UNIVERZA V LJUBLJANI

FAKULTETA ZA DRUŽBENE VEDE

Matej Ramuta

Vpliv sodobnih konfliktov na razvoj interneta

Diplomsko delo

Ljubljana, 2014

UNIVERZA V LJUBLJANI

FAKULTETA ZA DRUŽBENE VEDE

Matej Ramuta

Mentor: izr. prof. dr. Vladimir Prebilič

Somentor: doc. dr. Uroš Svete

Vpliv sodobnih konfliktov na razvoj interneta

Diplomsko delo

Ljubljana, 2014

Vpliv sodobnih konfliktov na razvoj interneta

Internet se je začel kot projekt ameriškega ministrstva za obrambo (DoD), ki je financiralo razvoj omrežja ARPANET. Cilj DoD je bil razviti omrežje, ki bi povezovalo glavne vojaške centre in bi vzdržalo tudi jedrski napad. ARPANET so v glavnem posvojili znanstveniki, kasneje pa se je z združitvijo ostalih omrežij komercializiral in postal sodobni internet. S širitvijo interneta se širi tudi polje svobode in možnost komuniciranja ter širjenja idej med ljudmi. Mnoge države poskušajo internet nadzorovati, nekatere ga tudi cenzurirajo, saj se prek interneta disidentske skupine organizirajo proti oblasti in pridobivajo nove somišljenike. Obstajajo različni načini cenzuriranja interneta, od najbolj preprostega manipuliranja DNS imenikov, do bolj zahtevnega, kot je globoko pregledovanje in filtriranje paketkov v internetnem omrežju. Vsem načinom cenzure pa nasproti stojijo načini izogibanja cenzuri, ki predvsem temeljijo na enkripciji podatkov ter P2P protokolih. Voditelji nekaterih držav že glasno razmišljajo o uvedbi nacionalnega interneta/intraneta, kjer bi lažje nadzorovali in omejevali aktivnosti državljanov. Vendar pa je odcepitev od globalnega interneta malo verjetna, predvsem zaradi medsebojne prepletenosti svetovnega gospodarstva.

Ključne besede: internet, sodobni konflikti, varnostna dilema, cenzura, P2P.

The influence of modern conflicts on the future development of the internet

Internet started out as the ARPANET network that was financed by the U.S. Department of Defense (DoD). Their goal was to develop a network that would connect DoD's three main military centers and would survive a nuclear attack. ARPANET was mostly used for scientific research and later, through merging with other computer networks, commercialized and evolved into the modern internet. The fields of freedom, communication and sharing ideas spread with the internet. Many countries try to control it and some also censor it because internet helps dissident groups to organize and gather new members. There are many ways how to censor the internet, from the most simple, like DNS poisoning to more advanced like deep packet inspection. But every mean of censorship faces some means of avoiding it with technologies that use encryption and peer-to-peer (P2P) networking. Some world leaders are seriously considering building their own national internets/intranets that would be physically separated from the global internet and would help them easily control and censor their citizens. But these plans are highly unlikely to materialize due to the fact that global economies are highly intertwined.

Keywords: internet, modern conflicts, security dilemma, censorship, P2P.

Kazalo

1 Uvod ... 6

2 Metodološki okvir ... 7
2.1 Cilji in namen ... 7
2.2 Hipoteze ... 7
2.3 Metodologija ... 7
2.4 Zgradba diplomskega dela ... 7
2.5 Temeljni pojmi ... 8
2.5.1 Konflikt ... 8
2.5.2 Varnostna dilema ... 9
2.5.3 Internet ... 9

3 Zgodovina interneta ... 10
3.1 Hladna vojna ... 10
3.2 ARPANET ... 10
3.3 Združitev omrežij in nastanek sodobnega interneta ... 11
3.4 Domenski sistem ... 13
3.5 Svetovni splet ... 13
3.6 Iskra Delta ... 14

4 Študije držav in konfliktov, kjer je internet igral eno ključnih vlog ... 16
4.1 Egipt ter revolucija v 2011 ... 16
4.2 Turčija in protesti v Gezi parku ... 17
4.3 Rusija ... 18
4.4 Iran ... 19
4.5 Kitajski veliki požarni zid ... 21
4.6 NSA škandal ... 22
4.7 Seznam načinov blokiranja neželenih vsebin in aktivnosti na internetu ... 23

5 Prihodnji razvoj interneta 25
5.1 ICANN 25
5.2 Možni scenariji prihodnjega razvoja interneta 25
5.2.1 (Inter)nacionalni interneti 25
5.2.2 Trenutni internet z močnejšo mednarodno komponento 26
5.2.3 Popolnoma decentraliziran internet 26

6 Sklep in verifikacija hipotez 30

7 Literatura 31

1 Uvod

Internet je v zadnjih dvajset letih močno povezal in prepletel gospodarstva držav, pa tudi njihove kulture in običaje, ter omogočil številnim ljudem hitrejši in obsežnejši dostop do znanja in informacij. Prinesel pa je tudi nove izzive na področju varnosti, tako osebne (pravica do zasebnosti), kot tudi državne in meddržavne varnosti.

Ker se je internet, z vsemi svojimi aplikacijami, predvsem elektronsko pošto in svetovnim spletom, tako zelo zasidral v življenja ljudi in delovanja držav (vsaj t.i. prvega in drugega sveta), je pomembno, da njegove varnostne in tehnološke vidike proučuje tudi obramboslovje, ki je seveda interdisciplinarno.

Sam razvoj interneta se je začel na pobudo ameriškega ministrstva za obrambo, dandanes pa se, kot lahko vidimo v medijih, uporablja tudi za potrebe boja za oblast, organiziranja množičnih protestov, nadzorovanja lastnih državljanov ter industrijskega, političnega ali vojaškega vohunjenja. Glavni gradnik interneta, protokol TCP/IP, nekatere vojske že preizkušajo in uporabljajo na bojišču, s čimer ustvarijo lastno omrežje za komunikacijo in poveljevanje, ki pa ni povezano v internet (Bratuša 2006, 6−7), zato se v diplomski nalogi tega področja ne bom dotaknil. Namesto tega bom proučil sodobne konflikte in varnostne dileme ter njihov vpliv na bodoči razvoj interneta.

Smer, v katero se bo razvijal internet oziroma kako bodo svoja nacionalna računalniška omrežja razvijale posamezne države, je zelo pomembna tako za njihovo gospodarstvo, nacionalno varnost ter tudi meddržavno varnost. V diplomski nalogi bom zato ugotavljal, kateri so možni scenariji razvoja interneta v luči omenjenih sodobnih konfliktov.

2 Metodološki okvir

2.1 Cilji in namen

Do sedaj, v kratki zgodovini obstoječega interneta, smo bili vsi vajeni enega sistema, torej enega interneta. Namen te diplomske naloge je ugotoviti, kako na bodoči razvoj interneta vplivajo sodobni konflikti in varnostne dileme, ter na kakšen način bi se lahko internet razvijal naprej.

Cilj diplomske naloge je predstaviti začetni razvoj interneta, njegov prehod iz vojaške v civilno sfero, proučiti sodobne konflikte in varnostne dileme, ki so se ob tem pojavili ter njegov trenutni in prihodnji razvoj v luči teh konfliktov.

2.2 Hipoteze

- Zaradi sodobnih konfliktov in varnostnih dilem, želijo nekatere države povečati svoj nadzor nad internetom.
- Zaradi ameriškega nadzora nad domenskim sistemom, nekatere države razmišljajo o vzpostavitvi lastnih internetov.

2.3 Metodologija

V diplomskem delu bom uporabil:

- analizo primarnih in sekundarnih virov,
- historično metodo, s katero bom opisal zgodovinski razvoj interneta,
- študije primerov konfliktov, kjer je internet igral eno izmed ključnih vlog ter
- metode deskripcije, sintetizacije in kvalitativne analize, predvsem pri ugotavljanju smeri prihodnjega razvoja interneta oziroma internetov.

2.4 Zgradba diplomskega dela

V prvem delu diplomskega dela bom opisal zgodovinski razvoj interneta ter njegovih protokolov. V drugem delu bom analiziral nekaj izbranih konfliktov in varnostnih dilem, kjer je internet igral eno ključnih vlog. V zadnjem delu pa bom poskušal ugotoviti možne nadaljnje smeri razvoja interneta, ki se kažejo predvsem zaradi omenjenih konfliktov.

2.5 Temeljni pojmi

2.5.1 Konflikt

Uporabil bom definicijo konflikta Heidelberškega inštituta (HIIK), ki pravi, da je konflikt "pozicijska razlika med vsaj dvema odločnima in direktno vpletenima stranema glede vrednot, ki so relevantne za družbo. Te strani uporabljajo vidne in povezane ukrepe izven obstoječih, formalnih postopkov ter ogrožajo temeljne funkcije države, mednarodni red ali pa imajo možnosti za to." (HIIK 2014).

HIIK deli konflikte glede na intenzivnost na način, kot je prikazan v tabeli 2.1.

Tabela 2.1: Stopnje intenzivnosti konflikta po metodologiji Heidelberškega inštituta.

Stopnja intenzivnosti	**Termin**	**Opis**
1	Spor (ang. dispute)	Pozicijska razlika glede vrednot nacionalnega pomena, kjer ena stran izrazi svoje zahteve in jih druga tudi tako dojame.
2	Nenasilne krize (ang. non-violent crises)	Nenasilni ukrepi, ki pa so tik pred uporabo nasilja. Primeri: verbalni pritisk, grožnja z uporabo sile, uvedba ekonomskih sankcij.
3	Nasilne krize (ang. violent crises)	Nasilna kriza je napeta situacija, kjer vsaj ena od strani uporabi nasilne metode v posamičnih incidentih.
4	Omejena vojna (ang. limited war)	Konflikt postane omejena vojna takrat, ko je sila uporabljena večkrat zapored na organiziran način.
5	Vojna (ang. war)	V vojni je nasilje kontinuirano uporabljeno na organiziran in sistematičen način. Strani v konfliktu izvajajo obsežne ukrepe, odvisnih od situacije. Obseg uničenja je ogromen in dolgotrajen.

Vir: HIIK (2014).

