Cenzura interneta kao kontrolni mehanizam modernog doba

Čačija, Paula

SVEUČILIŠTE U ZAGREBU
FILOZOFSKI FAKULTET
ODSJEK ZA INFORMACIJSKE I KOMUNIKACIJSKE ZNANOSTI
Ak. god. 2020./2021.

Paula Čačija

Cenzura interneta kao kontrolni mehanizam modernog doba

Završni rad

Mentor: dr. sc. Tomislav Ivanjko, doc.

Zagreb, svibanj 2021.

Izjava o akademskoj čestitosti

Izjavljujem da je ovaj rad rezultat mog vlastitog rada koji se temelji na istraživanjima te objavljenoj i citiranoj literaturi. Izjavljujem da nijedan dio rada nije napisan na nedozvoljen način, odnosno da je prepisan iz necitiranog rada, te da nijedan dio rada ne krši bilo čija autorska prava. Također izjavljujem da nijedan dio rada nije korišten za bilo koji drugi rad u bilo kojoj drugoj visokoškolskoj, znanstvenoj ili obrazovnoj ustanovi.

Sadržaj

Sadržaj ii
1. Uvod 1
2. Povijest cenzure 2
3. Promjene s pojavom interneta 4
4. Cenzura interneta u Kini 6
4.1. Motivi cenzure, vrste problematičnog sadržaja i posljedice po korisnike takvog sadržaja 6
4.2. Tehnike cenzuriranja 9
5. Cenzura interneta u Saudijskoj Arabiji 11
5.1. Motivi cenzure, vrste problematičnog sadržaja i posljedice po korisnike takvog sadržaja 11
5.2. Tehnike cenzuriranja 13
6. Cenzura interneta u Siriji 15
6.1. Motivi cenzure, vrste problematičnog sadržaja i posljedice po korisnike takvog sadržaja 15
6.2. Tehnike cenzuriranja 18
7. Trinaest neprijatelja interneta 19
8. Zaobilaženje cenzure 22
9. Zaključak 24
10. Literatura 25
Sažetak 30
Summary 31

1. Uvod

Od samog početka pisma pa sve do 21. stoljeća, pristup informacijama nikada nije bio jednostavniji nego danas. Načini su razni, a razlikujemo one „opipljive“ poput odlaska u knjižnicu, samostalnog kupovanja knjiga, časopisa ili novina, od „neopipljivih“ načina (online): posjeti portalima, forumima, čitanje e-knjiga i na kraju krajeva - korištenje društvenih mreža. To ostavlja dojam da su informacije javno dobro dostupno bilo kome u bilo kojem trenutku, na bilo kojem mjestu. No, kolika je razina spoznaje o drugoj strani priče? Kolika je razina spoznaje manjka određenih informacija i načina pristupa istima? U tom slučaju se pojavljuje praksa čiji su se principi počeli primjenjivati već samim izumom pisma pa sve do danas - cenzura.

S obzirom na to da je pisana riječ oduvijek bila jedno od glavnih oružja s kojima su vlasti rukovale, potreba za kontrolom i filtriranjem informacija je rasla proporcionalno uz rast količine dostupnih informacija (Hebrang Grgić, 2008: 135). No, današnji oblici cenzuriranja se bitno razlikuju od onih prije 20. stoljeća - više ne postoji spaljivanje knjiga i knjižnica, a kažnjavanje i proganjanje „opasnih“ pisaca je postalo iznimno teško s obzirom na brojnost pisaca i informacija koje se nalaze na mrežnim stranicama. Budući da je predominantni medij današnjice internet, to ujedno pretpostavlja i da su vlasti usmjerile sve svoje napore prema cenzuriranju informacija na njemu, a ne više u knjigama, časopisima i sl.

Neovisno o tome što se filtriranje provodi i u zapadnim demokracijama, najekstremniji slučajevi se pojavljuju u komunističkim državama poput Kine, Kube i Sjeverne Koreje, ali i u nekomunističkim arapskim državama od kojih se ističu Saudijska Arabija i Iran. Cilj ovog rada je istražiti razne motive i načine cenzure na internetu u 21. stoljeću koji se razlikuju od države do države ovisno o njihovim potrebama - sve ih povezuje cenzura interneta u političke svrhe jer je to neizostavan faktor, no svaka od tri države koje planiram detaljnije obraditi ima još jedan bitni aspekt koji se nadograđuje na politički - Kina cenzurira pretežito u propagandne svrhe, Saudijska Arabija u religijske, a Sirija očajnički pokušava zadržati mir na svojem teritoriju. Neizbježno pitanje koje se postavlja je mogu li građani uopće izbjeći tu cenzuru i pristupiti željenom sadržaju (na što ću pružiti odgovor u nastavku rada).

2. Povijest cenzure

Aleksandar Stipčević, pojam cenzura definira kao: „...sustav mjera koje poduzimaju vlasti ili oni koji tu vlast predstavljaju, za sprječavanje javnog iznošenja ideja i mišljenja koje vlasti drže oprečnim svojim interesima, odnosno onim moralnim i društvenim normama koje vrijede u određenoj sredini i vremenu.“ (Stipčević, 1992: 30). Ona poprima različite oblike ovisno o različitim ideologijama te se metode provođenja cenzure značajno razlikuju od države do države, a ponekad čak i unutar iste države. Kroz povijest, već kod starih Grka, učeni ljudi su „prepoznali“ kako neselektivno čitanje knjiga (posebice kod mladeži) može pokvariti i upropastiti čovjeka. Metode kojima su se vodili su zabrana čitanja i slušanja pjesama, kao i progon samih pjesnika iz države. Rimski car August je također prepoznao štetu koju ljubavne pjesme imaju na čitatelje, pa je pjesnika Ovidija poslao u progonstvo i naredio da se njegove knjige izbace iz knjižnica (Stipčević, 2000: 141-142). S vremenom su Grci i Rimljani shvatili da su veći problem predstavljale knjige koje su, kako Stipčević kaže: „...bile tako vješto napisane da mnogi nisu u prvi mah ni slutili da čitaju opasne i štetne knjige.“ (Stipčević, 2000: 143). Tematika kojom su se bavili pisci „štetnih knjiga“ su bile kritike društvenih institucija ili pojedinaca iz višeg društvenog sloja.

Kršćanstvo, nakon svoga dolaska, nije odbacilo cenzuru kao oblik ograničavanja pristupa informacijama već je, dapače, prihvatilo tradiciju filtriranja informacija. Trebalo je pronaći način kako postupiti s nemoralnim i poganskim knjigama. Shvaćajući da neće moći uništiti djela poznatih grčih i rimskih autora, odlučili su zabraniti čitanje takvih tekstova, posebice kod redovnika, redovnica, svećenika i ostalih pobožnih ljudi koji su trebali služiti kao primjer svome narodu. Također, djela antičkih pisaca su bila dostupna samo uskom krugu učenih ljudi i većinom su se nalazila na sigurnome, u samostanskim knjižnicama, tako da običan puk nije ni imao pristup tim knjigama (Stipčević, 2000: 145). Najveća tragedija koju je doživjela pisana riječ onoga vremena dogodila se 391. godine kada su kršćani spalili Aleksandrijsku knjižnicu (Stipčević, 2000: 267). Taj čin je stavio točku na i u borbi kršćana protiv poganske pisane riječi.

Srednji vijek se smatra relativno mirnim razdobljem zbog apsolutne dominacije Crkve, no sve se promjenilo Gutenbergovim otkrićem tiskarskog stroja sredinom 15. stoljeća. Nakon Gutenbergovog tiskanja *Biblije,* Crkva i vlasti su uvidjele očiglednu opasnost masovnog tiskanja knjiga, jer su one odjednom postale dostupne svima koji su ih mogli kupovati, ne samo učenim ljudima. Broj pisaca koji su pisali lascivne i pornografske knjige se znatno povećao, te je Crkva izdala *Indeks zabranjenih knjiga* (Stipčević, 2000: 146), a

također, jedna od davno ustoličenih mjera je bila preventivna cenzura, gdje su autori slali svoja djela državnim i crkvenim vlastima prije njihove objave te se cenzura onda provodila na bezbolan način (Stipčević, 1994: 8).

Autori zabranjenih knjiga i tekstova su na razne načine pokušavali zaobići stroga pravila - domaću cenzuru su pokušali izbjeći tiskanjem knjiga izvan domovine, a također su sebe pokušali zaštititi objavljivanjem netočnih osobnih podataka poput imena, mjesta tiskanja, izdavača itd.

Za dvadeseto stoljeće, manji problem su predstavljale pornografske i ljubavne knjige, te je fokus vladajućih bio na znanstvenim i stručnim tekstovima te politički i ideološki nepoćudnim knjigama. Kako objašnjava Stipčević, totalitarni režimi su bili uvjereni da „knjige, u kojima se iznose teorije i misli suprotne vladajućoj ideologiji, mogu nanijeti veliko zlo društvu.“ (Stipčević, 2000: 149) što je smanjilo pritisak s nemoralnih ljubavnih knjiga. Brojne represije su se nastavile - od popisa zabranjenih knjiga, čišćenja i spaljivanja knjiga kao i progona autora. Nakon propasti komunističkog sustava, mnoštvo knjiga je bilo spaljeno zbog samog propagandnog sadržaja, a neke su se uništavale jer su se jednostavno smatrale suvišnima (Hebrang Grgić, 2008: 147). S demokracijom se pojavilo zagovaranje slobode izražavanja i jednakost pristupa informacijama za sve, no krajem 20. stoljeća, sve većom rasprostranjenosti i uporabom interneta, vlasti se susreću s novim problemima s kojima se njihovi prethodnici nisu morali suočavati.

