gde složenost, dodata radi robusnosti, takođe dodaje nove ranjivosti, što ponovo vodi novim i spiralnim složenostima. To je upravo fenomen koji je princip jednostavnosti osmišljen da izbegne.»[79]

Robusnost je veoma važan princip dizajna interneta, skoro jednak E2E i navođen u velikom broju RFC-a. Uveo ga je Jon Postel u RFC 761 „Protokol kontrole transmisije“[80] iz 1980. god. gde kaže: „Implementacije TCP treba da slede opšti princip robusnosti: budi konzervativan u onom što činiš, a liberalan u onom što prihvataš od drugih.“[81] Zatim je u RFC 1122 „Zahtevi od internet hostova – o komunikacionim slojevima“[82] iz 1989. god. ova verzija principa proširena. Tu se navodi stav da softver treba da bude napisan da se suoči sa svakom zamislivom greškom, čak i onom malo verovatnom. „Uopšteno, najbolje je pretpostaviti da je mreža puna zlih entiteta koji će slati pakete dizajnirane da imaju najgore moguće efetke. Ta pretpostavka će voditi odgovarajućem zaštitnom dizajnu.“[83] Istovremeno, priznaje se da ljudsko zlo nije tako sposobno i moćno, već da su najozbiljniji problemi

[77] Ibid. str. 21-22.
[78] Ibid. str. 22.
[79] Ibid. str. 22.
[80] U pitanju je RFC 761 “Transmission Control Protocol”, koji je u međuvremenu zamenjen drugim RFC-ovima. http://tools.ietf.org/html/rfc761
[81] RFC 761 str. 13.
[82] RFC 1122 „Requirements for Internet Hosts – Communication Layers“ http://tools.ietf.org/html/rfc1122
[83] RFC 1122 str. 12.

na internetu izazvani prethodno neviđenim mehanizmima koje su izazvali događaji male verovatnoće.

> „Drugi deo principa je skoro jednako važan: ... nije mudro koristiti legalne ali opsukrne osobine protokola. Nije mudro odlutati daleko od očiglednog i jednostavnog, inače će se nepovoljni efekti pojaviti na drugom mestu. Naravoučenije iz ovoga je 'budi oprezan prema hostovima koji se čudno ponašaju (na engl. misbehaving hosts)'; softver treba da bude spreman ne samo da preživi druge hostove koji se čudno ponašaju, nego i da sarađuje da bi se ograničila količina poremećaja koje takvi hostovi mogu da izazovu zajedničkom komunikacionom sistemu."[84]

Principi arhitekture interneta u novom milenijumu

Inžinjerska zajednica, koja je najzaslužnija za razvoj interneta, na prelazu u novi milenijum je postala svesna da će se Internet menjati pod uticajem aktera koji su devedesetih godina uključili u njegov razvoj. Tako su napisana dva zanimljiva rada: prvi su napisali Klark, Solins, Vroclavski i Braden 2002. godine "Tučnjava u sajberspejsu: definisanje sutrašnjeg interneta"[85] a drugi Klark, Solins, Vroclavski i Faber 2003. godine "Bavljenje stvarnošću: arhitektonski odgovor na zahteve stvarnog sveta od evoluirajućeg interneta".[86]

Tekst o "Tučnjavi" počinje jednostavno:

> "Internet je stvoren u jednostavnijim vremenima. Njegovi stvaraoci i prvi korisnici delili su zajednički cilj - hteli su da izgrade mrežnu infrastrukturu da bi povezali sve kompjutere na svetu, tako da do tad nepoznate aplikacije mogu da se izmisle da bi se tu primenile."[87]

Međutim, ta opšta svrha koja je internet pokrenula i hranila više ne postoji, a to postavlja nove zahteve pred tehničku arhitekturu interneta – pre svega zahtev da se prilagodi toj tučnjavi između aktera. Kao akteri na internetu navode se: korisnici,

---

[84] Ibid. Str.13.

[85] David D. Clark, Karen R. Sollins, John Wroclawski, Robert Braden, "Tussle in Cyberspace: Defining Tomorrow's Internet" *SIGCOMM'02*. August 19-23, 2002, Pittsburgh. 347-356. Dostupno na http://conferences.sigcomm.org/sigcomm/2002/papers/tussle.pdf (U daljem tekstu "Tučnjava")

[86] David D. Clark, Karen Sollins, John Wroclawski, Ted Faber, "Addressing Reality: An Architectural Response to Real-World Demands on the Evolving Internet" *SIGCOMM 2003*, August 25-27, 2003, Karlsruhe. 247-257. Dostupno na http://groups.csail.mit.edu/ana/Publications/PubPDFs/Addressing%20Reality%20an%20architectural%20response%20to%20real%20world%20demands%20on%20the%20evolving%20internetworld.pdf (U daljem tekstu "Bavljenje stvarnošću")

[87] "Tučnjava", str. 347.

komercijalni ISP-ovi, provajderi mreže, vlade, vlasnici autorskih prava, provajderi sadržaja, a uz to

> "postoje 'dobri korisnici' i spemeri, dominantni ISP-ovi i mali igrači, provajderi mreže sa više ili manje rigidnosti, liberalne i konzervativne vlade itd. Rezultirajuće tuče se protežu na sve strane: individualna prava versus država, konkurenti koji žele profit, otpor prema onima sa zlim namerama, oni sa tajnama versus onih koji žele da otkriju tajne i oni koji žele anonimnost versus oni koji žele da ih identifikuju i pozovu na odgovornost."[88]

Zato bi principi dizajna trebalo da omogućavaju razne varijante ishoda umesto da dizajn diktira samo jedan ishod. Autori su predložili da ova dva principa budu uvažena kod narednog dizajna interneta:

- Modularizuj dizajn prema linijama tučnjave, tako da se jedna tuča ne preliva na druge i ne ometa teme koje s time nemaju veze (tzv. izolacija tučnjave).
- Dizajniraj za izbor, kako bi se dozvolilo različitim akterima da izraze svoje preference.

Poštovanjem ovih principa, arhitektura interneta bi mogla da ostvari dva cilja. Prvi i najvažniji cilj je da se sačuva mreža otvorenom i transparentnom za nove aplikacije. Ovaj izbor cilja odgovara na "jedan od najdubljih strahova za internet danas, onaj da će izgubiti svoje kvalitete otvorenosti: otvorenost za inovacije, otvorenost za pristup, otvorenost za izbor usluga".[89]

Drugi cilj koji predlažu je osnaživanje korisnika. To je preferenca ka tome da korisnik, a ne pružalac usluga ili provajder softvera, bude u stanju da bira koje aplikacije će upotrebiti, koje servere i usluge i sl. „Mnogima je osnaživanje korisnika osnovni princip interneta".[90] (podvukla aut.)

U tekstu o «Bavljenju realnošću» autori su krenuli od konstatacije da zbog sve veće uloge u društvu tokom godina internet je prolazio kroz znatne tehnološke i filozofske promene, pa je „introspekcija o ovim promenama već trebalo da bude obavljena".[91] Autori smatraju da sada osnovni izazovi sa kojima se sreće arhitektura mreže dolaze od sve važnijeg mesta mreže u društvu. To se razlikuje od situacije u prošlosti, kada su najfundamentalnija pitanja sa kojima se arhitektura sretala bila primarno

[88] "Tučnjava" str. 348.
[89] "Tučnjava" str. 353.
[90] "Tučnjava" str. 355.
[91] „Bavljenje stvarnošću" str. 247.

tehnološka i orijentisana na funkcionisanje. „Na internetu danas, osnovne pretpostavke o poverenju, autonomiji i zajedničkim ciljevima su pred osporavanjem. Kako sve više ljudi i institucija koristi internet da međusobno intereaguju, ... treba se baviti kredibilitetom – što je mnogo širi koncept od tradicionalne bezbednosti.“ [92] Ukoliko se akteri razvoja interneta ne počnu baviti tim novim pitanjima, kao što je kakvu kontrolu ima vlasnik širokopojasne veze nad sadržajima koji prolaze tom vezom ili kako se politika rutiranja nekog ISP-a odnosi prema javnoj politici – a ta pitanja nisu bila deo originalnog dizajna interneta – to će ispasti na njihovu štetu odnosno štetu interneta. Autori su stoga predložili da nove teme postanu deo centralnih principa interneta, i to: 1. primat dizajna za promene, 2. kontrolisana transparentnost i 3. centralnost prostora za tučnjavu.

Primat dizajna za promene znači da dizajneri mreže treba da očuvaju generalnost i evolutabilnost, a ujedno smanjuju troškove zadržavanja tih odlika. Generalnost u mreži dozvoljava da mreža prihvata aplikacije koje nisu ni postojale i tehnologije koji su drastično različite u karakteristikama od onih u vreme kad je mreža nastala. Ovaj princip se navodi i kao argument u korist arhitektonskog minimalizma – arhitekture u kojoj postoji mali, pomno ograničen set globalnih nepromenljivih i zajedničkih funkcija, a sve ostalo je prepušteno lokalnom definisanju.

Prostor za tučnjavu je potreban pošto korisnici imaju interese koji su neprijateljski jedni prema drugima i pošto postoji trajni proces sukoba, takozvane tučnjave. O tome je već bilo reči iznad.

Ideja o kontrolisanoj transparentnosti je nešto što dalekosežno utiče na suštinu interneta jer u mrežu dodaje nove sigurnosne servise koji tu nikada nisu postojali. Takvi uređaji (na pr. fajervol) krše transparentnost mreže. Do ovoga dolazi jer (kažu posmatranja iz stvarnog sveta) korisnici žele sigurnosnu arhitekturu u mreži, ne samo na krajevima mreže. Autori su ovim predlogom polako otvorili vrata za filtriranje neželjenog sadržaja (sadržaja iz ne-kredibilnih čvorova) unutar mreže. Imali su u vidu uređaje koji ograničavaju ili verifikuju ponašanje i koji su pozicionirani na granicama mreža, u tačkama gde se menjaju pretpostavke kredibilnosti. Razmotrili su model sigurnosti koji podrazumeva da različiti delovi mreže mogu vidjeti zaštićene oblasti sa različitim stepenom jasnoće. Potpuno nekredibilinim izvorima oblast će biti mračna; kako izvori pokazuju više kredibilnosti, tako im više servisa i krajeva postaje vidljivo,

[92] „Bavljenje stvarnošću“ str. 247.

a potpuno kredibilni eksterni izvori kao i unutrašnji izvori vide sve usluge. To je bio tek predlog modela: "ovaj pristup još uvek nije postao odgovarajuća sigurnosna arhitektura mreže."[93] Kasniji razvoj interneta se priklonio tome. Autori su uočili:

> "Možda je najradikalnija ideja iz ove analize ta da jednostavni E2E model transparentnosti treba da bude zamenjen kompleksnijom idejom kontrolisane transparentnosti. To implicira aktivne elemente u mreži, što dalje implicira tučnjavu oko toga ko kontroliše te uređaje."[94]

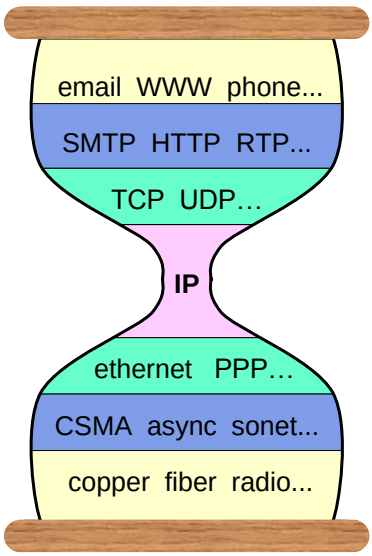
Rad se završava diskusijom o odnosu između arhitekture mreže i aplikacija kojima služi, o čemu će biti reči u narednom odeljku.

Sudbina principa E2E

Princip E2E se nekad predstavlja na način da se arhitektura interneta odslikava po modelu peščanog sata. Peščani sat je dobra metafora zahvaljujući svojoj karakterističnoj formi tj. uskom struku, a u modelu arhitekture interneta uzani struk peščanog sata je minimalni IP sloj.

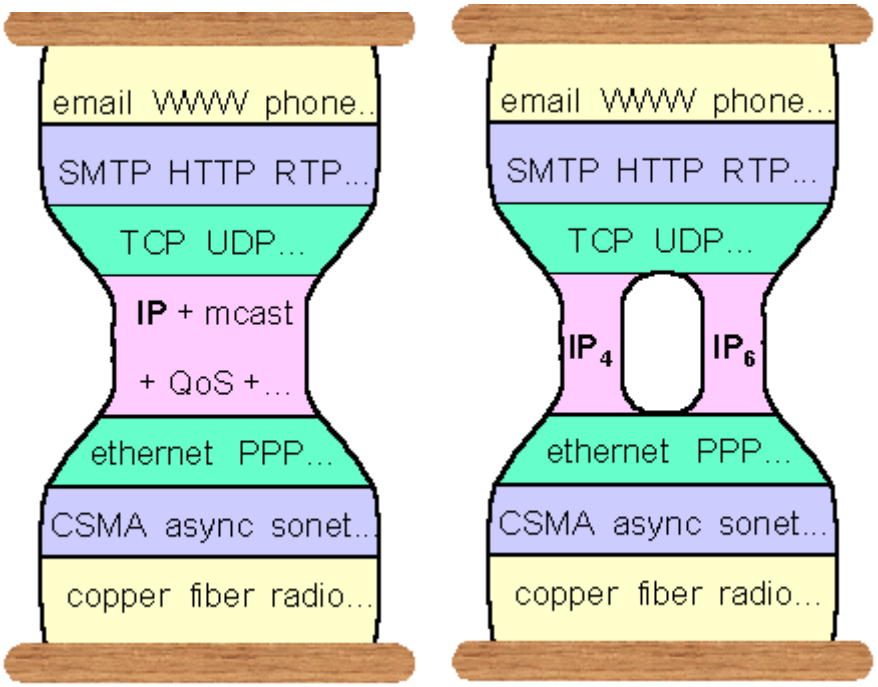
Stiv Diring je 2001. god. napravio jednu zanimljivu prezentaciju za skup IETF-a u Londonu. Prezentacija se zove «Posmatrajući struk protokolskog peščanog sata»[95] i na duhovit način ilustruje neke od promena u razmiljašnjima o internet protokolu i arhitekturi interneta.

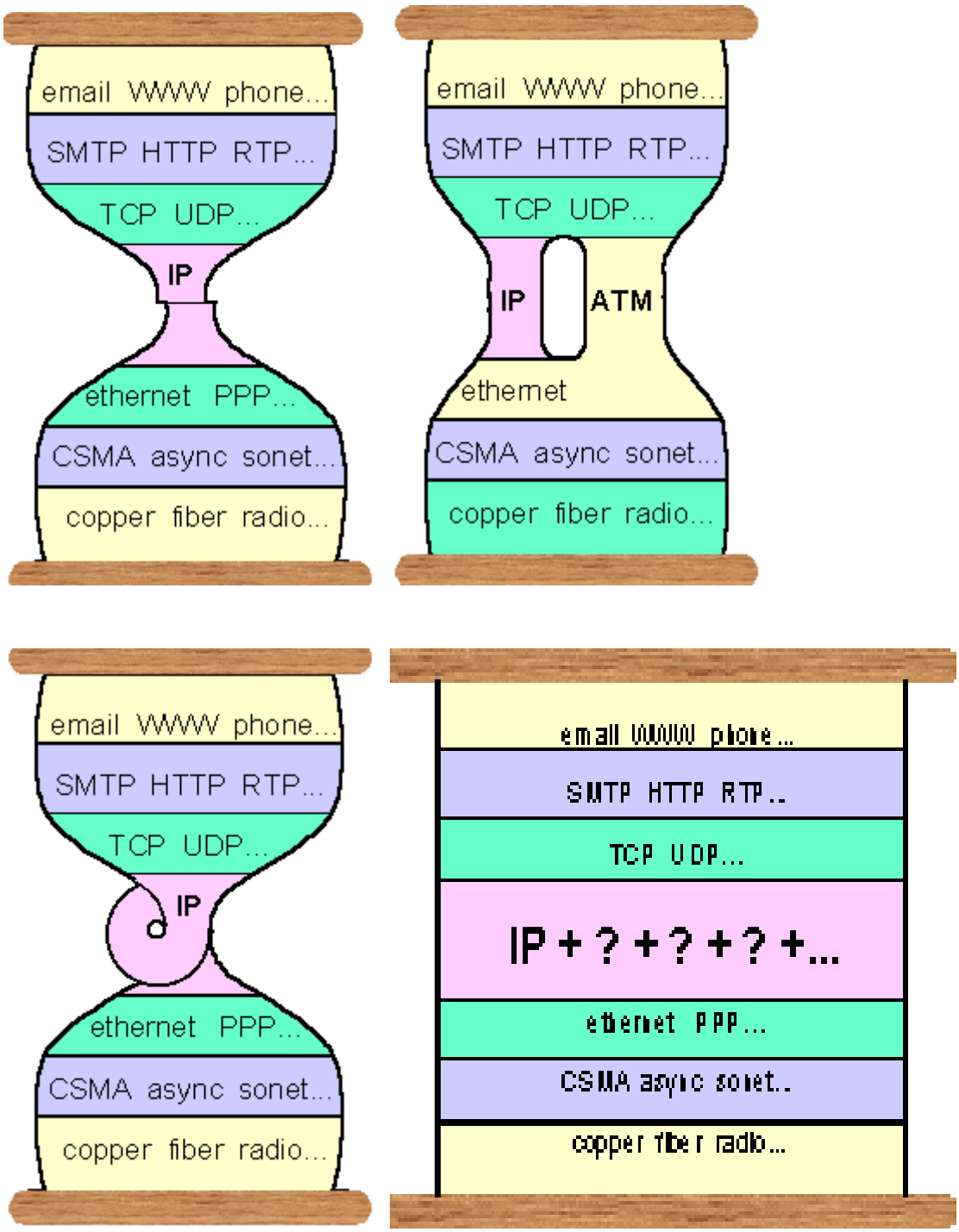
Diring kreće od teze da je u vreme nastanka internet imao pravilan izgled peščanog sata:



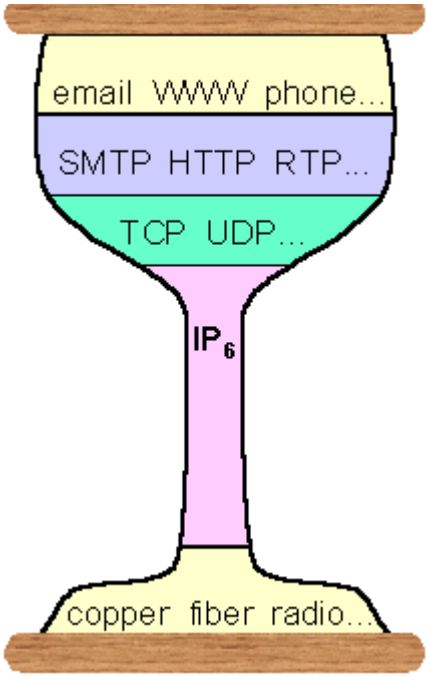
[93] „Bavljenje stvarnošću" str. 251.
[94] „Bavljenje stvarnošću" str. 256.
[95] Steve Deering, Watching the Waist of the Protocol Hourglass, IETF 51, London. Dostupno na http://www.cs.virginia.edu/~cs757/slidespdf//////deering-hourglass-london-ietf.pdf

Međutim, vremenom su predlagana i sprovođena razna «podešavanja». Tako se IP sloj najpre malo ugojio jer je tražio od slojeva ispod sebe više funkcionalnosti. Potom se IP sloj podelio na dve verzije, za IPv4 i IPv6. Dalje, IP sloj je slomljen pa zakrpljen, pri čemu se misli na nekompatibilnost dve verzije protokola, koja je kasnije popravljena. IP sloj je doživeo i položaj delimične zavisnosti od sloja linka. Konačno, prilagođen je i tuneliranju tzv. IP sloj preko IP sloja. Međutim, iskušenja da struk nestane su sve brojnija, jer pojavljuju se nastojanja da se u njega umetnu stvari kao što su pomagači TCP-a, asistencija za pouzdani multikast, kaše (cache) za presretanje paketa, rutiranje na bazi sadržaja i dr.





Budućnost IP sloja je još uvek nejasna, ali predlog Stiva Diringa je bio da IP sloj ponovo smrša i od peščanog sata se pretvori u vinsku čašu. To bi se postiglo uvođenjem IPv6, a time i vraćanjem jednostavnosti i funkcionalnosti.



Sudbina principa robusnosti

U tekstu iz 2011. god. Erika Almana „Princip robusnosti ponovo razmotren“[96] pojašnjava se da je ovaj princip „tokom mnogo godina bio prihvaćen kao dogma.“[97] Iako uveden od samog početka u dizajn interneta, prvo samo za TCP a kasnije i za ostale protokole, da bi se povećala interoperabilnost među mrežama odnosno verovatnoća da će dva kraja mreže moći da stupe u komunikaciju, vremenom je počeo i da stvara dve vrste problema.

Jedna vrsta problema tiče se same interoperabilnosti. Običan ljudski jezik može biti dvosmislen ali u stvarnom životu dvosmislenost se lako prevazilazi, no u tehničkom svetu to nije tako. U žargonu kompjuterista „kompjuteri su nemilosrdni“.[98] Stoga se dešava da dve specifikacije, jednoznačne ali sročene različito, ne budu u stanju da se uzajamno rastumače. Može se desiti da specifikacije naprave implicitne pretpostavke o okruženju u koje dolaze (na primer, maksimalna veličina paketa koju protokol ili hardver podržava) ili da kod implementacije dobiju novu funkcionalnost koja isprva nije bila predviđena i tada se pokažu greške.

---

[96] Eric Allman (2011). „The Robustness Principle Reconsidered: Seeking a Middle Ground" *Communications of the ACM*, Vol. 54 No.8, 40-45. Dostupno na http://cacm.acm.org/magazines/2011/8/114933-the-robustness-principle-reconsidered/fulltext

[97] Ibid. str. 40.

[98] Ibid. str. 40.

Druga vrsta problema tiče se bezbednosti jer atmosfera interneta se baš jako promenila. „Princip robustnosti je formulisan za internet onih koji sarađuju. Svet se dosta promenio od tada. Sve, čak i usluge koje mislite da vi kontrolišete, je sumnjivo.“[99]

Alman analizira i preformulaciju ovog principa koja glasi: budi konzervativan u onom što generišeš i još konzervativniji u onom što primaš. Ipak, po Almanu ni konzervativnost u primanju nije rešenje problema jer kad ne bi bilo liberalnosti u onom što se prima, protokoli se ne bi mogli proširivati i inovirati, isprobavanje novih verzija protokola bi bilo skoro nemoguće. „Skoro svaki uspešni protokol će morati da bude proširen u ovom ili onom momentu.“[100] Alman smatra da treba kod kreiranja standarda biti umeren, tj. uzeti u obzir oba faktora: i da je promena konstantna i da je svet neprijateljsko mesto, dakle i promenu i opasnost.

Moguće je da je jedan način dostizanja ravnoteže oba faktora ponuda koju su Sasaman, Paterson i Bratus objavili 2012. u tekstu „Zakrpa za Postelov princip robusnosti“.[101] Tekst se bavi suptilnostima u dizajnu protokola kroz tehničke primere, dakle u njemu preovlađuje inžinjerski jezik, ali su autori započeli tekst konstatacijom da je Postelov princip stekao duboki filozofski i politički značaj i stvorio svet programerske misli, intuicije i stava koji je načinio internet onakvim kakav jeste: sveprisutan, opšte interoperabilan i pogodan za upotrebnu komunikacione tehnologije za širenje političkih sloboda. Međutim, taj svet novih revolucionarnih oblika komunikacije je

> „sada suočen sa krizom nebezbednosti koja erodira poverenje korisnika u njegove softvere i platforme. Videvši platforme internet komunikacije toliko slabe i ranjive na sredstva mehaničkih napada kojih se lako mogu dokopati represivni autoriteti, spremnost korisnika da koriste platforme za poruke koje su im važne će se na kraju uništiti.“[102]

[99] Ibid. str. 44.
[100] Ibid. str. 44.
[101] Len Sassaman, Meredith L. Patterson, Sergey Bratus. (March/April 2012). “A Patch for Postel’s Robustness Principle”. *Secure Systems*, 87-91. Dostupno na http://langsec.org/papers/postel-patch.pdf (U daljem tekstu “Zakrpa”)
[102] “Zakrpa” str. 87.

Da se to ne bi dogodilo, ono što ovi autori predlažu je tzv. zakrpa za Postelov princip[103] koja bi mogla glasiti: budi liberalan u onom što primaš, a to bi se dalje moglo razložiti kao:

- Budi određen u onom što primaš.
- Tretiraj ulaz kao jezik, prihvati ga sa dostpunom kompjuterskom moći, kreiraj 'prepoznavača' iz gramatike njegovog jezika.
- Tretiraj komjutersku moć za rukovanje ulazom kao privilegiju i štedi je kad god je moguće.“[104]

Jedna od novih poruka koju ovde vidimo je da se kod protokola počinje gledati i to koliko to zahtevaju/troše kompjutersku moć, odnosno da im se greške mogu teže tolerisati ako zahtevaju/troše veću kompjutersku moć.

Arhitektura interneta kao prepreka istraživanjima

U literaturi koja se bavi neophodnim promenama interneta može se naći dosta živopisan termin «okamenjivanje arhitekture interneta». Upotrebili su ga Tarner i Tejlor u svom radu «Diversifikacija interneta»[105] za konferenciju IEEE GLOBECOM 2005. godine. Oni daju konstataciju da internet trpi negativne efekte inercije budući da su u njemu kreirane velike barijere uvođenju novih disruptivnih tehnologija. Pri tome su uočili da „postoje prilike za upotrebu novih protokola viših slojeva i novih tehnologija veze i fizičkog sloja, ali je mrežni sloj postao nedodirljiv.“[106] Založili su se za diversifikovani internet (umesto sadašnjeg interneta jedne arhitekture) odnosno pluralizam mrežnih arhitektura koje koegzistiraju na zajedničkoj mreži-supstratu (umesto mrežnog sloja) i predložili kako bi se to tehnički moglo sprovesti. Način je uvođenje nad-slojeva preko sloja mreže, virtuelizacija i pravljenje meta-mreža.

Ovo je samo jedan primer toga da je sama istraživačka zajednica preokupirana razvojem interneta uočila potrebu da se dalje vrše istraživanja novih arhitektura interneta, a za to je potrebno pre svega testiranje (baza za testiranje/testbed). Kao

[103] Autori vide svoj pokušaj u smislu da „naš predlog nije nespojiv sa intuicijama koje stoje u pozadini Postelovog principa, ali mogu se shvatiti kao strože čitanje koje treba da rukovodi njegovom primenom zarad bezbednijeg dizajna protokola.“ Ibid. str. 91

[104] „Zakrpa” str. 91.

[105] Jonathan S. Turner, David E. Taylor, “Diversifying the Internet” Dostupno na http://www.academia.edu/2200075/Diversifying_the_internet

[106] Ibid. str. 1.

odgovor na to pokrenut je u SAD projekat GENI, čija je svrha da konstruiše bazu za testiranje na kojoj bi se validirale nove arhitekture.

Ovakva istraživanja su moguća jer je savremeni hardver za umrežavanje postao veoma različit od onog koji je bio dostupan ranije. Razlika nije samo u brzini uređaja nego u većoj programabilnosti. Veća programabilnost znači da isti element može podržati više programa u isto vreme. Drugim rečima, takvi mrežni elementi izazito podržavaju neku formu virtualizacije.

Prateći ovaj trend Nacionalna fondacija za nauku je od 2006. god. pokrenula projekt GENI.[107] U okviru ovog projekta izgrađena je posebna mrežna infrastruktura tzv. GENI okosnica/platforma koja služi tome da se na njoj postave razne eksperimentalne mreže, a ma koliko bile različite, one tu mogu da koegzistiraju.

GENI platforma je zapravo kolekcija hardverskih mrežnih komponenti od kojih svaka komponenta može biti isečena na kriške (na engl. sliced) odnosno deljena među različitim korisnicima odnosno može raditi na različitom softveru. Mogućnosti komponenata su izložene za testiranje. Time je faktički GENI omogućila eksperimente bez prejudiciranja kako će se mrežni element koristiti, mrežni elementi su dati kao gradivni blokovi od kojih se mogu sklapati različiti sistemi. Sklapanje je dodatno olakšano setom gotovih „biblioteka“[108] koje pomažu da se lakše upravlja odabranim softverom. Tako se više celovitih mrežnih arhitektura može sklopiti i operacionalizovati na istoj platformi s tim da svaka bude samo ograničena na svoje kriške potrebnih komponenata.

GENI izokreće tradicionalne slojeve aplikacije i mreže: GENI supstrat posmatra te novonapravljene mreže kao aplikacije koje iz njega uzimaju samo svoje kriške – tako da eksperimentalne mreže postaju svojevrsna aplikacija u odnosu na GENI supstrat. Aplikacijama iliti eksperimentalnim mrežama je prepušteno da same otkriju koji mrežni resursi su im potrebni i kako da ih koriste. Aplikacije direktno pristupaju fizičkim resursima u (dodeljenoj) kriški. Pisanje aplikacija ipak ne postaje time mnogo zahtevnije, jer autorima je olakšano dostupnim „bibliotekama“ i uslugama. Ono što je najvažnije jeste da tu prestaje da postoji „uski struk“. U komunikaciji sa drugim mrežama u ovom sklopu nije obavezna upotreba ijednog zajedničkog

[107] Global environment for network innovation; http://www.geni.net/?page_id=2

[108] Pojam “biblioteka” (na engl. Libraries) će se koristiti pod navodnicima da ukaže razliku od značenja pojma u svakodnevnom govoru.

protokola (uskog struka, TCP/IP). Pitanje povezanosti s kraja na kraj ostaje u potpunosti stvar koju će morati da reši novonapravljena mraža za sebe.

Jedna od prednosti uočenih kroz korišćenje GENI platforme je mogućnost da obračun troškova postane jasniji: svaka aplikacija iliti eksperimentalna mreža sada eksplicitno koristi jasno određene resurse (kriške), a ne implicitno sve resurse na internetu, pa tako može da plati samo za njih. U običnom internetu plaćanje među ISP-ovima je bazirano na merenju paketa tj. saobraćaja, dok bi po šemi GENI platforme samo plaćali virtualizovane resurse niskog nivoa. To eksperimentatorima ostavlja dosta prostora da diferenciraju svoje servise, inoviraju i samim tim kontrolišu svoje troškove.

Arhitektura interneta iz perspektive aplikacija

Sa novim milenijumom sve više se počeo uključitvati novi aspekt u razmatranje arhitekture interneta - odnos mreže i aplikacija. Kao što smo naveli, već u tekstu „Bavljenje realnošću: arhitektonski odgovor na zahteve stvarnog sveta od evoluirajućeg interneta“ prezentiran je stav koji uzima u obzir interes aplikacija.

„U prošlosti, arhitekti mreže su dizajnirali mrežu i potom ostavljali dizajnere aplikacija da rade šta žele, bez mnogo smernica.“[109] U novom vremenu se funkcije mreže gledaju iz perspektive aplikacija. Svaka aplikacija koristi ono što nađe, ali dizajneri aplikacija razmišljaju i u korist druge vrste generalnosti – mogućnosti da funkcionišu na različitim vrstama infrastrukture ... i stoga da postignu širi obuhvat od samog interneta. To znači da dizajneri mreže moraju uzeti u obzir da će interkonekcija na nivou aplikacija uvek biti manje opšta a više obuhvatna nego što je opšta internet konekcija. Autori daju primer senzorske mreže. Ove mreže mogu biti „prikačene“ na internet i kao rezultat toga biće dostupne na internetu. Ali one često neće primenjivati internet protokole. Tačka interkonekcije između interneta i senzorske mreže će skoro sigurno biti svesna aplikacije. „Mnogi ljudi mogu biti spremni da prihvate ovu tvrdnju implicitno, ali nespremni da je prihvate kao ograničenje arhitekture.“[110] Jer ako to prihvatimo, dobijamo jasnu podelu između dva dela mreže – dela gde čuvamo glavne principe dizajna interneta (univerzalni prenos paketa, transparentnost, rutiranje na bazi adresa, podrška nepoznatim aplikacijama) i onih delova gde se primenjuju neki

[109] „Bavljenje“, str. 254.
[110] „Bavljenje“, str. 255.

drugi principi. Rešenje koje autori predlažu za izlaz iz ove situacije je savet dizajnerima aplikacija da se jasno svrstaju u jedan blok odnosno

> „ili primenjujte opšti internet protokol ili se prikačite na tačku konekcije (verovatno sa informacijama o sesijama) pa sprovodite svoj mehanizam za aplikacije. Ovaj drugi način postoji danas i treba da se pitamo šta da uradimo da ga podržimo a ne da ga osuđujemo.“[111]

Jednu sličnu poruku tim novim trendovima uputio je i RFC 3426 „Opšta razmatranja o arhitekturi i politici“[112] iz 2002. godine. Već tada se uočavao gubitak koherentnosti u ukupnoj arhitekturi interneta, jer su delovi arhitekture počeli da budu dizajnirani od manjih zajednica (ne cele internet zajednice) koje su imale sopstvene interese i nisu obraćale pažnju na to da se sve uklopi u širu sliku. Ovaj RFC predlaže da nova smernica za dizajniranje protokola glasi: „Utvrdi da li je predloženi protokol dugoročno ili kratkoročno rešenje i utvrdi dugoročne troškove i izlaznu strategiju za sva kratkoročna rešenja.“[113] On je i pun pitanja na koja u tom momentu nisu postojali jasni odgovori ali iza pitanja se u stvari nalazio bio poziv kreatorima novih aplikacija da razmisle. Na primer (pitanja nisu data integralno već su izabrana i parafrazirana – prim.aut.): „Zašto predlažeš ovo rešenje, umesto nekog drugog ili umesto korišćenja postojećih protokola i procedura?“ „Zašto predlažeš rešenje na ovom sloju a ne na nekom drugom?“ „Da li si razmotrio širi kontekst, dok ograničavaš svoj rad na dizajnu na deo celine?“ „Kako se arhitektonski dobici predloženog novog protokola porede sa arhitektonskim gubicima?“ „Koliko je taj protokol robustan?“ „Da li je protokol dizajniran za promenu, tako da dozvoli različitim akterima da izraze svoje preference gde je to prikladno?“ „Da li protokol štiti interese budućnosti čuvajući evolutivnu sposobnost interneta? Da li omogućava budući razvoj?“[114]

Ova razmatranja nisu zaustavila trend. Ubrzo se otišlo dalje i stiglo se do tačke u razvoju komunikacionih tehnologija, u kojoj postaje najvažnije kako izgraditi, primeniti i imati u funkciji distribuirane aplikacije sa velikim brojem korisnika. Ovaj pristup se u literaturi naziva aplikacija-centričnim i polazi od toga da se pisanje aplikacija može odvijati u okruženju u kome se za primenu nove aplikacije na daljinu stvaraju virtuelni ruteri (protokoli rutiranja specifični za datu aplikaciju) i virtualni

---

[111] „Bavljenje“, str. 255.
[112] RFC 3426 “General Architectural and Policy Considerations” https://www.rfc-editor.org/rfc/pdfrfc/rfc3426.txt.pdf
[113] Ibid. str. 2.
[114] Ibid. str. 3-4.

linkovi (gde aplikacija otkriva dostupnost resursa), i kreira povezivanje preko raznovrsnih mreža. Sve to pak funkcioniše u vidu nad-slojeva (overlays) na postojećoj arhitekturi interneta. To je okruženje u kome aplikacija praktički pravi svoju mrežu. To je faza koja sledi nakon rušenja granice između aplikacija i mreže, odnosno preokreta uobičajnog shvatanja da se aplikacije nalaze na krajevima sistema a mreža nosi pakete.

Zbog pozicije Srbije u odnosu prema Evropskoj uniji, za potrebe ovog rada zanimljivo je dati pristup dizajniranju budućeg interneta od strane ekspertske grupe formirane od strane Evropske komisije, koja je 2012. god. pripremila stajalište o budućoj arhitekturi interneta.[115] Smer u kome bi išle promene jednog broja osnovnih principa (tako što bi im se ponešto dodalo tj. njihovom postojećem opisu) karakteriše sledeće: (lista nije potpuna – prim.aut.)

- Princip modularnosti treba da bude proširen principom polimorfizma – polimorfizam bi omogućio da iste apstraktne i autonomne labavo uparene komponente imaju različita funkcionalna i nefunkcionalna ponašanja pod različitim okruženjima ili okolnostima.
- Princip jednoznačnog imenovanja i adresiranja treba da bude proširen – predviđa se da će u budućnosti ne samo krajevi i njihovi 'privesci' morati biti jednoznačni i jedinstveni tamo gde se pojavljuju i koriste, nego će takvi takođe morati biti i podaci i usluge. "Ako se jedni isti podaci (tj. isti po sadržaju, vrsti, kvalitetu, bezbednosti, ...) i/ili usluge (tj. funkcionalno ili nefunkcionalno spajanje) mogu obezbediti na drugi način (na primer sa drugog servera ili drugim metodom), to je prihvatljivo, pa u mnogim slučajevima čak i poželjno, pod uslovom da je dati kvalitet bolji (ili trošak manji)."[116]

Pošto su uvereni da internet evoluira u pravcu potpunog komunikacionog ekosistema, ponudili su i zametke nekih potpuno novih principa dizajna arhitekture interneta, od kojih ćemo ovde izdvojiti samo neke, kao što su:

- Svesnost o resursima treba da zaživi u svim slojevima mreže. Sadašnji pristup mreže se označava kao nesvestan usluga. Svaki sloj mreže treba da bude

[115] *Future Internet Design Principles*. (Jan. 2012). Future Internet Architecture (FIArch) Group, coordinated by eight FP7 CSA projects supported by the DG Informatin Society and Media of the European Commission, Dostupno na http://www.future-internet.eu/uploads/media/FIArch_Design_Principles_V1.0.pdf
[116] Ibid. str. 20

svestan sebe kao seta usluga, koji radi u izolaciji ali i sarađuje sa drugima kako bi se omogućilo holističko pružanje usluge. To znači da je svaki nivo svestan svojih efekata na nivoe iznad sebe u smislu ispunjenja ili ne ispunjenja onog što je garantovano, a istovremeno i da svaki nivo pregovara i dogovora određene garancije sa nivoima ispod sebe.

- Logika zavisnosti (na engl. dependability logic) umesto dosadašnjeg nedostatka načina da mrežna infrastruktura procesuira pouzdano, odgovorno i proverljivo. Budući internet bi morao da poseduje sposobnosti za samo-prilagođavanje i samo-učenje kako bi se snalazio u promenama uslova procesuiranja, jer samo tako će moći biti pouzdaniji itd.

Ostvarivanje tog novog internet ekosistema ne samo da „traži principe dizajna koji idu dalje od umrežavanja i primitivnih usluga," nego i ima u krajnjem ekonomsku logiku, tj. logiku profita. Važno je da internet „bude dizajniran tako da čini održivim investiranje intelekta, inovacija i resursa u smislu ukupnog pozitivnog povraćaja (investiranog – prim.aut.)."[117] Akcenat je, dakle, na sposobnosti interneta da zadovolji nove aplikacije, a samim tim i kreira veće zadovoljstvo korisnika aplikacija. Glavno za budućnost je da dizajnom treba omogućiti da internet zajednice nagrade arhitekturalne module/komponente koje daju pozitivni povraćaj investicija, a obeshrabre module/komponente sa negativnim povratom.

Pritisci na arhitekturu interneta – njen kraj

U tekstu indikativnog naslova „Kraj arhitekture interneta"[118] Timoti Rosko je konstatovao da se na postojeću arhitekturu interneta vrše pritisci sa tri strane:

pritisci iznutra – traže se funkcionalnosti koje arhitektura u ovom obliku ne može da pruži (bezbednost, otpornost na napade tipa DDoS, kvalitet usluge s kraja na kraj) a uvedene su funkcionalnosti koje se ne uklapaju sa tom arhitekturom (fajervolovi, translatori internet adresa itd.);

pritisci odozgo – postoji pragmatičan pristup da se arhitektura ostavi kakva jeste a da se na nju dodaju nove arhitekture kao nadslojevi (overlays), koji dovode da podmreža

[117] Ibid. str. 26.

[118] Timothy Roscoe "The End of Internet Architecture" *SIGCOMM* 2006. 55-60. Dostupno na http://conferences.sigcomm.org/hotnets/2006/roscoe06end.pdf

otežano vrši saobraćaj pri čemu podmreža više nije slepa za aplikacije nego nadslojevi i podmreža zaviruju jedno u drugo;

pritisci spolja – dovodi se u pitanje kakav je odnos interneta prema drugim mrežama, odnosno proces asimilacije; interakcija interneta sa drugim mrežama svodila se na to da su one morale da nose IP pakete. Sada imamo telefonske mreže, senzorske mreže, mreže velikih kompanija, a one se ne drže tipičnih principa arhitekture interneta.

Ono što se kod ove Roskove teze o pritiscima može kritikovati je poistovećivanje arhitekture sa „uskim strukom peščanog sata" odnosno TCP/IT. Tačno je da u GENI „mreži" ne postoji uski struk – u njoj aplikacije direktno kontaktiraju sa fizičkim resursima razdvojenim na kriške na najnižem mogućem nivou apstrakcije (i koriste „biblioteke" i usluge koje im olakšavaju taj posao). Ali nije tačno da je cela arhitektura identična sa uskim strukom.

Rosko smatra da je problem u samoj ideji arhitekture mreže, ideji da mreža ima neku arhitekturu.

> „Pošto opisi internet arhitekture referiraju ili na nepostojeću sadašnost ili na idealizovanu prošlost ili na (verovatno neostvarivu) budućnost, treba se zapitati koja je uloga arhitekture interneta danas. Drugim rečima, šta *ideja* arhitekture interneta radi? Koji su efekti tog pojma koji je u opštoj upotrebi, koji je deo 'zdravog razuma'?"[119]

Rosko dolazi do zaključka da manje-više ta ideja samo smeta. Ona je propustljiva granica između dve oblasti, istraživanja sistema i istraživanja mreža, ali se ne uklapa ni u jednu od njih. Da bi se uklopila u sadašnje istraživanje mreža, morala bi preći u plural – arhitekture mreža, a čak ni tada ne bi pogađala suštinu. Naime, i u pluralu arhitektura interneta zadržava „prevaziđenu distinkciju između rutera i krajeva mreže".[120] Rosko postavlja pitanje koje odražava pogled iz ugla kreatora aplikacija: „Ako imaš sposobnost da stvaraš virtuelne mašine, virtuelne rutere i virtulane veze, sa udaljenosti, preko različitih mreža, kako napisati aplikaciju koja će funkcionisati u takvom okruženju? Koje usluge ... i druge komponente bi mogle takvoj aplikaciji da budu korisne?"[121] On je verovao da u tom momentu (2006. godine) ne postoji nikakav koncenzus o tome kakvo bi to okruženje trebalo da bude, pa tako ni da li bi eventualno imalo i neku „arhitekturu".

[119] Ibid. str. 56-57.
[120] Ibid. str. 59.
[121] Ibid. str. 59.

TREĆE POGLAVLJE

Post-arhitekturalni internet

Do sada smo prikazali putanju od uvođenja do napuštanja arhitekture iz razmatranja o dizajnu interneta. Ta putanja je pređena u nekih deset godina - od 1996. do 2006. godine (mada je uvođenje verovatno teklo od samog početaka interneta, dakle i pre 1996. godine, a napuštanje verovatno teklo kao proces čije prve naznake izbijaju na prelazu u novi milenijum, dok je Roskov tekst iz 2006. godine samo to tematizovao).

Kao što je ranije rečeno, u ovom radu arhitektura je predstavljena kao sinonim sa tumačenjem interneta od strane mrežnih dizajnera, tokom koga su se oni upustili u kreiranje šireg viđenja ovog tehničkog sistema. U ovom širem viđenju tehničkog sistema obavezno mesto su imali njegovi ciljevi, principi (kojima se rukovode inžinjerske odluke o protokolima i dr.) i vrednosti (poverenje, autonomija, osnaživanje korisnika i dr.). Arhitektura je bila rezultat određenog samo-razumevanja i opis poduhvata izgradnje interneta, izneta od strane onih koji su želeli da razumeju i opišu. Ta vrsta *modus operandi* je nakon nekog vremena nadjačana tendencijama koje su ustoličile fragmentirani i usko specijalizovani pogled na internet.

Postavlja se pitanje: šta se dešava kada (više) nema arhitekture interneta, ali ima interneta? Na koji način se dalje može filozofski sagledavati internet, koji se razvija kontinuirano i u post-arhitekturalnoj fazi? Nastavak ovog rada nudi odgovor na to pitanje.

I dalje kao filozofi, a i u ime brojnih drugih zainteresovanih strana, želimo da razumemo i opišemo ovaj fenomen. Za izvršavanje tog zadatka imamo neka uporišta i u post-arhitekturalnoj fazi. Rasplažemo pojmom interneta kao tehničkog sistema sa jednim brojem suštinskih komponenata – TCP/IP, DNS, AS i BGP, ISP, RIR. Vidimo da su sve ove suštinske komponente, osim TCP/IP, ostale nepoljujane (nakon 2006. godine). Time se omogućava da nastavak istraživanja dizajna interneta bude usmeren na praćenje sudbine ovih ostalih suštinskih komponenti. Njihovu sudbinu određuju oni koji upravljaju njima, ali isto tako i prostorni razmeštaj i ekonomski faktori. Drugim rečima, post-arhitekturalne teme o dizajnu interneta bi bile: upravljanje internetom i njegove interakcije sa teritorijalnim i ekonomskim fenomenima.

Internet kroz paradigmu RFC

Jedan aspekt dizajna interneta, inicijalno tesno vezan sa arhitekturom, nadživeo je sve promene koje su pogodile arhitekturu interneta u njegovoj 40-ak godina dugoj istoriji. To je negovanje prakse RFC-a. Ova praksa je više od metodologije rada i ima dobre preduslove da postane zaštitni znak interneta.[122]

Zahtev za dostavljanje komentara ili RFC (od engl. Request for Comments) označava dokumente u kojima se opisuju razne stvari vezane za funkcionisanje interneta (kao što su specifikacije, protokoli, procedure itd.). Taj naziv, a i samu praksu na koju naziv referira izmislio je Stiv Kroker sa Univerziteta Kalifornija u Los Anđelesu aprila 1969. godine, kada je zvanično poslao prvi RFC. To je bio neformalni poziv upućen svim istraživačima koji su se interesovali za ARPANET projekt da se uključe u diskusiju. Takvih istraživača je naravno bilo nekoliko i neformalno su bili okupljeni u „radnu grupu za mrežu". Svako ko je hteo je mogao da se pridruži sastancima i diskusijama. Svako je mogao i da pokrene diskusiju o temi koju smatra bitnom. RFC 1 je poslat u papirnoj verziji. Kasniji RFC-i su slati putem ARPANET-a čim je ova mreža proradila. Od RFC 3 odlučeno je da ova procedura postane običajna praksa. Posle dobijanja komentara od zainteresovanih tj. posle diskusije o predmetu kome je RFC posvećen, urednik dotičnog RFC-a je imao zadatak da u pisanoj formi sažme zauzeto gledište i dostavi ga svima odnosno objavi za dalje korišćenje. Od 1969. do 1998. god. glavni urednik RFC-a bio je Jon Postel, jedna od vodećih ličnosti među osnivačima interneta (jedan od internet pionira). Objavljeni RFC su se nizali označeni rednim brojevima. Jednom objavljen, RFC se nikada ne menja, već se, ukoliko ima potrebe za izmenama, kreira novi a za stari se napominje da je obezvređen (deprecated, obsolete). Ukupan broj RFC-ova koji su promenili status je 243,[123] što je zaista mali deo svih RFC-ova jer zaključno sa februarom 2016. god. popis svih RFC sadrži njih 7772. Aktuelni broj je dakle nešto manji od toga i zato što kod ponekog broja stoji „nije objavljen" tj. to je prazan broj iz raznih tehničkih razloga.

RFC su klasifikovani na nekoliko kategorija, od onih koji definišu standarde ili predložene standarde, preko najbolje tekuće prakse, informativnih, eksperimentalnih, istorijskih, do onih čija je svrha nejasna. RFC čija je svrha nejasna su obično RFC starijeg datuma koji danas možda ne bi ni bili objavljeni, ali su u svoje vreme pre

[122] Jedna analogija bi glasila celina RFC-ova je za interneto ono što je acquis communotaire za Evropsku uniju.

[123] Popis RFC-ova koji su promenili status nalazi se na https://www.rfc-editor.org/status_changes.php

nego što je stupila na snagu sadašnja klasifikacija bili objavljeni. Oni su upravo dokaz promene tokom decenija atmosfere u internet zajednici. Atmosfera je od ležerne, nepretenciozne, zaljubljeničke u internet, išla ka uozbiljenoj, deideologizovanoj, onoj koja favorizuje specijaliziranost i fragmentarnost. Ono što je ostalo isto nezavisno od protoka godina je viđenje autorstva RFC-a kao pragamtičnog, baziranog na iskustvu, na dostignuću pojedinaca ili malih radnih grupa. Svi RFC-ovi zajedno doprinose tradiciji RFC-a, svedočanstvo su kontinuirane evolucije interneta, a odražavaju i snagu koncenzusa i nenametanja bilo čega. Čak ni oni RFC-ovi u kojima je opisan neki internet standard (takvih je vrlo malo) nisu nalik zakonu, tj. nešto što nameće normu, već su više kao pomoć korisnicima da lakše rešavaju nedoumice oko najrazličitijih protokola, aplikacija itd.

Za izradu jednog RFC-a obično je potrebno mesec ili dva vremena. Sada postoji i lista čekanja, tj. trenutno (februar 2016. god.) oko 130 dokumenata o raznim pitanjima vezanim za internet čeka da ih IETF razmotri i da urednik odluči da li će biti objavljeni (od ovih 130 samo jedan dokument je podnet još 2012. i par njih iz 2014. godine, dok svi ostali zaista ne čekaju dugo).[124]

Najvažnija inovacija vezana za RFC odigrala se jula 2007. god. kada su definisani kanali za RFC. Tada je rešeno da će postojati četiri kanala, odnosno izvora iz kojih kreće predlog i izrada RFC: 1) IETF, 2) IRTF, 3) IAB i 4) nezavisno predlaganje. IETF ima prednost nad drugim kanalima u smislu da se kvalitet RFC-a koji predlažu druga tela proverava da ne bi bio u sukobu sa onim što daje IETF. Jedino IEFT ima mogućnost da kreira RFC koji bi doneli standarde i najbolju trenutnu praksu, ali ostale kategorije RFC-a mogu kreirati svi kanali.[125]

Posebno je zanimljiva jedna vrsta RFC-ova, koji se klasifikuju kao informacioni RFC, a koji sadrže prvoaprilske šale i humorističke priče/duhovitosti vezane za period Božića –naravno, inspirisane internetom u najširem smislu. Letimični pregled ovog „žanra“ RFC-a može se naći na vikipediji[126] gde je bavljenje šaljivim RFC-ovima kao bavljenje kuriozitetom. Inače je uključivanje šala u aktivnosti dizajna interneta potpuno neistraženo. Ono je, po meni, deo inicijalne arhitekture interneta, možda jedini koji je (neopaženo) preživeo. Zato ćemo ovde samo ukazati na ove RFC-ove.

[124] Popis RFC-ova koji su na čekanju nalazi se na https://www.rfc-editor.org/current_queue.php
[125] Preuzeto sa http://en.wikipedia.org/wiki/Request_for_Comments
[126] Pogledati https://en.wikipedia.org/wiki/April_Fools'_Day_Request_for_Comments

Šala je prvi put objavljena u jednom RFC 1973. god. To je bio RFC 527 pod nazivom „ARPAWOCKY“[127] kao parodija na šaljivu besmislenu pesmu Luisa Kerola Jabberwocky. ARPA je, razume se deo naziva prve internet mreže ARPANET-a. (U prevodu Ivana V. Lalića Jabberwocky je prevedeno kao Karazubijada (srpski jezik), a u prevodu Antuna Šoljana kao Hudodrakija (hrvatski jezik)).

Takođe je i 1978. god. objavljena prvoaprilska šala u RFC 748 „Opcija TELNET nasumično izgubljeno“[128] na temu gubljenja paketa koja je bila parodija, ali su je neki shvatali i ozbiljno, pa je uz ovaj RFC jedno vreme stajala napomena „pogledaj datum objavljivanja“.

Počev od 1989. god. prvoaprilske šale su se uobičajile. Jedna od boljih je bila ona Dejvida Vaicmana (David Waitzman) iz 1990. god. pod nazivom „Standard za transmisiju IP datagrama na avianskim nosačima“ (RFC 1149[129]), koja je čak doživela i nekoliko ažuriranja. Avianski nosači su ptice, odnosno u ovom slučaju domaći golubovi, koji su upotrebljeni da prenesu internet pakete. Izveden je eksperiment koji je pokazao da je u tom načinu transmisije nepovoljan racio gobitka paketa, varirajuće vreme odgovora itd.

Za Prvi april 1996. napravljen je RFC 1925 pod nazivom „Dvanaest istina o umrežavanju“[130] u kome su sažete „fundamentalne istine koje leže u osnovi svakog umrežavanja“. Tačnije bi bilo reći da je tu reč o izrazima frustracije eksperata u njihovom svakodnevnom poslu. Neke od „istina“ glase: „Mora da proradi“, „Bez obzira koliko se trudiš i bez obzira koliki je prioritet, ne možeš povećati brzinu svetlosti“, „Lakše je prebacivati problem tamo amo (na pr. prebaciti problem u drugi deo ukupne arhitekture mreže) nego rešiti ga“, „Uvek je nešto“ itd.

Za Prvi april 1998. godine nastao je RFC 2324 „Hipertekst protokol za kontrolu ločića za kafu“[131] ili skraćeno HTCPCP. „Kafe ima širom sveta. U svetu u kome su kompjuteri sveprisutni, kompjuteristi sve više žele da pripremaju kafu. Kuvanje kafe je umetnost, ali distribuirana inteligencija umreženog sveta transcendira umetnost.

[127] RFC 527 “ARPAWOCKY” http://tools.ietf.org/html/rfc527
[128] RFC 748 “TELNET randomly-lose Option” http://www.rfc-archive.org/getrfc.php?rfc=748
[129]RFC 1149 “A Standard for the Transmission of IP Datagrams on Avian Carriers” https://tools.ietf.org/html/rfc1149
[130] RFC 1925 “Twelve Networking Truths” http://tools.ietf.org/html/rfc1925
[131]RFC 2324 “Hyper Text Coffee Pot Control Protocol (HTCPCP/1.0)” http://tools.ietf.org/html/rfc2324

Stoga, postoji jaka, tamna, bogata potreba za espresno dizajniranje protokola za kuvanje kafe.“[132]

U 2000. godini šala je imala naziv „Set protokola beskonačnog majmuna (SPBM)“ (RFC 2795[133]) i bila je usmerena na tzv. teoremu beskonačnog majmuna a dokument „uključuje protokole za majmune i organizacije koje imaju interakciju sa njima“. Ova teorema (po jednoj od svojih mnogobrojnih formulacija) kaže da kada bi se neograničen broj majmuna stavio za tastature kompjutera na beskonačno vreme, oni bi, nasumično udarajući dirke, skoro sigurno otkucali kompletno delo Vilijama Šekspira. „Skoro sigurno“ je precizno definisan matematički termin, dok je „majmun“ metafora za bilo koji uređaj koji proizvodi beskonačne nasumične sekvence slova i simbola. U ovom RFC autori se, koristeći tipičan jezik kompjuterskih protokola, šale na račun komunikacije između pisaca i kritičara.

Nešto novijeg datuma, RFC 5841 iz 2010. god. predlaže (kako naslov najavljuje) „Opciju TCP za označavanje raspoloženja paketa“.[134] Šala se tiče često korišćenih emotikonica. „Paketi ne mogu da osećaju. Oni su stvoreni sa ciljem da prenose podatke iz jednog sistema u drugi. Ipak, jasno je da u specifičnim situacijama neka doza emocije može da se izvede ili doda.“[135] Na primer, paket koji je odbačen i zato mora biti ponovo poslat se može opisati kao besan ili frustriran, ali isto to se može reći i za njegovog vlasnika. Paketi po sebi ne „osećaju“ ali „ljudskost izražena u paketu u celini izvire iz ljudi“. Tako se predlažu sledeće znaci tj. emotikonice za sledeća raspoloženja:[136]

ASCII	Raspoloženje
=====	====
:)	Srećan
:(	Tužan
:D	Razgaljen (obuzet zabavom)
%(	Zbunjen
:o	Smoren (obuzet dosadom)
:O	Iznenađen
:P	Glup ili tupav
:@	Frustriran
>:@	Besan
:|	Apatičan

[132] Ibid. str. 1.
[133] RFC 2795 “The Infinite Monkey Protocol Suite (IMPS)” http://tools.ietf.org/html/rfc2795
[134] RFC 5841 “TCP Option to Denote Packet Mood” http://www.ietf.org/rfc/rfc5841.txt
[135] Ibid. str. 2.
[136] Ibid. str. 3.

;) Tajanstven
>:) Zao

A potom slede i duhovita bliža objašnjenja za svako raspoloženje.

S obzirom na špijunsku aferu koja je jako uznemirila javnost 2013. godine, a koja se ticala Nacionalne sigurnosne agencije SAD-a – skraćeno NSA - ne iznenađuje da je 2014. godine tema prvoaprilske šale i RFC 7169 bila „Ekstenzija sertifikata NSA (nećeš sačuvati tajnost – no secrecy afforded)“.[137]

> „Istorijski, klijenti i serveri su težili da zadrže privatnost svojih šifri; međutim, tajnost njihovih privatnih šifri ne može uvek biti očuvana. U određenim okolnostima, klijent ili server bi mogli da osete da su prinuđeni da u budućnosti daju svoje šifre trećoj strani. Neki klijenti i serveri su već bili prisiljeni da podele svoje šifre i hteli bi da obaveste sve strane o ažuriranju sertifikata u smislu da su njihove šifre zapravo date trećoj strani.“[138]

Kada vide ovu novu ekstenziju („nećeš sačuvati tajnost“) korisnici treba da budu na oprezu i da se duboko zamisle. „Užurbana analiza bezbednosti nikad nije dobra. U krajnjem, šiframa ne treba verovati. Tajnost je teška.“[139]

Prvoaprilska šala u 2015. godini odnosila se na „Romantično/zeleno rutiranje u IPv6“ (RFC 7511[140]). Ona je bila u duhu „’zelenog IT’ pri čemu će paketi biti rutirani tako da dobiju što je moguće više svežeg vazduha“.

Do sada je u ovom radu „iskorišćen“ tek jedan mali deo RFC-ova: 9 ozbiljnih (RFC-ovi 675, 761, 871, 882, 1122, 1958, 3426, 3439 i 4271) i 9 šaljivih (RFC-ovi 527, 748, 1149,1925, 2324, 2795,5841, 7169, 7511). No i to je dovoljno da se stekne slika o svojevrsnoj vezi između njih i interneta kojim se bave.

Ovde dajemo jedan širi popis RFC-a koji bi mogli biti zanimljivi filozofima i generalno ne-inžinjerima, jer na jednostavan (ne-tehnički) način iznose detalje važne za arhitekturu interneta i duh zajednice internet stručnjaka. (Neki od gore navedenih 18 RFC-ova su uključeni u popis.)

[137] RFC 7169 “The NSA (No Secrecy Afforded) Certificate Extension” https://tools.ietf.org/html/rfc7169
[138] Ibid. str.2.
[139] Ibid. str.2.
[140] RFC 7511 “Scenic Routing for IPv6” https://tools.ietf.org/html/rfc7511

Tabela 2 Lista RFC-ova od interesa za istraživanje arhitekture interneta.

Broj	Naslov RFC (preveden na srpski)	Autor/i	Vreme nastanka	Status
0527	ARPAWOCKY	R. Merryman.	Maj 1973.	Nepoznat
0602	"Čarape su okačene pored dimnjaka brižno "...	R.M. Metcalfe.	Decembar 1973.	Nepoznat
0967	Sve žrtve na gomili.	M.A. Padlipsky.	Decembar 1985.	Nepoznat
0968	U sred noći pre početka.	V.G. Cerf.	Decembar 1985.	Nepoznat
1087	Etika i internet.	DARPA, Internet Activities Board.	Januar1989	Nepoznat
1118	Autostoperski vodič kroz internet.	E. Krol.	September 1989.	Informativan
1121	Prvi čin - pesme.	J. Postel, L. Kleinrock, V.G. Cerf, B. Boehm.	September 1989.	Informativan
1135	Pantljičara kod interneta.	J.K. Reynolds.	Decembar 1989.	Informativan
1149	Standard za transmisiju IP datagrama na avianskim nosačima	D. Waitzman	April 1990.	Informativan
1173	Odgovornosti menadžera kompjutera i mreža: Rezime "usmene tradicije" interneta.	J. VanBokkelen.	Avgust 1990.	Informativan
1272	Računovodstvo interneta: Objašnjenje.	C. Mills, D. Hirsh, G.R. Ruth.	Novembar 1991.	Informativan
1287	Ka budućoj arhitekturi interneta.	D. Clark, L. Chapin, V. Cerf, R. Braden, R. Hobby.	Decembar 1991.	Informativan
1290	Ima zlata u prokletim mrežama! Ili Traženje blaga na pogrešnim mestima.	J. Martin.	Decembar 1991.	Informativan. Zamenjen RFC1402
1296	Rast interneta (1981-1991).	M. Lottor.	Januar 1992.	Informativan
1336	Ko je ko na internetu: Biografije članova IAB, IESG i IRSG.	G. Malkin.	Maj 1992.	Informativan. Zamenjuje RFC 1251
1359	Konektovanje na internet – Šta institucije koje se konektuju treba da očekuju.	ACM SIGUCCS.	Avgust 1992.	Informativan
1462	Za vašu informaciju o "Šta je internet?"	E. Krol, E. Hoffman.	Maj 1993.	Informativan
1775	Biti "na" internetu.	D. Crocker.	Mart 1995.	Informativan
1855	Smernice netikecije.	S. Hambridge.	Oktobar 1995.	Informativan
1882	12 dana tehnologije pre Božića.	B. Hancock.	Decembar 1995.	Informativan
1925	12 istina o umrežavanju.	R. Callon.	April 1996.	Informativan
1935	I šta je uostalom taj internet?	J. Quarterman, S. Carl-Mitchell.	April 1996.	Informativan
1958	Arhitektonski prinicipi interneta.	B. Carpenter, ur.	Jun 1996.	Ažuriran sa RFC3439 Informativan
2150	Umetnosti: Centar za deljenje pozornice na internetu.	J. Max, W. Stickle.	Oktobar 1997.	Informativan
2235	Hronologija interneta.	R. Zakon.	Novembar 1997.	Informativan
2321	RITA – Pouzdani alat za rešavanje problema mreža.	A. Bressen.	April 1998.	Informativan
2324	Hipertekst protokol za kontrolu	L. Masinter.	April 1998.	Ažuriran sa

	šolje kafe (HTCPCP/1.0).			RFC7168 Informativan
2468	SEĆAM SE IANA-e (čitulja za J.Postela).	V. Cerf.	Oktobar 1998.	Informativan
2775	Transparentnost interneta.	B. Carpenter.	Februar 2000.	Informativan
2804	Politika IETF prema snimanju/špijuniranju.	IAB, IESG.	Maj 2000.	Informativan
3092	Etimologija "Fu-a".	D. Eastlake 3rd, C. Manros, E. Raymond.	April 2001.	Informativan
3098	Kako odgovorno reklamirati korišćenjem emejla i novinskih grupa ili– kako NE $$$$$ PRAVITI NEPRIJATELJE BRZO! $$$$$.	T. Gavin, D. Eastlake 3rd, S. Hambridge	April 2001.	Informativan
3426	Opšta razmatranja o arhitekturi i politici.	S. Floyd.	Novembar 2002.	Informativan
3439	Neke smernice i filozofija o arhitekturi interneta.	R. Bush, D. Meyer.	Decembar 2002.	Informativan Ažurirao RFC 1958
3607	Ponovno razmatranje kriptoanalize kineske lutrije: Internet kao alat za probijanje koda.	M. Leech.	September 2003.	Informativan
3724	Uspon sredine i budućnost E-2-E: Refleksije o evoluciji arhitekture interneta.	J. Kempf, R. Austein, IAB.	Mart 2004.	Informativan
3935	Misija IETF-a.	H. Alvestrand.	Oktobar 2004.	Najbolja tekuća praksa
4924	Refleksije o transparentnosti interneta.	B. Aboba, Ed., E. Davies.	Juli 2007.	Informativan
5241	Prava davanja imena (krštenja) IETF-ovih protokola.	A. Falk, S. Bradner.	April 2008.	Informativan
5841	Opcija TCP za označavanje raspoloženja paketa.	R. Hay, W. Turkal	April 2010.	Informativan
6529	Protokol Host/Host za ARPA mrežu.	A. McKenzie, S. Crocker.	April 2012.	Istorijski
6561	Preporuke za čišćenje botova u mrežama ISP-ova.	J. Livingood, N. Mody, M. O'Reirdan.	Mart 2012.	Informativan
6586	Iskustva iz čiste IPv6 mreže.	J. Arkko, A. Keranen.	April 2012.	Informativan
6592	Nulti paket.	C. Pignataro.	April 2012.	Informativan
6921	Razmatranja o dizajnu Brže-od-svetlosti (BOS) komunikacije.	R. Hinden.	April 2013.	Informativan
6948	Neka merenja na Svetski dan Ipv6 iz perspective krajnjeg korisnika.	A. Keranen, J. Arkko	Juli 2013.	Informativan
7033	WebFinger (Prst veba).	P. Jones, G. Salgueiro, M. Jones, J. Smarr.	September 2013.	Informativan
7168	Hipertekst protokol za kontrolu šolje kafe modifikovan za pijenje čaja (HTCPCP-TEA).	I. Nazar.	April 2014.	Informativan Ažurirao RFC 2324
7169	Ekstenzija sertifikata NSA (Nećeš sačuvati tajnost).	S. Turner.	April 2014.	Informativan
7282	O koncenzusu i "hm-anju" u IETF.	P. Resnick.	Jun 2014.	Informativan
7435	Oportunistička bezbednost: Nekakva zaštita većinu vremena.	V. Dukhovni.	Decembar 2014.	Informativan
7457	Sumiranje poznatih napada na bezbednost transportnog sloja (TLS) i datagram TLS (DTLS).	Y. Sheffer, R. Holz, P. Saint-Andre.	Februar 2015.	Informativan
7500	Principi za rad registara IANA-e.	R. Housley, Ed., O. Kolkman, ur.	April 2015.	Informativan

7511	Romatnično/zeleno rutiranje za IPv6.	M. Wilhelm.	April 2015.	Informativan
7624	Tajnost u suočavanju sa sveobuhvatnim nadzorom: model pretnje i definisanje problema.	R. Barnes, B. Schneier, C. Jennings, T. Hardie, B. Trammell, C. Huitema, D. Borkmann.	Avgust 2015.	Informativan
7704	IETF sa više raznovrsnosti i profesionalnim ponašanjem.	D. Crocker, N. Clark.	Novembar 2015.	Informativan

Internet kao izuzetak (izuzetnost interneta)

Inicijalna arhitektura interneta povezivala se sa vrednostima otvorenosti, inovativnosti, slobode, nediskriminacije, demokratičnosti itd. Manuel Kastels je to najbolje sažeo: „Internet je stvoren nevjerojatnim križanjem visoke znanosti, vojnih istraživanja i liberterijanske kulture.“[141] Isto tako i: „internet je smišljeno oblikovan kao tehnologija slobodne komunikacije.“[142] Ovaj ugao gledanja na internet kao otvoren i slobodan, zastupljen u diskusiji o arhitekturi, je pomalo neočekivano još jednom tematizovan u novom kontekstu - kontekstu interneta finansijski moćnih korporacija koje se bave internet sadržajima. To se desilo zahvaljujući Timu Vuu, američkom filozofu koji se bavi problemima i razvojem interneta. Iako internet kao medij izlazi iz okvira ovog rada, ovde ćemo ukratko pogledati način tematizovanja tj. kako se ista vrednosna obojenost (do sada prikazana u arhitekturi) diskutuje u kontekstu tržišta komunikacija. Radi se o ponovnom vraćanju jedne teme nakon što je prva generacija internet pionira, najvećih zagovornika ove teme, utihnula. Vraćanje se odigralo u formi dileme da li je u budućnosti moguć, internet prožet liberalnim vrednostima.

