Centar Informacijske Sigurnosti

Cenzura na Internetu

lipanj 2011.

CC BY NC SA

CIS-DOC-2011-06-016

Upozorenje

Podaci, informacije, tvrdnje i stavovi navedeni u ovom dokumentu nastali su dobrom namjerom i dobrom voljom te profesionalnim radom CIS-ovih stručnjaka, a temelje se na njihovom znanju i petnaestak godina iskustva u radu u informacijskoj sigurnosti. Namjera je da budu točni, precizni, aktualni, potpuni i nepristrani.

Ipak, oni su dani samo kao izvor informacija i CIS ne snosi nikakvu izravnu ili posrednu odgovornost za bilo kakve posljedice nastale korištenjem podataka iz ovog dokumenta.

Ukoliko primijetite bilo kakve netočnosti, krive podatke ili pogreške u ovom dokumentu, ili imate potrebu komentirati sadržaj molimo Vas da to javite elektroničkom poštom na adresu info@CIS.hr.

O CIS-u

CIS izrađuje pregledne dokumente (eng. white paper) na teme iz područja informacijske sigurnosti koji će biti korisni zainteresiranoj javnosti, a u svrhu **podizanje njezine svijesti o informacijskoj sigurnosti** i **sposobnosti za čuvanje i zaštitu informacija i informacijskih sustava**. Pored toga, CIS razvija i održava mrežni portal www.CIS.hr kao referalnu točku za informacijsku sigurnost za cjelokupnu javnost; izrađuje obrazovne materijale namijenjene javnosti; organizira događaje za podizanje svijesti o informacijskoj sigurnosti u javnosti i pojedinim skupinama te djeluje u suradnji sa svim medijima.

CIS **okuplja mlade** zainteresirane za informacijsku sigurnost i radi na njihovom pravilnom odgoju i obrazovanju u području informacijske sigurnosti te pripremu za **profesionalno bavljenje informacijskom sigurnošću**.

Centar informacijske sigurnosti [CIS] nastao je 2010. godine na poticaj Laboratorija za sustave i signale[LSS] Zavoda za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu, a kao posljedica 15togodišnjeg rada na istraživanju, razvoju i primjeni informacijske sigurnosti. LSS je među ostalim potaknuo osnivanje CARNetovog CERTa i sudjelovao u izradi Nacionalnog programa informacijske sigurnosti RH.

Smisao CISa je da bude **referentno mjesto za informacijsku sigurnost** za javnost, informatičare i posebno za mlade te da sustavno podiže njihovu svijest i sposobnosti u području informacijske sigurnosti.

Rad CISa podržava Ministarstvo znanosti, obrazovanja i sporta Republike Hrvatske, a omogućuju sponzori.

Prava korištenja

Ovaj dokument smijete:

- Dijeliti - umnožavati, distribuirati i priopćavati javnosti,
- Remiksirati - prerađivati djelo

pod slijedećim uvjetima:

- Imenovanje - Morate priznati i označiti autorstvo djela na način da bude nedvojbeno da mu je autor Laboratorij za sustave i signale, Fakulteta elektrotehnike i računarstva, Sveučilišta u Zagrebu.
  To morate napraviti na način koji ne sugerira da Vi ili Vaše korištenje njegova djela imate izravnu podršku LSSa.
- Nekomercijalno - Ovo djelo ne smijete naplaćivati ili na bilo koji način koristiti u komercijalne svrhe.
- Dijeli pod istim uvjetima - Ako ovo djelo izmijenite, preoblikujete ili koristeći ga stvarate novo djelo, preradu možete distribuirati samo pod licencom koja je ista ili slična ovoj i pri tome morate označiti izvorno autorstvo Laboratorija za sustave i signale, Fakulteta elektrotehnike i računarstva, Sveučilišta u Zagrebu.

Detalji licence dostupni su na: http://creativecommons.org/licenses/by-nc-sa/3.0/hr/legalcode

Sadržaj

1. Uvod

Internet je pun raznih ograničenja u obliku cenzure. Razlozi za cenzuru su višestruki. Cenzura se koristi za zaštitu od ilegalnih sadržaja na Internetu (pedofilske stranice, sadržaji koji šire mržnju), zaštitu djece te zaštitu korporativnih interesa. Za cenzuriranje sadržaja na Internetu koriste se web filtri, koji mogu raditi na dva načina: *keyword blocking* i *blacklist.* U nekim državama cenzura se iskorištava za sprječavanje mišljenja, ograničavanje osobnih sloboda i političke svrhe. Primjeri takvih zemalja su Kina, Kuba, Egipat, Iran i dr. Takvu vrstu cenzure ne odobrava većina ostalih zemalja svijeta i zbog nje su nastale organizacije koje se bave sprječavanjem cenzure. Najpoznatije takve organizacije su ACLU (eng. *American Civil Liberties Union*) i *Reporters Without Borders.* Više o temi što je cenzura može se pronaći u poglavlju 2.