3. Promjene s pojavom interneta

Začetak modernog interneta javlja se 60-ih godina 20. stoljeća, no jedna od njegovih najznačajnih komponenti se ustalila kao standard 1983. godine - komunikacijski protokol (*Transfer Control Protocol/Internetwork Protocol - TCP/IP*) koji je omogućio komunikaciju različitih računala (Online Library Learning Center, n. d.). Upravo ta komponenta čini internet onime što danas i je. Leiner et al. (2009: 22) opisuju internet kao globalnu mrežu sa sposobnostima „emitiranja" diljem svijeta, kao mehanizam za diseminaciju informacija, medij za suradnju i interakciju između pojedinaca i njihovih računala, bez obzira na njihove zemljopisne lokacije. Internet je revolucionarizirao načine na koje se vijesti šire te je potpuno izbrisao granice između država u virtualnom širenju dobrih i (potencijalno) opasnih informacija. Upravo stvaranje takve jedinstvene, dinamične, inkluzivne i demokratske mreže se pokazalo kao velika prijetnja državama koje inače ekstenzivno kontroliraju lokalni protok informcija.

S obzirom na to da ne postoji međunarodni sporazum ni zakon koji propisuje striktna pravila korištenja interneta, države su se same morale pobrinuti o načinima kontrole i filtriranja informacija kojima njihovi građani mogu pristupiti, što su neke od njih iskoristile s ciljem cenzuriranja određenog sadržaja. Hebrang Grgić (2008: 157) je u svom radu te načine cenzure podijelila prema intenzitetu na potpunu, djelomičnu ili odabranu cenzuru. Potpuna i djelomična cenzura se provode u totalitarnim državama (poput Kine, Kube, Sjeverne Koreje, Saudijske Arabije, Irana), a odabrana cenzura se provodi u demokracijama i filtrira se sadržaj štetan za određene grupe korisnika, npr. djecu. Također, definirala je četiri osnovne vrste cenzure na internetu - političku, sigurnosnu, cenzuru internetskih alata i društvenu cenzuru (Hebrang Grgić, 2008: 158). Politička cenzura obuhvaća i vjersku, a zabranjuje se pristup informacijama koje su u suprotnosti s vladajućom ideologijom. Sigurnosna cenzura onemogućava pristup sadržaju vezanom uz vojne sukobe i probleme s granicama. Cenzura internetskih alata kontrolira mrežne stranice koje omogućavaju komunikaciju elektronskom poštom i društvenim mrežama (Facebook, Whatsapp, YouTube), alate za pretraživanja (Google, Yahoo, Bing) itd., dok je društvena cenzura najčešća u demokratskim državama poput Francuske, Njemačke ili Ujedinjenog Kraljevstva, gdje se neprimjerenim sadržajem smatraju pornografija, stranice povezane s nasiljem, terorizmom, zloupotrebom droga i slično. Ovaj rad se neće baviti filtriranjem informacija u demokratskim državama, pošto je postotak kontroliranog sadržaja minimalan u usporedbi s postotkom u državama poput Kine, Sirije, Saudijske Arabije i ostalima koje će biti navedene u nastavku.

Sami načini cenzure variraju, od zakona koji zabranjuju određene aktivnosti na internetu, zahtijevanja da davatelji internetskih usluga (engl. *Internet Service Provider - ISP*[1]*)* blokiraju mogućnost pristupa određenim mrežnim stranicama, pa do kanaliranja interneta kroz posredničke poslužitelje (engl. *proxy server*[2]) koji su kontrolirani od strane države (Brown, 2008: 1). Kroz primjere cenzure interneta u Kini, Saudijskoj Arabiji i Siriji ovaj rad će dati uvid u suvremene motive i načine provođenja cenzure u svijetu u propagandne svrhe, religijske i svrhe opstanka cijelih društava.

[1] Davatelj internetskih usluga (engl. Internet Service Provider, akronim ISP), tvrtka koja korisnicima nudi usluge vezane uz pristup internetu i udomljavanje internetskih sadržaja (engl. hosting), tj. registriranje domene, smještaj mrežnih stranica, elektroničke pošte, mrežne trgovine i sl (Hrvatska enciklopedija, mrežno izdanje, 2021.)

[2] Posrednički poslužitelj (engl. Proxy Server), računalo koje stoji između klijenta i glavnog poslužitelja kao posrednik, a najčešće se koristi za posluživanje mrežnih stranica, tj. uporabu interneta. (Wikipedia, 2019)

4. Cenzura interneta u Kini

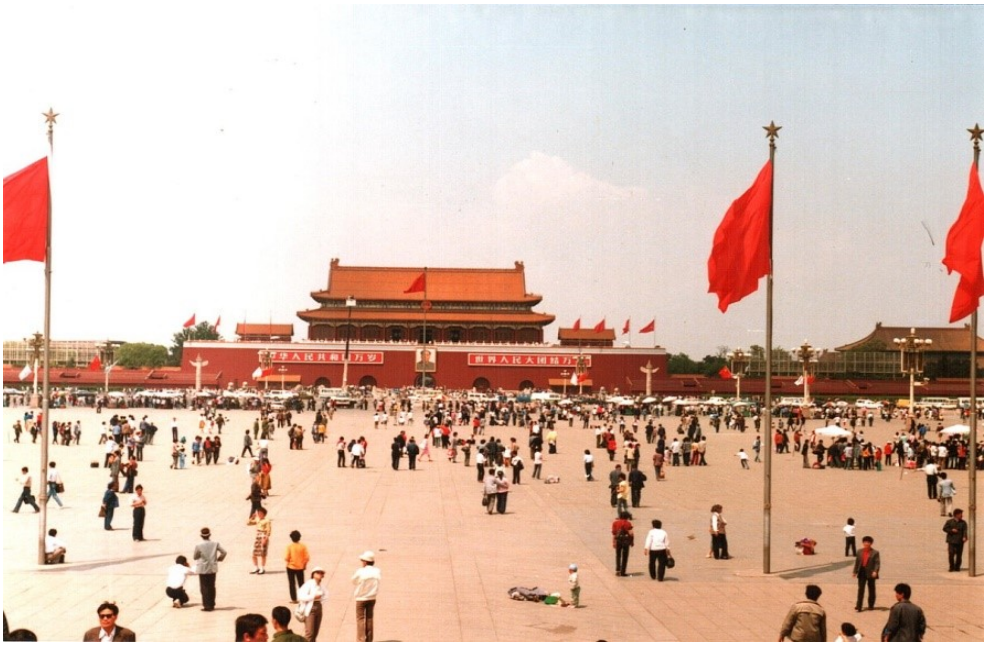
4.1. Motivi cenzure, vrste problematičnog sadržaja i posljedice po korisnike takvog sadržaja

Kina je država s bogatom poviješću cenzure, a ekstremni pothvati im nisu nepoznanica. Tako je car Č'in Ši-hunag-ti 213. g. pr. Kr. naredio da se spali velik broj štetnih knjiga na lomačama te je uz to naredio da se pobije 470 učenih ljudi i time onemogući daljnja proizvodnja loših tekstova (Hebrang Grgić, 2008: 137). Današnje metode cenzuriranja u Kini obuhvaćaju jedan od najvećih i najsofisticiranijih sustava za filtriranje informacija na internetu (Fu, Chan i Chau, 2013: 2). Kineska vlada se nikada nije eksplicitno izjasnila o specifičnoj vrsti podataka koje cenzurira, ali im je misao vodilja zaustaviti potencijalno kontaminiranje svijesti kineskih građana od strane zapadnjaka. Wang Chen, kineski službenik na području informacija, je to najbolje izrazio ovim riječima: „Sve dok je naš internet povezan s globalnim internetom, postojat će kanali i načini na koje će se štetne strane informacije pojavljivati na našem lokalnom internetu. Sve dok je naš internet otvoren za javnost, postojat će kanali i načini da korisnici interneta izražavaju svakakva mišljenja na internetu.“ (Mueller, 2011: 181). Kinezi kažu kako filtriraju samo stranice na kojima se nalazi neprimjeren sadržaj poput terorizma ili bilo kakvog drugog oblika nasilja. U nastavku rada, sagledavanjem vrste podataka kojima njihovi građani nemaju pristup, može se donijeti zaključak da je jedan od ciljeva kineskih vlasti zapravo smanjiti mogućnost rasprava o senzibilnim političkim temama te također spriječiti potencijalnu organizaciju prosvjeda i protuvladinih skupova.

Tehnologija koju Kina koristi za cenzuru će biti detaljnije obrađena kasnije, no za potrebe ovog rada bitno je znati da Kinezi nemaju pristup određenim stranicama ili dobivaju polovične povratne informacije jer se cenzura većinom provodi filtriranjem ključnih riječi (Lee i Liu, 2012: 131). Neke stranice i pojmovi koje Kinezi ne mogu dohvatiti su informacije o neovisnosti Tajvana i pokretu za neovisnost Tibeta, a možda najistaknutiji slučaj je incident na Tiananmenskom trgu u središtu Pekinga. Protesti iz 1989. na Tiananmenskom trgu su bili studentski prosvjedi koji su zagovarali demokraciju, slobodu govora i tiska. Prosvjedi su trajali danima, a s obzirom na to da je broj prosvjednika prešao milijun, kineske vlasti su uporabile vojsku te su 4. lipnja započeli s nasilnim gašenjem prosvjeda. Smatra se da je ubijeno do 10 000 ljudi te je incident prozvan masakrom (Tiananmen Square Protests, 2019). Kada kineski građani upišu pojam „Tiananmenski trg“ u svoje internet tražilice, povratne informacije se bitno razlikuju od onih koje bi dobili u Europi ili Sjevernoj Americi. Ono što

građani vide su uobičajene slike trga, bez ikakvih članaka ili referiranja na masakr ili proteste. Slika 1) prikazuje rezultate koje tražilica vraća kada se upiše Tiananmenski trg (ili protesti na Tiannanmenskom trgu) u Europi ili Sjedinjenim Američkim Državama, a Slika 2 prikazuje povratne informacije tražilica u Kini.