Zapravo u svom eseju iz 2010. godineTim Vu se zapitao : da li postoji izuzetnost interneta, i to izuzetnost koja ne bi bila prolazna već trajna odlika?[143]

Ovo pitanje je zanimljivo po tome što ga Vu na neki način postavlja po drugi put. Naime, Vu priznaje da je njegova prethodna knjiga, *Ko kontroliše internet*, koju je napisao 2006. godine zajedno sa Džekom Goldsmitom,[144] dokazala da internet nije

[141] Manuel Castells. (2003). *Internet galaksija. Razmišljanje o internetu, poslovanju i društvu*, Naklada Jesenski i Turk, Zagreb. .Str. 28.
[142] Ibid. str. 15.
[143] Tim Wu. (2010). “Is Internet Exceptionalism Dead?” in: *The Next Digital Decade: Essays on the Future of the Internet*. Eds. Berlin Szoka and Adam Marcus.TechFreedom, Washington D.C. Dostupno na http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1752415 (U daljem tekstu „Izuzetnost“)
[144] Jack Goldsmith and Tim Wu. (2006). *Who Controls the Internet? Illusions of a Borderless World*. New York, Oxford University Press.

izuzetak. Tadašnja teza zagovornika izuzetnosti bila je da se izuzetnost sastoji u tome što internet nije pod kontrolom vlada tj. suvernih država, i u ovoj knjizi je teza pobijena odnosno dokazano je da internet nije izuzetak po tome (što ne podleže zakonima teritorijalnih država).[145] Ispostavilo se da je Vu u međuvremenu naišao na drugu mogućnost u čemu bi se mogla sastojati izuzetnost interneta – u ideologiji interneta.

«Ako je internet izuzetan na trajan način, to mora biti zbog njegove ideologije koja se izražava u njegovoj tehnologiji.»[146] Otkud ideologija? Vu zapravo svoju tezu povezuje sa tezom Aleksisa de Tokvila o američkoj izuzetnosti. „De Tokvil svodi američku izuzetnost na konkretne osobine SAD – religioznost njenog osnivanja, blizina a ujedno udaljenost od Evrope i, kako je on pisao, 'hiljadu posebnih ciljeva'".[147] Kako Vu pronalazi kod drugih autora koji tumače De Tokvila, američka izuzetnost se prvenstveno sastoji u tome da SAD potiču iz revolucionarnog događaja i da im je razlog postojanja konkretna ideologija. Vu citira Hofstedera koji je rekao: „Naša sudbina kao nacije je bila ne da imamo ideologiju nego da budemo jedna ideologija".[148] Dakle, teza koju Vu iznosi je sledeća:

> «Kada pogledamo internet, njegov nastanak i razvoj, možemo naći isti obrazac revolucije, ideologije i mnogih 'posebnih ciljeva'. Iako je dobar deo toga bio čisto tehnološki, postojale su i duboko revolucionarne ideje, čak i u tehnološkim standardima, u srcu interneta, premda se ponekad do njih došlo na slučajan način ili iz pragmatičnih razloga.»[149]

Ideologija interneta (i njegovih osnivača) bila je jedna vrsta pragmatičnog libertarijanizma. Vu u prilog tome citira znamenitu izreku Dejvida Klarka: „Odbacujemo kraljeve, predsednike i glasanje. Verujemo u približni koncenzus i funkcionalni kod", ali i Postelovo „Budi liberalan u onom što primaš od drugih."[150]

Sledeće potkrepljenje koje Vu donosi je ovo:

> „Kada je Vint Cerf ... prebacio internet na TCP/IP protokol 1982. godine (njegovo efektivno 'lansiranje'), većina informativnih mreža ... se mogla opisati kao diktature od vrha ka dnu. Jedan entitet – obično

[145] Knjiga *Who Controls ...* iz današnje perspective deluje kao napor da se smanji entuzijazam koji je na početku milenijuma postojao oko fenomena i pojma globalizacija. "Internet se video kao suštinski katalizator savremene globalizacije, i imao je centralno mesto u debatama o tome šta globalizacija znači i kuda vodi." Str. 179. Međutim, autori knjige su tu upozorili da teorije globalizacije i interneta pogrešno razumeju i jako podcenjuju važnost teritorijalnih vlada. Str. 180.
[146] "Izuzetnost" Str. 183.
[147] "Izuzetnost" Str. 183.
[148] "Izuzetnost" Str. 183
[149] "Izuzetnost" Str. 183.
[150] "Izuzetnost" Str. 184.

> neka firma ili deo države (ili oba), kao AT&T ili BBC, je odlučivao kakva će ta mreža biti. Suprotno tome, internetom se vladalo više kao federacijom mreža, i u nekim aspektima kao republikom korisnika. To je implicitno u sposobnosti bilo koga da poseduje IP adresu, postavi internet stranicu i objavljuje informacije – nešto što nikad nije bilo i ni sada nije tačno ni za jednu drugu mrežu.“[151]

Na bazi ovih opservacija i argumenata, Vu izvodi da je dovoljno uverljiva teza da bi internet mogao biti izuzetak. Ipak, drugo je pitanje da li bi ta izuzetnost mogla biti trajno stanje. Po njemu, odgovor je negativan. Ono što internet čini izuzetnim je samo prva faza u razvoju dotične tehnologije. «Prolaznost *svih* sistema sugeriše da barem nešto od onog što sada uzimamo kao intrinsično našem informacionom životu i prirodi interneta *će* izbledeti.»[152] Drugim rečima, Vu (u pomenutom eseju) očekuje preokret u kome «otvorenost prestaje, biva zamenjena boljom produktivnošću i čvršćom kontrolom. Drugim rečima, sve se vraća u normalu, ili u najmanju ruku u ono što se smatralo normalnim kroz veći deo ljudske istorije.»[153]

To što je u pomenutom eseju nagovestio da predviđa da će se internet promeniti na način na koji su se promenile pre njega i sve druge komunikacione tehnologije u 20. veku, Vu je detaljno istražio u zasebnoj knjizi posvećenoj istoriji komunikacionih tehnologija (pretežno u SAD-u). Radi se o knjizi o pod nazivom G*lavni prekidač: uspon i pad informacionih imperija.*[154] Za naslov knjige je iskoristio donekle sugestivan i vrlo ilustrativan termin glavni prekidač (na engl. master switch). (Termin je pozajmio od Freda Fenlija, predsednika jedne američke televizijske kuće, koji je izjavio: “Imamo debate o slobodi govora ali pravo pitanje je ko kontroliše glavni prekidač, ko komanduje osnovnom arhitekturom koja određuje ko govori“.[155])

Na bazi istorijskog pregleda razvoja komunikacionih tehnologija u SAD-u (telefona, radija, filma, televizije), Vu je postavio tezu o cikličnom kretanju koje se dešava svakom novom mediju. Otvoreno je pitanje da li je Vu tu tezu i dokazao, što nije predmet ovog rada. Međutim, ako bi bilo dokazano, to ciklično kretanje bi moglo da predvidi i budućnost interneta. Krug podrazumeva da novi medij započinje otvorenošću, pluralizmom, amaterizmom i podsticanjem inovativnosti, ali vremenom

---

[151] “Izuzetnost” Str. 184.
[152] “Izuzetnost” Str. 187.
[153] “Izuzetnost” Str. 185.
[154] Tim Wu. (2010). *The Master Switch: The Rise and Fall Of Information Empires.* New York Vintage Books.
[155] Navedeno prema Vuovom intervjuu u televizijskoj emisiji *The Agenda* kanala TVO. Dostupno na http://www.youtube.com/watch?v=M-ZXNaXvSUE

biva zarobljen od zagovornika centralizma i dovodi do monopola i kosolidacije tj. do nastanka tzv. informacionog carstva. Sa tim carstvom nastaje i ozloglašeni glavni prekidač, ili nekoliko njih. Vu je imenovao kompanije koje danas imaju glavni prekidač za internet – pre svega su to Gugl, Epl i Fejsbuk, kompanije preko kojih smo u vezi sa informacijama, zabavnim sadržajem i svojim društvenim kontaktima.

Gostujući u jednoj od brojnih televizijskih emisija vezanih za svoju knjigu koja je uzburkala javnost, Vu je rekao:

> „Bez izuzetka, vrle nove tehnologije dvadesetog veka – čije slobodno korišćenje je u početku bilo ohrabrivano, u cilju daljih izuma i individualne ekspresije – na kraju su evoluirale u privatno kontrolisane industrijske džinove, divove 'starih medija' u 21. veku, u kojima su protok i priroda sadržaja strogo kontrolisani zarad trgovine.“[156]

Ono što se može smatrati slabim tačkama u Vuovoj tezi da će internet potpasti pod dominaciju monopolista jeste sledeće:

- globalna dimenzija interneta tj. činjenica da se veliki deo interneta «dešava» izvan SAD-a i da pomenute američke kompanije imaju konkurente u Aziji i drugde;
- činjenca da tri pomenute kompanije (koje se prvenstveno bave sadržajima na internetu) nisu ni blizu toga da postanu vlasnici fizičkog sloja interneta, infrastrukture koja je u posedu trenutno finansijski mnogo jačih kompanija;
- činjenica da vlada SAD ali ni druge vlade barem nominalno ne podržavaju kreiranje monopola objedinjavanjem svih slojeva interneta u istim rukama, jer bi to ugrozilo interese brojnih aktera, uključivo i običnih korisnika, a samim tim i interese političara kada dođe do izbora.

Bilo kakvo da je naše mišljenje danas o ovim kompanijama na koje Vu upozorava, ostaje pitanje da li su baš one od presudnog značaja za izuzetnost interneta u načelu. Internet se jako brzo menja, pojavljuje se internet stvari (o čemu će biti reči u poglavlju 7) i moguće je da će se za 5 ili 10 godina pojaviti nove moćne kompanije koje će nuditi neku novu uslugu korisnicima. Da li će i te nove kompanije imati istu putanju tj. ciklus, od decentralizovanih ka centralizovanim odnosno monopolu? Da se podsetimo, pitanje je glasilo: da li izuzetnost, određena u smislu ideologije, može

[156] Weisberg, J. and Wu, T. (11. nov.2010). Discusija o knjizi *The Master Switch* za New America Foundation. Dostupno na https://www.youtube.com/watch?v=7uxJwBu-gK0 (pristupljeno 29.02.2016.)

ostati trajna odlika interneta? Odgovor mora glasiti: ne možemo znati. Svakako to nije ni garantovano ni isključeno.

Vu zaključuje svoj esej zanimljivim obrtom: ako može da se smatra neospornom paralela između američke izuzetnosti (u De Tokvilovom smislu) i izuzetnosti interneta (u smislu njegove ideologije otvorenosti, pluralizma itd.), a budući da se američka izuzetnost nastavlja i preko 200 godina od svog nastanka, onda bi i izuzetnost interneta mogla da se nastavi pod istim uslovima naredni niz godina. Vu smatra da je glavni uslov: da mi to želimo. Još preciznije rečeno: da budemo u stanju da to odbranimo. Taj stav zastupa i autoka ovog rada: odgovornost za vrednosnu obojenost i budućnost interneta je na krajnjim korisnicima. Vu objašnjava:

> «Možda je vrlo 'prirodno' da demokratija, posle nekoliko decenija ili pre, sazri u diktaturu neke vrste, s obzirom na frustracije i neefikasnosti demokratske vlade. ... Ali ideja američkog ekcepcionalizma imala je u sebi posvećenost da se pokuša izbeći ta sudbina, ... SAD ostaju izuzetak od starog pravila da republike neizbežno kolabiraju u diktaturu pod zamahom velikog vođe. Internet je za sada izuzetak od pravila da otvorene mreže neizbežno postaju zatvorene i dominirane od strane države ili malog broja moćnih monopolista. Dvadeset pet godina nakon dot.com, mi bismo mogli da tvrdimo da i dalje imamo republiku informacija – ako je možemo sačuvati.»[157]

Ovde nećemo komentarisati tezu o republikama kao nestabilnima političkim oblicima, osim što ćemo napomenuti da politička teorija o tome nije jednoglasna. Ipak, paralela po kojoj, kao što opstanak političkog sistema zavisi od građana tako i opstanak decentralizovanog interneta zavisi od korisnika interneta, ima argument sebi u prilog. Taj argument je uvažavanje faktičke moći velikog broja - bilo građana bilo korisnika interneta. Disperzija moći je podloga za subverziju neprihvaćenog poretka, bilo da je reč o političkoj zajednici bilo o internetu. Zato se izuzetnost interneta može očuvati.

[157] „Izuzetnost“ Str. 187.

ČETVRTO POGLAVLJE

Upravljanje internetom – definicija

Upravljanje internetom je višeslojno i višeaktersko. Korisno je razlikovati upravljanje u užem i širem smislu – u užem smislu misli se na rad (transnacionalnih) institucija koje vrše upravljanje ključnom infrastrukturom interneta, dok u širem smislu misli se na suverene države koje donose politike regulisanja brojnih oblasti u kojima se aktivnosti vrše na internetu ili su na određeni način povezane sa internetom (trgovina, kriminal, sloboda govora, intelektualna svojina i autorska prava i sl.).

U upravljanje internetom u užem smislu ubrajaju se tri funkcije: tehnička standardizacija, raspodela i dodela specifičnih internet resursa i politika rešavenja sporova (oko standarda ili resursa). Ove funkcije se nalaze pod kontrolom transnacionalnih ekspertskih tela sa raznovrsnim članstvom odnosno tela *sui generis*.

S druge strane, u strukturi interneta ključnu ulogu imaju ISP-ovi (iz svih segmenata: tier 1, 2 i 3) kao oni koji korisnicima omogućavaju pristup internetu. Kontrola nad ISP-ovima kao i nad klijentima tj. korisnicima interneta je u rukama nacionalnih vlada, tj. ovu kontrolu sprovode države na svojoj teritoriji. Države time dobijaju prostor da regulišu pitanja iz domena upravljanja internetom u širem smislu. To bi se odnosilo na pitanja sprovođenja zakona, prevencije kriminala i sajber bezbednosti, zaštite podataka, zaštite privatnosti, nadzora itd. Neka od ovih pitanja imaju prekogranične efekte i zahtevaju saradnju država, tako da se u nivo upravljanja u širem smislu uključuju i međunarodne organizacije (Ujedinjene nacije, Savet Evrope i dr.). Takođe se javljaju i udruženja korisnika odnosno organizacije civilnog društva koje žele da se čuje glas najšireg kruga zainteresovanih strana.

Uz pomenute aktere, postoji i realnost posebnog tipa upravljanja, tzv. mrežnog upravljanja koje se posebno vidi na delu kod ponašanja autonomnih sistema i rutiranja, a ponekad i u kriznim situacijama za infrastrukturu interneta. To je tip upravljanja koji je formalno neuređen, ali deluje u praksi; ključ njegovog uspeha je u ličnoj inicijativi najmotivisanijih aktera, ali i u čuvanju odnosa moći među akterima kojim su oni u datom trenutku zadovoljni.

Tela koja upravljaju internet standardima

U sada već 40-ogodišnjoj istoriji postojanja interneta postojalo više tela koja su se bavila kreiranjem internet standarda, ali i menjala svoje funkcije, prestajala da postoje i sl. Stoga će se ovde ukratko predstaviti tela[158] koja danas imaju najdominantniju ulogu u ovome.

Internet društvo (Internet Society, skraćeno ISOC)[159] osnovano je 1992. god. a inicijalno da je vodio Vinton Cerf. Jedan razlog za osnivanje ove organizacije je da se od sudskih tužbi zaštite pojedinci koji su uključeni u kreiranje internet standarda, odnosno da odgovornost za kreiranje internet standarda preuzme na sebe jedna krovna organizacija. Drugi razlog postojanja organizacije je obezbeđivanje finansiranja za rad na internet standardima. Organizacija zadržava i autorsko pravo nad svim objavljenim RFC-ima. Od 2002. god. ISOC upravlja Registrom javnog interesa, što znači da alocira imena domena pod top level domenom .org. Takav domen košta oko 7 USD, ali zbog interesa koji vlada za ovim domenima, obezbeđuje znatan prihod ovoj organizaciji. Organizacija je registrovana u Vašingtonu kao neprofitna korporacija, sa kancelarijama u Ženevi (Švajcarska) i Restonu (SAD), a prihvata i organizaciono i individualno članstvo. U ISOC-u radi oko 30 zaposlenih a ima upravni odbor od maksimalno 20 osoba, u koji se bira na period od 3 godine od strane različitih segmenata članstva.

Odbor za internet arhitekturu (Internet Architecture Board - IAB)[160] osnovan je 1992. godine sa ciljem da nadgleda razvoj internet standarda posebno iz dugoročne perspektive. Ima 13 članova, koji nastupaju u individualnom svojstvu, kao istaknuti stručnjaci. Slično telo postojalo je pod drugim nazivom još od 1979. godine. Formalno je u statusu odbora unutar IETF i savetodavnog tela u ISOC-u. Odbor vrši imenovanja u razna druga tela i služi kao drugostepeno telo za razmatranje žalbi vezanih za procedure primenjene kod razvoja internet standarda.

Inžinjerska radna jedinica za internet (Internet Engineering Task Force - IETF)[161] osnovana 1986. godine je radno telo u kome se razvijaju stanardi interneta. Njen

[158] U razvoju internet standarda ili u širenju interneta određeni doprinos su dala organizacije: Internet System Consortium, Institute of Electrical and Electronics Engineers, International Telecommunications Union itd.
[159] Zvanična internet stranica ove organizacije nalazi se na http://www.internetsociety.org/
[160] Zvanična internet stranica ove organizacije nalazi se na https://www.iab.org/
[161] Zvanična internet stranica ove organizacije nalazi se na http://www.ietf.org/

osnovni zadatak je „učiniti da internet bolje radi“. Ona proizvodi publikacije u kojima su opisani internet standardi, odnosno bavi se najurgentnijim operativnim i tehničkim problemima na internetu i predlaže rešenja kroz specifikaciju standarda. IETF nije pravno lice, već se sastoji od otvorenog i dobrovoljnog međunarodnog članstva koje se tri puta godišnje okuplja uživo a izvan toga komunicira putem imejl lista. Najčešće su članovi IETF inžinjeri, dizajneri, operatori, prodavci i istraživači. Odluke se donose približnim koncenzusom, sa naglaskom na otvorenosti, pravičnosti i inkluzivnosti. Način rada je preko formiranja radnih grupa u jednoj od osam tematskih oblasti: aplikacije, rutiranje, bezbednost, transport itd. Trenutno ima oko 120 radnih grupa. Svaka radna grupa imenuje jednu osobu koja je predsedavajući radne grupe i koja je formalna kontakt osoba između grupe i direktora tematske oblasti. Proces rada u radnoj grupi odvija se u skladu sa standaradizovanim procesom koji je definisan u RFC 2026 „Proces internet standarda – revizija 3“.[162] Rezultat rada tj. predloženo rešenje znači samo: „IETF se dogovorio da ’ako hoćeš da uradiš datu stvar, ovo je opis kako to da uradiš’“.[163] Pridržavanje standarda je dobrovoljno i „standard ne implicira bilo kakav pokušaj od strane IETF da naredi njegovu upotrebu ili da kontroliše njegovo korišćenje – već samo da „ako kažeš da radiš to i to prema standardu, uradi ga na ovaj način“.[164] Standardi mogu imati različite „nivoe zrelosti“ odnosno mogu biti: a) predloženi standard b) nacrt standarda i c) puni internet standard. Postoji procedura kako rešenja mogu napredovati od jednog nivoa do drugog. Međutim, većina standarda nikad ne prelazi prvi nivo zrelosti jer ostvaruju svoju svrhu i bez tog ozvaničenja.

Inžinjerska uprava za internet (Internet Engineering Steering Group - IESG) je izvršno telo IETF-a i zadužena je za osiguranje kvaliteta rada IETF. To čini kroz ustanovljavanje i gašenje radnih grupa, izbor njihovih predsedavajućih, praćenje napretka i koordinaciju među njima, kao i odobravanje njihovih dokumenata. Sastoji se od predsedavajućeg IETF i direktora tematskih oblasti. Članovi IESG biraju se kroz isti postupak kao i članovi IAB.

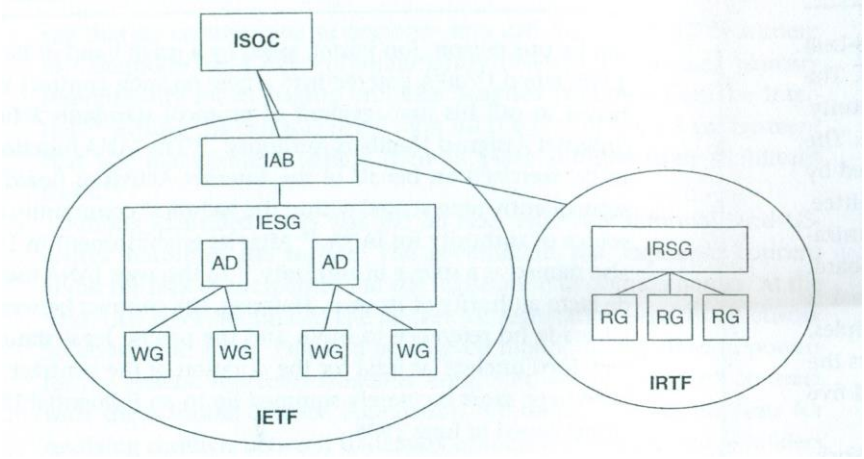
Istraživačka radna jedinica za internet (Internet Research Task Force - IRTF) fokusira se na dugoročna pitanja u istraživanju interneta. Način rada sličan je kao kod IESG, ona radi kroz istraživačke grupe. Trenutno ima 12 istraživačkih grupa, za

[162] RFC 2026 “The Internet Standard Proces – Revision 3” https://www.ietf.org/rfc/rfc2026.txt
[163] *Internet Governance* Str. 98.
[164] *Internet Governance* Str. 99.

pitanja kao što su borba protiv spema, kripto zaštita, kontrola zakrčenja na internetu i sl. I ona ima svoje izvšrno telo (Internet Research Steering Group – IRSG) tj. urpavu. U upravi se osim članova iz ostalih tela nalazi i ad hoc slobodno članstvo (ad hoc membership at large).

Organizaciona shema ovih tela izgleda ovako:[165]

Ilustracija 8 Dijagram - organizaciona šema tela koja upravljaju internet standardima



Preuzeto sa Lee A. Bygrave and Jon Bing, eds. *Internet Governance: Infrastructure and Institutions*, New York, Oxford University Press. 2009 Str. 100.

Tela koja upravljaju raspodelom i dodelom internet domena i adresa

telo koje upravlja internetom u smislu vršenja raspodele i dodele ključnih resursa, a to su internet domeni i adrese je **Korporacija za dodeljena internet imena i brojeve** (Internet Corporation for Assigned Names and Numbers – ICANN),[166] po mnogima i sinonim sa upravljanjem infrastrukturom interneta. Ona postoji od 1998. godine. Pre njenog formiranja istu funkciju je vršilo neformalno ustanovljeno Telo za dodeljene internet brojeve (Internet Assigned Numbers Authority – IANA).

Osnovni zadaci koje ICANN obavlja su:

[165] *Internet Governance* Str. 100.
[166] Zvanična internet stranica ove organizacije nalazi se na https://www.icann.org/

1. kreiranje politike i smernica za alociranje blokova internet brojeva (IP adresa),
2. nadgledanje rada autoritativnog rut server sistema (DNS),
3. nadgledanje politike koja određuje okolnosti pod kojima će se novi top level domeni dodati u rut sistem,
4. koordinacija dodele ostalih tehničkih parametara interneta neophodna za održavanje univerzalne povezanosti na internetu,
5. ostale aktivnosti potrebne za koordinaciju specifičnih funkcija upravljanja sistemom imena domena.[167]

ICANN je registrovan u Kaliforniji kao neprofitna korporacija za javno dobro i ima ugovorni odnos sa Ministarstvom trgovine SAD, koji se periodično obnavlja.

Za funkcionisanje interneta (i komunikaciju među računarima u mreži) bilo je vitalno da se funkcija dodeljivanja internet brojeva (IP adresa) obavlja tehnički besprekorno. Jon Postel je bio stručnjak, zaposlen u jednom američkom institutu, koji je praktično sam obavljao tu funkciju uključujući i zadatak ažuriranja rut servera. On je sam i smislio nekakvo telo nazvavši ga IANA. Zbog nespornog ugleda koji je uživao među kolegama inžinjerima, bilo je moguće da stvar funkcioniše bez preciznog pravnog statusa takvog tela. IANA je uživala veliku moć nad internetom a da praktično formalno nikad nije ni formirana. Glavni server je fizički bio lociran na institutu u sklopu Univerziteta Južne Kalifornije koji je bio učesnik u projektima DARPA. Međutim, kada je istekao ugovor između instituta na kome je radio Postel i DARPA, američka vlada je odlučila da sve funkcije IANA budu prenete na novo telo ICANN. Imenovan da rukovodi ICANN-om bio je upravo Postel, ali je nedugo potom umro.

Sam transfer „nadležnosti“ od IANA na ICANN nije prošao bez izvesnog otpora, koji je trajao nekih deset dana. Iako je Jon Postel po mišljenju mnogih bio pravi heroj interneta, u ovom slučaju argumenti vlade SAD zašto je potrebno drugo telo su bili validni. Dotadašnji režim upravljanja jedinstveno dodeljenim parametrima interneta imao je značajne nedostatke. Bio je uređen ad hoc, dominantno SAD-centričan, sa manjkom konkurencije u registraciji imena domena (samo jedna kompanija NSI-Network Solutions Inc je bila ovlašćena za registraciju tri najvažnija top level domena .com, .net i .org) a ni procedura za rešavanje sporova oko imena domena nije bila optimalna.

[167] *Internet Governance* Str. 106.

Prilikom formiranja ICANN-a 1998. godine izrečena je jedna rečenica koju ne treba zanemariti ni danas. Savetnik predsednika SAD Klintona Ira Magaziner bio je taj koji je inžinjerima i tehnokratima okupljenim oko Cerfa ukazao da vlada SAD neće prepustiti kontrolu nad internetom. „SAD su platile za internet, on je stvoren pod njihovim okriljem, i ono što je najvažnije sve što su Postel i Network Solutions Int. radili bilo je na bazi ugovora sa vladom“.[168]

ICANN ima planirani budžet od 200 miliona USD za 2014. godinu, od čega bi se 46 miliona USD smatrali kao profit (iako su neprofitna organizacija). Prihodi u budžetu se generišu delom od akreditacionih naknada (koje plaćaju firme koje žele da se bave registracijom genričkih top level domena) i transakcionih naknada (deo cene koju korisnik plaća na svaku registraciju domena ili obnavljanje ili transfer istog), a delom od naknada koje plaćaju registri top level domena. Po trenutnom stanju, registri nacionalnih domena (kodova za zemlje) nisu u obavezi da finansiraju ICANN, ali neki od njih daju dobrovoljne priloge i razmatraju uvođenje naknada. Deo prihoda bi trebalo da dolazi od aukcija novih generičkih top level domena.[169] Ipak, uvođenje novih top level domena nije samo finansijski motivisano. Smatra se da broj registrovanih top level domena ostaje otprilike isti, bez obzira na uvođenje novih i širu paletu za izbor, budući da se sa uvođenjem novih u jednakoj meri smanjuje broj starih top level domena.[170]

ICANN ima 306 zaposlenih, i ne postoji nikakvo individualno ili organizaciono članstvo. Formalno ustrojstvo organizacije se sastoji od:

- odbora direktora, kome pomažu:
    - organizacije za podršku i
    - savetodavni komiteti.

Odbor direktora ICANN-a se sastoji od 15 članova sa pravom glasa i 6 članova bez prava glasa koji dolaze iz srodnih tela.

Organizacije za podršku (na engl. Support organizations, skraćeno SO) u ICANN-u su nadležne za procese izgradnje politike u svojim oblastima. Ima ih tri:

- Organizacija za podršku u oblasti adresa (ASO) - savetuje Odbor direktora vezano za internet adrese,

[168] Jack Goldsmith and Tim Wu. (2006). *Who Controls the Internet? Illusions of a Borderless World*. New York, Oxford University Press. Str. 41.

[169] Nismo uspeli da dođemo do podatka koliki je prihod od aukcije novih top level domena za period od 2013. god. do danas.

[170] Navedeno prema: http://www.thedomains.com/2013/08/27/icann-approves-200-million-dollar-budget-for-2014-306-employees-still-no-revenue-from-new-gtld-auctions/

- Organizacija za podršku u oblasti generičkih imena (GNSO) - savetuje Odbor direktora vezano za generičke top level domene,
- Organizacija za podršku u oblasti kodova za zemlje (CCNSO) - savetuje Odbor direktora u vezi sa imenima top level domena za države.

Svaku od ovih organizacija za podršku sačinjavaju krovna udruženja aktera direktno zainteresovanih za dotičnu oblast – regionalni internet registri, komercijalni i poslovni korisnici interneta, ne-poslovni korisnici interneta, registri top level domena, nacinalni registri, provajderi internet usluga, zaštitnici intelektualne svojine i sl. U ovim organizacijama kreiranje politike kreće odozdo nagore i teži najvećem mogućem koncenzusu učesnika, a ako dođe do odluke, predlog se iznosi pred Odbor direktora koji samo usvaja ili odbacuje predlog.

Savetodavnih komiteta (na engl. Advisory Committee, skraćeno AC) ICANN-a ima četiri:

- Savetodavni komitet za vlade država (GAC),
- Savetodavni komitet za bezbednost i stabilnost (SSAC),
- Savetodavni komitet za rut server sistem (RSSAC),
- Dobrovoljni savetodavni komitet (ALAC) koji odražava geografsku i društvenu raznovrsnost.

Od savetodavnih komiteta posebno je važan Vladin savetodavni komitet (GAC), koji služi da se politici upravljanja ovim važnim resursima da što veća međunarodna dimenzija, kao kontrateža ranijoj SAD-centričnosti. Vlade svih država mogu biti članice GAC-a a po pozivu to mogu i međunarodne organizacije, kompanije i sl. Uticaj ovog tela je vremenom sve više rastao, tako da postoje i mišljenja da je GAC dobio nešto slično pravu veta. U tome je jedinstven među komitetima. Odbor direktora treba pažljivo da razmotri savet koji mu je dao GAC, a u slučaju da ne usvoji savet GAC-a, treba da obavesti o razlozima za takvu odluku. „Dve strane treba da u dobroj veri i na brz i efikasan način pokušaju da nađu uzajamno prihvatljivo rešenje“.[171] Ako do toga ne dođe, Odbor direktora ICANN mora još jednom da obrazloži svoju odluku. Izjava Odbora će biti bez predrasuda o pravima i obavezama članova GAC-a tj. ticaće se suštine razmatranog pitanja a ne forme.

U samom GAC-u članovi rade na bazi dostignutog konsenzusa, a ako njega nema, predsedavajući GAC-a o tome obaveštava Odbor direktora ICANN-a.

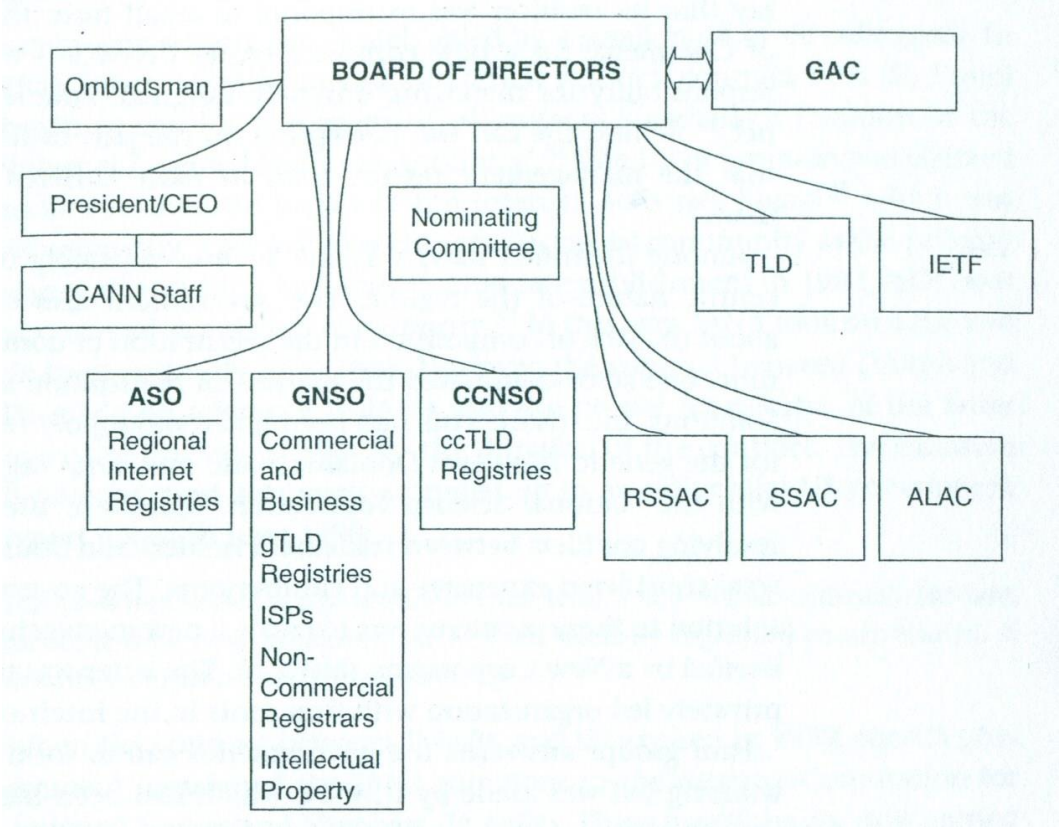
[171] *Internet Governance*, str. 109.

Treba naglasiti da GAC nije organizacija osnovana sporazumom država, niti su članovi GAC-a obavezni da u GAC-u zastupaju zakone koji su važeći u njihovoj zemlji. Kako upućeni opisuju, GAC je više kao šačici vlada koje se dogovoraju o određenoj politici i naginju građenju koncenzusa. Ponegde se uticaj GAC-a na odluke ICANN-a oslikava metaforom «kamilin nos koji viri iz šatora».

Na kraju, u ICANN-u postoji i komitet za imenovanja (Nominating Committee NOMCOM), koji ima ulogu da izabere 8 od 16 članova Odbora ICANN-a, pri tome vodeći računa da odražava raznovrsnost u smislu geografije, kultura, veština, iskustva i perspektiva. S druge strane, članovi ovog komiteta su takođe izabrani od svih ovih tela i po nekim mišljenjima sve izgleda jako komplikovano i „kao da svako izabira svakog“.[172]

Od 2004. god. ICANN je oformio i kancelariju Ombudsmana za nezavisnu unutrašnju ocenu žalbi na nepravičan tretman od bilo kog od ovih tela. Ombudsman nema moć da izmeni odluke u pitanju ali može da posreduje i daje preporuke.

Ilustracija 9 Dijagram - organizaciona šema ICANN



Preuzeto sa Lee A. Bygrave and Jon Bing, eds. *Internet Governance: Infrastructure and Institutions*, New York, Oxford University Press. 2009 Str. 107.

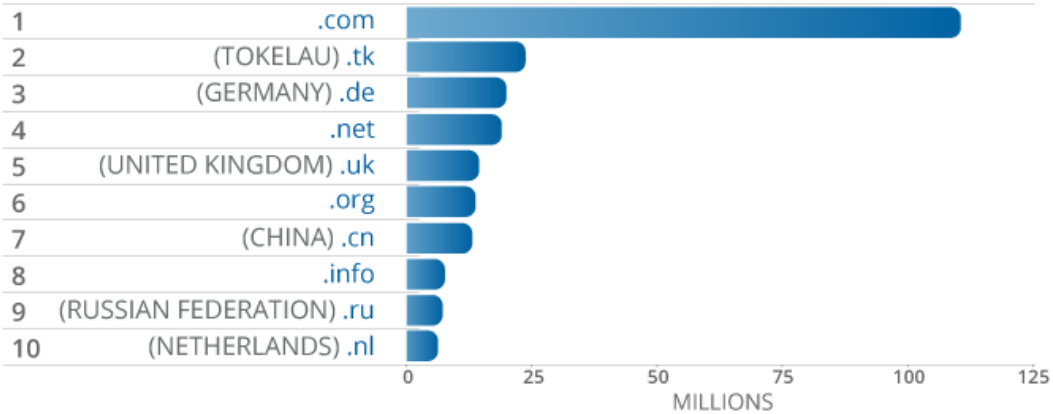
[172] *Internet Governance*, str. 110.

U radu ICANN-a neke aktivnosti ne izazivaju skoro nikakve kontroverze, kao što je slučaj sa dodelom IP adresa, gde se može dobiti slika da je tu reč o telu za tehničku koordinaciju. Međutim, neke aktivnosti izazivaju značajne političke, ekonomske i moralne posledice, pri čemu se menja i slika o ICANN-u kao neutralnom. On postaje telo koje donosi vrednosne sudove. Primer je uvođenje novih top level domena, oko čega su po pravilu nastajali konflikti. Konkretno 2005. god. dat je predlog da se uvede domen .xxx za označavanje pornografskih sajtova, koji je izazvao veliki otpor religioznih grupa, pa i nekih vlada (SAD, Brazil) i bio odbačen 2007. god. Od 2008. god. počela je da se sprovodi liberalizacija politike uvođenja top level domena, tako da se isti ili sličan predlog može ponoviti.

U nastavku ćemo prikazati šta statistika govori o raspodeli internet resursa. Ažurirana statistika dostupna je kvartalno u izveštajima kompanije Verizajn, koja je najveći operater registra internet domena.[173]

Krajem 2013. god. bilo je registrovano više od 271 milion internet domena. Top level domen .com imao je 112 miliona domena, potom sledi .net sa 15,2 miliona domena i .org sa 10,3 miliona domena. Ukupno svi domeni nacionalnih država (kodovi za zemlje) imaju 123,5 miliona domena. Osnovni prikaz distribucije po zemljama i tipovima najzastupljenijih (registrovanih) top level domena je dat ovde:[174]

Ilustracija 10 Rangiranje primarnih level domena po veličini na kraju 2013. godine



Preuzeto iz: *The Domain Name Industry Brief Q4 2013 Highlights* by Versign, http://visual.ly/domain-name-industry-brief-q42013

[173] Ovi izveštaji su dostupni na stranici http://www.verisign.com/en_US/innovation/dnib/index.xhtml?loc=en_US&dmn=dnib

[174] Navedeno prema http://visual.ly/domain-name-industry-brief-q42013

Ilustracija 11 Rangiranje domena kodova za zemlje po broju korisnika na kraju 2013.

Preuzeto iz: *The Domain Name Industry Brief Q4 2013 Highlights* by Versign, http://visual.ly/domain-name-industry-brief-q42013

Interesantno je da se među kodovima za zemlje na tako prominentnom mestu pojavljuje domen .tk. Ovaj kod pripada Tokelau, to jest trima ostrvcima koja se nalaze u blizini Novog Zelanda. Iznajmljivanjem domena sa njihovim kodom bavi se firma iz Holandije. Toliki broj registrovanih domena objašnjava se time što se ti domeni koriste za nelegalne aktivnosti. Svi ti milioni .tk domen nemaju baš nikakve veze sa stanovništvom ili poslovnim subjektima u ovoj „zemlji".

Donosimo i presek stanja distribucije slobodnih i registrovanih top level domena prema dužini imena domena.[175]

Tabela 3 Podaci o mogućim, registrovanim i dostupnim imenima domena

LENGTH OF .com DOMAIN NAME	TOTAL NUMBER OF POSSIBLE .com DOMAIN NAMES	NUMBER OF NAMES REGISTERED IN .com	NUMBER OF NAMES AVAILABLE TO BE REGISTERED IN .com
13	230.6 quintillion	8.6 million	over 230.5 quintillion
12	6.2 quintillion	8.9 million	over 6.1 quintillion
11	168.4 quadrillion	9.0 million	over 168.3 quadrillion
10	4.6 quadrillion	8.7 million	over 4.5 quadrillion
9	123.0 trillion	7.9 million	over 122.9 trillion
8	3.3 trillion	6.9 million	over 3.2 trillion
7	89.9 billion	5.8 million	over 89.8 billion
6	2.4 billion	5.2 million	over 2.3 billion
5	65.6 million	3.1 million	over 62.4 million
4	1.8 million	928.5 thousand	over 845.6 thousand

Preuzeto iz: *The Domain Name Industry Brief Q4 2013 Highlights* by Versign, http://visual.ly/domain-name-industry-brief-q42013

Povremeno se javljaju kritike na račun ICANN-a, i to iz nekoliko uglova:

- kritike načina osnivanja,
- kritike načina rada,
- kritike supervizije od strane vlade SAD-a.

[175] Navedeno prema: http://visual.ly/domain-name-industry-brief-q42013

Vezano za način osnivanja ICANN-a, pojedini kritičari zameraju to što je ovo telo osnovano van granica ustavnog i administrativnog prava SAD-a (po njima bi trebalo podlegati ovom pravu), dok drugi pak zameraju to što jeste ipak u američkom sistemu (po njima bi trebalo biti u međunarodnom sistemu). Koja god strana bila u pravu, ICANN je privatna korporacija koja podleže jurisdikciji savezne države Kalifornije. Ona nema status javnog organa (ni američkog, ni međunarodnog), ali vrši javna ovlašćenja i u samoj svojoj misiji ima smer da služi javnom interesu. ICANN uživa autonomiju privatnog subjekta ali teži da postupa kao globalna transnacionalna organizacija. Neki smatraju da bi se u budućnosti ICANN mogao pretvoriti u međunarodnu organizaciju *sui generis*.

Vezano za način rada, ICANN-u se zamera netransparentnost, sporost, arbitrarnost odlučivanja (naročito u pogledu tema proširenja rut sistema), nedovoljna reprezentativnost grupa iz civilnog društva u kreiranju politika i sl. Postoje i kritike vezane za finansiranje, tj. previsoka sredstva koja se prikupe godišnje (profit) a ne stoje u balansu sa troškovima funkcionisanja ovog tela. Tako jedan od predloga ide u smeru da bi ICANN trebalo da transferiše deo sredstava za pomoć najnerazvijenim zemljama, na primer preko određenog UN fonda.

Vezano za superviziju ICANN-a od strane vlade SAD-a, smatra se da ona narušava transnacionalni legitimitet ICANN-a. Postoji jedan argument koji u toj stvari ima prevagu: «U dugoj istoriji interneta, SAD nisu nikad blokirale pristup internetu nekoj drugoj zemlji, uključujući sukobljene strane.»[176] Pravni okvir koji bi u neku ruku davao legitimitet blokiranju interneta bi recimo bile sankcije koje UN uvede nekoj državi, ali čak i u tim okolnostima zemlji protiv koje su uvedene sankcije do sada nikada nije ukidana mogućnost da bude povezana na internet.

Osnovne vrednosti ICANN-a stoje u njegovom osnovnom aktu, a formulisane su u sklopu njegovih 11 ciljeva:[177]

1. očuvanje i poboljšanje operacionalne stabilnosti, pouzdanosti, bezbednosti i globalne interoperabilnosti interneta;
2. poštovanje kreativnosti, inovacije i toka informacija koje je omogućio internet time što će se aktivnosti ICANN-a ograničiti samo na pitanja u

[176] Jovan Kurbalija.(2011). *Uvod u upravljanje internetom*. Beograd Albatros plus. Str. 79.
[177] Prema https://www.icann.org/resources/pages/guidelines-2012-05-15-en

ICANN-ovoj misiji koja zahtevaju ili mogu imati značajne koristi od globalne koordinacije;

3. u meri u kojoj je to izvodljivo i odgovarajuće, delegiranje koordinativnih funkcija na ili uvažavanje uloge kreatora politike drugih odgovornih tela koja odražavaju interese pogođenih strana;

4. traženje i podržavanje širokog informisanog učešća koje je reprezentativno za funkcionalnu, geografsku i kulturnu raznovrsnost interneta na svim nivoima kreiranja politike i odlučivanja;

5. tamo gde je izvodljivo i odgovarajuće, zavisno od tržišnih mehanizama, promovisanje i održavanje kompetitivnog okruženja;

6. uvođenje i promovisanje konkurencije u registraciji imena domena gde je to praktično i korisno za javni interes;

7. primenjivanje otvorenih i transparentnih mehanizama kreiranja politike koji a) promovišu dobro informisane odluke bazirane na savetima stručnjaka i b) osiguravaju da najpogođeniji entiteti mogu asistirati u procesu kreiranja politike;

8. odlučivanje primenom dokumentovanih politika na neutralan i objektivan način, uz poštovanje integriteta i pravičnosti;

9. postupanje onom brzinom koja odgovara potrebama interneta pri čemu se kao deo procesa odlučivanja pribavlja informisani stav najpogođenijih entiteta;

10. podnošenje računa internet zajednici kroz mehanizme koji poboljšavaju efektivnost ICANN-a;

11. ostajući ukorenjen u privatnom sektoru, uvažavanje da vlade i javne vlasti nose odgovornost za javnu politiku i ozbiljno uzimanje u obzir preporuka vlada ili javnih vlasti.

Ako se pogladaju ovi ciljevi koje je ICANN postavio sam sebi vidimo da podržavaju saradnju i dogovor, kao i profesionalizam. Moguće ih je iščitati (uključivo i vrednosti implicirane u njima) u instrumentalnom ali i u intrinsičnom vrednosnom ključu. Delegiranje drugima, uključivanje drugih, uvažavanje stučnog mišljenja pa i poštovanje (shvaćeno kao uvažavanje mišljenja onih kojih se to tiče ali i polaganje računa pred njima) mogu spadati i u sredstva za neki cilj i u cilj po sebi. Isto važi i za podržavanje konkurencije, koje je dodatno ograđeno „ukoliko je to u javnom interesu“. Jedino bi se ciljevi 1 i 2 (očuvanje stabilnosti, pouzdanosti, bezbednosti i

globalne interoperabilnosti i očuvanje kreativnosti, inovacija i toka informacija) mogli smatrati kao čisto intrinsična vrednosna preferencija.

Tela koja upravljaju politikom rešavanja sporova u vezi sa internet standardima i resursima

Već opisana tela koja upravljaju standardima i resursima ujedno kreiraju i sprovode politike rešavanja sporova oko ovih ključnih resursa.

Način rešavanja sporova vezanih za proces nastajanja standarda unutar IETF je prikazan u RFC 2026 „Proces internet standarda – revizija 3“ iz 1996. godine.
„Koliko je moguće (IETF – prim.aut.) proces je osmišljen tako da se mogu napraviti kompromisi i može postići izvorni koncenzus, no ima prilika kada i najrazumniji i najstručniji ljudi nisu u stanju da se slože. Da bi se postigli ciljevi otvorenosti i pravičnosti, takvi sukobi moraju biti rešavani procesom otvorenog pregleda i rasprave.“[178] Tu su izložene procedure po kojima se postupa kada dođe do nesuglasica u radnim grupama. Osoba koja se ne slaže sa preporukom radne grupe treba da razgovara o tome sa predsedavajućim radne grupe; ako se tako ne postigne dogovor, bilo koja strana se može obratiti direktoru oblasti; ako ni na ovom nivou nema dogovora, bilo koja strana se može obratiti IESG u celini. „IESG će tada razmotriti situaciju i pokušati da je razreši na način po svom izboru“,[179] ali ako se ni na ovom nivou ne postigne dogovor, bilo koja strana se može žaliti IAB-u, koji će takođe pokušati da razreši situaciju na način po svom izboru. „Odluka IAB-a je konačna u pogledu pitanja da li su poštovane procedure internet standarda i u pogledu svih pitanja tehničkog karaktera.“[180] Sem toga, dalji lekovi su dostupni samo u slučajevima u kojima se tvrdi da su same procedure (na primer, procedure opisane u ovom dokumentu) neadekvatne ili nedovoljne za zaštitu prava svih strana u pravičnom i otvorenom procesu stvaranja internet standarda. Pritužbe na toj osnovi se mogu podneti Odboru poverenika ISOC-a. „Poverenici će razmotriti situaciju na način po

[178] RFC 2026 “The Internet Standard Proces – Revision 3” Ovaj RFC je izmenjen RFC 6410 iz 2011. godine ali te izmene se ne odnose na rešavanje sporova. Dostupno na https://www.ietf.org/rfc/rfc2026.txt Citirano mesto je na str. 22.
[179] Ibid. str. 22.
[180] Ibid. str. 23.

svom izboru i izvestiti IETF o ishodu svog pregleda. Odluka Poverenika o završetku njihovog razmatranja će biti konačna u pogledu svih aspekata spora.“[181]

Sporovi oko internet domena su najčešće povezani sa pravom zaštite patenata i žigova, tj situacijom da se razni akteri spore oko nekog imena domena (na primer, kada onaj ko je registrovao domen i onaj ko ima pravo da koristi to ime nisu isto lice). Način rešavanja sporova vezanih za podelu i dodelu internet resursa predviđen je ICANN-ovom Jedinstvenom politikom rešavanja domenskih sporova (Uniform domain-name dispute-resolution policy – UDRP).[182] Odeljak 4. stav a. ove politike kaže da se od korisnika domena zahteva da se podvrgne obaveznoj administrativnoj proceduri kada neka treća strana (’tužitelj’) izjavi u skladu sa Pravlinikom, da:

(i) ime domena o kome se radi je identično ili zbunujuće slično trgovačkoj marci ili marci usluge na koju tužitelj polaže prava i

(ii) korisnik domena o kome se radi nema prava niti legitimne interese u vezi sa tim imenom domena i

(iii) ime domena o kome se radi je registrovano i koristi se u lošoj veri.

Teret dokazivanja ova tri elementa je na tužitelju. Sam spor se vodi pred telom koje je kod ICANN-a registrovano kao ovlašćeno za rešavanje sporova.[183] Ukoliko se išta iz navoda tužitelja dokaže, telo pred kojim se vodio spor donosi odluku, a ICANN je izvršava. Sankcija se uglavnom svodi na ukidanje prava na sporni domen korisniku koji je tužen. Takođe je moguće da odluka bude da tužitelj nije u pravu, te da ime spornog domena ostane postojećem korisniku.

Države kao upravljači interneta (na svojoj teritoriji)

Mogućnost država da budu upravljači interneta na svojoj teritoriji potiče iz činjenice da su neki od aktera interneta u domenu njihovih nacionalnih jurisdikcija. U domenu jurisdikcije su ISP-ovi, kompanije koje prodaju kompjutersku i komunikacionu

[181] Ibid. str. 23-24.
[182] https://www.icann.org/resources/pages/policy-2012-02-25-en
[183] Jedno od tela koje je ICANN ovlastio za rešavanje sporova oko imena domena je i Svetska organizacija za intelektualno vlastništvo (WIPO). Tu su još i Asian Domain Name Dispute Resolution Centre, National Arbitration Forum, Czech Arbitration Court – Arbitration Center for Internet Disputes i Arab Center for Domain Name Dispute Resolution. Prema https://www.icann.org/resources/pages/providers-6d-2012-02-25-en

tehnologiju, kompanije koje se bave internet sadržajima, banke koje učestvuju u onlajn plaćanjima, firme koje posluju preko interneta, kao i o građani koji su individualni korisnici interneta – svi nabrojani su životno povezani sa svojom državom tj. državom u kojoj su fizički i pravno prisutni. Iako je ova veza postojala od samog nastanka interneta, i država i kompanije i pojedinci (i čitava internet zajednica) su to prisustvo države kao aktera u upravljanju istakli i aktuelizovali tek u poodmakloj fazi razvoja interneta.

Aktivnosti fizičkih i pravnih lica povezane s internetom legitiman su predmet regulacije od strane države, na isti način i iz istih razloga kao što su to njihovi pandani u oflajn životu. Zemaljski zakoni važe i u digitalnom svetu ili sajber prostoru. Tu se ne misli samo na poreske propise, obligaciono pravo i sl. nego i na krivični zakon. Na primer širenje mržnje, pretnja, prevara, ugovor, intelektualno vlasništvo – podležu istim pravilima bilo da su nastali putem interneta bilo da su nastali bez doticaja sa internetom. Iako je u ranim fazama interneta to bilo negirano, danas se uopšteno smatra da je dobro da legitimni pravni poredak važi i u onlajn svetu. To je naročito dobro jer time država ostaje zadužena da se bori i protiv sajber kriminala, koji je remetilački faktor u razvoju interneta. Može se reći da je pravna regulacija i sprovođenje zakona najveći pozitivan uticaj države na internet tj. države kao upravljača interneta.

Sledeći pozitivni uticaji države na internet bi bili: promocija ulaganja u poboljšavanje fizičke infrastrukture interneta na svojoj teritoriji, uvođenje e-servisa za građane (državne usluge dostupne putem interneta), aktivan odnos prema obučavanju stanovništva za korišćenje interneta, podsticaji dostupnosti informaciono-komunikacione tehnologije kroz niže stope poreza za IT robe, sprečavanje stvaranja monopola u onlajn svetu (kod kompanija za internet sadržaje), nalog kompanijama da prilagode svoje delovanje u skladu sa izbegavanjem nepotrebnog prikupljanja ličnih podataka građana itd.

Međutim, država kao upravljač interneta može otići u drugu krajnost, i vršiti negativan uticaj na slobodu i privatnost građana.

Prvo, radi se o pokušaju vlasti neke države da uredi arhitekturu interneta i/ili sadržaj komunikacije na internetu u skladu sa svojim željama - ako ne u celom svetu onda barem na svojoj teritoriji. Primer takvog nastojanja je Kina, domovina ne samo Velikog zida nego i Velikog fajervola (firewall). Upravljanje internetom u Kini je takvo da Vlada NR Kine drži monopol nad svim internet vezama koje ulaze ili izlaze

iz zemlje odnosno postavlja Ministarstvo informatičke industijre kao čuvara/ključara interneta.[184] Osim toga, Vlada NR Kine zabranjuje određene sadržaje u internet komunikaciji, tako što nalaže operaterima da blokiraju IP adrese na kojima se nalaze materijali koji su subverzivni za državnu vlast i socijalistički sistem, štetni za nacionalno jedinstvo, vezani za pornografiju, kockanje ili nasilje, podržavajući za sujeverje, uvredljivi i dr. Čak i kada bi neki sofisticirani korisnici u Kini bili u stanju da zaobiđu ove barijere, koristeći proxy servere i sl. ako budu uhvaćeni u prestupu slede im sankcije koje previđa kineski kazneni sistem te u krajnjem, domet nacionalne regulacije na internetu je time potpun.

Iz političkih, religioznih ili drugih razloga, u blažem vidu nego kad je reč o Kini, vlade nekolikih država povremeno krenu da ograničavaju pristup informacijama na internetu, i to čine putem direktnih naredbi provajderima internet usluga, koji onda shodno tome postavljaju tehničku barijeru i prisiljavaju svoje korisnike da poštuju naredbe vlasti. Posebno u tom filtriranju pristupa prednjače nedemokratske vlade u Aziji, na Srednjem istoku i u Severnoj Africi. Skorašnji primer iz 2014. god. je zabrana pristupa sajtovima Ju tjub i Tviter u Turskoj.[185]

Drugo, pojedine države se upuštaju u neovlašćeno masivno prikupljanje elektronskih podataka građana. U aferi Snouden 2013. godine ovo je spektakularno otkriveno kod najrazvijenijih država sveta, sa reputacijom stabilnih demokratija i najvišim standardima ljudskih prava. O ovome će biti više reči u poglavljima 5 i 8. Ovde vredi napomenuti da ovo postupanje država nije upravljanje internetom, već je to zloupotreba moći i kontrole, pa je prvenstveno *de facto* stanje koje je lišeno pravne legitimnosti. Moglo bi se reći da sigurnosne službe države (kako bi došle u posed i pristupiti podacima po potrebi) hakiraju najvažnije sisteme komunikacije na svojoj teritoriji. To najčešće radi deo jedne grane vlasti (izvršne) tajno tj. bez znanja građana, korisnika i/ili ostalih grana vlasti (parlamenta, sudstva).

Za razliku od transnacionalnih tela koja upravljaju internetom, država kao upravljač interneta (na svojoj teritoriji) može ponekad da doživljava internet kao pretnju po sebe, ili po svoju vladajuću elitu, pre svega zbog snage internet aktivizma, o čemu će biti reći u poglavlju 8.

---

[184] *Internet Governance* str. 69. Podaci o stanju interneta u Kini i drugim državama koje blokiraju, filtriraju ili osporavaju internet sadržaj dostupni su na internet stranici organizacije Open Net Initiative, s tim da je organizacija prestala da prati stanje 2012. godine https://opennet.net/

[185] Alev Scott. (28. mart 2014).„Turkey's You Tube and Twittr bans show a government in serious trouble" *The Guardian*, Dostupno na http://www.theguardian.com/commentisfree/2014/mar/28/turkey-youtube-twitter-ban-government-trouble

Konvencija Saveta Evrope o sajber kriminalu

Budući da kriminal na internetu vrlo često ima prekogranične elemente, neke države su vrlo rano utvrdile potrebu da međusobno sarađuju u cilju njegovog sprečavanja. Ipak, takve države su u manjini globalno gledano.

Prvi međunarodni sporazum koji se bavi kriminalom vezanim sa internetom je Konvencija Saveta Evrope o sajber kriminalu, potpisana u Budimpešti 2001. god., koja je stupila na snagu 1. jula 2004. godine. Uz nju je nastao i dodatni protokol, koji je stupio na snagu 1. marta 2006. god. Ova Konvencija se bavi krivičnim delima počinjenim preko interneta ili drugih kompjuterskih mreža, kao i ovlašćenjima i procedurama potrebnim u borbi sa njima, kao što su pretraživanje kompjuterskih mreža, presretanje podataka i sl.

Glavni cilj Konvencije[186] je zajednička politika država potpisnica u pogledu kriminalizacije određenih vrsta krivičnih dela, da bi ova kriminalizacija efikasno zaštitila društvo od tih krivičnih dela. Zajednička politika država potpisnica se sprovodi putem usvajanja odgvarajućih zakonskih okvira i pospešivanja međunarodne saradnje u ovom domenu.

Konvencija definiše sledeća krivična dela: neovlašćeni pristup, neovlašćeno presretanje, remećenje podataka, remećenje sistema, zloupotreba uređaja, krivotvorenje povezano sa kompjuterima, prevara povezana sa kompjuterima, krivična dela vezana za dečiju pornografiju i krvična dela vezana za autorska i srodna prava.

Konvencija reguliše i sledeće oblasti procesnog prava: hitno čuvanje uskladištenih podataka, hitno čuvanje i delimično odavanje podataka o saobraćaju, nalog za uspostavljanje, pretraživanje i konfiskovanje kompjuterskih podataka, sakupljanje podataka o saobraćaju u realnom vremenu i presretanje sadržaja podataka. Uz to, konvencija ima odredbu o posebnoj vrsti prekograničnog pristupa uskladištenim kompjuterskim podacima koji ne zahteva uzajamnu pomoć (uz pristanak i tamo gde je javno dostupno). Konvencija predviđa uspostavljanje jasne saradnje među državama

[186] Dokument je dostupan sa internet stranici Saveta Evrope http://www.coe.int/en/web/cybercrime/the-budapest-convention Na srpskom jeziku nalazi se na internet stranici Narodne skupštine u delu koji se odnosi na donete zakone pod brojem 486-09 od 18. marta 2009. godine.

potpisnicama, uključivo i njihove nadležne kontakt osobe koje bi bile dostupne na bazi 24/7, u cilju hitne pomoći među državama potpisnicama.

Dodatni protokol kriminalizuje širenje rasističkog i ksenofobičnog materijala preko kompjuterskih sistema kao i širenje pretnji i uvreda motivisanih rasizmom i ksenofobijom.

Do marta 2014. Konvencija je ratifikovana u 42 zemlje, pri čemu među njima su i neke zemlje ne-članica Saveta Evrope, kao što su Japan, Australija itd. [187] Posebno je važno da je ovaj sporazum (bez dodatnog protokola) 2006. god. ratifikovao i SAD.

Republika Srbija je ratifikovala ovaj sporazum 2009. god. (takođe i dodatni protokol), s tim da je zvanični naziv konvencije na našem jeziku Konvencija o visokotehnološkom kriminalu. Da bi se ispunile obaveze iz ove Konvencije, u Srbiji su doneti ili izmenjeni brojni zakoni: Zakon o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala, Krivični zakonik, Zakonik o krivičnom postupku, Zakon o policiji, Zakon o autorskim i srodnim pravima, Zakon o posebnim ovlašćenjima radi efikasne zaštite prava intelektualne svojine, Zakon o telekomunikacijama, Pravilnik o uslovima za pružanje internet usluga i sadržaju odobrenja, zakoni o javnom tužilaštvu, uređenju sudova i dr. Uopšteno govoreći:

> „Borba protiv visokotehnološkog kriminala u Srbiji podrazumeva procesuiranje izvršilaca dela protiv bezbednosti računarskih podatka ... i dela protiv intelektualne svojine, imovine i pravnog saobraćaja i druga krivična dela kod kojih se kao objekat ili kao sredstvo izvršenja javljaju računari, računarske mreže, računarski podaci kao i njihovi proizvodi u materijalnom ili elektronskom obliku.“[188]

Obuhvaćena su i dela protiv sloboda i prava čoveka i građanina, polne slobode, javnog reda i mira i ustavnog uređenja i bezbednosti Republike Srbije, za koje se zbog načina izvršenja ili upotrebljenih sredstava sa sigurnošću može zaključiti da su dela visokotehnološkog kriminala. Takođe je uvedeno u Srbiji i krivično delo pravljenje, nabavljanje i davanje drugom sredstava za izvršenje krivičnih dela protiv bezbednosti računarskih podataka. To što postoji zakon je za pohvalu, ali treba reći da je broj ovih dela u porastu kao i da broj sudski rešenih slučajeva nije veliki.