2.5.2 Varnostna dilema

Termin "varnostna dilema" je prvi uporabil John H. Herz leta 1950 (Roe 1999, 183), s čimer je obrazložil, da zagotavljanje varnosti (na ravni posameznika, oblasti, države ali skupine držav) v smislu povečevanja vojaške moči ali drugih varnostnih naporov, lahko povzroči občutek večje ogroženosti druge strani ter jo vodi v ukrepe za povečevanje njene varnosti. Tovrstni ukrepi na obeh straneh lahko eskalirajo v konflikt večjih razsežnosti (na primer vojno).

V kontekst varnostne dileme lahko uvrstimo tudi nedavno razkriti ameriški program prisluškovanja domačim in tujim državljanom, ki je bil namenjen boju proti terorizmu, vendar pa je kršil pravico ljudi do zasebnosti in po razkritju spodbudil pomemben del računalniško izobraženih ljudi k uporabi in razvoju računalniških orodij, ki močno omejujejo sposobnost obveščevalnih agencij pri nadziranju predvsem internetnega prometa.

2.5.3 Internet

Internet je globalno omrežje računalniških omrežij, ki temeljijo na uporabi istega protokola, TCP/IP. Razvoj računalniških omrežij se je začel po drugi svetovni vojni, vodilno vlogo pa je imela vojaška raziskovalna agencija DARPA, ki je razvijala svoje omrežje ARPANET.

Sodobni internet je nastal z združitvijo več svetovnih računalniških omrežij v 80. letih 20. stoletja. Z razmahom dveh njegovih največjih aplikacij, elektronske pošte in svetovnega spleta, pa je v svetu povzročil telekomunikacijsko in informacijsko revolucijo, ki traja še danes.

3 Zgodovina interneta

3.1 Hladna vojna

Konec 40. let prejšnjega stoletja, je imel svet dve velesili z jedrskim orožjem: Združene države Amerike in Sovjetsko zvezo. Kmalu se je začelo pojavljati vprašanje totalne, jedrske vojne ob tem pa tudi strah pred zmotnim začetkom take vojne, ko bi ena od strani, zaradi izpada ali napake v lastnem komunikacijskem sistemu, domnevala, da je ta izpad povzročila druga stran z jedrskim napadom in bi zato "odgovorila" na neobstoječi napad s svojim protinapadom z jedrskim orožjem (Living Internet 1996a).

Kljub zaostanku v znanstvenih raziskavah takoj po drugi svetovni vojni (predvsem na področjih novih oborožitvenih sistemov, raket in vesolja) je Sovjetska zveza kmalu ujela, ter z uspešno opravljeno misijo Sputnik tudi prehitela ZDA. Takratni predsednik Eisenhower je zato leta 1958 ukazal ustanovitev Agencije za napredne obrambne analize (DARPA - Defense Advanced Research Projects Agency), katere naloga je bila "preprečiti tehnološka presenečenja, kot je bila izstrelitev Sputnika, ki so signalizirala prednost Sovjetske zveze pri osvajanju vesolja" (DARPA 2005, 1).

Oktobra 1962 je DARPA v svoji strukturi ustanovila Službo za tehnike procesiranja informacij (Information Processing Techniques - IPTO) ter na čelo te službe postavila Josepha Lickliderja (Living Internet 1996a). Licklider je bil v znanstveni sferi prepoznaven s svojimi deli, v katerih je opisoval uporabo digitalnih knjižnic, oddaljenega dostopa do računalnikov ter omrežja računalnikov. Naloga, ki mu jo je zaupala DARPA, je bila ustvariti komunikacijsko omrežje med glavnimi računalniki ameriškega Ministrstva za obrambo v Pentagonu, Cheyenne Mountain bunkerjem ter poveljstvom Strateških zračnih sil (Strategic Air Command - SAC), ki bi bilo zelo robustno in vzdržalo tudi morebitni jedrski napad (Living Internet 1996b). Kljub temu, da je Licklider že po dveh letih zapustil IPTO, je njegovo delo nadaljeval njegov naslednik, Robert Taylor, ki je rekrutiral Lawrencea Robertsa z MIT za vodenje projekta izgradnje omrežja ARPANET (Abbate 2000, 44).

3.2 ARPANET

DARPA sama ni nikoli imela lastnih razvojnih laboratorijev, temveč je vedno najemala zunanje inštitucije (tako javne kot zasebne) ter financirala njihove projekte (prav tako, 36). Podoben problem povezljivosti računalnikov, kot ga je imelo Ministrstvo za obrambo na svojih ključnih lokacijah, je imela tudi DARPA sama s temi zunanjimi laboratoriji. Zato ne

čudi, da je bil ARPANET zasnovan kot omrežje, ki bo povezalo ameriške raziskovalne inštitucije z vzhodne (MIT, Harvard, BBN) in zahodne (Stanford, Berkeley, UCLA, RAND) obale, ki so delali na DARPA projektih (prav tako, 45).

Ključna za vzpostavitev ARPANET-a je bila metoda paketnega prenosa (ang. packet switching). To pomeni, da se sporočila, ki jih pošiljamo preko omrežja, razdeli na manjše enote (paketke) s fiksno določeno velikostjo 1024 bitov. Zelo kratko sporočilo bi bilo lahko poslano v enem paketku, daljša pa v večih. Vsakemu paketku se določi IP naslov tako prejemnika kot pošiljatelja ter še nekaj drugih podatkov (npr. število vseh paketkov, ki sestavljajo sporočilo, njihov vrstni red itd.). Paketke usmerjevalnik (ang. router) pošlje k naslovniku, vendar ne nujno vse po isti poti v omrežju. Pri prejemniku se paketki zopet sestavijo nazaj v sporočilo. V kolikor se na poti kakšen paketek "izgubi", lahko računalnik prejemnika zahteva od pošiljatelja ponovni prenos (Living Internet 1996c; Abbate 2000, 17−18).

Za metodo paketnega prenosa so zaslužni trije ljudje, ki so idejo razvijali vzporedno in, vsaj na začetku, neodvisno drug od drugega. To so bili Američan Paul Baran (Rand Corporation), Britanec Donald Davies (National Physical Laboratory - NPL) in Američan Leonard Kleinrock (MIT) (Abbate 2000, 36; Kleinrock 2010). Metodo sta tako kot temeljni način prenosa podatkov vzporedno uporabila tako ARPANET, kot tudi računalniško omrežje, ki so ga razvijali v britanskem NPL.

Za prva štiri stičišča omrežja ARPANET so bili določeni Stanford Research Institute, UC Santa Barbara, UC Los Angeles in Univerza v Utahu (Abbate 2000, 56), ki so jih povezali v omrežje v letu 1969. Kmalu so sledile prve aplikacije, najprej oddaljeni dostop in pošiljanje datotek, kasneje v letu 1972 pa še ena najpomembnejših: elektronska pošta (prav tako, 68−69).

3.3 Združitev omrežij in nastanek sodobnega interneta

Omrežju ARPANET je hitro sledilo še več drugi omrežij. Nekatere je financirala in vzpostavila DARPA sama, ko je preizkušala paketni prenos prek radijskih valov (ALOHAnet in kasneje PRNET) ter satelitske povezave (SATNET). ALOHAnet je v omrežje povezal računalnike na Havajih, SATNET pa je na začetku povezal dve ameriški stičišči (ang. node) v Marylandu in Zahodni Virginiji z dvema evropskima - enim v Londonu in drugim na Norveškem (prav tako, 120−121).

Nastajati pa so začela tudi zasebna, komercialna računalniška omrežja. Prvo tako je naredilo ravno podjetje, ki je bilo pogodbenik agencije DARPA in je močno sodelovalo pri razvoju ARPANET-a - podjetje Bolt, Beranek and Newman (BBN). BBN je celo rekrutiral dotedanjega direktorja agencije DARPA, Larryja Robertsa, da vodi ta projekt, imenovan Telenet. Telenet je svoje računalniško omrežje nudilo predvsem zasebnemu sektorju (Mathison in drugi 2012).

Seveda pa razvoj računalniških omrežij ni bil omejen le na ZDA. V Evropi sta svoji omrežji razvijali tako Velika Britanija (PLN pod vodstvom njihovega pionirja na področju paketnega prenosa, Donalda Daviesa), kot tudi Francija (Cyclades) (Abbate 2000, 123).

Ob vznikanju vseh teh računalniških omrežij pa se je pojavil nov problem: njihova medsebojna povezljivost. Zaradi tehnološke nekompatibilnosti tako znanstvenik iz enega omrežja ni mogel direktno komunicirati z znanstvenikom, ki je imel računalnik v drugem, nekompatibilnem omrežju. Tega problema sta se hitro zavedla Bob Kahn (DARPA) in Vinton Cerf (Stanford), zato sta razvila protokol, ki je postal standard in omogočal povezljivost in zanesljiv paketni prenos v in med različnimi omrežji - TCP (Transmission Control Protocol) (prav tako, 123−127).

Zaradi uspešnega razvoja projekta ARPANET, se je zanj začela bolj zanimati tudi vojaška sfera, za potrebe katere je bil v prvi vrsti tudi začet. V letu 1975 je nadzor nad ARPANET projektom prevzela agencija Ministrstva za obrambo DCA (Defense Communications Agency) z namenom uporabiti omrežje za potrebe oboroženih sil. Kmalu pa so ugotovili, da je ARPANET dokaj ranljiv za morebitne "hekerske" napade, saj znanstveniki, ki so do tedaj v največji meri predstavljali uporabnike omrežja, v svoji dobri veri niso strogo nadzirali, kdo uporablja omrežje ter so omogočali skorajda prost prenos datotek in dokumentov z računalnikov v omrežju. DCA se je zato odločila ARPANET razdeliti na dva dela. Prvi del je še zmeraj ostal pod istim imenom in bil predan nazaj agenciji DARPA ter tako bil še naprej na voljo znanstvenikom in akademikom. Drugi del pa so poimenovali MILNET in je bil uporabljen izključno za potrebe uslužbencev ameriškega Ministrstva za obrambo ter oboroženih sil. Uporabljal je orodja za enkripcijo podatkov ter bil skoraj popolnoma ločen od omrežja ARPANET (povezan le na nekaj zelo varovanih vozliščih) (prav tako, 134−143).