Cenzura se može ostvariti na više načina. Osim prije spomenute podjele cenzure (*keyword blocking* i *blacklist*), cenzura se još dijeli na tehničku, netehničku i *"brute-force"* cenzuru. Pod tehničkom cenzurom podrazumijeva se onemogućavanje pristupa pojedinim web stranicama, gdje pristup onemogućavaju pružatelji mrežnih usluga. Tehnička cenzura se može ostvariti na više načina: blokiranjem IP (eng. *Internet Protocol*) adrese, DNS (eng. *Domain Name System*) blokiranjem, URL (rng. *Uniform Resource Locator*) blokiranjem, filtriranjem paketa te ponovnom inicijalizacijom Internetske veze. Svaki od tih načina ima svoje prednosti i nedostatke. Netehnička cenzura podrazumijeva cenzuru koju korisnik regulira samo za sebe, odnosno nije cijela korisnikova mreža cenzurirana. „*Brute-force*" cenzura se prevodi kao cenzura „silom" a u današnje vrijeme se jako rijetko susreće. Dijeli se na potpuno blokiranje i uklanjanje rezultata pretraživanja. Opis načina cenzuriranja može se pronaći u poglavlju 3.

U svrhu zaobilaženja cenzure i blokiranja sadržaja na Internetu razvijeno je više tehnika pomoću kojih se može doći do necenzuriranog sadržaja. Te tehnike uključuju korištenje različitih posredničkih (eng. *proxy*) servisa, programskih rješenja za uklanjanje cenzure te korištenje virtualnih privatnih mreža. Posebnost takvih servisa je ta da mogu dohvatiti i prikazati URL adrese cenzuriranih web stranica koristeći posredničke poslužitelje. Programskih rješenja za zaobilaženje cenzure ima više, a poznatiji među njima su *Java Anon Proxy, JonDos, Psiphon* i *Freenet*. U ovom dokumentu najviše je pojedinosti dano o alatu *Java Anon Proxy* jer je on besplatan, najrašireniji i solidnih je tehničkih mogućnosti. U zaobilaženju cenzure na Internetu koriste se i VPN mreže (eng. *Virtual Private Network*). VPN mreže omogućuju pojedincima i tvrtkama razmjenu i pristup informacijama s bilo kojeg računala u svijetu i kao takve ne podliježu pravilima cenzure koje neka država nalaže. O načinima zaobilaženja cenzure više se može pročitati u poglavlju 4.

U poglavlju5 dani su primjeri SAD-a, države koja na primjeren način provodi cenzuru Interneta te Kine, države koja cenzuru Interneta koristi u političke svrhe i oduzima građanima pravo na izražavanje i informacije. U Hrvatskoj cenzura nije zakonski posebno određena, ali postoje neki zakoni koji se nje dotiču. Izvod tih zakona može se pronaći u poglavlju 6. Pri kraju dokumenta, u poglavlju7, iznose se očekivanja vezana za cenzuru Interneta u budućnosti. Već i sada javljaju se dvije različite struje ljudi vezane uz cenzuru Interneta. S jedne strane su zagovornici građanskih prava, a s druge strane vlade i cenzori koji sumnjaju u ljudsko prosuđivanje. Po svemu sudeći, ipak se očekuje smanjenje cenzure u zemljama s jako izraženom cenzurom, ali i jačanje cenzure u svrhu uklanjanja sadržaja kao što su dječja pornografija, pozivi na mržnju, terorizam i slično.

2. Što je cenzura na Internetu?

Internet pruža vrlo brz pristup praktički neograničenoj količini informacija i većina korisnika Internet upravo tako koristi. Ipak, za određene korisnike Internet je pun ograničenja, zabrana i restrikcija u obliku cenzure.

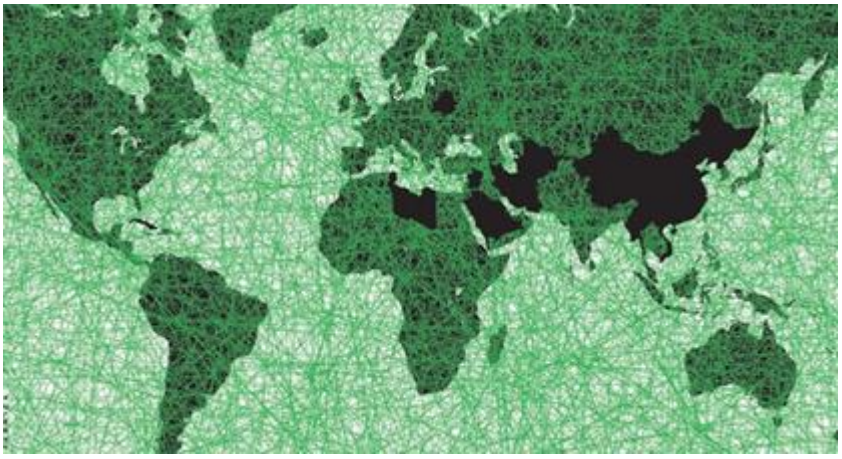
Razlozi cenzure na Internetu su u rasponu od dobronamjernih ciljeva, primjerice zaštita djece od neprimjerenih sadržaja, sprječavanje širenja terorizma ili zaštita autorskih prava, pa do ekstremnih ciljeva kojima se cijeloj naciji onemogućava pristup Internetu i njegovim sadržajima. Bez obzira na razloge, cenzura ima jednak utjecaj. Prihvaćena definicija je da je cenzura blokiranje pristupa Internetskim stranicama za koje se smatra da su nepoželjne.