---

[187] Među evropskim zemljama koje su potpisale konvenciju ali je još uvek nisu ratifikovale (dakle, nisu u obavezi da je primenjuju u unutrašnjem pravu) su: Grčka, Irska, Luksemburg, Poljska, Švedska, Turska. Isti slučaj je i sa Kanadom i Južnoafričkom Republikom. Rusija nije ni potpisala konvenciju.

[188] prof. Dr Milan Milošević i prof.dr. Željko Nikač. (2010). „Izmene u zakonodavstvu Republike Srbije i borba protiv visokotehnološkog kriminala“. (str. 236-244). u *Zloupotreba informacionih tehnologija i zaštita*, ur. Slobodan R. Petrović, Beograd: IT Veštak. Dostupno na http://www.itvestak.org.rs/ziteh_10/zbornik_radova/Milosevic%20Milan,%20Nikac%20Zeljko%20VTK.pdf Str. 239.

Postavlja se pitanje da li ovaj međunarodni sporazum može da postane globalni standard. U dosadašnjoj primeni konvencija se pokazala efikasnom, a zemlje koje je primenjuju su stekle vredno iskustvo u implementaciji. Ipak, da bi postala globalni standard, bio bi potreban koncenzus u okviru UN po pitanju proceduralnih aspekata i mera saradnje predviđenim u Konvenciji, a čini se da toga nema. Iz ugla obuhvata konvencije, smatra se da pokriva tek oko trećine internet korisnika na svetu. Podržale su je, ali ne i potpisale, Organizacija za azijsko-pacifičku ekonomsku saradnju, Organizacija američkih država, Intepol. S druge strane Kina, Rusija i Brazil pokazuju rezerve prema Konvenciji i nisu potpisnice. Postoji izvesna skepsa da bi se njihovo pristupanje moglo uopšte očekivati, posebno imajući u vidu da se (Kina, Rusija) sumnjiče da sponzorišu različite forme sajber napada zarad političkih ciljeva, te „kako bi se one mogle saglasiti sa visokim standardima međunarodne saradnje za istraživanje i procesuiranje sajber kriminala?“[189]

Zemlje koje nisu sklone pristupanju ovoj Konvenciji predlažu drugo polje saradnje, tj. usvajanje kodeksa ponašanja u sajber prostoru, koji bi sadržavao i odredbe namenjene sprečavanju upotrebe interneta od strane terorista. Kodeks ponašanja ne bi bio u sukobu sa konvencijom, ali još uvek nije otišao dalje od predloga.

Najverovatnije je da se univerzalna saradnja država na polju zajedničke borbe protiv kriminala na internetu ne može očekivati u doglednoj budućnosti, dok u ograničenom vidu u jednoj manjoj grupi zemalja (okupljenih oko Saveta Evrope) postoje zameci takve saradnje.

Sajber konfrontacije između država

Paralelno sa opcijom saradnje na zajedničkoj borbi protiv sajber kriminala, između jednog broja država prisutna je u određenoj meri sajber konfrontacija. Postojeći okvir međunorodnog prava ne štiti u dovoljnoj meri građane ni u jednoj državi od potencijalnog sajber ratovanja. Ove konfrontacije možemo odrediti u dva oblika:

1. međusobno špijuniranje država i
2. napad na ključne infrastrukturne objekte u drugoj državi.

[189] Brian Harley. (23. mart 2010). „A Globoal Convention on Cybercrime?“ *Science and Technology Law Review*. Dostupno na http://www.stlr.org/2010/03/a-global-convention-on-cybercrime/

Međusobno špijuniranje država nije praksa koja se pojavila sa internetom, ali je zahvaljujući njemu olakšana. Ozbiljnost problema potiče od lake dostupnosti softvera koji omogućava (bilo kome u čijem je posedu, što ne mora nužno biti država) da presreće privatne elektronske komunikacije širom sveta. Po objavama portala Vikiliks iz 2011. postoji najmanje 95 kompanija koje proizvode i distribuiraju takav softver, od čega su 32 u Americi, 17 u Velikoj Britaniji, a ostale u oko 12 država širom sveta. „Bilo koja tehnologija sa tako velikim potencijalom za kršenje osnovnih prava treba da bude fokus najvećeg stepena pravne zaštite, naročto ako je u rukama privatnih kompanija koje posluju po čisto poslovnim ciljevima“.[190] Na primer, u cilju sprečavanja širenja ovog softvera mogli bi se primeniti isti međunarodno-pravni mehanizmi koji se odnose na promet robe dvostruke namene ili oružja – ukoliko bi postojala želja država da se odreknu špijuniranja.

Nema jasnih podataka u kojoj meri države vrše napade na ključne infrastrukturne objekte van svojih granica. Najnavođeniji primer upotrebe sajber oružja koji se za sada može dati je kompjuterski virus Stuxnet koji je SAD iskoristila da izvrši sabotažu na nuklearnom reaktoru u Iranu. Navodno je ovaj virus razvijan od 2005. i upotrebljavan u malim razmerama isključivo u Iranu kako bi ostao tajan, dok 2009. godine javnost nije doznala za njega zbog agresivnije primene od strane SAD saveznika Izraela. Međutim, štagod da je Stuxnet radio, to nije zaustavilo iranski nuklearni program već se protiv Irana morala još niz godina primenjivati široka paleta međunarodnih sankcija, pritisaka, pretnji i sl. Konačno je početkom 2016. god. postignut dogovor između Irana i zemalja koje su se protivile njegovom nuklearnom programu.

Iako o njoj ima premalo informacija, sajber konfrontacija država koja se vrši preko infrastrukture globalnog javno dostupnog interneta i te kako utiče na krajnje moralno vrednovanje interneta i zato se ovde mora dodatno razmotriti.

«Da li smo u digitalnom hladnom ratu?»[191] je pitanje kojim se bavio američki profesor Milton Miler tokom jednog skupa u Ženevi 2013.godine. Miler zastupa tezu da nismo u hladnom ratu jer «pravi hladni rat na internetu bi značio da dve strane imaju svaka svoje komunikacione protokole. (Sada) još uvek niko ne predlaže

[190] Emilio Godoy „Cybercrime Treaty Could Be Used to Go After Cyberspionage“ Dostupno na http://www.ipsnews.net/2013/10/cybercrime-treaty-could-be-used-to-go-after-cyberespionage/

[191] Milton Mueller. (17. maj 2013). “Are We in Digital Cold War?”GigaNet workshop *The Global Governance of the Internet: Intergovernmentalism, Multistakeholderism and Networks*. Dostupno na http://www.internetgovernance.org/wordpress/wp-content/uploads/DigitalColdWar31.pdf (U daljem tekstu “Hladni rat”)

konkurentski nekompatibilan komunikacioni protokol koji bi omogućio jednom delu sveta da se okrene od TCP/IP i kongregira oko konkurentskog standarda koji bi isključio liberalne ekonomije».[192] Čak i Severna Koreja i Iran koriste TCP/IP. Miler ukazuje da ne postoji alternativni rut DNS, niti različit sistem registra internet adresa. Zapravo, nije samo internet per se taj koji povezuje naš svet informacija i komunikacija; „to čine i 802.11 standardi za WiFi, operativni sistemi Vindous, Epl i Android, proizvođači uređaja u Koreji, Kini, Evropi i SAD. Do izvesne mere, to čine i Tviter, Gugl i Fejsbuk, za koje se svuda primeti da nedostaju kada budu aktivno blokirani.»[193] Za vreme hladnog rada na primer,

> «postojao je američki Intelsat sistem za Zapad. Sovjeti mu nisu pristupili pa se žalili da u njemu dominira SAD. Nisu pokušavali da navedu da ITU preuzme kontrolu nad njim. Radije su kreirali Intersputnik, alternativni satelitski sistem koji je pokrio istočni blok. Takođe, trgovina, imigracija i putovanja između Istoka i Zapada bili su visoko restriktivni.»[194]

Miler daje još jedan argument u prilog tezi o tome da se hladni rat ne dešava, naime to da sajber oružje nije revolucionarni faktor sposoban da promeni vojno takmičenje među državama globalnih razmera, u čemu se slaže sa Ridom koji smatra da su vojni aspekti sajber aktivnosti drastično preuveličani.[195] Miler argumentuje na sledeći način: «stvari koje nazivamo sajber oružjem nisu stvorile novu vrstu sukoba koji je promenio stratešku ravnotežu među državama uključenim u vojni sukob.»[196] Sajber oružje se ne može porediti sa pokretnom artiljerijom koju je uvela Francuska krajem petnaestog veka, ili sa nuklearnim oružjem u dvadesetom veku koje je napravljeno i primenjeno za samo šest godina (1939-1945) nakon čega je diktiralo odnose među velikim silama narednih pola veka. Za razliku od tog,

> «govorimo i pišemo o sajber ratovanju zadnjih 15 godina; za to vreme nijedna država nije srušena, nijedna moć upravljanja nije stečena ili izgubljena, nijedno iscrtavanje teritorijalnih granica nije se desilo na temelju isključivo ili makar primarno sajber napada i sajber oružja.»[197]

Milton usvaja da internet beleži slučajeve izazivanja haosa u sajber prostoru, socijalnog protesta, privremenih poremećaja, špijunaže, krađe podataka, sabotaže ali

[192] Ibid. Str.9.
[193] Ibid. Str. 10.
[194] Ibid. Str. 10.
[195] Thomas Rid. (Feb. 2012). „Cyber War Will Not Take Place“ *Journal of Strategic Studies*, Vol. 35, No 1.5-32 (Prevod naslova na srpski „Sajber rat se neće dogoditi“.)
[196] "Hladni rat" Str. 11.
[197] "Hladni rat" Str. 11.

za sada nema dokaza da bilo šta od toga može da vodi smrti i razaranju širokih razmera, niti promeni strateške ravnoteže između država, niti da može stvoriti neku vrstu borbe između alternativnih oblika države[198]. Miltonova ocena je da je glavni efekat koji je sajber oružje stvorilo jedna nepoželjna politička dinamika u međunarodnim odnosima, ali isto tako i na unutrašnjem planu u SAD i drugde (gde se izaziva homogenizaciju društva i koncentraciju moći u vojnim krugovima a oslabljuje zagovornike internet slobod i liberalne demokratske države).

Ipak, ako prihvatimo kao tačan stav da na internetu sada ne prolazimo kroz hladni rat, koji bi bio tačan opis onog što se događa? Evidentno je da na internetu danas imamo u mirnodopsko vreme primenu sajber oružja i sajber napade iz jedne zemlje na drugu tj. njenu kritičnu infrastrukturu. Jedino što ne znamo je kako nazvati tu situaciju.

Debate o upravljanju internetom u međunarodnoj areni

Imajući u vidu prethodno izneto o državama kao upravljačima interneta (na svojoj teritoriji) i saradnji kao i konfrontaciji koje se među njima dešavaju, sasvim se može prihvatiti opis da se u upravljanju internetom reflektuju određene **tenzije**, koje se mogu okarakterisati kao: „vlast naspram legitimiteta, digitalni liberalizam naspram digitalnog realizma, komercijalizam naspram ideala civilnog društva, interesi razvijenih zemalja naspram interesa zemalja u razvoju“.[199] Od ishoda razrešenja tih tenzija zavisi budućnost interneta.

Osim opisa onog što se događa, opisa kontura date situacije kao tenzije, čini se da je prihvatljiv i opis da se vode međunarodne debate o upravljanju internetom. U tom smislu, reći ćemo nešto više o ovim debatama (koji tabore su sukobljeni,šta su teme).

Ko su tabori koji stoje na dve strane ove međunarodne debate? To su zagovornici slobode i zagovornici državne regulacije interneta, ili tzv. liberalne slobodoljubive država i autoritarne nedemokratske države, ili, kako Miler još predlaže, mlađe nacionalne države (one koje su se pojavile u periodu posle drugog svetskog rata) i

[198] Pojam «borba oblika države» potiče iz knjige Filipa Bobita *Ahilov štit: rat, mir i tok istorije*. Philip Bobbitt *The Shield of Achilles: War Peace and the Course of History* New York Anchor Books 2002. Bobitovo viđenje je da su svi ratovi u dvadesetom veku bili samo epizode jednog velikog rata koji se vodio da bi se odredilo koji od tri oblika nacionalne države će zameniti devetnaestovekovne imperijalne države Evrope: tržišno orijentisana parlamentarna demokratija, komunizam i fašizam. O ovom viđenju Peter Conrad. (16. jun 2002).„Achilles's last stand“. *The Guardian* Dostupno na http://www.theguardian.com/books/2002/jun/16/history.homer

[199] *Internet Governance* str. 4.

starije davno-ustanovljene kosmopolitske države. Po Mileru, mlađe države najjače su posvećene suverenističkom ili neo-vestfalskom pristupu upravljanju internetom, dok starije davno-ustanovljene kosmopolitske države lakše prihvataju nove forme transnacionalnog upravljanja (pod tim se misli na ICANN – prim.aut.). Pod mlađim nacionalnim državama Miler pre svega misli na Kinu, koja predvodi zemlje G77 u zalaganju za međuvladin suverenistički pristup politici interneta. Kina promoviše alternativnu ideologiju o ulozi informacija u društvu sa naglaskom na agresivno upravljanje javnim izražavanjem, na sprečavanju iskakanja i nepoželjnosti neslaganja, a poželjan je cilj «harmoničnog» interneta. Ali možemo primetiti da Milerova kategorizacija nije precizna, pošto prema njoj u tzv. mlađe države spada recimo Češka, koja ne insistira na suverenističkom pristupu, a ne spada Brazil, koji insistira na ovom pristupu internetu. Dalje, nije ničim potkrepljeno da postoji veza između starosti države i njenog viđenja upravljanja internetom. Ipak, donekle arogantno Miler izjavljuje:

> «... trebalo je nekoliko decenija da nauče da su socijalističke i komunističke ideologije ... katastrofalno kontraproduktivne kao vodiči u ekonomskoj politici, pa će im možda trebati dekada ili dve da nauče da je vladanje teritorijalne nacionalne države nepovratno kontraproduktivno u domenu komunikaciono-informacione politike u 21. veku.»[200]

Od tema međunarodne debate, treba pomenuti temu odgovarajuće institucionalne forme upravljanja internetom.[201] Mlađe države i autoritarne države daju prednost pregovaranju međudržavnih sporazuma za globalno upravljanje internetom. Nasuprot tome, kompanije i akteri civilnog sektora (kao i starije države) podržavaju organski razvijene institucije interneta (kao što je IETF ili ICANN), za koje smatraju da obezbeđuju transnacionalno upravljanje i primenjuju otvorenije participativne mehanizme odozdo na gore. Participacija u ovim institucijama je otvorena svima. Ipak, prema dosadašnjim činjenicama, malo je verovatno da će se u njihov rad uključiti mlađe i autoritarnije države. Čak i da se to desi, neizvesno je s kojim ciljem bi ovi akteri ušli u „transnacionalno“ upravljanje internetom.

Povodom izbora međudržavni sporazum ili transnacionalne institucije (IETF, ICANN itd.) mogući jei sledeći komentar: bez obzira što se radi o pozivu transnacionalnih institucija svima na učešće koji je upućen nediskriminativno, bilo kome ko ima neku

[200] “Hladi rat” Str.6.
[201] Ibid. Str. 8.

političku agendu, to u praksi nije sprovodivo. Jedna grupa gotovo sigurno nikada neće da se umeša u proces tehničkog upravljanja.

> «Iako se to čini kao demokratičnije, u stvarnosti to je otvaranje vrata organizovanim posebnim interesima. G. i g-đa Obični Korisnici Interneta neće provoditi nedelje i nedelje svog vremena čitajući imejlove o agregaciji ruta, blokovima adresa nevezanim za provajdere i strategijama migracije ka IPv6. Jedini ljudi koji će imati posvećenost i energiju da uđu u te procese biće organizovane interesne grupe ... usmerene na borbu sa drugim takvim grupama (provajderi sadržaja, zaštitnici autorskih prava i sl.)“.[202]

Ovaj komentar zapravo osnažuje poziciju nacionalne države jer nacionalna država ostaje (iz ugla građana) pravo mesto za rešavanje pitanja javnih politika. Građanima je bliža (njihova) nacionalna država, nego što bi bila tela za tehničku koordinaciju interneta. Iz toga onda sledi da ova tela treba da zadrže samo tehničku misiju i da se odupru sopstvenom zatrpavanju političkim funkcijama. Politička pitanja upravljanja internetom bi trebalo, koliko god je moguće, rešavati međudržavnim sporazumima.

Druga tema diskusije je tzv. komunikaciona politika.[203] Komunikacija na netu može biti slobodna ili ograničena. Civilno društvo razvijenih država i zemalja sa srednjim prihodom naklonjeno je slobodi interneta, i protivi se cenzuri, nadzoru, monopolu i rigoroznoj zaštiti intelektulne svojine, a podržava inovacije, slobodu izražavanja i privatnost. Na drugoj strani su države sa autoritarnim tendencijama koje žele da povrate suverenu moć nad digitalnim komunikacijama, da bi opresirale vlastito civilno društvo i moguću opoziciju, a i zaštitile lokalnu političku ravnotežu od kosmopolitskog potresa. One se zanimaju za zaštitu svog političkog *status quo* i od domaće opozicije i od stranog političkog i kulturnog uticaja tj. hegemonije SAD-a.

Interesantno je da su ove dve teme diskusije povezane utoliko što zagovornici multiakterskog pristupa su u savezu sa zagovornicima slobode interenta, a zagovornici međuvladinog upravljanja naginju ka više regulacije i kontrole interneta.

Uz to, obe diskusije su se još dodatno zakomplikovale nakon što je 2013. godine u afer Snouden obelodanjeno da je Vlada SAD-a, tradicionalni glasnogovornik slobode interneta, sprovodila nadzor nad internet komunikacijom putem svoje agencije za nacionalnu sigurnost NSA. Nakon ovog otkrića, na strani bloka predvođenog SAD-om izgubljen je dobar deo kredibiliteta. Američka podrška organskim institucijama

[202] Milton Mueller, Branden Kuerbis and Michel van Eeten. (26. nov. 2008). “Regional Address Registries, Governance and Internet Freedom” Internet governance project. Syracuse University. Str. 24.

[203] “Hladni rat” str. 9.

upravljanja internetom počela je da deluje kao oportunistička, nedosledna i parcijalna, inherentno licemerna. Kritičari su u poziciji da kažu: SAD podržava ICANN zato što je ICANN naklonjen SAD-u i omogućava privilegovane oblike uticija. Ipak, istina je negde na sredini.

U ovom radu ćemo izostaviti opis i analizu ranijih dešavanja u međunarodnoj areni na temu upravljanja internetom, kao što su dva zasedanja Svetskog samita o informacionom društvu (2003. i 2005. godine) održanih pod okriljem Ujedinjenih nacija ili zasedanja Foruma o upravljanju internetom, jer nemaju eksplanatorni značaj za pitanja od interesa u ovom radu.

Mrežno upravljanje internetom

Osim upravljanja transnacionalnih tela (tela *sui generis*) i država, u realnom životu interneta se pronalazi još jedan model upravljanja internetom, uz već pomenute modele (međudržavni sporazum i transnacionalna institucija). On bi se mogao nazvati mrežno upravljanje i odlikuju ga privatni glavni akteri. Taj model je prikazan u radu "Bezbednost interneta i umreženo upravljanje u međunarodnim odnosima" Milera, Šmita i Kirbisa iz 2012. godine.[204] Ovi autori iznose mišljenje da je „mrežno upravljanje urođeni oblik globalnog upravljanja internetom i predstavlja pravilo a ne izuzetak u ključnim aspektima njegovog funkcionisanja".[205] Autori koriste definiciju mrežnog upravljanja preuzetu od nemačkog politikologa Frica Šarfa, koji je precizira da je tu na delu «sistem dobrovoljnog pregovaranja u kome su partneri slobodni da biraju između pregovaranja i jednostranog delovanja» i takođe «polupermanentne strukture u kojima se dešavaju pojedinačne interakcije, a podrazumevaju pamćenje prethodnih susreta i očekivanja budućih odnosa.»[206] Ovakvo mrežno upravljanje kao poseban oblik upravljanja, karakterisano labavim vezama, tzv. slabim upravljanjem, nehijerarhijskim upravljanjem, nije dovoljno poznato (ni teorijski, ni praktično) u

[204] Milton Mueller, Andreas Schmidt and Brenden Kuerbis. (March 2013). "Internet Security and Networked Governance in International Relations" *International Studies Review* Vol. 15, Issue 1, 86-104. Dostupno na http://onlinelibrary.wiley.com/doi/10.1111/misr.12024/abstract (U daljem tekstu "Umreženo upravljanje".)
[205] Ibid. Str. 87.
[206] Ibid. str. 89.

krugovima koji se bave temom regulisanja interneta, pa zato i ne zauzima prominentno mesto u aktuelnim debatama.

Ovaj oblik organizovanja (umreženo delovanje) najpre je otkriven u ekonomskoj nauci i njenom delu koji se bavi izučavanjem firmi, tako što je devedesetih godina 20. veka uočena nova vrsta ponašanja firmi, najpre nazvana hibridom između tržišta i hijerarhijske strukture. Tu bi spadale franšize, autsorsovani (preneti van firme) procesi, istraživački savezi itd. Ono što je zajedničko tim oblicima je odnos među firmama, koji je stabilniji od obične tržišne transakcije, i lateralni umesto hijerarhizovanih kanala komunikacije. No, primena tog koncepta na druge društvene nauke pa i međunarodne odnose nije samo mehanička i autori upozoravaju protiv grešaka koje se dešavaju.

> „Veliki izvor zabune dolazi od naše povećane sposobnosti da predstavljamo društvene odnose (ili bilo šta drugo) kao mreže koristeći grafove i srodne matematičke tehnike. Sve popularnija upotreba mrežnog predstavljanja u političkim naukama ... daje sposobnost da se nađu 'mreže' bilo gde i bilo kada se to poželi. Ako se pogleda gomila skorašnjih radova koji pominju 'mreže' u međunarodnim odnosima i političkim naukama, vidi se ... arbitrarno određivanje neke vrste entiteta kao čvora i arbitrarno označavanje neke vrste odnosa među njima kao veze, a to je propraćeno grafovima i nekom matematičkom analizom tako napravljenog mrežnog modela.“[207]

Koje argumente autori daju u prilog tezi da je mrežno upravljanje upravo ono što se dešava u upravljanju internetom?

Prvi argument da je mrežno upravljanje prisutno u funkcionisanju interneta je rutiranje koje sprovode autonomni sistemi. Kao što smo već objasnili, oni koordiniraju svoje delovanje, ali je svaki slobodan da definiše svoje vlastite politike i donosi svoje vlastite odluke o tome kakve su objave rutiranja drugih operatera i koje pakete će prihvatiti ili odbaciti.

> „IETF nema nikakvu hijerarhijsku vlast nad operaterima; dok god ostaju pri BGP i drugim relevantnim standardima, operateri to rade svojom voljom, da bi održali kompatibilnost sa svojim komunikacionim partnerima. Zloupotrebe i nekorektna ponašanja se sankcionišu prvenstveno odlukom pojedinačnog operatera da blokira rute i mreže povezane sa lošim ponašanjem. Politike i prakse rutiranja kao celina nisu podvrgnute hijerarhijskoj regulaciji jednog tela.“[208]

[207] Ibid. Str..90.
[208] Ibid. str..92.

Ono što treba podvući po autorima je da ne postoji nijedan nacionalni ili transnacionalni sistem regulacije koji direktno interveniše u rutiranje kao takvo, ali s time se ne možemo složiti 100%-tno imajući u vidu kineske autonomne sisteme.

Svoj argument baziran na rutiranju autori ojačavaju i analizom dva incidentna slučaja u praksi rutiranja na internetu i reagovanjima svetske mreže na njih.

Prvi slučaj je iz februara 2008. god. kada je operater (AS) iz Pakistana napravio pometnju. Naime, pakistanska vlada je naredila svom operateru (telekomu) da blokira internet stranicu Ju tjub u Pakistanu, što je on i učinio – u svojoj tabeli „ugasio" je rutu ka Ju tjubu. No, usled neprecizne konfiguracije pakistanskog operatera, tu informaciju o ruti je preuzeo i njegov provajder međunarodne konekcije (njegov tier 1)[209] pa se informacija proširila celim svetskim sistemom rutiranja i posledično više nijedan korisnik bilo iz koje zemlje nije mogao da pristupi stranici Ju tjuba. Situacija je otklonjena dosta brzo, za 30 do 120 minuta su svi operateri AS na svetu ispravili tu grešku.

Drugi incident je iz aprila 2010. god. kada je kineski operater (telekom) poremetio više ruta koje su se ticale sajtova i operatera u SAD i Evropi. Tu se globalna pometnja nije desila, pošto većina operatera AS iz ostatka sveta ima nepoverenje prema kineskom tretiranju interneta, pa su bili na oprezu.

Ovde treba uneti jednu napomenu. Pod izgovorom da žele da spreče takve pometnje, od strane vlade SAD bio je zagovaran sistem RPKI (Resource Public Key Infrastructure). Suština tog predloga je da se kreira „sidro poverenja" – telo koje bi validiralo dobre rute i izdavalo sertifikate kredibilnim operaterima AS, drugim rečima uvođenje hijerarhije nad informacijama o rutama. Do sada, sistem RPKI nije zaživeo, a odgovor zbog čega leži u tome da su operateri AS znali da

> „ko god bi izdavao sertifikate u sidru poverenja bi mogao da dobije značajnu moć nad entitetima koji koriste te sertifikate niže od njega u hijerarhiji, pošto bi to telo bilo u stanju da oduzme sertifikat ili postavlja uslove za njega. Oduzimanje sertifikata bi moglo sprečiti validiranje objavljivanja ruta i tako onemogućiti rutiranje tog operatera. Stoga ... nisu uspeli da ... dobiju jaku podršku mrežnih operatera".[210]

[209] U pitanju je telekomunikaciona firma iz Hong Konga PCCW International.
[210] „Umreženo upravljanje" str. 95.

Budući da je ovaj napor naišao na otpor jer bi dramatično uticao na odnose moći među akterima u ovoj industriji, vlada SAD nije nametnula svoju volju. Autori primećuju: „Države se prilagođavaju mrežnom upravljanju, ne gaze preko njega“. [211]

Drugi argument u prilog mrežnom upravljanju kao optimalnom obliku za upravljanje internetom je po meni nešto slabiji od prvog, ali vredi da bude pomenut. U pitanju je slučaj Confiker botneta iz 2008. god. (Confiker je naziv kompjuterskog virusa, botnet je mreža kompjutera zaraženih virusom.) Nepoznati subjekt je tada na veliki broj računara koji su radili pod operativnim sistemom Microsoft Windows ubacio vrlo sofisticirani virus iliti maliciozni softver tj. malver i uz pomoć istog kreirao mrežu robotskih kompjutera. Dotični malver je bio jako moćan u širenju, inovativan i otporan na pokušaje čišćenja i suzbijanja, takoreći bio je tehnički impresivan i superioran, i zarobio je neuobičajeno veliki broj kompjutera, dakle napravio bazu sa mogućnošću za veoma ozbiljan napad. Mreže robotskih kompjutera ili botnetovi su česta roba u kriminalnom podzemlju. Vlasnici najčešće iznajmljuju botnet drugim kriminalcima koji ga koriste da iznude novac od kompnija pretnjama rušenja kompanijskih veb sajtova. Isto tako, botnet može da posluži za napad na vladine mreže ili drugu kritičku infrstrukturu neke države. Ono što je čudno u slučaju Confiker botneta je da on nije upotrebljen pa se ne zna koja mu je bila svrha.

Borba protiv botneta i virusa odvija se po određenoj taktici. Malver se obično hvata na tzv. ćupovima s medom, namerno slabo osiguranim mašinama sa direktnom vezom sa internetom koje treba da privuku virus. Kada virus dođe na njih, istraživači ga analiziraju, sprovedu reversni inžinjering i dodaju zaštitu protiv njega u antivirus programe. To je trebalo uraditi i sa Confiker malverom, samo što je za to bio potreban veliki broj novih internet domena. Pretpostavka je bila da će na jednom od ovih domena vlasnik botneta instalirati sistem komande i kontrole koji naređuje zarobljenim računarima šta da rade. No, celo rešenje je zavisilo od dovoljno velikog broja „ćupova sa medom“ tj. novih domena.

Borba protiv Confikera je zavisila od dobre volje registratora internet domena iz raznih delova sveta, koji bi dnevno registrovali stotine domena i to u različitim generičkim domenima i bez naknade. Preko 100 registratora je podržalo inicijativu. Ali nisu samo oni bili u igri. Spontano je formirana tzv. radna grupa za Confiker, u

[211] Ibid. str. 95.

kojoj su bili tehnički eksperti koji su igrom slučaja profesionalno bili odgovorni za neki deo interneta (pa su ih šefovi pustili da se okrenu radu na ovome) ili su dobrovoljno posvetili svoje vreme tom slučaju nezavisno od svog zanimanja ili uloge. Miler, Šmit i Kirbis naglašavaju:

> «Doprinos tradicionanih organizacija u sektoru sigurnosti kao što su policijska tela, tela tajnih službi, vojna tela i nacionalni tim za odgovor na kompjuterske incidente bio je zanemarljiv. Obuzdavanje pretnje je izvršila labava koalicija dobre volje službenika, preduzetnika i pojedinaca. Niko od bitnih aktera nije ugovorno ili pravno bio obavezan da doprinese opštem trudu oko odgovora na incident.» [212]

To je bila jedna virtualna ad hoc grupa koju su činili pojedinci koji su radili za kompanije vlasnike pojedinih delova interneta. Neki pojedinci su se znali od ranije, neki upoznali tokom ove akcije. Brojni akteri su dakle delili jedan zajednički interes – tehničku dobrobit interneta. Njihovi partikularni privatni interesi konvergirali su i proizveli javno dobro – suzbijanje opasnog virusa na internetu. Po Mileru, Šmitu i Kirbisu: „Ovo je bio primer da samoupraljvanje internet zajednice funkcioniše“.[213]

Nekih ograničenja ovog argumenta svesni su i autori.

Prvo, očigledno ograničenje je da odgovor nije globalan. Tim koji se borio protiv Confikera bio SAD-centričan, informacije o akciji nisu date registratorima internet domena u Kini. Razlog je očigledno strah da bi deljenje informacija o Confiker botnetu sa Kinom poništilo stečenu prednost tehnološkog znanja.

Drugo, ako bi napadači vršili napade većeg obima ili sa većom učestalošću, na primer dva akutna conficker-a istovremeno, pitanje je da li bi se taj model odgovora na pretnju mogao ponoviti i biti uspešan. Ovde se radilo o dobrovoljnom vremenu posvećenom manuelnim, repetitivnim, a ipak pažljivo izvršenim intervencijama na kodu. Međutim, „mnogi od učesnika u ovim dobrovoljnim zajednicama saradnje su motivisani radoznalošću za rešavanjem novih izazovnih tehnoloških problema. Repetitivni zadaci ubijaju uživanje homo ludensa.»[214]

Treće, treba znati da malver Confiker nije u potpunosti pobeđen, jer on i dalje postoji na zaraženim kompjuterima širom sveta, a vlasnici tih kompjutera ne mogu se prinuditi da očiste svoje kompjutere od ovog virusa. Pri tome, tehnički je izvodljivo očistiti većinu ili čak sve zaražene kompjutere (pošto su zaraženi i samim tim ranjivi) - bez pristanka i znanja vlasnika. Pravno posmatrano, to bi bilo krivično delo,

[212] Ibid. str. 96.
[213] Ibid. str. 97.
[214] Ibid. str. 97.

hakovanje, čak iako je benevolentno. Nikakva neformalna radna grupa nema pravo da to uradi.

Ovde ćemo samo dodati napomenu da se i u tom pogledu situacija menja, time što u nekim slučajevima vidimo da prodavaci opreme, softvera, pristupa internetu, unose u svoje ugovore sa kupcima odredbu o nasilnom ažuriranju uređaja koje su prodali. Time dobijaju pristanak kupca da vrše neke aktivnosti sa njegovim/njenim uređajem, tako da bi taktika prinudne „daljinske dezinfekcije“ čak i mogla da se legitimno primeni u slučaju da botnet (čiji je vaš uređaj nesrećno postao deo) postane platforma napada za rušenje kritičke infrastrukture.

Zašto ovaj drugi argument smatram slabijim od prvog? On počiva na benevolentosti aktera da se zajedno suprotstave određenom napadu. Ali ova vrsta benevolentnosti je situaciono stvorena. Može se prihvatiti da bi se ponovila u sličnoj vrsti situacije, ali u kontekstu interneta ima bezbroj vrsta situacije. Uz to, postoji razlika u benevolentnosti kada se radi o incidentnom (novom, zanimljivom, dramatičnom) i kada se radi o redovnom (rutinskom, dosadnom). Ovaj argument nam ne govori ništa o mogućnosti benevolentnog okupljanja aktera u redovnim situacijama na internetu.

Vidimo da je mrežno upravljanje na internetu prisutno u delu koji se tiče rutiranja i da većina aktera želi da ga zadrži zato što se tako čuva raspodela moći među njima. S druge strane, mrežno upravljanje nema jasnu situaciju sa resursima (dobrovoljni angažman itd.) i ne može do kraja rešiti incidentne situacije i izazove sajber kriminala zato što mora ostati u granicama zakona i međunarodnih sporazuma. Ako postoje garancije individualnih sloboda, privatnosti, svojine i suverenosti država u onlajn svetu, preuzete iz oflajn sveta, mrežno upravljanje se tome pokorava, čak i kad je tehnički gledano u prilici da nametne svoje prioritete dobrobiti interneta. Zato je benevolentnim (globalnim) tehničkim ekspertima potrebna veća saradnja sa nacionalnim organima za primenu zakona.

Miler, Šmit i Kirbis su dali savet nacionalnim državama, sa kojim se možemo složiti, o tome kako da gledaju na mrežno upravljanje. Države se mudro prilagođavaju mrežnom upravljanju ne tako što vrše direktnu hijerarhijsku kontrolu nad njim, nego „tako što se ubacuju u tehničke i operativne mreže i pokušavaju da oblikuju standarde i prakse u multiakterskom okruženju“.[215] Po našem mišljenju, kapacitet državnih

[215] Ibid. str. 100.

struktura da se ubace u ove mreže je tek u zametku i baziran na ličnoj inicijativi. Nasuprot tome, bilo bi produktivnije planirati saradnju državnih struktura sa naučno-istraživačkim ustanovama sopstvene zemlje, kako bi pojedinci iz ove sfere mogli da «predstavljaju» državu u ovim ad hoc mrežama, ako i kad se za to ukaže potreba.

Mrežno upravljanje daje doprinos u inovaciji načina funkcionisanja infrastrukture interneta. Ono je do sada uspešno pružilo otpor nekim tekućim izazovima. Nema razloga da tako ne bude i u budućnosti, ali to zavisi i od prirode budućih izazova. „Premda (mrežno upravljanje – prim. aut.) može imati propuste i padove ponekad, pokušaji da se uvedu više hijarhijski organizacioni oblici neće biti laki i stvaraće sopstvene sukobe i probleme, posebno ako hijerarhija bude doticala države koje se nadmeću“.[216]

[216] Ibid. str. 101.

PETO POGLAVLJE

Neregulisani internet – tamni internet

Rasprava o upravljanju internetom ne sme da ispusti iz vida i jednu činjenicu iz realnosti – tamni internet (na engl. Dark Web). To je metaforički rečeno mlađi nestašniji brat interneta, nastao zahvaljujući jednom softveru za enkripciju. Softver je bio TOR, engleska skraćenica od The Onion Router, što bi na srpskom moglo da se zgodno prevede: luk(avi) ruter. Danas je TOR postao specifična alternativna mreža internetu.

TOR je stvorila mornarica SAD-a 2002. god. za zaštitu svojih komunikacija, ali je došao i do ruku van mornarice SAD-a. Logika ovog softvera je da usmerava digitalni saobraćaj koristeći internet ali u posebnoj mreži preko serije posebnih luk(avih) rutera, dodajući slojeve enkripcije na raznim nivoima, tako da (manje tehnički visprenim licima) postane nemoguće da prate korisnike interneta i internet stranice koje oni posećuju. TOR je doneo praktičnu anonimnost za sve koji je žele. Anonimno surfovanje internetom je bila privlačna ideja mnogima i iz raznih razloga.

Mnogi korisnici TOR-a koriste ovaj softver da bi sačuvali privatnost svoje komunikacije ali isto tako i za kriminalne aktivnosti. Tipična aktivnost je kupovina droge, ali moguće je i sve drugo što bi na internetu i u realnom životu bilo nelegalno. Šta god da je u pitanju, i vlasnici nedozvoljenog sadržaja i korisnici istog se okreću posredniku odnosno TOR-u koji prikriva njihov indentitet i njihovo kretanje na internetu. Početna stanica ili centralno mesto okupljanja u TOR-u je nelegalna internet stranica koja se naziva Put svile (the Silk Road).

Dok na internetu morate imati domen koji se nalazi u ICANN-ovom DNS-u, u TOR-u postoje alternativni .onion domeni. Korisnik (regularnog interneta) treba samo da instalira TOR softver na svoj računar, i da otvori nalog u TOR, da bi potom sve ostalo vezano za saobraćaj obavljao sam softver. Čak i regularna IP adresa koju taj korisnik koristi za regularni internet će putem TOR-a biti sakrivena tj. postaće nevidljiva tako da se ne može pratiti od strane korisnikovog provajdera internet usluga, a posledično ni od državnih organa reda. Korisnik TOR-a može da posećuje sve stranice date u TOR sistemu, kao i da postavlja svoje itd. «Ovde ne postoje zakoni i slobodni ste da objavljujete šta god hoćete i niko nikad neće moći ni da vas identifikuje a kamoli da

vas zaustavi.»[217] Korisnik TOR-a može tajno da komunicira sa drugim korisnikom TOR-a, tako što tom partneru da niz karaktera generisanih u TOR-u za tu namenu. Da bi stvar bila još efikasnija, za plaćanje u TOR mreži uvedena je posebna valuta, bitkoin, uz još neke mogućnosti plaćanja. Bitkoin je takođe mogao da kupi/razmeni bilo ko ko poseduje novac u realnom svetu.

Dosta sličan ali ne i identičan pojam je Duboki veb (na engl. Deep web), koji obuhvata sve vrste sadržaja kojima se ne može tipično pristupiti preko (regularnog, javnog) interneta – bilo zašto što imaju nestandardno ime domena, bilo zato što ka njima ne vode linkovi sa drugih stranica, bilo zato što su nemogući za indeksaciju za standardne pretraživače. Još jedan termin za ove skrivene delove mreže u koje se, uz odgovarujću zaštitu, ulazi iz interneta je Nevidljivi internet (na engl. Invisible Internet).

Tamni internet je mračna strana javnog interneta. On je svakako baza nezanemarljivog kriminalnog miljea.[218] Ipak, osim što ga prati ta negativna konotacija, postoje mišljenja da je on u isto vreme i pozitivan fenomen, odnosno bastion odbrane slobode. Dok su se internet arhitektura i infrastruktura promenile u smeru manje slobode za korisnika, tamni internet je uveo kontratežu tom smeru. Jedan komentator ovako komentariše postojanje tamnog/dubokog/ nevidljivog veba: «To je prirodan i neizbežan odgovor na pokušaj vlade da primeni više kontrole nego što tehnorati osećaju da je prihvatljivo».[219]

Tehnički vispreni hakeri su jednostavno promenili arhitekturu interneta na ovaj način. Kako je to bilo moguće, otkuda im takva moć?

---

[217] Iz: Roger Davies. (25. jun 2011). "What is Dark Internet, How to Access Onion Domains and Configure Hosting for the Dark Web". Dostupno na http://www.rogerdavies.com/2011/06/dark-internet/

[218] Danas je sajber kriminal identičan organizovanoj kriminalnoj aktivnosti u oflajn svetu. Jedna moguća klasifikacija sajberkriminalnih aktivnosti izgledala bi ovako:

- Upadi u informaciono-komunikacione sisteme zarad monetarnih i drugih koristi
- Presretanje informacija zarad špijunaže
- Manipulacija informacijama ili mrežama
- Uništavanje podataka
- Zloupotreba procesorskih kapaciteta
- Krivotvorene robe
- Tehnike izbegavanja pravde

U mračnom internetu dakle postoji pravo tržište sajber kriminalnih usluga, tako da kupac, koji može biti i kompjuterski nepismen, uz pomoć novca lako da može da izvrši (naruči) aktivnosti koje želi. On/a može da bira da li će ići na iznajmljivanja ili kupovinu malvera, da li želi «Usluga prevare», «Usluga napada», «Usluga izbegavanja pravde». Uz ponudu ide naravno i nešto nalik cenovniku, tj. to je katalogu sa cenama. Treba napomenuti da se u mračnom internetu nude i usluga koje nisu kriminalne, kao što su lažni profili na društvenim mrežama, prodaja lajkova na njima itd..

[219] Roger Davies, opus cit.

Odgovor je jednostavan: ključ moći leži u enkripciji. Osnovna činjenica od koje se polazi jeste ova: Jednostavnije je šifrovati informaciju nego dešifrovati je, a dešifrovanje je matematička operacija.[220] Stoga enkripcija (softver za enkripciju) daje mogućnost svakom pojedincu, koji raspolaže dovoljnim znanjem, da sačuva svoje tajne na internetu, i time preokreće odnos moći između pojedinca korisnika interneta, s jedne strane, i vlade, kompanije ili bilo kog drugog ko želi da ga nadzire. Korisnik interneta samo treba da odluči da primeni šifriranje svoje komunikacije, za šta su mu već na raspolaganju besplatni programi. Oni su relativno jednostavni za primenu, ali i nešto tehničkog razumevanja dobro dođe. Kada se ti uslovi ispune, moglo bi se reći korisnik (regularnog interneta) može da nestane sa interneta i istovremeno bude na njemu.

Dva primera – poruke svetu iz Tamnog interneta

Prvi primer: napad na trgovinski lanac Target

Po nekima najveći sajber kriminal odigrao se pred božićne praznike 2013. god. u SAD-u, a reč je o napadu na trgovinski lanac Target (drugi lanac po veličini u SAD). U vreme kada se obavlja najveći obim prodaje u Target radnjama, napadači su postavili na server ove firme svoj softver (program) koji se vezao za čitače kartica na prodajnim mestima ovog lanca. Softver je uzimao podatke sa magnetskih traka svih platnih kartica uvučenih u čitače i sa svih korisničkih naloga kupaca u sistemu (korisnički nalozi sadrže imena, adrese, telefonske brojeve, imejl adrese kupaca). Tokom dve nedelje na taj način je ukradeno 40 miliona platnih kartica i 70 miliona korisničkih naloga kupaca. Target je nakon što je vest procurela novinarima priznao da je predmet napada tj. da ima problem sa bezbednošću – ali tek više dana nakon što je napad izvršen. U istraživanje slučaja uključile su se nadležne američke službe. U svom objavljenom izveštaju su ovaj maliciozni softver (malver) nazvale Kaptoxa (na ruskom jeziku krompir). Drugi naziv koji se sreće je Black POS odnosno Crni čitač kartica.

[220] Dešifrovanje je zapravo rešavanje matematičkog problema.

Časopis International Business Times je započeo svoj članak[221] o tom događaju sledećim pitanjem: „Šta imaju zajedničko dva ruska programera, ukrajinski kriminalac i dva meksička krijumčara? To zvuči kao početak etničkog vica, ali nije u pitanju vic“[222] nego činjenica da su svi ti ljudi bili povezani sa ovim sajber napadom na Target.

Istraga je pokazala da je tvorac malvera neko sa nadimkom ree4, te da taj nalog koristi osoba poznata po tome da zarađuje novac programiranjem alata za hakere i poučavanjem hakera. Ispostavilo se da iza nadimka ree4 stoji jedan 23ogodišnji Rus, rok muzičar Rinat Šabaev, koji je priznao da je napisao deo softvera. Šabaev je izjavio da je njegova jedina namera bila da napiše kod i proda ga, a ne da ga koristi pošto je svestan da je korišćenje nezakonito. „Ja sam ga napisao za prodaju. Neka ga drugi ljudi koriste, pa to pada na njihovu savest.“[223]

Istraga je dalje dovela do toga da je onaj ko je zapravo iskoristio malver jedan Ukrajinac iz Odese pod nadimkom Rescator, koji vodi upućenima poznate prodavnice na tamnom internetu u kojima se prodaju ukradene platne karatice. Pravo ime „prodavca“ ukradenih kartica je Andrej Hodirevski. Kao državljanin Ukrajine mogao bi biti dostupan organima SAD-a tek u vrlo komplikovanom scenariju saradnje. Da stvar bude zaista kao u vicu, jedini koji su uhapšeni i procesuirani za ovaj napad su bili državljanin i državljanka Meksika, koji su uhapšeni u Teksasu (SAD) zbog nošenja 90 platnih kartica za koje se utvrdilo da su deo onih ukradenih u napadu na Target.[224]

Na ovom primeru se vide neke od osobina sajber kriminala, kao što su to da zahteva minimalne resurse za veliku potencijalnu štetu, da ga je moguće počiniti u jurisdikciji u kojoj počinilac nije fizički prisutan i da često delimično nije nezakonit. Ne samo da više lica umešanih u ovo delo nisu mogla biti lako procesuirana, nego ni skupljanje zvaničnih dokaza protiv njih nije lako.

[221] Ryan W. Neal. (24. jan. 2014). “Russian Coders, Ukrainian Cybercriminal, Mexican Smugglers and The Largest Cybercrime in History” *International Business Times*. Dostupno na http://www.ibtimes.com/russian-coders-ukrainian-cybercriminal-mexican-smugglers-largest-cybercrime-history-1547854

[222] Neal, opus cit.

[223] Neal, opus cit.

[224] Neal, opus cit. Tekst se završava duhovitom konstatacijom da će se desiti još mnogo ovakvih propusta „pre nego što trgovci mogu kupcima prodati obećanje stvarne privatnosti“.

Drugi primer: afera Dejvida Snoudena

Afera je izbila kada je juna 2013. godine Amerikanac (tada 28 godina) Djevid Snouden dostavio novinskim kućama *The Guardian* i *The Washington Post* fajlove koje je prikupio dok je radio u Nacionalnoj bezbednosnoj agenciji SAD (NSA)[225] U fajlovima su se nalazile informacije o onome što je radila NSA (informacije obuhvataju period 2010-2012), a što je Snoudenu, koji nije pravnik, bilo zdravorazumski jasno da nije u skladu sa zakonima SAD-a, niti sa osnovnim principima i vrednostima na kojima ta zemlja počiva. Iako su to tajne informacije i on je radeći za NSA bio u obavezi čuvanja tajnosti, smatrao je da treba obavestiti javnost o tome. Novinari koji su mu pomogli – Laura Poitras[226] i Glen Grinvald[227] - su delili njegovo mišljenje. Do sada je objavljen samo deo Snoudenovih fajlova (ili NSA fajlova)[228] zbog snažne kontra akcije od strane NSA, ali je i to objavljivanje dovelo do ogromnih reakcija kako u SAD tako i u ostatku sveta.

Kako je Snouden očekivao da će biti gonjen za svoj čin, neposredno pre početka afere otišao je u Hong Kong, gde je obavljena primopredaja informacija između njega i američkih novinara. Zahvaljujući garancijama slobode štampe u SAD, novinari su bili zaštićeni od pravnog gonjenja. Snouden je pak morao biti u begu od američkih tajnih službi nakon izbijanja afere i vrlo brzo se obreo u Moskvi, gde mu je odobren privremeni azil, a kasnije i rezidencijalna viza koja traje i dalje. U SAD-u je protiv Snoudena podignuta optužnica po tri osnova: za krađu imovine vlade, za nedozvoljeno odavanje informacija o odbrani i za namerno odavanje poverljivih informacija. SAD od Rusije traži njegovo izručenje. U očima dela američke javnosti, Snouden je izdajnik. Za branioce slobode, u SAD i van nje, Snouden je heroj, koji se po cenu samožrtvovanja suprotstavio zloupotrebi američkih vlasti koje su prekršile osnovne slobode. Može se pretpostaviti da za NSA radi više hiljada ljudi, ali je samo jedan – Snouden - imao lične kapacitete potrebne da uspešno javno razotkrije određena postupanja. Po do sada dostupnim izvorima, Snoudenov motiv je bila briga za javni interes tj. za zaštitu privatnosti miliona ljudi.

[225] National Security Agency – u daljem tekstu će se koristiti skraćenica NSA.
[226] Laura Poitras je dobila kao reditelj nagradu Oskar za najbolji dokmentarni film 2015. godine, a reč je o filmu *CitizenFour* u kome se nalaze njeni intervjui sa Snoudenom
[227] Glenn Greenwald je 2014. godine objavio knjigu *No Place to Hide: Edvard Snowden, the NSA and the US Surveillance State.* Picador.
[228] Prvi tekst (Grinvaldov) u *The Gardijan* izašao je 6. juna 2013.godine o nadzoru mobilnih telefona, a drugi (autori Barton Gellman i Poitrasova) u *Washington Post* 7. juna 2013. godine o nadzoru interneta.

Iako je tačno da je Snouden formalno gledano prekršio zakon, postavlja se pitanje: "da li je stvarno kršenje zakona reći javnosti da njeni lideri krše zakon?"[229]

Ilustracija 12 Fotografija Edvarda Snoudena

Preuzeto sa: http://www.elciudadano.cl/2014/12/01/129766/edward-snowden-recibe-el-premio-nobel-alternativo-por-el-riesgo-de-extradicion-no-podra-asistir-a-la-ceremonia/

Ilustracija 13 Naslovna strana filma CitizenFour

Preuzeto: http://www.imdb.com/title/tt4044364/?ref_=nm_knf_i1

Afera Snouden ne bi zaslužila prostor u ovom radu samo zato što se radi o tome da je Snouden, da bi dopreo do novinara kojima je verovao, koristio tamni internet odnosno TOR, tj enkriptovanu komunikaciju, kao i mnogi drugi za ono što žele da urade tajno. Niti bi se našla u ovom radu samo zato što je Snouden, po svemu sudeći, u svom činu bio posvećen opštem dobru, na uštrb lične koristi, jer je to slučaj i sa mnogim drugim tehnološki suverenim korisnicima interneta (dobrim hakerima, tvorcima otvorenih protokola, učesnicima u kolaborativnim projektima tipa Vikipedije i dr.).

Ono glavno što daje zasluženo mesto Snoudenovom otkriću u ovom radu je sama sadržina tog otkrića, važna informacija o infrastrukturi interneta koja do juna 2013. godine nije bila izrečena (barem ne na tako glasan način). Ta informacija glasi: na

[229] John Robinson Jr. (21. apr. 2014). "The Snowden Disconnect: When the Ends Justify the Means" Dostupno na http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2427412 (U daljem tekstu "Snowden Disconnect") Str. 20.

internetu je na delu sajber-nadzor i privatnost korisnika interneta je ugrožena. Internet je mreža svih mreža koja se strateški nadzire od strane NSA (i nekih drugih službi bezbednosti u vodećim svetskim državama).

Nadzirani internet – na više načina

Razmatranje o nadziranom internetu treba da krene od važne informacije o internetu koja je stigla od Edvarda Snoudena do nas, uz pomoć tamnog interneta, o tome da agencija vlade SAD-a na nedozvoljeni način "posmatra" internet i skladišti digitalne podatke iz internet saobraćaja bez obzira ko su njihovi vlasnici i koje su njihove svrhe. No, to je tek deo uvida o nadziranom internetu. Osim jedne ili više država, osim kriminalaca, treba reći da internet nadziru i komercijalni akteri, privatne kompnaije koje posluju preko interneta. Dok kriminalci nemaju nikakvo opravdanje zašto to čine, a država pokušava da opravda to postupanje nacionalnim interesom tj. opštim dobrom, privatne kompanije kao argument za to nude interes samih nadziranih tj. korisnika (jer će kroz prikupljenje informacije o njima biti u stanju da im pruže bolju uslugu).

Nadzor nad građanima koji vrši država verovatno je postojao i pre pojave interneta. U ovom radu se mora reći nešto više o Snoudenovom otkriću vezanom za internet, ali treba znati da je u Snoudenovim dokumentima i dokaz da je nadzor mnogo širi. Pod istim tretmanom, pored interneta, je i mobilna telefonska komunikacija u SAD (telefonska kompanija Verizajn predaje NSA metapodatke sa mobilnih telefona svojih korisnika) i telefonska komunikacija van SAD (program MYSTIC u sklopu koga se prisluškuju telefonski pozivi u ciljanoj zemlji, na primer Iraku, ali uz mogućnost da budu prisluškivani i pozivi iz SAD-a). Što se tiče samog interneta, američka NSA kroz program PRISM, zajedno sa partnerskom službom GCHQ u Velikoj Britaniji, nadzire internet saobraćaj na način da je prikačena na servere glavnih kompanija na internetu (Epl, Gugl, Majkrosoft i Fejsbuk[230]) i na okosnicu interneta tj. najveće ISP-ove (iz grupe tier 1) i da kopira svaki bit podataka koji prolazi internetom preko ovih servera. Uzimaju se metapodaci o imejl adresama i IP adresama, lokacijama, posećenim internet stranicama i svim drugim tragovima na internetu. Ovi metapodaci

[230] Nazivi stranih kompanija u ovom radu se navode u transkribovanoj formi, jer su dovoljno poznati pa se njihovi originalni nazivi na engleskom jeziku mogu podrazumevati kao poznati.

se skladište u NSA na neko vreme (tačno trajanje nepoznato). Program se sprovodi verovatno od 2007. godine, a danas se zvanično zove SIGAD US-984XN.[231]

Kao objašnjenje zbog čega je taj program uveden NSA navodi: "prevazilaženje nedostataka u normalnoj proceduri FISA[232] za dobijanje sudskog naloga za svaki zahtev za presretanje."[233] Drugim rečima, zaposleni u NSA su smatrali da FISA "štiti privatnost osoba koje nemaju prava na privatnost (stranaca, kada njihov internetski saobraćaj prelazi preko teritorije SAD-a – prim.aut.). Očigledno, NSA ne veruje u osnovno pravo na privatnost."[234] To je priznao čak i predsednik SAD-a izjavivši: "Strahovi za našu privatnost u doba interneta i big-data analitike su opravdani."[235] Ono što se može dodati je da uzrok straha leži zapravo u odmetnutoj ili "odmetnutoj" vladinoj agenciji.

Margaret Hu u svom članku "Taksonomija Snoudenovih otkrića"[236] iz 2015. godine je razvrstala koje vrste postupaka NSA izvodi nad podacima / metapodacima, odnosno koje su vrste postupaka za koje smo saznali iz objavljenih materijala. Ona dolazi do sledećih vrsta postupaka NSA:

- Sve skupi. ("Collect It All.")
- Sve procesuiraj. ("Process It All.")
- Sve iskoristi za napad. ("Exploit It All.")
- Sve omiriši (u cilju izdvajanja meta). ("Sniff It All.")
- Sve podeli sa partnerima. Saznaj sve. ("Partner It All." "Know It All.")

Ovde ne možemo detaljno objašnjavati svaku od navedenih vrsta postupaka NSA. Huova zaključuje da se ovime ilustruje "kako smo svedoci istorijski značajnog prelaza sa metoda nadzora malih podataka na metode nadzora velikih podataka (big-data analitika[237] – prim. aut.)".[238]

---

[231] „Snowden Disconnect", str. 9.
[232] FISA je skraćenica za Foreign Intelligence Surveillance Act, Zakon za nadzor tajnih službi, donet u SAD-u 1978. god. po kome tajne službe za nadzor na teritoriji SAD-a moraju tražiti nalog od posebnog suda kreiranog tim zakonom (skraćenica FISC).
[233] "Snowden Disconnect", str..11.
[234] Ibid. str..12.
[235] Ibid. str..15.
[236] Margaret Hu, "Taxonomy of the Snowden Disclosures" in Washington and Lee Law Review, Vol. 72, 2015. Dostupno na http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2730245 (U daljem tekstu "Taksonomija")
[237] Pojam big-data analitika je težak za definisanje, ali za potrebe ovog rada ćemo reći da je to oba "I tehnologija konfigurisanja informacionog hardvera da bude sposoban da prosejava, sortira i istražuje velike količine podataka ali i process koji podrazumeva iskopavanje obrazaca u podacima, destilovanje obrazaca u predviđajuću analizu i primenu te analitike na nove podatke." "Taksonomija" str. 1698.
[238] "Taksonomija" str.1688.

Ipak, Snoudenova otkrića nisu bila otkrivanje potpuno nepoznate stvari. On je prvi doneo dokaze, što je veoma važno, ali o nadzoru nad internetom američka štampa je pisala godinama pre 2013. Tako imamo primer pisanja *The Wall Street Journal*-a iz 2008. godine – jedan dugačak tekst Siobana Gormana pod nazviom „Domaće špijuniranje NSA raste dok agencija skuplja podatke“.[239] Prve rečenice ovog teksta već same po sebi dovoljno govore i daju jasnu sliku da se tu radi o višegodišnjem procesu:

> „Pre pet godina, kongres je ugasio eksperimentalni antiteroristički program Petnagona namenjen tome da usisa elektronske podatke o ljudima u SAD da bi tragao za sumnjivim obrascima. Oponenti su ga nazvali preširokim upadom u privatnost Amerikanaca, čak i nakon terorističkih napada 11. septembra. No rad na prosejavanju podataka nije nestao. NSA, nekada ograničena na nadzor u inostranstvu, gradila je u suštini isti sistem.“[240]

Članak objašnjava kako je NSA napravio „malo poznate“ aranžmane sa telekomunikacionim kompanijama, bankama, institucijama koje vode evidencije putovanja i sl. Time je NSA obezbedila način da dobija ove tzv. transakcione podatke od drugih službi ili privatnih kompnija (čak i iz tzv. crnih/tajnih programa). Sve te podatke (tada je upotrebljen termin transakcioni podaci) potom njeni sofisticirani softverski programi analiziraju u smislu otkrivnaja sumnjivih obrazaca.

> „Nije jasno koliko ovih raznih vrsta podataka se kombinuje i analizira u jednoj bazi podataka kod NSA. Jedan zvaničnik iz službi bezbednosti je rekao da rad NSA povezuje ukupno oko dvanaest antiterorističkih programa.“[241]

O planiranim troškovima ovih poduhvata stoji da je budžet NSA za rad na prosejavanju podataka poverljiv, ali ga je „jedan zvaničnik procenio na preko 1 milijarde USD.“[242]

Interesantno je da već ovaj članak navodio da je jedan broj zaposlenih u NSA izrazio zabrinutost da bi agencija mogla prekoračiti svoja ovlašnjenja upadanjem u nadzor nad domaćim stanovništvom, ali je autor članka preko toga samo preneo izjave glasnogovornika NSA da NSA striktno poštuje zakone i propise. S druge strane, navodi se da je program nadzora terorista izazvao već 38 sudski tužbi protiv

[239] Siobhan Gorman. (10. mart 2008). “NSA’s Domestic Spying Grows As Agency Sweeps Up Data”. *The Wall Street Journal*. Dostupno na http://www.wsj.com/articles/SB120511973377523845
[240] Gorman, opus cit.
[241] Gorman, opus cit.
[242] Gorman, opus cit.

kompanija koje su sarađivale sa vladom, tako da „Bela kuća želi da kompanijama koje pomažu vladin nadzor da imunitet od sudskih tužbi po osnovu povrede privatnosti, ali su demokrati u kongresu to blokirali.“[243]

Za razliku od argumentisanja na bazi procedure FISA, te 2008. godine argumentacija sigurnosnih službi je bila malo drugačija. Gorman prenosi da se sigurnosne službe zalažu da vlada uvede nova pravila u pogledu privatnosti, a opravdanje koje je navedeno se može parafrazirati ovako: pošto ljudi ionako rutinski stavljaju detalje iz svog života na stranicama društvenih mreža kao što je Maj spejs, njihov idnentitet ne bi trebalo da ima istu zaštitu kao u prošlosti. „Umesto toga, samo njihova 'esencijalna privatnost' ili 'ono što bi oni želeli da zaštite o svom životu i poslovima' treba da bude pod velom.“[244] Nije navedeno šta se pod esencijalnom privatnošću konkretno misli.

Nadzor koji vrše kompanije ima sasvim drugu metodologiju, drugi prizvuk, obim i obrazloženje. U ovom nadzoru radi se o praćenju traga veb sajta (web tracking), što bi se moglo opisati na sledeći način: kada korisnik ode na neki veb sajt (njegov uređaj pošalje HTTP zahtev), ta stranica koju je posetio „hvata“ njegove podatke, često ga i ne obaveštavajući o tome. Te podatke kompanije čiji su sajtovi posećeni međusobno (komercijalno) razmenjuju, odnosno jedna u korist druge prate tragove. Veoma jasnu analizu razmera ovog fenomena doneo je rad Timotija Liberta „Izlaganje skrivenog veba: analiza HTTP zahteva trećih strana na uzorku od milion veb sajtova“[245] iz 2015. godine. „Nalazi studije ukazuju da blizu 9 od 10 veb sajtova daje korisničke podatke stranama za koje korisnik verovatno nije svestan; preko 6 od 10 veb sajtova ubacuje kukije trećih strana; preko 8 od 10 veb sajtova ubacuje na kompjutere korisnika kod Javascript koji potiče od spoljnih strana.“[246] Analiza je ukazala i da korisnicima mogu biti praćeni tragovi od strane više entiteta u tandemu, kao i da je 1 od 5 veb sajtova potencijalno ranjiv prema trenutno poznatim tehnikama špijuniranja NSA.

S druge strane, Libert referira na rezultata više anketa u kojima se došlo do stavova korisnika koji su protiv ovakvih praksi. U velikom procentu još 1999. godine su

[243] Gorman, opus cit.
[244] Gorman, opus cit.
[245] Timothy Libert. (Oct. 2015). “Exposing the Hidden Web: An Analysis of Third-Party HTTP Requests on One Million Websites” *International Journal of Communication*, arXiv:1511.00619 Dostupno na https://timlibert.me/pdf/Libert-2015-Exposing_Hidden_Web_on_Million_Sites.pdf Analiza je obuhvatila najboljih milion sajtova, koji su rangirani na listi Alexa (ćerka firma Amazona) u maju 2014. godine..
[246] Ibid. str.2.

korsnici iskazivali zabrinutost za privatnost na internet stranicama, a istraživanja iz 2009. su beležila da korisnici smatraju da bi trebalo da postoji neki zakon koji ljudima daje pravo da znaju sve što posećeni veb sajt znao o njima. Ukoliko zakon zvuči previše drastično, postojala je i ideja da veb sajtovi uvedu DNT standard ("Nemoj pratiti" na engl. Do Not Track) kao opciju za posetioce, ali se to nije desilo. Kompanije su povećavale svoje praćenje tragova korisnika, ne obazirući se na upozorenja da to ugrožava privatnost. "Razlog koji bi stručnjaci za marketing mogli da navedu u prilog tome da je onlajn skupljanje podataka prihvatljivo je taj da kupci prave trade-off između privatnosti i popusta; međutim je studija[247] iz 2015. godine pokazala da se 91% učesnika ne slaže sa stavom 'ako mi kompanije daju popust, pravična razmena je da prikupe informacije o meni bez mog znanja'".[248] Ne ulazeći u kredibilnost rezultata, možemo se zapitati: ako je to tako, ako je tako mnogo onih koji smatraju da nije pravično da se o njima skupljaju informacije bez njihovog znanja, zašto korisnici i dalje posećuju te sajtove i obavljaju aktivnosti na njima?

Ove kompanije (Libert im daje nadimak trekeri, na engl. Trackers) su uveliko poznate. Ovde donosimo Libertov prikaz statistike o ovoj aktivnosti kompanija. Daleko najjači treker je kompanija Gugle, sa 78% praćenih sajtova, zatim slede Fejsbuk sa 32%, Akmai (koji hostuje sadržaje Fejsbuka i drugih kompanija) sa 23% i Tviter sa 18%. (Gugl ima više stotina domena, od kojih su neki logični, kao što je google.com ili google.fr a neki relativno prikriveni, na pr. 1e100.net ili ggpht.com To važi i kod ostalih kompanija. To nije nedozvoljeno, ali znači da će se trag nečije istorije surfovanja moći hvatati i sa tih manje poznatih adresa.)

[247] U pitanju je studija J.Turow, M.Hennessy and N.A. Draper. (2015). "The tradeoff fallacy, how marketers are misrepresenting American consumers and opening them up to exploitation". *The Annenberg School for Communicaiton, University of Pennsylvania,* Navedeno prema: Libert, opus cit. str. 9.

[248] Ibid. str. 3.