Kljub širitvi omrežja ARPANET, pa ta ni vključeval vseh ameriških izobraževalnih in raziskovalnih ustanov, zato se je ameriška javna agencija NSF (ang. National Science Foundation) odločila ustanoviti svoje omrežje, NSFNET (Living Internet 1996č). Zaradi

skupnih ciljev se je NSFNET nato z ARPANET-om tudi medsebojno povezal, kasneje, v letu 1989, ko se je DARPA odločila zaradi dotrajanosti ARPANET ukiniti, pa ga je nadomestil, saj je imel modernejšo arhitekturo in bil hitrejši (Abbate 2000, 193−195). Enaka usoda je kasneje doletela tudi omrežje NSFNET in njegova vloga ter omrežni promet se je prenesel na privatne ponudnike interneta (ISP), večinoma že obstoječa večja ameriška telekomunikacijska podjetja (Sprint, Bell itd.) (Harris 1996).

3.4 Domenski sistem

Vsakemu računalniku v omrežju je dodeljen IP naslov, ki je podoben telefonski številki (primer: 173.194.39.180 je IP naslov Googla). Ker pa si je te številke težko zapomniti, imamo domenski sistem, ki je neke vrste imenik in povezuje določen IP naslov z določeno domeno (primer: www.google.com te pripelje na omenjeni 173.194.39.180 IP naslov).

.com je t.i. vrhnja internetna domena. Pristojnost dodeljevanja vrhnjih domen je najprej imela DARPA, ki je postavila prve vrhnje domene: .mil (military), .edu (educational), .gov (government), .com (commercial), .org (other organizations) in .net (network resources). Kasneje je nadzor nad dodeljevanjem domen prevzela NSF (ko je NSFNET nadomestil ARPANET), ko pa je bil internet privatiziran, pa se je pojavilo vprašanje, kdo naj ima pravico oziroma nadzor nad dodeljevanje vrhnjih domen. Pristojnost je najprej dobila državna neprofitna organizacija InternNIC, leta 1998 pa je bila pristojnost prenesena na ICANN (Internet Corporation for Assigned Names and Numbers), prav tako neprofitno organizacijo, ki ima vzpostavljen sporazum z ameriško vlado (Abbate 2000, 189−206).

3.5 Svetovni splet

Verjetno najbolj pomembna ter najbolj uporabljana aplikacija, ki teče na internetu, je svetovni splet (World Wide Web). Svetovni splet sestavljajo spletne strani, ki “tečejo” na strežnikih in do katerih lahko dostopamo s posebnim programom: spletnim brskalnikom.

Za očeta svetovnega spleta velja Tim Berners-Lee, takrat raziskovalec v fizikalnem laboratoriju CERN v Ženevi. V laboratoriju so že zelo zgodaj, zaradi velike količine podatkov, ki so jih morali pošiljati med različnimi računalniki znotraj CERN-a, naredili svoje omrežje računalnikov, kasneje pa se še povezali v evropsko omrežje EUnet, ki je bilo povezano z ameriškim ARPANET-om (prav tako, 210).

Kljub temu, da so osebni računalniki v 80ih že pričeli dobivati grafični vmesnik, je bil internet še daleč od tega. V kolikor nisi dobro vedel, kaj iskati in kje bi določen dokument lahko našel,

je bilo iskanje zelo težko. Rešitev za ta problem je leta 1990 podal Tim Berners-Lee, z iznajdbo svetovnega spleta, ki temelji na hipertekstu (ang. hypertext), s katerim je omogočeno lažje deljenje povezav do drugih dokumentov, ne glede na to, ali so na istem računalniku, ali ne (prav tako, 213−214).

Sama ideja hiperteksta je sicer obstajala že prej - iznašel jo je Ted Nelson leta 1963 (Living Internet, 1996d). Vendar pa jo je efektivno implementiral šele Berners-Lee, ko je s svojo skupino na CERN-u iznašel protokol HTTP (ang. hypertext transfer protocol), označevalni jezik HTML (ang. hypertext markup language) ter prvi spletni brskalnik, imenovan WorldWideWeb. Svetovni splet se je hitro razširil, najprej v druga raziskovalna središča, nato pa z novimi izboljšavami po celotnem internetu. Ena pomembnejših izboljšav je prišla z enote Univerze v Illinoisu, NCSA (ang. National Center for Supercomputing Applications), kjer je tamkajšnji raziskovalec Marc Andreessen naredil izboljšan brskalnik Mosaic, ki se je kasneje razvil v Netscape, ta pa v današnjo Mozillo Firefox (Abbate 2000, 214−217).

Svetovni splet je s svojim protokolom HTTP močno povečal uporabnost interneta, tako na gospodarskem področju (trgovina, oglaševanje), kot tudi na področju medčloveške komunikacije, širjenja idej in lažje koordinacije organiziranega delovanja ljudi za doseganje skupnih ciljev.

3.6 Iskra Delta

Pomembno vlogo v začetnem razvoju informacijske tehnologije, računalnikov in računalniških omrežij, pa je igralo tudi slovensko podjetje Iskra Delta. Iskra Delta je nastala v 70. letih 20. stoletja, kot oddelek Elektrotehne, ki se je ukvarjal z zastopstvom enega večjih ameriških proizvajalcev računalnikov, DEC[1] (Digital Equipment Corporation) (Škrubej 2008, 25−26).

Oddelek se je na začetku ukvarjal le s prodajo in servisiranjem DEC-ovih računalnikov, kasneje pa se je Delta odločila izdelati lasten računalnik, ki je temeljil na DEC-ovem mikroprocesorju ter njegovi arhitekturi. Razlog za to je bil čisto ekonomski - lažje je bilo namreč dobiti devize za nakupe sestavnih delov računalnika, kot pa za celotni računalnik. Delta je zato maja 1978 predstavila prvi jugoslovanski računalnik (Delta 340), ki je bil sestavljen tako iz domače, kot tuje strojne in programske opreme (prav tako, 36).

[1] Računalniki podjetja DEC so bili med drugim uporabljeni tudi pri izgradnji omrežja ARPANET ter za razvoj Microsoftove verzije programskega jezika Basic, ki sta ga razvila Bill Gates in Paul Allen (prav tako, 5−8).

Delta se je kasneje po nalogu slovenskega republiškega izvršnega sveta odcepila od Elektrotehne, ki je bila trgovsko podjetje, ter se pridružila konglomeratu Iskra pod imenom Iskra Delta. Pri tem sta se z Delto združila še računalniška razvojna oddelka Gorenja in Iskre (prav tako, 47−48).

Okrepljena Iskra Delta je v 80ih presenetila zahodno strokovno javnost z uspešno izgradnjo mikroračunalnika Partner ter večjedrnega računalnika Triglav (Trident), saj ta ni pričakovala, da bi bilo neko podjetje iz komunistične Jugoslavije zmožno razviti kaj tako naprednega (prav tako, 63−71). Deltin največji projekt pa je bil izgradnja računalniškega omrežja za kitajsko policijo (leta 1986), ki je povezal 10 največjih kitajskih mest, nekatera med seboj oddaljena tudi več tisoč kilometrov (prav tako, 123).

Kljub tovrstnim uspehom, je podjetje ob prehodu Jugoslavije v tržno gospodarstvo šlo v stečaj, čeprav je imelo v zadnjem letu (po navedbah takratnega direktorja) 81 milijonov USD prihodkov, 8,3 milijone USD dobička ter 2000 zaposlenih (prav tako, xiv).

4 Študije držav in konfliktov, kjer je internet igral eno ključnih vlog

4.1 Egipt ter revolucija v 2011

Egipt je polpredsedniška demokracija (glede na zadnjo sprejeto ustavo), z večinsko muslimanskim prebivalstvom, in igra ključno vlogo za stabilnost regije, predvsem kar se tiče varnosti judovske države Izrael. V Egiptu je sicer pred letom dni (julija 2013) vojska izvedla državni udar, v katerem je bil odstavljen prvi demokratično izvoljeni predsednik Egipta v zgodovini te države, Mohamed Mursi. V sedanjem času (konec maja in konec julija 2014) pa potekajo volitve novega predsednika države ter članov parlamenta (Wedeman in drugi 2013).

Internet je bil v Egiptu uveden leta 1993, najprej namenjen nekomercialni (znanstveni) dejavnosti, leta 1996 pa je bil komercializiran in predan v splošno uporabo (Hatem Ali 2009, 208). Kljub temu večino internetne infrastrukture nadzoruje država, prek nacionalnega telekomunikacijskega podjetja (Dainotti in drugi 2011, 5).

V januarju 2011 je egiptovska mladina prek družbenih omrežij (Facebook, Twitter) organizirala ogromen protest[2] proti tedanjemu avtokratskemu režimu Hosnija Mubaraka (Sharp 2011, 2). V želji zatreti organizacijo protestov, je oblast 28. januarja 2011 za celih 5 dni izklopila dostop do interneta. To pa je imelo na obiskanost protestov ravno nasproten učinek, saj je veliko ljudi ravno zaradi izpada interneta bilo odrezano od informacij o dogajanju na protestu in so se zato osebno odpravili ven v središče dogajanja (Hatem Ali 2009, 185). Ta primer je s tem pokazal na zanimivo varnostno dilemo, ko oblast v želji onemogočiti komunikacijo med protestniki, s tem lahko izzove njihovo večjo fizično udeležbo na protestih.

Internetni aktivizem, usmerjen proti oblasti, je v Egiptu obstajal že pred protesti v 2011, v obliki disidentskih blogov, organiziranja manjših protestov prek družabnih omrežij ter objavljanja posnetkov mučenja (ki so ga izvajale varnostne sile Egipta) na YouTube. Oblast vse do leta 2011 na te oblike političnega aktivizma ni odgovarjala s cenzuro interneta, temveč je uporabljala druge represivne prijeme, kot so grožnje in aretacije teh internetnih aktivistov (prav tako, 208−210).

Kljub nedavnemu državnemu udaru, ter *de facto* vladavini vojske v Egiptu, internet trenutno ni cenzuriran, se pa v luči volilne kampanje, kjer nasprotniki favorita predsedniških volitev,

[2] Revolucijo, ki se je začela s tem protestom, lahko po heidelberški definiciji konflikta označimo kot nasilno krizo.

generala Al Sisija, uporabljajo socialna omrežja tudi za zasmehovanje in žaljenje Al Sisija, pojavljajo pozivi (s strani njegovih podpornikov), naj se določene spletne strani ter ključne besede na socialnih omrežjih cenzurirajo. Za zgled temu postavljajo nedavno cenzuro socialnih omrežij s strani Turčije (Al Jazeera 2014).