Cenzuru na Internetu ne koriste samo pojedinci, kompanije ili vlade, već i niz programa kojima se ograničava ili zabranjuje pristup nekim stranicama. Skup programa koji se bavi cenzurom na Internetu poznat je pod nazivom „web filtri“, odnosno „*censorware*”.

Velik broj web filtara se temelji na dvije glavne tehnike blokiranja. Prva tehnika je *blacklist*, odnosno crna lista nepoželjnih stranica. Ta se lista redovito ažurira, a svaki pokušaj pristupa nekoj stranici s liste neće uspjeti. Druga tehnika blokiranja sadržaja na Internetu je *keyword blocking.* Njome se skeniraju ključne riječi web stranice i stranica se blokira ukoliko se otkriju „zabranjene“ riječi. Oblik cenzure na Internetu je i blokiranje zaposlenicima pristup određenim stranicama tijekom radnog vremena. To se radi kako im različiti sadržaji ne bi odvlačili koncentraciju ili loše utjecali na njihovu učinkovitost. Takav način cenzure je zanemariv u usporedbi s onom koja se javlja u pojedinim zemljama. Naime, neke su zemlje toliko rigorozne po pitanju cenzure da svojim stanovnicima pružaju vrlo malu količinu informacije koje su često po njihovim kriterijima politički korektne. Većina svjetskih zemalja cenzuru Interneta koristi da bi blokirala određene sadržaje, a najstrože cenzuriranje Interneta imaju sljedeće zemlje: Kina, Kuba, Egipat, Iran, Sjeverna Koreja, Sirija, Tunis, Saudijska Arabija, Mianmar, Vijetnam, Uzbekistan, Turkmenistan te Bjelorusija (Slika 1). Jedna od najpoznatijih cenzura na Internetu je ona koja se provodi u Kini. Naime, u toj se zemlji koristi napredno filtriranje mreže poznato pod nazivom *Great Firewall of China.* Više o cenzuriranju u Kini može se naći u nastavku dokumenta u potpoglavlju 5.2.

Filtriranje sadržaja Interneta radi se iz više razloga i oni su navedeni u nastavku.

- **Zaštita djece**. Djeca danas koriste Internet jednako kao i odrasli te na taj način imaju pristup informacijama čiji sadržaj ne razumiju niti mogu procijeniti njegovu opasnost. Pod zaštitom djece podrazumijeva se zaštita od svih sadržaja koji su nezakoniti te od nekih koji su neprimjereni za maloljetnike (primjerice pornografija). Uz to, djeca mogu pristupati raznim društvenim mrežama i programima za razmjenu poruka u realnom vremenu (eng. *chat*). Na taj način mogu stupiti u kontakte s raznim vrstama zlonamjernih ljudi i kriminalaca.
- **Zaštita od ilegalnih sadržaja na Internetu.** Pod ilegalnim ili nezakonitim stranicama smatraju se pedofilske stranice, sadržaji za širenje mržnje, poticanje na sukobe među društvenim ili nacionalnim skupinama, sadržaji koji nude štetne informacije primjerice način na koji je moguće proizvesti eksplozivne uređaje, sadržaji koji potiču na samoubojstvo, anoreksiju i slično.
- **Zaštita korporativnih interesa**. Ova se vrsta cenzure odnosi na tvrtke čiji zaposlenici imaju mogućnost pristupa Internetu. U interesu tvrtke je da oni mogu pristupati bitnim i korisnim podacima te da mogu međusobno komunicirati. Ipak, na tzv. slobodnom Internetu je jednako lako doći do korisnih, kao i do nepoželjnih sadržaja. Mogućnost zaposlenika za pristup Internetu može smanjiti produktivnost, stvoriti neugodnu atmosferu na poslu (primjerice ukoliko netko naočigled sviju pristupa neprihvatljivim stranicama), itd.