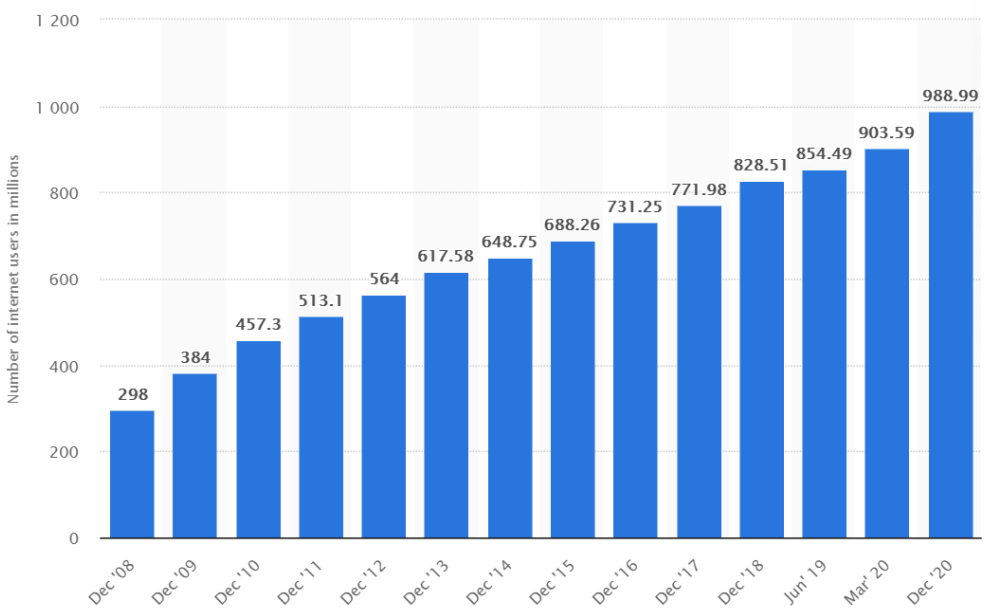
Slika 1. Tiananmenski trg za vrijeme demonstracija 1989. godine
(Izvor: https://www.history.com/news/who-was-the-tank-man-of-tiananmen-square)



Slika 2. Slika Tiananmenskog trga koja ne prikazuje demonstracije
(Izvor: https://en.wikipedia.org/wiki/1989_Tiananmen_Square_protests)

Također, 2011. godine su aktivisti pozivali na revoluciju jasmina, po uzoru na val revolucija koje su se događale u Sjevernoj Africi i na Bliskom Istoku. Većina stanovnika nije ni imala priliku vidjeti poziv na revoluciju, s obzirom na to da su kineske vlasti odmah cenzurirale riječ jasmin (kin. *mòlìhuā* -茉莉花) te su čak označili riječ 'danas' (kin. *jīntiān*, 今天） kao osjetljivu, kako bi spriječili slučajne nailaske na poziv na proteste (Lee i Liu, 2012: 126).

U lipnju 2010. godine, Kina je brojala 430 milijuna korisnika interneta, 32% populacije (Mueller, 2011: 177), a statistike iz 2021. godine pokazuju da su se brojke i više nego udvostručile, brojeći skoro milijardu korisnika kao što je vidljivu na Grafikonu 1 (Thomala, 2021). S takvim velikim brojem korisnika (engl. *netizens*), popis cenzuriranih stranica se širio, te tako danas uključuje: Facebook, Twitter, YouTube, Google, Snapchat, Whatsapp, Messenger, The New York Times, Wall Street Journal, Washington Post, mnogo probranih Wikipedia stranica, Netflix, Hulu, Amazon Prime Video, Gmail, Google Drive, Dropbox i mnoge druge. Ovaj popis vidno izgleda kao lista najposjećenijih stranica bilo kojeg Europljanina ili Amerikanca, a za sve zainteresirane, postoje različite stranice koje provjeravaju je li određena mrežna stranica cenzurirana u Kini: http://www.chinafirewalltest.com/ , https://www.comparitech.com/privacy-security-tools/blockedinchina/ , https://www.websitepulse.com/tools/china-firewall-test. Wikipedia također nudi ekstenzivan popis blokiranih stranica, s datumima kada je cenzura započela i informacijama ako su neke stranice prestali cenzurirati (poput Zooma ili japanskog Yahooa).



Grafikon 1. Povećavanje broja internet korisnika u Kini od prosinca 2008. do prosinca 2020. (Thomala, 2021)

4.2. Tehnike cenzuriranja

Kako objašnjavaju Lee i Liu (2012: 130-131), Kina je u početku koristila dva različita filtera za cenzuriranje informacija na internetu: filter uključivanja (engl. *inclusion filter*) i filter blokiranja (engl. *exclusion filter*). Kineska vlada je priložila listu zabranjenih stranica i njihovih adresa te je naredila davateljima internetskih usluga da blokiraju navedene mrežne stranice uz pomoć kompanije Cisco. No, filteri se nisu pokazali kao najbolje rješenje zato što je filter uključivanja dozvoljavao previše stranica s obzirom na stalno pojavljivanje novih, a filter blokiranja nije blokirao dovoljno stranica jer je bilo teško pronaći sve potencijalno opasne stranice. Zbog toga su spas našli u tehnici analize sadržaja (engl. *content analysis*[3]) koja je zabranila da korisnici pristupe bilo kakvim mrežnim stranicama ili URL-ovima koji su u sebi sadržavali ključne riječi kao što su ranije spomenute „Tiananmanov trg", „samostalnost Tibeta" itd.

Kako bi bio jasniji način na koji kontroliraju protok podataka, mora se spomenuti Veliki kineski vatrozid (engl. *The Great Firewall*), koji je dobio ime lukavom igrom riječi po uzoru na dobro poznati Kineski zid koji je također štitio kineski narod od nepoželjnih protivnika. Veliki kineski vatrozid je izgrađen (uz pomoć tvrtke Cisco) na mrežnoj okosnici Kine (Lee i Liu, 2012: 133), a mrežna okosnica je upravo centralni segment neke mreže (Sveznadar, n. d.) koji povezuje lokalne mreže (LAN-ove[4]) i mreže širokog područja - globalne mreže (WAN-ove[5]) (Šegrc, 2020). Kroz mrežnu okosnicu teče svo internetsko pregledavanje i bilo kakav mrežni promet što omogućava Kineskom vatrozidu da oblikuje jedan virtualni prsten oko cijele zemlje i time osigurava vladinu kontrolu nad mrežom.

Kako Lee i Liu objašnjavaju u svom radu (2012: 133-134), s obzirom na to da online informacije ulaze u Kinu kroz četiri priključne točke, kineska vlada kontrolira informacije tako što kontrolira te priključne točke. Time se kontrola proteže na davatelje internetskih usluga jer svaki od njih je priključen na bar jednu priključnu točku. Davatelji internetskih usluga dobivaju pristup mrežnoj okosnici, ali pod kontrolom vlade što znači da kad krajnji korisnici plaćaju pristup internetu jednom od nekoliko stotina davatelja internetskih usluga (ISP-ova), njihova aktivnost je odmah limitirana. Kineska vlada je vrlo jednostavno osigurala

[3] Analiza sadržaja (engl. Content Analysis), metoda istraživanja koja služi za utvrđivanje prisutnosti određenih riječi, tematike ili koncepta u nekom tekstu ili sl (Columbia Public Health, n.d.)

[4] Lokalna računalna mreža (engl. Local Area Network, akronim LAN), područna mreža namijenjena povezivanju računala i drugih mrežnih uređaja na manjim udaljenostima, npr. u okviru jedne zgrade, postrojenja ili kuće (Wikipedia, 2021, b)

[5] Mreža širokog područja (engl. Wide Area Network, akronim WAN), obično se prevodi kao globalna mreža koja pokriva veće zemljopisno područje: gradove, države ili kontinente. Koristi se za međusobno povezivanje udaljenih računala ili lokalnih mreža. (Wikipedia, 2014)

nadzor nad stotinama davatelja internetskih usluga tako što su postavili kontrolu nad samo četiri priključne točke svog interneta. Strategija koja je omogućila Kinezima da ovako dobro kontroliraju protok podataka u njihovoj zemlji je dobro vremenski uspostavljena intervencija u stvaranju sustava koji budno prati ponašanje i uzaludne pokušaje korisnika.

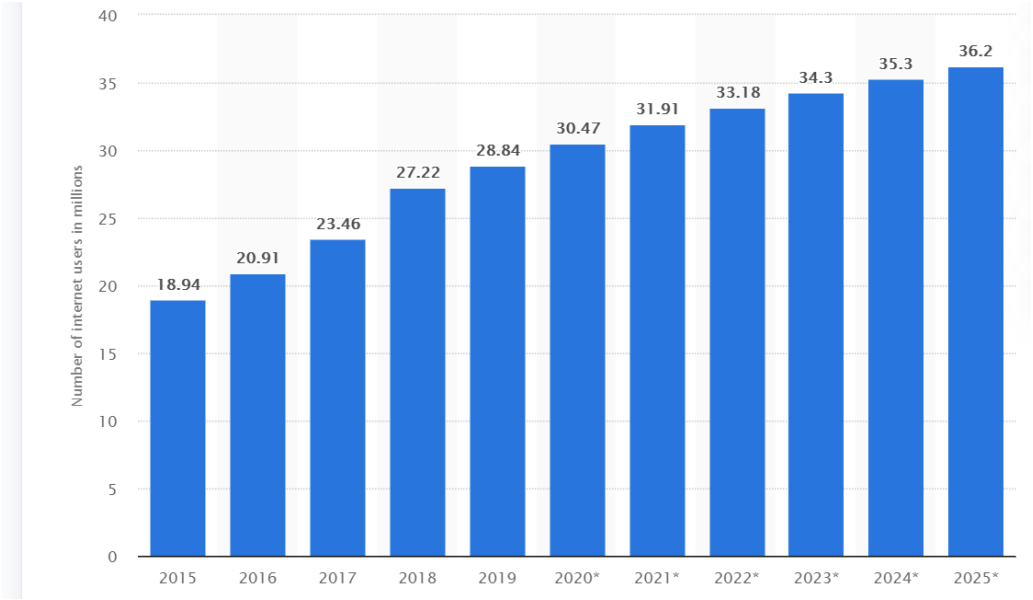
Ono što omogućava ovakvom sustavu da opstane je to što korisnici interneta u Kini većinom ni ne znaju da su se susreli s cenzuriranim stranicama, pošto će pokušaj pristupa zabranjenoj mrežnoj stranici izgledati kao tehnička pogreška, te će korisnici većinom nastaviti bezbrižno surfati internetom. Također, prema istraživanju iz 2005. godine koje je provela Kineska akademija društvenih znanosti, čini se da su Kinezi postigli svoj cilj - većina korisnika se služi internetom kako bi se zabavili, a ne pretraživali političke teme. Čak i studenti koji pripadaju mlađim generacijama i svjesni su cenzure od strane države (time su i svjesni da postoje načini zaobilaska cenzure) ne žele pristupiti zabranjenim stranicama ili ako žele, to je radi testiranja svojih vještina, a ne zato što ih zapravo zanima zabranjeni sadržaj (Lee i Liu, 2012: 146).