4.2 Turčija in protesti v Gezi parku

Turčija je parlamentarna demokracija, na čelu katere je že več kot desetletje Recep Tayyip Erdogan, ki vodi konservativno Stranko za pravičnost in razvoj. Od lanske pomladi (pomlad 2013) Turčijo pretresajo protesti, ki bi jih po heidelberški definiciji lahko označili kot nasilne krize, saj vsaj ena od strani (predvsem država) uporablja tudi nasilne metode v posamičnih incidentih.

Protesti so se začeli 27. maja 2013, ko je manjša skupina protestnikov zasedla Gezi park, eno redkih zelenih površin v evropskem delu Istanbula, z namenom preprečitve uničenja parka in izgraditve nakupovalnega centra. 29. maja je policija nenasilne protestnike napadla s solzivcem in jih tako nasilno odstranila z območja parka. Vendar pa je ta akcija imela ravno nasprotni učinek, saj je povečala zavedanje ljudi o protestu in spodbudila ogromno povečanje števila protestnikov. S tem se je tudi razširil nabor vzrokov za proteste, med drugim nasprotovanje Erdoganovemu avtokratskemu načinu vodenja države, vpletanju Turčije v državljansko vojno v Siriji ter vpeljevanju elementov religije v javne institucije (npr. šole) (Arango 2013). Erdogan je že kmalu po začetku protestov javno kritiziral Twitter in družbena omrežja, s pomočjo katerih so protestniki organizirali protest ter širili svoje ideje in zahteve (Letsch 2013).

To pa ni bil prvi primer negodovanja Erdoganove oblasti nad spletnimi vsebinami. Dostop do YouTube-a je bil zaradi tovrstnih vsebin v zadnjem desetletju že večkrat občasno onemogočen[3], kljub temu pa je, po spletnih analitikah sodeč, bil vedno med 10 najbolj obiskanimi spletnimi stranmi v Turčiji, saj so uporabniki znali najti pot naokoli blokade. Oblasti so omejitev dostopa ponavadi uveljavile prek DNS strežnikov pri lokalnih ponudnikih interneta. Vsak izmed teh ponudnikov ima namreč svoj DNS strežnik, ki deluje kot imenik in povezuje domenska imena z IP naslovi strežnikov, ki gostijo spletne strani. Uporabniki so se tovrstni blokadi izognili tako, da so v omrežnih nastavitvah svojega računalnika zamenjali IP

[3] Samo v prvi polovici leta 2013 je Turčija podala Googlu skoraj 1700 zahtev po odstranitvi določenih vsebin s spleta - trikrat več kot katera koli druga država. Google je večino zahtev zavrnil (Euronews 2014).

naslov DNS strežnika svojega lokalnega ponudnika interneta z IP naslovom nekega tujega strežnika, ponavadi Googlovega (Bilgin 2012, 19).

Pred lokalnimi volitvami marca 2014, ko je bilo ozračje v državi zaradi predvolilne kampanje in korupcijskega škandala zelo napeto, je premier Erdogan na predvolilnem shodu zagrozil z blokado Twitterja. Le nekaj ur zatem je dostop do Twitterja dejansko bil onemogočen z že omenjeno tehniko blokade spletne strani na DNS strežnikih turških ponudnikov interneta (Hurriyet Daily News 2014). Teden dni kasneje je bil onemogočen tudi dostop do YouTube-a (Mlot 2014).

Ker so uporabniki brez velikih težav to blokado zaobšli, je država reagirala z direktno blokado IP naslovov Twitterja pa tudi IP naslovov Googlovega DNS strežnika. To je sicer začasno zmanjšalo dostop turških uporabnikov do omenjenega družbenega omrežja, vendar pa so iznajdljivi uporabniki hitro našli druga orodja s katerimi so zaobšli blokado, npr. program za anonimno dostopanje do spletnih vsebin, Tor (Orcutt 2014).

Po lokalnih volitvah, na katerih je močno slavila stranka premierja Erdogana, je minister za telekomunikacije, Lutfi Elvan, na neformalnem pogovoru z novinarji potrdil, da vlada razmišlja o vzpostavitvi svojega “ttt protokola, namesto www” (Haaretz 2014). Www protokol sicer ne obstaja, vendar pa je minister verjetno mislil na vzpostavitev nacionalnega interneta.

4.3 Rusija

Rusija je polpredsedniška demokracija, ki jo že več kot desetletje vodi Vladimir Putin s stranko Enotna Rusija. Putin je na čelo države prišel kot naslednik Borisa Jelcina in že kmalu spoznal moč medijev, še posebej televizije. Ravno zaradi slednje, bolj natančno TV postaje Borisa Berezovskega (ORT), je v dokaj kratkem času postal prepoznaven v javnosti - pa tudi priljubljen in zato na predsedniških volitvah leta 2000 zmagal že v prvem krogu. Vendar pa je kmalu po volitvah spoznal tudi drugo stran moči medijev, ko mu je ob aferi Kursk močno upadla javnomnenjska podpora, tudi po zaslugi ORT, ki mu je takrat obrnila hrbet. Zato ne čudi, da se je kmalu odločil spraviti pod svoj nadzor tri največje ruske televizijske postaje (ORT, RTR in NTV), njihovi lastniki pa so bili svoje deleže prisiljeni prodati Putinu naklonjenim oligarhom ter oditi v izgnanstvo (Freiberg 2012).

Televizija je v Rusiji trenutno najmočnejši medij ter orodje, prek katerega se lahko vpliva na javno mnenje. Vendar pa v zadnjih letih raste število uporabnikov interneta - Rusija je tako na

drugem mestu med državami sveta po številu blogov, ruski jezik pa je deveti na svetu po številu spletnih strani (to mesto si deli s Francijo) (Rogoza 2012, 3).

Zaradi državnega nadzora nad večino TV, radijskih in tiskanih medijev, Putinova politična opozicija vedno bolj uporablja internet za širjenje svojih idej ter politično akcijo. Po parlamentarnih volitvah 4. decembra 2011 so tako s pomočjo spleta organizirali proteste v ruski prestolnici Moskvi, ki se jih je prvi dan udeležilo med 25 tisoč in 60 tisoč ljudi, v kasnejših dneh pa po navedbah organizatorjev tudi do 160.000 (Barry 2011).

Protestniki so za organizacijo in širjenje svojih idej uporabili tudi zelo priljubljeno rusko družbeno omrežje VKontakte (VK - nekakšna ruska različica ameriškega Facebooka), zato je ruska obveščevalna služba FSB kmalu (po navedbah direktorja VK Durova) zahtevala ukinitev profilov protivladnih aktivistov in aktivističnih skupin na tem omrežju. Pavel Durov, ustanovitelj in izvršni direktor VK, je zahteve FSB zavrnil (Razumovskaya 2011). Aprila 2014 je Durov odpotoval iz Rusije ter evropskim medijem sporočil, da je bil odstavljen z mesta izvršnega direktorja VK ter da so nadzor nad družbenim omrežjem prevzeli ljudje, povezani s Putinom. Razlog naj bi bila njegova nepripravljenost cenzurirati disidentske skupine ter podatke o njih sporočati oblastem (Kravtsova 2014).

Leta 2012 je ruska Duma sprejela zakon, ki omogoča vladi samovoljno cenzuriranje spletnih strani. Razlog naj bi bil boj proti spletnim stranem s pedofilsko vsebino, vendar pa je po mnenju kritikov zakon bil sprejet z namenom cenzuriranja političnih nasprotnikov (BBC 2012). Kritika je postala utemeljena marca 2014, ko je Rusija pričela blokirati dostop do spletnih strani ruskih disidentov, med drugim tudi Garija Kasparova in Alekseja Navalnega, ravno na podlagi zakonodaje sprejete leta 2012 (Gutterman 2014). Mesec dni kasneje je Duma sprejela tudi zakon, ki bloge enači z mediji, ukinja anonimnost komentarjev in prepoveduje določene besede in besedne zveze (MacFarquhar 2014).

Putin je v intervjujih že večkrat namignil na možnost vzpostavitve ločenega, nacionalnega interneta (Freiberg 2012). Aprila 2014 je internet označil za "projekt ameriške obveščevalne agencije CIA" in dejal, da bi morali "Rusijo zaščititi pred njim" (MacAskill 2014).

4.4 Iran

Iran je islamska republika, ki je uradno predsedniška demokracija, vendar pa ima v njej odločilni vpliv skupina islamskih klerikov (ajatol), združenih v Iranski svet varuhov. Kljub močnemu vplivu religije in konservativizma, je Iran tehnološko ena naprednejših držav v

regiji, saj naj bi imelo dostop do interneta kar 45 milijonov od 75 milijonov prebivalcev Irana (Tajdin 2013).

Junija 2009 so v Iranu potekale predsedniške volitve, na katerih sta se pomerila takratni predsednik Ahmadinedžad ter reformist Mousavi. Na volitvah je zmagal Ahmadinedžad, ki pa so ga Mousavi in njegovi privrženci obtožili volilne prevare, zato so se že kmalu po razglasitvi rezultatov pričeli nasilni in množični protesti (Worth 2009). Organizatorji so za organizacijo protestov ter obveščanje o dogajanjih na njih v dobršni meri uporabili tudi spletna družbena omrežja, še posebej Twitter. Zato se je protestov v zahodnih medijih hitro prijel nadimek "Twitter revolucija" (The Washington Times 2009).

Mousavijevi privrženci so med drugim tudi izvedli DDoS napad na spletne strani predsednika Ahmadinedžada, zaradi česar je nato oblast v odgovor (in poskus zajezitve organizacije protestov) blokirala dostop do interneta za 20 ur (Moscaritolo 2009). DDoS (ang. Distributed denial of service) napad je tehnika s katero se prek ogromnega števila računalnikov (običajno povezanih v skupno mrežo, t.i. botnet) izvede napad na neki strežnik. Sama tehnika je dokaj preprosta, saj napadalčevi računalniki samo preko pošiljanja velikega in ponavljajočega se števila zahtev (ang. request) obremenijo napadeni strežnik, ki tako ne more ustrezno odgovoriti vsem zahtevam, tudi tistim ki ne prihajajo z napadalčevega omrežja računalnikov in posledično spletna stran na tem strežniku postane nedostopna.

Iranske oblasti že dlje časa cenzurirajo internet, predvsem s filtriranjem določenih besed, ki so na črnem seznamu. Tovrstnega načina cenzure ni mogoče zaobiti s šifriranim protokolom HTTPS (HTTP Secure), saj ga Iran popolnoma onemogoča. Omogoča pa navadni HTTP protokol, vendar ga filtrira (Nazeri 2013, 3−5).