Ilustracija 14 Grafikon – Procenat praćenih veb sajtova od strane prvih 50 kompanija

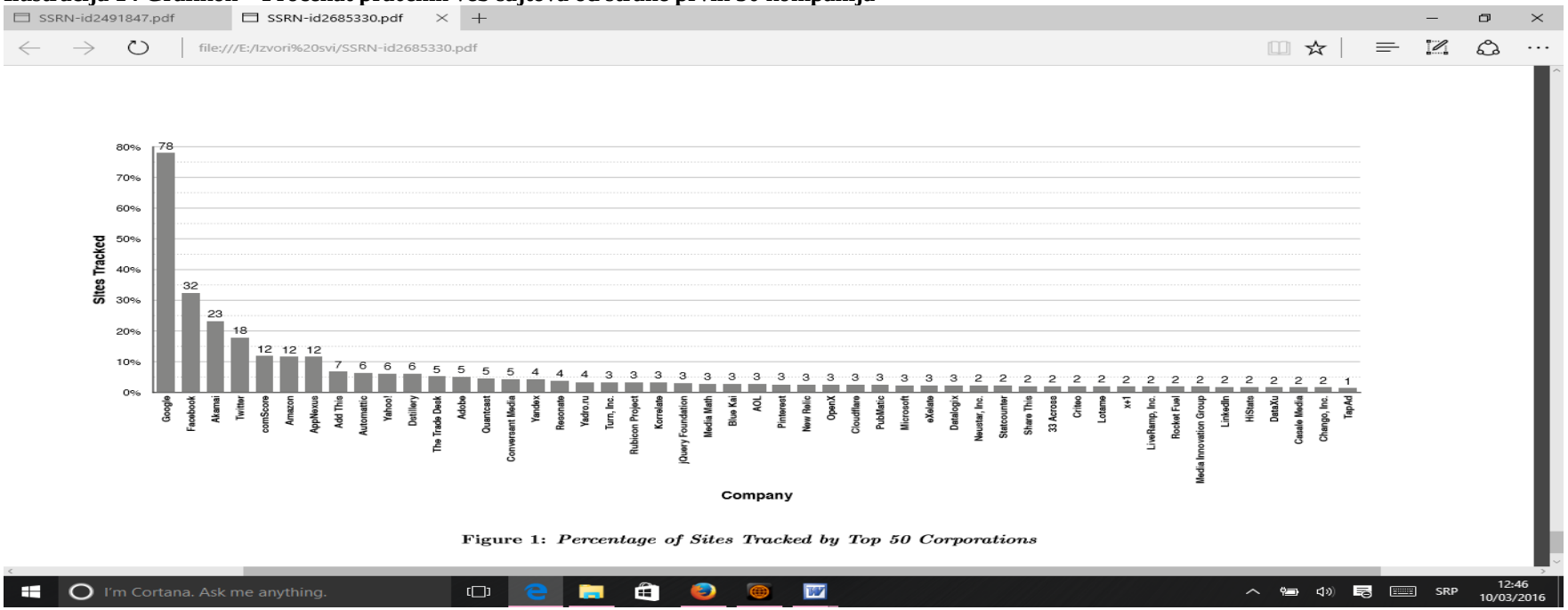


Figure 1: ***Percentage of Sites Tracked by Top 50 Corporations***

Preuzeto iz: Timothy Libert “Exposing the Hidden Web: An Analysis of Third-Party HTTP Requests on One Million Websites”

International Journal of Communication, October 2015. str. 10. arXiv:1511.00619

Da li se može zaključiti da korisnici prećutno pristaju da trekeri "hvatanju" podatke o tome šta korisnici rade na internetu? Čini se da je tako, što mogu tumačiti prevashodno time da korisnici interneta nisu do kraja preuzeli odgovornost za same sebe.

Libert je pak skloniji da uobliči pitanje na drugi način: kako možemo da usaglasimo očekivanja korisnika i ponašanje kompanija? "Postoje tri glavna rešenja koja se trenutno primenjuju: mehanizam za 'opt-out', dodaci u pretraživačima tj. brauzerima i mehanizam DNT."[249] Iako svako od ovih rešenja ima određenu efikasnost, sva ona počivaju zapravo na tome da bilo internet kompanija bilo država uradi nešto kako bi se praksa praćenja tragova uskladila sa željama korisnika interneta. Ova rešenja ne upućuju da korisnik sam uradi nešto da njegovi podaci ne bi bili praćeni kada posećuje svoje omiljene veb sajtove. O ovoj temi biće više reči u poglavljima 8 i 9.

Iz dosadašnjih razmatranja o upravljanju internetom jasno je da ovaj tehnički sistem veoma težak za upravljanje i ima više izazova od onog što glavni akteri mogu da savladaju. Uočava se jedno jezgro regulisanosti i stabilnosti, vezano za ključnu infrastrukturu, ali oko tog jezgra se prostire široki obod gde, što se tiče upravljanja, nekih prihvaćenih pravila nema. Tu vlada haotično sudaranje, ali ponekad i poklapanje partikularnih interesa. Ipak, tokom decenija je upravljanje u jezgru opstalo i ostalo održivo, iako ko-egzistira sa tim i takvim obodom.

Deo interneta koji izmiče regulaciji može biti zanimljiv na dva načina: u odnosu na kriminalnu sferu kojoj je dao stanište i u odnosu na potencijal subverzivnosti koji mu je implicitan. Zbog tog svog potencijala subverzivnosti, tamni internet je potkopao sliku o javnom zvaničnom internetu i otvorio temu naličja interneta. Neupravljani internet je tako postigao dve stvari:

1. stekao kredibilitet i neku vrstu legitimiteta kod kritički osvešćenih korisnika interneta i
2. umanjio moć zvaničnih aktera, pre svega države i kompanija, rušeći deo tajnosti i gurajući ih u debatu koju nisu želeli.

Tamni internet je uputio izazov običnim korisnicima javnog interneta da se suoče sa realnošću.interneta koji koriste. O tome će biti još reči u poglavlju 8.

[249] Ibid. str. 7.

ŠESTO POGLAVLJE

Internet i njegova materijalno prostorna realizacija

Internet je tehnički sistem koji ima svoju materijalno-prostornu realiizaciju. Videli smo da je to sistem koji je od jasne stigao do nejasne arhitekture, a zatim i to da se upravljanje ovim sistemom raslojava na jedno jezgro regulisanosti i stabilnosti, vezano za ključnu infrastrukturu, oko koga se prostire široki obod gde nema prihvaćenih pravila. Sada sledi sagledavanje šta se dešava sa prostiranjem mreže, njenih glavnih čvorišta, u prostoru.

Možda najlepša knjiga na temu materijalno-prostorne strane interneta je ona američkog novinara Endrua Bluma *Cevi: ono iza scene na internetu*[250] objavljena 2012. god. Blum je krenuo od internet kabla iz svoje kuće i poželeo da vidi kuda dalje vode cevi. U tom poduhvatu, obišao je lokacije kao što su Dals (The Dalles) u Oregonu (SAD) – mesto gde kompanija Gugl ima svoje servere, tj. data centar, i Prinvil (Prineville) u Oregonu (SAD) – gde to isto ima kompanija Fejsbuk, deo Londona koji čini kej Temze Doklands (Docklands) i deo Amsterdama koji čini Istočnoindijski kej, selo Portkurno (Porthcurno) na britanskoj obali u Kromvolu – mesto gde se sastaju podmorski optički kablovi i selo Sejšal (Seixal) na delu portugalske obale blizu Lisabona – mesto gde se nalaze kablovi za Zapadnu Afriku. Ovaj svojevrstan putopis je, kako se lepo izrazio jedan komentator, protivotrov za digitalni misticizam, mada se i u samom Blumovom tekstu može naći tu i tamo patetika, kao na primer kada za susret dva optička kabla koristi analogiju ruke boga na Mikelanđelovoj fresci. Njegovi opisi su kao „visoko kvalitetne fotografije graničnog pojasa između fluidnih podataka i fiksnih lokacija, sablasnih liminalnih mesta na šavu globalnog mozga i geološke kore“.[251] Osnovna poruka koju čini se Blum želi da naglasi je: „Sve što radite onlajn putuje kroz neku cev.“[252] (Cev označava optičko vlakno obloženo gumenim i plastičnim slojevima.)

Iz knjige se može naslutiti da jedan mali broj lokacija prima, razmenjuje i transmituje veliki deo internet saobraćaja i komunikacija na planeti. A te lokacije su tu gde jesu zbog razloga geografije, istorije i novca.

---

[250] Andrew Blum. (2012). *Tubes: Behind the Scenes at the Internet*. London: Penguin Books.

[251] Boyd Tonkin. (23 jun 2012). „Tubes: behind the scenes at the Internet, By Andrew Blum“. *Independent* Dostupno na http://www.independent.co.uk/arts-entertainment/books/reviews/tubes-behind-the-scenes-at-the-internet-by-andrew-blum-7873068.html

[252] Tonkin, opus cit.

Geografija interneta

Distribucija i prikaz interneta tj. njegove infrastrukture u prostoru, predmet je interesovanja geografa već krajem prošlog veka. Mnoštvo različitih analiza nastojalo je da sagleda prostorne obrasce koje je internet doneo i objasni ih. Geografska dimenzija interneta se obično razlaže na tri nivoa: gde je tehnička infrastruktura, gde su korisnici i gde se proizvode sadržaji (najpopularniji veb sajtovi). Bilo je i primera prebrzo izvedenih zaključaka o geografiji interneta. Tu mislimo na novinara Francisa Kernkrosa kome se 1997. god učinilo da je zbog postojanja interneta (koji je fascinirao upadljivom lakoćom pribavljanja informacija sa velikih udaljenosti skoro momentalno) „razdaljina mrtva" pa je to stavio u naslov svoje knjige[253]. Ubrzo je Kernkros 2001. god. relativizovao svoj opis: „Smrt razdaljine je razlabavila stisak geografije. Nije ga uništila."[254]

U tekstu Edvarda Maleckog „Ekonomska geografija infrastrukture interneta"[255] iz 2000. godine nalazi se pregled iz kog možemo videti neke važne materijalno-prostorne aspekte interneta. Za potrebe ovog rada fokusiraćemo se na okosnicu interneta i njenu vezu sa gradovima tj. urbanim oblastima.

Za okosnicu interneta bili su presudni novi telekomunikacioni igrači kao i stare telefonske kompanije. Premda je neka infrastruktura već decenijama bila postavljena u javnoj telefonskoj mreži, „pojava paketnog saobraćaja ... izazvala je ulaganje u optičke kablove, koji omogućavaju brži prenos koji nije potreban kod glasovne komunikacije."[256] Naime, paketni saobraćaj traži linkove velike brzine (širokopojasni link) a širokopojasno označava brzinu transmisije veću od 64 kilobita u sekundi, što je normalna brzina za telefoniranje. „Međutim, deregulacija ili liberalizacija su možda jednako značajni kao i tehnologija u formiranju strukture interneta."[257] Univerzalna usluga, koja je bila obvezna za telefonske kompanije, nije ostala obavezna i za nove

[253] Frances Cairncross. (1997). *The Death of Distance: How the Communications Revolution Is Changing Our Lives*. Boston, Harvard Business School Press.
[254] Navedeno prema Malecki. Pogledati fusnotu niže.
[255] Edwarad J. Malecki "The Economic Geography of the Internet's Infrastructure" in *Economic Geography* Vol. 78, No 4, October 2002, 399-424. Dostupno na http://www.jstor.org/stable/4140796?origin=crossref&seq=1#page_scan_tab_contents
[256] Ibid. str. 402.
[257] Ibid. str. 405

telekomunikacione nosače (kerijere). Stoga su oni mogli da oportunistički iskoriste potražnju za internetskim priključcima u najvećim svetskim gradovima. Iz toga je proizašla poslovna strategija ovih telekomunikacionih nosača, koja je zacrtala njihov cilj da postanu globalni provajderi optičkih veza od grada do grada nudeći raznovrsnost ruta i zaobilazeći telefonsku mrežu. Tu situaciju tačno opisuje pojam „arhipelag ekonomija“ – arhipelag čine gradovi ili delovi gradova, enklave, „premijum umreženi prostori“ između kojih su (u datom momentu, tj. 2000. god.) ostala nepozvezana „mrežna geta“. Odlučujuća razlika između prvih i drugih je uspešnost u privlačenju kompanija i profesionalaca da se lociraju baš tu. Takođe i gradovi međusobno počinju da se hijerarhizuju, zahvaljujući broju kompanija (nosača odnosno internet provajdera) koje u njima lociraju svoje operacije i koje se međusobno povezuju.

Malecki uključuje u svoju analizu pojam alpha, beta i gamma svetskih gradova. (Klasifikacije potiče iz 1998. god. od Radne grupe za globalizaciju i svetske gradove Univerziteta Lobourou). Kriterijum za klasifikaciju je ekonomski položaj grada u globalnoj ekonomiji, pri čemu je snaga internet povezanosti jedan od elemenata. Kao alpha gradove Malecki navodi London, Njujork, Tokio i Pariz. Kao beta gradove navodi Čikago, Hong Kong, Los Anđeles, Milano i Singapur. Inače postoje još i gamma gradovi, to su gradovi koji povezuju manje ekonomske regione u svetskoj ekonomiji i, ispod njih, gradovi sa samodovoljnošću koji nisu očigledno zavisni od drugih svetskih gradova. Malecki izdvaja primer Amsterdama, koji je po ovoj klasifikaciji gamma grad, no u samom vrhu je povezanosti gradova u Evropi.

> „Međunarodne rute su koncentrisane u alpha svetskim gradovima do određenog stepena, ali kao što se vidi iz tabele ... set najbolje povezanih gradova je u Evropi a redundantnih ruta visokog kapaciteta je manje u azijskim gradovima: Tokio (na 15. mestu), Hong Kong (na 28. mestu) i Singapur (na 33. mestu). Čikago (na 14. mestu), Milano (na 16. mestu) i Los Anđeles (na 25. mestu) padaju daleko ispod svog mesta prema metageografiji Radne grupe.“[258]

On zaključuje da „Evropa stvara koherentan pan-region i daje protivtežu širokopojasnom kolonijalizmu Sjedinjenih država koji je delovao nadmoćniji pre samo dve godine.“[259]

[258] Ibid. str. 406.
[259] Ibid. str. 406.

Tabela 4 Vodeći evropski gradovi međunarodni internet hub-ovi u 2000. god.

Rang	Grad	Međunarodni širokopojasni link (Mbps)
1	London	86,590
2	Amsterdam	68,302
3	Pariz	62,197
4	Njujork	61,071
5	Frankfurt	52,332
6	Stokholm	18,652
7	Brisel	18,631
8	Ženeva	17,849
9	Toronto	16,399
10	Dizeldorf	15,863

Preuzeto iz Edwarad J. Malecki "The Economic Geography of the Internet's Infrastructure" in *Economic Geography* Vol. 78, No 4, October 2002, pp. 399-424. str. 407.

U isto vreme Malecki navodi da je „osnovna grupa od sedam metropolitanskih oblasti (San Francisko/San Hoze, Vašington DC, Čikago, Njujork, Dalas, Los Anđeles i Atlanta) zadržala svoju dominaciju kao centralnih čvorišta interneta u Sjedinjenim državama".[260] (Ove cifre su bazirane na javnoj okosnici interneta.)

Malecki se još bavio i prostornim razmeštajem IX-ova, delom internet industrije koji se odnosi na interkonekciju. U IX-ovima imamo naplaćivanje za povezivanje odnosno hijerarhijsko bilateralno povezivanje mreža gde manja mreža plaća većoj mreži za povezivanje sa njom kao njihov privatni dogovor/ugovor (na eng. private peering). Odluka da se negde stvori IX (tačka interkonekcije) bazira se na očekivanoj budućoj tražnji ali i na strategiji ubiranja prednosti prvog poteza u nekom regionu. „Interkonekcije između mreža nisu javno poznate i spadaju među mnoge neregulisane aspekte interneta."[261] Ispod ovih IX-ova stoje i povezivanja manjih mreža međusobno, koje se naziva kolokacija, ali se ne zna koji deo saobraćaja odlazi na tu vrstu veza.

[260] Ibid. str. 407.
[261] Ibid. str. 416.

Posmatrajući broj IX-ova uočava se nejednaka globalna geografija IX-ova kako u SAD tako i u svetu. Trenutno ih ima više od 300 u svetu.

Aneks 2 donosi mapu IX-ova.

Tabela 5 Tačke interkonekcije po regionima sveta u 2000. godini

Kontinent	Broj IX-ova	Naziv, lokacija i broj povezanih ISP-ova
Afrika	2	Kejptaun – 11
Azija i Bliski istok	40	HKIX Hong Kong – 49, JPIX Tokio – 36, iIX-JKTIX Džakarta – 35, L2IX Seul – 32, THIX Bangkok – 27
Evropa	78	LINX London – 82, AMS-IX Amsterdam – 71, M9-IX Moskva – 54, DeCIX Frakfurt – 51, SFINX Pariz – 47, VIX Beč – 43, BNIX Brisel – 30
Latinska Amerika	5	Interet NAP Bogota – 12, Chile NAP Santijago – 9
S.Amerika – Kanda	5	TorIX Toronto – 11
S.Amerika – SAD	94	MAE-East Vašington DC – 116, NAP Čikago – 93, MAE-West San Hoze – 83, PAIX Palo Alto – 80, NAP Njujork (Nju Džersi) – 32

Preuzeto iz Edwarad J. Malecki "The Economic Geography of the Internet's Infrastructure" in *Economic Geography* Vol. 78, No 4, October 2002, pp. 399-424. str. 415.

Ono na što Malecki opravdano skreće pažnju je i da širokopojasne veze nisu jedini indikator pojave interneta u prostornoj ekonomiji, već su to i imena internet domena. Postoji uočeni obrazac da je gustina domena veća u većim gradovima, što se objašnjava ne samo brojem stanovnika, nego i prihodom, obrazovanjem itd.

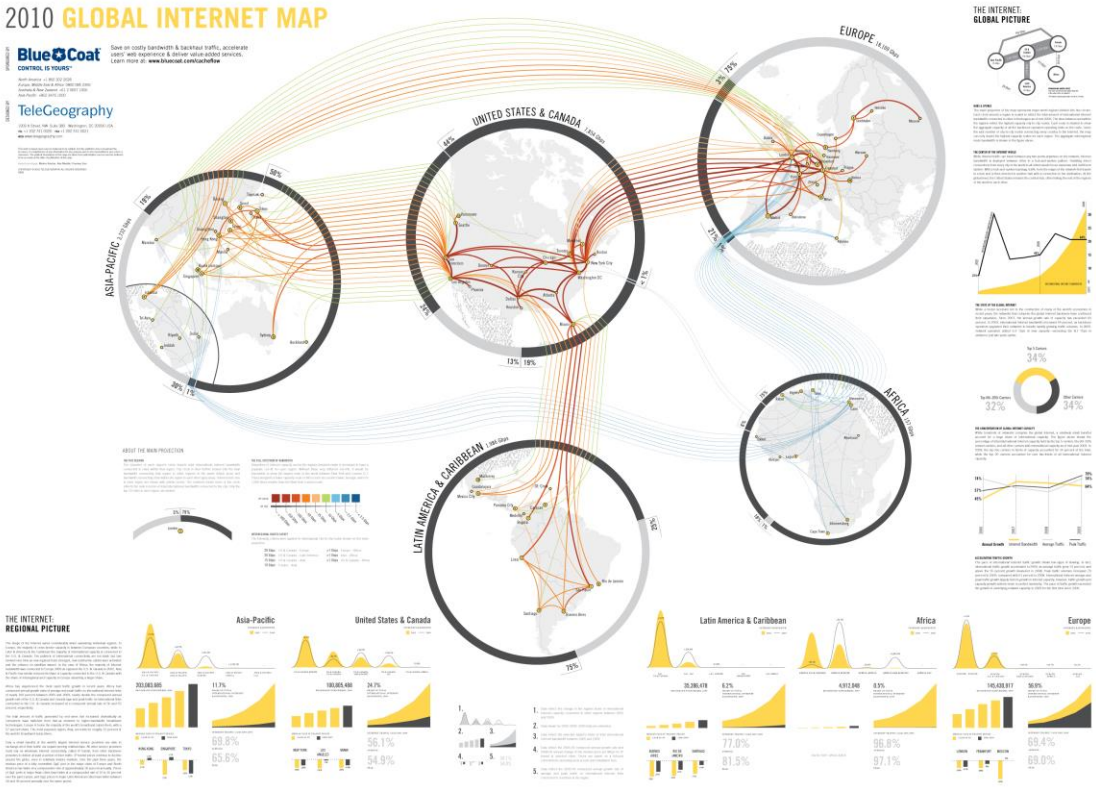
Inače, iz ovog rada Maleckog je kompletno izostavljeno prostorno prikazivanje interneta iz ugla proizvođača internet sadržaja, tj. sedišta kompanija koje se time bave, jer u vremenu obuhvaćenim radom, 2000. godine, ove kompanije još uvek nisu raspolagale upadljivim uticajem. Kada se danas, 2016. godine, prostorno vizuelizuje internet, taj segment se navodi jer ima eksplanatornu vrednost širu od one vezane za brzine i obrasce povezivanja mreže.

U zaključku Malecki podvlači da je evoluirajuća mreža mreža još jednom osnažila urbanu hijerarhiju. Iako neki vide sveprisutnost komunikacija kao spas za ruralne i udaljene oblasti, „rast novih tehnologija 'ne rezultira automatski u decentralizaciji ekonomske aktivnosti'. Urbane aglomeracije ostaju bolje povezane sa tržištima i komptetitivnim inovacijama u proizvodima i uslugama.“[262]

Mape interneta

Internet se u materijalno prostornom obliku prikazuje ili mapira na različite načine. Tako na primer uticajna firmaTeleGeography prikazuje internet na konvencionalnim geografskim mapama preko kojih su ucrtane linije koje označavaju okosnicu interneta tj. kapacitete veza između najvećih svetskih ISP-ova. Primeri mapa se nalaze ovde.

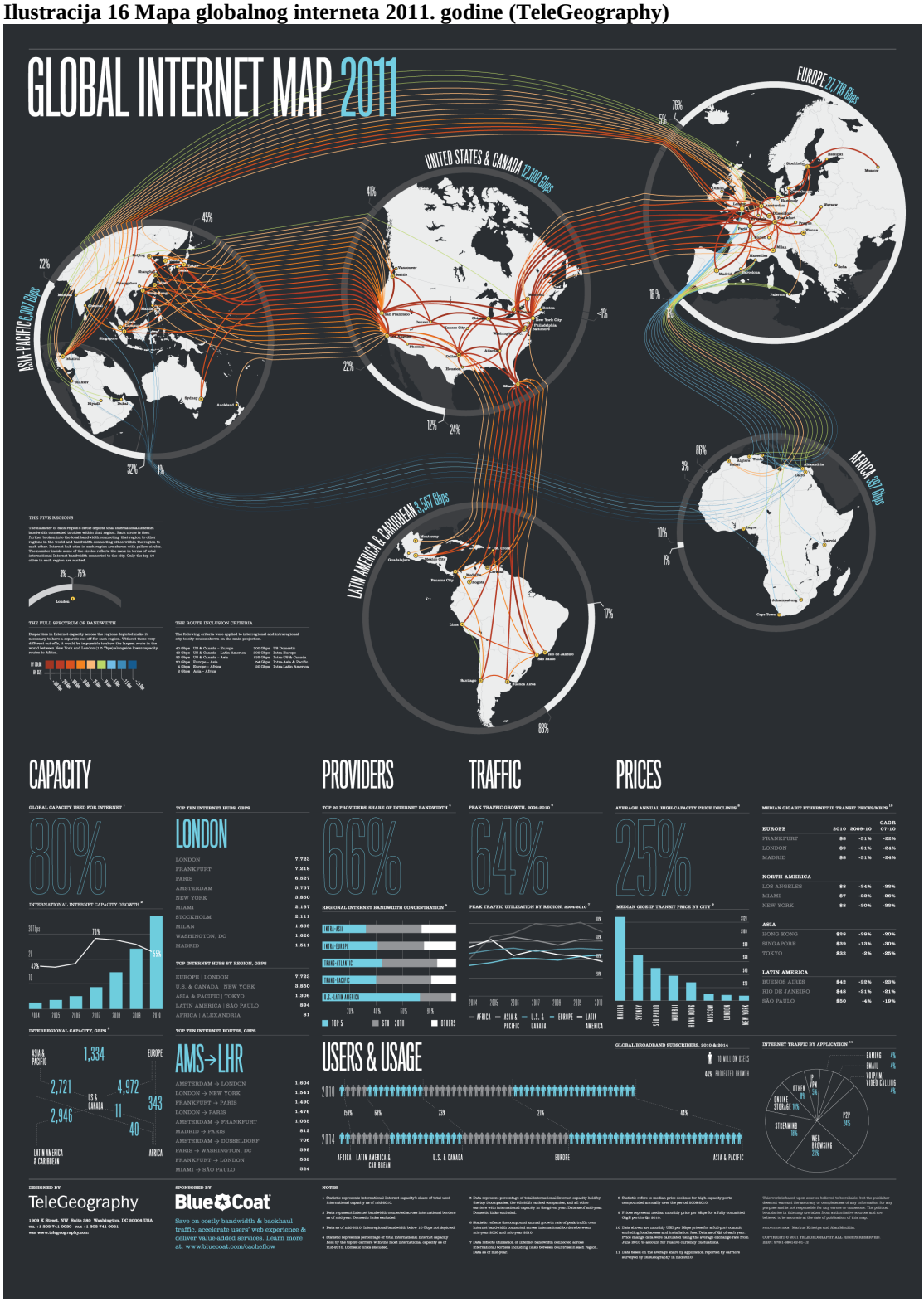
Ilustracija 15 Mapa globalnog interneta 2010. godine (TeleGeography)



Preuzeto sa: https://www.telegeography.com/telecom-resources/map-gallery/global-internet-map-2010/index.html

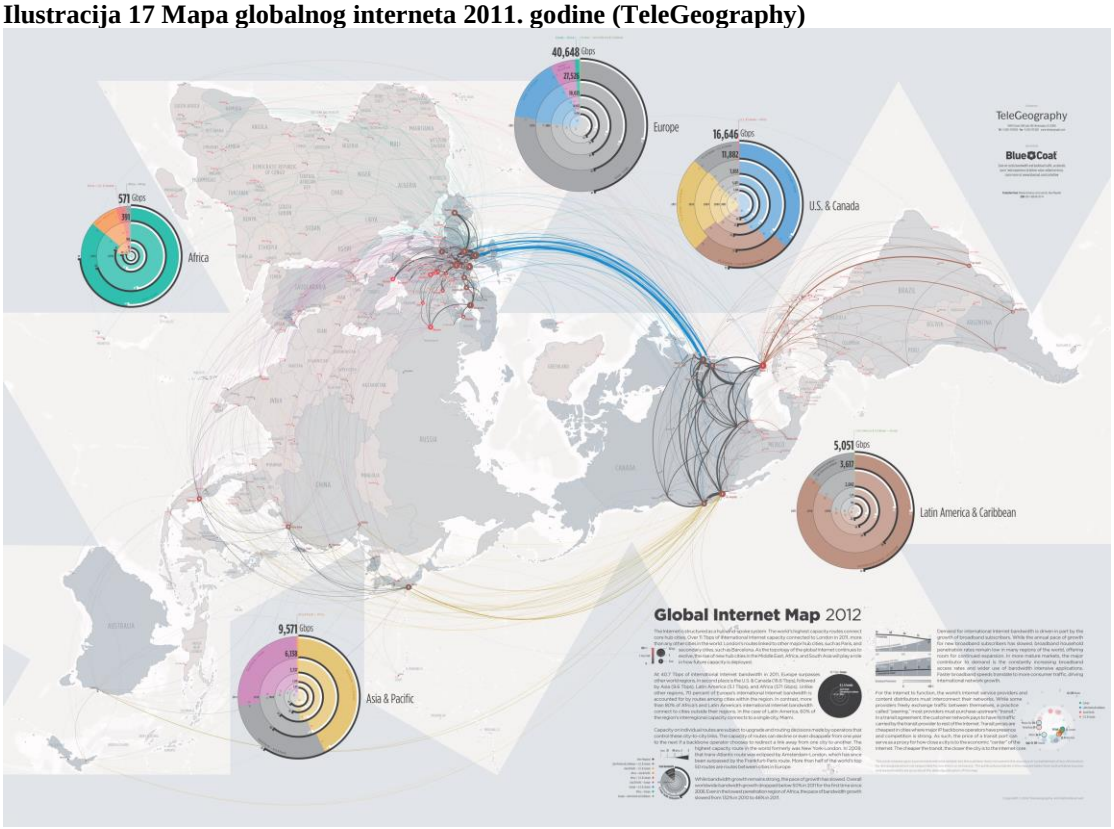
[262] Ibid. str. 419.

Ilustracija 16 Mapa globalnog interneta 2011. godine (TeleGeography)



Preuzeto sa: https://www.telegeography.com/telecom-resources/map-gallery/global-internet-map-2011/index.html

Ilustracija 17 Mapa globalnog interneta 2011. godine (TeleGeography)



Preuzeto sa: https://www.telegeography.com/telecom-resources/map-gallery/global-internet-map-2012/index.html

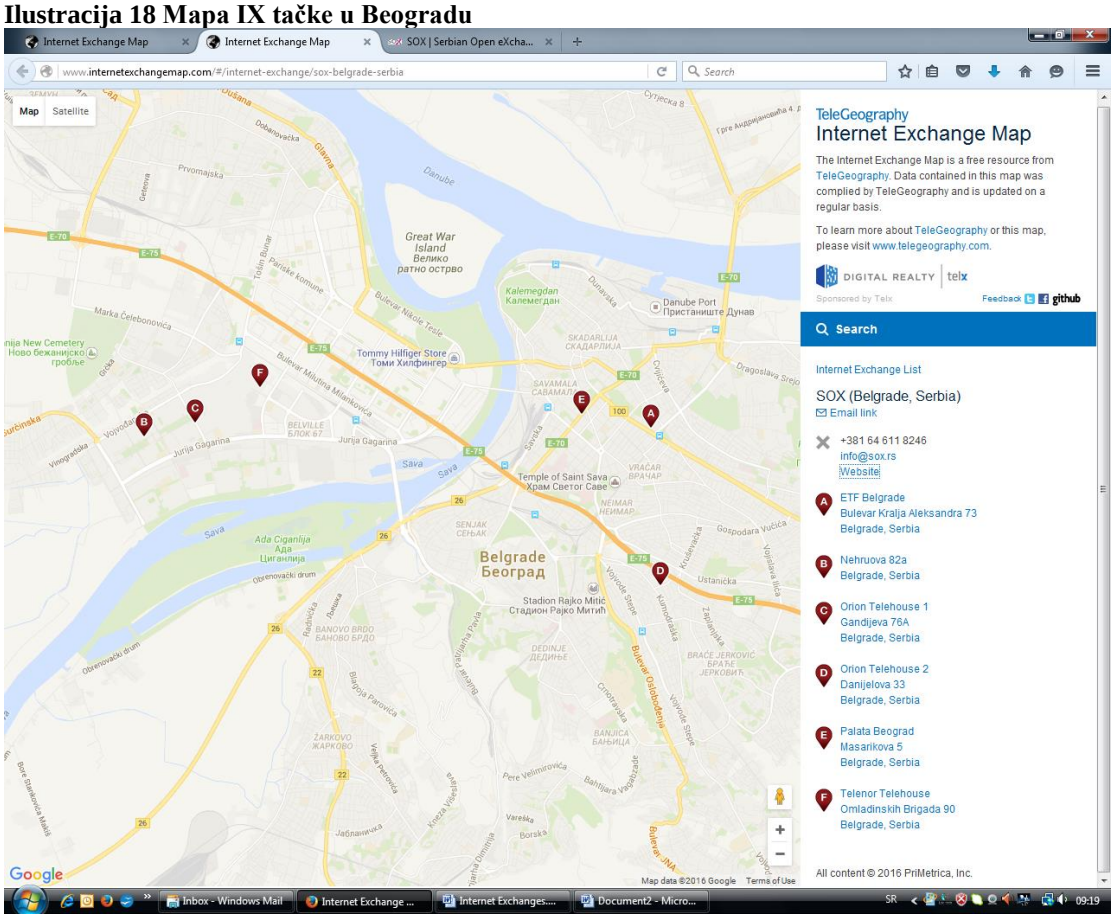
TeleGeography daje i mapu (kao i ažurirani potpuni popis) svih IX tačaka na svetu. Ilustracija ove mape (evropski i pacifički ugao) nalazi na kraju rada kao Prilog 1. Na ovom mestu donosimo i TeleGeography prikaz IX tačke u Beogradu, koja se naziva SOX.rs.

Serbian Open eXchange (SOX.rs) sprovodi otvorenu politiku pristupa. Potencijalni korisnik koji poseduje sopstveni AS broj i ruter sa odgovarajućim karakteristikama, može postati korisnik SOX usluga, na potpuno otvoren i nediskriminatorski način. SOX koristi BGP community mehanizam koji daje potpunu kontrolu nad oglašavanjima IPv4 & IPv6 adresnog prostora jednog korisnika, ka drugim korisnicima. Neki od ISP-ova koji koriste SOX.rs su: Telekom Srbija, SBB, Orion Telekom, Telenor Srbija, VIP Mobile, Gama Electronics, YUnet, Verat, Beotel, Radijus Vektor, Sattrakt, AVCom, IKOM, Targo Telekom, Mainstream, Registar nacionalnog internet domena RNIDS, Elektrotehnički fakultet i drugi.

Septembra 2013. godine SOX.rs je u saradnji sa ICANN izvršio poboljšanje internet infrastrukture u cilju povećanja otpornosti na potencijalne zloupotrebe ili napade

DNS-a. SOX.rs je instaliro novu DNS Anycast kopiju ICANN-ovog rut servera L na jednoj od 6 glavnih lokacija u Beogradu. Time je smanjeno vreme odgovora (povećana brzina rutiranja) u Srbiji i regionu. SOX-ova operatorska kupa se širi preko 6 zemalja Južne Evrope, i odgovara za preko 50 miliona krajnjih korisnika interneta.

Ilustracija 18 Mapa IX tačke u Beogradu

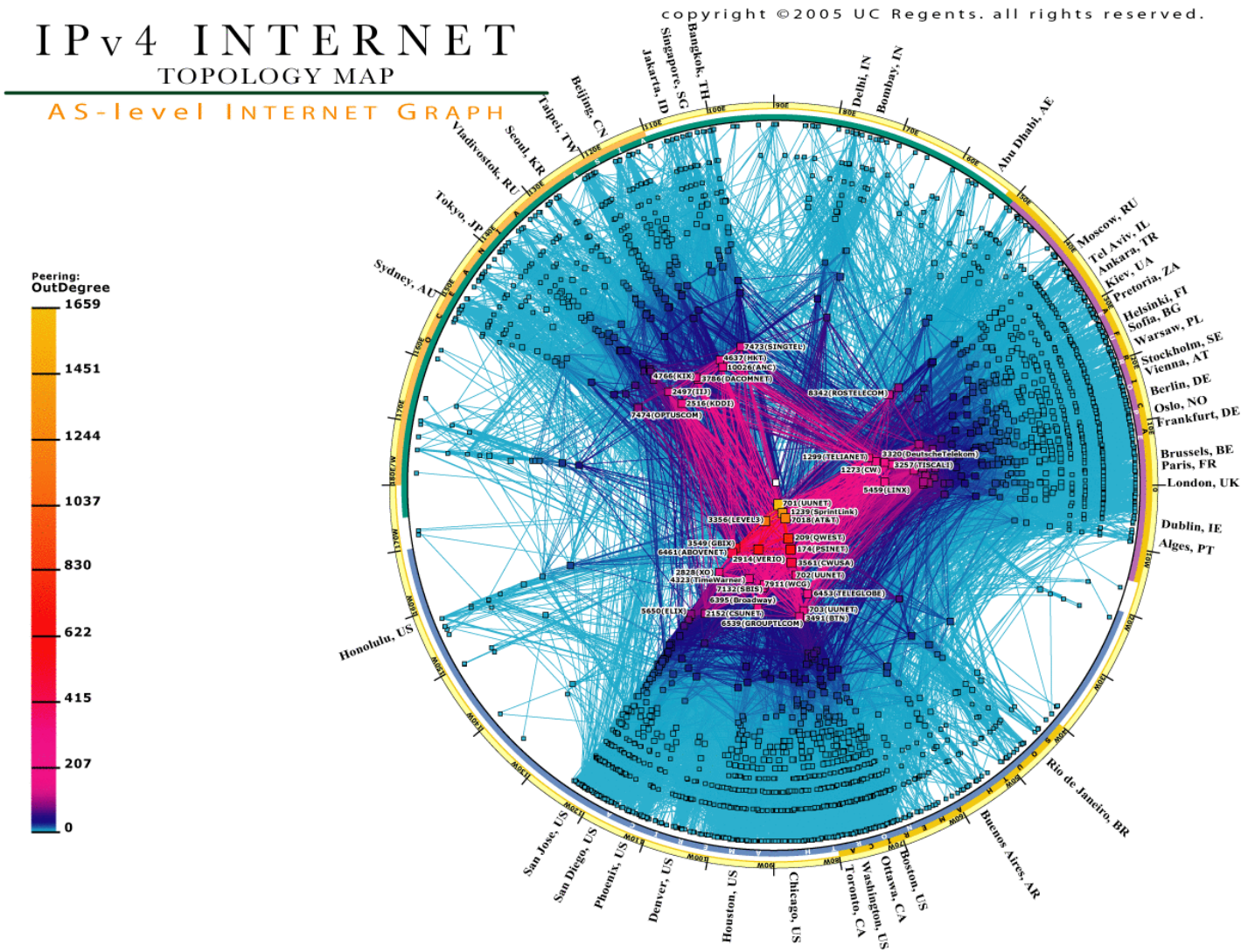


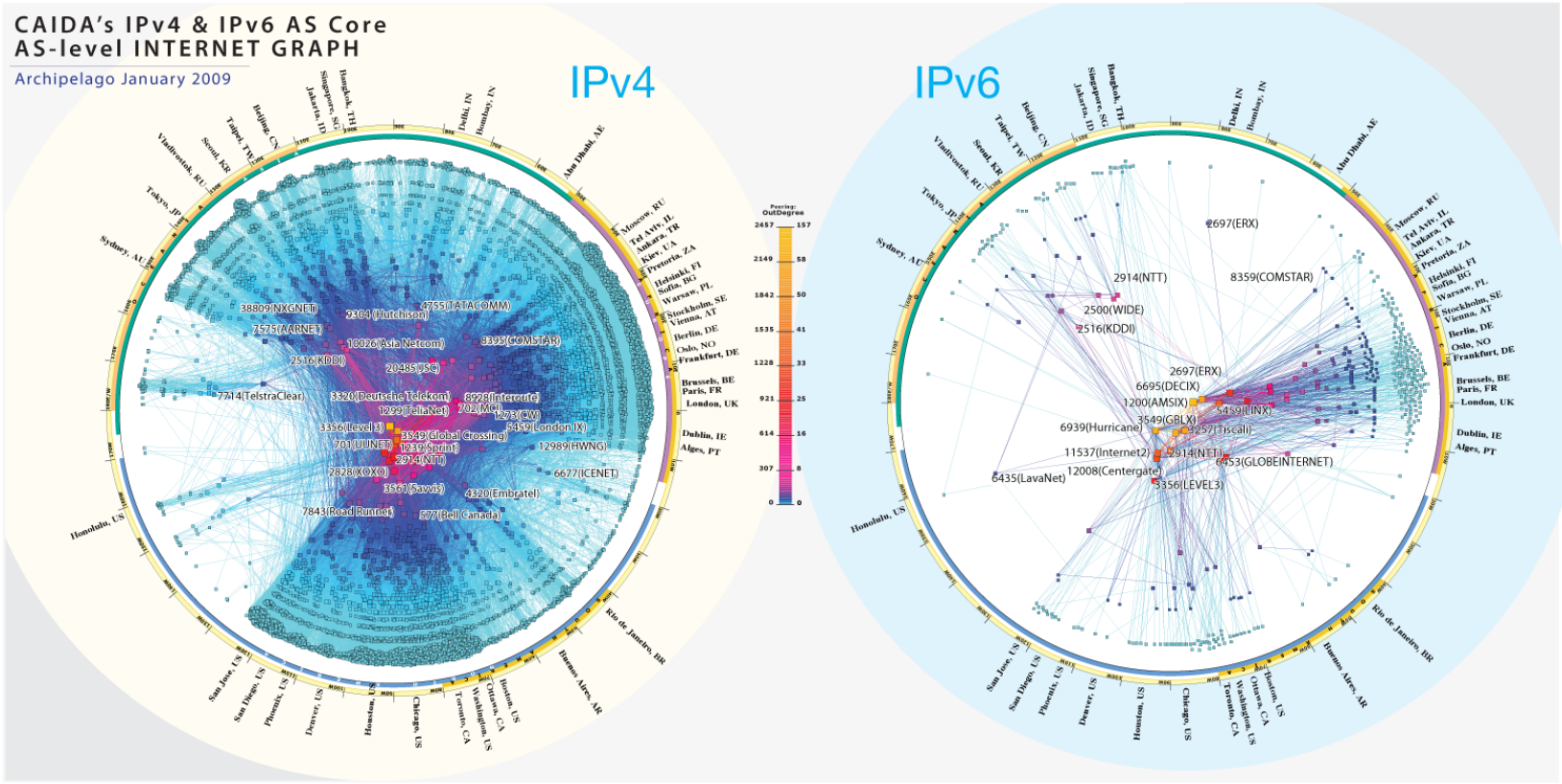
Preuzeto sa: https://www.telegeography.com/telecom-resources/internet-exchange-map/index.html

Sledeći način prikazivanja interneta koji treba imati u vidu je onaj koji radi Superkomjuterski centar Univerziteta u San Dijegu (Center for Applied Internet Data Analysis, skraćeno CAIDA). On pravi mape iz polarnog preseka u koje ucrtava autonomne sisteme tako što ugao daje po geografskoj dužini na kojoj im je sedište, a udaljenost od centra po broju autonomnih sistema sa kojima su upareni. Primeri takvih mapa se nalaze ovde.[263]

Ilustracija 19 IPv6 Internet Topology Map
Ilustracija 20 IPv4 and IPv6 AS Internet Core Map

[263] http://www.caida.org/research/topology/as_core_network/2015/


IPv4 INTERNET
TOPOLOGY MAP
AS-level INTERNET GRAPH
copyright ©2005 UC Regents. all rights reserved.
Peering:
OutDegree
1659
1451
1244
1037
830
622
415
207
0
Singapore, SG
Bangkok, TH
Jakarta, ID
Delhi, IN
Bombay, IN
Abu Dhabi, AE
Moscow, RU
Tel Aviv, IL
Ankara, TR
Kiev, UA
Pretoria, ZA
Helsinki, FI
Sofia, BG
Warsaw, PL
Stockholm, SE
Vienna, AT
Berlin, DE
Oslo, NO
Frankfurt, DE
Brussels, BE
Paris, FR
London, UK
Dublin, IE
Alges, PT
Rio de Janeiro, BR
Buenos Aires, AR
Boston, US
Ottawa, CA
Washington, US
Toronto, CA
Chicago, US
Houston, US
Denver, US
Phoenix, US
San Diego, US
San Jose, US
Honolulu, US
Sydney, AU
Tokyo, JP
Vladivostok, RU
Seoul, KR
Beijing, CN
Taipei, TW
7473(SINGTEL)
4637(HKT)
10026(ANC)
4766(KIX)
2786(DACOMNET)
2497(IIJ)
2516(KDDI)
7474(OPTUSCOM)
8342(ROSTELECOM)
1299(TELIANET)
3320(DeutscheTelekom)
3257(TISCALI)
1273(CW)
5459(LINX)
701(UUNET)
1239(SprintLink)
7018(AT&T)
3356(LEVEL3)
209(QWEST)
3549(GBIX)
6461(ABOVENET)
174(PSINET)
2914(VERIO)
3561(CWUSA)
2828(XO)
4323(TimeWarner)
702(UUNET)
7911(WCG)
7132(SBIS)
6453(TELEGLOBE)
6395(Broadway)
703(UUNET)
5650(ELIX)
2152(CSUNET)
6539(GROUPTLCOM)
3491(BTN)



ANALYSIS TEAM . Bradley Huffaker . kc claffy
SOFTWARE DEVELOPMENT Young Hyun . Matthew Luckie
POSTER DESIGN Connie Lyu

	Number of IP address	Number of IP links	Number of ASes	Number of ASlinks
IPv4	4,853,991	5,682,419	17,79	50,333
IPv6	4,752	17,036	489	1,904

ARK HOSTS . AARNet . APAN . ARIN . ASTI . CAIDA . Canarie . CENIC . CNRST . FORTH . FunkFeuer . HEANet . Iowa State University . KREONet2 . National Research Council Canada . NIC Chile . Northeastern University . Purdue University . Southern Methodist University . TWAREN . Universitat Leipzig . Universitat Politecnica de Catalunya . University of Cambridge . University of Hawaii . University of Luxembourg . University of Napoli . University of Oregon . University of Waikato . University of Zurich . US Army Research Lab . Verizon

COOPERATIVE ASSOCIATION FOR INTERNET DATA ANALYSIS
San Diego Supercomputer Center . University of California, San Diego
500 Gilman Drive, mc0505 . La Jolla, CA 92093-0505 . 858-534-5000 . http://www.caida.org/
http://www.caida.org/research/topology/as_core_network/

This visualization represents macroscopic snapshots of IPv4 and IPv6 Internet topology samples captured in January 2009. The plotting method illustrates both the extensive geographical scope as well as rich interconnectivity of nodes participating in the global Internet routing sytem.

For the IPv4 map, CAIDA collected data from 33 monitors located in 30 countries on 5 continents. Coordinated by our active measurement infrastructure, Archipelago (Ark[1]), the monitors probed paths toward 7.4 million /24 networks that cover 95% of the routable prefixes seen in the Route Views[2] Border Gateway Protocol (BGP) routing tables on 1 January 2009.

For the IPv6 map, CAIDA collected data from 6 Ark monitors located in 4 countries on 2 continents. This subset of monitors probed paths toward 1,491 prefixes which represent 88.9% of the globally routed IPv6 prefixes seen in Route Views BGP tables on 1 January 2009.

We aggregate this IP-level data to construct IPv4 and IPv6 Internet connectivity graphs at the Autonomous System (AS) level. Each AS approximately corresponds to an Internet Service Provider (ISP). We map each observed IP address to the AS responsible for routing traffic to it, i.e., to the origin (end-of-path) AS for the IP prefix representing the best match of this address in the BGP routing tables. For the IPv4 graph, we used the BGP IPv4 routing table provided by Route Views. For the IPv6 graph, we used the IPv6 routing table collected by RIPE NCC[3].

$$\text{radius} = 1 - \log\left(\frac{\text{outdegree(AS)} + 1}{\text{maximum outdegree} + 1}\right)$$

$$\text{angle} = \left(\frac{\text{longitude of the AS's BGP prefixes}}{\text{in netacq}}\right)$$

The position of each AS node is plotted in polar coordinates (radius, angle), that are calculated as follows.

The outdegree of an AS node is the number of next-hop ASes that we observed accepting our probe traffic as it left this AS. The link color reflects outdegree value, from lowest (blue) to highest (yellow). Toward the center of the graph we have manually labeled some of the highest outdegree ASes with their associated ISPs.

To determine the longitude of an AS, we used the IPv4 BGP table from Route Views to find a set of announced IPv4 prefixes for each AS. We subdivided prefixes into the smallest prefixes that Digital Envoy's NetAcuity[4] mapped to a single geographic location in January 2009. We then calculated the AS angle coordinate from the weighted average (by number of IP addresses in each mapped prefix) of the longitude coordinates of all such subdivided prefixes. NetAcuity currently only supports IPv4 mapping, so we use the IPv4-derived locations for ASes in both graphs.

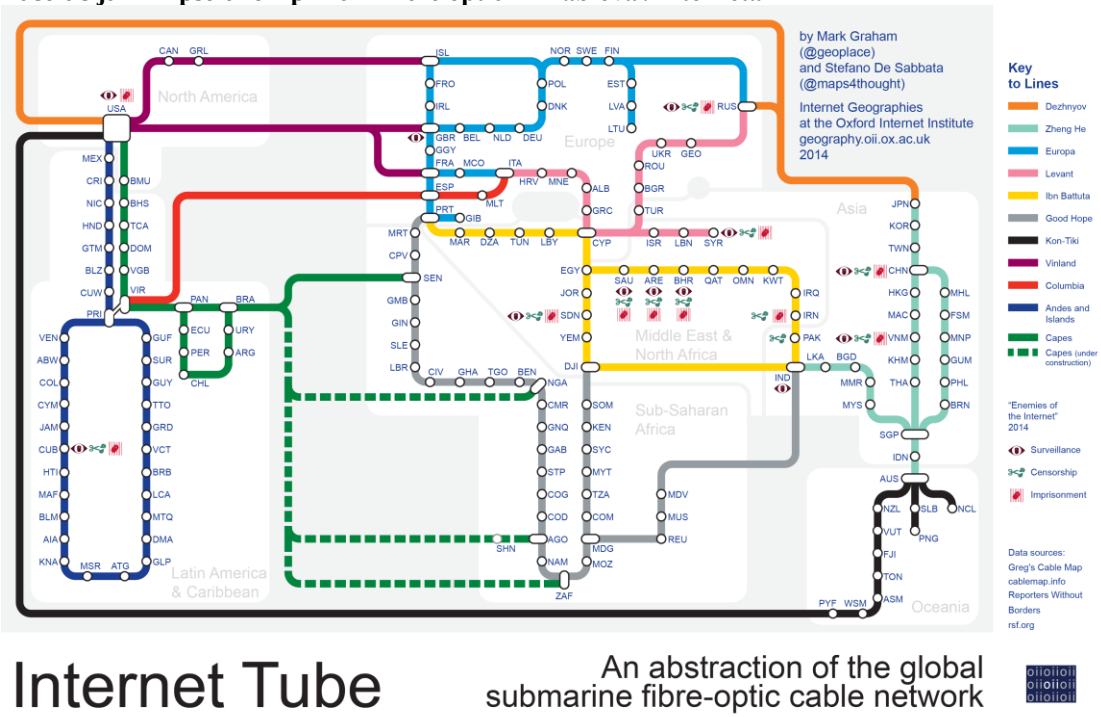
Calculating AS coordinates as described above results in a large number of overlapping nodes (hundreds in the case of the IPv4 graph) which distort the graph's edge. To better visualize so many ASes at the edge, we refined our node placement algorithm to spread out overlapping nodes. This modification creates bulges in the outermost ring of the AS-core, corresponding to longitudes with substantial Internet infrastructure deployment, which also correlates with populous regions of the globe.

The IPv6 graph grew from 486 AS nodes in January 2008 to 515 nodes in January 2009. Over the same period we saw an increase in the number of IPv4 ASes from 18K to almost 23K. Whether these changes represent actual new AS allocations or result from modifications in our measurement methodology is not clear. Compared with the AS-core graph of January 2008, we observed a westward shift in the position of ISP TelstraClear due to its increased presence (per NetAcuity's mapping) in Australia.

[1] Ark http://www.caida.org/projects/ark/
[2] Route Views http://www.routeviews.org/logo.png
[3] RIPE NCC http://www.ripe.net/
[4] digital envoy http://www.digitalenvoy.net/

Treći način prikazivanja interneta imamo kod Oksfordskog internet instituta, koji je, na primer, mrežu podmorskih optičkih kablova (veoma bitnu u okosnici interneta) složio u mapu koja veoma liči na čuvenu popularnu mapu linja podzemne železnice u Londonu. Ta dosta originalna mapa interneta se nalazi ovde.

Ilustracija 21 Apstraktni prikaz mreže optičkih kablova / interneta



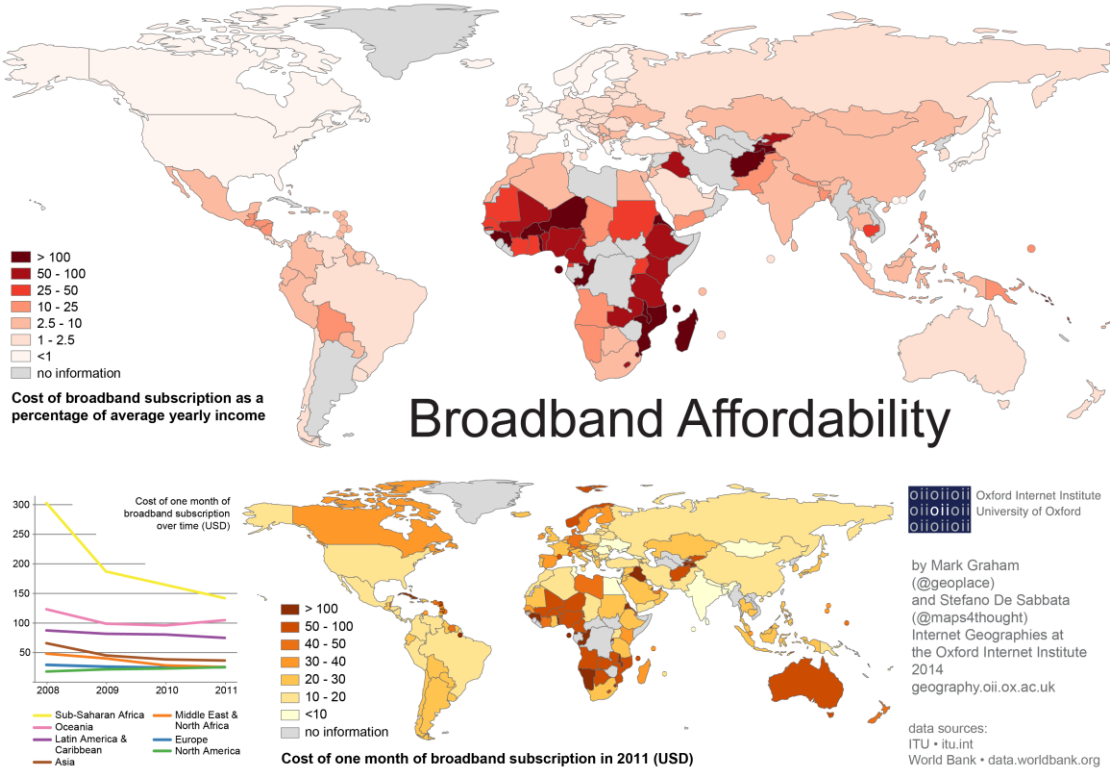
Preuzeto sa http://geography.oii.ox.ac.uk/?page=internet-tube

Ono što nam ova mapa pokazuje je da su SAD najpovezanija zemlja u svetu, sa podmorskim kablovima koji izlaze na obe njene obale. Druga najpovezanja u globalnom smislu je Velika Britanija a treća Senegal. Na mapu je stavljen i deo kablova koji idu ka Nigeriji i Južnoj Africi (WASACE kabl, SACS kable) a koji su u izgradnji. Ovde donosimo još neke mape Oksfordskog internet instituta, koje daju uvid u infrastrukturu interneta.

Obavezno treba obratiti pažnju na mapu cenovne dostupnosti interneta (širokopojasne veze) u svetu. Ova mapa se naziva još i mapa digitalne podele sveta. Iz nje je jasno da je cena priključka na internet u Africi van domašaja prosečnog stanovnika. Postoje zemlje Podsaharske afrike, gde je cena priključka na širokopojasni internet veća od prosečnog prihoda stanovnika, a visoke cene u odnosu na prihode stanovništva su u

Afganistanu i Tažikistanu, Kubi i Solomonovim ostrvima. U apsolutnim iznosima, najjeftiniji priključak je u Indiji i Šri Lanci, a najskuplji u Evropi i Severnoj Americi.

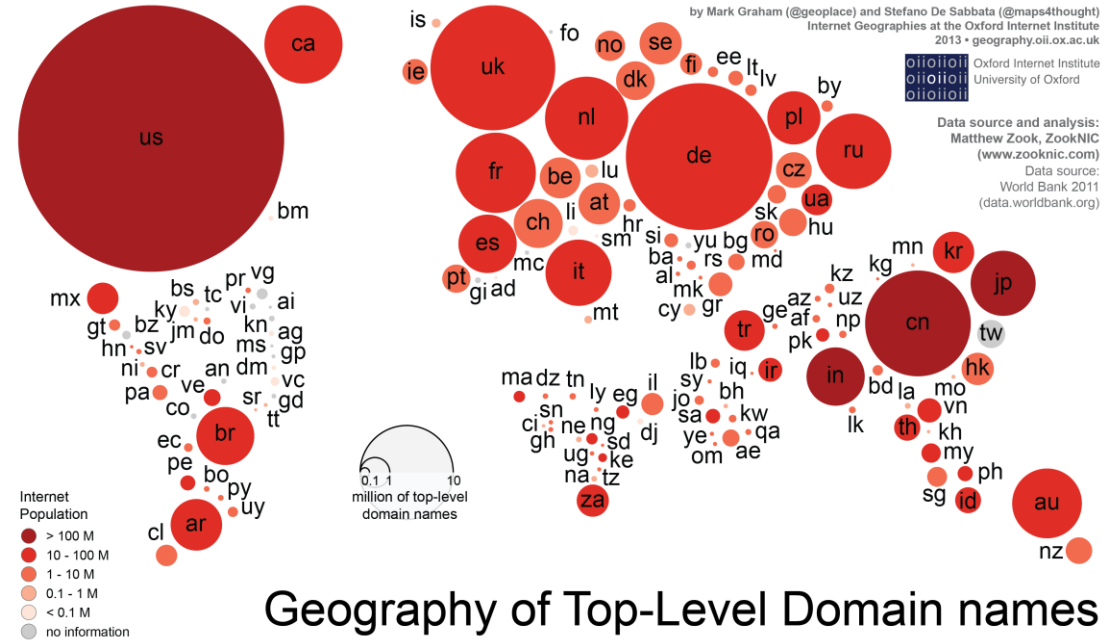
Ilustracija 22 Mapa dostupnosti interneta



Preuzeto sa http://geography.oii.ox.ac.uk/?page=broadband-affordability

Takođe donosimo i mapu brojnosti internet domena po zemljama. Mapa internet domena pokazuje da je 78% domena registrovano u Evropi i Severnoj Americi, dok je u Aziji 13%, Latinskoj Americi 4%, Okeaniji 3% i zajedno na Bliskom istoku i u Africi samo 2% udela u svetskim internet domenima. Imena domena su povezana sa proizvodnjom internet sadržaja. Uobičajeno je da korisnici interneta u Evropi i Severnoj Americi registruju domen i imaju veb stranicu, dok je to retkost u ostatku sveta. Posebno u Kini se vidi da ima manje domena nego u Velikoj Britaniji pri čemu Kina ima deset puta veću intenet populaciju od Velike Britanije. Brojčanost internet populacije ne garantuje njenu aktivnost na internetu. „Zanimljivo je da postoji značajna pozitivna korelacija između rangiranja zemlje prema GNI per capita pokazatelju i broja imena domena po korisniku interneta. Rangiranje zemlje prema GNI per capita pokazatelju objašnjava oko 50% varijanse u rangiranju po broju imena domena po internet korisniku.“

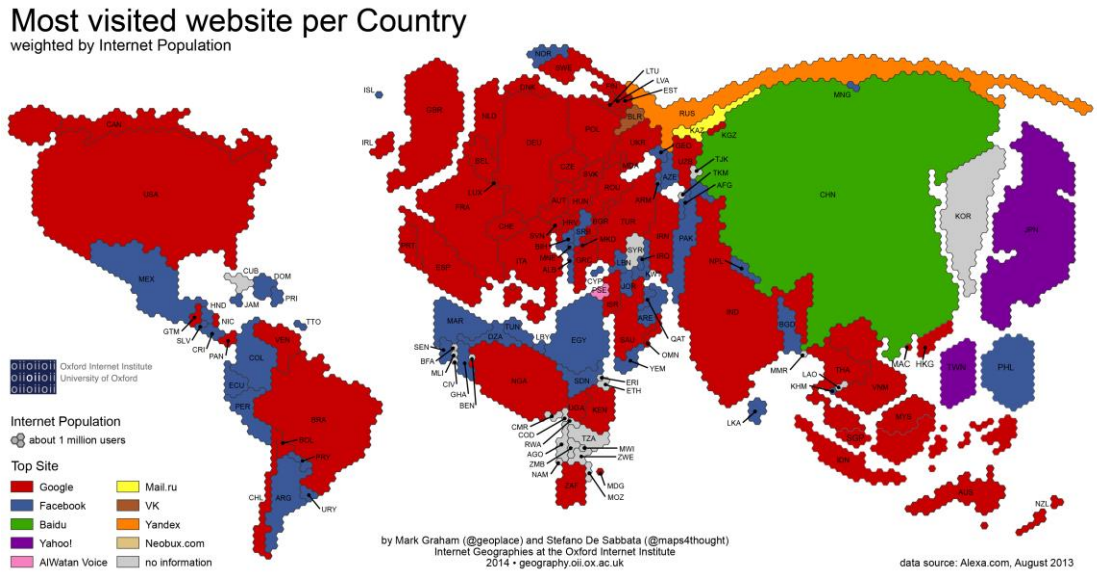
Ilustracija 23 Mapa distribucije primarnih internet domena po zemljama



Preuzeto sa http://geography.oii.ox.ac.uk/?page=geography-of-top-level-domain-names

Prethodnu mapu dobro je uporediti sledećom - mapom najuticajnijih internet imperija (vodećih kompanija) po zemljama. Iz toga vidimo da su pojedini internet domeni uticajni daleko van svoje zemlje registracije.

Ilustracija 24 Mapa najposećenijih internet sajtova po zemljama

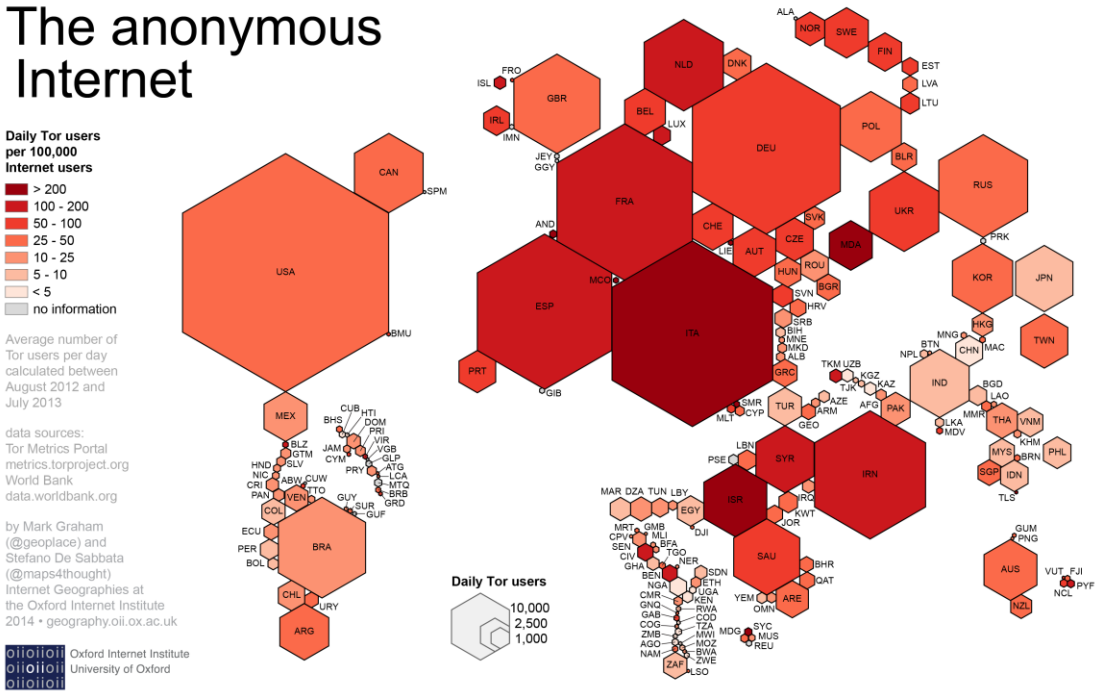


Preuzeto sa http://geography.oii.ox.ac.uk/?page=age-of-internet-empires

Prikaz ćemo završiti mapom anonimnosti na internetu. Ova koju prenosimo potiče iz perioda 2012/13 i bazirana je na podacima samog TOR sistema. Tada je bilo preko

5.000 čvorova u mreži, i preko 750.000 korisnika je dnevno dolazilo u sistem. Najveći broj korisnika TOR-a je dolazio iz Evrope, a posebno iz Italije (oko 76.000 korisnika dnevno). Disproporcionalno veliki broj korisnika TOR-a u odnosu na ukupno stanovništvo registruje se kod San Marina, Monaka, Andore, Lithenštajna, ali i Moldavije. Drugi region po broju korisnika TOR-a je Bliski istok i Severna Afrika, posebno zemlje kao što je Iran, Izrael itd.

Ilustracija 25 Mapa distribucije anonimnosti na internetu po zemljama



Preuzeto sa http://geography.oii.ox.ac.uk/?page=tor

Sajber spejs

Bez obzira što je materijalno prostorni oblik interneta proučen i dostupni su njegovi odgovarajući vizuelni prikazi, i dalje nastavlja da se koristi jedna prostorna metafora – sajber prostor ili sajber spejs. Ova metafora nije uvek bila shvatana kao metafora, određeni broj ljudi tokom 1990-tih je u nju i bukvalno verovao. Tome je Mark Graham sa Univerziteta Oksford posvetio pomalo ciničan tekst pod nazivom „Geografija/Internet: eterične alternativne dimenzije sajber spejsa ili prizemljene

uvećane stvarnosti?“[264] On smatra da „mnogi načini na koje diskutujemo, zamišljamo i pristupamo internetu zavise od netačnih i nekorisnih prostornih metafora“[265], pod kojima pre svega misli na metaforu sajber spejsa.[266] Ova metafora je loša jer nam prikriva mnoge obrasce i prakse koje se vrše i nastaju kroz interakciju između informaciono-komunikacionih tehnologija i društva, interakciju između ljudi, informacija, protokola (koda) i mašina kroz digitalne mreže.