5. Cenzura interneta u Saudijskoj Arabiji

5.1. Motivi cenzure, vrste problematičnog sadržaja i posljedice po korisnike takvog sadržaja

U Saudijskoj Arabiji, i generalno arapskim zemljama, odnos prema pravu slobode govora, pravima ljudi i pristupu informacijama je znatno drugačiji nego u većini zapadnih zemalja, a bitna razlika je u tome što su tek nedavno počeli (djelomično) uvažavati ta prava (Shishkina i Issaev, 2018: 3). Kako bi lakše shvatili poziciju i razloge Saudijske Arabije u cenzuriranju interneta i medija, najbitnije je sagledati činjenice iz religijske perspektive. Saudijska Arabija, odnosno Kraljevina Saudijska Arabija, čini središte islamske religije s gradovima Mekkom i Medinom, koji su centar muslimanskih hodočašća i dva najsvetija islamska grada. Važnost Saudijske Arabije za islamsku religiju je jednaka važnosti Vatikana za katolike, što stvara veliki pritisak za vladajuće i ne ostavlja prostor za greške u interpretiranju religijskih pravila (Fatani, 2011: 2). Sva religijska pravila kojima se muslimani vode u životu dolaze iz njihove svete knjige, Kurana, a poznatija su pod imenom Šerijatski zakon. Kako Shishkina i Issaev (2018: 3) objašnjavaju, problem koji se javlja u interpretaciji zakona je taj da se može shvatiti na više načina (kao što je slučaj, na primjer, kod zakona izražavanja osobnog mišljenja) što znači da zakonodavci stvar uzimaju u svoje ruke i primjenjuju zakon prema svom subjektivnom stajalištu, odnosno prema stajalištu vladajućih. Tako vladajući smatraju da se bilo kakav sadržaj koji predstavlja opasnost njihovoj kulturi, sigurnosti ili religiji mora filtrirati, a građanima zabraniti pristup istom.

Godine 1999., građani Saudijske Arabije su dobili pristup internetu. No, prije otvaranja interneta javnosti, vlasti Saudijske Arabije su provele dvije godine gradeći kontroliranu infrastrukturu, kako bi sav promet na internetu dolazio putem servera kontroliranih od strane vlade. Postoji cijeli odjel odnosno jedinica koja se bavi filtriranjem podataka, a nalazi se na njihovom istraživačkom institutu Grad kralja Abdulaziza za znanost i tehnologiju u Rijadu, poznatiji pod inicijalima KACST (engl. *King Abdulaziz City for Science and Technology*). KACST je odgovoran za razvoj i kordinaciju zakona i pravila korištenja interneta te upravljanje vezom globalnog i nacionalnog interneta. Uz to, njihova zadaća je sve prijaviti saudijskom kralju Abdullah Bin Abdul-Azizu i premijeru (Fatani, 2011: 1). Zanimljiva činjenica je da se samo 25 vladinih zaposlenika bavi cenzurom, što ne predstavlja veliku brojku s obzirom na obujam posla - u 2021. godini Saudijska Arabija broji preko 33 milijuna korisnika interneta, što čini skoro 96% njihove populacije, a povećanje broja korisnika je vidljivo iz Grafikona 2 (Statista Research Department, 2020).



Grafikon 2. Povećanje broja korisnika interneta od 2015. nadalje, s predviđanjima do 2025. (Statista Research Department, 2020)

Teško je dokučiti koje specifične informacije vlasti cenzuriraju, jer objašnjenja su poprilično generalna i obuvaćaju bilo kakav neprimjereni sadržaj, što u slučaju Saudijske Arabije obuhvaća pornografiju, terorizam, političku aktivnost, izražavanje suprotnog mišljenja od vladajućih, kritiziranje vladajućih i bilo kakav sadržaj koji je u suprotnosti s njihovom religijom. Kada je u pitanju politička aktivnost, u Saudijskoj Arabiji je situacija drugačija nego u Kini, jer je u Kraljevini bilo kakva politička aktivnost jasno zabranjena, a također ne postoje političke stranke ni državni izbori. Upravo zbog toga se saudijske vlasti već godinama bore s *blogerima* koji analiziraju i komentiraju društveno-političku scenu u državi, gdje su nerijetki slučajevi uhićenja blogera te gašenja i blokiranja raznih portala i foruma koje vode politički aktivisti (OpenNet Initiative, 2009). Također, vlasti su smatrale da aplikacije poput Whatsappa i Facebooka igraju ključnu ulogu u degradaciji morala građana (Rahimi i Gupta, 2020: 61), što ih je potaknulo da zabrane pristup spomenutim stranicama i aplikacijama, no u zadnjih par godina su započeli s popuštanjem mjera te se građani ipak iznova mogu služiti Whatsappom, Facebookom, Skypeom, Twitterom, Snapchatom...

Tipovi stranica kojima je također zabranjen pristup su: teološki orijentirane stranice koje kritiziraju islam ili zagovaraju religijsku toleranciju, zdravstvene stranice koje spominju spolno prenosive bolesti poput HIV-a ili spominju zdravstvene probleme tipične za žene, zabavne stranice s uvredljivim šalama ili koje nude filmove za skidanje. Posebnu pozornost posvećuju zabrani pristupa stranicama s bilo kakvim homoseksualnim sadržajem, političkim temama gdje se kritizira i analizira Saudijska Arabija, s terorističkim sadržajem, s

pornografskim sadržajem i edukacijske stranice koje pružaju mnoštvo informacija na temu feminizma i jačanja položaja žena u društvu (Fatani, 2009: 195).

Jedan od poznatijih online skandala je slučaj Hamza Kashgarija koji je uvrijedio utemeljitelja islama Muhameda putem Twitter platforme. Saudijski kolumnist i bloger Hamza Kashgari je odlučio objaviti tri Twitter statusa posvećena Proroku, u spomen na njegov rođendan koji je slavilo mnoštvo muslimana. Njegovi statusi su bili sarkastične prirode, a glavni problem je to što je Proroka prikazao kao običnog čovjeka, a tako mu se i obraćao. Njegove objave naišle su na teške osude, a na Facebooku su se formirale grupe koje su pozivale na smaknuće blogera. Nakon što se Kashgari upoznao s online reakcijama, obrisao je statuse i u roku par sati je pobjegao u Maleziju, no vlasti Saudijske Arabije su zahtjevale da ga se izruči te je bio deportiran nazad u Kraljevinu gdje i dalje služi zatvorsku kaznu (Fatani, 2011: 3-4).

Kako bi si olakšali posao, u rujnu 2010. godine Ministarstvo informacija je predložilo zakon koji bi zahtijevao da online portali, novine, blogovi, forumi i sl. prvo moraju steći dozvole kako bi vodili blogove ili pisali članke za novine. Zakon je stupio na snagu 2011. godine, a već 2012. je postalo ilegalno biti novinar na internetu bez dozvole. Neki od zahtjeva koje novinari trebaju ispuniti za stjecanje dozvole su: moraju imati više od 20 godina, saudijsko državljanstvo, završenu srednju školu i ono najzanimljivije je da ih mora krasiti „dobro i pristojno ponašanje“, što je toliko generalan zahtjev da omogućava zabranu prakticiranja novinarstva praktički bilo kome, ovisno o tome kako vladajući procjene ponašanje aplikanta (Fatani 2011: 3).

5.2. Tehnike cenzuriranja

Najbitniji način filtriranja online informacija je taj koji se provodi uz pomoć tehnologije, a ne zakona, a ni u kom slučaju se ne smije izostaviti ključan faktor koji pomaže u regulaciji: svijest samih građana.

Fatani (2009: 195) objašnjava da s ciljem lakšeg filtriranja informacija na internetu, sav globalni internetski promet se kanalira kroz posrednički poslužitelj (engl. *proxy server*) kojeg reguliraju državne službe. Saudijska vlada cenzurira internet tako što su svi zahtjevi za pristup stranicama na internetu prvo poslani prema vladinom posredničkom poslužitelju koji je posrednik između korisnika koji traži informaciju i onog koji ju pruža. Vladin poslužitelj, koji je vođen od strane jedinice za internet sustave na već spomenutom instititutu KACST, procjenjuje zahtjev na temelju svog kriterija filtriranja te odgovara na upit prema njemu. Za

razliku od Kine, davatelji internet usluge (*ISP*-ovi) ne moraju blokirati nikakve stranice, zato što to radi vladin posrednički poslužitelj, ali moraju bilježiti aktivnost korisnika u trajanju do 1 mjesec, a informacije koje čuvaju su IP adrese, korisnička imena, datumi aktivnosti, HTTP kodovi koje su korisnici koristili i URL-ovi i web adrese kojima su pristupali.