Od protestov leta 2009 so se iranski cenzorji naučili, da ni dobro popolnoma onemogočiti dostopa do interneta ali do družabnih omrežij, saj s tem povečajo jezo ljudi (varnostna dilema). Namesto tega raje uporabljajo tehniko upočasnjevanja dostopa (ang. traffic shaping/bandwidth throttling), s katero upočasnijo dostop do določenih spletnih strani v tolikšni meri, da niso več mogoče za normalno uporabo (Holmes 2013).

Ker je v Iranu več kot polovica populacije mlajše od 35 let, je velik del prebivalstva dobesedno zrasel z računalniki, zato so tehnološko vešči in znajo najti pot okoli tovrstnih tehnik cenzuriranja (Tajdin 2013). Najpogostejši način je uporaba virtualnih privatnih omrežij (VPN - virtual private network). Uporabnik se prek VPN programa na varen in šifriran način

poveže z VPN strežnikom v tujini (kjer ni cenzure) in nato preko tega strežnika dostopa do spletnih strani, ki so v njegovi državi prepovedane. Pri tem je potrebno poudariti, da je zaščitena in šifrirana le povezava med uporabnikom in VPN strežnikom, ne pa tudi med VPN strežnikom in končno spletno stranjo, do katere hoče uporabnik dostopiti (Villeneuve 2008). Zaradi uporabe tovrstnih tehnik so družbena omrežja Twitter, YouTube in Facebook zelo razširjena med mladimi Iranci (Tajdin 2013).

Leta 2013 je na Ahmadinedžada na predsedniškem mestu nasledil reformist Rouhani, ki se zavzema za zmanjšanje cenzure interneta. Sam je celo začel uporabljati Twitter in prek njega recimo sporočil, da je imel telefonski klic z ameriškim predsednikom Barackom Obamo - prvi tak stik med iranskim in ameriškim predsednikom po islamski revoluciji 1979. Tudi iranski minister za kulturo, Ali Jannati, je dejal, da bi se moralo umakniti blokado družbenih omrežij (Holmes 2013). Kljub temu si konservativni del politike prizadeva za uvedbo nacionalnega interneta, saj naj bi s tem "izboljšali internetni dostop ter zaščitili državo pred kibernetskimi napadi" (Tajdin 2013). Iran še pomni škodo, ki jo je njihovemu jedrskemu programu leta 2010 povzročil zahodni računalniški virus Stuxnet (Simpson 2013).

4.5 Kitajski veliki požarni zid

Kitajska je socialistična ljudska republika, ki jo vodi komunistična stranka. V gospodarskem smislu država že dolgo ni več (popolnoma) socialistična, temveč ima mešan ekonomski sistem s podjetji tako v državni, kot zasebni lasti, ter kapitalističnim prostim trgom.

Po vzoru jasminovih revolucij, ki so v letu 2011 zajele arabski svet, so poskušali kitajski disidenti prek družbenih omrežij organizirati proteste na Kitajskem. Ti poizkusi so klavrno propadli, saj so jih kitajske oblasti z represijo in številčno premočjo represivnih organov, uspele že v kali zatreti (FlorCruz 2011; Page 2011).

Kitajske oblasti še pomnijo pro-demokratične proteste na trgu Tiananmen junija 1989, ki so bili mnogo obsežnejši. Zato Kitajska vsako leto ob obletnici teh protestov poostri svojo cenzuro interneta, predvsem dostop do storitev podjetja Google (Levin 2014).

Kitajska ima zelo dodelan sistem cenzure, v javnosti poimenovan Veliki požarni zid (The Great Firewall) (prav tam). V njem poleg običajnih tehnik blokiranja dostopa do določenih spletnih strani s pomočjo domenskega sistema (DNS) uporablja tudi druge tehnike, predvsem

pregledovanje in blokiranje spletnega prometa na podlagi ključnih besed[4]. V kolikor so zaznane prepovedane ključne besede z določene spletne strani, se dostop računalnika do te strani avtomatično blokira za nek časovni okvir – ponavadi do 1 ure. Raziskovalci s Cambridgea pa so ugotovili, da se to dejstvo lahko obrne tudi proti cenzorjem samim, saj je možno ponarediti izvor paketka ter mu dodati naslov nekega vladnega računalnika (Clayton in drugi 2006, 1−11).

Ljudje se na tovrstno blokado odzivajo na inovativen način, tako da namesto prepovedanih ključnih besed uporabljajo druge - šifre. Namesto prepovedanih izrazov, kot sta npr. "Tiananmen" in "4. junij 1989" so oblikovali šifre, kot je "8x8", ki je krajšava za 64, ki označuje 6. mesec (junij) in 4. dan. Dosti se uporablja tudi sleng in narečne besede, ki jih je med 45 različnimi dialekti kitajščine veliko na izbiro. Mnogo uporabnikov spleta pa za dostop do blokiranih spletnih vsebin in storitev uporablja tudi VPN strežnike v tujini[5] (Shadbolt 2011).

Kitajske oblasti pa cenzure ne izvajajo le s tehničnimi sredstvi, ampak tudi z ekonomskimi. Podjetja, ki želijo poslovati na Kitajskem, se morajo podrediti zahtevam po cenzuri. Tako je na primer leta 2004 Yahoo posredoval kitajskim oblastem podatke o štirih kitajskih disidentih, ki so bili nato aretirani in obsojeni na dolgoletne zaporne kazni. Ker pa se zahodna podjetja v veliko primerih upirajo cenzuri, še bolj pa razkrivanju podatkov o uporabnikih kitajskim oblastem, jih poskušajo le-te čim bolj omejevati, tudi s podporo domačim podjetjem, ki nudijo konkurenčne storitve. Tako so na Kitajskem zrasle kopije Googla (Baidu), Twitterja (Sina Weibo), Facebooka (Renren), kjer kitajske oblasti lažje izvajajo cenzuro in nadzor nad uporabniki spleta (Figliola 2010, 6).

4.6 NSA škandal

Poleti 2013 sta časnika The Guardian in The Washington Post začela razkrivati obseg prisluškovanja, ki ga je nad ameriškimi državljani izvajala obveščevalna agencija NSA. Slednja je s pomočjo ameriških informacijskih in telekomunikacijskih podjetij izvajala obsežen nadzor nad komunikacijo tako državljanov ZDA kot tudi državljanov drugih držav. (Greenwald 2013a; Timberg 2013).

[4] Gre se za pregledovanje vsebine paketkov. Po analizi Univerze v Cambridgeu, naj bi Veliki požarni zid uspel pregledati do ⅔ vseh paketkov, ki potujejo po kitajskem internetnem omrežju (Clayton 2006, 12).
[5] Način dostopa do spletnih strani prek VPN je opisan v podpoglavju o Iranu.

Prisluškovalni program je razkril Edward Snowden, ki je do teh podatkov in informacij prišel kot uslužbenec NSA. Snowden je tik pred razkritjem odpotoval v Hong Kong in se tako izognil aretaciji s strani Združenih držav Amerike. Le-te so pritiskale tako na Hong Kong, kot tudi na druge države, pri čemer je veliko držav temu pritisku podleglo. Snowden se je zato odločil odpotovati v Srednjo ali Južno Ameriko, vendar pa obtičal na moskovskem letališču, saj evropske države niso omogočile preleta letala s Snowdnom na krovu skozi njihov zračni prostor (Greenwald 2013b).

ZDA so pritisnile tudi na podjetja oziroma storitve, ki jih je uporabljal Snowden in ki so omogočale večjo zasebnost njegovih komunikacij. Eno izmed njih je bilo podjetje Lavabit, ki je ponujalo storitve elektronske pošte. Po pritisku ameriških oblasti, je direktor podjetje raje zaprl, kot pa se uklonil njihovim zahtevam po izdaji podatkov svojih strank (Poulsen 2013).

Kljub uporabi tovrstnih načinov pritiska, pa se je Obamova administracija odločila reformirati zakonodajo in omejiti obseg prisluškovanja. V podjetjih, predvsem neameriških, se je povečalo zavedanje o pomenu varovanja podatkov in uporabe enkripcije, predvsem zaradi industrijskega vohunjenja. V računalniških krogih pa se je povečalo število projektov (ter participacija na njih), ki povečujejo zasebnost uporabnikov. NSA škandal lahko po heidelberški definiciji označimo kot konflikt prve stopnje - spor glede vrednot nacionalnega, pa tudi nadnacionalnega, pomena (Rosenbach 2014).

4.7 Seznam načinov blokiranja neželenih vsebin in aktivnosti na internetu

Načini, na katere lahko države blokirajo neželeni internetni promet (Figliola 2010, 20−21):

- **Blokiranje ključnih besed**: Blokiranje paketkov, ki vsebujejo določene ključne besede, ki so na "črni listi".
- **Blokiranje spletnih domen na ravni DNS**: V domenskem imeniku, se IP računalnika, na katerega je vezana domena podvržena blokadi, zamenja z IP naslovom računalnika, ki uporabnika obvesti, da spletna stran ni več ne voljo.
- **Blokiranje IP naslovov**: Ker se blokadi domene lahko izogne z direktnim vpisom IP naslova v URL, je ukrep stopnjo višje direktna blokada IP naslova neželene spletne strani. Na ta način se prepreči prihod vseh paketkov iz tega IP naslova.
- **Dušenje pasovne širine (ang. bandwidth throttling)**: Omeji se količino podatkovnega prometa, ki je poslan prek interneta. Tako se ne popolnoma onemogoči dostopa do interneta, ampak le dovolj omeji, da postane veliko manj uporaben.

Tovrsten pristop uporabljajo oblasti v določenih državah (Iran, Egipt, Turčija, …) v primeru množičnih protestov, organiziranih prek spletnih družbenih omrežij.

- **Klasifikacija prometa (ang. traffic classification)**: Omejevanje ali blokada paketkov, ki uporabljajo določen protokol (npr. FTP ali HTTPS), tudi določena vrata (ang. port).
- **Globoko pregledovanje paketkov (ang. deep packet inspection)**: Metoda pregledovanja vsebine celotnega paketka, s katero je na primer možno (že omenjeno) blokiranje ključnih besed.
- **Plitko pregledovanje paketkov (ang. shallow packet inspection)**: Metoda, s katero se pregleda le glavo paketka (ang. header), kjer so zapisani podatki o paketku, kot na primer protokol ter izvorni naslov paketka. S tem se omogočita že omenjena blokada IP naslovov in klasifikacija prometa.