Graham uočava da se ovom metaforom koriste savremeni političari i kreatori politika. Kao primere navodi[267] izjavu predsednika SAD Baraka Obame iz 2009. godine „Sajber spejs je stvaran.“ i Londonsku konferenciju o sajber spejsu u organizaciji Vilijema Hejga (Wiliam Hague) i Ministarstva spoljnih poslova Velike Britanije iz 2011. godine, gde je britanski premijer Dejvid Kameron izjavio da „ne smemo ostaviti sajber spejs otvorenim za kriminalce“, ruski ministar izjavo da „internet treba da bude nateran da poštuje granice i državnu suverenost“, a Karl Bilt, bivši švedski premijer, izjavio da treba doneti svetlo čak i u najskrivenije uglove interneta tako što „više neće biti mračnih prostora za mračna dela“. Graham dalje navodi da u mnogim državama postoje ne samo politike i zakoni nego i formirani državni organi koji sadrže reč sajber u svom nazivu. Čuveni primer je deo vojnog establišmenta SAD-a - Sajber komanda, ili disciplina na pravnim fakultetima - sajber pravo. Ovde ipak moramo pohvaliti Republiku Srbiju koja, verovatno ne iz razloga upućenosti u oblast proučavanja interneta već iz razloga očuvanja 'čistote' srpskog jezika, ne koristi reč sajber u nazivima zakona, državnih tela i sl. nego je prednost data rečima „visokotehnološki“ kriminal ili ministarstvo/uprava/agenda za „informaciono društvo“. Graham veruje da se političari i kreatori politika teže odvajaju od metafore sajberspejsa jer su „*prirodno* zabrinuti zbog neregulisanih aktivnosti koje je teško geografski negde smestiti (italik aut.)“[268] pa im je lakše da ih smeste „tamo negde“ (na primer gore citirani „mračni ćoškovi interneta“).

---

[264] Mark Graham „Geography/Internet: Ethereal Alternate Dimensions of Cyberspace or Grounded Augmented Realities?“ *The Geographical Journal* 179(2) 177-182. Dostupno na http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2166874 (U toj verziji, korišćenoj ovde, paginacija 1-14)

[265] Ibid. str. 2.

[266] Reč sajber spejs je skovao Vilijam Gibson 1984. god. a dodatno naglasio Džon Peri Barlou u svojoj „Deklaraciji nezavisnosti sajber spejsa“ iz 1996. god. Ibid. str. 4-5. Internet je preuzeo „ontičku ulogu“, čemu je doprineo i sam engleski jezik u delu stavljanja gramatičkih predloga ispred imenice koji asociraju na neku prostornost („na internet/u“).

[267] Ibid. str. 2-3.

[268] Ibid. str. 8.

Obični korisnici interneta u 2015. godini su svesni načina na koje se internet ukorenjuje u svakodnevni život, no Graham želi da kritikuje njihove preteče. Ti preteče (ili mi sami pre 20 godina?) su zamišljali mrežu kao ulaz u drugu dimenziju, sa ogromnim mogućnostima za komunikaciju.

Osnovna „presuda“ koju Graham donosi za sajber spejs glasi:

> „'Sajber spejs' je ... zamišljen i kao eterična alternativna dimenzija koja je istovremeno beskonačna i sveprisutna ... i kao fiksiran u određenoj lokaciji, premda ne-materijalnoj lokaciji ... 'Sajber spejs' tada postaje 'globalno selo' Maršala Mek Luana (1962.)“.[269]

Povrh toga, on dodaje još oštrije i da je sajber spejs bio „kolektivna halucinacija interneta: bez-telesno mesto, ali svejedno mesto, paradoksalno prožeto drugačijom vrstom prostornosti koja dozvoljava globalno okupljanje čovečanstva.“[270] Ovoj tezi[271] nedostaje kvalifikovanost – za neke, nekada itd.

Kontra Grahamovoj tezi treba reći da je sajber spejs bio više od puke eterične dimenzije: u SAD-u su postojale sudske presude koje su između ostalog morale da odrede ovaj pojam da bi odlučile o primeni prava između tužitelja i tuženog. I – daleko od toga da su sajber spejs tretirale kao halucinaciju. Jedan takav sudski spor je onaj iz 2000. godine između dve internet kompanije, Ibej protiv Biders edža (eBay v. Bidder's Egde). Ukratko, radilo se o tome da je Biders edž razvio i koristio softver kojim je skupljao informacije sa internet stranice Ibej, agregirao ih u smislu cena, i plasirao na svojoj internet stranici. Ibej ga je tužio za neovlašćeni upad u pokretninu (na engl. trespass to shattels) po analogiji sa neovlašćenim upadom u nekretninu (na engl. trespass to land). Sud je presudio u korist Ibeja. Međutim, u presudi se moglo uočiti da nije jasno šta je ta pokretnina, analogna nekretnini, koja je bila meta navodnog krivičnog dela. Pravni stručnjaci su ovu situaciju analizirali kao brkanje pojmova sajber spejsa (veba) i servera.

> «Sud u jednom momentu posmatra pokretninu (server) iz virtuelne perspektive i fokusira se na njega kao na 'prostor' i 'mesto' koje krajnji korisnik posećuje i zauzima, a u drugom momentu posmatra pokretninu iz perspektive realnog prostora i fokusira se na tehničko

[269] Ibid. str. 5-6.
[270] Ibid. str. 6.
[271] „U konačnom, mesta nikada ne mogu imati ontološku sigurnost i uvek su 'trenutna, dovedena u postojanje praksama (ugrađenim, društvenim, tehničkim), uvek ponovo stvorena svaki put kad smo na njima (mestima-prim.aut.)' (Kitchin and Dodge 2007,335). Stoga, čak i ako bismo odabrali da koristimo prostornu metaforu za onlajn interakcije, singularno 'globalno selo' koje se podrazmeva u popularnim imaginacijama 'sajber spejsa' bi ostalo neprikladno kao način zamišljanja relacionih i kontingentnih načina na koje su ta mesta upriličena, praktično doživljena i dovedena u postojanje.» Ibid. str. 7.

> funkcionisanje servera i njegov kapacitet da procesuira i odgovori na upite drugih krajnjih korisnika.»[272]

Ta virtuelna perspektiva je sajber spejs perspektiva – u sajber spejsu Ibej je aukcijska kuća u koju dolaze posetioci da bi kupovali, odnosno mesto za obavljanje biznisa. Ona je kao obična nekretnina, s tim da je u virtuelnoj dimenziji. Međutim, iz ugla realnog sveta, ona je ipak (samo) internet stranica, tj. aplikacija koja se procesuira na nekom serveru, tj. kompjuterskoj mašini određenog kapaciteta i sa jasnim parametrima koji je čine da je njena svrha da interaguje sa upitima korisnika. «'Zemlja u sajber spejsu' je zapravo virtuelni konstrukt izveden iz, između ostalog, aplikacija koje rade na kompjuterima.»[273] Ako se gleda iz eksterne perspektive u odnosu na sajber spejs, ovde se radilo o tome da je kompjuter Biders edža, prikačen na «jednom kraju interneta» poslao zahtev za podacima ka kompjuteru Ibeja prikačenom «na drugom kraju interneta» i ovaj mu je odgovorio, što je događaj poput bilo koje druge komunikacije na internetu. Po tom viđenju, tu se radilo o pristupu informacijama, a ne o povredi. Sud je ipak doneo presudu na bazi metafore tj. da je sajt Ibeja analogan aukcijskoj kući u stvarnom svetu.

Ono što bi bio mudar odnos prema sajber spejsu svodi se na poentu ne da treba prestati koristi reč sajber spejs, nego da treba znati pozadinu i funkciju te reči. Reč je o metafori; metafore odražavaju, otelovljuju i reprodukuju načine razmišljanja i konceptualizovanja našeg sveta, a promenom metafore razmišljanje će se usmeriti ka drugim smerovima. Postoji mnoštvo načina za konceptualizovanje tokova informacija kroz internet. Po Grahamu treba posmatrati i analizirati „načine na koje konzumiramo, izvršavamo, komuniciramo i kreiramo preko interneta.“[274] U krajnjem, geografija interneta nam poručuje da

> „internet nije jedno apstraktno mesto ili digitalno globalno selo, nego mreža koja omogućava selektivna povezivanja između ljudi i informacija. To je mreža koju odlikuju veoma nejednake geografije i ... koja ponavlja globalne obrasce vidljivosti, reprezentacije i glasa na koje smo naviknuti u oflajn svetu.“[275]

[272] Brett M. Rischmann, (2004). “The Prospect of Reconciling Internet and Cyberspace”, *Loyola University Chicago Law Journal*, vol. 35, 205-234. Str. 225.
[273] Ibid. str. 227-228.
[274] Graham, opus cit. Str. 7.
[275] Ibid. Str. 9-10.

SEDMO POGLAVLJE

Internet u interakciji sa komercijalnom/ekonomskom sferom – početak puta

Po Kastelsu, internet je preobrazio poslovanje u istoj meri kao što je poslovanje preobrazilo internet.[276] To je bio dvosmeran odnos. Ovde nećemo detaljno razraditi kako je internet revolucionirao svetsku ekonomiju u zadnoj deceniji 20. veka, već će fokus biti na tome kako je ekonomija uticala na razvoj interneta (posebno njegove arhitekture i infrastrukture). Početak interakcije interneta sa ekonomskom sferom je bio momenat kada su izvršene privatizacija i komercijalizacija internet infrastrukture.

Komercijalizacija interneta započela je privatizacijom okosnice interneta, poznate kao NSFNET (mreža Nacionalne fondacije za nauku) koja je izvršena 1995. godine, a zatim je usledila i privatizacija DNS (sistema imena domena) 1998. godine. Privatizacija, a posebno ona okosnice interneta nije tek istorijska anegdota, pošto su njene posledice ostale trajne.

Privatizacija je uvek više politički nego ekonomski čin.[277] Privatizacija (ustupanje javne svojine privatnom sektoru) bi prema ekonomskoj nauci trebalo da ima za ciljeve: niže troškove, niže cene, više inovacija, povećano ulaganje, bolje usluge i dr. Svi ovi ciljevi se postižu konkurencijom koja mora postojati u privatnom sektoru.

U razvoju interneta krajem 1980-tih glavnu ulogu ima NSFNET, koja je povezivala oko 200 univerziteta, federalnih agencija i sl. koji su bili povezani kroz nekoliko regionalnih mreža. NSF je u to vreme imala decidiranu Politiku prihvatljivog korišćenja, koja je zabranjivala upotrebu mreže za svrhe koje nisu povezane sa istraživanjem i obrazovanjem. Međutim, uočavalo se da postoji potreba za drugim vrstama korišćenja mreže, pa je NSF ohrabrila je regionalne mreže da se okrenu i komercijalnim klijentima. Zbog toga su od dotadašnjih neprofitnih organizacija ove regionalne mreže postale profitne organizacije to jest kompanije. Logika tog poteza je bila da se prihodima od novih komercijalnih klijenata priključenih na mrežu dalje razvija mreža i da se kroz ekonomiju obima ostvare niže cene za sve korisnike.

[276] Manuel Castells. (2003). *Internet galaksija. Razmišljanje o internetu, poslovanju i društvu*. Zagreb: Naklada Jesenski i Turk. Str. 68.

[277] Jay P. Kesan and Rajiv C. Shah. (2001). "Fool Us Once Shame On You – Fool Us Twice Shame On Us: What We Can Learn From the Privatizations Of the Internet Backbone Network and the Domain Name System" *Washington University Law Quarterly* Vol. 79, 89-219. Str. 132. Dostupno na http://papers.ssrn.com/sol3/papers.cfm?abstract_id=260834 (U daljem tekstu „Privatizations")

Politika prihvatljivog korišćenja je promenjena 1992. godine tako da dozvoljava komercijalno korišćenje mreže pod uslovom da to povećava sposobnost mreže za istraživanje i obrazovanje.[278]

Početkom 1990-tih je usledio plan za redizajniranje i gašenje mreže NSF, tako da su umesto regionalnih mreža centralno mesto dobile tačke za pristup mreži (NAPs - Network Access Points), koje bi bile u javno-privatnom vlasništvu jedan određeni broj godina, a kasnije u privatnom vlasništvu. Od strane vlade je naloženo „da se regionalne mreže otkače sa okosnice mreže NSF do oktobra 1994. godine i povežu na komercijalne provajdere, koji bi bili međupovezani preko tačaka za pristup mreži (NAP-ova).“[279] Tako je i bilo. Firme koje su napravile 4 NAP-a su: Sprint u Njujorku, MFS u Vašingtonu, Ameriteh u Čikagu i Pacific Bell u Kaliforniji, dok je peta firma, MCI dobila zadatak da održava brzu vezu između NAP-ova.[280]

Neki teoretičari su mišljenja da procesi kojima je vlada SAD-a prepustila kontrolu nad internetom privatnom sektoru nisu bili najkorektniji. Ovi procesi predmet su široke kritičke analize, čak i rasprave pred kongresom. Kritike[281] koje opširno daju Kesan i Šah se u najkraćem mogu formulisati na sledeći način:

- Vlada je odlučivala netransparentno.
- Vlada je delovala bez konsultovanja javnosti.
- Vlada nije tretirala sve aktere jednako u proceduralnom smislu tj. favorizovala je pojedine aktere.

Posledice privatizacije okosnice interneta su takve da je mala grupa provajdera stavila pod trajnu kontrolu celo tržište i ograničila konkurenciju, ali nije jasno da li je vlada kao cilj privatizacije imala takvo stvaranje monopola/oligopola, odnosno zbog čega nije ojačala konkurenciju. Kesan i Šah prenose ocenu da je: „Vlada tretirala privatizaciju kao cilj po sebi a ne kao sredstvo da se ostvari poželjna javna svrha olakšavanja konkurencije na tržištu. Kao rezultat toga, korisnici su prisiljeni da plaćaju više cene za usluge ...“[282] Ključno pitanje koje je ostalo nerešeno tokom privatizacije je pitanje interkonekcija provajdera u NAP-ovima ili drugde. Vlada nikada nije donela politiku interkonekcije, tražeći na primer da interkonekcija između

[278] Ibid. Str. 113.
[279] Ibid. str. 115.
[280] Ibid. str. 119. Takođe se može dodati i da su Sprint, U.S.West, MCI i NYNEX evidentirani dve godine ranije kao donatori Demokatske stranke u SAD-u koja je pobedila na izborima 1992. godine.
[281] Ibid. str. 94.
[282] Ibid. str. 97.

provajdera mora biti ne-diskriminativna, već je to ostavljeno na volju samih aktera. Njihova volja je, ekonomski i iz ugla profita sasvim logično, bila da stvore oligopolno tržište i da ne dozvole ulazak na tržište manjih igrača. „Nije moralo biti tako. Tržišna dominacija je bila jasno predvidljiva i ona je posledica vladinog oslanjanja na promenu tehnološke infrastrukture bez obaziranja na to što nedostaje politika interkonekcije.“[283]

Slična situacija se ponovila i sa privatizacijom DNS-a. Tu je jedna kompanija, Network Solutions Inc. (skraćeno NSI) dobila ugovor sa vladom da održava glavni rut server, a potom joj je izmenjen ugovor i bilo odobreno da naplaćuje registraciju imena domena (gde je spadao i domen .com), pri čemu je cena godišnje registracije domena bila 50 dolara. Pojedini teoretičari ovo u šali nazivaju „džek pot promena ugovora“.[284] Sem toga, ugovor sa ovom firmom je nakon isteka prvog roka i produžen, a upućeni kažu: „Ministarstvo trgovine je produžilo ugovor sa NSI a da nije ni razmotrilo bilo koju drugu firmu koja bi mogla voditi taj registar.“[285] Ugledni internet pionir Jon Postel je još 1995. godine sugerisao da treba stvoriti bar 50 novih registratora koji bi delovali kao konkurencija NSI, ali to nikada nije uvaženo, a cena registracije domena je ostala ista. Kompanija NSI se jako brzo obogatila i već 1999. godine ušla na listu 500 najbogatijih (Fortune 500), a 2000. godine je telekomunikaciona kompanija VeriSign dala ponudu da otkupi NSI koja je iznosila 21 milijardu USD. Pošto je ponuda prihvaćena, može se reći da je bila realna. Od tada pa sve do danas, VeriSign upravlja registrom .com domena.

Ova dva primera privatizacije ključnih internet resursa ukazuju da interes javnosti nije došao u prvi plan kada se odigrala promena finansiranja infrastrukture interneta. Presudni značaj imali su strateški i političko-ekonomski razlozi. Došla je do izražaja ekonomska filozofija liberalizma, ali s tim da se umesto implusa ka konkurenciji uputio implus ka oligopolu/monopolu. Vlada SAD-a, koja je dugi niz godina finansirala ovu infrastrukturu, prepustila je da dalje finansiranje preuzme na sebe privatni biznis, a privatni biznis je to uradio jer je bilo očigledno da će i obični korisnici interneta biti spremni da plaćaju internet usluge, gde će se otvarati i prostor

[283] Ibid. str. 156.
[284] Ibid. str. 182. U prvoj godini registrovanja domena, kompanija NSI je imala preko milion registracija, pri čemu je godišnja cena bila 50 USD. Operativni trošovi kompanije bili su minimalni, pošto je 90% transakcija vršeno automatski.
[285] Ibid. Str. 186.

za profit privatnog biznisa. Veličinu profita pak presudno je odredio oligopolni/monopolski položaj nekoliko kompanija.

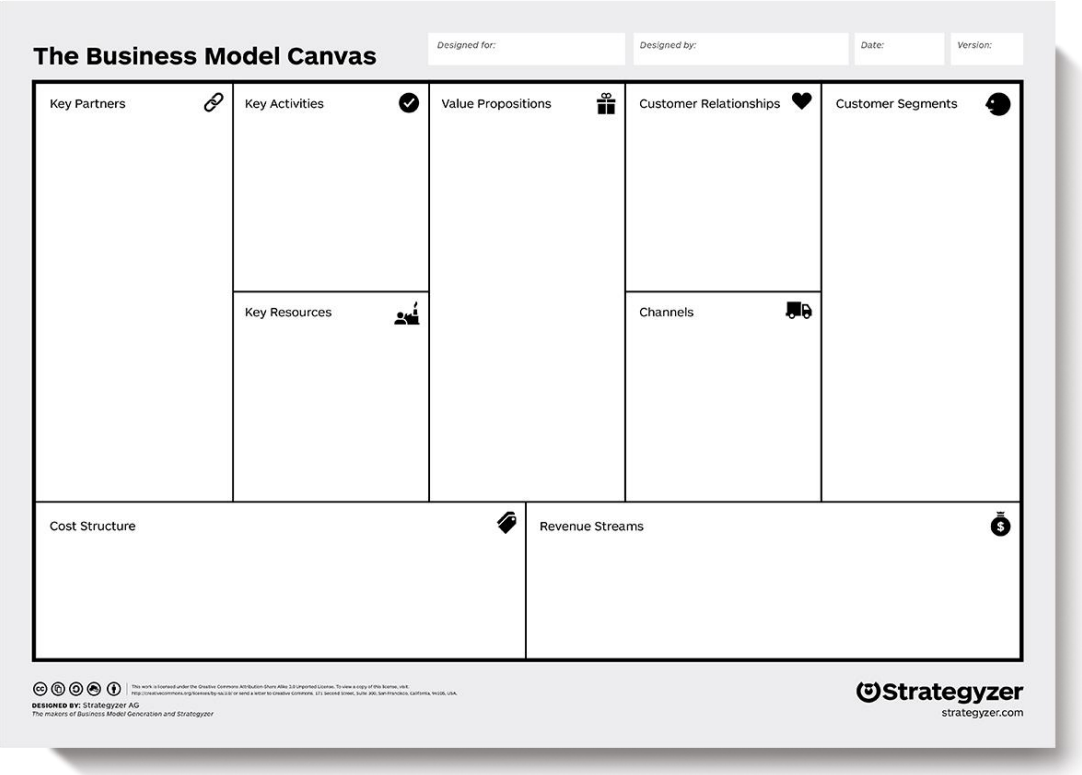
Dot.com (internet kompanije)

Za razvoj interneta se vezuje uspon nove vrste kompanija tzv. internet kompanija ili dot.com-a. Zapravo, vezuje se i propast jednog broja njih takođe. Sam naziv dolazi od imena primarnog internet domena .com. Sve kompanije o kojima se radi su imale domen, najčešće upravo .com. Domen odnosno prisustvo na internetu je bila njihova glavna filozofija. Time se sugeriše da je upravo internet imao presudnu ulogu u čitavom poslovanju tj. poslovnom planu takve kompanije. Geografski posmatrano, radi se o kompanijama i preduzetnicima iz Silikonske doline, dela San Franciska (SAD) u drugoj polovini 90-tih godina prošlog veka.

Uspon dot.com-a je imao neku vrstu šematskog toka. Krenuo bi tako što bi budući preduzetnici imali neku inovativnu ideju, koja se bazirala na povezivanju nekih proizvoda ili usluga sa internetom, odnosno na korišćenju interneta na neki do tada neviđen način. Uz to, odmah su tražili odgovor kako da se ta ideja prevede u poslovni plan,[286] što podrazumeva detaljno objašnjenje kako nameravano poslovanje dovodi do

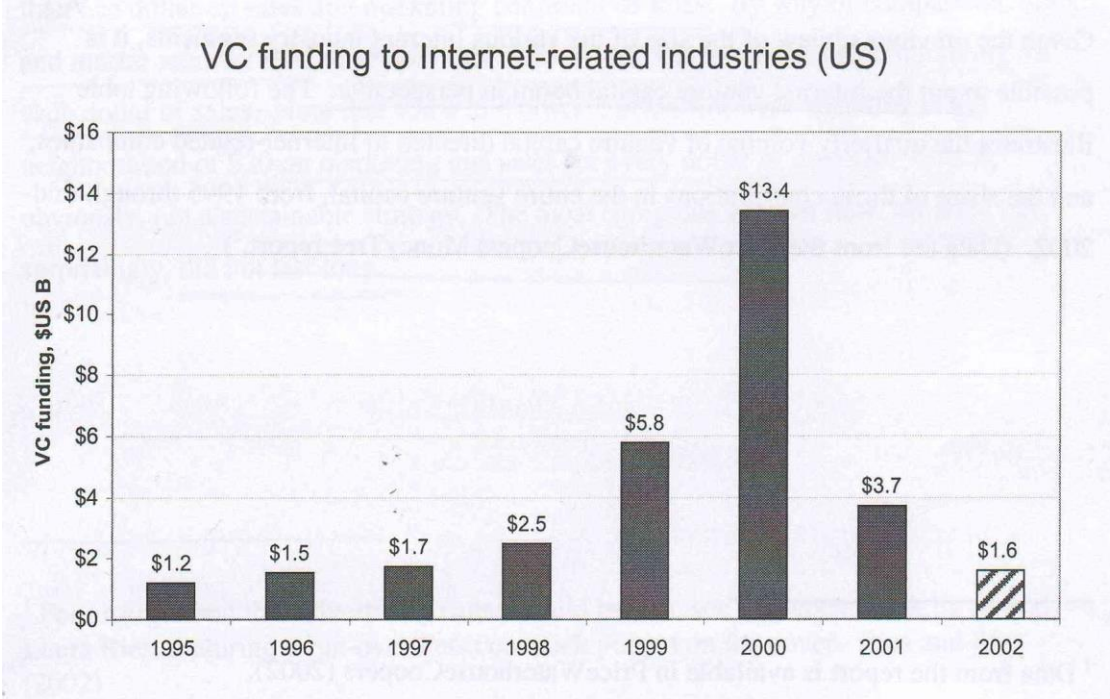
[286] Pojam poslovni plan označava alat za strateško preduzetničko promišljanje. Ima više definicija ovog pojma, čime se ne možemo baviti ovde. Jedna definicija glasi: "Pisani dokument koji detaljno opisuje kako će nova firma postići svoje ciljeve. Biznis plan će biti plan napisan iz marketinškog, finansijskog i operativnog ugla gledanja. Ponekad se priprema i za stare firme koje treba da krenu u nekom novom smeru." Preuzeto sa http://www.investopedia.com/terms/b/business-plan.asp Jedan od načina izrade biznisa plan naziva se "platno" (na engl. canvas) i znači da se bukvalno popunjavaju delovi jedne slike. Ovde dajemo jedno prazno platno za poslovni plan. Preuzeto sa http://www.businessmodelgeneration.com/canvas/bmc

prihoda i profita. Potom bi svoj poslovni plan, inovativnu ideju, predstavili fondovima rizičnog kapitala[287] nudeći udeo u budućem prihodu i profitu u zamenu za neophodni kapital za realizaciju svog poslovnog plana. Po ove preduzetnike srećna okolnost je bila da je finansijsko tržište bilo sklono da im stavi na raspolaganje kapital. Procene o visini finansiranja koje je tako dato su različite, ali su to svakako iznosi koji su omogućili formiranje poslovanja praktično iz ničega (opipljivog) . Jedna procena o visini tako plasiranog kapitala data je u donjem grafikonu, koji potiče iz izveštaja konsultantske kuće PriceWaterhouseCoopers iz 2002. godine.



[287] Na engl. Venture capital funds, skraćeno VC.

Ilustracija 26 Grafikon – Finansiranje internet kompanija od strane VC fondova



Preuzeto iz: Shawn O'Donnell „An Economic Map of the Internet" Telecommunications Policy Research Conference TRPC September 2002 str. 9. Dostupno na http://www.scribd.com/doc/293404410/TPRC-2002#scribd

Ovih blizu 30 milijaradi USD nije došlo iz jednog izvora. Radi se o većem broju investicionih fondova, raznih vrsta, među kojima su bili i fondovi rizičnog kapitala čija logika delovanja je preuzimanje rizičnog proslovnog projekta radi natprosečno visokog profita. Veliki broj pokušaja (finansiranih poslovnih projekata) je bio neuspešan, i uloženi kapital se gubio, ali je bilo i uspešnih, koji su davali natprosečno visoke profite.

Treba zapaziti da je sve zavisilo od procene (samog preduzetnika, a potom i investicionog fonda) da će se dotični novi proizvod ili usluga vezani za internet moći komercijalizovati. Iz ne baš samo racionalnih razloga, ulagači su verovali u uspeh poduhvata. Ulagači su čak imali veliko strpljenje, dajući tako priliku inovaciji da poluči rezultate. Čitava berza (odnosno veliki broj igrača na berzi) je delila takav pogled na ove kompanije, čak i kada ništa od njihovog poslovanja još nije bilo dokazano kao uspešno. „Tržišta kapitala su bila sama srž razvoja Internet kompanija i cijele nove ekonomije.[288] Vrednosti dot.com-a su unovčavane na berzi, inicijalnom ponudom akcija, neviđeno uspešno, sa vrtoglavo visokim cenama tih akcija na berzi.

[288] Castells. Opus cit. Str. 91.

Kupci akcija su često bile velike kompanije iz sektora kompjuterske opreme (na pr. Intel, Cisco). Činilo se da sam redosled poteza „ideja pa novac pa implementacija ideje pa zarada“ nikome nije bio sporan – do jednog momenta.

Oštar pad vrednosti tehnoloških deonica je počeo 10. marta 2000. Zašto je nastupila promena raspoloženja tržišta ostalo je predmet proučavanja do danas. Neko je to slikovito opisao kao ekonomija koja prkosi zakonima gravitacije. Jednom kad je tržište odlučilo da je Internet tehnologija budućnosti, bilo koja deonica povezana s internetom imala je trenutnu premiju, bez obzira na njen visoki rizik i najčešće nerealne poslovne izglede. A kada su tržišta od marta 2000. počela negativno da reaguju na ono što je shvaćeno kao preterano vrednovanje tehnoloških deonica, devalvacija mnogih od tih deonica je sledila nevezano sa stvarnom uspešnošću određene firme.

Ipak, posle ovog zemljotresa iz 2000/2001. nije bilo povratka na staro. Bez finansiranja inovativnih početnika (od strane kompanija ili fondova spremnih na rizična ulaganja) ne bi ni došlo do ostalih promena u poslovanju koje su u konačnom dovele do jedne potpuno nove ekonomije. U tom kratkom periodu (manje od 10 godina) već je zaživela nova ekonomija.

> „Iz vihora dot.com tvrtki izašao je novi privredni okoliš u čijem je središtu bilo e-poslovanje. Pod e-poslovanjem podrazumevam sve poslovne radnje kod kojih se izvedba ključnih operacija upravljanja, financiranja, inovacija, proizvodnje, distribucije, prodaje, odnosa sa zaposlenicima te odnosa s kupcima odvija najvećim dijelom putem ili na Internetu ili drugim računalnim mrežama, bez obzira na vrstu veze između virutelnih i fizičkih dimenzija tvrtke.“[289]

Velika zasluga internet kompanija je da su samim postojanjem uvele novine u poslovanju, vezane za internet, kod svih - i do tada tradicionalne firme bile su naterane da izlaze na internet. Naročito se to videlo kod načina interakcije sa kupcima, pošto je svaki dot.com imao prednosti u smislu direktnije veze s kupcima radi primanja narudžbina i poboljšanja svojih usluga za korisnike. Tako su tradicionalne kompanije sledile trend i krenule paralelno u plasiranje proizvoda i usluga na intenetu i u klasičnim trgovinama. Od tipičnih *Brick-and-mortar (cigla i malter)* preduzeća došlo se do *Click-and-mortar* (*klik i malter*) preduzeća. Takođe se odigrala i promena u brzini poslovanja, jer su tradicionalne kompanije morale da

[289] Ibid. str.79.

slede tempo novih kompanija. U krajnjem je to rezultiralo za sve firme kraćim vremenskim trajanjem poslovnog ciklusa, ciklusa inovacija i finansijskog ciklusa.

Jedno od objašnjenja za neuspeh nekih dot.com-a upućuje na preterano visoke troškove oglašavanja koje su ove kompanije imale. Takvi budžeti za oglašavanje su svesno davani jer „veliki broj dot.com firmi očekivao je da će biti u stanju da stvori brend svojih akcija kroz reklamiranje“.[290] Šon O'Donel donosi grafikon sa brojkama troškova prodaje i marketinga u odnosu na prihode, klasifikovano po profilima firmi iz različitih segmenata e-poslovanja: trgovine, proizvodnja sadržaja, finansije, provajderi internet usluga.

Ilustracija 27 Grafikon – Odnos troškova prodaje i marketniga kod pojedinih vrsta firmi

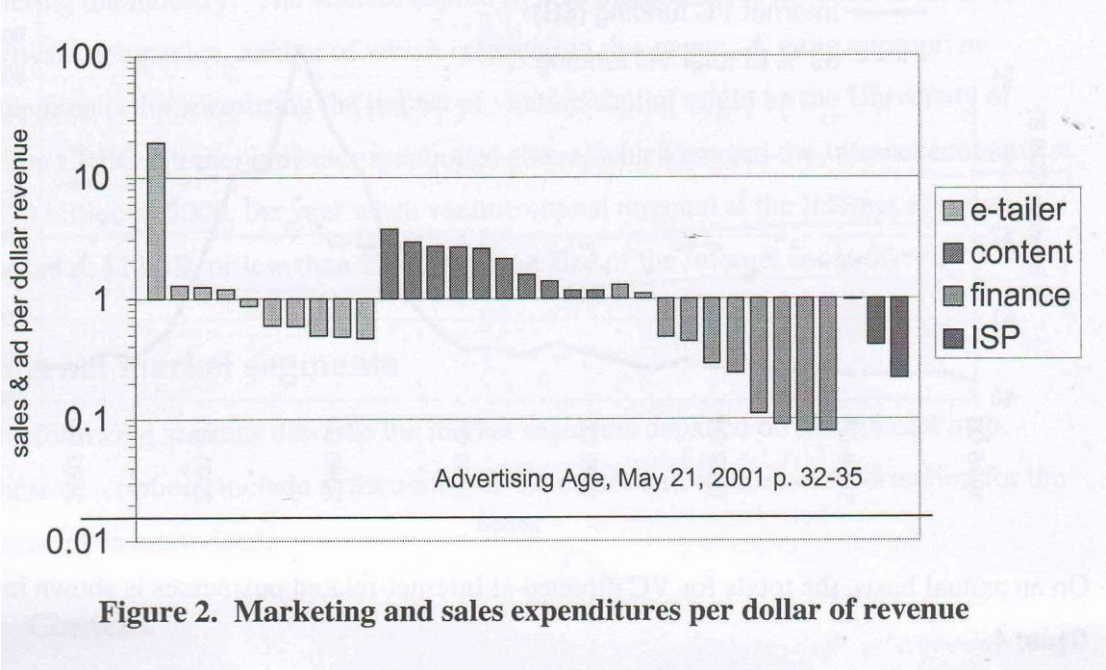


Figure 2. Marketing and sales expenditures per dollar of revenue

Preuzeto iz: Shawn O’Donnell „An Economic Map of the Internet“ Telecommunications Policy Research Conference TRPC September 2002 Str. 8. Dostupno na http://www.scribd.com/doc/293404410/TPRC-2002#scribd

Najneracionalniji u trošenju su bili pojedini akteri sektora trgovine i proizvodnje sadržaja. O'Donel podvlači:

> „Kompanije koje su iznad linije „1“ trošile su više od jednog dolara na prodaju i marketing za svaki dolar prihoda; one ispod ove linije trošile su (razumno) manje od dolara na prodaju i marketing za dolar prihoda. Upoređenja radi, cigla-i-kreč trgovci troše između 15 i 40 centi na prodaju i marketing za svaki dolar prodaje. Zapazite da su neki od

[290] Shawn O’Donnell, „Economic Map of the Internet“, RPRC 2002. Str.7.

> najgorih slučajeva trošili red veličina oko 20 dolara na marketing i prodaju za svaki dolar prihoda. To očigledno nije bila održiva strategija.“[291]

Međutim, ono što O'Donel ne pominje je to da se može smatrati da je tako intenzivno, čak iracionalno oglašavanje doprinelo dobrobiti interneta, odnosno ojačalo njegovu poznatost i popularnost i interesovanje za njega kod svih delova društva.

Ako se pogledaju godine osnivanja nekih od danas najvećih internet kompanija, vidimo da su neke «preživele» i taj turbulentan period, dok su druge dosta mlađe. Na primer, Amazon je osnovan 1994. godine, Jahu 1995., Gugl 1996., Skajp 2003., Fajerfoks (mozila) 2004., Fejsbuk 2004., Tviter 2006. godine.

Tamni optički kablovi

U ekonomiji interneta sve češće se nailazi na pojam prekapacitiranost odnosno tamni optički kablovi.

Tamni optički kablovi[292] (na engl. dark fiber) su termin koji označava potencijalni kapacitet mreže u telekomunikacionoj infrastrukturi, ali isto tako i instalirane optičke kablove koji nisu u vlasništvu ili pod kontrolom provajdera internet usluga ili tradicionalnih nosača (kerijera) telekomunikacionog saobraćaja. Obično se radi o mreži optičkih kablova koju su uspostavile firme u domenu izgradnje puteva, naftovoda, gasovoda i slično. Naime, uočeno je da se kod uspostavljanja optičke mreže oko 60% troškova tiče projektovanja, dobijanja dozvola, građevinskih radova i same instalacije na terenu, dok su sami optički kablovi tek mali deo troškova. Stoga su kompanije koje inače izvode gradnju takvih objekata radi efikasnosti i uštede troškova, počele da grade i optičku mrežu tokom izgradnje onog što im je primarni cilj - put, naftovod, gasovod i slično. To je racionalno, jer se za isti trošak izgradnje dobija dodatni resurs. Ove kompanije su time stvorile pretpostavku za mnogo više kapaciteta internet veza nego što je trenutna potreba interneta. Ako same ne bi htele da se bave ovim resursom, taj resurs odnosno višak kapaciteta u optičkim kablovima bi mogao nekog drugog da zanima, i kao što ćemo uskoro videti, to se i desilo.

Ova uočena pojava je delovala zabrinjavajuće za postojeće aktere u oblasti provajdera internet usluga jer teorijski daje mogućnost da vlasnik optičke mreže postane i sam

[291] Ibid. Str. 7.

[292] Optičko vlakno je „tamno“ dok se laserima i drugom opremom ne osvetli. Da bi postalo „svetlo“ potrebno je instalirati opremu na krajevima.

jedan od aktera na njihovom tržištu, odnosno uđe u posao provajdera internet usluga i značajno snizi cene širokopojasnog interneta. Dok to ne učini, on je samo provajder mreže (na eng. network service provider).

Da stvari budu još zaoštrenije na ovom tržištu, primetan je trend da se neki od sadašnjih krupnih korisnika ISP-ova spremaju da sutra to više ne budu. Radi se o najvećim internet kompanijama (džinovima) kao što je Gugl, Fejsbuk, Amazon, Majkrosoft i dr. O tome je dosta pisala američka štampa 2013. godine, od čega će ovde biti prikazan mali deo.[293] Ovo je značajno jer ukazuje da je na vidiku promena odnosa moći[294] u smislu toga kako se vrši saobraćaj na internetu i ko je taj ko ima ili će imati usko grlo ili izvlači profit na tom putu.

> „Ukratko, prosto svaka velika tehnološka kompanija koja zavisi od interneta želi udeo u cevima koje isporučuju njene podatke i usluge. Čak i delimično vlasništvo nad tim cevima daje duševni mir ovim ogromnim provajderima usluga. Prvo, osiguravaju da će imati dovoljno širokog pojasa da usluže potrošače i kompanije širom sveta. To ... takođe dozvoljava da zaobiđu bilo koja prepucavanja sa telekomomima oko mrežne neutralnosti a u isto vreme da prate i štite svoje mreže od spoljašnih očiju kao što su NSA ili strane vlade.“[295]

Još jedan od razloga koji se sreće je da je internet kompanijama bitna i ušteda na troškovima električne energije jer je ekonomičnije umesto izgradnje data centara u oblastima gde je struja skupa postaviti kablove da se ta oblast poveže sa data centrima koji su već u funkciji.[296]

Trenutno se čini da nije moguće pribaviti mapu instaliranih tamnih optičkih kablova.

---

[293] Dan Rowinski. (17. dec. 2013). „White Spaces & Dark Fiber: Internet Giants Angle For Control of the Internet's Pipes“. Dostupno na http://readwrite.com/2013/12/17/internet-backbone-google-amazon-facebook-microsoft

[294] „Ravnoteža između telekoma i internet džinova je bila, da se tako izrazimo, delikatna u zadnjih deset ili više godina. Kako su veb usluge rasle, tako su pritiskale mreže kablovskih i mobilnih kompanija. Sam Netflix je odgovoran za blizu trećine ukupnog internet saobraćaja u SAD; Netflix i Google-ov You Tube zajedno odgovaraju za oko polovine korišćenja interneta u SAD.“ Rowinski, opus cit.

[295] Rowinski, opus cit.

[296] Drew Fitzgerald and Spencer E. Ante. (16. dec. 2013). “Tech Firms Push to Control Web's Pipe” *The Wall Street Journal* Dostupno na http://www.wsj.com/articles/SB10001424052702304173704579262361885883936 Inače, isti članak donosi i podatak da Gugl već ima oko 100.000 milja kablova širom sveta, a poređenja radi kompanija Sprint, koja upravlja optičkom mrežom preko kontinentalnog dela SAD, ima kablove ukupne dužine manje 40.000 milja. (1 milja iznosi 1,6093 km)

Internet stvari (IoT - Internet of Things)

Najnoviji bum internet kompanija očekuje se na temelju širenja interneta stvari. To je promena koja može drastično da izmeni sam karakter interneta.

Termin „internet stvari“ se pripisuje kao autoru Kevinu Aštonu (Kevin Ashton) budući da je još 1999. godine upotrebio te reči u nekoj prezentaciji, iako fenomen na koji se taj termin odnosi tada nije postojao u praktičnoj primeni, a tek kod retko koga i u zamisli. Fenomen je ostvaren tj. ušao u život ljudi nakon 2012. godine, a od 2015. doživljava ekspanziju – komercijalno ali i u akademskim istraživanjima. Kao sličan, ali ne identičan, termin, sreće se i „Internet svega“ (Internet of Everything) koji je smislio Džon Čembers (John Chambers) iz kompanije Cisco.[297] Još jedan originalan naziv je kovanica tingternet[298] (thingternet - spoj engleskih reči „internet“ i „thing“) – za sada bez prevoda na srpski jezik. U ovom radu koristiće se termin internet stvari.

Internet stvari označava internet na koji se priključuju najrazličitiji senzori i aktuatori smešteni u/na fizičkim objektima da bi se među njima odvijala komunikacija putem interneta. Osnovne komponente interneta stvari su senzori i aktuatori i naravno - internet. „Senzori se ugrađuju da detektuju neku specifičnu fizičku promenu i samo tu programiranu promenu, i da pretvore taj događaj u ono što je čitljivo nekom posmatraču ili drugom elektronskom instrumentu“ dok „aktuatori pokreću ili kontrolišu neku mašinu ili sistem kao odgovor na neki signal na način kako je unapred specifikovano.“[299] Cena ovih komponenti je veoma dostupna i to otvara put primeni u najrazličitijim kontekstima, a internet je ionako (već bio) sveprisutan.

U literaturi se sreće i ova definicija interneta stvari:

> „integrisani deo budućeg interneta koji uključuje postojeći i evoluirajući internet i mrežni razvoj i može se pojmovno odrediti kao dinamička globalna mrežna infrastruktura sa samo-konfiguirajućim sposobnostima bazirana na standardnim i interoperabilnim komunikacionim protokolima, u kojoj fizičke i virtualne 'stvari' imaju identitete, fizičke atribute i virtualne ličnosti, koriste inteligentne interfejse i skladno su integrisane u informacionu mrežu.“[300]

---

[297] Navedeno prema: Scott R. Peppet. (2014). „Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security & Consent“. *Texas Law Review* Vol. 93,.85-177. Dostupno na http://www.texaslrev.com/wp-content/uploads/Peppet-93-1.pdf (U daljem tekstu „Regulisanje interneta stvari“) Str. 88.

[298] Navedeno prema: Dutton, William H. (20. jun 2013).*The Internet of Things* OII Working Paper commissioned as part of the UK Government's Proceedings of Foresight Horizon Scanning Papers Available at SSRN: http://ssrn.com/abstract=2324902 or http://dx.doi.org/10.2139/ssrn.2324902 (U daljem tekstu *Internet of Things*) str. 8.

[299] *Internet of Things*, str. 9.

[300] Definicija potiče iz: dr.Vermesan, O., Dr. Friess, P., Guillemin, P., Gusmeroli, S., Sundmaeker, H., Dr.Bassi, A., Jubert, I.S., Dr. Mazura, M., Dr. Harrison, M., Dr. Eisenhauee, M., Dr.Doody, P.

Da li je internet stvari – internet? Strogo posmatrano - nije, ukoliko se smatra da je internet stvoren za komunikaciju ljudi ili tačnije ljudi putem kompjutera. Međutim, iz drugog ugla – jeste, jer se i ova druga komunikacija odvija u istoj mreži na bazi istog otvorenog protokola, s tim da sada ne više ljudi nego fizički objekti šalju elektronske informacije. (Samim tim, prestaju da budu jednostavni fizički objekti i postaju informaciono-komunikaciona tehnologija.[301])

Po nekim mišljenjima, ovo je zaista autentično nova primena interneta, a po drugima se tu radi o kvantitativnoj a ne kvalitativnoj promeni. „Da li kompanije i industrija samo pokušavaju da promovišu nešto kao 'novu novu stvar' ili je to ozbiljan odmak od prošlih tehnoloških sistema?“[302]

Po Datonu, postoji 4 razloga zašto možemo smatrati da je to suštinski nov tehnološki razvoj, i to zato što su novi: vizija, konteksti primene, društvene implikacije i izazovi upravljanja. Nova vizija usmerava fokus pažnje na objekte koji su onlajn, a ne na ljude, i to se vidi u domenima pametne logistike, pametnih gradova, pametnih kuća i sl. Novi kontekst primene se vidi na primeru nadzora kretanja – ranije se u nekoj ustanovi moglo senzorima nadzirati kretanja ljudi ili objekata, ali to je bila zatvorena lokalna primena, dok su sada isti signali/informacije onlajn i može im se pristupiti tehnički iz čitavog sveta. Nove društvene implikacije se vide na primeru senzora za praćenje bioloških parametara čoveka – oni donose tzv. kvantificirano sopstvo i „samospoznaju kroz brojeve“ odnosno otkrivaju mnogo toga o korisniku samom njemu ili njoj, a potencijalno i drugima. Novi izazovi upravljanja postaju jasniji kada se uzme u obzir red veličina ovih sistema i podataka, brzina, preciznost sadržaja, dinamičnost, deljenje podataka i drugo.

S druge strane, ističe se da su korisne aplikacije za identifikaciju, praćenje traga i senzorsku tehnologiju postojale i ranije a da u mnogim slučajevima „ova oblast nema jak ubedljiv poslovni model. Drugim rečima, još uvek nije sprovodiva i verovatno nije čak ni za onog poslovičnog ćoška.“[303] Razmatrajući šta bi se moglo ostvariti u

---

„Internet of Things Strategic Research Roadmap“, u: Vermesan, O and Friess, P., eds. *Interet of Things - Global Technological and Societal Trends*, River Publishers, Denmark, 2011, 9-52, 10. Ovde navedena prema: McKay Cunningham, „Next Generation Privacy: The Internet of Things, Data Exhaust, and Reforming Regulaltion by Risk of Harm“ in *Groningen Journal of International Law*, Vol. 2(2), 2014. pp. 115-144. Dostupno na https://groningenjil.files.wordpress.com/2015/01/grojil_vol-2-ed-2_cunningham.pdf str. 136.

[301] *Internet of Things,* str.4.

[302] Ibid. str. 13.

[303] Ibid. str. 23.

budućnosti, jedan od mogućih ishoda (scenarija) je da iako je internet stvari izvodljiv tehnički i finansijski, nije verovatno da će moći da prevaziđe solidan broj organizacionih, institucionalnih i političkih prepreka. Društvena inercija, u kombinaciji sa zaista složenim pravnim, etičkim i društvenim pitanjima koja se javljaju, radi protiv njega i usporava ga. Danton daje jednu zanimljivu opasku:

> „Stepen do koga su nacije u stanju da preskoče ove teškoće bi mogao da zavisi od strukture političkog odlučivanja u svakoj zemlji. Na primer, manje je verovatno da će liberalniji demokratski režimi brzo napredovati sa internetom stvari, imajući u vidu spektar pitanja oko njegovog upravljanja i korišćenja. Rani razvoj u Singapuru i Kini ilustruje vrednost odlučivanja odgozgo-na dole.“[304]

Još detaljnije razmatranje problema koje Dantonov tekst nagoveštava nalazi se u navodno prvom radu iz oblasti prava i interneta stvari „Regulisanje interenta stvari: prvi koraci ka upravljanju diskriminacijom, privatnošću, bezbednošću i pristankom“ Skota Pepeta iz 2014. godine. (Prvi rad se odnosi na američku pravnu teoriju i praksu.) Pepet najpre daje tipologiju senzora namenjenih širokoj potrošnji, od kojih je senzore nekih tipova (ukupno 20) lično ispitao da bi proverio modus operandi. Zatim iznosi četiri pravna problema koja je identifikovao u vezi sa ovim senzorima (i predlaže isto toliko rešenja, kojima se ovde nećemo baviti). Treba napomenuti da Papet nije obradio sve oblasti primene, tj. izostavljeni su industrijski i komercijalni senzori koji se koriste u fabrikama, skladištima, lukama itd. kao i ambijentalni senzori i senzori koje koristi vlada.[305]

Pet tipova uređaja sa interneta stvari koji su trenutno dostupni su: zdravstveni i fitnes seznori, crne kutije u automobilima, kućni i senzori pametne električne mreže, senzori sa radnog mesta i senzori u današnjim pametnim telefonima.

Zdravstveni i fitnes senzori se dalje dele na podgrupe: opšti merači, nosivi senzori (u formi odeće), epidermalni senzori (koji se lepe na kožu), senzori koji se gutaju ili koji se ugrađuju u telo. Ovde ćemo navesti samo najpoznatije uređaje iz ovih grupa: iBGStar (merač glukoze u krvi), Propeller Health (prati lekove za astmu), Scanadu Scaut (prati vitalne znake), Scanadu Scanaflow (analiza urina), HappyFork (viljuška koja broji zalogaje), Beam Touthbrush (četkica za zube koja meri pranje zuba), FitBit (narukvica koja prati parametre fizičkih vežbi), Nike Fuel Band (narukvica koja prati parametr fizičkih vežbi), FINIS Swimsense (narukvica koja prati plivanje), Electric

[304] Ibid. p.24.
[305] „Regulisanje interneta stvari“ str. 96.

Foxy Move (majca koja prati fizičke vežbe), Nike+shoes (patike koje prate fizičke vežbe), BSE (brushalter koji prati indikatore raka dojke), Sensoria Fitness Smart Socks (čarape koje prate fizičke vežbe), MC10 BioStamp (flaster prati mnoge parametre od srčanog ritma do izloženosti ultravioletnim zracima), Sano Intelligence (flaster koji prati krvotok), PillCam (kamera u obliku pilule), SmartPill (pilula koja meri Ph nivo u telu).

Automobilski senzori se odnose na uređaje za snimanje događaja (na engl. EDR - event data recorders) poznatije pod nazivom crne kutije, potrošačke uređaje kao što su Automatic Link („FitBit za vaš auto“), ZenDrive itd. i najzad na uređaje koje primenjuju osiguravajuća društva za potrebe kreiranja premije osiguranja kao što je Progresive Snapshot.

Od kućnih uređaja najpoznatiji je Nest thermostat (podešava temperaturu u kući zavisno od pokreta), a tu su i Brillion home oven (senzor za rernu), WattVision (senzor za upotrebu energije), Wimoto Growth (senzor za zalivanje biljaka), Belkin (procesor za više različitih kućnih senzora), Quirky (procesor za više različitih kućnih senzora). Pametna električna mreža je sistem za uštedu električne energije u domaćinstvu kroz energetsku efikasnost.

Primeri senzora na radnom mestu su Hy Green – sistem za praćenje higijene ruku kod osoblja u bolnici, narukvice za merenje produktivnosti radnika u trgovinama Tesco i sistem bedževa za snimanje glasa u Bank of America.

Konačno, možda je najfascinantnije od svega koja količina senzora se nalazi u pametnim mobilnim telefonima, koji su verovatno naj-sveprisutnija senzorska mreža danas.

> „Takvi telefoni sada generalno sadrže kompas (koji određuje fizičku orijentaciju), akcelerometar (koji prati kretanje uređaja u prostoru), monitor ambijentalnog svetla (za podšavanje osvetljenja ekrana), senzor blizine (da li je telefon blizu vašeg lica), žiroskop (koji prati vertikalno-horizontalnu orijentaciju telefona), kao i GPS, osetljiv mikrofon i više kamera. U toku je istraživanje koje bi poboljšalo pametne telefone u detekciji nivoa ultravioletnog zračenja (za sprečavanje raka kože), nivoa zagađenja (kao pomoć u praćenju životne sredine) i razne indikatore zdravlja, aktivnosti i dobrostanja, uključujući senzore koji mogu da prate nivoe alkohola u krvi i telesne masti.“[306]

[306] Ibid. str.109-110.

Neki čak predviđaju da će se sledeća generacija pametnih telefona zvati „kognitivni telefoni“[307] i znaće mnogo više o korisniku, posebno zahvaljujući ukrštanju podataka sa drugim senzorskim ali i društvenim mrežama, ličnim kalendarima itd.

Što se tiče problema koji se javljaju u vezi sa ovim senzorima i podacima koje proizvode, mogu se pobrojati: fuzija senzora, teškoće anonimiziranja, teškoće zaštite, nepogodnost za izbor i pristanak korisnika. Svi oni su dosta izazovni.

Fuzija senzora znači da senzorski podaci teže da se kombinuju na neočekivane načine, iz čega dolazi do mogućnosti izvođenja ozbiljnih zaključaka iz na prvi pogled bezopasnog izvora podataka (na primer, od podataka sa FitBit narukvice do zaključaka o prihvatljivosti kandidata za zaposlenje). „U svetu povezanih senzora 'sve može da otkrije sve'. Senzorski podaci su tako bogati, precizni i fino podešeni da podatak iz bilo kog senzornog konteksta može biti vredan u različitim, ako ne i svim drugim, ekonomskim ili informacionim kontekstima.“[308] Iako ne znamo empirijski da se to zaista i dešava, to bi moglo da se desi, što je dovoljan razlog za zabrinutost.

Teškoće anonimiziranja pogađaju dosadašnji način baratanja podacima. Uobičajeno, zaštita ličnih podataka se vrši tako što se oni anonimizuju odnosno de-identifikuju u masi ostalih, tako da se smatra da na taj način čuvaju privatnost. Ipak, ovo rešenje se pokazuje kao nepouzdano, jer se podaci mogu od de-identifikovanih lako ponovo da identifikuju – uz pomoć vrlo malo spoljnih informacija. Papet tu referira na veoma uticajnu studiju koja je upravo to dokazala.

> „Istraživači sa MIT su nedavno analizirali podatke o 1,5 miliona korisnika mobilnih telefona u Evropi u periodu od 15 meseci i otkrili su da je relativno lako izvući potpunu informaciju o lokaciji za pojedinačnu osobu iz tog anonimiziranog seta podataka ... bilo je potrebno samo locirati tog pojedinačnog korisnika 4 puta u toku godine na nekoliko stotina jarda[309] udaljenosti od transmitera bilo kada u trajanju od jednog sata. Sa 4 takva poznata podatka, istraživači su mogli identifikovati 95% korisnika u tom setu podataka.“[310]

Objašnjenje lakoće identifikacije se krije u inherentnoj razbacanosti tako velikih setova podataka.

---

[307] Ibid. str.111.
[308] Ibid. str.114.
[309] 1 jard iznosi 0,9144 metra.
[310] „Regulisanje interneta stvari“ str. 122. Studija o kojoj se radi je: Yves-Alexandre de Montjoye, Cesar A. Hidalgo, Michel Verleysen & Vincent D. Blondel, *Unique in the Crowd: The Privacy Bounds of Human Mobility*, 3 scientific report 2013. doi:10.1038/srep01376 Dostupno na http://www.nature.com/articles/srep01376

Međutim, postojeći zakoni koji štite privatnost ne klasifikuju u zaštićene podatke (podatke identifikacije ličnosti) ove nove podatke (uključivo i biometrijske) nastale od senzora koje vezujemo za internet stvari. Razlika postoji: senzorski podaci su samo pogodni da identifikuju ličnosti (identifikacija se može ali ne mora desiti), što ne znači da ih sada odmah treba štititi na isti način kao ime, adresu ili JMBG. (To pokazuje da se još uvek veruje u mogućnosti anonimizacije, bez obzira na dokaze njenog lakog otklanjanja.) Slično tome, zakoni i propisi koji regulišu obavezu obaveštavanja korisnika (tzv. notifikacija) o povredama bezbednosti podataka takođe ne važe za ovu vrstu podataka. Ako bi FitBit-ov server bio napadnut, kompanija ne bi bila u obavezi da obavesti korisnike o tome ili da snosi pravne posledice zbog takvog slučaja.

Teškoće zaštite podataka u internetu stvari su veoma znatne. Uređaji sa interneta stvari su inherentno ranjivi na povrede bezbednosti podataka i to iz dva razloga: ovi uređaji se proizvode bez dovoljnog osvrtanja na prioritet zaštite podataka i ovi uređaji su kompaktni i mali, te stoga teški za dodavanje procesora za enkripciju ili dodavanje jače baterije za rad aplikacije koja garantuje jaču bezbednost podataka.[311] Za razliku od pametnog telefona koji se može ažurirati za bolju bezbednost podataka, ovi senzori nemaju takve mogućnosti ažuriranja. Ros Anderson je na tu temu postavio jedno smešno pitanje, koje dovoljno ilustruje probleme. „Šta se dešava ako neko napiše kompjuterski virus kojim preuzme klima uređaj i onda ga uključuje i isključuje iz daljine? Tako bi mogali i da sruštie električnu mrežu ako to želite.“[312]

Na kraju, iz ugla pravnika teško je ustanoviti pristanak korisnika ovih senzorskih uređaja jer korisnici obično nisu ni obavešteni o politici privatnosti kompanije koja im prodaje senzorski uređaj i mogućnostima da biraju ili odbace predložene uslove iz nje.

Bez obzira na izložene teškoće i nedoumice, industrija interneta stvari je sve više u usponu. Vraćajući se na već pominjane investicione fondove, koji ulažu u inovativne kompanije u oblasti interneta, sve ukazuje da je internet stvari najnoviji ljubimac investicionih fondova u 2015. godini. Istraživačka firma CB Insights koja se bavi praćenjem investicionih fondova (i koju podržava Nacionalna fondacija za nauku SAD-a) objavila je studiju *Analizirajući pejzaž interneta stvari* u kojoj konstatuje da

[311] “Regulisanje interneta stvari” str.127.
[312] Ibid. str. 128.

„IoT kompanije napadaju ... sve“.[313] Tu se nalazi podatak da se finansiranje novih IoT kompanija udvostručilo u zadnjih pet godina (768 miliona USD 2010. do 1,9 milijarde USD 2014.) a broj transakcija takođe (91 u 2010. i 221 u 2014.).[314] Karakteristično je da je više od 60% finansiranih kompanija tek u fazi ranog finansiranja, najveći broj njih u 2013. godini. Najbolje finansirane kompanije su View (staklo i prozori povezani sa internetom), Proteus Digital Health (senzori koji se gutaju) i Jawbone (senzori na odeći). Nove IoT kompanije u 2015. godini privukle više od 1 milijarde USD, u poređenju sa nešto manje od 1,4 milijarde USD za prethodnih pet godina.[315] Finansirane nove kompanije su smeštene u Silikonskoj dolini u Kaliforniji, čak 59% svih finansiranih je tu, dok je 7% smešteno u Masačusecu, po 5% u Teksasu i Njujorku.[316] Studija ukazuje na intenzivno ulaganja u kompanije koje se bave dronovima,[317] (koji su takođe u nekom smislu deo interneta stvari) u koje je zaključno sa trećim kvartalom 2015. uloženo 300 miliona USD, kao i na to da još uvek nijedna kompanija iz IoT nije dospela do faze zrelosti. Inače, od IoT kompanija na berzu su za sada izašle FitBit, GoPro i Oculus.[318]

Ono što za sada nedostaje je mišljenje običnih korisnika interneta o internetu stvari. Da li će im se dopasti ponuda ili će ostati uzdržani – možda je još prerano znati. Smatram da će korisnici biti radoznali i da će inicijalno interesovanje za ove senzore biti veliko, pod uslovom da je cenovno dostupno širokom krugu korisnika. Ipak, pošto se ovi senzori moraju ugraditi u moderne životne stilove, njihov uspeh je diskutabilan. Fitnes senzori zavise od fitnesa kao dela životnog stila, kućni senzori zavise od kulturnih navika u pogledu stanovanja itd. Čini se da najlakši prodor može doći kod senzora u medicinskim primenama.

Scenariji budućnosti interneta – internet 2025. godine

Ulaganja investicionih fondova u pravilu nagoveštavaju budućnost odnosno koji proizvodi i usluge će se proširiti tako da to oseti većina čovečanstva. Zato se može

[313] CB Insights *Analyzing the Internet of Things Investment Landscape* 2015. Dostupno na www.cbinsights.com Str. 5.
[314] Ibid. str.9.
[315] Ibid. str. 26.
[316] Ibid. str. 31.
[317] Ibid. str. 15.
[318] Ibid. str. 19.

ozbiljno računati da internet stvari ide ka nama i sve nam je bliže. Internet stvari je internet budućnosti.

Najčešći oblik razmišljanja o budućnosti interneta je u formi kreiranja scenarija. Scenarija su divergentne priče o budućnosti koje služe da pomognu istraživanju mogućih budućnosti interneta. Problem sa ovim pričama je da su to zaista priče, više ili manje detaljni, više ili manje kontračinjenički opisi situacija, bez doticanja uzročno-posledičnih veza u fenomenima na koje se referira, pa se ne mogu koristiti u filozofskoj analizi. Donekle korisna je jedna studija o scenarijima koju je objavila kompanija Cisco[319] 2010. godine i koja obuhvata horizont do 2025. godine. I njihove priče (ima ih 4)[320] dočaravaju moguće buduće obrasce korišćenja interneta, koji su tek površno povezani sa stanjem infrastrukture i potezima glavnih aktera, ali ono što je najzanimljivije u tom pokušaju jeste navođenje nekih pretpostavki evolucije interneta "na koje se može računati sa pouzdanošću". Cisco smatra kao pouzdano da:

1. najveći rast tržišta povezanog sa internetom desiće se van današnjih naprednih odnosno ekonomija visokog prihoda;
2. globalnom upravljanje internetom će ostati nepromenjeno u osnovi;
3. "digitalni urođenici" će se odnositi prema internetu na upadljivo drugačije načine od ranijih generacija;
4. današnja tastatura neće biti primarni interfejs sa internetom;
5. potrošači će priključak na internet plaćati na širi spektar načina.[321]

Drugi način na koji se mogu razumeti tokovi razvoja interneta u budućnosti bio bi dovođenje do krajnjih konsekvenci pojedinih elemenata koji se već uočavaju. (Ono što je zanimljivo da se tim načinom stiže do ishoda relativno sličnih Cisco-ovim pričama-scenarijima).

Krajnja konsekvenca najlošijeg razvoja događaja u pogledu bezbednosti interneta svodi se na to da internet postane nebezbedno mesto, sa hiljadama vandala, prevaranata i sajber terorista, protiv kojih je borba stalna, skupa i ne baš uspešna. To bi korisnike odbilo od korišćenja interneta, a takođe bi zatvorilo e-trgovinu, čuvanje podataka u oblaku i još mnoge poslovne opcije. Snage reda ne bi mogle da se efikasno

[319] Cisco Global Business Network. 2010. *The Evolving Internet: Driving Forces, Uncertainties and Four Scenarios to 2025*, Dostupno na http://newsroom.cisco.com/dlls/2010/ekits/Evolving_Internet_GBN_Cisco_2010_Aug_rev2.pdf (pristupljeno 20.02.2016.)

[320] Ibid. str.2.

[321] Ibid. str.5.

bore sa sajber kriminalcima. «Patroliranje policije u virtualnom svetu je teže nego patroliranje policije u fizičkom svetu.»[322] Ovaj scenario ukazuje migraciju sa interneta i njegovu propast.

Krajnja konsekvenca uticaja ekonomske krize koja se primećuje u velikom delu sveta je da korisnici interneta ne žele/ne mogu da troše novac i zadovoljavaju se samo osnovnim funkcionalnostima/uslugama na internetu, po mogućstvu što jeftinijim, jer ne raspolažu kupovnom moći za nešto više. Takav stav korisnika daje prednost kompanijama (mahom lokalnim, jer i vlada u toku ekonomske recesije teže da nastupaju protekcionistički te globalne kompanije imaju problema) koje nude jeftine pakete ili pakete odmerene do zadnjeg bita. Korisnici su vremenski malo na internetu pa samim tim nisu u poziciji da «postanu zavisni od interneta». Ovo je scenario koji ukazuje da bi internet budućnosti mogao biti žrtva ekonomske krize, lošiji i manje sofisticiran od interneta kakav poznajemo danas (2015. godina).

Krajnja konsekvenca enormnog povećanja broja korisnika interneta bez strateškog razvoja i jačanja infrastrukture koja toliki saobraćaj može da podrži je internet generalno sniženog kvaliteta. Mogu postojati izuzeci, ostrvca dobre infrastrukture i usluga, barem kod onih koji mogu da plate odgovarajuću cenu za takav premijum kvalitet. Za većinu korisnika, dostupan internet je zagušeni internet. To više nije globalni internet, već nalik malim izolovanim mrežama u moru jedne mreže koja otežano funkcioniše. Ovo je scenario koji ukazuje da bi internet budućnosti mogao biti raslojeniji od interneta kakav poznajemo danas (2015. godina).

Na kraju, moguć je i jedan dobar razvoj događaja, scenario uspešnog razvoja interneta, koji se bazira na neograničenom ulaganju u infrastrukturu, razvoju tehnologije i rastu broja korisnika. Krajnja konsekvenca eksplozivnog razvoja u smeru interneta stvari dovodi do scenarija u kome je konektivnost svega i svakoga postala realnost i u kome su „svi (ili velika većina) uvek na mreži, uvek percipirajući, uvek interreagujući i uvek promenljivi.“[323]

[322] Ibid, str..21.
[323] Ibid. str.17.

OSMO POGLAVLJE

G. i gđa Obični Korisnik u savremenom internet okruženju

Do sada smo prikazali infrastrukturne odlike interneta koje proističu iz načina upravljanja i neupravljanja njime, načina materijalnog rasprostiranja i načina razvoja diktiranog ekonomskim faktorima. Sve ove infrastrukturne odlike, kao i one arhitekturalne o kojima je bilo reči ranije, veoma direktno su kreirale i kreiraju položaj običnog korisnika na internetu. Ali taj položaj takođe zavisi i od samog korisnika, njegove aktivnosti ili pasivnosti. Zato će ovde pažnja biti usmerena na analizu položaja običnog korisnika iz ugla resursa, alata i potencijala ugrađenih internetom u taj položaj. Drugim rečima, ovde je cilj utvrditi kakav je položaj običnog korisnika sagledan kroz internetom proizvedenu redistribuciju moći između običnog korisnika i drugih aktera.