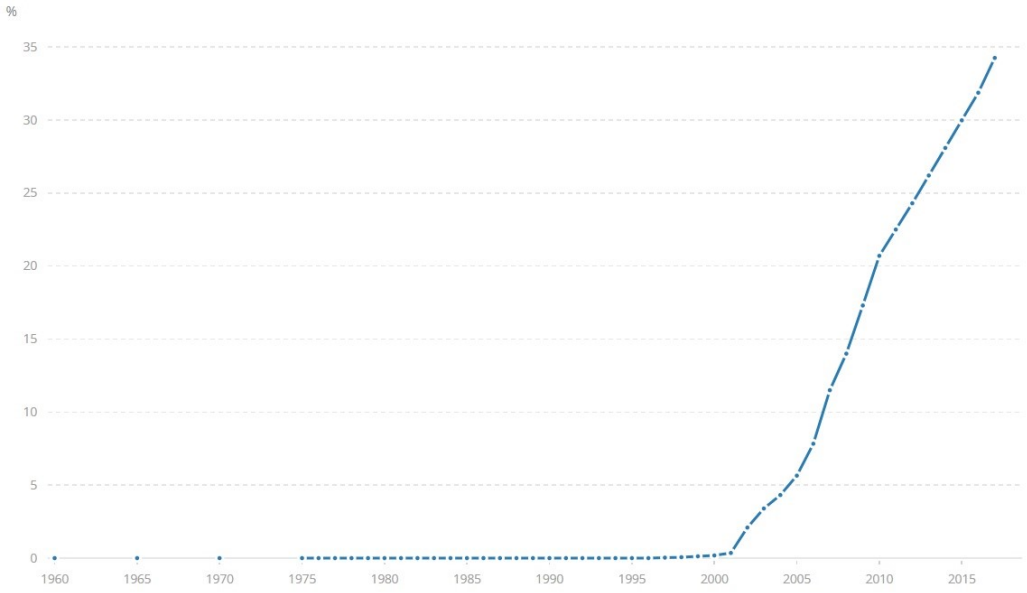
Kada korisnik pokuša pristupiti stranici koja je cenzurirana, dobiva povratnu informaciju da je ta stranica zabranjena i da joj ne može pristupiti (Abdulaziz, 2012: 145). Takav način cenzure se bitno razlikuje od onoga u Kini, jer saudijske vlasti ne skrivaju činjenicu da brane pristup određenim stranicama, čak se trude objasniti iz kojeg razloga je ona cenzurirana. No, najzanimljivija komponenta filtriranja je ostavljena za kraj, a to je svijest građana na koju se oslanjaju. Kako Abdulaziz objašnjava (2012: 145), korisnicima je dozvoljeno, štoviše potiče ih se, da prijave stranice koje žele da se cenzuriraju jer ih smatraju nemoralnima ili su u suprotnosti s njihovim uvjerenjima. Tako korisnici mogu slati zahtjeve za blokiranje različitih stranica, ali također mogu tražiti da se blokiranje poništi, u slučaju ako su prijavili krivu stranicu. Nakon toga vladini službenici pregledavaju zahtjeve i odgovaraju na njih u skladu s pravilima koja su im propisana. Saudijska Arabija je na takav način mudro uključila građane u filtriranje interneta, dajući im prividan osjećaj moći koji ih potiče na preuzimanje incijative u svoje ruke.

6. Cenzura interneta u Siriji

6.1. Motivi cenzure, vrste problematičnog sadržaja i posljedice po korisnike takvog sadržaja

Cenzura interneta u Siriji je također ekstenzivna, smatra se jednom od najekstenzivnijih u svijetu, a razlozi su primarno politički i usko su povezani s ratnim stanjem i ciljevima očuvanja mira ili s druge strane nemira. Reguliranje korištenja interneta se i dalje koristi kao vrsta oružja u ratu i nestabilnosti koji vladaju Sirijom već godinama. U proljeće 2011. godine, pod valom prosvjeda koji su zahvatili arapske države tzv. Arapsko proljeće, započeo je građanski rat u Siriji s predsjednikom Bašar al-Asadom i njegovom vladom na jednoj strani i pobunjenicima protiv njegove vladavine na drugoj. Moglo bi se reći da je građanski rat u Siriji medijski najpopraćeniji rat u povijesti čovječanstva kada to gledamo iz perspektive zapadnjaka, no objavljivanje ili pristup informacijama na području Sirije je predstavljalo iznimnu opasnost i izazov mnogim novinarima, blogerima i aktivistima na tom području.

Prevladavajući problem u Siriji tijekom svih ratnih godina je kako se spojiti na mrežu. Zbog razaranja, bombardiranja i oružanih sukoba koji su uslijedili 2011. godine i nakon, infrastruktura u mnogim gradovima i mjestima je pretrpjela neizmjernu štetu (Freedom House, 2019b). Više od polovice stanovnika zemlje se ne može spojiti na mreže sirijskih davatelja internetskih usluga i zato su se okrenuli prema WiMax mrežama (bežičnoj tehnologiji koja omogućava širokopojasni bežični pristup internetu uz upotrebu radio frekvencijskog spektra od 3,5 GHz i 26 GHz (Androić, 2007), internetskim kablovima ili turskim wi-fi operaterima koji pružaju uslugu interneta lokalnim distributerima, a onda oni pružaju iste usluge stanovnicima Sirije. Korisnici na sjeveru Sirije se oslanjaju na turske mreže kako bi se spojili na internet, no u središnjoj i južnoj Siriji, vladine mreže su glavni izvori za pristup internetu. Na područjima koja su pod vladinom kontrolom, Sirijski telekom (engl. *Syrian Telecommunications Establishment* - *STE*) je glavni internetski poslužitelj i nadzornik telekomunikacija te na taj način omogućava vladinu strogu kontrolu nad mrežom i online aktivnostima (Freedom House, 2019b). Bez obzira na sve neprilike na tom području, Sirija danas broji preko 8 milijuna korisnika, što čini više od 35% njezinih stanovnika, a Grafikon 3 (The World Bank, n. d.) prikazuje kako je raslo povećanje broja internet korisnika od 1960. pa do 2017. godine.



Grafikon 3. Povećanje broja internet korisnika od 1960. do 2017.
(The World Bank, n. d.)

Kako Freedom House (2019a) objašnjava, sirijski zakoni dozvoljavaju osnivanje privatnih tvrtki za pružanje internetskih usluga, no kako bi uopće došlo do osnivanja tvrtke potrebno je pribaviti dozvolu od strane sigurnosnih službi. Proces pribavljanja dozvole obuhvaća analizu aplikanta: istražuje se njegovo političko stajalište, prošlost, njegovi rođaci, prijatelji i suradnici, a tek nakon provođenja tih radnji se razmatra može li osoba dobiti dozvolu. Bilo tko tko je povezan s protivnicima vladinog režima je, naravno, odbijen. U Siriji trenutno postoji 27 licenciranih davatelja internetskih usluga, no otvaranje novih mreža je izazov s obzirom na nestabilnost u državi i oštećenost bitne infrastrukture.

Kada način spajanja na internet postoji, vlasti su se odlučile na provođenje cenzure na razne načine, od blokiranja raznih mrežnih stranica ili društvenih mreža pa do isključivanja interneta i onemogućavanja bilo kakvog umrežavanja u periodu od nekoliko sati. Vjeruje se da vlada filtrira SMS poruke od 2011. godine, a glavni fokus je na saznavanju datuma planiranih protesta te onda pokušaju sprječavanja širenja potrebnih informacija. Navodno su sirijski telekomunikacijski operateri neko vrijeme morali blokirati SMS poruke koje sadrže riječi poput „revolucija“ ili „demonstracije“. Što se tiče kontrole interneta, većina cenzuriranih stranica su opozicijske stranice, stranice koje zagovaraju ljudska prava, a sadržaj koji je posebno opasan je bilo kakva politička, društvena, kulturalna ili ekonomska kritika vladinog režima, otkrivanje korupcije u državi, komentiranje osjetljivih tema koje uključuju

predsjednika al-Assada, njegovog preminulog oca, vojsku ili poznate državne dužnosnike (Freedom House, 2019b).

Mrežne stranice koje su bile blokirane su novine Enab Baladi i radio SouriaLi koji su pružali nepristrane informacije građanima. Također su bile blokirane kuvajtske novine Al-Seyassah, regionalni mediji poput Al-Jazeere, a i nepolitičke stranice kao što su Wikipedija i Wordpress blogerska domena. Ono što je zanimljivo je da su sve te stranice postale dostupne kroz 2017. i 2018. godinu bez ikakvog objašnjenja.

Vladajući imaju razne načine postupanja prema građanima koji pristupaju blokiranim stranicama, objavljuju nepoželjan sadržaj ili na bilo koji način izražavaju svoje nedozvoljeno mišljenje. Tako je u srpnju 2018. novinar iz Damaska morao obrisati objavu na Facebooku gdje je opisao uvjete življenja u državi jer su ga sigurnosne službe obavijestile kako ne smije pričati o takvim stvarima (Freedom House, 2019b). Kako su objavili Reporteri bez granica (2019), u prosincu 2018. godine policija je uhitila Wissaam Al-Taira, urednika Damascus Now novina, zato što se počeo interesirati oko korupcije u državi. Pušten je nakon osam mjeseci bez ikakvog objašnjenja i opravdanja za zadržavanje. Ovaj slučaj se može smatrati najblažom povredom ljudskih prava, s obzirom na brojne slučajeve novinara i blogera koji su bili uhićeni i mučeni, a neki na kraju i ubijeni. Tako je bloger Jehad Jamal završio u pritvoru 2012. godine, četiri godine nakon su ga ubili u Saydnaya vojnom zatvoru (kojeg nazivaju klaonicom), a njegova žena je dobila potvrdu o muževoj smrti tek 2020. godine (Reporters Without Borders, 2019).

Problematični nestanci i uhićenja građana su postojala i prije građanskog rata - u lipnju 2007. godine vojska je uhitila Karima Arbajija jer je bio jedan od aktivista na poznatom sirijskom forumu koji se bavio društvenim i političkim problemima (Human Rights Watch, 2007). Također, u istom mjesecu su uhitili Tareka Biasija koji se usudio uvrijediti sirijske sigurnosne službe na internetu, a u rujnu iste godine Ali Zein al-'Abideen Mej'an je osuđen na dvije godine zatvora zato što mu ponašanje nije bilo u skladu s dozvoljenim te je ugrozio međunarodne odnose objavivši komentare kojima je osuđivao Saudijsku Arabiju (Human Rights Watch, 2007). Najveći problem svih uhićenja je što vlasti ne žele dati informacije gdje se zadržane osobe nalaze, čak ni obiteljima uhićenih.

6.2. Tehnike cenzuriranja

Kako objašnjavaju Chaabane et al. (2014: 1) sirijska vlada ima različite tehnike cenzuriranja: blokiranje mrežnih stranica na temelju IP adrese, blokiranje pristupa cijelim podmrežama, blokiranje pristupa izraelskim domenama (ali su 2018. godine vratili pristup, iz nepoznatih razloga), filtriranje prema ključnim riječima i prema kategoriji sadržaja. Jedna (od mnogih) mana cenzuriranja sadržaja prema ključnim riječima je ta da puno 'nevinog' sadržaja završi blokirano jer sustav za cenzuriranje ne može procijeniti kontekst i da neka riječ nije korištena u opasne svrhe.