5 Prihodnji razvoj interneta

5.1 ICANN

ICANN je neprofitna organizacija, registrirana v Kaliforniji, ki koordinira globalni domenski sistem (DNS). Nadzor nad tem sistemom je organizaciji predalo ameriško ministrstvo za trgovino (ki ga je pred tem dobilo od Ministrstva za obrambo) tako, da je z ICANN-om sklenilo pogodbo (ang. AoC - Affirmation of Commitments). Prihodki ICANN-a so v večini vezani na provizije, ki jih dobi od prodajalcev domen (kot na primer: GoDaddy, Domenca itd.) (Kruger 2009, 3−5).

Ameriški vpliv nad DNS sistemom ni bil nikoli po godu ostalim mednarodnim igralcem, zato sta si še posebej OZN in EU prizadevala za prenos nadzora nad vrhnjimi domenami na neko mednarodno telo (Svete 2005, 21−22; Kruger 2009, 8). ZDA sicer niso nikoli uporabile svojega vpliva nad ICANN-om, da bi vsilile svojo politiko - recimo prepovedale katero izmed vrhnjih domen ali onemogočile kakega ponudnika spletnih domen. Tudi ob zadnjem povečanju števila vrhnjih domen, ko je bila med drugim dodana .xxx domena, ki jo Obamova administracija sicer ni odobravala, je pa tudi ni poskušala ustaviti (Macri 2014).

Leta 2015 se izteče pogodba med ICANN-om in ameriško vlado. Po koncu pogodbe bo nadzor nad vrhnjimi domenami v celoti v rokah ICANN-a, ki se bo prestrukturiral in imel nov sistem upravljanja. Ta bo vključeval tudi mednarodne igralce, pri čemer pa tu ne bo šlo le za predstavnike vlad tujih držav, temveč predvsem za predstavnike civilne družbe, internetnih skupin in drugih organizacij[6] (Gross 2014).

5.2 Možni scenariji prihodnjega razvoja interneta

5.2.1 (Inter)nacionalni interneti

Več voditeljev držav je že izrazilo ali namignilo na željo po ustanovitvi nacionalnega interneta, oziroma bolje poimenovanega “intranet”. Tri države, ki že imajo tak sistem, so Severna Koreja, Kuba in Mjanmar. V teh državah imajo močno cenzuriran nacionalni intranet, namenjen državljanom. Poleg intraneta pa imajo tudi popolnoma ločeno linijo do svetovnega interneta, ki jo lahko uporabljajo samo za to pooblaščeni ljudje (Rhoads 2011).

[6] Na primer VeriSign, podjetje, ki kotira na ameriški borzi Nasdaq in ima nadzor nad vrhnjima domenama .com in .net (prav tam).

Države, ki prav tako glasno razmišljajo o nacionalnem intranetu, so med drugim Rusija, Kitajska, Iran in Turčija. Ker imajo te države podoben pogled na kontrolo interneta, bi se lahko zgodilo, da bi ustvarile skupni, internacionalni internet, ki bi bil močno cenzuriran in nadzorovan, saj je imeti vsak svoj nacionalni intranet manj ekonomično. V praksi bi to naredili tako, da bi imeli omrežja v svoji verziji interneta fizično ločena od svetovnega interneta (torej ločena fizična infrastruktura). Glede na geografsko bližino omenjenih držav tak podvig ne bi bil nemogoč. Večjo oviro bi predstavljal nek drug dejavnik: globalna prepletenost gospodarstev. Podjetja iz avtokratskih držav močno sodelujejo s podjetji zahodnih držav, zato je zaradi čisto gospodarskih interesov in lobijev razdelitev interneta na zahodni in vzhodni internet (po vzoru hladne vojne) zelo malo verjetna (Hustad 2013; Raymond 2013, 5−6).

5.2.2 Trenutni internet z močnejšo mednarodno komponento

Najbolj verjeten scenarij je, da bo internet še vedno ostal globalen, monoliten, ter da se bo leta 2015 res zgodila reforma nadzora nad domenskim sistemom, kjer bo nad upravljanjem slednjega bdelo več različnih, tako vladnih kot nevladnih, organizacij z različnih delov sveta. S tem se bo efektivno utišalo kritike, da je internet pod nadzorom ZDA, ki so temeljile na dejstvu, da ima ICANN sklenjeno pogodbo z ameriško vlado o upravljanju domenskega sistema (Gross 2014).

Ker internetno povezavo omogočajo predvsem velika podjetja - ponudniki interneta (ISP) - nekatera tudi v državni lasti, bodo države še zmeraj ohranjale nadzor nad omrežji na njihovem ozemlju. Preko teh ISP-jev bodo lahko avtoritarni režimi še vedno izvajali cenzuro, ki pa bo na drugi strani imela inovativne uporabnike, ki se bodo poskušali cenzuri čim bolj izmikati.

5.2.3 Popolnoma decentraliziran internet

Kljub temu, da je internet že v osnovi bil zamišljen kot decentralizirano omrežje računalnikov, kjer napad na eno točko ne bi uničil celotnega sistema, pa internet ni v celoti (ali ni dovolj) decentraliziran. Področja, kjer so mogoče izboljšave so domenski sistem, strežniški prostor in tudi sama internetna infrastruktura.

Z domenskim sistemom upravlja ICANN, ki določa vrhnje domene, sami domenski imeniki pa so razpršeni po celotnem svetu in z njimi upravljajo ponudniki domen in ponudniki interneta. To sicer daje določeno stopnjo decentraliziranosti, vendar je število tovrstnih imenikov v posamezni državi majhno in ve se, katera podjetja jih omogočajo, zato lahko država s pritiskom na ta podjetja vsili blokado določenih domen. V Sloveniji je tak primer

blokada spletne stavnice Bwin (www.bwin.com), ki jo na zahtevo oblasti blokirajo vsi slovenski domenski imeniki (Lukić 2012).

Tudi strežniški prostor je podobno kot domenski imeniki razpršen po svetu. Ponujajo ga predvsem posebej specializirana podjetja (ponavadi ta, ki ponujajo tudi domene), seveda pa si lahko svoj strežnik postavi vsak malo bolj izkušen računalničar. Kljub temu pa je možna še večja stopnja decentralizacije in anonimizacije, ki onemogočita pritisk avtoritarnih oblasti na lastnike strežnikov z namenom cenzure spletnih vsebin.

5.2.3.1 Tor

Ena najbolj dodelanih rešitev, ki omogočajo popolno decentralizacijo domenskega sistema ter anonimizacijo ponudnikov strežniškega prostora, je projekt Tor. Tor je s finančnim vložkom pomagal vzpostaviti ameriški mornariški razvojni laboratorij (ang. U.S. Naval Research Laboratory) za potrebe "zaščite vladnih komunikacij" (Tor project 2014a), po drugih podatkih pa tudi zato, da bi ga lahko uporabljali kitajski disidenti (Krebs 2007).

Tor uporablja svoj domenski sistem, ki je popolnoma decentraliziran s pomočjo distribuirane zgoščene tabele (ang. distributed hash table). Distribuirana zgoščena tabela je preprosta baza podatkov, kjer se podatki shranjujejo v obliki ključa in vrednosti, ki je dodeljena ključu - torej na enak način, kot delujejo običajni domenski imeniki (Tor project 2014b).

Anonimizacijo strežnikov pa Tor zagotovi tako, da v svojem domenskem imeniku ne shranjuje IP naslova strežnika (ob določeni domeni), temveč le njegov javni ključ. Uporabnik Tora svojo zahtevo dostopa do določene spletne strani enkriptira s tem ključem, sama zahteva pa nato preko naključnih vozlišč (ang. nodes) v omrežju pride do želenega strežnika, ki s svojim zasebnim ključem dekriptira zahtevo ter nato po isti poti pošlje nazaj ponovno enkriptirane podatke. Vsako vozlišče v omrežju pozna le vozlišče pred njim in za njim, ne pa tudi celotne poti od uporabnika do strežnika. Tako je omogočena popolna anonimizacija tako uporabnika, kot tudi strežnika (prav tam).

5.2.3.2 Freenet

Kljub temu, da Tor ponuja popolno decentralizacijo DNS sistema ter anonimizacijo strežnikov, pa ne ponuja popolne decentralizacije strežniškega prostora. V kolikor bi napadalec nekako lociral lokacijo strežnika, na katerem je spletna vsebina, ki jo želi onemogočiti, bi z uspešnim napadom (fizičnim ali pa virtualnim) efektivno onemogočil dostop do nje. Ta problem rešuje projekt Freenet, ki uporablja t.i. distribuirano shranjevanje

podatkov. Vsak od uporabnikov da omrežju Freenet na razpolago delček svojega trdega diska, kamor se shranijo enkriptirani podatki, torej celotne spletne strani ali njihovi deli. Strežniški prostor je tako popolnoma decentraliziran in porazdeljen med vsemi uporabniki, poleg tega pa enkriptiran, kar omogoča večjo varnost in anonimnost uporabnikov (Freenet 2014).

5.2.3.3 Decentralizirana internetna infrastruktura

Veliko trši oreh, kot popolna decentralizacija domenskega sistema in strežniškega prostora, pa je decentralizacija internetne infrastrukture. Trenutno internetno infrastrukturo sestavljajo fizični kabli (predvsem kabli iz optičnih vlaken), ki jih imajo v lasti večji ponudniki interneta (pri nas na primer Telekom in T-2). Vsak izmed teh ponudnikov interneta[7] ima svoje omrežje uporabnikov. Da pa lahko ti uporabniki komunicirajo z uporabniki omrežij drugih ponudnikov interneta, pa morajo biti ta omrežja med seboj povezana, kar se zgodi na stičnih točkah NAP (ang. network access point) (Tyson 2001). Nacionalne oblasti lahko prek pritiska na ISP-je oziroma s fizičnim zasegom infrastrukture popolnoma izklopijo dostop do interneta ter komunikacijo med uporabniki v teh omrežjih, kar se je na primer zgodilo januarja 2011 v Egiptu.