Savremeni trenutak u kome se čovek i internet nalaze izraelski filozof Johai Benkler opisuje na sledeći način:

> «Na početku 21. veka nalazimo se u jeku borbe oko institucionalnog eko sistema digitalnog okruženja. Široki spektar zakona i institucija ... se rasklapa i sklapa zarad toga da se pripremi teren za jedan ili drugi način obavljanja stvari. Kako se ove bitke budu završile u sledećoj deceniji ili kasnije značajno će uticati na to ... u kom obimu i kojoj formi ćemo moći – kao autonomni pojedinci, kao građani i kao učesnici u kulturama i zajednicama – da određujemo svet.»[324]

Dobra metafora ove situacije može se naći u tekstu Dejvida Klarka iz 2007. godine, iako je tema tog teksta (neutralnost interneta) nešto što ovo istraživanje ne obuhvata. Klark je tadašnju borbu (oko neutralnosti interneta) opisao ovako:

> „Stara šala o gorilama ide ovako: 'Gde će da sede gorile od 800 funti[325]? Gde god hoće.' A gde se gorile od 800 funti biju? Biju se tamo gde imaju kontakt jedna sa drugom ili (u okolnostima interneta) gde se interkonektuju. ISP-ovi se međusobno povezuju i povezuju se sa provajderima sadržaja. ... treba da bude jasno da je ono što se dešava

[324] Yochai Benkler *The Wealth of Networks. How Social Production Transforms Markets and* Freedom. Yale University Press New Haven and London 2006. Dostupno na http://www.benkler.org/Benkler_Wealth_Of_Networks_Chapter_1.pdf str. 2.
[325] 800 funti je oko 360 kg.

> sa potrošačem je nusproizvod toga kako se razrešavaju bitke među velikim igračima.“[326]

U prethodnim poglavljima predstavili smo ove velike „bitke“ i to kako se one direktno tiču dizajna arhitekture mreže. To je prvo što treba zapaziti ako jer reč o opisu sadašnjeg trenutka interneta iz ugla prosečnog korisnika.

Drugo što treba uključiti u presek sadašnjeg momenta je to da broj korisnika interneta u svetu, prema najnovijim dostupnim podacima, iznosi 3,4 milijarde, što je oko 46% ukupnog stanovištva na planeti, i da se broj korisnika stalno i rapidno povećava, tako da je samo u periodu 2010-2015 ukupan rast 832,5%.[327] U posmatranom periodu stope rasta su najveće u Africi, na Bliskom istoku, u Latinskoj Americi sa Karibima i Aziji – to su prostori na kojima prosečnom stanovništvu internet tek sada postaje dostupan, za razliku od Severne Amerike i Evrope gde je internet „zaživeo“ pre. Detaljniji pregled statistike korisnika prema geografsko-političkom kriterijumu dostupan je u Prilogu 2 na kraju rada.

Statistike u ovoj oblasti prate brojne parametre korisnika interneta, ne samo elementarne kao što je broj po državama. Na primer, propraćeno je i ono što korisnici rade na internetu, od broja poslatih mejlova, okačenih fotografija i sl. do utrošene električne eneregije i emisije ugljendioksisda povezanih sa internetom. Formirana je internet stranica pod nazivom *Internet live stats*, koja funkcioniše zahvaljujući ulaznim podacima tri moćne organizacije - Međunarodne telekomunikacione unije, Svetske banke i Ujedinjenih nacija demografski odsek – i to je mesto gde se svi ti brojni parametri ažuriraju u realnom vremenu, iz sekunda u sekund. I ova statistika jasno predočava sliku o rastu interneta. „Prva milijarda korisnika dostignuta je 2005. godine. Druga milijarda 2010. godine. Treća milijarda 2014. godine.“[328] (Kao korisnik interneta računa se „pojedinac koji može pristupiti internetu iz kuće u kojoj živi, preko kompjutera ili mobilnog uređaja.“ [329] Uzrast pojedinca nije bitan za status korisnika interneta.) A daleke 1993. godine (od koje kreće posmatrani period) bilo je samo 14.161.570 internet korisnika. Takođe, ponavlja se i opis nejednakosti na internetu:

---

[326] David D. Clark. (2007). “Network Neutrality: Words of Power and 800-Pound Gorillas” u *International Journal of Communication* 1, 701-708. Str. 706.

[327] Podatak sa internet stranice http://www.internetworldstats.com/stats.htm (pristupljeno 29. feb. 2016.)

[328] Podaci su sa http://www.internetlivestats.com/internet-users/#trend (pristupljeno 29.feb.2016.)

[329] Podaci su sa http://www.internetlivestats.com/internet-users/ (pristupljeno 29.feb.2016.)

> „Godine 2014. skoro 75% (2,1 milijarda) svih internet korisnika (2,8 milijarde) živelo je u vodećih 20 država. Ostalih 25% (0,7 milijarde) distribuirano je među ostalih 178 država. ...Kina, zemlja sa najviše korisnika (642 miliona 2014. godine) predstavlja skoro 22% ukupnog broja, i ima više korisnika nego tri sledeće zemlje zajedno (SAD, Indija i Japan).“[330]

Kao što smo već naveli, studija korisnika interneta nije tema ovog rada, koji se bavi arhitekturom i infrastrukturom interneta. Međutim, u meri u kojoj korisnici utiču na razvoj interneta i u meri u kojoj dolazi do uzimanja korisnika u obzir (na primer kada države nastupaju u ime korisnika kao svojih građana ili kompanije nastupaju u ime korisnika kao svojih klijenata) u sukobima među glavnim akterima interneta, obični korisnici interneta ulaze u fokus ovog istraživanja.

Ono najvažnije što je internet doneo za gospodina i gospođu Običnog Korisnika interneta nalazi se u ove četiri oblasti:

1. Lako uključivanje u globalnu ekonomiju,
2. Lak pristup kulturi i obrazovanju,
3. Mogućnost za internet politički aktivizam,
4. Regulisanje privatnosti pojedinca.

Ove četiri oblasti nisu slučajno poređane ovim redosledom, jer kao kriterijum rangiranja može se uzeti količina sukoba između ključnih aktera koji se vode u konkretnoj oblasti. Oko toga kako će se obični korisnik interneta uključiti u ekonomske tokove ima najmanje kontroverzi i problema, dok se odluke vezane za stepen privatnosti običnog korisnika interneta donose (*de facto* i *de jure*) u intenzivnoj raspravi i sukobljavanju.

Na drugačiji način sagledano, situacija sa običnim korisnikom interneta može se odrediti kao zbir dobitaka i gubitaka koje je pojedinac ostvario u novom informacionom okruženju.

U dobitke se obično ubrajaju:

- nova dimenzija individualne slobode,
- novi prostor za uživanje, negovanje i kreiranje kulture,
- nova platforma za bolju demokratsku participaciju,
- novi mehanizam za ekonomski razvoj (globalna ekonomija).

[330] Podaci su sa http://www.internetlivestats.com/internet-users/ (pristupljeno 29.feb.2016.)

Gubitak se prvenstveno ogleda u smanjenju, možda čak i nestanku privatnosti pojedinca, što se dešava na tri načina:

- kroz svođenje korisnika interneta na robu,
- kroz izloženost nadzoru,
- kroz izloženost sajber kriminalu i
- potencijalno kroz izloženost sajber ratovanju država.[331]

Ovde ćemo reći nešto više o gubicima, a potom o dobicima.

Običan korisnik u internet okruženju - gubici

Obični korisnik interneta danas, bio toga svestan ili ne, suočen je sa rizikom smanjenja ili gubitka privatnosti, makar se bavio samo najjednostavnijim aktivnostima na internetu. Osim toga, neretko se čuju i glasovi koji obezvređuju privatnost,a dolaze iz nekoliko sfera, od političke i kulturne do etičke i komercijalne. Zajednički im je stav da privatnost više nije (društvena) norma, da ni onaj kome pripada na nju ne gleda kao (ličnu) neprocenjivu vrednost.

Kulminacija „napada“ na privatnost je dovela do tačke kada se treba preispitati njeno značenje u post-Snouden eri. Obični korisnici su tada, ako ne i ranije, morali najjasnije primetiti i svoju izloženost i ranjivost na internetu i vrednost „svojih“ podataka (jer zbog čega bi oni bili prikupljani, izuzev zašto što imaju vrednost?). S jedne strane postoji država sa svojim bezbednosnim službama koje, sudeći po aferi Snouden, krše privatnost građana zarad nacionalne bezbednosti, a s druge strane u duhu skupljanja podataka postupaju i internet kompanije zarad sopstvenog profita, a na treći način to rade i sajber kriminalci.

Možemo se zapitati da li postoje neke uzročno-posledične veze između logika razmišljanja ovih aktera, pa čak i čuveno pitanje ko je prvi počeo. Po nekima stvari su tekle ovako: „Nije se NSA probudio jednog dana i rekao 'hajde da sve špijuniramo'. Oni su pogledali i rekli 'Hej, korporacije špijaniraju sve. Hajde da sebi nabavimo jednu kopiju'“.[332] To mišljenje deli i Pol Beran, koji podvlači:

> „Da podaci nisu najpre bili prikupljani od strane komercijalnih organizacija, vlasti ne bi bile u stanju da im pristupe, direktno ili indirektno, legalnim ili nelegalnim sredstvima. Da bi se ljudi zaštitili

[331] Iz razloga nedovoljne dostupnosti informacija i analiza, tema sajber ratovanje izlazi iz okvira ovog rada.

[332] Prema www.reformcorporatesurveillance.org a autor je Bruce Schneier, kriptograf i stručnjak za bezbednost. Citat postoji i kod Bernala, videti niže.

> od vladinih upada u njihov privatni život ... treba da se uzmu u obzir upadi, skupljanje podataka i čuvanje podataka od strane komercijalnih organizacija.“[333]

Moglo bi se desiti da je pre i jednih i drugih ideja pala na um kompjuterskim hakerima, posebno onom njihovom delu koji se okrenuo unosnom kriminalu.

Sajber kriminal, iako ima bezbroj formi, takođe u jednoj svojoj formi danas napada privatnost pojedinca preko kompanija. Primer takvog napada je slučaj iz 2011. godine kada su sajber kriminalci hakovali banku Sitigrup (Citigroup) i 360.000 računa njenih klijenata, pri čemu su od 3.400 klijenata uzeli novčane iznose od čak 2,7 miliona USD.[334] Klijenti banke nisu ništa pogrešno uradili, njihova jedina „greška“ je bila otvaranje računa u ovoj banci. Sajber napadi su se dešavali i na korisnike mreže video igara kompanije Sony, onlajn trgovinu Amazon itd. Kompanija koja se bavi zaštitom od virusa Symantec objavila je 2011. godine da je do tog momenta identifikovano 403 miliona varijanti virusa.[335] U šali su novinari čak nazvali 2011. godinu Godinom hakera.[336] Hakeri su napadali i manje kompanije. Kuningam je izričit: „Ako kompanije kao što je Citigroup ... ne mogu da zaštite informacije od povećanog hakovanja, privatnost podataka je nekako iluzorna.“[337]

Iz ovih primera može se zaključiti da povrede privatnosti korisnika interneta koje dolaze posredno, preko odnosa klijent-kompanija, jesu posledica prevelikog poverenja korisnika u kompanije. Ono je nekritčko, tim pre ako se uzme u obzir ponašanje kompanija (praćenje tragova veb sajtova) o kome smo govorili u poglavlju 5. Paradoksalno je da korisnici masovno (i često savršeno dobrovoljno) daju svoje lične podatke kompanijama, a ove ih masovno prikupljaju – i onda uzimaju još više (često tajno). Kao što je već rečeno, za ograničenje kompanijskog nadzora nad klijentima morali bi da ustanu oni koji su nadzirani, ti isti klijenti tj. korisnici interneta. To je za sada pod velikim znakom pitanja.

Smatram da je izuzetno važno podizanje svesti o ovoj ulozi koju bi sami korisnici trebalo da odigraju da bi se masovno prikupljanje podataka i nadzor stavili pod kontrolu. Ovde ću navesti nekoliko aktera koji deluju u tom smeru podizanja svesti.

---

[333] Paul Bernal, „The Right to be Forgotten in the post-Snowden era“ *Privacy in Germany*, No 5, 2014. Dostupno na http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2689685 str. 13.

[334] McKay Cunningham, “Privacy in the age of the Hacker: Balancing global privacy and data security law” u *The George Washington Interational Law Review*. Vol. 44, 2012. Dostupno na http://docs.law.gwu.edu/stdg/gwilr/PDFs/44-4/2-%20Cunningham.pdf Str. 644.

[335] Ibid. str. 685.

[336] Ibid. str. 673.

[337] Ibid. str. 646.

Kao prvo treba pomenuti pokret Reformcorporatesurveillance.org[338]. On je svojevrsna parodija na pokret najvećih internet kompanija protiv vladinog špijuniranja Reformgovernmentsurveillance.org (o kome će biti reči ubrzo) i, iako vizuelnim izgledom liči na internet stranicu moćnog konkurenta, zapravo te iste kompanije okupljene u Reformgovernmentsurveillance.org optužuje za pomaganje vladi kod nadzora građana. Reformcorporatesurveillance.org posebno upozorava javnost:

> „Kompanije poput Gugl, Fejsbuk, Jahu i Majkrosoft vam nude besplatne usluge u razmenu za vaše podatke. Drugim rečima, u razmenu za vašu privatnost i u krajnjem vaše građanske slobode. ... Ove kompanije zarađuju analizirajući vaše informacije i ponašanje kako bi kreirale vaš profil koji će prodati drugima. Vi niste njihov kupac, vi ste proizvod koji oni prodaju svojim pravim kupcima. Vi ste podatak koji se iskopava.“[339]

Nije baš jasno ko stoji iza ovog konkretnog sajta ili pokreta, što utiče na kredibilitet apela. Ipak zvuči privlačno ideja o alternativama korporacijskom internetu.

Logično je zapitati se zbog čega su usluge Gugla ili Fejsbuka ili Tvitera za nas, korisnike interneta, besplatne ili ko to plaća zapravo. Pretpostaviti da deo prihoda ovih kompanija dolazi od reklamne industrije je na mestu, ali efikasnost ovog reklamiranja ne uliva pouzdanje da je to celi odgovor. Deo koji upotpunjuje odgovor može biti da se sa tim stotinama miliona korisnika interneta (od čega smo mi deo) kreiraju serije podataka (od čega su naši podaci deo) koje su pogodne za buduću eksploataciju pomoću big-data analitike. Takva roba i u tim količinama, kao što su podaci sa Gugla, Fejsbuka, Tvitera i slično, nikada u ljudskoj istoriji nisu postojali. Zato se ni ne može znati hoće li big-data analitika na takvim podacima proizvesti štetne posledice po pojedince i društvo.

Na tome se vidi kako ozbiljna etička odgovornost leži na internet kompanijama koja grade takve sisteme gde se beleži sve o svakoj osobi u sistemu. One bi u nekom momentu bile stavljene pred koliko ekonomski toliko i moralni izbor da „prodaju“ svoje korisnike. Nema nikakvih garancija da bi odluka kompanije u tom momentu bila na primer izbor ispravne stvari, lojalan čin i sl.

[338] http://reformcorporatesurveillance.com/index.html
[339] http://reformcorporatesurveillance.com/index.html

Pomoć u podizanju svesti kod samih korisnika daje u tekstu „Praroditeljski greh interneta“[340] Itan Cukerman, koji objašnjava kako se stiglo do toga da „nadzor postane defoltni, ako ne i jedini, poslovni model interneta.“[341] On tvrdi da je praroditeljski greh interneta – oglašavanje. „Intenet nas špijunira na svakom ćošku ne zato što su Zakenberg, Brin i Pejdž intrigantski zlobni mozgovi nego zato što su dobre namere pošle po zlu.“[342] A evo i kako se to desilo:

> „Ono što smo hteli da uradimo je da izgradimo alat koji će olakšati svima bilo gde da dele znanje, mišljenja, ideje i slike slatkih mačaka. Kao što je svima poznato, imali smo nekih problema, pre svega problema oko poslovnog modela, koji su nas sprečili da uradimo ono što smo hteli na način kako smo se nadali da to uradimo.“[343]

Cukerman objašnjava da je u periodu 1994-1999. postalo jasno da jedini poslovni model koji omogućava finansiranje internet kompanija onaj u kome se nudi reklamiranje. Ujedno je „smišljen“ način reklamiranja sa pop-ap prozorima koji iskaču na internet stranici koju korisnik posećuje. Posebno taj tip oglasa izaziva iritaciju kod posetilaca internet stranica jer moraju da ga sklanjaju da bi došli do onog što ih stvarno zanima. Međutim, pokazalo se da su uvođenje oglašavanja plus stalni rast broja korisnika koji kompanija beleži bivali dovoljni da kompanija dobije finansiranje od investitora. Zato se još više polagalo na oglašavanje, a da bi oglašavanje vredelo više, da bi se isplatilo, mora da bude što više ciljano. „Dokazati da ćete targetirati više i bolje od Fejsbuka zahteva da odete dublje u svet nadzora.“[344] To često znači da se kompanija upušta u trgovinu informacijama sa drugim data-brokerima, na primer upušta se u praćenje mobilnih telefona korisnika da bi se skupljale informacije za složenije korisničke profile. „Jednom kada smo pretpostavili da je reklamiranje defoltni model za podršku internetu, sledeći korak je očigledan: potrebno nam je više podataka da bismo mogli da kažemo da su naši ciljani oglasi delotovorniji.“[345] Ono što je paradoksalno u tome je da su se korisnici interneta navikli na to, da sada očekuju da će sve što rade onlajn biti stavljeno u profil koji će automatski određivati koji oglasi i sadržaji će im se nabacivati. To je jedna vrsta

[340] Ethan Zuckerman. (14. avg.2014). „The Internet's Original Sin“ *The Atlantic* Dostupno na http://www.theatlantic.com/technology/archive/2014/08/advertising-is-the-internets-original-sin/376041/
[341] Zuckerman, opus cit.
[342] Zuckerman, opus cit.
[343] Zuckerman, opus cit.
[344] Zuckerman, opus cit.
[345] Zuckerman, opus cit.

dobrovoljnog učešća u eksperimentalnoj manipulaciji. Kod jednog broja korisnika je to izazvalo bes i ogorčenost, ali oni su ostali manjna; većina je istrenirana da je to u redu.

Dakle, način razmišljanja običnih korisnika, o kome Cukerman govori, bi bio otprilike ovakav: ako se otvorimo za sve veće i veće nadziranje, bilo od korporacija ili od vlada, alati i sadržaji koje želimo na internetu ostaće besplatni. A besplatnost je tu važna. Bez besplatnih sadržaja za takve korisnike, korisnička baza interneta bi bila daleko manja. Cukerman podseća da veći deo sveta ni danas nema kreditnu karticu, da sistemi za onlajn plaćanje nisu svuda dostupni, kao i da su troškovi mikrotransakcija često nerealni. To je ukratko izložen argument zašto je internet koji se finansira reklamama dobar. „Veb koji se izdržava od reklama raste brzo i otvoren je za one koji ne mogu ili ne žele da plate.“[346]

Ipak, spoj veba i reklama vodi ka eskaliranju prikupljanja podataka i nadzora nad korisnicima. Postoje i druge negativne posledice, kao što je na primer to da u takvom vebu bitni su samo klikovi, brojevi posetilaca na vebu, tzv. reklamerska metrika, a usmerenost na što više klikova srozava kvalitet sadržaja. No, to izlazi iz okvira ovog rada, gde je u našem fokusu nadzor i gubitak privatnosti.

Cukerman pominje i Macieja Ceglovskog (Maciej Ceglowski) koji je ovde zanimljiv jer je 2009. godine kreirao veb www.pinboard.in u kome nudi uslugu, koja se plaća, bezbednog beleženja sajtova koje korisnik posećuje na internetu, gledanja sajtova bez reklama i uz obavezu da podaci o korisniku nikada neće biti prodati trećoj strani. Poruka Ceglovskog je jednostavna: „Ako vi ne plaćate za svoje markiranje sajtova, to radi neko drugi, a njegovi interesi možda nisu u skladu sa vašim.“[347]

Po Cukermanu, to bi mogla biti inspiracija za debatu o budućim rešenjima zarađivanja na internetu, koja bi bolje štitila privatnost korisnika. Cukerman se pita: koliko bi koštalo kada bi Fejsbuk bio slobodan od oglasa i obećao da naš sadržaj i metapodatke neće prodavati nego će ih uništiti nakon nekog vremenskog perioda? Ili, da li bi Gugl pristao da platimo skromnu članarinu za njegove usluge pa da nas oslobodi ovog „očiglednog, surovog nadziranja“? Ceglovski smatra da je vreme da počnemo da plaćamo za privatnost i da podržimo usluge koje volimo a napustimo usluge koje su besplatne ali prodaju nas – svoje korisnike i našu pažnju – kao proizvod/robu.

Smatram da običan korisnik interneta danas mora doneti ličnu odluku o ovim temama.

---

[346] Zuckerman, opus cit.
[347] Prema www.pinboard.in

Običan korisnik u internet okruženju - dobici

Dobici koje običan korisnik ima od interneta su raznovrsni i nezanemarljivi. Kao što je već rečeno, ogledaju se u sferi slobode, politike, kulture itd.

Nova dimenzija individualne slobode je sintagma kod koje treba pokazati oprez. Tu imamo nekoliko različitih individualnih sloboda uguranih pod zajednički imenitelj. Prva individualna sloboda o kojoj se radi je sloboda izražavanja – ona ista davnašnja sloboda izražavanja čoveka, ali sada sa internetom ima svoju drugačiju, tehnički napredniju operacionalizaciju, postaje delotvornija nego u razdoblju pre interneta. Zatim tu je sloboda mišljenja – takođe davnašnja, ali uz pomoć interneta znatno olakšana, jer se operacionalizacija dolaženja do svih vrsta informacija tehnički drastično poboljšala i po-raznovrsnila (uz manju zavisnost od komercijalnih masovnih medija). Sledeća sloboda je sloboda organizovanja i udruživanja – jednako ne-nova u svojoj suštini ali jednako nova u svetlu mogućnosti. Zahvaljujući internetu, ljudi mogu ući u razne oblike saradnje kroz labavo povezivanje sa drugima, kroz širi spektar projekata (i onlajn i oflajn). Uzmimo na primer običan konferencijski poziv u kome ljudi iz različitih delova sveta komuniciraju kao da su u istoj prostoriji. Internet je i novi instrumenat za mobilizaciju pristalica. Tako imamo primere onlajn političke tribine gde kandidat za javnu funkciju putem interneta komunicira sa auditorijumom iz raznih delova zemlje u svrhe svoje predizborne kampanje, ili oragnizacije protesta na ulicama sa internom kao mestom obaveštavanja i izveštavanja. Ovako protumačena, sintagma „nova dimenzija ljudske slobode“ pravilno ukazuje da postoje novi aspekti u ljudskoj slobodi u informacionom okruženju, ali da ne diraju u ono što je kao srž slobode postajalo i pre pojave interneta.

Na polju kulture internet je izazvao brojne promene, verovatno veće ako se kultura tumači kao kulturna industrija nego ako se kultura tumači kao individualno strvaranje kulture i kreativnost. Diskusija te teze izlazi iz okvira ovog istraživanja. Samo kao napomena, može se reći da je internet učinio kulturu transparentnijom i dostupnijom, i dinamizovao kulturnu produkciju. U jednoj rečenici taj uticaj bi se mogao sažeti kao retoričko pitanje: „Da li će postojati ijedan neobjavljeni pesnik u 21. veku?“[348]

[348] Autor rečenice je Eben Moylen, a navedeno prema: Lowrence Lessig, *Code: version 2.0*. (2006). New York, Basic Books. str. 236.

O uticaju interneta na kreativnu industriju (uključujući i individualnog kulturnog stvaraoca) govori se u knjizi *Slobodna kultura* Lorensa Lesiga. On kaže: „... u ovoj knjizi nije toliko reč o samom internetu. Ovde su u pitanju posledice koje ostavlja internet na deo naše tradicije ... Ta tradicija je način na koji se stvara naša kultura.“[349]

Na prelazu milenijuma internet je izazvao veliku debatu o tretiranju intelektualne svojine i autorskih prava na internetu nakon što je masovna intelektualna piraterija upalila alarm čitavoj kreativnoj industriji i industriji zabave - zbog gubitka prihoda. Rezime tih turbulencija je taj da su ključni akteri shvatili da internet ireverzibilno menja odnos snaga i da treba naći srednje rešenje, tako da je uspostavljena ravnoteža na tom tržištu. Čuveni Nepster, softver za masovno (nelegalno) deljenje muzike, je ugašen ali zato funkcionišu skladno Google Play Store i iTunes.

U odnosu na politički sistem, uticaj inteneta je delovao pre svega kroz novu restrukturisanu javnu sferu. Ova javna sfera je nova odnosno različita od prethodnih po tome što ima kao svog aktera pojedinca sa više moći (koju generiše internet). To je pojedinac koji jeste ili može biti ne samo angažovaniji nego i „opasniji“ i efikasniji posmatrač društvenog i političkog prostora, učesnik u javnim debatama, zagovornik neke svrhe ili cilja. „Opasan“ u ovom kontekstu znači „teže ga je pobediti“, jer je efikasniji tehnološki, organizaciono i na druge načine. Ovaj savremeni internetom-podržan učesnik javne sfere je zaslužan za nekoliko postignuća koja polako ulaze u glavni tok (na engl. mainstream) savremenog društvenog i političkog života.

Prvo postignuće je decentralizovano vršenje funkcije psa čuvara (watchdog) političkog i društvenog sistema. Sa bilo koje strane, a ne samo iz očekivanih institucionalnih kanala, mogu u javnost isplivati važne informacije koje zahtevaju korektivne intervencije u političkom i društvenom sistemu. Primer toga je veb Vikiliks, o čemu će biti reči kasnije.[350]

Drugo postignuće je oživljavanje društvenih pokreta koji traže reforme političkog sistema, bilo da se radi o slobodnim demokratskim državama (na primer u SAD-u pokret occupy.org iz 2011. godine) ili o neslobodnim autoritarnim državama (na primer Arapsko proleće). Moguće je da bi do ovih pokreta došlo i bez interneta, ali ex-post-facto znamo da su se inicijatori pokreta oslanjali na onlajn kanal delovanja i iz njega crpli više moći nego što bi imali u svetu bez interneta.

[349] Lorens Lesig. (2006). *Slobodna kultura*. Beograd: Službeni glasnik. Str. 9-10.

[350] Misija Vikiliksa (Wikileaks) je da prima informacije od uzbunjivača, da ih pruži javnosti na uvid i da se onda brani od neizbežnih pravnih i političkih napada. Najpoznatiji poduhvati objavljivanja do sada su bili iz 2010. godine kolateralno ubistvo, irački ratni dnevnici i tajni diplomatski telegrami SAD.

O novoj informacionoj ekonomiji (na internetu zasnovanoj ekonomiji) bilo je reči u poglavlju 7. U smislu u kome se ovde radi, kao dobitku za običnog korisnika interneta u vidu otvaranja lakšeg pristupa globalnom tržištu i ekonomskim akterima širom sveta sa kojma bi mogao da posluje, internet jeste odigrao pozitivnu ulogu. U određenoj meri internet daje troškovno efikasniji kanal prodaje i šansu za uključivanje u proizvodne saradnje sa drugima (na primer kroz crowdfunding – finansiranje poduhvata prezentiranih na određenim platformama). Međutim, taj dobitak ne treba preuveličavati,[351] posebno imajući u vidu da je najveći ekonomski uspeh pripao kompanijama baziranim na inovativnosti i preduzetništvu posebnog tipa, koje su bile blagoslovene spremnošću investicionih fondova da ih podržavaju. Ta dva sastojka su odredila glavnu dinamiku internet ekonomije u smislu Silikonske doline, o čemu je bilo reči u poglavlju 7. Za veliku većinu običnih korisnika, koji ne žive u Silikonskoj dolini, ili koji nisu do te mere inovativni, ekonomska korist od interneta je skromnija.

Internet okruženje i pristup kuturi i obrazovanju (studija slučaja)

Doprinos interneta razvoju kulture i obrazovanja može se sagledati kroz fenomen platformi za onlajn učenje i masovnih otvorenih onlajn kurseva na njima.

Platforma za onlajn učenje je najprostije rečeno internet stranica na kojoj se nalazi ponuda gotovih akademskih kurseva iz raznih oblasti, koje bilo ko može da odabere i besplatno konzumira/pohađa onlajn (dolaskom na internet stranicu / kurs). Pošto je termin „(obrazovni) kurs“ prisutan i u oflajn delu života, preciznije je ovu vrstu koja je onlajn nazvati MOOK[352] Na platformama dominiraju MOOK-ovi na engleskom jeziku, ali postoji jedan broj na drugim svetskim jezicima. MOOK se može opisati kao interativni udžbenik smešten na internetu, u kome se nalaze unapred pripremljeni materijali, kao što su tekstovi, filmovi (video), primeri za vežbu, kvizovi, projekti i dr.

[351] Verujemo da je Benklerov stav preoptimističan odnosno netačan, ali vredi ga citirati zbog utopijskog prizvuka vizije takvog sveta: «Kadgod neko negde ... poželi da napravi nešto što zahteva ljudsku kreativnost, uz kompjuter i priključak na mrežu, on ili ona to može da napravi – sam/a ili u saradnji sa drugima.» Benkler tu podrazumeva: jer će već naći kapital koji je potreban da se to napravi. Ono što želi da istakne je da mreža omogućava ljudima da sarađuju kao ljudska i kao društvena bića, a ne kao tržišni akteri kroz sistem cena.

[352] Na engl. Masssive open online course, skr. MOOC

Polaznik[353] MOOK-a ima mogućnost da se poveže sa drugim polaznicima istog MOOK-a u delu koji se naziva forum, gde se diskutuje o idejama, materijalima za kurs, ali i bilo čemu drugom. Može i da onlajn komunicira, u unapred jasnim terminima, sa profesorima i osobljem zaduženim za taj MOOK. Sem toga, svaki MOOK ima predviđen sistem ocenjivanja stečenog znanja polaznika, i u slučaju da polaznik zadovolji kriterijum, može dobiti sertifikat o svom stečenom znanju i veštinama. Taj sertifikat je besplatan, ali njegova papirna (validnija) vrsta, koju bi nosilac sertifikata koristio na tržištu rada na primer se plaća 49 USD (naravno, i samo plaćanje je onlajn).

Dve najpoznatije platforme za onlajn učenje pokrenute su 2012. godine u SAD-u. To su:

- Coursera – koju su pokrenuli naučnici bliski univerzitetu Stanford i
- edX – koju su zajednički pokrenuli univerziteti MIT i Harvard.

Karakteristično za platformu Coursera je da je u samom startu ponudila dva MOOK-a na teme koje su inače najaktuelnije i u o oflajn univerzitetskom sistemu SAD-a. To su neuronauka – MOOK *Learning How To Learn* (autori Barbara Oakley i Terry Sejnowski) i data-nauka (analitika podataka) – MOOK *Mashine Learning* (autor Andrew Ng). Oba MOOK-a su imala milionski auditorijum. Broj ponuđenih MOOK-ova se meri stotinama, a realizuju se kroz partnerstvo sa više stotina fakulteta i ustanova. Misija Coursera platforme glasi: "Mi pružamo univerzalni pristup najboljem obrazovanju na svetu."[354]

Platforma edX je ima za misiju: „povećati pristup visokokvalitetnom obrazovanju za svakog bilo gde da se nalazi, poboljšati nastavu i učenje u kampusu i onlajn i unaprediti nastavu i učenje kroz istraživanje."[355] Po sopstvenim rečima, jedina su platforma koja je i neprofitna i bazirana na otvorenom kodu, što znači da svi nastavnici i tehnički stručnjaci, bilo gde da se nalaze na planeti, mogu uzeti ovaj softver, po želji ga koristiti ili menjati. Umesto da svaki fakultet, institut itd. kreće od nule i pravi svoj kod za internet udžbenik odnosno MOOK, može uzeti ovaj već dostupan kod i uneti samo sadržaje koje želi. Oni ambiciozniji mogu da doprinesu inovacijama koda, tj. ponuditi još bolje karakteristike ovoj platformi, na korist onima

[353] Reč polaznik, iako u muškom rodu, u ovom radu se koristi tako da označava polaznike oba pola. Takođe važi i za reč korisnik.
[354] https://www.coursera.org/about/
[355] https://www.edx.org/about-us

koji uče. edX ima u ponudi preko 650 kurseva iz društvenih nauka, matematike i kompjuterskih nauka, a na ovim MOOK-ovima je radilo oko 1700 nastavnika/saradnika. edX daje i podatak da su od nastanka do danas izdali preko 580.000 sertifikata onima koji su učili i završili njihove MOOK-ove. Smatra se da imaju preko 5 miliona polaznika.[356]

Broj sertifikata je zapravo bolno mesto ovog koncepta obrazovanja. Smatra se da su platforme za onlajn učenje u tri godine postojanja na svim MOOK-ovima uspele da privuku oko 25 miliona polaznika, ali je broj polaznika koji su završili svoj započeti MOOK veoma mali, čak ispod 10%. Takav stepen odustajanja je lošiji od rezultata univerzitetskog obrazovanja u realnom životu i još uvek se utvrđuju njegovi razlozi.

Po nekim istraživanjima o tome ko su korisnici platformi za onlajn obrazovanje ispada da je 60% njih iz razvijenih zemalja (članica OECD), 60% njih ima stalno zaposlenje i 80% njih već ima najmanje osnovnu diplomu fakulteta (BA). Ovom profilu ljudi MOOK-ovi su zanimljivi kao intelektualna razonoda, drugim rečima nije toliko presudno da im pohađanje MOOK-a obezbedi opipljive profesionalne ili obrazovne koristi. Međutim, jedan od motiva za kreiranje MOOK-ova je otvorenost tj. dostupnost za neprivilegovane, kako u razvijenim zemljama tako i u zemljama u razvoju. MOOK entuzijasti naglašavaju da je veliki broj korisnika MOOK-ova iz Indije i Kine i da ovi korisnici ipak u solidnim procentima „prijavljuju“ da imaju i opipljive koristi od ovakvog učenja.

U svom tekstu za *Wall Street Journal*, osnivačica Coursera platforme Dafne Koler objašnjava gde vidi tržište za njih:

> „Pogledajte Indiju, koja ima 600 miliona ljudi mlađih od 25 godina i zastareo univerzitetski sistem koji se muči da stvori radnu snagu koja je potrebna za treću najveću ekonomiju sveta. Jedna analiza od pre nekoliko godina je pokazala da, da bi se zadovoljile te obrazovne potrebe korišćenjem tradicionalnih metoda, Indija bi morala da izgradi 1500 kampusa i da nađe, što je poseban izazov, kvalitetno osoblje koje bi radilo u njima.“[357]

Ona takođe vidi veće potrebe za obrazovanjem i u SAD-u, navodeći da ljudi koji danas imaju preko 50 godina promenili su posao u svom radnom veku prosečno 11,3

---

[356] Analiza o polazniicma za prve dve godine postojanja je u sledećem izveštaju: Ho, A. D., Chuang, I., Reich, J., Coleman, C., Whitehill, J., Northcutt, C., Williams, J. J., Hansen, J., Lopez, G., & Petersen, R. (2015). *HarvardX and MITx: Two years of open online courses* (HarvardX Working Paper No. 10). doi:10.2139/ssrn.2586847

[357] Daphne Koller. (26. april 2015). “The Future of College: It’s Online” *The Wall Street Journal*, Dostupno na http://www.wsj.com/articles/the-future-of-college-its-online-1430105057

puta, i to je trend koji se nastavlja; pretpostavka je da novi posao zahteva nova znanja i veštine. U tom smislu, bolje obrazovanje uz manje troškove ima svoje sigurno mesto. Kad je reč o troškovima, po Kolerovoj, navodno se cena pravljenja jednog onlajn kursa kreće od 40 hiljada do 325 hiljada USD.[358]

Postoje i kritike uperene ka onlajn obrazovanju.

Uočava se tenzija i razlika u potrebama između dve grupe korisnika MOOK-ova: jednih koji traže lično intelektualno obogaćivanje (i pohađaju MOOK jer vole da uče) i drugih koji su orijentisani na karijeru (i pohađaju MOOK jer traže smislenu diplomu za tržište, posebno u oblastima kompjuterskih nauka gde u zemljama u razvoju postoji manjak specifične radne snage). Ukoliko se za svaku grupu ne uvede ono što joj je potrebno, to bi moglo smanjiti popularnost ovog koncepta obrazovanja.

Dejvid Bromvič (David Bromwich) sa Jejla smatra da „MOOK pokret ide uz bok sa tendencijom mehanizacije obrazovanja“ i „obeshrabruje složenije promišljanje o sadržini i ciljevima obrazovanja“.[359] Na to mu Barbara Oklej, gore pomenuta autorka najpopularnijeg MOOK-a, odgovara ovako:

> „Ja upućujem izazov kritičarima MOOK-a. Napravite sopstveni onlajn kurs. Snimite kamerom najzanimljivije, najdublje predavanje koje ste ikada održali u svom životu. Ako ne mislite da je vaše predavanje dovoljno dobro, snimajte ga ponovo dok ne budete zadovoljni njime. Objavite svoj video da bude dostupan milionima studenata širom sveta, ne samo onoj nekolicini privilegovanih na vašim časovima. Smislite takva pitanja za kviz na kojma najviše vaši studenti greše. Naučićete više nego što sada znate o dometu i mogućnostima MOOK-ova.“[360]

Za potrebe ovog rada, autorka je lično isprobala obe platforme za onlajn učenje u periodu 2014-2016. Registrovala se kao polaznica na 12-ak MOOK-ova iz oblasti društvenih nauka i umetnosti, od čega su 2 MOOK-a bila iz oblasti filozofije, po jedan na Coursera i edX. Ponuda filozofskih MOOK-ova u katalozima i Coursera i edX je u rasponu 5-10 kurseva, što je u ravni sa ponudama iz oblasti umetnosti. Autorka je ciljano odabrala 2 filozofska MOOK-a koja će pohađati tako da: bude po 1 sa svake platforme, da bude 1 američki i 1 evropski, da po tematici što bliže pokrivaju kurseve

[358] Iz intervjua sa Julijom Stiglic iz Coursera. Roger Ridall. (13. mart 2015). “Coursera’s Stiglitz: MOOC revolution is just beginning [SXSWedu2015]” *Educatin Dive* Dostupno na http://www.educationdive.com/news/courseras-stiglitz-mooc-revolution-is-just-beginning-sxswedu-2015/374642/

[359] Prema Barbara Oakley. (29. okt. 2015). “Why Virtual Classes Can Be Better Than Real Ones” Dostupno na http://nautil.us/issue/29/scaling/why-virtual-classes-can-be-better-than-real-ones

[360] Oakley, opus cit.

koje je autorka u sklopu osnovnih studija filozofije 1990-tih pohađala na Filozofskom fakultetu Univerziteta u Beogradu.

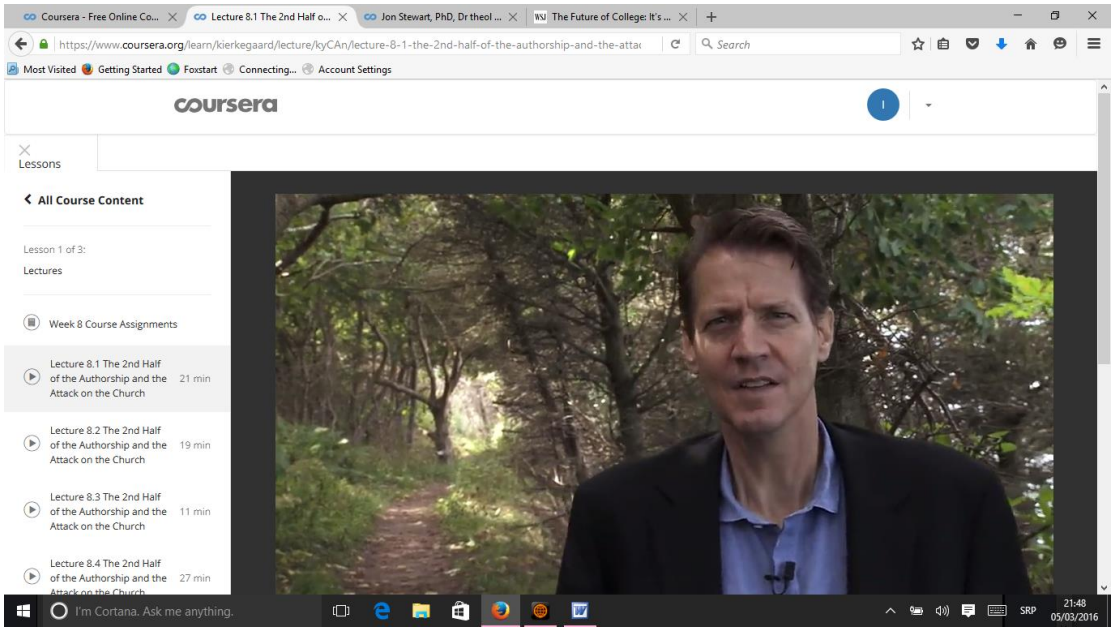
MOOK posvećen filozofiji Serena Kjerkegora, pod nazivom *Soeren Kierkegaard – Subjectivity, Irony and the Crisis of Modernity*, približno odgovara delu kursa iz Istorije filozofije III iz vremena studiranja autorke. MOOK je napravio i na Coursera platformi postavio Teološki fakultet sa Univerziteta Kopenhagen. Autor MOOK-a je prof. Jon Stjuart (Jon Steward) iz Centra za studije Kjerkegora. MOOK ima trajanje od 8 nedelja. (Autorka je pohađala od 6. oktobra do 10. decembra 2014. godine. To je bilo vreme za „uživo" održavanje kursa, a ovaj MOOK je dostupan i bilo kada u toku godine za pohađanje „po svom ritmu".) Organizovan je kroz 8 predavaja i 8 kvizova vezanih za ta predavanja, koja nose nazive: Kjerkegorov život i rad kao „sokratski zadatak", Kjerkegor, Martensen i hegelijanizam, Kjerkegorovo shvatanje Sokrata, Kjerkegor, Hajberg i istorija, Kjerkegor, Miler i Šlegel, Put u Berlin i početak autorstva, Razvoj pseudonimiranih dela, Drugi deo autorstva i napad na crkvu. Uz predavanja su dostupni slajdovi. U zadnjoj nedelji kursa piše se esej od 2.000 reči na temu vezanu za kurs. Esej ocenjuju anonimno drugi polaznici kursa, prema jasno obrazloženim kriterijumima i instrukcijama. Svaki polaznik koji je priložio svoj esej na ocenjivanje ima istovremeno obavezu da oceni barem 3 rada drugih polaznika koja mu se anonimno dodeljuju ("jer je i ocenjivanje tuđih radova bitno u procesu učenja").. Za sva predavanja dostupna je literatura razumnog obima (relevantni odlomci inače veoma obimnih dela) na engleskom jeziku. Time se jasno ističe da je MOOK namenjen međunarodnom „tržištu" a ne nužno studentima u Danskoj. Posebni dodatni kvaliteti kursa su:

- kratki intervjui sa gostima, tj. predavačima sa drugih fakulteta koji su specijalisti za Kjekregora i
- snimanje predavanja na preko 20ak lokacija (interijera i eksterijera) u Kopenhagenu.

Nije postojala nijedna tehnička greška vezana za odvijanje MOOK-a tokom navedenog vremena pohađanja.

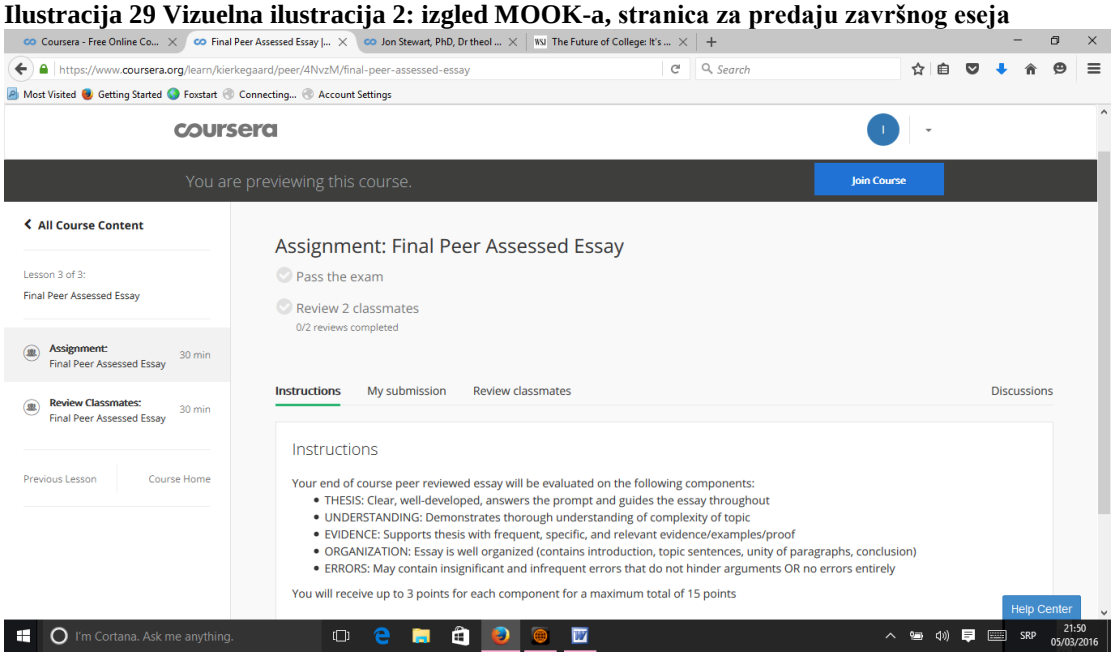
Donosimo par vizuelnih ilustracija ovog MOOK-a

Ilustracija 28 Vizuelna ilustracija 1: izgled MOOK-a, deo predavanja iz osme, zadnje nedelje kursa



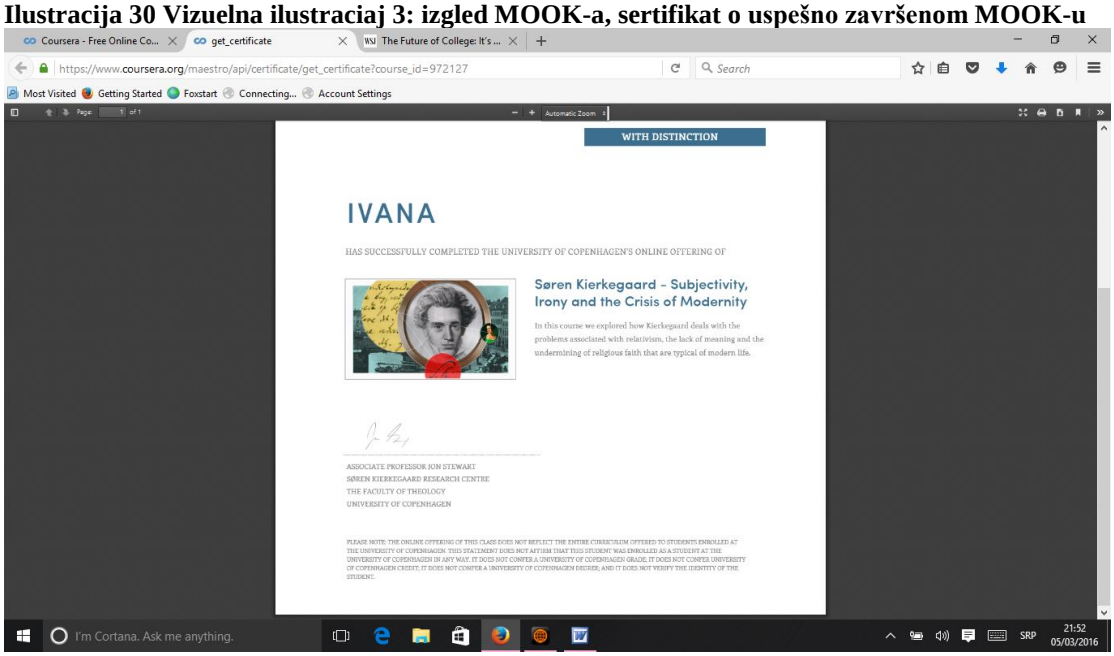
Preuzeto sa www.coursera.com

Ilustracija 29 Vizuelna ilustracija 2: izgled MOOK-a, stranica za predaju završnog eseja



Preuzeto sa www.coursera.com

Ilustracija 30 Vizuelna ilustraciaj 3: izgled MOOK-a, sertifikat o uspešno završenom MOOK-u



Preuzeto sa www.coursera.com

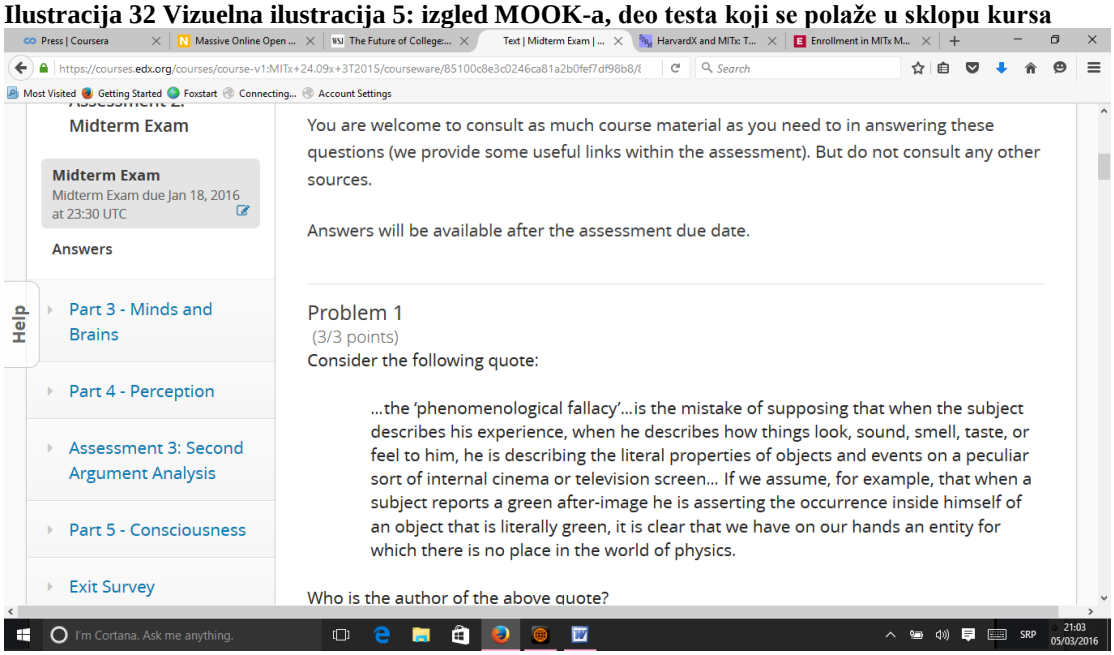
MOOK posvećen savremenoj analitičkoj filozofiji, pod nazivom *Minds and Mashines* približno odgovara delu kursa iz Istorije filozofije IV iz vremena studiranja autorke. MOOK je pripremio i postavio na edX platformi američki MIT (Tehnološki institut Masačusec). Autor MOOK-a je prof. Aleks Birn (Alex Byrne), šef odeljenja za filozofiju na tom fakultetu. MOOK ima trajanje od 16 nedelja. (Autorka je pohađala od 17. novembra 2015. do 07. marta 2016. godine. To je bilo vreme za „uživo“ održavanje kursa. Kurs nije dostupan u svako vreme u toku godine tj. za pohađanje „po svom ritmu“.) Literatura za ovaj kurs je uključivala 25 tekstova, među kojima su radovi Dekarta (R.Descartes), Serla (J.Searl), Turinga (A.Turing), Čerčlanda (P.Churchland), Bloka (N.Block), Rajla (G.Ryle), Patnama (H.Putnam), Kripkea (S.Kripke), Smarta (J.Smart), Plejsa (U.Place), Vilijamsona (T.Williamson), Hardina (C.Hardin), Monda (B.Maund), Nejgela (T.Nagel), Džeksona (F.Jackson), Čalmersa (D.Chalmers), Taja (M.Tye) i drugih. Tekstovi, ukoliko su dužeg obima, su prilagođeni u smislu da je njihova integralna verzija komprimirana tako da samo pojedini delovi, relevantni za MOOK, stoje u izvornom obliku, a ostali delovi su maksimalno parafrazirani (na par rečenica). Tekstovi su sukcesivno „otvarani“ kao priprema za predavanja. MOOK se sastoji od 25 video snimaka predavanja (održanih u amfiteatru fakulteta), sa dostupnim slajdovima, 4 testa koja se ocenjuju i više primera test pitanja koja se ne ocenjuju. Nije bilo gostujućih predavača. Postojale su manje tehničke greške (na pr. zabune šta je pod kojim brojem videa, potreban tekst

nije u rečenom terminu okačen, greška u testu i sl.) vezane za odvijanje MOOK-a tokom navedenog vremena pohađanja, ali su veoma brzo ispavljane (u roku od 1 dan). Donosimo par vizuelnih ilustracija ovog MOOK-a.

Ilustracija 31 Vizuelna ilustracija 4: izgled MOOK-a, deo predavanja iz druge nedelje kursa

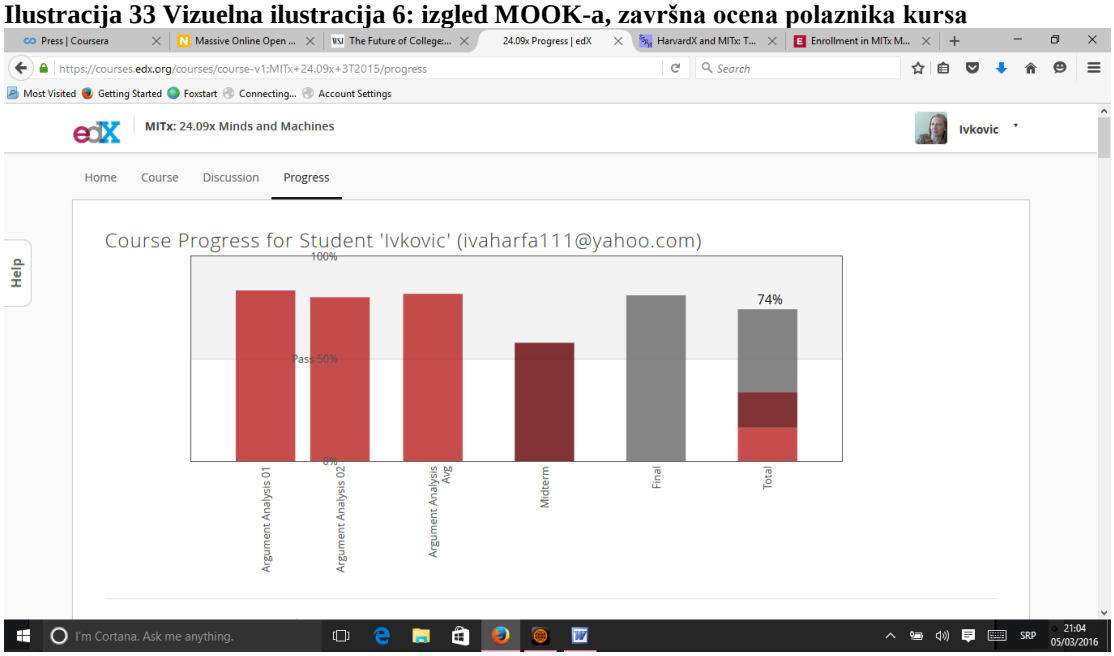
Preuzeto sa www.edx.org

Ilustracija 32 Vizuelna ilustracija 5: izgled MOOK-a, deo testa koji se polaže u sklopu kursa



Preuzeto sa www.edx.org

Ilustracija 33 Vizuelna ilustracija 6: izgled MOOK-a, završna ocena polaznika kursa



Preuzeto sa www.edx.org

Ono što određuje korisničko iskustvo polaznika ova dva kursa je utisak jasnoće, organizovanosti, tehničke besprekornosti, doslednosti i podudarnosti između najavljenog i realizovanog. Veliki konfor dolazi od mogućnosti da se kurs pohađa u vremenu po izboru polaznika (bilo koje doba dana i nedelje) i od dostupnosti potpune literature samo jednim klikom. Sticanje znanja je potpomognuto diskusijama na forumima. Efikasnost učenja povećana je time što se teški delovi mogu sporije i višekratno prelaziti i što je moguće dobiti korisne odgovore na forumu. Stalan i lak uvid u sopstveni progres kod polaznika jača odlučnost da se kurs proprati do kraja. Svaki detalj je podešen tako da se ostvari maksimum znanja u vremenu koje će polaznik posvetiti tom MOOK-u.

U korisničkom iskustvu u MOOK-u *Minds and Mashines* prisutan je osećaj da niste vi ti kojima se obraća predavač. Za to je odgovoran sam izbor scenarija odnosno odluka da se snima aktuelno predavanje u amfiteatru gde postoji interakcija predavač-studenti – a samim tim nema obraćanja onima koji tome pristupaju preko interneta, oni ostaju van okvira dešavanja. Nasuprot tome, MOOK *Soeren Kierkegaard – Subjectivity, Irony and the Crisis of Modernity* je osigurao da predavač deluje kao da se obraća baš vama koji ga pratite, što je mnogo prijatnije i stimulativnije za učenje.

Ako se poredi učenje filozofije putem onlajn platforme i učenje filozofije oflajn, na konvencionalan način na fakultetu, može se zaključiti da su svi aduti na strani onlajn učenja osim jednog: mogućnosti da se razvije osećaj pripadnosti grupi. U onlajn

učenju, čak iako je jasno da hiljade i hiljade ljudi uče, ili pokušavaju da uče, istovremeno i isto što i vi, ne postoji nikakav osećaj zajednice, grupe, istovremenog prisustva, gužve. To je izraženo individualna aktivnost, pa čak i sterilna izolacija po defoltu, gde se samo eventualno uz znatan trud može uspostaviti povezanost. Nasuprot tome, učenje na konvencionalan način na fakultetu ima prednost da je polaznik deo grupe i grupa je po defoltu (početno stanje), a distanciranje od grupe eventualno opcija po izboru.

Na bazi sopstvenog korisničkog iskustva kao i šireg razmatranja fenomena platforma za onlajn učenje, autorka zastupa mišljenje da je ovaj vid učenja veoma pogodan za učenje filozofije i da može znatno i troškovno veoma efikasno da unapredi nivo znanja kako obrazovanih filozofa tako i početnika.

Internet okruženje i politički aktivizam

Pojam politički aktivizam se u ovom radu uzima u značenju preduzimanja odlučne akcije (najčešće u formi protesta ili demonstracija) za postizanje određenog političkog cilja oko koga postoji neka kontroverza u društvu.

Razmatranje pitanja šta se dešava sa političkim i uopšte društvenim aktivizmom u eri interneta najčešće se svodi na polemiku oko toga da li je internet neutralan, i ako nije, na čijoj je strani: naklonjeniji onima koji učvršćuju slobodu ili naklonjeniji onima koji učvršćuju kontrolu.

Ovo je u mnogome jedna uska vizura preuzeta iz ugla spoljne politike. Većinski stav (a i stav zvaničnog SAD-a) je da je internet „radi za“ borce za slobodu i demokratiju i da doprinosi rušenju autoritarnih režima. Suprotno mišljenje zastupa teoretičar interneta, Amerikanac beloruskog porekla, Evgenij Morozov. Svoja gledišta je izneo kroz novinske istupe kao i u knjizi *Internet obmana: mračna strana slobode interneta*.[361] On objašnjava da je vera u moć interneta da demokratizuje društva potekla iz „kuhinje“ neokonzervativaca u SAD-u (za vreme mandata Džordža W. Buša) i da odražava paradigmu hladnog rata koja je ovim zvaničnicima bila bliska.

Kori Doktorou se slaže sa tim objašnjenjem.

[361] Evgeny Morozov. (2011). *The Net Delusion: The Dark Side of Internet Freedom*, New York: Public Affairs.

> „Morozov je u pravu kad tvrdi da zapadni političari imaju simplicističko shvatanje o odnosu interneta prema spoljnoj politici, ali to nije samo problem sa spoljnom politikom – isti političari fantastično ne shvataju ni posledice interneta po autorska prava, slobodu govora, obrazovanje, zapošljavanje i svaku drugu temu koja je bitna.“[362]

Koliko hladnoratovska paradigma ne pogađa suštinu uticaja interneta u savremenom svetu Morozov pokazuje i razgrađujući lažnu analogiju između berlinskog zida i sajber zida. Po njoj, fizičke zidove je jeftinje srušiti nego sagraditi; sa njihovim digitalnim ekvivalentima je obrnuto - jeftinje sagraditi nego srušiti. Isto tako, jednom kada su fizički zidovi srušeni, neće se pojaviti novi, ali kada se jedne digitalne barijere uklone, javljaju se nove i potpuno različite barijere na njhovom mestu. Kontrola na interntu uzima razne forme i ide dalje od pukog blokiranja sajtova.

Osnovni stav koji Morozov brani bi glasio: internet neće osloboditi svet. Diktatori tj. autoritarni režimi opstaju. Štaviše, oni počinju da primenjuju digitalnu represiju (i to je upravo ona „mračna strana slobode interneta“); za ovaj osnovni stav se kod Morozova može naći niz potkrepljujućih empirijskih primera.

Jedan od najjasnijih primera su zbivanja u Iranu 2009. godine, kada su održani izbori na kojima je pobedio Mahmoud Ahmadinejad, a nakon njih je usledila kriza oko uspostavljanja vlasti zbog narodnog protesta protiv ovog vođe (masovne demonstracije i sl.). Za vreme ovih događaja na društvenoj mreži Tviter (inače kompaniji u američkom vlasništvu) razvila se veoma živa aktivnost, otelotvorena u broju i učestalosti tvitova, koje su slali Iranci koji žive u emigraciji i Iranci koji žive u zemlji. Tviter se u glavnom koristio da se objave protesti koji se već dešavali i da se pažnja sveta usmeri na činove nasilja koje je počinio režim.[363] Međutim, u nekom momentu je Džered Koen (Jared Cohen) zvaničnik iz američkog Stejt departmenta poslao mejl kompaniji Tviter kako bi je zamolio da odloži svoje planirano održavanje sistema kako bi Iranci mogli nesmetano da koriste mrežu. U imejlu je upotrebio reči koje bi se mogle parafrazirati kao: u toku „Tviter revolucija“.

Mnogi stručnjaci su to hitro negirali. Na primer, David Rotkof je objasnio: tako nešto kao što je virtuelna revolucija ne postoji, Tviter revolucija je preterivanje (over-

[362] Cory Doctorow. (25. jan. 2011). “We need a serious critique of net activism” *The Guardian*, Dostupno na http://www.theguardian.com/technology/2011/jan/25/net-activism-delusion

[363] Evgeny Morozov. (17.jun 2009). “Iran Electins: A Twitter Revolution?” *The Washington Post*, Dostupno na http://www.washingtonpost.com/wp-dyn/content/discussion/2009/06/17/DI2009061702232.html

statement).[364] Sam Morozov to formuliše: tvitovi ne ruše vlade, ljudi ruše vlade. A zapravo, tvrdi dalje ovaj autor, ti ljudi koji ruše vlade su nakon ovakvog gesta iz Stejt departmenta imali samo više problema, budući da su iranske vlasti postale opreznije, promenile dotadašnje shvatanje interneta kao sredstva ekonomskog razvoja. Zapadna ubeđenost u oslabađajuću moć tehnologije „uznemirila je" vladajuće strukture u Iranu koji pre toga nisu bili zainteresovani za kontrolu interneta i - oni su počeli da kontrolišu internet. Pošto su im Amerikanci blago rečeno rekli da internet „radi" protiv njih, iranske vlasti su uhvatile toga da pretvore internet u alat za špijuniranje i propagandu prema svojim građanima. Jer, kao što Morozov, tačno primećuje i podseća: diktatori nisu budale ili ludaci već ekstremno bistri i tehnički pismeni političari.

Morozovljevo gledište se može donekle prihvatiti, ali po autorki ovog rada, treba zaobići vizuru iz ugla spoljne politike i «širenja demokratije». Jer, taj slučaj Irana je imao ograničeno vreme trajanja i već je prevaziđen. Od tada se pojavio novi fenomen širenja radikalnog islamskog fundamentalizma putem interneta. Pripadnici pokreta Islamska država Iraka i Levanta (ISIL) putem inerneta objavljuju snimke brutalnog ubijana svojih protivnika i uništenja kulturnog nasleđa, kako bi izvezli strah građanima zapadnog sveta. Stoga, ne treba ostati na primerima već treba dostići apstraktniji uvid u interakciju interneta, represije i aktivzima u načelu.