Zahtjevi koje korisnici podnesu kada žele pristupiti nekoj stranici se cenzuriraju na dva načina: odbijeni su (engl. *policy__denied*) i korisnik jednostavno ne može pristupiti mrežnoj stranici ili preusmjeravaju (engl. *policy_redirected*) korisnika na drugi URL (Cheebane et al., 2014: 8). Također, aplikacije putem kojih osobe komuniciraju, poput Skypea, su pod jakom cenzurom, dok je filtriranje na društvenim mrežama rezervirano za posebne stranice i korisničke račune. No, glavni cilj sirijskih vlasti je targetirati aplikacije koje pružaju usluge slanja trenutačnih poruka (engl. *Instant Messaging*[6]) jer se preko njih najviše šire informacije koje pozivaju na otpor vladajućima - nekada s više uspjeha, a nekada s manje (Cheebane et al., 2014: 1).

[6] Slanje istovremenih poruka (engl. Instant Messaging), oblik komunikacije u realnom vremenu, između dvoje ili više ljudi, koja se bazira na napisanom tekstu, govoru ili sl. Popularne platforme za slanje istovremenih poruka su Skype, Whatsapp, Facebook Messenger itd. (Wikipedia, 2017)

7. Trinaest neprijatelja interneta

Reporteri bez granica (engl. *Reporters without borders,* fra. *Reporters sans frontières*) je nevladina organizacija sa sjedištem u Parizu koja zagovara i brani slobodu tiska i medija. Zagovaraju novinare, aktiviste, blogere ili obične građane koji su kažnjeni, zatvoreni ili su se prema njima poduzimale druge represivne mjere radi njihovog angažmana i pisanja tekstova koji su vlastima bili nepoćudni. Svake godine objavljuju listu neprijatelja interneta te su tako 2016. godine objavili listu od 13 država koje smatraju neprijateljima kada je u pitanju sloboda govora, objavljivanje informacija ili bilo kakvo novinarsko ili istraživačko djelovanje. Od tih 13 zemalja, na listi se nalaze već spomenute Kina, Saudijska Arabija i Sirija, a uz njih su: Bjelorusija, Mjanmar (Burma), Kuba, Egipat, Iran, Sjeverna Koreja, Tunis, Turkmenistan, Uzbekistan i Vijetnam (Reporters Without Borders, 2016).

Bjelorusija je posebno poznata po blokiranju mrežnih stranica koje iznose stajališta dijametralno suprotna predsjedniku Alexandru Lukashenku u svrhu izražavanja kritičkog mišljenja, a posebice ako su te mrežne stranice pod domenama drugih država (Freedom House, 2019a). Za vrijeme izbora cenzura postaje najekstenzivnija, te su tako prije i nakon izbora 2020. godine blokirali preko 70 mrežnih stranica koje su ukazivale na ishod predsjedničkih izbora za koji građani vjeruju da je namješten (Xynou i Filasto, 2020).

Mjanmar cenzurira sva oporbena djelovanja protiv vojne hunte (Reporters Without Borders, 2016). Takvo stanje je bilo karakteristično za prvo desetljeće 21. stoljeća, a ponovno se nastavlja krajem drugog desetljća, s kratkim razdobljem demokracija i slobode koje je uslijedilo nakon izbora 2010. godine, kada su demokratske snage došle na vlast. Najnoviji incidenti cenzuriranja interneta su se dogodili u veljači 2021. godine kada je vojska ponovno izvršila puč, svrgnula demokratski izabranu vlast iz 2020. godine i nasilno gušila prodemokratske proteste - uz gašenja interneta koja su trajala više od dva tjedna, a stranice poput Facebooka, Twittera i Instagrama su bile blokirane kako građani ne bi mogli dogovarati proteste i razmjenjivati informacije (Sasipornkarn, 2021).

Kuba je država u kojoj manje od 2% stanovništva ima pristup internetu, a oni koji imaju mogu mu pristupiti samo u kafićima koji pružaju internet uslugu ili na sveučilištima, no i na tim mjestima su njihove aktivnosti strogo kontrolirane i limitirane. Mediji su kontrolirani od strane kubanske komunističke partije koja potencira prodržavnu propagandu, dok su privatni mediji zabranjeni. Kao i u većini spomenutih država, blokirane su sve mrežne stranice koje kritiziraju političko stanje u državi ili promoviraju ljudska prava i slobodu

govora. Za one koji pokušavaju pristupiti zabranjenim mrežnim stranicama, ilegalno se spajaju na internet ili u najgorem slučaju, pišu proturevolucijske članke (za strane mrežne stranice), predviđene su zatvorske kazne od 5 do 20 godina (Reporters Without Borders, 2016).

Mrežne stranice koje Egipat blokira smatraju se opasnim za nacionalnu sigurnost ili ekonomiju države, a građani koji pristupaju istima su strogo kažnjavani (Reporters Without Borders, 2016). Smatra se da su vlasti blokirale više od 600 mrežnih stranica i to samo od svibnja 2017. godine, a sve su ili povezane s medijskim portalima, političkim platformama ili platformama koje se zalažu za ljudska prava (EuroMed Rights, 2020). U skladu s takvim postupanjima, 2018. godine Egipat je donio zakon kojim je odobreno i olakšano blokiranje mrežnih stranica, bez obzira na dosadašnje već potpisane međunarodne sporazume kojima se obvezuju na uvažavanje ljudskih prava. Uz to, Egipat je 2015. godine bio proglašen drugom državom na svijetu po broju zatvorenih novinara.

U usporedbi s Iranom, Egipćani izgledaju kao početnici u cenzuriranju interneta. Tako se Iran može pohvaliti s preko 10 milijuna filtriranih „nemoralnih“ mrežnih stranica, a to su većinom stranice s pornografskim sadržajem, političke ili religijske stranice. Također, targetirane su i stranice koje se zalažu za prava žena, što je česta praksa u arapskim državama. Iran je već blokirao društvene mreže i alate uključujući Twitter, Facebook i Telegram - poznatu aplikaciju za razmjenjivanje poruka, no u zadnjih par godina intencija je na još jačem ograničavanju kao i da iranska vojska preuzme kontrolu nad internetom (Reporters Without Borders, 2016).

Sjeverna Koreja je prozvana crnom rupom interneta, s obzirom na to da globalnom internetu mogu pristupiti samo najviši državni službenici. Na nekim sveučilištima, studenti i zaposlenici imaju limitirani pristup internetu, a podrazumijeva se da je sva aktivnost kontrolirana i da je većina stranica blokirana. Za ostatak populacije, online aktivnost je dostupna samo putem Kwangmyonga, besplatnog javnog intraneta s limitiranim brojem stranica i usluga koje nudi, a koje su većinom povezane s nacionalnom politikom, ekonomijom, kulturom i znanošću (Reporters Without Borders, 2016).

Tunis je država koju je karakterizirala najrepresivnija kontrola interneta u svijetu. Stanje je bilo najlošije pod predsjednikom Zine El Abidine Ben Alijem koji je vladao od 1987. pa sve do 2011., no od tad se stanje znatno poboljšalo, tako da je pristup Facebooku, YouTubeu i sličnim stranicama dozvoljen, makar je zabilježeno da su 2011. godine blokirali nekoliko Facebook profila koji su imali namjeru „...uništiti reputaciju vojne institucije i

njenih vladara," (Wikipedia, 2021, a). Neovisno o poboljšanju situacije, svi kafići koji nude usluge interneta su i dalje kontrolirani od strane države, a sadržaj na webu nadzire policija (Reporters Without Borders, 2016) uz cenzuriranje bilo kakvih pornografskih sadržaja, što je također česta praksa arapskih država.

U Turkmenistanu internet nije samo cenzuriran, nego je i zabranjen za većinu stanovnika države. Turkmenistan je država koja ima manji postotak online građana čak i od Kube, brojeći samo 1 % stanovništva koje ima pristup internetu (Reporters Without Borders, 2016). Vladajući kontroliraju sve državne medije i koriste ih za promoviranje propagandnog sadržaja (IPHR, 2020). Građani koji uspiju pristupiti internetu se suočavaju sa sporim internetom i jako lošom kvalitetom mreže, a društvene mreže i aplikacije za komunikaciju su blokirane.

U Uzbekistanu samostalni privatni mediji ne postoje, a autocenzura prevladava na blogovima ili forumima zbog straha od posljedica ako se objavi nešto što vladajući ne odobravaju. Tabu teme su: primjena metoda mučenja od strane sigurnosnih službi, masakr u Andijanu iz 2005. godine ili iskorištavanje milijuna djece koja svake godine pod prisilom skupljaju pamuk (Stroehlein, 2008). Za one koji se usude izvještavati o tim temama slijedi zatvorska kazna, a vjerojatnost mučenja ili u konačnici smrtnog ishoda je velika. Vladajući koriste sve snage da zabrane slobodu govora online te također blokiraju ogroman broj mrežnih stranica.

Po načinu i ciljevima cenzuriranja, Vijetnam jako podsjeća na Kinu. Svi poslužitelji internet usluga se mogu spojiti samo na mrežne točke koje kontrolira vlada, što im jako olakšava filtriranje informacija. U 2018. godini je donesen zakon koji omogućava vladi da neometano kontrolira, briše i blokira podatke koje smatraju opasnošću za nacionalnu sigurnost, društveni mir i poredak (Reporters Without Borders, 2016). Takvi generalni opisi ostavljaju prostor za široki obuhvat sadržaja cenzure, ovisno o tome kako vladajući žele protumačiti neki sadržaj. Ono na što se najviše fokusiraju je sadržaj protiv vladajućih struktura i kritike istih.

8. Zaobilaženje cenzure

Koliko god se vlasti različitih država trudile da njihovi stanovnici ne osjete odnosno ne percipiraju cenzuru kao problematičnu, i dalje postoji mnoštvo pojedinaca koji su svjesni cenzure te ju pokušavaju zaobići i pristupiti željenom sadržaju. Zahvaljujući brojnim znalcima, hakerima i ekspertima na području računalne tehnologije, razvijeno je mnoštvo alata i softvera koji služe za zaobilaženja cenzure . U ovom radu ću predstaviti dva najčešće korištena alata: FreeGate aplikaciju koja funkcionira preko posredničkog poslužitelja i drugu opciju - virtualne privatne mreže.