Tak problem lahko reši popolnoma decentralizirano omrežje. Najbolj napredna rešitev na tem področju je brezžično zankasto omrežje (ang. wireless mesh network), ki se vzpostavi po P2P pristopu[8] (ang. peer-to-peer). Naprave v omrežju se med seboj povežejo prek brezžične povezave, za koordinacijo pošiljanja podatkov pa uporabljajo že omenjeno distribuirano zgoščeno tabelo. Tako preprosto infrastrukturo se lahko uporabi za koordinacijo protestov in širjenje informacij, ki jih želijo oblasti cenzurirati. Vendar pa trenutno ta tehnologija še ni primerna za gostitev večjih spletnih strani, ki zahtevajo večjo pasovno širino, kot je na primer spletna stran za deljenje video vsebin, YouTube. Enako velja za projekta Tor in Freenet (Roos 2007).

Mesh networking sicer ni v široki uporabi, vendar pa bi se lahko njegova priljubljenost in uporabnost povečala že v bližnji prihodnosti, ko bo zaradi vzpona interneta stvari (ang. internet of things) med nami vedno več pametnih naprav[9], ki bodo komunicirale druga z drugo (ang. machine-to-machine - M2M). Ob dovolj velikem številu takih naprav ter velikosti

[7] Torej tisti, ki imajo v lasti fizično omrežje in ne prodajajo naprej omrežja nekoga drugega.
[8] Enak pristop uporabljata Tor in Freenet, pa tudi druge decentralizirane tehnologije (protokoli), kot na primer Bitcoin in BitTorrent.
[9] Tukaj niso mišljeni le pametni telefoni, temveč čisto običajne stvari, kot na primer hladilnik, ki se bodo razvile v naprave sposobne "pametnega" komuniciranja z drugimi napravami.

prostora, ki bi ga bile sposobne pokrivati, bi lahko nastala decentralizirana internetna infrastruktura.

6 Sklep in verifikacija hipotez

V sodobnih konfliktih, predvsem nasilnih protestih proti avtoritarni oblasti, ki jih lahko po heidelberški definiciji označimo kot nasilne krize, postaja internet vedno bolj pomembno sredstvo organiziranja in boja. Zato lahko na podlagi proučenih primerov konfliktov v splošnem potrdim svojo prvo hipotezo, da želijo države, zaradi sodobnih konfliktov, povečati svoj nadzor nad internetom. Izjema je tu le ameriški NSA škandal, kjer po razkritju prisluškovanja ameriškim in tujim državljanom, teče reforma zakonodaje ter same organizacije NSA (Timm 2014). V večini ostalih držav, so ob konfliktih voditelji držav zaostrili svojo retoriko in napovedali močnejši nadzor nad internetom.

Tudi drugo hipotezo, da zaradi ameriškega nadzora nad internetom nekatere države razmišljajo o vzpostavitvi lastnih internetov, lahko potrdim, kljub temu da ni čisto točna. ZDA imajo nadzor le nad domenskimi strežniki, vendar so ga predale v zunanje izvajanje in ne posegajo vanj. Še več, naslednje leto naj bi se ZDA popolnoma odpovedale temu nadzoru. Nekateri voditelji tujih držav (Rusija, Turčija, Iran) so dejstvo, da imajo ZDA nadzor nad domenskim sistemom, uporabili za upravičevanje povečevanja lastnega nadzora nad internetom. Hipotezo potrjujem zato, ker so nekateri svetovni voditelji res izrazili željo po vzpostavitvi lastnega interneta (intraneta), vendar pa je verjetnost za dejansko uresničitev tega dokaj majhna.

Kot glavni razlog za to bi izpostavil vlogo gospodarstva. V današnjem svetu so globalna gospodarstva med seboj že toliko prepletena ter odvisna od poslovanja prek interneta, da bi tovrsten ukrep lahko močno škodil podjetjem v teh državah. Popolnoma ločenemu internetu bi tako gospodarska elita nasprotovala, ne pa nujno tudi večjemu državnemu nadzoru in cenzuri interneta. Če vzamemo za primer Kitajsko, so tam namreč zrasla ogromna internetna podjetja, ki so v bistvu kopije ameriških internetnih velikanov (Google, Facebook, Twitter), ki jih kitajska vlada cenzurira. V kolikor te cenzure ne bi bilo, bi verjetno imela ravno ta ameriška podjetja na kitajskem trgu največji tržni delež.

Med tremi scenariji prihodnjega razvoja interneta, je najbolj verjeten obstanek globalnega (monolitnega) interneta, kot ga poznamo že sedaj, ob različnih stopnjah državne kontrole v različnih državah. Elementi tretjega scenarija, ki ponujajo večjo decentralizacijo ter anonimnost na internetu, pa bodo (še naprej) poskušali rušiti državno cenzuro v avtoritarnih državah.

7 Literatura

1. Abbate, Janet. 2000. *Inventing the internet*. Cambridge (ZDA): MIT.
2. Al Jazeera. 2014. *Sisi mocked in Egypt internet campaign.* Dostopno prek: http://www.aljazeera.com/news/middleeast/2014/03/sisi-mocked-egypt-internet-campaign-201433022548298607.html (28. maj 2014).
3. Arango, Tim. 2013. Peaceful Protest Over Istanbul Park Turns Violent as Police Crack Down. *New York Times*, 31. maj. Dostopno prek: http://www.nytimes.com/2013/06/01/world/europe/police-attack-protesters-in-istanbuls-taksim-square.html (30. maj 2014).
4. Barry, Ellen. 2011. Rally Defying Putin's Party Draws Tens of Thousands. *New York Times*, 10. december. Dostopno prek: http://www.nytimes.com/2011/12/11/world/europe/thousands-protest-in-moscow-russia-in-defiance-of-putin.html (4. junij 2014).
5. BBC. 2012. *Russia internet blacklist law takes effect.* Dostopno prek: http://www.bbc.com/news/technology-20096274 (4. junij 2014).
6. Bilgin, Fevzi. 2012. *The Challenges of Democracy and Press Freedom in Turkey*. Washington DC: Rethink Institute. Dostopno prek: Google Books (30. maj 2014).
7. Bratuša, Tomaž. 2006. *Hekerski vdori in zaščita*. Ljubljana: Pasadena.
8. Clayton, Richard, Steven J. Murdoch in Robert N. M. Watson. 2006. *Ignoring the Great Firewall of China*. Cambridge: University of Cambridge. Dostopno preko: http://www.cl.cam.ac.uk/~rnc1/ignoring.pdf (9. junij 2014).
9. Dainotti, Alberto, Claudio Squarcella, Emile Aben, Kimberly C. Claffy, Marco Chiesa, Michele Russo in Antonio Pescape. 2011. *Analysis of Country-wide Internet Outages Caused by Censorship*. Dostopno prek: http://www.caida.org/publications/papers/2011/outages_censorship/outages_censorship.pdf (28. maj 2011).
10. DARPA. 2005. *Bridging The Gap Powered By Ideas*. Arlington: DARPA. Dostopno prek: http://www.dtic.mil/cgi-bin/GetTRDoc?Location=U2&doc=GetTRDoc.pdf&AD=ADA433949 (16. maj 2014).
11. Euronews. 2014. *Clashes in Turkey as internet censorship protests turn violent*. Dostopno prek: http://www.euronews.com/2014/01/18/clashes-in-turkey-as-internet-censorship-protests-turn-violent/ (30. maj 2014).
12. Figliola, Patricia. 2010. *U. S. Initiatives to Promote Global Internet Freedom*. Washington: Congressional Research Service. Dostopno prek: Google Books (9. junij 2014).

13. FlorCruz, Jaime. 2011. *'Jasmine' protests in China fall flat*. Dostopno prek: http://edition.cnn.com/2011/WORLD/asiapcf/02/20/china.protests/ (9. junij 2014).
14. Freenet. 2014. *What is Freenet?* Dostopno prek: https://freenetproject.org/whatis.html (13. junij 2014).
15. Freiberg, Philip. 2012. *Putin's Zugzwang*. Dostopno prek: Google Books (4. junij 2014).
16. Greenwald, Glenn. 2013a. NSA collecting phone records of millions of Verizon customers daily. *The Guardian*, 6. junij. Dostopno prek: http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order (11. junij 2014).
17. --- 2013b. Edward Snowden: the whistleblower behind the NSA surveillance revelations. *The Guardian*, 9. junij. Dostopno prek: http://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance (11. junij 2014).
18. Gross, Grant. 2014. U.S. government pulls out of ICANN. *PCWorld*, 14. marec. Dostopno prek: http://www.pcworld.com/article/2108780/us-government-to-end-formal-relationship-with-icann.html (12. junij 2014).
19. Gutterman, Steve. 2014. *Russia blocks internet sites of Putin critics*. Dostopno prek: http://www.reuters.com/article/2014/03/13/us-russia-internet-idUSBREA2C21L20140313 (4. junij 2014).
20. Haaretz. 2014. *Leaving the Web: Will Turkey ditch 'www' for 'ttt'?* Dostopno prek: http://www.haaretz.com/news/world/1.586483 (30. maj 2014).
21. Harris, Susan in Elise Gerich. 1996. *Retiring the NSFNET Backbone Service: Chronicling the End of an Era.* Dostopno prek: http://www.merit.edu/research/nsfnet_article.php (22. maj 2014).
22. Hatem Ali, Amir. 2009. The Power of Social Media in Developing Nations: New Tools for Closing the Global Digital Divide and Beyond. *Harvard Human Rights Journal* 24 (1). Dostopno prek: http://harvardhrj.com/wp-content/uploads/2009/09/185-220.pdf (28. maj 2014).
23. HIIK. 2014. *Methodology*. Dostopno prek: http://hiik.de/en/methodik/index.html (21. maj 2014).
24. Holmes, David. 2013. State of censorship: *How Iran censors the Internet (and how its citizens get around it)*. Dostopno prek: http://pando.com/2013/11/12/state-of-censorship-how-iran-censors-the-internet-and-how-its-citizens-get-around-it/ (5. junij 2013)
25. *Hurriyet Daily News*. 2014. Turkey blocks Twitter, after Erdoğan vowed 'eradication', 20. marec. Dostopno prek: http://www.hurriyetdailynews.com/turkey-blocks-twitter-

after-erdogan-vowed-eradication.aspx?PageID=238&NID=63884&NewsCatID=338 (30. maj 2014).