Neosporno je to da je internet zaista instrument, alat preko koga zagovornici bilo čega i protivnici bilo čega imaju efikasan sistem komunikacije i organizacije. Internet jeste veoma pomogao medijskom sukobljavanju između disidenata i najrazličitijih režima protiv kojih se oni bune. U Iranu internet je protestante stavio rame uz rame sa režimom, koji je na drugim poljima daleko moćniji od njih. Internet ojačava i disidente i vlast ali ih ojačava disproporcionalno, više ojačava disidente nego vlast, samim tim što potire ono u čemu je vlast već bila u prednosti (kontorlisane kanale komunikacije). Možemo da uočimo da je za aktivizam na internetu glavna odlika upravo (na internetu zasnovana) redistribucija moći u načelu.

Ako se pogleda tzv. Orvelova trilogija autoritarizma: cenzura, propaganda i nadzor,[365] i pretpostavi da ona postaje digitalna trilogija, postavlja se pitanje da li se digitalni aktivisti mogu boriti sa ovim snagama?

---

[364] David Rothkopf. (17. jun 2009). "There's no such thing as a virtual revolution" *Foreign Policy*, Dostupno na http://foreignpolicy.com/2009/06/17/theres-no-such-thing-as-a-virtual-revolution/

[365] Sintagmu koristi Morozov. Opus cit.

U domenu cenzure, tehnologija omogućava i efiksnije cenzurisanje (režimu) i efikasnije izbegavanje cenzure (aktivistima), tako da je tu rezultat izjednačen.
U domenu propagande, režimi mogu koristiti botove i/ili pristalice za svoju digitalnu propagandu, mogu ostaviti kritički sadržaj onlajn i krenuti da se suočavaju sa tim kritičkim sadržajem tako što (preko botova i otvoreno) daju svoju verziju događaja, paralelno sa verzijom događaja koju daju aktivisti. Tu nema garancija koja strana će nadvladati. Čini se da je i na ovom polju rezultat (režim protiv oponenata) izjednačen.
U domenu nadzora, pak olakšani nadzor putem interneta daje veću moć autoritarnoj strani koja ima cilj da vrši digitalnu represiju. Represivne vlade mogu da prate onlajn aktiviste preko virusa, malvera, gps-a na mobilnim telefonima i sl. No to isto mogu da rade i hakeri, koje aktivistički krugovi mogu da kooptiraju te da onlajn špijuniraju vladu. U skladu sa sloganom: «Mi gledamo, mi smo gledani i mi se gledamo» aktivisti mogu da fotografišu ili snime i stavljaju na internet sve nepopularne i nezakonite postupke vlade. Za to im je potreban samo mobilni telefon. A uvek postoji i opcija enkripcije, o kojoj je već bilo reči. Odnos snaga je još jednom izjednačen.
Na osnovu toga, autorka je na stanovištu da je netačno otpisati internet aktiviste kao poražene u borbi protiv autoritarnih i drugih režima. Taj odnos je izjednačen i internet aktivisti (svih opredeljenja) imaju neke šanse za ostvarivanje pobede, ako su dovoljno lukavi.

Vratimo se na trenutak na gore pominjanu tezu da tvitovi ne ruše vlade, ljudi ruše vlade. Treba reći da internet, nevezano sa odnosom moći koji kreira između autoritarnih režima i njegovih oponenata, i sa tim da slabi vlade koje ne umeju da ga koriste kao svoj alat, ipak donekle, na indirektna način, slabi i stranu oponenata. Oko toga se slažu i Rotkof i Morozov i svi drugi posmatrači internet aktivizma. Internet je kriv za fenomen mikro-aktivizma. Mikro-aktivizam znači da nakon govora/pisanja i „kliktanja“ na internetu, skoro niko neće biti naveden da izađe iz kuće i uradi nešto značajno. Korisnici interneta se zadovoljavaju minialnim učešćem (menjanje slike na avataru i sl.) i gube aktivističku energiju za bilo koju svrhu. Stari način organizovanja protesta tražio je od aktivista da se nosi sa teškoćama, rizicima, tražio je odricanja, a samim tim je učvršćivao posvećenost cilju. Nasuprot tome, aktivizam na Tviteru daje iluziju da je učinjeno dovoljno i olabavljuje rešenost i posvećenost aktivističkom cilju. Ne traži se žrtva, hrabrost, fizička konfrontacija ili izlaganje fizičkoj opasnosti.

Paradoksalno, sa tvitovima kao opcijom, rušenje vlade, posebno u nekoj nasilnijoj i krvavijoj varijanti, je teže nego ikad.

Još jedna teza o aktivizmu na internetu, koja takođe ostavlja po strani samu promenu odnosa moći, ukazuje na manu slobode govora na internetu kao takve. Na internetu bilo ko može da šalje bilo kakve informacije. Po Morozovu je baš ta lakoća objavljvanja ono što ne valja, i to iz nekoliko razloga, od kojih će se ovde dati samo jedan: zatrpavanje banalnostima. Internetom se šire trivijalnosti, ogovaranja i ništavnosti, zatrpavajući ozbiljnu misao i refleksiju. Kori Doktorou je ovo prokomentarisala na sledeći način:

> „Teško da je on (Morozov – pri.aut.) prvi koji je primetio ... mogao je isto tako citirati i Toroovog Valdena: 'Stalo nam je da iskopamo tunel ispod Atlantika i dovedemo Stari svet nekoliko nedelja bliže novom; ali može biti da prva vest koja će procureti do širom otvorenog američkog uha bude vest da je princeza Adelaida dobila veliki kašalj.'“[366]

U moru banalnosti, digitalni aktivizam treba da se izbori da u prvi plan dođu njegova ponuda alternativnih narativa, stvaranje osećaja zajedničke patnje, mobilizacija pristalica. To zahteva posebnu vrstu umešnosti, delimično i marketinških znanja.

Internet okruženje – otpori ugrožavanju privatnosti

Pošto aktivizam obuhvata različite svrhe za koje se građani mogu zalagati, od borbe za demokratiju do regurtovanja pristalica islamskih ultra fundamentalista, svakako u jednu kategoriju aktivizma se ubraja i digitalni aktivizam koji se odnosi na otpor nadzoru na internetu. On je vrsta aktivizma koja ima za svrhu određenu viziju interneta ali posredno podrazumeva i viziju društva. To je društvo u kome države, kompanije i svi drugi akteri odustaju od ugrožavanja privatnosti građana na internetu.

O otporu prema kompanijama već smo govorili i istakli da taj otpor nije veliki. Nešto je veći otpor prema državi kao pretnji privatnosti običnih korisnika interneta. (Samo u retkim slučajevima kod istog subjekta se spaja otpor nadzoru i od strane država i od strane kompanija, na primer u pokretu Anonymous.)

[366] Doctorow, opus cit.

Ovde će biti predstavljena tri vida otpora koji se razlikuju po svemu, a slažu samo u tome da se državu ne bi smelo pustiti da nastavi sadašnju praksu manje više tajnog masovnog nadzora građana.

Prva vrsta otpora je pokret Reformgovernmentsurveillance.org[367] iza koga stoje najjače internet kompanije današnjice (njih osam[368] i sve su američke) čiji kredibilitet je narušen Snoudenovim otkrićima koja impliciraju da su ove kompanije sarađivale sa NSA u nadzoru na korisnicima. Ustajući protiv nelegalnog nadzora, vodeće internet kompanije istupaju u svoje ime ali i u ime svojih korisnika na neki način. One ne izjavljuju da ne žele da sarađuju sa vlastima, nego traže više transparentnosti o zahtevima koje dobiju od vlade SAD-a da predaju podatke o korisnicima. Prema sadašnjim propisima, internet kompanija mora da ćuti o zahtevu koji dobije od vlade, ne sme da obavesti ni korisnika čiji su podaci predmet zahtva ni javnost uopšte, jer bi objavljivanje ugrozilo nacionalne interese. Kompanije vide transparentnost o ovome kao prvi preduslov za debatu o vladinim nadležnostima u pogledu nadzora. „Vlade bi trebalo da dozvole kompanijama da objavljuju broj i vrstu vladinih zahteva za korisničkim informacijama (koje su primile – prim.aut). Povrh toga, i same vlade bi trebalo da ažurno objave te podatke.“[369]

Druga vrsta otpora masovnom nadzoru na internetu koji sprovodi država je pokret koji se naziva i sajferpank[370] a koji se vezuje za Džulijana Asanža (Julian Assange),

Asanž, državljanin Australije, 45 godina, je kompjuterski programer i neka vrsta hakera, uz to osnivač organizacije i sajta Vikiliks. On je za neke međunarodni borac za slobodu i borac protiv totalitarnih tendencija u zapadnim demokratijama. S druge strane, Asanž je osoba u SAD proglašena visokotehnološkim teroristom i neprijateljskim borcem uključenim u sajber rat na temelju njegove uloge u nastanku afere/a Vikiliks. Zato je trenutno u poziciji višegodišnjeg azilanta u Ambasadi Ekvadora u Londonu (od avgusta 2012. godine). Iako u mnogim delovima sveta (Rusija, Brazil itd.) uživa podršku i simpatije, u slučaju da napusti Ambasadu Ekvatora u Londonu, Asanž bi najverovatnije bio izručen SAD-u pod bilo kojim pravnim izgovorom.

---

[367] https://www.reformgovernmentsurveillance.com/
[368] AoL, Apple, Facebook, Google, LinkedIn, Microsoft, Twitter, Yahoo!
[369] https://www.reformgovernmentsurveillance.com/
[370] Sajferpank ulazi u srpski jezik od engl. Cypherpunk, što je kovanica od cypher-šifra i punk-vrsta otpora konvencionalnosti. Od 2006. godine reč se nalazi u Oksfordskom rečniku engleskog jezika.

Ilustracija 34 Asanž na naslovnoj strani magazina Tajm

Preuzeto sa http://media.photobucket.com/user/Fam0uslyUnkn0wn /media/2010TIMEpersonoftheyearASSANGE.jpg.html? filters[term]=julian%20assange&filters[primary]=images&sort=1&o=25

Asanž je izvršni urednik Vikiliksa, organizacije koju je sam formirao 2006. godine i koja se zasniva na internet stranici na kojoj se objavljuju poverljivi dokumenti koji su od interesa za javnost. Ono što je ovu stranicu dovelo u sukob sa vladom SAD je objavljivanje više grupa dokumenata – tokom 2010. i 2011. godine – o ratovima koje SAD vodi u Avganistanu i Iraku, o diplomatskim telegramima američkih diplomata i o logoru Gvantanamo. Iako je i Asanžovo delovanje sjajan primer korišćenja interneta kao alata za političko delovanje, ovde se Asanž pominje zbog njegove filozofije (sajferpank) koju propagira nezavisno od svog anti-američkog političkog delovanja.

U jednoj rečenici sažeta filozofija koju zastupa Asanž glasi: privatnost za slabe, transparentnost za moćne (privatnost za pojedince, transparentnost za države i korporacije – prim.aut.).[371] Pod moćnima se ne mora smatrati isključivo vlada SAD-a. Za Asanža je karakteristično da propagira otpor masovnom nadzoru koji sprovode vlade (demokratskih država) - putem enkripcije. S jedne strane su optički kablovi, sateliti i serveri, koje kontroliše presretač, a s druge strane su korisnici interneta, tj.

[371] Džulijan Asanž. (2013). *Sajferpanks. Sloboda budućnost interneta*. Beograd: Albion Books. Str.15.

presretnuti. Odnos snaga je krajnje nejednak na štetu korisnika interneta. Međutim, nejednakost snaga presretača i presretnutog može se izmeniti šifrovanjem tj. enkripcijom (pomoću softvera za enkripciju, koji je svima besplatno dostupan). Jednostavnije je šifrovati informaciju nego dešifrovati je. Dešifrovanje je teško, podrazumeva izvođenje matematičkih operacija velikog obima i nikakva sila prinude ne može rešiti matematički problem. Po Asanžu se šifrovanjem ostvaruje, barem delimično, sloboda od masovnog presretanja elektronskih komunikacija, ergo sloboda od državne kontrole, ergo mogućnost da pojedinac sačuva svoju privatnost.

Asanž je jednostran i veoma oštar u kritici interneta: "Internet, najveće sredstvo naše emancipacije, je pretvoren u najopasnije sredstvo podrške totalitarizmu i pretnju ljudskoj civilizaciji."[372] Zbog nezakonitog masovnog skupljanja metapodataka koje se tajno sprovodilo i verovatno i dalje sprovodi u zapadnim zemljama, Asanž smatra da se Zapad nimalo ne razlikuje (sa NSA kao vladarom sajber bezbednosti) od vladara koji je vladao unutrašnjim bezbednosnim snagama neke druge nacije pre pedeset godina. (Na primer, bivša Istočna Nemačka.) To je ista autoritarna struktura, koja će samo privlačiti ljude koji će je zloupoterbljavati. Nepostojanje odgovornosti je ugrađeno u taj tehnološko-bezbednosni sistem, i zbog toga je sistem opasan.

Asanžova briga za slobodu pojedinca u perspektivi izražena je u sledećem komentaru:

> „Mislim da će jedini ljudi koji će biti u mogućnosti da zadrže slobodu kakvu smo imali pre recimo 20 godina – jer je država nadzora do sada dosta stvari eliminisala, iako mi toga još uvek nismo svesni – biti oni koji su visoko obrazovani kada je u pitanju unutrašnjost sistema. To će biti samo visoko-tehnološka pobunjenička elita koja je slobodna, ti pametni pacovi koji će moći da trče svuda po operi."[373]

Treći vid protesta dolazi od međunarodnog (hakerskog) pokreta Anonymous, koji je nastao kao labava veza hakera na internetu 2003. godine. Oni nemaju lidera, i teško je fiksirati do koje filozofije tačno drže. Poznati su kao napadači na razne veb sajtove, zbog čega su mnogi njihovi članovi i uhapšeni. Najčešći oblici delovanja pokreta su vandalizam veb sajtova, hakiranje i objavljivanje tajnih informacija. Ovaj pokret smatra da je u eri identitetskog kapitalizma i društva nadzora odluka da ostaneš anoniman čin otpora protiv pogleda koje ti upućuju kompanije i policija. U cilju anonimnosti, članovi pokreta u javnosti nose maske na licu, tzv. maske Gaja Foksa (Guy Fawkes).

[372] Ibid. str. 9.
[373] Ibid. str. 136.

Ilustracija 35 Anonimusi sa maskama Gaja Foksa

Preuzeto sa https://i.ytimg.com/vi/FAECyLvSCHg/mqdefault.jpg

Njihov moto glasi: "Znanje je besplatno. Mi smo Anonymous. Mi smo Legion. Mi ne opraštamo. Mi ne zaboravljamo. Očekujte nas."[374] Koliko je poznato, ovaj pokret je imao ili ima pripadnike i u Srbiji.

Domet ova tri vida protesta protiv masovnog nadzora nad internetom - onog koji pružaju internet kompanije, onog koji pružaju pristalice pokreta sajferpanka i Anonymous-a - za sada je relativno ograničen. Velika većina običnih korisnika interneta se ponaša kao da internet nadzor ne postoji i da privatnost nije ugrožena.
Ipak, možemo dodati jedan umetnički gest koji je na tragu svojevrsne borbe protiv nadzora i kontrole koji poništavaju privatnost pojedinca. Radi se o skulpturi koju je napravio italijanski vajar Davide Dormino a koja je bila postavljena 1. maja 2015. godine u Berlinu na popularnom Aleksandrovom trgu. Skulptura je celina od tri figure koje predstavljaju "tri savremena heroja koji su izgubili svoju slobodu zarad istine" (radi se o Snoudenu, Asanžu i Bredliju Meningu[375]) uz koje stoji četvrta prazna stolica – na koju su pozvani da stanu svi, obični građani.

[374] Navedeno prema http://www.yalelawtech.org/anonymity-online-identity/we-are-anonymous-we-are-legion/

[375] Bradley Manning, nakon promene pola Chelsea Manning je saradnik Asanža, koji je 2013. godine u SAD-u osuđen zbog špijunaže i služi kaznu od 35 godina u zatvoru.

Ilustracija 36 Fotografija skultupre Anything to Say? Monument of Liberty; Davide Dormino

Preuzeto sa http://davidedormino.com/2015/05/27/anything-to-say-a-monument-to-courage/#jp-carousel-532

Ilustracija 37 Foto skulpture Anything to Say? Monument of Liberty; Davide Dormino

Preuzeto sa http://davidedormino.com/2015/05/27/anything-to-say-a-monument-to-courage/#jp-carousel-533

DEVETO POGLAVLJE

Lični podaci – čuvati ili prodati?

U prethodnom poglavlju smo prikazali glavne konture pozicije običnog korisnika na internetu. Iz rečenog proizilazi da bi razvoj interneta u budućnosti mogao običnog korisnika dovesti do toga da ima manje privatnosti ili je nema uopšte. To zahteva da se sagleda kakva je zaštita ličnih podataka na internetu i šta se u tom smislu može reći o budućim trendovima.

Skoro uvek se govor o privatnosti na internetu započinje iz ugla zaštite privatnosti odnosno zaštite ličnih podataka od raznih napada koji se na nju vrše, što je i najčešći način kako se tome pristupa. Implicitno se zaštita izjednačava sa čuvanjem (u posedu onog ko ima na to pravo) i zadržavanjem za sebe/kod sebe. Međutim, postoji i linija razmišljanja (a i po neki primer iz prakse) po kojoj, ako su već podaci nova vrsta imovine[376] tj. nova vrsta robe, vlasnik podataka je slobodan da odluči da te podatke dobrovoljno proda kome god želi. Umesto da se to radi netransparentno, bez njegovog znanja, često uz kršenje zakona, pravni i privredni okvir bi se mogao podesiti tako da se olakša ova transakcija. Za početak, treba urediti da on ima kontrolu nad svojim podacima. Dakle, radi se o izjednačavanju subjekt podatka – vlasnik podatka, i potom mu se vraća moć odlučivanja o tome šta će s podatkom raditi.

Prve korake u ovom smeru napravio je u Nemačkoj poslanik Stranke zelenih Malte Špic, koji je zatražio od svog mobilnog operatera Nemačkog telekoma da mu dostavi sve podatke koje poseduje o njemu. To nije išlo glatko, ali je na kraju, uz pomoć suda, poslanik Špic uspeo da dobije od svog telekoma svoje podatke. U pitanju su bili podaci vezani za njegov broj mobilnog telefona u šestomesečnom periodu (koji je zakonski period u kome kompanije imaju pravo čuvanja ličnih podataka korisnika), od avgusta 2010. do februara 2011. godine. Dobio je jednu eksel tabelu u kojoj je bilo oko 36.000 redova, a svaki red se odnosio na jednu transakciju izvršenu na tom mobilnom broju. Tabela je javno objavio, kako bi javnost mogla da se uveri o tome šta sve ova vrsta ličnih podataka može da otkrije o nečijem životu. Sakriveni su samo podaci o brojevima telefona ljudi sa kojima je Špic komunicirao. Ukupno, njegov telefon je bio uključen 78% vremena u datom periodu.

[376] Ono što treba zapaziti je da je ovde implicitna pretpostavka da moji podaci nisu ja, već su nusproizvod mog življenja u digitalnom dobu. To je pretpostavka koja se može tematizovati, pa i odbaciti. To izlazi iz okvira ovog rada.

> «Ovaj profil otkriva kada je Špic šetao ulicom, kada se vozio vozom, kada je bio u avionu. Pokazuje gde je bio u gradovima koje je posetio. Pokazuje kada je radio i kada je spavao, kada je bio dostupan a kada nedostupan na telefonu. Pokazuje kada je radije telefonirao a kada radije slao SMS-ove. Pokazuje koje pivnice voli da posećuje u svoje slobodno vreme. Sve u svemu, otkriva ceo jedan život.»[377]

I sve to je samo iz mobilnog telefona, bez ukrštanja sa njegovim drugim Špicovim javno dostupnim ličnim podacima, kao što su tvitovi i postovi na fejsbuku i sl. sa kojima je ukrštanje više nego jednostavno.

Poruka koju je Špic imao za javnost glasi: «Samo-određenje i život u digitalnom dobu nije kontradikcija, ali morate da se borite za svoje samo-određenje danas. Recite svojim prijateljima, privatnost je vrednost 21. veka i nije zastarela.»[378]

Postoji i slučaj Holanđanina Šona Bakla (Shawn Buckles)[379] koji je 2014. godine ponudio da proda svoje podatke putem aukcije. Javila mu se kompanija The Next Web i kupila njegove podatke za 228 funti (da ih upotrebi kao primer na nekoj stručnoj konferenciji). Za tu cenu dobili su sve njegove informacije, od pretraživanja interneta do imejlova, u određenom periodu. Bakl je izvršio direktnu prodaju. Ipak, najčešća prodaja bi bila ona preko posrednika, tj. firmi koje preprodaju lične podatke, a one manje vrednuju podatke. Aktuelna cena ličnih podataka na tržištu je zapravo dosta niža od onog što je Bakl zaradio. Po nekim navodima, kompanija Datacoup plaća za lične podatke tek nekih 8 USD mesečno.

Zapravo se ne može znati da li je ta cena realna i koliko podatak stvarno vredi nekoj kompaniji. Posebno tome doprinosi činjenica da se podaci prodaju u anonimiziranoj formi i u gomili (na primer, kupuje se 1000 profila za 220 USD – vrednost jednog dolazi na 22 centa). Uz to, kompanije imaju i druge načine da do istih podataka dođu, trgujući sa drugim kompanijama, zaobilazeći samog subjekta podataka.

Iz kruga inovativnih preduzetnika koji žele da razviju biznis otkupljivanja ličnih podataka vredno pažnje je ovo gledište:

> «Za 4-5 godina, pola sveta neće mariti o svojim podacima a druga polovina hoće. Polovina koja hoće će biti sve više i više zgrožena onim što se dešava i okrenuće se kompanijama koje će im vratiti njihove

[377] Kai Biermann. (10. mart 2011). «Betrayed by our own data» *Die Zeit* Dostupno na http://www.zeit.de/digital/datenschutz/2011-03/data-protection-malte-spitz

[378] Malte Spitz. (Jun 2012). *Your phone company is watching* Dostupno na http://www.ted.com/talks/malte_spitz_your_phone_company_is_watching

[379] Billy Ehrenberg. (22. apr. 2014). «How much is your personal data worth?» *The Guardian* Dostupno na http://www.theguardian.com/news/datablog/2014/apr/22/how-much-is-personal-data-worth

> podatke tako da sami ne samo mogu s njima raspolagati i razumeti ih, nego ih i eksploatisati.»[380]

Koja polovina sveta će biti svako od nas? Ono što je sigurno je da iz ugla poštovanja osobe, šta god svako od nas odabrao - moralo bi da bude stvar ličnog izbora. Uz to, ljudi imaju pravo da budu nedosledni, kao i da prioritizuju svoje razloge po svom nahođenju. Na primer, može se destiti da će jedna ista osoba rado ispričati prijateljima (pa čak i ne tako bliskim) na internetu šta je pojela za doručak, ali neće dopustiti da ta ista informacija dođe od kompanije koja reklamira hranu ili koja prodaje zdravstveno osiguranje. Zato je čuveni slogan «privatnost je mrtva», pod uslovom da je tačan - potpuno relativan, jer ne precizira *koja* privatnost je mrtva.

Možda osnovno pitanje koje treba razjasniti je: zbog čega je nečiji lični podatak vredan zaštite? U demokratskim sistemima, sama ličnost je vredna zaštite i raspolaže jasno određenim individualnim pravima, a shodno tome i njeno vlasništvo (makar ono bilo veoma nov fenomen, kao što su digitalni podaci) je vredno zaštite. Kao i kod ostalih prava, da bi vlasnik podataka mogao da ima samo-određenje po pitanju šta će s njima raditi, potrebno je da mu država osigura pravni okvir u kome će njegova prava biti garantovana.

EU direktiva o zaštiti podataka

Kastels se pri kraju svoje knjige pita: zašto ne poverimo vladama, barem onim demokratskim, regulisanje isrpavnih načina korišćenja interneta.[381] Potvrdu da se to, ili deo toga, može realizovati imamo u zaštiti privatnosti pravnim sistemom u Evropskoj uniji i par zemalja koje su sledile njen standard zaštite privatnost. Možemo se nadati da će se ovaj standard zaštite primeniti i u našoj zemlji, u sklopu harmonizacije propisa u procesu pridruživanja EU.

Kao prethodna napomena mora se istaći da je u ovom istraživanju uzeta kao jedini okvir zaštite privatnih podataka Direktiva Evropske unije (95/46/EC)[382] zato što je taj

---

[380] Ben Woods (17. sept.2013) «What's the true value of your personal data? Meet the people who want to help you sell it» *TNW News* Dostupno na http://thenextweb.com/insider/2013/09/17/whats-the-true-value-of-your-personal-data-meet-the-people-who-want-to-help-you-sell-it/

[381] Manuel Castells, Opus cit. Str. 229.

[382] Directive 95/46/EC on the Protection of Individuals with Regard to the Processing of Pesonal Data and on the Free Movement of Such Data. Ovaj pravni akt postoji na svim zvaničnim jezicima Evropske unije. Engl. http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31995L0046&from=en Hrvatski http://eur-lex.europa.eu/legal-content/HR/TXT/PDF/?uri=CELEX:31995L0046&from=en Opširna objašnjenja primene ove direktive nalaze se na http://ec.europa.eu/justice/data-protection/

okvir relevantan, kako u sadašnjem trenutku tako i u budućnosti, za korisnike interneta u Republici Srbiji, s obzirom na kandidaturu za članstvo i započete pregovore o članstvu u ovoj organizaciji. Uz to, Sjedinjene američke države, zemlja rođenja interneta, nemaju[383] sveobuhvatnu legislativu koja se tiče zaštite privatnosti podataka, niti postoji apsolutno pravo na privatnost. Zaštita privatnosti u SAD-u se pretežno bazira na prvom, četvrtom i petom amandmanu Ustava SAD. Odredbe o zaštiti podataka su sektorske i fragmentirane od industrije do industrije (telekomi, banke, itd.) i po nivoima (federalna država, nacionalni nivo). Stoga se u ovom radu odustalo od donošenja modela SAD, a prevagu su odneli razlozi praktičnosti i želja da obuhvat ovog rada odgovara njegovoj svrsi.

Direktiva EU je uspostavila pravo na privatnost kao osnovno pravo, a građanima EU kao subjektima podataka dala važna prava koja se odnose na njihove podatke kao što su: pravo da pristupe podatku, pravo da uskrate dozvolu za korišćenje podatka, pravo da im se netačan podatak ispravi i pravo na otštetu u slučaju nezakonitog procesuiranja podatka. Lične podatke je definisala široko, tako da to nisu samo ime, JMBG i adresa, nego i svi drugi podaci koji mogu voditi ka ličnoj identifikaciji direktno ili indirektno (na primer podaci koji bi ukazali na fizički, fiziološki, mentalni, ekonomski, kulturni ili društveni identitet osobe). Direktiva je isto tako široko definisala „procesuiranje podataka“: prikupljanje, snimanje, organizovanje, skladištenje, prilagođavanje ili menjanje dobijanje, konsultovanje, korišćenje, otkrivanje transmisijom ili diseminacijom ili na drugi način činjenje dostupnim, sređivanje ili kombinovanje, blokiranje, brisanje ili uništavanje.[384] Shodno tome, skoro da nema načina da neko ko komercijalno koristi internet ne dođe u kategoriju kontrolora podataka, iz čega mu sleduju određene obaveze. Tu se pre svega misli na obaveštavanje i dobijanje saglasnosti subjekta podataka.

Direktiva teži da ima ekstra-teritorijalno dejstvo (van EU), jer pristup podacima građana EU dopušta samo onim spoljnim akterima koji dolaze iz država sa odgovarajućim sistemom zaštite ličnih podataka. Ako to nije slučaj, spoljni akteri koji žele pristup podacima građana EU moraju imati opremu lociranu na teritoriji EU, čime se na njih primenjuje upravo direktiva. Ipak, direktiva je dozvolila izuzetke, a

[383] McKay Cunningam, „Privacy in the age of the hacker: balancing global privacy and data security law“ in *The George Washington International Law Review*, Vol 44. 2012. pp 643-697. Dostupno na http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2138307 str. 665.
[384] Directive 95/46/EC član 2(b).

jedan od njih je *Sporazum o sigurnoj luci*,[385] koji je sklopila sa SAD-om 2000. godine. Zahvaljujući tome kompanije iz SAD-a mogu da u praksi izbegnu poštovanje direktive, mada je bilo određenih akcija sa strane EU da se to spreči.

Zbog svega navedenog, kaže se da ova direktiva ima takozvani omnibus pristup zaštiti. Još jedan karakterističan epitet je „ćebe regulativa". Ona teži da pravno zaštiti sve lične podatke građana EU, čak dobija epitet „apsolutistička". No razvoj tehnologije, a posebno razvoj interneta stvari, dovode u pitanje njenu održivost.

Kritike ove direktive su brojne. Akcentuje se da ona pogađa previše – čak i ono procesuiranje podataka koje je bezopasno. Takođe u svetlu novih dokaza da se i jednom anonimizirani podaci mogu lako ponovo (u kombinaciji sa drugim podacima) re-identifikovati, direktiva dolazi dotle da pogađa univerzalno – sve podatke pretvara u lične. Zatim se zamera to što ne dozvoljava izuzetke, na primer ni procesuiranje podataka u cilju zaštite sigurnosti.[386] Dalja zamerka se tiče toga da direktiva ne hvata u mrežu najopasnije prkršioce zaštite ličnih podataka: 1. službe koji se pozivaju na zaštitu nacionalnog interesa u samim državama članicama EU (što je dosta fluidan koncept) i 2. pojedine američke kompnaije koje procesuiraju lične podatke ali zbog *Sporazuma o sigurnoj luci* ne postoji realna kontrola toga da li poštuju standarde predviđene direktivom (postoje sumnje da umesto poštovanja postoji mimikrija poštovanja). Ipak, najveći nedostatak direktive leži u tome što nije u skladu sa trenutkom, odnosno nastupanjem interneta stvari. Ona je bila adekvatna u prethodnom periodu kada se radilo o aktivnom deljenju podataka, tj. kada sama osoba ostavlja svoje podatke na internetu. Smatra se pak da u okruženju interneta stvari, osoba ne može znati precizno koliko njenih podataka je uzeto, ko ih kontroliše i za koju svrhu. Direktiva o tom slučaju ne kaže ništa specifično, a uobičajeno obaveštavanje i saglasnost subjekta podataka su tu praktički dovedeni do neprepoznatljivosti i neprimenjivi.

Digitalni podaci mogu biti na mnogo mesta odjednom, putovati hiljade kilometara u deliću sekunde i lako prikupljeni bez ikakvog obaveštenja ili saglasnosti. Uz to,

---

[385] Odluka Evropske komisije iz 2000. godine dostupna je na http://www.personuvernd.is/media/frettir//2000_518_EC.pdf a za više detalja o trenutnoj primeni sporazuma http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm

[386] McKay Cunningham, „Next Generation Privacy: The Internet of Things, Data Exhaust, and Reforming Regulaltion by Risk of Harm" in *Groningen Journal of International Law*, Vol. 2(2), 2014. 115-144. Dostupno na https://groningenjil.files.wordpress.com/2015/01/grojil_vol-2-ed-2_cunningham.pdf (U daljem tekstu „Next Generation Privacy") str.128.

postoji ogroman broj izvora podataka – od postova na društvenim mrežama preko mobilnih telefona do senzora u privatnim kućama i u javnom prostoru.

„Možda prevareni mitom onlajn anonimnosti, korisnici stalno razbacuju bitove sebe dok pretražuju Google, kupuju stvari onlajn, postuju fotografije, lajkuju restorane i traže mesta za odmor. Ove onlajn akcije izgledaju besplatne; ali nisu.“[387] Šta se pod tim misli Kuningam objašnjava jednim zapažanjem Laniera i jednim rečitim podatkom: „'Dominantan princip nove ekonomije, informacione ekonomije, u zadnje vreme je bio da se sakrije vrednost informacije.' Google prima više od tri milijarde upita za pretragu svakog dana – i sve ih sačuva.“[388] Naravno, to čine i druge internet stranice, što potvrđuju istraživanja (o čemu je bilo reči u poglavlju 8). Na sve to, dodaju se i pasivno generisani podaci, čijeg postojanja građani najčešće nisu ni svesni. Na primer, snimci nadzornih kamera u gradu ili podaci iz sistema elektronske naplate putarina.

> „Obaveštenje, saglasnost, pristup i korekcija, iako su korisni alati za regulisanje korisnikovog dobrovoljnog davanja ličnih informacija, ne pogađaju lične podatke koji se pasivno dobijaju. Sadašnji zakoni o privatnosti podbacuju kada podaci 'nastaju na udaljenosti od neposrednog opažanja pojedinca i gde su saglasnost, učešće i svesnost retko održivi'.“[389]

U tom smislu, Kuningam traga za privatnošću sledeće generacije. Suština njegove linije razmišljanja se svodi na sledeće:

> „Ovaj članak zastupa da informaciona privatnost ne može biti postignuta proglašavanjem privatnosti za fundamentalno pravo, kriminalizovanjem svakog procesuiranja ličnih informacija i sprovođenjem zakona na bazi obaveštenja i pristanka. ... Postepeno napredujuće i praktično zakonodavstvo bolje ostvaruje taj cilj.“[390]

Kuningam se zalaže da zakonodavno regulisanje treba da krene od otkrivanja rizika štete nastale upotrebom podataka u pojedinačnim kontekstima (i to štete iz ugla korisnika), čime bi se otkrila vrednost konkretnih podataka i potom usvojile zaštitne politike koje bi za fokus imale upotrebu podataka čija upotreba nanosi najviše štete (narušavanje privatnosti). Mora se izvršiti prioritizacija u pogledu ozbiljnosti ili verovatnoće nastanka štete, ali i uzeti u obzir različita senzibilnost prema privatnosti u različitim državama. Međutim, Kaningam ne daje koje su to upotrebe koje nanose

[387] „Next Generation Privacy“ str. 132.
[388] Ibid. str. 132.
[389] Ibid. str. 142.
[390] Ibid. str. 118.

najviše štete – posebno ne u Evropi (pošto pominje čitače auto tablica u nekim američkim federalnim državama). Verovatno taj nedostatak odgovora nije slučajan, budući da je zaista teško znati koja vrsta podataka je važnija od neke druge i šta donosi kakvu štetu privatnosti i na koji način.

Presuda Evropskog suda pravde u predmetu Gugl

Reforma evropskog režima zaštite ličnih podataka[391] morala bi da obuhvati mnoge oblasti ali svakako je jedan element već bacio u senku sve ostalo. Radi se o tzv. pravu da budeš zaboravljen/a. Ma koliko čudno zvučao sam naziv, važnost onoga što je implicirano u ovom pravu je nesporna. Sud Evropske unije je maja 2014. godine prvi put doneo jednu odluku vezanu za to pravo, i to u korist tog prava a u predmetu koji se ticao kompanije Google Španija.[392] Smatra se da je to deo trenda sve većeg interesovanja za privatnost od strane sudova i sve veće spremnosti sudova da donose odluke sa dalekosežnim posledicama.

Pravo da budeš zaboravljen/a svodi se na to da osoba ima pravo da zahteva da onaj kod koga se konkretni podatak nalazi (što su najčešće kompanije i državne institucije) izbriše njen lični podatak i uzdrži se od daljeg širenja tog podatka, ako su ispunjeni određeni uslovi:[393]

(a) lični podatak nije više potreban u odnosu na svrhe za koje je uzet ili procesuiran,

(b) subjekt podatka povlači svoj pristanak na bazi koga je podatak procesuiran ili je istekao period važenja pristanka,

(c) subjekt podatka se protivi procesuiranju ličnog podatka,

(d) procesuiranje podatka nije u skladu sa propisom na druge načine.

Ovo pravo kreira jasnu obavezu onom kod koga se lični podatak nalazi, a to su najčešće kompanije i državne institucije, da izvrši korake u cilju brisanja podatka, kao

[391] Kao podloga reforme EU propisa u ovoj oblasti u opticaju je nacrt General Data Protection Regulation, ali to je tek radni dokument i ne baš blizu usvajanja.

[392] C-131/12, *Google Spain SL, Google Inc. v Agencia Espanola de Protecion de Datos (AEPD), Mario Costeja Gonzalez*. Navedeno prema Paul Bernal, „The Right to be Forgotten in the post-Snowden era" *Privacy in Germany*, No 5, 2014. Dostupno na http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2689685 str. 3.

[393] Paul Bernal, „The Right to be Forgotten in the post-Snowden era" *Privacy in Germany*, No 5, 2014. Dostupno na http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2689685 (U daljem tekstu „Right to be Forgotten") str. 4.

i u cilju informisanja trećih strana da subjekt podatka traži njegovo brisanje. Upravo ove obaveze su ono što smeta kompanijama, zbog čega se protive pravu da budeš zaboravljen/a, jer to zahteva da utroše resurse da bi izvršili takav zahev. Sem toga, kompanije nisu sigurne ni da mogu izvršiti takav zahtev, jer podatak može da postoji u više različitih oblika, i brisanje na jednom mestu ne garantuje da je definitivno obrisan.

S druge strane, pravo da budeš zaboravljen/a bi moralo da bude usklađeno sa pravilima o slobodi izražavanja, koja ne trpi naloge takve vrste u pogledu govora/izražavanja. Usklađivanje dva prava kada su u sukobu je uvek poseban izazov. Ipak, ovde se situacija jasnije sagledava ako se napravi razlika između govora i podataka u raznim oblicima. Na primer, podaci u raznim oblicima su: istorija pretraživanja na internetu, profili, individualno logovanje na sajtove, metapodaci o komunikaciji, podaci socijalnog mapiranja, geolokacijski podaci, transakcije iz onlajn kupovine, zdravstveni podaci i drugo. Oni nisu govor i nikada nisu ni bili nameravani od strane osobe da budu javni. Za razliku od klasičnog govora, oni mogu drastično da povrede privatnost i autonomiju osobe. Zbog čega bi se oni tretirali kao javni i pogodni za javno pretraživanje? Jedini razlog koji se može naći: jer je to zgodno kompanijama koje prikupljaju te podatke. O opravdanosti tog razloga je dovoljno reći da profit kompanije nije u istoj ravni kao zaštita individualnog prava.

Ovo je ujedno i „zaplet“ sada čuvenog sudskog predmeta sa Guglom u sporu. Spor se ticao jednog Španca koji je otkrio da kada ljudi pretražuju njegovo ime na Guglu nalaze jednu staru priču – zvanični oglas u novinama iz 1998. godine – o aukcijskoj prodaji stvari koje su mu pripadale u cilju izmirenja dugova po osnovu socijalnog osiguranja. On je dugove izmirio pre aukcije, koja se nikad nije ni održala. Ovaj čovek je najpre tražio da novine uklone taj oglas sa interneta, što je odbila Španska agencija za zaštitu podataka (AEPD) pošto je oglas bio deo javnih dosijea i novine su bile u obavezi da o tome izveste. Čovek je dalje tražio od Gugla da skloni linkove ka tom oglasu (čime bi oglas bilo teže naći na internetu), sa čim se AEPD složio i izdao naredbu Guglu da tako postupi. Međutim, Gugl se žalio te je predmet stigao do Evropskog suda pravde. Evropski sud pravde je presudio:

> „Kako subjekt podataka, u svetlu svojih osnovih prava po Članovima 7 i 8 Povelje o osnovnim pravima Evropske unije,[394] ima pravo da

[394] Povelja o osnovnim pravima Evropske unije (Charter of Fundamental Rights of the EU 2000/C 364/01) je dostpuna na internet stranici http://www.europarl.europa.eu/charter/pdf/text_en.pdf (zadnji put posećeno 29.feb.2016.) Inače, Članovi 7 i 8 ove Povelje glase:

> zahteva da informacija o kojoj se radi više ne bude dostupna opštoj javnosti po osnovu uključivanja na takvu jednu listu rezultata pretraživanja, ova prava su jača, po pravilu, ne samo od ekonomskog interesa operatora pretraživača nego i od interesa opšte javnosti da ima pristup toj informaciji u sklopu pretraživanja koje se odnosi na ime subjekta podataka.“[395]

Ovakvo eksplicitno davanje veće težine privatnosti u odnosu na ekonomski interes kompanija i na pravo javnosti da zna je bilo iznenađenje, ali je posredno poremetilo odnos snaga posebno između aktera uključenih u debatu o reformi sistema zaštite podataka u Evropi. Do ove odluke suda, zagovornici zaštite privatnosti videli su u reformi šansu da se ona bolje zaštiti. Nakon ove odluke suda, kompanije vide u reformi šansu da ublaže ovaj standard koji im je sud nametnuo i smanje svoje obaveze.

Po Bernalu, akademska zajednica iz ove oblasti kao da je doživela šok ili strujni udar od ove presude suda i postala maksimalno aktivna, „više od 75 blogova, novinskih članaka i tome slično napisano je samo u prvom mesecu nakon ove presude, uključujući tekstove takvih istaknutih imena kao što su Mayer-Schoenberger, Morozov, Posner, Solove i Zittrain, kao i odgovori od strane tela za internet Velike Britanije, radne grupe za član 29 i drugih.“[396] Time se ovde ne možemo detaljnije baviti, uz izuzetak jedne vrste komentara, koja ima veze sa arhitekturom interneta. To su komentari koji ukazuju na veliku (tehničku) kompleksnost uklanjanja informacije sa interneta. Takođe treba uočiti da se ovime velika moć stavlja u ruke Gugla, kao najmoćnijeg internet pretraživača trenutno, jer direktno njegovim delovanjem (od njegove odluke) se brisanje neke informacije sprovodi ili ne sprovodi. Ipak, reći da odluka suda daje tu moć Guglu ne odgovara istini, budući da on tu moć već ionako ima.

„Član 7.
Poštovanje privatnog i porodičnog života
Svako ima pravo na poštovanje njegovog ili njenog privatnog života, doma i komunikacija.
Član 8.
Zaštita ličnih podataka
1. Svako ima pravo na zaštitu ličnih podataka koji ga/je se tiču.
2. Takav podatak mora biti procesuiran pravično za specifične svsrhe i na osnovu pristanka osobe koje se tiče ili neke druge legitimne osnove postavljene zakonom. Svako ima pravo na pristup podacima koji su prikupljeni o njemu ili njoj, i pravo da ih koriguje.
3. Poštavanje ovih pravila će biti predmet kontrole nezavisnog tela.“

[395] „Right to be Forgotten“ str. 7.

[396] Ibid. str. 8. Kompendijum akademskih komentara na ovu temu kreiran na univerzitetu Kembridž dostupan je na nternet stranici www.cambridge-code.org/googlespain.html

Nakon presude Evropskog suda pravde, kompanija Gugl je poštovala presudu. Otvorila je obrazac kojim korisnici mogu da pošalju zahtev za brisanje neke informacije i obavezala se da će oceniti svaki zahtev pojedinačno. U prvih mesec dana „Gugl je rekao da su dobili od 70.000 zahteva, što je veliki broj ali u kontekstu reda veličina na Gugl je relativno mali. U približno istom periodu Gugl je primio zahteve za uklanjnanje više od 25 miliona URL-ova na osnovu povrede autorskih prava.“[397] Međutim, sumnju da će Gugl zaista poslušati Evropski sud pravde izazvalo je to što je u brisanju podataka posebno bio revnostan kad bi bilo zatraženo da se brišu novinski članci, skorijeg datuma i isključivo britanskih novinara.[398] Čini se da bi tim brisanjem novinskih članaka mogla da se isprovocira javnost, barem ona u Velikoj Britaniji, tradicionalno osetljiva na remećenje slobode govora, da ustane protiv odluke suda i prava da se bude zaboravljen/a. Ipak, za sada se to očekivanje nije ispunilo.

Februara 2016. godine statistika koju Gugl objavljuje[399] vezano za zahteve za brisanje podataka iz pretraživanja koja stižu iz Evropske unije govori da je kompanija od 29. maja 2014. godine do danas (mart 2016. – prim.aut.) primila 399.249 zahteva, koji su se odnosili na 1.398.030 URL-ova i da je 57,4% URL-ova u tom kontekstu uklonjeno. Dostupni su i podaci po zemljama, pa je tako 85.093 zahteva stiglo iz Francuske, 68.829 iz Nemačke, 48.816 iz Velike Britanije, 38.109 iz Španije i 29.865 iz Italije. Iz Hrvatske je poslato 4.168 zahteva za brisanje podataka iz rezultata pretraživanja.

Bernal ističe jedan aspekt prava da se bude zaboravljen/a koji bi mogao da olakša situaciju sa količinom zahteva za brisanje podataka. Tu se ne radi o totalnom brisanju, već o modifikaciji rezultata pretraživača. Običnim ljudima „realna briga nije trajno brisanje podataka ili novo pisanje istorije, već to da ono što drugi ljudi (ili organizacije) nalaze o njima prilikom običnog pretraživanja ili relativno površne istrage ne bude prenaglašeno u korist starih ili irelevantnih informacija.“[400] Autori Selinger i Hartzog su to nazvali „opskurizacija“ (na engl. obscurity).[401] Pod time misle da informacija postaje bezbednija ako je do nje teže doći. Stručan i odlučan lovac na podatak opremljen odgovarajućim alatima će uvek naći tu informaciju, ali za

[397] “Right to be Forgotten”, str. 10.
[398] Ibid. 10-11.
[399] https://www.google.com/transparencyreport/removals/europeprivacy/?hl=en
[400] “Right to be Forgotten” str. 14.
[401] Woodrow Herzog and Evan Selinger. (17. jan. 2013). “Obscurity. A Better Way to Think About Your Data Than ‘Privacy’”. *The Atlantic.* Dostupno na: http://www.theatlantic.com/technology/archive/2013/01/obscurity-a-better-way-to-think-about-your-data-than-privacy/267283/

šire narodne mase taj napor koji moraju da ulože će igrati ulogu odvraćanja. Prava vrsta „opskurizacije“ podataka bi se dobila ako bi Gugl razvio algoritme za pretragu koji bi automatski davali manju vrednost starijim, manje relevantnim pričama, a time bi dobijao manji broj zahteva za brisanje.[402]

Lokalizacija podataka

Pored prava da budeš zaboravljen/a na internetu, za internet kompanije pojavljuje se još jedna vrsta obaveza, na osnovu toga što jedan broj vlada širom sveta podiže barijere slobodnom protoku informacija. Vlade, motivisane brigom oko privatnosti, bezbednosti, nadzora i primene zakona, donose propise kojima obavezuju (strane) internet kompanije da lokalizuju podatke na njihovoj teritoriji, a ne da ih čuvaju na serverima u inostranstvu.

> „Prva generacija graničnih kontrola interneta težila je da zadrži informacije van zemlje – od nacističkih parafernalija do materijala koji krši autorska prava. Nova generacija graničnih kontrola interneta ne teži tome da zadrži informacije napolju, nego da zadrži podatke unutra. Dok se prva generacija bavila relativno suženim krugom isključenih informacija, nova generacija teži držanju svih podataka o pojedincima unutar zemlje.“[403]

U literaturi se mere koje ograničavaju transfer podataka preko nacionalnih granica nazivaju „lokalizacija podataka“. Spektar takvih mera je veoma širok, a broj država koje se odlučuju da ih uvedu se povećava, pri čemu to nisu samo neliberalne nedemokratske države, već ima i članica kluba najuspešnijih.

„Zamislite internet u kom podatak mora da stane na nacionalnoj granici, bude pregledan da li mu je dozvoljeno da napusti zemlju i eventualno plati porez kad izlazi. Iako to može zvučiti kao mašta, to bi bio uticaj raznih preduzetih ili planiranih mera.“[404] Kao posledice tih mera bili bi očekivani: ekonomski pad u informacionoj industriji, povećanje troškova i prekid nekih sada dostupnih globalnih usluga.

Zagovornici lokalizacije podataka navode argumente za ove mere – one će poboljšati bezbednost i privatnost. Njima se onemogućava inostrani nadzor (što je donekle

[402] „Right to be Forgotten“ str. 14.
[403] Anupam Chander and Uyen P. Le. (April 2014).„Breaking the Web: Data Localization vs. the Global Internet“ *US Davis Legal Studies Research Paper Series*, Dostupno na: http://ssrn.com/abstract=2407858 Str. 3.
[404] Ibid, str.3-4.

diskutabilno) i uvodi primena domaćih zakona. Protivnici lokalizacije ukazuju da baš to ne stoji, ove mere će erodirati privatnost i bezbednost, jer će povećati rizik od kriminalnih napada na domaće servere i rizik domaćeg nadzora. Ono što donekle nije predmet spora jednih i drugih je domaći ekonomski razvoj koji se kreira ovim merama. Tu je sporna samo njegova veličina.[405] Iako je taj domaći ekonomski razvoj poželjan, vlade koje žele da primene obavezu „serveri u zemlji" ne mogu unapred znati da li će inostrane kompanije pristati na izgradnju te infrastrukture na njihovoj teritoriji ili će to smatrati neekonomičnim i povući se.[406]

U radu Čandera i Le, pobrojano je 16 država koje su uvele neki vid mera za lokalizaciju podataka: EU kao celina, Francuska, Nemačka, Švedska, Rusija, Kazahstan, Kina, Indija, Indonezija, Malezija, Južna Koreja, Tajvan, Tajland, Vijetnam, Austrlija, Brazil i Kanada. Zadržaćemo se samo na nekima, u nameri da se ilustruje dijapazon i logika (pokušaja) ovakvih regulisanja.

Kanada na nivou nacionalne države ne zabranjuje transfer ličnih podataka van Kanade, ali dve njene pokrajine, Britanska Kolumbija i Nova Škotska, su donele zakone po kojima lične informacije u posedu javnih ustanova moraju biti uskladištene i dostupne samo u Kanadi, osim onih koje potpadaju pod nekoliko ograničenih izuzetaka.[407]

Evropska unija je međunarodni protok podataka uredila već prikazanom Direktivom o zaštiti podataka iz 1995. godine. Podaci se mogu slati van EU samo ukoliko zemlja u koju se šalju ispunjava standarde za zaštitu podataka u dovoljnoj meri, što je u praksi omogućilo slanje u nekih 12 jurisdikcija (Švajcarska, Australija, Novi Zeland, Argentina, Urugvaj, Kanada i još nekoliko manjih ostrva bliskih Velikoj Britaniji), a posebnim Sporazumom o sigurnoj luci između EU i SAD omogućeno je i slanje u SAD. Međutim, od 2013. godine u pripremi je reforma direktive i sporazuma EU iz ove oblasti, tokom koje se može očekivati da će se pooštriti kriterijumi i standardi

[405] „Lokalizacija podataka, kao i većina protekcionističkih mera, vodi samo malim dobicima za nekoliko lokalnih preduzeća i radnika, dok u isto vreme izaziva značajne štete šire gledano u ekonomiji. Domaće koristi od lokalizacije podataka idu nekolicini vlasnika i radnika u data centrima i nekolicini kompanija koje servisiraju te centre. S druge strane, štete od lokalizacije podataka su raširene, na teret malih sredjih i velikih preduzeća kojima je onemogućen pristup globalnim uslugama koje im mogu poboljšati produktivnost." Ibid. str. 35.

[406] „Izgradnja data centra u Brazilu košta u proseku 60,9 miliona USD, a izgradnja u Čileu i SAD-u koštaju 51,2 miliona USD odnosno 43 miliona USD. Funkcionisanje data centra ostaje skupo zbog velikih troškova energenata i drugog – mesečno u proseku 950.000 USD u Braziilu, 710.000 u Čileu i 510.000 u SAD-u." Ibid. Str.36-37.

[407] Ibid. Str.7.

upravo u smeru veće lokalizacije podataka. Neke od vodećih zamalja EU preduzele su određene korake i samostalno, ne čekajući na ove reforme na nivou EU.

Francuska je investirala sredstva u sopstvenu infrastrukturu data centara, odnosno finansirala je dve kompanije Numergy i Cloudwatt za usluge oblaka (za skladištenje podataka), koji su nazvani „suvereni oblaci“ (serveri su na teritoriji Francuske). Takođe je u opticaju i predlog novog „poreza na podatke“ tj. predlog da se oporezuje „prikupljanje, upravljanje i komercijalna eksploatacija ličnih podataka generisanih od strane korisnika lociranih u Francuskoj“. Taj porez, koji bi plaćale strane kompanije koje zarađuju na podacima, bi smanjio prednost tih usluga koje su locirane van zemlje pa bi ove kompanije odlučile da drže podatke u Francuskoj.[408]

Nemačka je nakon afere Edvarda Snoudena objavila da će prekinuti saradnju sa bezbednosnim službama drugih država dok se ne dokaže da ove službe deluju u skladu sa principima zaštite ličnih podataka koji su valdini u EU. Uz to, Nemački telekom je lansirao uslugu „e-mail made in Germany“ tj. uslugu kod koje se rutiranje podataka obavlja samo kroz domaće servere.[409]

Kina zabranjuje (čak i kada je reč o aktu koji se formalno naziva „tehničkim smernicama“) transfer ličnih podataka van granica bez izričitog pristanka subjekta podataka ili eksplicitnog odobrenja regulatora, a ima i regulativu u cilju zaštite podataka vezanu za sektor banaka.[410] Pristanak subjekta podataka (veoma detaljan) na transfer njegovih/njenih podataka uvela je i Južna Koreja.[411] Ova zemlja je poznata i po tome što je zabranila inostrani pristup geografskim mapama svoje teritorije. (Navodno je mapu Južne Koreje, papirnu ili elektronsku, moguće dobiti samo u Južnoj Koreji.)

Indonezija, Malezija i Australija su donele propise kojima se zahteva uspostavljanje domaćih servera i data centara za razne oblike javnih usluga koje se tiču njihovog stanovništva.

Kazahstan pak zahteva da svi internet domeni sa kodom .kz rade na serverima fizički lociranim na teritoriji ove države.

Smatram da ove mere nikako ne vode razbijanju interneta, kako poručuje naslov teksta Čandera i Lea, niti da se mogu smatrati dovoljnim za zaključak da era globalnog interneta prolazi. Ove mere samo ukazuju da se priprema teren za novo

[408] Ibid. Str. 12.
[409] Ibid. Str. 15.
[410] Ibid. Str. 9.
[411] Ibid. Str. 22.

uređenej tj. ukidanje haosa koji je do nedavno vladao u pogledu raspolaganja ličnim podacima (i metapodacima) korisnika interneta.

Jedan izveštaj Svetskog ekonomskog foruma iz 2014. godine primetio je: rast podatka, sofisticiranost sveprisutnih kompjutera i protok podataka preko granica su rasturili sposobnost da se time efektivno upravlja na globalnom nivou.[412] Čini se da se ipak sa time ne moramo složiti. Efektivno upravljanje je moguće na nacionalnom a verovatno i na supranacionalnom nivou, posebno ako postoji odlučnost u tom smislu kod donosilaca odluka i krajnjih korisnika.

Krajnji zaključak ovog razmatranja je da je običan korisnik interneta u stanju, ako to želi, da se bori protiv nadzora koji nad njim vrše države i kompanije. Na raspolaganju mu je enkripcija, plaćanje za usluge do kojih mu je stalo na internetu, bojkot kompanija koje neetički i nezakonito postupaju, digitalni aktivizam protiv nadzora, posredno učešće u regulisanju interneta posredstvom države i verovatno neke nove opcije koje će se pojaviti u budućnosti, posebno u domenu interneta stvari. Zato se na kraju ovog rada daje mišljenje da se masovni nadzor na internetu može zaustaviti. Ključ zaustavljanja masovnog nadzora na internetu nalazi se u preuzimanju odgovornosti za sebe od strane običnih korisnika interneta. U krajnjem, moralno vrednovanje interneta, to da on bude na strani jačanja slobode i jednakosti, polazi od ponašanja običnih korisnika:

- njihovog pristanka ili nepristanka na to da budu praćeni dok su na internetu (lojalnost prema kompanijama koje su trakeri),
- njihove spremnosti ili nespremnosti da plate realnu novčanu cenu internet usluga umesto čega onda ta cena bude prikrivena i plaćena u valuti njihove privatnosti i
- njihovog izbora između blagonaklonosti prema konforu koji nudi internet stvari u zamenu za lične podatke i insistiranja na enkripciji gde god je to moguće u što većem stepenu.

[412] World Economic Forum (WEF) with A.T.Kearney, *Rethinking Personal Data: A New Lens for Strengthening Trust*. May 2014, dostupno na http://reports.weforum.org/rethinking-personal-data/ Ovde navedeno prema „Next Generation Privacy“ Str. 120-121.

DESETO POGLAVLJE

Zaključak

U ovom istraživanju se pošlo od toga da se filozofija uvek bavila i bavi onim što je bitno za ljudski život i da je odnos koji je uspostavljen između čoveka i interneta takav, da zaslužuje da se filozofija okrene tom fenomenu. Takođe se podrazumevalo da je filozofija jedinstveno pogodna da u ovoj temi (kao što radi sa svim temama) rasvetli i objasni ono podrazumevano, mit, racionalno saznanje, vrednosti, očekivanja i dr. Zato se tražio odgovor na pitanje:

- **kako filozofski odrediti i moralno vrednovati internet 2015. godine?**

Rezultat tog ispitivanja bi trebalo da pomogne nama, korisnicima interneta, da se kao moralni subjekti bolje snalazimo u svojim ulogama učesnika, kreatora, žrtava ili odlučioca o promenama interneta.

U istraživanju je odabran pristup da se internet sagleda iz onog njegovog dela koji je nevidljiv korisnicima. Internet je određen kao tehnologija, tehnološki izum i inžinjerski artefakt (mreža kompjuterskih mreža) koji ima svoj dizajn i koji je promenljiv. To je tehnički sistem, koji je kolekcija raznih komponenti, a neke među njima se mogu smatrati nužnim i dovoljnim uslovima interneta. Postavljeno je potpitanje:

- **koje su osnovne komponente interneta kao tehničkog sistema?**

Određeno je 5 elemenata (protokol kontrole transfera/internet protokol, skraćeno TCP/IP, sistem imena domena, skraćeno DNS, autonomni sistemi i protokol rutiranja, skraćeno AS i BGP, pružaoci ili provajderi internet usluga, skraćeno ISP i regionalni internet registri, skraćeno RIR) kao osnovna ili ključna infrastruktura interneta i objašnjen je njihov nastanak i funkcionisanje.

Kao tehnički sistem internet ima određeni dizajn, koji se može analizirati preko pojma arhitekture interneta. Proučavanje njegove arhitekture daje pogled na dešavanja, karakteristike i vrednosti implicirane u ovom tehnološkom sistemu. Postavljeno je potpitanje:

- **šta je sadržavala i sadrži arhtektura interneta?**

Arhitektura sa kojom je internet otpočeo svoj život je bila: komunikacioni sistem na bazi razmene paketa u kome se više odvojenih mreža povezuje preko procesora razmene paketa nazvanih ruteri. Distinktivni princip arhitekture od samog nastanka

interneta je E2E ili princip s-kraja-na-kraj. Ovaj princip je uveo odustvo diskriminacije u mreži i razdvojio da je posao mreže da prenosi datagrame (onoliko efikasno i fleksibilno koliko je moguće), a sve drugo treba da se obavlja na krajevima. Uz njega je išao čitav niz principa dizajna koji su skupa osnaživali otvoren i slobodan internet. Međutim, kako se internet širio i dolazili novi akateri, ovi prinicipi su potiskivani, gubila se koherentnost u mreži, novi akteri prilagođavali mrežu svojim potrebama. Oko 2005/06. godine stiglo se do tačke u razvoju komunikacionih tehnologija, u kojoj je najvažnije kako izgraditi, primeniti i imati u funkciji distribuirane aplikacije sa velikim brojem korisnika. Potisnuto je shvatanje da se aplikacije nalaze na krajevima sistema, a mreža nosi pakete. Aplikacije su prevagnule i došle u poziciju da prave mrežu po svojim potrebama. Izgubljena je transparentnost interneta. Time je prikazana putanja od uvođenja do napuštanja arhitekture iz razmatranja o dizajnu interneta.

Dalje, napuštanje arhitekture dodatno smo kvalifikovali navodeći dva aspekta koji su «preživeli». Prvi aspekt inicijalno tesno vezan sa arhitekturom, koji je nadživeo sve promene, je praksa izrade RFC-ova. Sama po sebi ta praksa ne može sačuvati izvorni smisao interneta u duhu njegovih pionira ali se ustoličava kao njegov zaštitni znak. Drugi je hipoteza o izuzetnosti interneta zbog koje bi on mogao opstati bez promene njegove inicijalne ideologije, pod uslovom da korisnici odluče da to žele. Radi se o hipotezi koja izvire iz paralele između američke izuzetnosti (u De Tokvilovom smislu) i izuzetnosti interneta (u smislu ideologije).

Nakon analize napuštanja arhitekture iz dizajna interneta, postavilo smo pitanje:

- **šta se dešava kada (više) nema arhitekture interneta, ali ima interneta**?

Filozofsko sagledavanje interneta, koji se razvija kontinuirano i u post-arhitekturalnoj fazi, usmereno je na tri post-arhitekturalne teme vezane za dizajn interneta: upravljanje internetom, njegovu interakciju sa teritorijalnim fenomenima i njegovu interakciju sa ekonomskim fenomenima.

- Postavljeno je potpitanje: **kakvo je upravljanje internetom?**

Upravljanje internetom je višeslojno i višeaktersko, te su izdvojene glavne odrednice. Internetom kao globalnim tehničkim sistemom upravljaju pre svega transnacionalne organizacije kao što su IETF i ICANN koje se staraju za upravljanje ključnom infrastrukturom interneta (protokolima, IP adresama i domenima). Uz to je sagledana realnost prisustva posebnog tipa mrežnog upravljanja, posebno vidljivog na delu kod

autonomnih sistema i rutiranja, a to je tip neformalnog ad hoc upravljanja koji čuva odnos moći među akterima (ISP-ovima) kojim su akteri trenutno zadovoljni.

Suverene države imaju ulogu upravljača interneta na svojoj teritoriji, pre svega kroz uticaj na ISP-ove, dok je njihova uloga u međunarodnoj areni ambivalentna. S jedne strane, u izvesnoj meri postoje pokušaji saradnje država oko zajedničke borbe protiv sajber kriminala, ali je s druge strane u određenoj meri je prisutna najčešće prikrivena sajber konfrontacija između pojedinih država. Najbolji opis stanja onog što se događa je međunarodna debata o upravljanju internetom, koja za sada nije dostigla koncenzus.

Upravljanje internetom nije sprečilo da se pojavi neupravljani internet tzv. tamni internet iliti mračna strana javnog interneta Objašnjeno je kako je tamni internet moguć zahvaljujući kriptografiji i posebno je istaknuto šta sve stiže iz tamnog interneta. Prvo, stiže konstantno sajber kriminal, jer je tami internet pravo tržište sajber kriminalnih usluga, i drugo, stigla je 2013. godine afera Edvarda Snoudena, koja je najširoj javnosti otkrila bitne informacije o arhitekturi interneta. Njegove informacije kažu: internet je nadzirana mreža mreža, a nadziru je bezbednosne službe SAD-a i drugih država.

Međutim, ukazano je i da je puna istina to da je internet sa više strana nadzirana mreža Osim jedne ili više država i osim kriminalaca, internet nadziru i komercijalni akteri, privatne kompnaije koje posluju preko interneta. Dok kriminalci nemaju nikakvo opravdanje zašto to čine, a država pokušava da opravda to postupanje nacionalnim interesom tj. opštim dobrom, privatne kompanije kao argument za praćenje i skupljanje podataka korisnika nude interes samih nadziranih tj. korisnika (jer će kroz prikupljenje informacije o njima biti u stanju da im pruže bolju ili jeftiniju uslugu).

U toj situaciji neizbežno je da se istakne uloga samih (nadziranih) korisnika interneta. Tamni internet je uputio izazov običnim korisnicima interneta da se suoče sa realnošću.interneta koji konzumiraju. Čini se da za sada korisnici nisu do kraja preuzeli odgovornost za same sebe.

- Postavljeno je potpitanje: **kako internet intereaguje sa teritorijalnim fenomenima?**

Jedan mali broj lokacija prima, razmenjuje i transmituje veliki deo internet saobraćaja i komunikacija na planeti. A te lokacije su tu gde jesu zbog razloga geografije, istorije i novca. Razmatrajući materijalno-prostornu realizaciju interneta istaknuta je veza

između okosnice interneta i velikih gradova tj. urbanih oblasti širom sveta. Fizička baza interneta, optički kablovi, moćni serveri i dr. premrežuju celu planetu, ali se najintenzivnije koncentrišu u alpha, beta i gamma svetskim gradovima. Internet ne samo da osnažuje urbanu hijerarhiju, nego preslikava odnose moći i nejednakosti koje postoje u oflajn svetu. Ogleda se to i na mapi cenovne dostupnosti širokopojasnog interneta u svetu, mapi brojnosti internet domena po zemljama, mapi internet imperija i dr.

Iz svoje ranije faze, internet je do danas zadržao vezu sa jednom metaforom – sajber spejsom. Ova metafora je u izvesnoj meri prepreka razumevanju interneta kao «mesta» koje se konstituiše raznovrsnim obrascima i praksama vezanim za interakciju između informaciono-komunikacionih tehnologija i društva, interakciju između ljudi, informacija, protokola (koda) i mašina/računara. Stoga je zadatak koji stoji pred običnim korisnicima da na primereniji način «teritorijalizuju» (demistifikuju) digitalnu mrežu odnosno internet. Poenta nije da treba prestati koristi reč sajber spejs, već da običan korisnik treba da obrati pažnju na mnoštvo načina za konceptualizovanje tokova informacija kroz internet i da analizira načine na koje on sam konzumira, komunicira i kreira preko interneta.