FreeGate je najpopularniji alat za zaobilaženje cenzure u Kini, Siriji, Iranu, Vijetnamu, Ujedinjenim Arapskim Emiratima i ostalim državama poznatima po filtriranju (Zhao et al., 2013: 13). Freegate sustav je kreirala privatna firma Dynamic Internet Technologies (DIT), koja je sama nastala 2001. godine s ciljem sigurnog slanja elektronske pošte iz Kine i u Kinu, a sve to koristeći posredničku mrežu (engl. *proxy network*) nazvanu „Dynaweb“ (Bernard, n. d.). S vremenom je Dynaweb postao alat za zaobilazak cenzure u punom smislu. U početku je proces funkcionirao tako da bilo koji korisnik može pristupiti Dynawebu ako URL svog preglednika usmjeri na jedan od DIT-ovih posredničkih poslužitelja. Kada se spoje na posrednički poslužitelj, mreža se koristi raznim šifriranjima i uz pomoć alata za zaobilaženje omogućavaju da korisnici neopaženo surfaju internetom. No, države poput Kine nisu bile naivne te su blokirali DIT-ove poslužitelje nakon pomnog promatranja, što je potaknulo Dynaweb da evoluiraju u mrežu s mnoštvom zrcalnih mrežnih stranica (engl. *mirror site* - replika drugih mrežnih stranica koje imaju različite URL-ove od izvorne mrežne lokacije, ali imaju gotovo identičan sadržaj) i kreiraju Freegate. Freegate je jednostavna aplikacija koju korisnici mogu preuzeti na svoje mobilne uređaje ili računala, a cilj je omogućiti korisnicima da brzo i jednostavno pristupe Dynawebu bez obzira na blokirane servere. Jedina mana je ta što teško može u potpunosti sakriti identitet nekog korisnika te zato posjetitelji Dynaweba trebaju biti svjesni rizika ako se koriste aplikacijom (Bernard, n. d.).

Nakon FreeGatea koji se služi spajanjem na različite posredničke poslužitelje, drugi najpoznatiji način zaobilaženja cenzure je spajanjem na virtualnu privatnu mrežu (engl. *virtual private network - VPN*). Osnovni cilj VPN-a je omogućiti firmama koje imaju podružnice na različitim lokacijama (ili u današnjem slučaju, kada zaposlenici rade od kuće) spajanje na svoju internu mrežu (intranet) kroz šifrirane tunele na internetu. To je tehnolgija koja omogućava sigurno povezivanje privatnih mreža u jednu zajedničku virtualnu privatnu

mrežu kroz internet, čime se ostvaruje siguran "tunel" između dvije krajnje točke (Mujarić, n. d.). No, VPN-ovi također mogu biti korišteni kako bi se nečije osobno računalo u državi s cenzurom spojilo na server u "slobodnom internetu", koristeći se istim principom. Mana korištenja VPN-a je ta da su dosta spori i nestabilni. Ako se koriste besplatni VPN-ovi onda će veza puknuti svakih 15-ak minuta, a većina njih se mora plaćati (Zhao et al., 2013: 12).

Kao što je pokazalo istraživanje provedeno od Zhao et al. (2013: 11-13), 50 % ispitanika (većinom studenata) smatraju da su stabilnost veze i brzina osnovna mjerila prema kojima će odabrati alat za zaobilaženje cenzure, a nakon toga uzimaju u obzir cijenu i lakoću pristupa. Primarni razlozi zaobilaženja cenzure su, naravno, pristup informacijama i izvorima koji su im zabranjeni na tražilicima poput Googlea ili na Wikipediji, a u tom slučaju postoji velika znatiželja i doza uzbuđenja u otkrivanju što se skriva s „druge strane interneta“. U slučajevima studenata koji su studirali u inozemstvu, motivacija proizlazi iz želje da ostanu u kontaktu s kolegama koje su upoznali pa se koriste raznim softverima za pristup Facebooku ili Twitteru.

9. Zaključak

Internet je postao središnji medij 21. stoljeća, brojeći milijarde korisnika iz svih dijelova svijeta. Upravo taj faktor - nevjerojatna poveznost stotina milijuna ljudi iz različitih krajeva, s različitim uvjerenjima, stavovima i iskustvima je doprinio u stvaranju tako inkluzivne i dinamične globalne mreže koja ne poznaje granice među državama. S vremenom, kako su potencijali interneta postajali sve očitiji i opipljiviji, vlasti određenih država su prepoznale opasnosti koje nose njegove glavne karakteristike. Od nekontroliranog dijeljenja informacija od bilo koga na bilo kojoj dostupnoj platformi, pa sve do ilegalnog preuzimanja filmova, pjesama, serija i slično.

Tako su države poput Kine, Saudijske Arabije, Irana, Sirije, Vijetnama, Kube i mnogih drugih počele posezati za, iz perspektive zapadnjaka, ekstremnim mjerama. Internet je prestao biti slobodan i otvoren prostor namijenjen za dijeljenje sadržaja i komuniciranje. Oni su ga sveli na njegov najogoljeniji oblik bez šarenila i raznovrsnosti koji čine internet onime što je. Snažna kontrola i zabrana pristupa određenim mrežnim stranicama su samo jedni od poteza tih država - uz to dolaze mnogobrojne kazne, uhićenja, mučenja daleko od očiju javnosti i u najgorim slučajevima - ubojstva. Tehnike kojima se služe za cenzuru su većinom blokiranje IP adresa, tuneliranje svog internet prometa kroz jedan jedini vladin poslužitelj ili filtriranje po ključnim riječima. Jako puno novaca je uloženo u razvijanje alata i softvera za detaljno cenzuriranje podataka, ali i za plaćanje samih radnika i operativaca koji stoje iza toga. Također, u nekim slučajevima trud je uložen i u prikrivanje činjenice da se cenzura uopće provodi, dok neke države to jasno daju do znanja svojim građanima i dapače, potiču građane da sami sudjeluju u procesu filtriranja informacija.

Bez obzira na to jesu li građani za ili protiv cenzure, uvijek postoji određena doza znatiželje i nemira koji vlada u ljudima kada znaju da se nešto aktivno skriva od njih. Tako se mnogo korisnika interneta u Kini, Iranu, Egiptu i mnogim drugim državama okreću alatima i softverima za zaobilaženje cenzure kako bi napokon pristupili željenim mrežnim stranicama. Jednom zapadnjaku je teško zamisliti i shvatiti sve ovo s obzirom na sustave vrijednosti kultura u kojima odrastamo. Koliko god pokušali razumjeti motive nekih država i čak ih opravdati, zaključak je većinom isti: cilj ne opravdava sredstvo, a u ovom slučaju, ni ciljevi nisu opravdani.

10. Literatura

1. Abdulaziz, A. (2012) Saudi Arabia Censorship: A Model for Workplace Productivity. *International Journal of Business, Humanitis and Technology*, 2(1), 1-6. URL: http://ijbhtnet.com/journals/Vol_2_No_1_January_2012/17.pdf [pristup: 26. 4. 2021.]

2. Androić, D. (2007) *WiMax tehnologija*. URL: http://www.phy.pmf.unizg.hr/~dandroic/nastava/mr/wimax_tehnologija.pdf [pristup: 2. 5. 2021.]

3. Bernard, D. (n. d.) *An Internet Primer for Healthy Web Habits: Freegate Opens a Door to Asia*. URL: https://projects.voanews.com/circumvention/freegate [pristup: 10. 5. 2021.]

4. Brown, I. (2008) Internet Censorship: Be Careful What You Ask for. U: Kirca, S. i Hanson, L. (ur.), *Freedom and Prejudice: Approaches to Media and Culture*. Istanbul: Bahcesehir University Press, str. 74-91. URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1026597 [pristup: 27. 4. 2021.]

5. Chaabane, A., Chen, T., Cunche, M., De Cristofaro, E., Friedman, A., Kaafar, M. A. (2014) Censorship in the Wild: Analyzing Internet Filtering in Syria. *Proceedings of the 2014 Conference on Internet Measurement, Vancouver*. URL: https://arxiv.org/pdf/1402.3401.pdf [pristup: 5. 5. 2021.]

6. Columbia Public Health (n. d.) *Content Analysis*. URL: https://www.publichealth.columbia.edu/research/population-health-methods/content-analysis [pristup: 24. 5. 2021.]

7. EuroMed Rights (2020) *NGOs Call on Egypt's Government to End Internet Censorship and Website Blocking*. URL: https://euromedrights.org/publication/ngos-call-on-egypts-government-to-end-internet-censorship-and-website-blocking/ [pristup: 5. 5. 2021.]

8. Fatani, R. (2009) Saudi Arabia: Saudi Arabian Strategic Internet Consulting (SASIc). U: Finlay, A. (ur.), *Global Information Society Watch 2009: Focus on Access to Online Information and Knowledge – Advancing Human Rights and Democracy* [e-book]. [S. l.]: Association for Progressive Communications : Hivos, str. 194-196. URL: https://giswatch.org/sites/default/files/saudiarabia.pdf [pristup: 26. 4. 2021.]

9. Fatani, R. A. Y. (2011) Securing Internet Rights in Saudi Arabia. U: Finlay, A. (ur.), *Global Information Society Watch 2011 Update: Internet Rights and Democratisation* [e-

book]. [S. l.]: Association for Progressive Communications : Hivos, str. 52-60. URL: https://www.giswatch.org/sites/default/files/gisw11_up_web_0.pdf [pristup 7. 6. 2021.]

10. Freedom House (2019a) *Belarus Freedom on the Net 2019*. URL: https://freedomhouse.org/country/belarus/freedom-net/2019 [pristup: 5. 5. 2021.]

11. Freedom House (2019b) *Syria: Freedom on the Net.* URL: https://freedomhouse.org/country/syria/freedom-net/2019 [pristup: 1. 5. 2021.]