26. Hustad, Karis. 2013. In light of NSA spying, Brazil may take a step back from World Wide Web. *The Christian Science Monitor*, 12. november. Dostopno prek: http://www.csmonitor.com/Innovation/2013/1112/In-light-of-NSA-spying-Brazil-may-take-a-step-back-from-World-Wide-Web (12. junij 2014).
27. Kleinrock, Leonard. 2010. *Personal History/Biography: the Birth of the Internet*. Dostopno prek: http://www.lk.cs.ucla.edu/personal_history.html (21. maj 2014).
28. Kravtsova, Yekaterina. 2014. Vkontakte Founder Flees Russia, Claims Persecution. *The Moscow Times,* 22. april. Dostopno prek: http://www.themoscowtimes.com/news/article/vkontakte-founder-flees-russia-claims-persecution/498715.html (4. junij 2014).
29. Krebs, Brian. 2007. *Attacks Prompt Update for 'Tor' Anonymity Network*. Dostopno prek: http://blog.washingtonpost.com/securityfix/2007/08/attacks_prompt_update_for_tor.html (13. junij 2014).
30. Kruger, Lennard. 2009. *Internet Domain Names: Background and policy issues.* Washington: Congressional Research Service. Dostopno prek: Google Books (12. junij 2014).
31. Letsch, Constanze. 2013. Social media and opposition to blame for protests, says Turkish PM. *The Guardian*, 2. junij. Dostopno prek: http://www.theguardian.com/world/2013/jun/02/turkish-protesters-control-istanbul-square (30. maj 2014).
32. Levin, Dan. 2014. China escalating attack on Google. *The New York Times*, 3. junij. Dostopno prek: http://www.nytimes.com/2014/06/03/business/chinas-battle-against-google-heats-up.html (9. junij 2014).
33. Living Internet. 1996a. *Internet History -- One Page Summary*. Dostopno prek: http://www.livinginternet.com/i/ii_summary.htm (21. maj 2014).
34. --- 1996b. *J.C.R. Licklider And The Universal Network*. Dostopno prek: http://www.livinginternet.com/i/ii_licklider.htm (21. maj 2014).
35. --- 1996c. *How packets work*. Dostopno prek: http://www.livinginternet.com/i/iw_packet_packet.htm (21. maj 2014).
36. --- 1996č. *NSFNET*. Dostopno prek: http://www.livinginternet.com/i/ii_nsfnet.htm (22. maj 2014).
37. --- 1996d. *Ted Nelson discovers HyperText.* Dostopno prek: http://www.livinginternet.com/w/wi_nelson.htm (28. maj 2014).

38. Lukić, Aleksandar. 2012. BWIN toži Slovenijo za 50 milijonov evrov. *Slovenske novice*, 17. junij. Dostopno prek: http://www.slovenskenovice.si/novice/slovenija/bwin-tozi-slovenijo-za-50-milijonov-evrov (12. junij 2014).
39. MacAskill, Ewen. 2014. Putin calls internet a 'CIA project' renewing fears of web breakup. *The Guardian*, 24. april. Dostopno prek: http://www.theguardian.com/world/2014/apr/24/vladimir-putin-web-breakup-internet-cia (4. junij 2014).
40. MacFarquhar, Neil. 2014. Russia Quietly Tightens Reins on Web With 'Bloggers Law'. *The New York Times*, 7. maj. Dostopno prek: http://www.nytimes.com/2014/05/07/world/europe/russia-quietly-tightens-reins-on-web-with-bloggers-law.html (4. junij 2014).
41. Macri, Giuseppe. 2014. *Ex-Bush admin official: Internet giveaway weakens cybersecurity, opens door to Web tax.* Dostopno prek: http://dailycaller.com/2014/03/15/ex-bush-admin-official-internet-giveaway-weakens-cybersecurity-opens-door-to-web-tax/#ixzz2w6iIj295 (12. junij 2014).
42. Mathison, S.L., L.G. Roberts in P.M. Walkers. 2012. *The history of telenet and the commercialization of packet switching in the U.S.* Dostopno prek: http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=6194380 (22. maj 2014).
43. Mlot, Stephanie. 2014. *Turkey expands Internet blocks from Twitter to DNS*. Dostopno prek: http://www.itproportal.com/2014/04/01/turkey-expands-internet-blocks-from-twitter-to-dns (30. maj 2014).
44. Moscaritolo, Angela. 2009. Iran election protesters use Twitter to recruit hackers. *SC Magazine*, 15. junij. Dostopno prek: http://www.scmagazine.com/iran-election-protesters-use-twitter-to-recruit-hackers/article/138545/ (5. junij 2014).
45. Nazeri, Nima in Collin Anderson. 2013. *Citation Filtered: Iran's Censorship of Wikipedia*. Dostopno prek: http://www.global.asc.upenn.edu/fileLibrary/PDFs/CItation_Filtered_Wikipedia_Report_11_5_2013-2.pdf (5. junij 2014).
46. Orcutt, Mike. 2014. Data Show Turkey's Tweeters Beating Ban. *MIT Technology Review*, 24. marec. Dostopno prek: http://www.technologyreview.com/view/525811/data-show-turkeys-tweeters-beating-ban (30. maj 2014).
47. Page, Jeremy in James Areddy. 2011. China mobilizes against activists. *The Wall Street Journal*, 28. februar. Dostopno prek: http://online.wsj.com/news/articles/SB10001424052748703933404576170152436754150 (9. junij 2014).

48. Poulsen, Kevin. 2013. Edward Snowden's Email Provider Shuts Down Amid Secret Court Battle. *Wired*, 8. oktober. Dostopno prek: http://www.wired.com/2013/08/lavabit-snowden/ (11. junij 2014).
49. Raymond, Mark in Gordon Smith. 2013. *Reimaging the Internet.* Dostopno prek: http://www.isn.ethz.ch/Digital-Library/Publications/Detail/?id=168426&lng=en (18. junij 2014).
50. Razumovskaya, Olga. 2011. *Russian Social Network: FSB Asked It To Block Kremlin Protesters*. Dostopno prek: http://blogs.wsj.com/emergingeurope/2011/12/08/russian-social-network-fsb-asked-it-to-block-kremlin-protesters/ (4. junij 2014)
51. Rhoads, Christopher in Farnaz Fassihi. 2011. Iran Vows to Unplug Internet. *The Wall Street Journal*, 28. maj. Dostopno: http://online.wsj.com/news/articles/SB10001424052748704889404576277391449002016 (12. junij 2014).
52. Roe, Paul. 1999. The intrastate security dilemma: Ethnic conflict as a "Tragedy"? *Journal of Peace Research* 36 (2): 183-202. London: Sage publications. Dostopno prek: http://www.jstor.org/stable/424669 (27. junij 2014).
53. Rogoza, Jadwiga. 2012. *The Internet in Russia: The Cradle of Civil Society*. Dostopno prek: http://www.isn.ethz.ch/Digital-Library/Publications/Detail/?id=142568&lng=en (23. junij 2014).
54. Roos, Dave. 2007. *How wireless mesh networks work*. Dostopno prek: http://computer.howstuffworks.com/how-wireless-mesh-networks-work.htm (13. junij 2014).
55. Rosenbach, Marcel. 2014. 'Nothing Is Perfect': Tim Berners-Lee on 25 Years of the Web. *Spiegel*, 12. marec. Dostopno prek: http://www.spiegel.de/international/world/interview-with-tim-berners-lee-on-25th-anniversary-of-world-wide-web-a-958304.html (11. junij 2014).
56. Simpson, Connor. 2013. *Stuxnet used an old movie trick to fool Iran's nuclear program*. Dostopno prek: http://www.nextgov.com/cybersecurity/2013/11/stuxnet-used-old-movie-trick-fool-irans-nuclear-program/74216/ (5. junij 2014).
57. Shadbolt, Peter. 2011. *How microbloggers vault the 'Great Firewall of China'*. Dostopno prek: http://edition.cnn.com/2011/WORLD/asiapcf/02/18/china.microblogs/index.html (9. junij 2014).
58. Sharp, Jeremy. 2011. *Egypt: The January 25 Revolution and Implications for U. S. Foreign Policy*. Washington: Congressional Research Service. Dostopno prek: Google Books (28. maj 2014).

59. Svete, Uroš. 2005. *Varnost v informacijski družbi*. Ljubljana: FDV.
60. Škrubej, Janez. 2008. *Hladna vojna in bitka za informacijsko tehnologijo*. Ljubljana: Pasadena.
61. Tajdin, Behrang. 2013. *Will Iran's national internet mean no world wide web?* Dostopno prek: http://www.bbc.com/news/world-middle-east-22281336 (5. junij 2013).
62. *The Washington Times*. 2009. EDITORIAL: Iran's Twitter revolution, 16. junij. Dostopno prek: http://www.washingtontimes.com/news/2009/jun/16/irans-twitter-revolution/ (5. junij 2014).
63. Timm, Trevor. 2014. Congress wants NSA reform after all. Obama and the Senate need to pass it. *The Guardian*, 20. junij. Dostopno prek: http://www.theguardian.com/commentisfree/2014/jun/20/congress-obama-nsa-reform-obama-senate (1. julij 2014).
64. Tor project. 2014a. *Tor: Overview*. Dostopno prek: https://www.torproject.org/about/overview.html.en (13. junij 2014).
65. --- 2014b. *Tor: Hidden Service Protocol*. Dostopno prek: https://www.torproject.org/docs/hidden-services.html.en (13. junij 2014).
66. Tyson, Jeff. 2001. *How internet infrastructure works*. Dostopno prek: http://computer.howstuffworks.com/internet/basics/internet-infrastructure2.htm (13. junij 2014).
67. Villeneuve, Nart. 2008. *VPN Services.* Dostopno prek: http://en.flossmanuals.net/bypassing-censorship/ch025_what-is-vpn/ (5. junij 2014).
68. Webster, Stephen. 2011. *Vodafone confirms role in Egypt's cellular, Internet blackout*. Dostopno prek: http://www.rawstory.com/rs/2011/01/28/vodafone-confirms-role-egypts-cellular-internet-blackout/ (28. maj 2014).
69. Wedeman, Ben, Reza Sayah in Matt Smith. 2013. *Coup topples Egypt's Morsy; deposed president under 'house arrest'*. Dostopno prek: http://edition.cnn.com/2013/07/03/world/meast/egypt-protests/ (28. maj 2014).
70. Worth, Robert in Nazila Fathi. 2009. Protests Flare in Tehran as Opposition Disputes Vote. *The New York Times*, 14. junij. Dostopno prek: http://www.nytimes.com/2009/06/14/world/middleeast/14iran.html?_r=0 (5. junij 2014).