- Postavljeno je potpitanje: **kako internet intereaguje sa ekonomskom sferom života?**

Ekonomski interesi su se umešali u razvoj interneta najpre u zadnoj deceniji 20. veka. To je ostvareno tako što su izvršene njegova privatizacija i komercijalizacija. Okosnica interneta, poznata kao NSFNET (mreža Nacionalne fondacije za nauku) odlukom vlade SAD-a je privatizovana 1995. godine, a sistem imena domena (DNS) takođe odlukom vlade SAD-a je privatizovan 1998. godine. Ove privatizacija su imale za posledicu stvaranje monopola/oligopola a ne konkurencije, i samim tim interes javnosti nije došao u prvi plan kada se odigrala promena finansiranja infrastrukture interneta. Vlada SAD-a, koja je dugi niz godina finansirala ovu infrastrukturu, prepustila je da dalje finansiranje preuzme na sebe privatni biznis, a privatni biznis je to uradio jer je bilo očigledno da će i obični korisnici interneta biti spremni da plaćaju internet usluge, gde će se otvarati i prostor za profit privatnog biznisa. Veličinu profita pak presudno je odredio oligopolni/monopolski položaj nekoliko kompanija.

Internet je uticao na promenu ukupne ekonomije time što je omogućio nastanak internet kompanija ili dot.com-a koje su uvele novine u dotadašnji način poslovanja, a time i prisilile tradicionalne kompanije da prate taj trend. Razvoj dot.com-a od druge

polovine 1990-tih zaživeo je zahvaljujući podršci finansijskih tržišta i investicionih fondova. Pokazano je da su i u 2015. godini investicioni fondovi skloni da podržavaju inovativne (tehnološke) kompanije koje svoje poslovanje baziraju na internetu, s tim da su sada aktuelne kompanije koje nude proizvode i usluge za internet stvari.

Internet stvari označava internet na koji se priključuju najrazličitiji senzori i aktuatori smešteni u/na fizičkim objektima da bi se među njima odvijala komunikacija putem interneta To je internet dosta drugačiji od onog koji poznajemo jer tu ne više ljudi nego fizički objekti šalju elektronske informacije putem interneta. Tu fizički objekti prestaju da budu jednostavni fizički objekti i postaju informaciono-komunikaciona tehnologija. Internet stvari je najverovatnije internet budućnosti. Ono što za sada nedostaje je mišljenje običnih korisnika interneta o internetu stvari. Da li će im se dopasti ponuda ili će ostati uzdržani – možda je još prerano znati jer ni sami ti proizvodi i usluge nisu do kraja spremni za tržište.

Kroz ispitivanje tri prethodna potpitanja uvek se moglo uočiti da vode ka ili upućuju na običnog korisnika interneta. On je taj koji je nadziran, i treba da učini nešto povodom toga. On je taj koji umesto metafore sajber spejsa treba da konptualizuje internet kao prostor koji počiva na interakcijama i u koji se preslikavaju sve oflajn strukture, uključujući nejednakosti. On je taj koji će prihvatiti internet stvari ili ga odbaciti. Da bi se našlo objašnjenje o utemeljenju tih očekivanja od običnog korisnika, postavljeno je pitanje:

- **kakva je pozicija na internetu koja pripada običnom korisniku?**

Infrastrukturne odlike interneta koje proističu iz načina upravljanja i neupravljanja njime, načina materijalnog rasprostiranja i načina razvoja diktiranog ekonomskim faktorima., kao i one arhitekturalne o kojima je bilo reči ranije, veoma direktno su kreirale i kreiraju položaj običnog korisnika na internetu. Ali taj položaj takođe zavisi i od samog korisnika, njegove aktivnosti ili pasivnosti. Zato je data analiza položaja običnog korisnika iz ugla resursa, alata i potencijala ugrađenih internetom u taj položaj, odnosno sagledan kroz internetom proizvedenu redistribuciju moći između običnog korisnika i drugih aktera.

Dobici za običnog korisnika u internet okruženju su veoma veliki. To su doprinos uvećanju individualne slobode, veće mogućnosti za pristup kulturi i kreiranje kulture, doprinos dostupnosti i efikasnosti obrazovanja, restrukturisana javna sfera u kojoj je osnažen pojedinac, šanse za ekonomski prosperitet na bazi lične inovativnosti i internet ekonomije.

Posebno je akcentovan doprinos interneta razvoju znanja kroz fenomen platformi za onlajn učenje i masovnih otvorenih onlajn kurseva na njima, koje su nastale 2012. godine. U formi studije slučaja izloženo je lično iskustvo jedne korisnice MOOK-ova iz filozofije iz Republike Srbije tj. autorke.

Sagledane su i razne vrste političkog aktivizma povezanog sa internetom. Data je analiza odnosa snaga vlade i vladinih oponenata u načelu. Prikazan je pogled na aktivizam iz vizure spoljne politike, iz vizure internet kompanija i konačno iz vizure podkulturnih alternativnih grupacija i pokreta.

Gubitak za običnog korisnika se prvenstveno ogleda u smanjenju, možda čak i nestanku privatnosti pojedinca, kroz izloženost nadzoru i kroz svođenje korisnika interneta na robu.. Kulminacija „napada“ na privatnost je dovela do tačke kada se treba preispitati njeno značenje u post-Snouden eri. Obični korisnici su tada, ako ne i ranije, morali najjasnije primetiti i svoju izloženost i ranjivost na internetu i vrednost „svojih“ podataka (jer zbog čega bi oni bili prikupljani, izuzev zašto što imaju vrednost?).

S obzirom na implikacije koje proizlaze iz pozicije običnog korisnika interneta, koje nisu samo manifestovane kao dobici za korisnika kao moralno autonomog subjekta, građanina i učesnika političke javne sfere, kulturno biće i ekonomskog aktera, nego na žalost podrazumevaju i gubitak privatnosti, bilo je potrebno razmatranje čiji fokus je na privatnosti korisnika i mogućim odnosima prema njoj. Postavljeno je potpitanje:

- **kakva je zaštita ličnih podataka na internetu?**

Najpre je ukazano na dilemu čuvati ili prodati lične podatke, s obzirom da postoji i linija razmišljanja (a i po neki primer iz prakse) po kojoj, ako su već podaci nova vrsta imovine tj. nova vrsta robe, vlasnik podataka je slobodan da odluči da te podatke dobrovoljno proda kome god želi. (Ono što treba zapaziti je da je ovde implicitna pretpostavka da moji podaci nisu ja, već su nusproizvod mog življenja u digitalnom dobu. To je pretpostavka koja se može tematizovati, pa i odbaciti, ali to izlazi iz okvira ovog rada.) Ipak, sa prodajom ličnih podataka postoje praktične teškoće oko samog dobijanja u posed svojih podataka od operatera u čijim rukama se nalaze i oko realne vrednosti i cene tih podataka.

Potom je prikazan okvir zaštite privatnih ličnih podataka koji daje Direktiva Evropske unije iz 1995. godine, smer reforme evropskog režima zaštite ličnih podataka i tzv. pravo da budeš zaboravljen/a, koje predstavlja prekretnicu u odnosu moći između korisnika i internet kompaija koje skupljaju lične podatke. Evropski sud pravde je

eksplicitnim davanjem veće težine privatnosti u odnosu na ekonomski interes kompanija i na pravo javnosti da zna stao je na stranu običnih korisnika, čime je ograničio dominaciju interesa profita internet kompanija. Isto tako, jedan broj država je krenuo ka uspostavljanju veće kotrole nad «izvozom» ličnih podataka svojih građana, što takođe ulazi u debatu o reformi sistema zaštite podataka (za sada barem) u Evropi. Time se u dobroj meri dobija osnov za osporavanje teze da je upotrebom ličnih podataka nemoguće efektivno upravljati (na globalnom nivou). Ispostavilo se da je efketivno upravljanje moguće na nacionalnom, a verovatno i na supranacionalnom nivou, posebno ako postoji odlučnost u tom smislu kod donosilaca odluka i krajnjih korisnika.

Iz svega iznetog stiže se do odgovora o tome kako filozofski odrediti i moralno vrednovati internet 2015. godine.

Najupečatljivija osobina interneta je njegova otvorenost. Ona je sadržana u tri bitna uslova:[413] tehnička izvedba/konstrukcija mreže je decentralizovana, svi protokoli su otvoreni tj. javno dostupni i podložni modifikacijama i institucije «vlasti na internetu» su otvorene za saradnju aktera i obraćaju pažnju na javni interes.

Internet je prožet vrednostima libertarijanske kulture, jer je u njegovom središtu slobodan pojedinac. Tačno je da u mreži postoje brojni moćni akteri, komericjalni, kriminalni, politički i drugi, u odnosu na koje je slobodan pojedinac manje moćan. Međutim, mreža je tako oblikovana da je pojedincu dozvoljeno samo-usmeravanje na internetu.[414] Kao instance samo-usmeravanja se mogu navesti: samo-objavljivanje (komuniciraj šta želiš), samo-organizovanje (komuniciraj kako želiš), samo-umrežavanje (komuniciraj s kim želiš). Ovi u mreži ugrađeni obrasci ponašanja pojedincu na internetu omogućavaju da bude suveren kao «kraj mreže» i čuvaju njegovu moć donosioca odluka.

Ako bi se moglo kantovski reći da slobodni pojedinac ima neku dužnost prema sebi, u načelu, onda bi u pogledu interneta ta njegova dužnost bila podrška istini o internetu jer jedino tako može biti kompetentan i informisan donosilac odluka. Videli smo da postoje heroji istine na internetu, ali običan korisnik ne mora ići tako daleko. Njegova dužnost bi bila da ne podržava niti dozvoljava (pravno, komercijalno, obrazovno itd.) sprečavanje softvera za enkripciju. Jedina garancija koja može postojati za to da će se

[413] Manuel Castells, Opus cit. Str. 40.
[414] Ibid. str. 66.

istina o internetu čuti je postojanje softvera za šifriranu komunikaciju i područje tamnog interneta.

Istina o internetu u sadašnjem momentu, oko koje postoji opšta saglasnost, jeste da internetom vlada nadzor nad korisnicima. Ovaj nadzor često se poredi sa situacijom iz Bentamovog panoptikona[415] ili Fukoovog razmatranja o njemu[416]. Panoptikon paradigma je manjkava jer svodi korisnika interneta na zatvorenika i nemoćnog aktera. Moguć je alternativni pogled na stvari u kome je korisnik u stanju, ako to želi, da se bori protiv nadzora koji nad njim vrše države i kompanije. Zato se na kraju ovog rada razmotrilo da li se masovni nadzor na internetu može zaustaviti i zaključilo da je to moguće.

Krajnji zaključak ovog razmatranja je da je običan korisnik interneta u stanju, ako to želi, da se bori protiv nadzora koji nad njim vrše države i kompanije. Na raspolaganju mu je enkripcija, plaćanje za usluge do kojih mu je stalo na internetu, bojkot kompanija koje neetički i nezakonito postupaju, digitalni aktivizam protiv nadzora, posredno učešće u regulisanju interneta posredstvom države i verovatno neke nove opcije koje će se pojaviti u budućnosti, posebno u domenu interneta stvari. Zato se na kraju ovog rada daje mišljenje da se masovni nadzor na internetu može zaustaviti. Ključ zaustavljanja masovnog nadzora na internetu nalazi se u preuzimanju odgovornosti za sebe od strane običnih korisnika interneta. U krajnjem, moralno

---

[415] Ideja o panoptikonu je opisana u *Predlogu za novi i jeftiniji način korišćenja i refome zatvora* Džeremija Bentama (Jeramy Bentham) iz 1798. godine. Panoptikon je zapravo zatvor, napravljen kao zgrada kružnog oblika, sa ćelijama na obodu i zatvorskim čuvarima u sredini kruga. Čuvari bi mogli biti skriveni od pogleda zatvorenika, ali bi osećaj opšteprisutnosti postojao jer iz centra kruga oni imaju stalan i savršen pogled na svaku ćeliju sa zatvorenikom (s kojim komuniciraju putem cevi). Čuvari bi imali psihološku nadmoć nad zatvorenicima ali bi se time osiguralo da zatvorenici promene svoje ponašanje i rade više kako bi izbegli kažnjavanje. Bentam je smatrao da je to humana institucija, u poređenju sa tadašnjim zatvorima, i da bi panoptikon imao višestruke koristi (popravljen moral, očuvano zdravlje, podstaknuta vrednoća, difuzno poučavanje, manji javni troškovi, gordijev čvor zakona o siromašnim raspetljan, sve na bazi jednostavne ideje arhitekture). Navedeno prema https://www.ucl.ac.uk/Bentham-Project/who/panopticon

[416] Mišel Fuko (Michael Foucault) je preuzeo Bentamovu ideju i razvio je dalje u delu *Nadzirati i kazniti. Rađanje zatvora.* Odatle potiče njegova izreka da je vidljivost zamka. "Panoptikon je mašina koja razdvaja dijadu videti / biti viđen: u perifernom prstenu, čovek je totalno viđen bez da ikada vidi; u centralnom tornju, čovek vidi sve bez da je ikada viđen." On apostrofira Bentamov uvid da se time dobija moć jednog uma nad drugim. „Stoga je glavni efekt panoptikona: stvoriti u zatvoreniku stanje svesne i permanentne vidljivosti koje osigurava automatsko funkcionisanje moći. Tako urediti stvari da je nadzor stalan po efektima, čak i ako je diskontinuiran u praksi; da savršenstvo moći teži da učini svoju aktuelnu primenu nepotrebnom, da arhitektonski sklop bude mašina za stvaranje i održavanje odnosa moći nezavisno od osoba koje su nosioci." Moć o kojoj je reč je moć disciplinovanja tipična za moderno doba. Preuzeto sa http://foucault.info/doc/documents/disciplineandpunish/foucault-disciplineandpunish-panopticism-html

vrednovanje interneta, to da on bude na strani jačanja slobode i jednakosti, polazi od ponašanja običnih korisnika:

- njihovog pristanka ili nepristanka na to da budu praćeni dok su na internetu (lojalnost prema kompanijama koje su trakeri),
- njihove spremnosti ili nespremnosti da plate realnu novčanu cenu internet usluga umesto čega onda ta cena bude prikrivena i plaćena u valuti njihove privatnosti i
- njihovog izbora između blagonaklonosti prema konforu koji nudi internet stvari u zamenu za lične podatke i insistiranja na enkripciji gde god je to moguće u što većem stepenu..

Direktno preuzimanje odgovornosti korisnika interneta bi vodilo uskraćivanju pristanka na praćenje, odricanju od lažne besplatnosti i odbijanju konfora koji ne osigurava privatnost, a verovatno i u ulaženje u sukob sa svima onima koji to ne poštuju. Za direktno preuzimanje odgovornosti potrebno je da moralni agent poseduje informisanost i kompetentnost, što važi za pristanak i odlučivanje u načelu (za bilo koju oblast života).

Indirektno preuzimanje odgovornosti bi bilo prepuštanje da država reguliše i ograniči upotrebu ličnih podataka. Pojedinac bi tu ukazao državi poverenje da brani njegov integritet, što nije samo po sebi nužno loše ili opasno (tako se dešavalo i u drugim oblastima života, na pr. regulacije saobraćaja, bezbednosti hrane i sl.). Ipak, rađa se i sumnja u to da bi specifičnost interneta za državu mogla biti izazov, jer bi zahtevala sasvim nov zakonodavni model. Mnogi su ukazali da je masovni nadzor u 2015. godini takav da bi bio samo u domenu naučne fantastike pre 30-ak godina i da je opasno primeniti stare modele na nove tehnologije. Mora se izbeći da se komunikacijama 21. veka upravlja uz pomoć modela iz 19. i 20. veka.[417] Ako bi država to izbegla, onda bi se i iz njene intervencije moglo stići do toga da internet u budućnosti očuva svoje sadašnje vrednosti ili barem ne odstupi drastično od njih.

Konačno, korisnici mogu i da ne tretiraju aktuelni kontekst u kome se nalaze, niti direktno niti posredstvom države. To nikakvo preuzimanje odgovornosti značilo bi stavljanje sopstvene sudbine i sudbine interneta u ruke kompanija i drugih entiteta, sa kojima korisnik ulazi na nepoznatu teritoriju. To je legitiman mada nije preporučljiv izbor. Autorka se nada da se, uz dovoljno podizanja svesti, taj izbor neće desiti.

[417] G. Michael Fenner. «Edward Snowden: Hero or Traitor». *Nebraska Lawyer*, November/December 2014. str. 19.

Internet treba koristiti, njegove dobre strane treba ugraditi u sopstvene životne izbore i životni stil, kao i u društvo čiji smo deo. Njegova loša strana, pretvaranje komunikacione tehnologije u tehnologiju za masovni nadzor, ne sme nas prepasti i zbuniti. Osnovna svrha ovog rada bila je davanje podloge za podizanje svesti o ulozi koju bi sami korisnici trebalo da odigraju u odnosu na trendove koji vode ka nadziranom internetu. Ako ta uloga bude pametno zamišljena i odigrana, pitanje zaštite ličnih podataka i zaštite privatnosti bi moglo biti prevaziđeno za 5 ili 10 godina. No, internet stalno menja svoju prirodu, tako da će se za 5 ili 10 godina otvoriti neka nova pitanja.

POPIS TABELA I ILUSTRACIJA

KORIŠĆENA LITERATURA

Knjige:

Asanž, Dž. (2013). *Sajferpanks. Sloboda budućnost interneta*. Beograd: Albion Books.

Benkler, Y.(2006). *The Wealth of Networks. How Social Production Transforms Markets and Freedom.* New Haven & London: Yale University Press.

Blum, A. (2012). *Tubes: Behind the Scenes at the Internet.* London: Penguin Books.

Bobbitt, P. (2002). *The Shield of Achilles: War Peace and the Course of History* New York: Anchor Books.

Bygrave, L. A. and Bing, J. (eds.). *Internet Governance: Infrastructure and Institutions*. New York: Oxford University Press.

Cairncross, F. (1997). *The Death of Distance: How the Communications Revolution Is Changing Our Lives*. Boston, Harvard Business School Press.

Castells, M. (2003). *Internet galaksija. Razmišljanje o internetu, poslovanju i društvu*. Zagreb: Naklada Jesenski i Turk.

Goldsmith,J. and Wu, T. (2006). *Who Controls the Internet? Illusions of a Borderless World*. New York: Oxford University Press.

Greenwald, G.(2014). *No Place to Hide: Edvard Snowden, the NSA and the US Surveillance State.* Picador.

Kurbalija, J. (2011). *Uvod u upravljanje internetom*. Beograd: Albatros plus.

Lesig, L. (2006). *Slobodna kultura*. Beograd: Službeni glasnik.

Lessig, L. (2006). *Code: version 2.0*. New York: Basic Books.

Morozov, E. (2011). *The Net Delusion: The Dark Side of Internet Freedom*. New York: Public Affairs.

Morozov, E. (2013). *To Save Everything, Click Here: The Folly of Technological Solutionism*. New York: Public Affairs.

Štavljanin, D. (2013). *Balkanizacija Interneta i smrt novinara*. Prag & Beograd: Radio Slobodna Evropa & Čigoja štampa.

Wu, T. (2010). *The Master Switch: The Rise and Fall Of Information Empires.* New York: Vintage Books.

Zittrain, J. (2008). *The Future of the Interne and How to Stop It.* New Haven & London: Yale University Press.

Članci u zbornicima:

Milošević, M. i Nikač, Ž. (2010). „Izmene u zakonodavstvu Republike Srbije i borba protiv visokotehnološkog kriminala“ (str. 236-244). *Zloupotreba informacionih tehnologija i zaštita*, Petrović, S.R. (ur.) Beograd: IT Veštak.

Vermesan, O., Friess, P., Guillemin, P., Gusmeroli, S., Sundmaeker, H., Bassi, A., & oth. (2011). „Internet of Things Strategic Research Roadmap“. (9-52) *Internet of Things - Global Technological and Societal Trends*..Vermesan, O. and Friess, P., (eds.). River Publishers.

Wu, T. (2010). “Is Internet Exceptionalism Dead?”(179-188) *The Next Digital Decade: Essays on the Future of the Internet*. Szoka, B. and Marcus, A. (eds.) Washington: TechFreedom.

Članci u naučnim časopisima:

Allman, E. (2011). „The Robustness Principle Reconsidered: Seeking a Middle Ground". *Communications of the ACM*, Vol. 54, No.8, 40-45.

Cerf, V.G. and Kahn, R.E. (1974). “Protocol for Packet Network Intercommunication”. IEEE Trans on comms, Vol Com-22

Chander, A. and Le, U.P.(2014). „Breaking the Web: Data Localization vs. the Global Internet“. *US Davis Legal Studies Research Paper Series*.

Clark, D.D. (1988).“The Design Philosophy of the DARPA Internet Protocols”. *Computer Communicatin Review*. Vol 18, No.4, 106-114.

Clark, D.D. (2007). “Network Neutrality: Words of Power and 800-Pound Gorillas”. *International Journal of Communication* 1, 701-708.

Clark, D.D., Sollins, K.R., Wroclawski, J.& Braden, R.. (2002). “Tussle in Cyberspace: Defining Tomorrow’s Internet” u *SIGCOMM*’ 2, 347-356.

Clark, D.D., Sollins,K., Wroclawski, J.& Faber, T. (2003). “Addressing Reality: An Architectural Response to Real-World Demands on the Evolving Internet”. *ACM SIGCOMM Workshop on Future Directions of Network Architecture 2003,* 247-257.

Cunningham, M. (2012). “Privacy in the age of the Hacker: Balancing global privacy and data security law”. *The George Washington Interational Law Review,* Vol. 44, 643-697.

Cunningham, M. (2014). „Next Generation Privacy: The Internet of Things, Data Exhaust, and Reforming Regulaltion by Risk of Harm“. *Groningen Journal of International Law*, Vol. 2(2), 115-144.

Hu, M. (2015). “Taxonomy of the Snowden Disclosures”. *Washington and Lee Law Review*, Vol. 72. 1679-1769.

Kesan, J.P. and Shah, R.C. (2001). “Fool Us Once Shame On You – Fool Us Twice Shame On Us: What We Can Learn From the Privatizations Of the Internet Backbone Network and the Domain Name System”. *Washington University Law Quarterly* Vol. 79, 89-219.

Libert, T. (2015). “Exposing the Hidden Web: An Analysis of Third-Party HTTP Requests on One Million Websites”. *International Journal of Communication*, arXiv:1511.00619

Malecki, E. J. (2002). “The Economic Geography of the Internet’s Infrastructure”. *Economic Geography* Vol. 78, No 4, 399-424.

Mark Graham, M. (2013). „Geography/Internet: Ethereal Alternate Dimensions of Cyberspace or Grounded Augmented Realities?“ *The Geographical Journal* 179(2), 177-182.

Mueller, M., Schmidt, A. and Kuerbis, B. (2013). “Internet Security and Networked Governance in International Relations” *International Studies Review* Vol. 15 (1), 86-104.

Peppet, S.R., (2014). „Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security & Consent“. *Texas Law Review* Vol. 93, 85-177.

Rid, T. (Feb. 2012) „Cyber War Will Not Take Place“ *Journal of Strategic Studies*, Vol. 35, 5-32.

Rischmann, B.M. (2004) “The Prospect of Reconciling Internet and Cyberspace”, *Loyola University Chicago Law Journal*, Vol. 35, 205-234.

Roscoe, T. (2006). “The End of Internet Architecture”. *SIGCOMM*, pp.55-60.

Saltzer, J.H., Reed, D.P.and Clark, D.D. (1984). „End-to-End Arguments in System Design“. *ACM Transactions in Computer Systems*, Vol. 2, No 4, 277-288.

Sassaman, L., Patterson, M.L. and Bratus, S. (2012). “A Patch for Postel’s Robustness Principle”. *Secure Systems*, March/April, 87-91.

Ostali članci i studije:

CB Insights. (2015). *Analyzing the Internet of Things Investment Landscape*. Preuzeto sa: www.cbinsights.com.

Cisco Global Business Network. (2010). *The Evolving Internet: Driving Forces, Uncertainties and Four Scenarios to 2025*, Preuzeto sa: http://newsroom.cisco.com/dlls/2010/ekits/Evolving_Internet_GBN_Cisco_2010_Aug_rev2.pdf

De Montjoye, Y.A., Hidalgo, C.A., Verleysen, M. & Blondel, V.D. (2013). *Unique in the Crowd: The Privacy Bounds of Human Mobility*, 3 scientific report doi:10.1038/srep01376

Deering, S. *Watching the Waist of the Protocol Hourglass*, IETF 51, London. Preuzeto sa: http://www.cs.virginia.edu/~cs757/slidespdf/////deering-hourglass-london-ietf.pdf

Dutton, W. H.. (2013) *The Internet of Things* OII Working Paper commissioned as part of the UK Government's Proceedings of Foresight Horizon Scanning Papers Preuzeto sa: http://ssrn.com/abstract=2324902 or http://dx.doi.org/10.2139/ssrn.2324902

Future Internet Architecture (FIArch) Group, coordinated by eight FP7 CSA projects supported by the DG Informatin Society and Media of the European Commission (Jan.2012). *Future Internet Design Principles* Preuzeto sa: http://www.future-internet.eu/uploads/media/FIArch_Design_Principles_V1.0.pdf

Isenberg, D. *Rise of the Stupied Network.* Preuzeto sa http://www.hyperorg.com/misc/stupidnet.html

Mathiason, J., Mueller, M., Klein, H., Holitscher, M. and McKnight, L..(2004) *Internet Governance: The State of Play*, The Internet Governance Project Preuzeto sa: http://www.internetgovernance.org/wordpress/wp-content/uploads/mainreport-final.pdf

Mueller, M. (17. maj 2013). “Are We in Digital Cold War?”GigaNet workshop *The Global Governance of the Internet: Intergovernmentalism, Multistakeholderism and*

Networks. Preuzeto sa: http://www.internetgovernance.org/wordpress/wp-content/uploads/DigitalColdWar31.pdf

Mueller, M., Kuerbis, B. and van Eeten, M. (26. nov. 2008). «Regional Address Registries, Governance and Internet Freedom» Internet Governance Project. Syracuse University. Preuzeto sa: http://www.internetgovernance.org/wordpress/wp-content/uploads/RIRs-IGP-hyderabad.pdf

O'Donnell, S. (2002) „Economic Map of the Internet", TPRC 30th Research Conference on Communication, Information and Internet Policy. Preuzeto sa http://digital.mit.edu/research/papers/162_ODonnell_Map.pdf

Robinson, J. Jr. (21. april 2014). "The Snowden Disconnect: When the Ends Justify the Means" Preuzeto sa: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2427412

Turner, J.S. and Taylor, D.E. "Diversifying the Internet" DOI 10.1109/GLOCOM.2005.1577741

Turow, J., Hennessy, M. and Draper, N.A. (2015) "The tradeoff fallacy, how marketers are misrepresenting American consumers and opening them up to exploitation". A Report from*The Annenberg School for Communicaiton, University of Pennsylvania.* Preuzeto sa https://www.asc.upenn.edu/sites/default/files/TradeoffFallacy_1.pdf

Vinton G. Cerf, *Computer Networking: Global Infrastructure for the 21st Century*. Preuzeto sa: http://homes.cs.washington.edu/~lazowska/cra/networks.html

Novinski članci:

Bernal, P. (2014). „The Right to be Forgotten in the post-Snowden era" *Privacy in Germany*, No 5.

Boadle, A. (22. apr. 2014)."Brazilian Congress passes Internet bill o rights" *Reuters*.

Conrad, P. (16. jun 2002). „Achilles's last stand". *The Guardian*

Davies, R. (25. jun 2011). "What is Dark Internet, How to Access Onion Domains and Configure Hosting for the Dark Web". Preuzeto sa http://www.rogerdavies.com/2011/06/dark-internet/

Doctorow, C. (25. jan. 2011). "We need a serious critique of net activism" *The Guardian*.

Dow Schuell, N. (9. sep. 2013). „The Folly of Technological Solutionism: An Interview with Evgeny Morozov“. *Public Books*.

Driscoll, K. (17. mar. 2013). “The God That Failed: Evgeny Morozov’s ‘To Save Everything, Click Here’”. *Los Angeles Review of Books*.

Ehrenberg, B. (22. apr. 2014). «How much is your personal data worth?» *The Guardian.*

Fitzgerald, D. and Ante, S.E. (16. dec. 2013). “Tech Firms Push to Control Web’s Pipe”. *The Wall Street Journal.*

G. Fenner, M. (Nov./Dec. 2014). «Edward Snowden: Hero or Traitor». *Nebraska Lawyer*, p.19.

Godoy, E. „Cybercrime Treaty Could Be Used to Go After Cyberspionage“. Preuzeto sa http://www.ipsnews.net/2013/10/cybercrime-treaty-could-be-used-to-go-after-cyberespionage/

Gorman, S. (10. mar. 2008). “NSA’s Domestic Spying Grows As Agency Sweeps Up Data”. *The Wall Street Journal*.

Harley, B. (23. mar. 2010). «A Globoal Convention on Cybercrime?“ *Science and Technology Law Review.*

Herzog, W. and Selinger, E. (17. jan. 2013). “Obscurity. A Better Way to Think About Your Data Than ‘Privacy’”. *The Atlantic.*

Koller, D. (26. apr. 2015). “The Future of College: It’s Online”. *The Wall Street Journal.*

Meyer, M. (2014). “Evgeny versus the Internet”. *Columbia Journalism Review* January/February.

Morozov, E. (17. jun 2009). “Iran Electins: A Twitter Revolution?” *Washington Post*.

Morozov, E. (2. okt.2013). „How to Stop a Sharkando“. *Die Zeit*.

Neal, R. W. (24. jan. 2014). “Russian Coders, Ukrainian Cybercriminal, Mexican Smugglers and The Largest Cybercrime in History”. *International Business Times*.

Oakley, B. (29. okt. 2015). “Why Virtual Classes Can Be Better Than Real Ones”. Preuzeto sa: http://nautil.us/issue/29/scaling/why-virtual-classes-can-be-better-than-real-ones

Ridall, R. (13. mar. 2015). “Coursera’s Stiglitz: MOOC revolution is just beginning [SXSWedu2015]” *Education Dive*

Rothkopf, D. (17. jun 2009). “There’s no such thing as a virtual revolution” *Foreign Policy*.

Rowinski, D. (17. dec.2013). „White Spaces & Dark Fiber: Internet Giants Angle For Control of the Internet's Pipes" Preuzeto sa: http://readwrite.com/2013/12/17/internet-backbone-google-amazon-facebook-microsoft

Scott, A. (28. mar. 2014) „Turkey's You Tube and Twitter bans show a government in serious trouble". *The Guardian*.

Tonkin, B. (23 jun 2012). „Tubes: behind the scenes at the Internet, By Andrew Blum" *The Independent*.

Woods, B. (17. sept.2013). «What's the true value of your personal data? Meet the people who want to help you sell it» *TNW News*.

Živković, B. „NJ.V. Internet". *Svet kompjutera* 4/2012.

Živković, B. „Raslojavanje". *Svet kompjutera* 3/2012.

Zuckerman, E. (14. avg. 2014). „The Internet's Original Sin" *The Atlantic*

Zvanični dokumenti:

Charter of Fundamental Rights of the Euroopean Union 2000/C 364/01 http://www.europarl.europa.eu/charter/pdf/text_en.pdf

Convention on Cyber Crime of the Council of Europe (Budapest Convention) http://www.coe.int/en/web/cybercrime/the-budapest-convention

Directive 95/46/EC on the Protection of Individuals with Regard to the Processing of Pesonal Data and on the Free Movement of Such Data. (Data Protection Directive) http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31995L0046&from=en

ECJ Court Decision C-131/12, *Google Spain SL, Google Inc. v Agencia Espanola de Protecion de Datos (AEPD), Mario Costeja Gonzalez*.

European Commission's Decision 2000/518/EC (Safe Harbor Treaty)

RFC 0527 "ARPAWOCKY" http://tools.ietf.org/html/rfc527

RFC 0675 „Specification of internet transmission control program" http://tools.ietf.org/html/rfc675

RFC 0748 "TELNET randomly-lose Option" http://www.rfc-archive.org/getrfc.php?rfc=748

RFC 0761 "Transmission Control Protocol" http://tools.ietf.org/html/rfc761

RFC 0871 "A Perspective on the ARPANET referene model" http://tools.ietf.org/html/rfc871

RFC 0882 “Domain Names – Concepts and Facilities” http://tools.ietf.org/html/rfc882
RFC 1122 „Requirements for Internet Hosts – Communication Layers“ http://tools.ietf.org/html/rfc1122
RFC 1149 “A Standard for the Transmission of IP Datagrams on Avian Carriers” https://tools.ietf.org/html/rfc1149
RFC 1925 “Twelve Networking Truths” http://tools.ietf.org/html/rfc1925
RFC 1958 “Architectural Principles of the Internet” https://www.ietf.org/rfc/rfc1958.txt
RFC 2026 “The Internet Standard Process – Revision 3” https://www.ietf.org/rfc/rfc2026.txt
RFC 2324 “Hyper Text Coffee Pot Control Protocol (HTCPCP/1.0)” http://tools.ietf.org/html/rfc2324
RFC 2795 “The Infinite Monkey Protocol Suite (IMPS)” http://tools.ietf.org/html/rfc2795
RFC 3426 “General Architectural and Policy Considerations” https://www.rfc-editor.org/rfc/pdfrfc/rfc3426.txt.pdf
RFC 3439 „Some Internet Architectural Guidance and Philosophy“ http://www.ietf.org/rfc/rfc3439.txt .
RFC 4271 „Border gateway protool-4 (BGP-4)“. http://tools.ietf.org/html/rfc4271
RFC 5841 “TCP Option to Denote Packet Mood” http://www.ietf.org/rfc/rfc5841.txt
RFC 7169 “The NSA (No Secrecy Afforded) Certificate Extension” https://tools.ietf.org/html/rfc7169
RFC 7511 “Scenic Routing for IPv6” https://tools.ietf.org/html/rfc7511
World Economic Forum & A.T.Kearney. (Maj 2014). *Rethinking Personal Data: A New Lens for Strengthening Trust*. http://reports.weforum.org/rethinking-personal-data/
Zakon o javnom informisanju i medijima Republike Srbije („Sl. glasnik RS“, br. 83/2014 i 58/2015)

Onlajn video izvori:

Malte Spitz. (Jun 2012). *Your phone company is watching* Dostupno na http://www.ted.com/talks/malte_spitz_your_phone_company_is_watching

Weisberg, J. and Wu, T. (11. nov.2010). Discusija o knjizi *The Master Switch* za New America Foundation. Dostupno na https://www.youtube.com/watch?v=7uxJwBu-gK0 (pristupljeno 29.02.2016.)

Wu, T. Intervju za program *The Agenda* sa Steve Paikin-om. Dostupno na http://www.youtube.com/watch?v=M-ZXNaXvSUE (pristupljeno 29.02.2016.)

Internet stranice sa relevantnim informacijama:

http://ec.europa.eu/justice/data-protection/

http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm

http://en.wikipedia.org/wiki/Request_for_Comments

http://foucault.info/doc/documents/disciplineandpunish/foucault-disciplineandpunish-panopticism-html

http://reformcorporatesurveillance.com/index.html

http://visual.ly/domain-name-industry-brief-q42013

http://visual.ly/domain-name-industry-brief-q42013

http://www.businessmodelgeneration.com/canvas/bmc

http://www.caida.org/research/topology/as_core_network/2015/

http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_9-1/autonomous_system_numbers.html

http://www.cs.ccsu.edu/~stan/classes/CS490/Slides/Networks5-Ch1-1.pdf

http://www.geni.net/?page_id=2

http://www.iana.org/domains/root/servers

http://www.ietf.org/

http://www.internetlivestats.com/internet-users/#trend

http://www.internetsociety.org/

http://www.internetworldstats.com/stats.htm

http://www.investopedia.com/terms/b/business-plan.asp

http://www.livinginternet.com/i/ii_arpanet_gateways.htm

http://www.thedomains.com/2013/08/27/icann-approves-200-million-dollar-budget-for-2014-306-employees-still-no-revenue-from-new-gtld-auctions/

http://www.verisign.com/en_US/innovation/dnib/index.xhtml?loc=en_US&dmn=dnib

http://www.yalelawtech.org/anonymity-online-identity/we-are-anonymous-we-are-legion/

http://www.youtube.com/watch?v=M-ZXNaXvSUE

https://en.wikipedia.org/wiki/April_Fools'_Day_Request_for_Comments

https://opennet.net/

https://www.coursera.org/about/

https://www.edx.org/about-us

https://www.google.com/transparencyreport/removals/europeprivacy/?hl=en

https://www.iab.org/

https://www.icann.org/

https://www.icann.org/resources/pages/guidelines-2012-05-15-en

https://www.icann.org/resources/pages/policy-2012-02-25-en

https://www.icann.org/resources/pages/providers-6d-2012-02-25-en

https://www.reformgovernmentsurveillance.com/

https://www.rfc-editor.org/current_queue.php

https://www.rfc-editor.org/status_changes.php

https://www.techopedia.com/definition/20115/internet-backbone

https://www.telegeography.com/telecom-resources/internet-exchange-map/index.html

https://www.ucl.ac.uk/Bentham-Project/who/panopticon

https://www.youtube.com/watch?v=7uxJwBu-gK0

www.cambridge-code.org/googlespain.html

www.pinboard.in

www.reformcorporatesurveillance.org

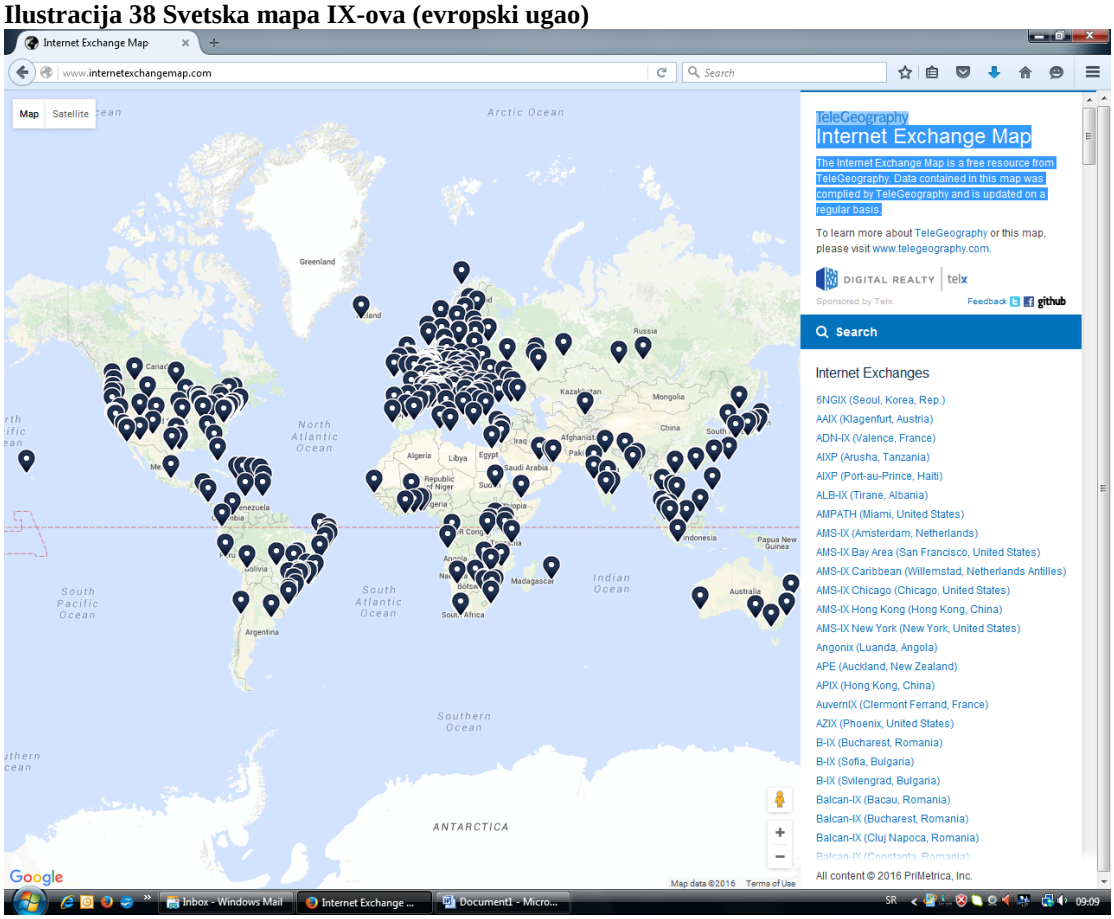
PRILOZI

Prilog 1

Ukupan popis[418] svih trenutno aktivnih tačaka internet razmene na svetu (februar 2016. godine), prema internet stranici Telegeography sadrži preko 300 IX-ova, koji su smešteni u preko 500 fizičkih zgrada. Ovaj broj je važan jer govori o značaju ovih tačaka za širenje interneta, a može se uporediti sa brojem država u svetu, koji je nešto preko 200 (gledano po broju članica Ujedinjenih nacija).

Ovde donosimo svetsku mapu IX-ova.

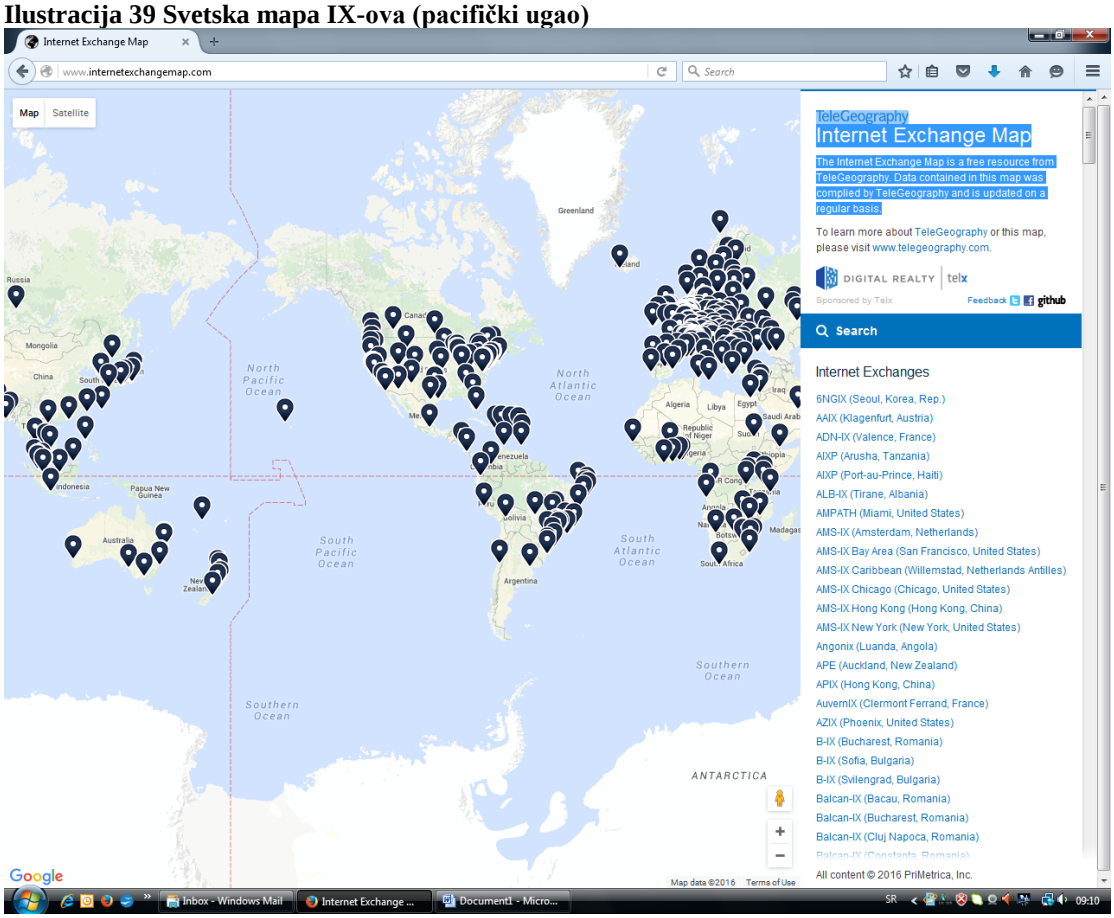
Ilustracija 38 Svetska mapa IX-ova (evropski ugao)



Preuzeto sa www.telegeography.com

[418] Internet Exchange mapa je besplatan javno dostupan resurs, koji je sastavila kompanija TeleGeography. https://www.telegeography.com/telecom-resources/internet-exchange-map/index.html

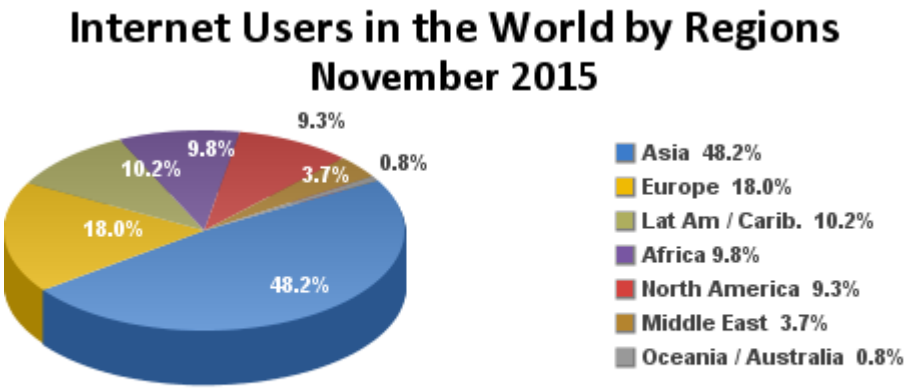
Ilustracija 39 Svetska mapa IX-ova (pacifički ugao)



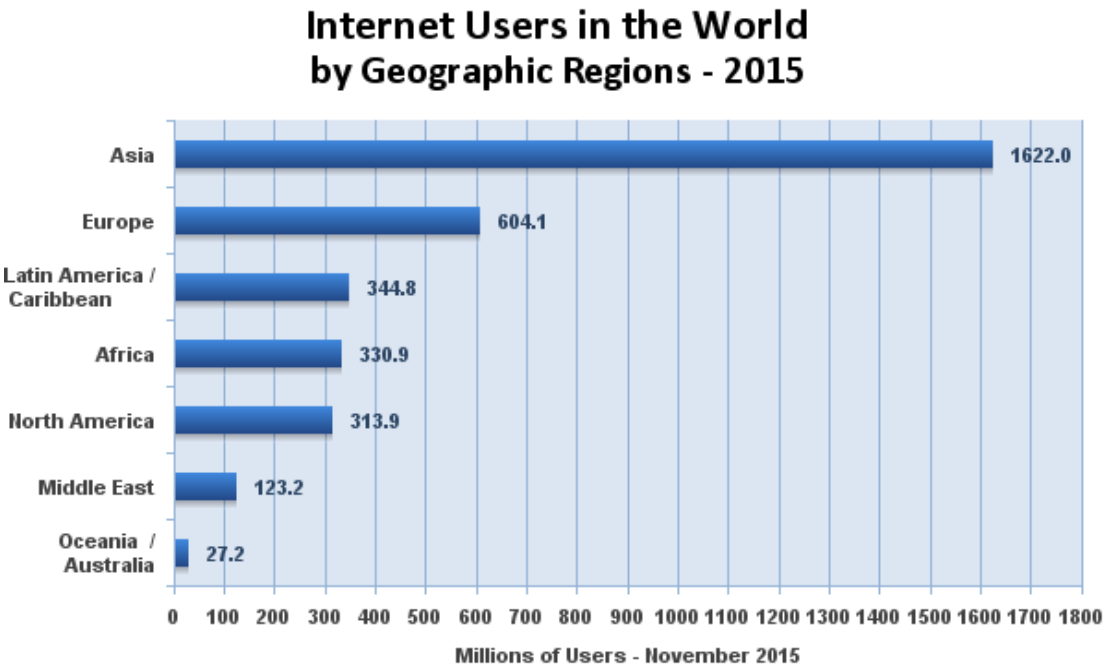
Preuzeto sa www.telegeography.com

Prilog 2

Ovde donosimo grafički prikaz statistike korisnika interneta po geografskim regionima i po državama, koji je preuzet sa internet stranice Internet World Stats.

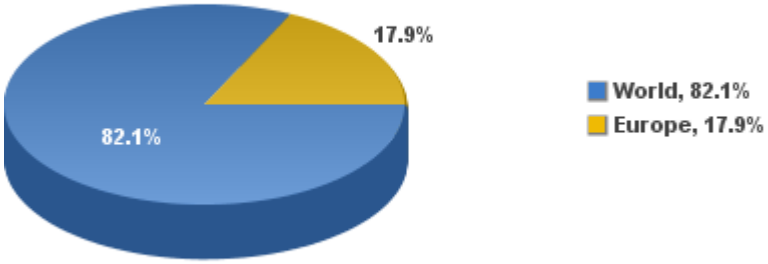


Source: Internet World Stats - www.internetworldstats.com/stats.htm
Basis: 3,366,261,156 Internet users on November 30, 2015
Copyright © 2015, Miniwatts Marketing Group



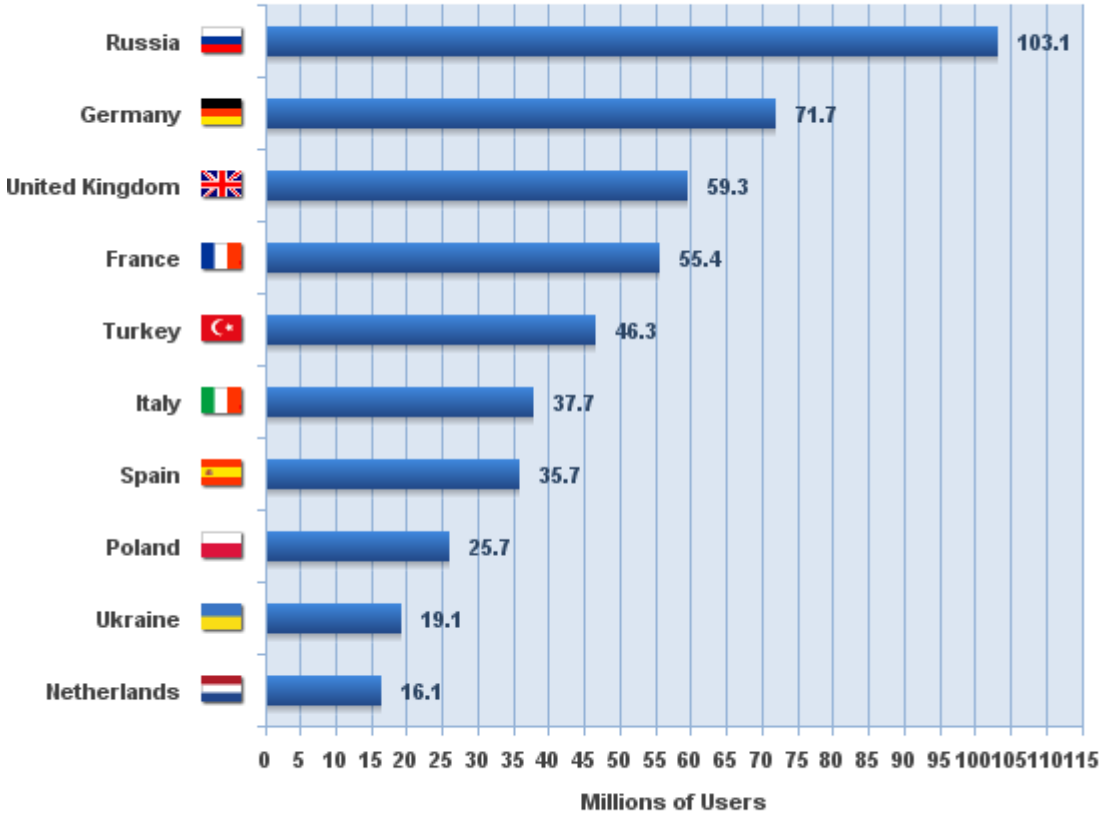
Source: Internet World Stats - www.internetworldstats.com/stats.htm
3,366,261,156 Internet users estimated for November 30, 2015
Copyright © 2016, Miniwatts Marketing Group

Internet Users in Europe
November 2015

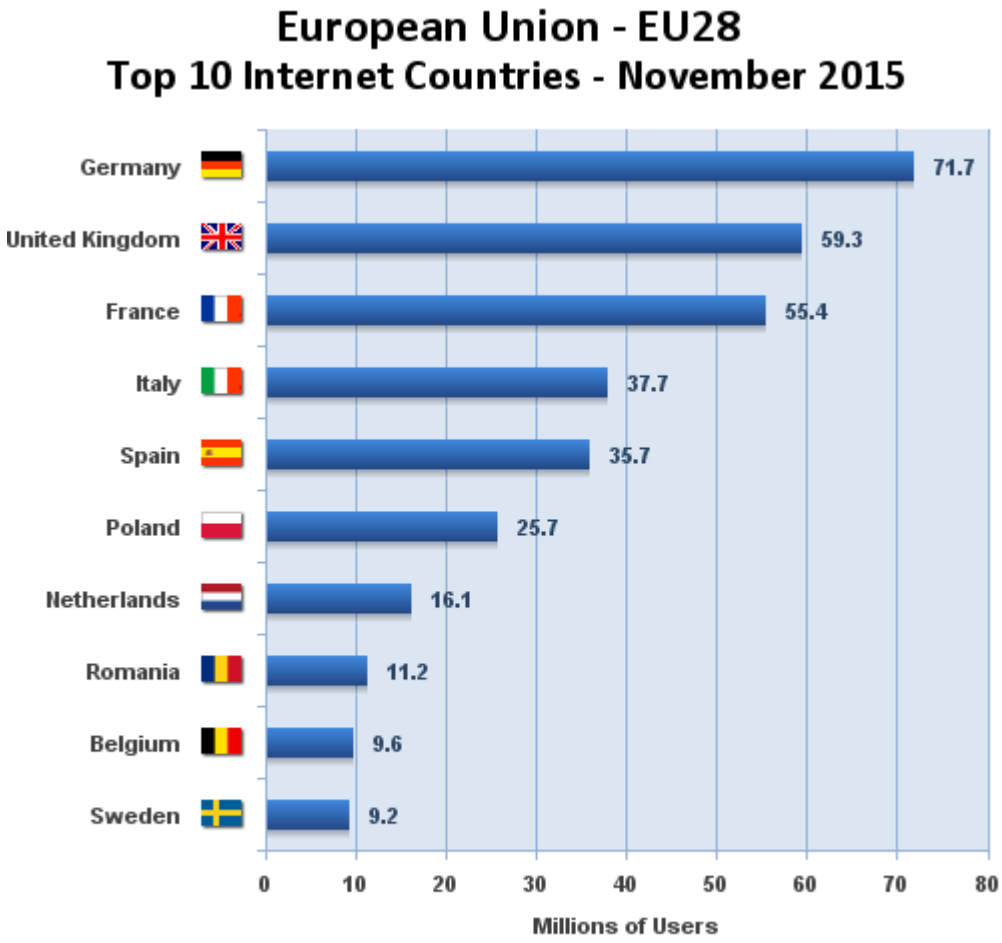


Source: Internet World Stats - www.internetworldstats.com
Based on 3,366,261,156 estimated world Internet users for Nov. 2015

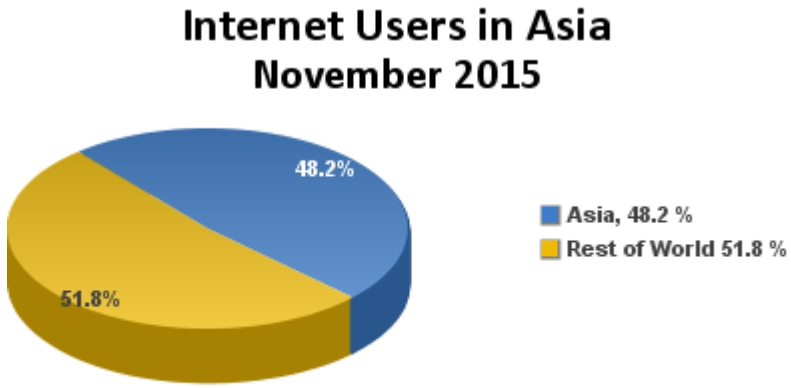
Internet Top 10 Countries in Europe
November 30, 2015



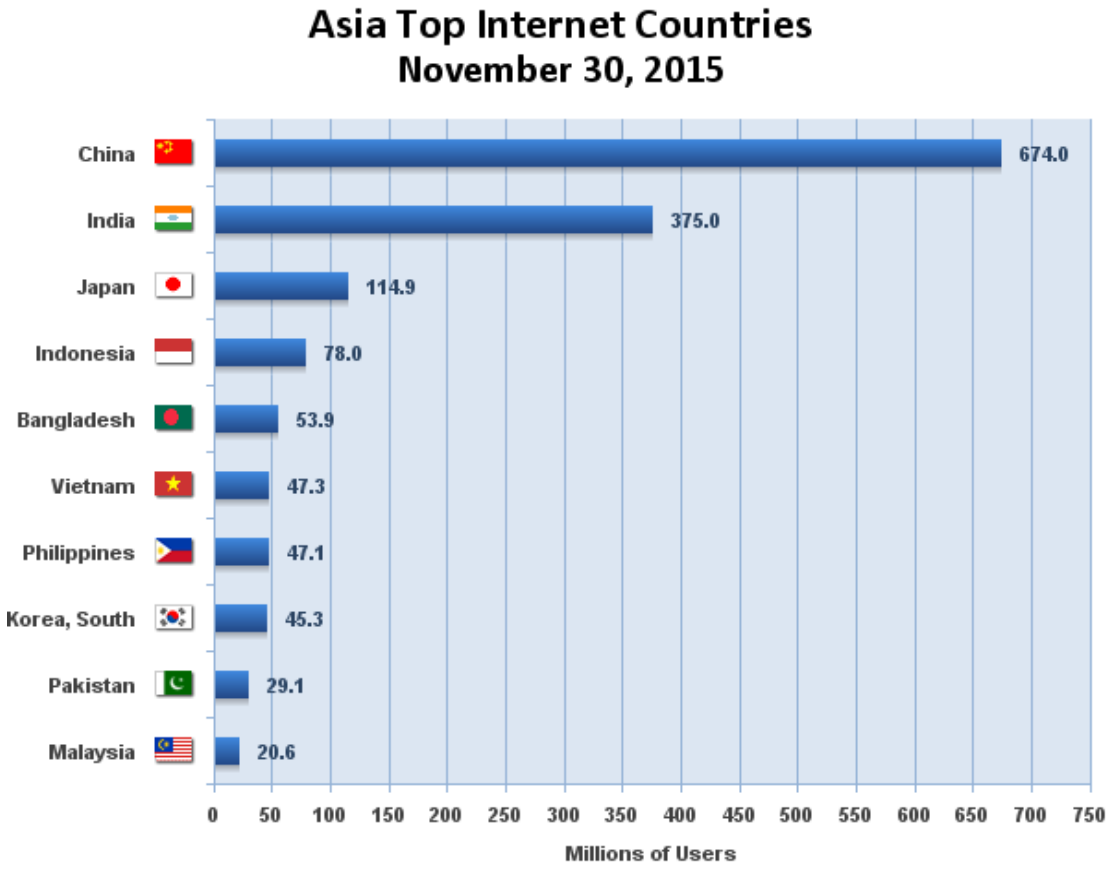
Source: Internet World Stats - www.internetworldstats.com/stats4.htm
Basis: 604,147,280 estimated Internet Users in Europe on Nov 2015



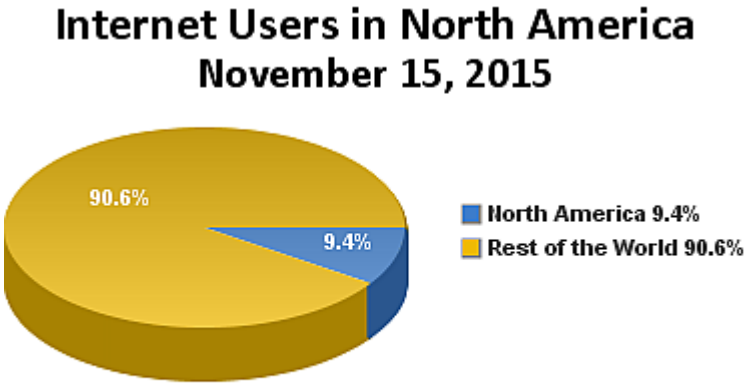
Source: Internet World Stats - www.internetworldstats.com/stats9.htm
402,937,674 estimated EU Internet users for November 2015



Source: www.internetworldstats.com/stats3.htm
1,622,084,293 Internet users in Asia estimated on Nov 30, 2015



Source: Internet World Stats - www.internetworldstats.com/stats3.htm
3,366,260,056 Internet users in the World estimated for Nov 30, 2015
Copyright © 2015, Miniwatts Marketing Group



Source: Internet World Stats - www.internetworldstats.com
313,867,363 Internet Users in North America as of 2015Q3
Copyright © 2015, Miniwatts Marketing Group

Biografija autorke

Ivana Ivković je rođena 1973. godine u Nišu, gde je završila osnovnu i srednju školu kao dobitnica Vukove diplome.

Na Filozofskom fakultetu u Beogradu filozofiju je diplomirala 1999. godine, sa prosečnim uspehom na studijama 9,33 i diplomskim radom o teorijji pravde Džona Rolsa, i magistrirala 2005. godine, sa prosečnim uspehom na studijama 10,00 i magistraskim radom *Poštovanje i / ili postvarivanje ličnosti u seksualnim praksama. Osnovi seksualne etike*. U periodu 2000-2003. radila je kao asistentkinja-pripravnica na Filozofskom fakultetu u Nišu, a u periodu 2007-2009. bila je angažovana od izdavačke kuće Službeni glasnik kao prevodilac filozofske literature (primenjene etike) sa engleskog na srpski jezik.

Takođe je na Fakultetu političkih nauka u Beogradu diplomirala 2001. godine, sa prosečnim uspehom na studijama 9,13 te time stekla zvanje diplomirane politikološkinje za međunarodne odnose. Radila je u više međunardonih organizacija i projekata u Beogradu, kao i u diplomatiji Republike Srbije (rang savetnik u Ambasadi Republike Srbije u Zagrebu u periodu 2010-2013.). Trenutno je zaposlena u Ministarstvu trgovine, turizma i telekomunikacija Republike Srbije, gde se bavi bilateralnom eknomskom saradnjom između Srbije i evropskih zemalja. Govori engleski, nemački i francuski jezik.

Изјава о ауторству

Потписана Ивана Ивковић
број уписа ДС/СС 05/4-02

Изјављујем

да је докторска дисертација под насловом

Моралне вредности у дизајну архитектуре интернета

- резултат сопственог истраживачког рада,
- да предложена дисертација у целини ни у деловима није била предложена за добијање било које дипломе према студијским програмима других високошколских установа,
- да су резултати коректно наведени и
- да нисам кршио/ла ауторска права и користио интелектуалну својину других лица.

Потпис докторанда

У Београду, 21.03.2016.

Изјава о истоветности штампане и електронске верзије докторског рада

Име и презиме аутора
Ивана Ивковић
Број уписа
ДС/СС 05/4-02
Студијски програм
Филозофија
Наслов рада
Моралне вредности у дизајну архитектуре интернета
Ментор
Проф. Др Јован Бабић, редовни професор,
Филозофски факултет, Универзитет у Београду

Потписана
Ивана Ивковић

изјављујем да је штампана верзија мог докторског рада истоветна електронској верзији коју сам предао/ла за објављивање на порталу **Дигиталног репозиторијума Универзитета у Београду.**
Дозвољавам да се објаве моји лични подаци везани за добијање академског звања доктора наука, као што су име и презиме, година и место рођења и датум одбране рада.
Ови лични подаци могу се објавити на мрежним страницама дигиталне библиотеке, у електронском каталогу и у публикацијама Универзитета у Београду.

Потпис докторанда

У Београду, 21.03.2016.

Изјава о коришћењу

Овлашћујем Универзитетску библиотеку „Светозар Марковић“ да у Дигитални репозиторијум Универзитета у Београду унесе моју докторску дисертацију под насловом:

Моралне вредности у дизајну архитектуре интернета

која је моје ауторско дело.
Дисертацију са свим прилозима предала сам у електронском формату погодном за трајно архивирање.
Моју докторску дисертацију похрањену у Дигитални репозиторијум Универзитета у Београду могу да користе сви који поштују одредбе садржане у одабраном типу лиценце Креативне заједнице (Creative Commons) за коју сам се одлучила.

1. Ауторство
2. Ауторство - некомерцијално
3. Ауторство – некомерцијално – без прераде
4. Ауторство – некомерцијално – делити под истим условима
5. Ауторство – без прераде
6. Ауторство – делити под истим условима

(Молимо да заокружите само једну од шест понуђених лиценци, кратак опис лиценци дат је на полеђини листа).

Потпис докторанда

У Београду, 21.03.2016.

Ivana Ivković