12. Fu, K. W., Chan, C. H., Chau, M. (2013) Assessing Censorship on Microblogs in China: Discriminatory Keyword Analysis and Impact Evaluation of the 'Real Name Registration' Policy. *IEEE Internet Computing*. 17(3), 42-50. URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2265271 [pristup: 20. 4. 2021.]

13. Hebrang Grgić, I. (2008) *Cenzura: neizostavan čimbenik razvoja ljudske misli i društva* [e-book]. Zagreb: Filozofski fakultet, Zavod za informacijske studije Odsjeka za informacijske znanosti. URL: http://darhiv.ffzg.unizg.hr/id/eprint/9737/1/CenzuraIHG.pdf [pristup: 29. 4. 2021.]

14. Hrvatska enciklopedija, mrežno izdanje (n. d.) *Davatelj internetskih usluga*. Leksikografski zavod Miroslav Krleža. URL: https://www.enciklopedija.hr/natuknica.aspx?ID=68638 [pristup: 24. 5. 2021.]

15. Human Rights Watch (2007) *Syria: Stop Arrests for Online Comments*. URL: https://www.hrw.org/news/2007/10/07/syria-stop-arrests-online-comments [pristup: 2. 5. 2021.]

16. International Partnership for Human Rights (IPHR) (2020) *Increased Internet Censorship: Mass Mobilisation for Regime-Praising Events Continues*. URL: https://www.iphronline.org/increased-internet-censorship-mass-mobilisation-for-regime-praising-events-continues.html [pristup: 8. 5. 2021.]

17. Lee, J. A., Liu, C. Y. (2012) Forbidden City Enclosed by the Great Firewall: The Law and Power of Internet Filtering in China. *Minnesota Journal of Law, Science, and Technology*. 13(1), 125-151. URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2035788 [pristup: 20. 4. 2021.]

18. Leiner, M. B., Cerf, V. G., Clark, D. D., Kahn, R. E., Kleinrock, L., Lynch, D. C., Postel, J., Roberts, L. G., Wolff, S. (2009) A Brief History of the Internet. *Computer Communication Review,* 39(5), 22-31. URL:

https://sites.cs.ucsb.edu/~almeroth/classes/F10.176A/papers/internet-history-09.pdf [pristup: 26. 4. 2021.]

19. Mueller, M. L. (2011) China and Global Internet Governance: A Tiger by the Tail. U: Deibert, R., Palfrey, J., Rohozinski R. i Zittrain J. (ur.), *Access Contested: Security, Identity, and Resistance in Asian Cyberspace,* [e-book] Cambridge: MIT Press Scholarship Online, str. 177-192. URL: http://access.opennet.net/wp-content/uploads/2011/12/accesscontested-chapter-09.pdf [pristup: 1. 5. 2021.]

20. Mujarić, E. (n. d.) *Virtualna privatna mreža (VPN)*. URL: http://mreze.layer-x.com/s060000-0.html [pristup: 10. 5. 2021.]

21. Online Library Learning Center (n. d.) *A Brief History of the Internet: Sharing Resources*. URL: https://www.usg.edu/galileo/skills/unit07/internet07_02.phtml [pristup: 29. 4. 2021.]

22. OpenNet Initiative (2009) *Internet Filtering in Saudi Arabia*. URL: https://opennet.net/sites/opennet.net/files/ONI_SaudiArabia_2009.pdf [pristup: 23. 4. 2021.]

23. Rahimi, N., Gupta, B. (2020) A Study of the Landscape of Internet Censorship and Anti-Censorship in Middle East. *EpiC Series in Computing*, 69, 60-68. URL: https://easychair.org/publications/open/6hvn [pristup: 28. 4. 2021.]

24. Reporters Without Borders (RSF) (2016) *List of the 13 Internet Enemies.* URL: https://rsf.org/en/news/list-13-internet-enemies [pristup: 5. 5. 2021.]

25. Reporters Without Borders (2019) *List of Issues for the Consideration of Syria's Periodic Report Under the International Covenant on Civil and Political Rights*. URL: https://tbinternet.ohchr.org/Treaties/CCPR/Shared%20Documents/SYR/INT_CCPR_ICS_SYR_42945_E.pdf [pristup: 2. 5. 2021.]

26. Sasipornkarn, E. (2021) *Myanmar Coup: Military Hardens Online Censorship Campaign*. Deutsche Welle. URL: https://www.dw.com/en/myanmar-coup-military-hardens-online-censorship-campaign/a-56574941 [pristup: 5. 5. 2021.]

27. Shishkina, A., Issaev, L. (2018) Internet Censorship in Arab Countries: Religious and Moral Aspects. *Religions*, 9(11), 1-14. URL: https://www.mdpi.com/2077-1444/9/11/358 [pristup: 25. 4. 2021.]

28. Statista Research Department (2020). *Saudi Arabia: Number of Internet Users 2015-2025*. URL: https://www.statista.com/statistics/462959/internet-users-saudi-arabia/ [pristup: 27. 4. 2021.]

29. Stipčević, A. (1992) *Cenzura u knjižnicama*. Zagreb: Filozofski fakultet, Zavod za informacijske studije Odsjeka za informacijske znanosti.

30. Stipčević, A. (1994) *O savršenom cenzoru.* Zagreb: Nakladni zavod Matice hrvatske.

31. Stipčević, A. (2000) *Sudbina knjige.* Lokve: Naklada Benja.

32. Stroehlein, A. (2008). *Internet Censorship*. URL: https://www.crisisgroup.org/europe-central-asia/central-asia/uzbekistan/internet-censorship-uzbekistan [pristup: 8. 5. 2021.]

33. Sveznadar (n. d.) *Mrežni pojmovnik: Backbone*. URL: http://www.sveznadar.info/20-WINTipsTricks/11-MrezaRazniPojmovi/03-1Pojmovnik-bacbone.html [pristup: 20. 4. 2021.]

34. Šegrc, M. (2020) *Mrežna okosnica*. URL: http://xn--matija-egrc-mhc.from.hr/2020/12/15/mrezna-okosnica/ [pristup: 20. 4. 2021.]

35. The World Bank (n. d.) URL: https://data.worldbank.org/indicator/IT.NET.USER.ZS?locations=SY [pristup: 25. 4. 2021.]

36. Thomala, L. L. (2021) *Number of internet users in China 2008-2020*. URL: https://www.statista.com/statistics/265140/number-of-internet-users-in-china/ [pristup: 25. 4. 2021.]

37. Tiananmen Square Protests (2019). URL: https://www.history.com/topics/china/tiananmen-square [pristup: 23. 4. 2021.]

38. Wikipedia (2021a) *Censorship in Tunisia.* URL: https://en.wikipedia.org/wiki/Censorship_in_Tunisia [pristup: 5. 5. 2021.]

39. Wikipedia (2021b) *LAN*. URL: https://hr.wikipedia.org/wiki/LAN [pristup: 24. 5. 2021.]

40. Wikipedia (2019) *Proxy*. URL: https://hr.wikipedia.org/wiki/Proxy [pristup: 24. 5. 2021.]

41. Wikipedia (2014) *WAN*. URL: https://hr.wikipedia.org/wiki/WAN [pristup: 24. 5. 2021.]

42. Wikipedija (2017) *Slanje trenutačnih poruka*. URL: https://hr.wikipedia.org/wiki/Slanje_trenuta%C4%8Dnih_poruka [pristup: 24. 5. 2021.]

43. Xynou, M., Filasto, A. (2020) *Belarus Protests: From Internet Outages to Pervasive Website Censorship*. URL: https://ooni.org/post/2020-belarus-internet-outages-website-censorship/ [pristup: 4. 5. 2021.]

44. Zhao, S., Dang, H., Gu, Y., Kang, L. (2013) Circumventing the Great Firewall: The Accommodation and Defiance of Internet Censorship among Chinese Students. *SSRN.* URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2258659 [pristup: 4. 5. 2021.]

Cenzura interneta kao kontrolni mehanizam modernog doba

Sažetak

Cenzura je praksa koja se pojavila s početkom pisma, a njezina popularnost je prisutna još i danas u 21. stoljeću. S obzirom na to da je internet postao predominantni medij, posebice među mlađim generacijama, većina ljudi se oslanja na internet tražilice, blogove, forume i portale kada se žele informirati o nekoj temi. Takav dinamičan i nereguliran izvor informacija predstavlja opasnost državama koje se aktivno trude oblikovati svijest svojih građana. Najistaknutije među njima su Kina, Saudijska Arabija, Sirija, Iran, Egipat, Kuba i mnoge druge, a cilj ovog rada je približiti čitateljima različite motive i načine kojima se spomenute države koriste kako bi filtrirali protok informacija na njihovim lokalnim mrežama. Tako iza svake cenzure stoje različiti razlozi cenzuriranja - politički, religijski, društveni ili ratni. Kako raste svijest građana o nemogućnosti pristupa određenim informacijama, proporcionalno raste i želja za zaobilaskom same cenzure, a tu dolaze u pomoć svakojaki alati i softveri razvijeni posebno u te svrhe. Naposljetku ostaje teško pitanje u kojoj mjeri je cenzura opravdana u državama bez demokratskog legitimiteta.

Ključne riječi: *cenzura, internet, motivi, informacije*

Internet censorship as a controlling mechanism of the modern era

Summary

Censorship is a practice with a long-standing tradition, having appeared alongside the invention of writing, and its popularity is still intact in the 21st century. Considering the fact that the Internet has become the predominant medium, especially among younger generations, most people rely on search engines, blogs, forums and online news websites when looking for information. Such a dynamic and unregulated source of information poses a threat to countries that actively try to shape their citizens' beliefs. The countries that undoubtedly stand out in their censorship practices are China, the Kingdom of Saudi Arabia, Syria, Iran, Egypt, Cuba and many others, making the aim of this paper to shed light on the different motives and techniques these countries use to filter the flow of information on their local networks. Thus, there are different reasons behind every act of censorship - some are political, some religious, social or even war-induced. As a consequence, the more people's awareness of censorship grows, the more they want to bypass it with the help of various online tools and software, designed specifically for those purposes. Eventually, the question that inevitably lingers is to what extent is censorship justifiable in countires without democratic legitimacy.

Key words: *censorship, the Internet, motives, information*