Slika 1. Zemlje s najstrožom politikom cenzuriranja Interneta
Izvor: mojotrotters.com

2.1. Organizacije za borbu protiv cenzure

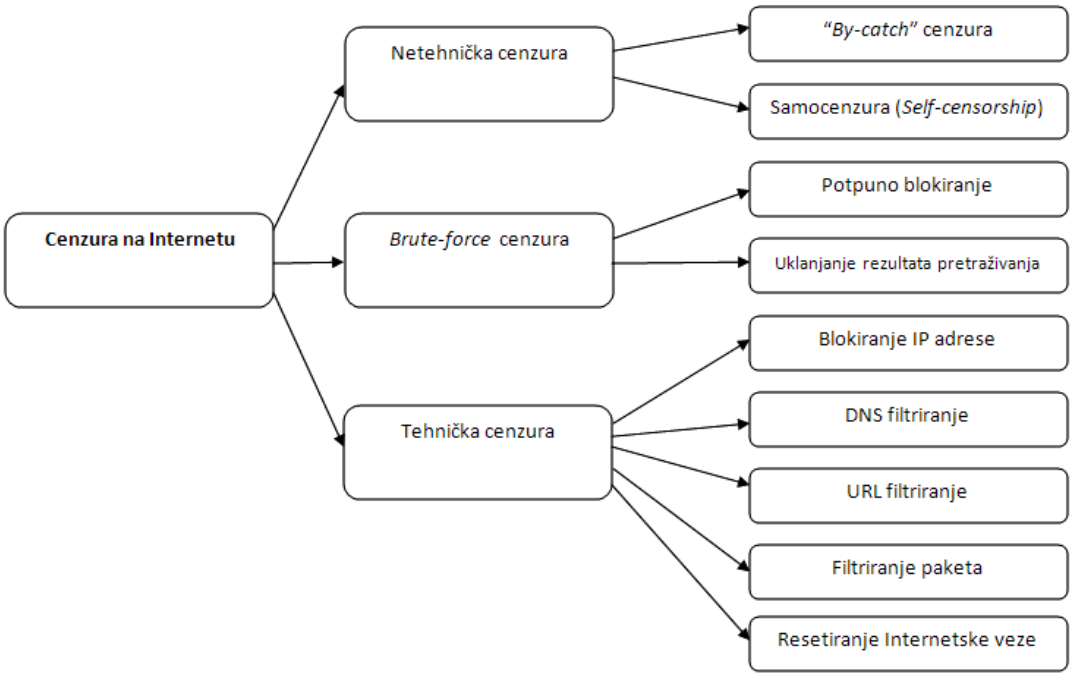
Cenzura na Internetu je dobra u nekim razumnim količinama. Neke države cenzuru koriste da bi cijeloj naciji zabranile pristup informacijama (npr. Kina) i zato postoje organizacije koje se bore protiv takve vrste cenzura. Neke od organizacija koje se bore protiv cenzure na Internetu su:

- **ACLU** (eng. *American Civil Liberties Union*) – organizacija osnovana u Americi 1920. godine čiji je cilj zaštita građanskih prava, zajamčenih ustavom i zakonom, svim građanima SAD-a. Organizacija danas broji preko pola milijuna članova i simpatizera.
- **Reporters Without Borders** - novinarsko udruženje osnovano 1985. godine čiji cilj je sloboda medija, borba protiv cenzure i zaštita novinara. Riječ je o međunarodnoj organizaciji koja putem ogranaka i dopisnika djeluje na svih pet kontinenata.
- **Censorware Project** i **Peacefire.org** - projekti kojima je cilj educirati korisnike o nedostacima web filtriranja. Peacefire.org je osnovan 1996. godine s ciljem zastupanja prava maloljetnika na slobodu govora, a danas broji preko 7000 članova. *Censorware* projekt je započela skupina pravnika, pisaca i aktivista 1997. godine, a cilj joj je razotkrivanje neučinkovitosti alata za web filtriranje i njihovih zlouporaba.
- **OpenNet Initiative** - skupina preko koje surađuju priznata svjetska sveučilišta (Harvard, Cambridge, Oxford i Toronto), s ciljem istraživanja i informiranja javnosti o načinima na koji pojedine države cenzuriraju informacije dostupne njihovim građanima. Na stranicama ove skupine mogu se pronaći interaktivne mape koje pokazuju prisutnost cenzure Interneta u svijetu.

3. Tehnike cenzure na Internetu

Tehnika cenzure na Internetu ima više, a dijele se na dvije veće skupine. Kao što je prije spomenuto, te dvije skupine su *blacklist* i *keyword blocking.* Po drugoj podjeli Internetska cenzura se dijeli na (Slika 2):

- tehničku cenzuru,
- netehničku cenzuru te
- *"Brute-force"* cenzuru.



Slika 2. Tipovi cenzure na Internetu
Izvor: LSS

3.1. Tehnička cenzura

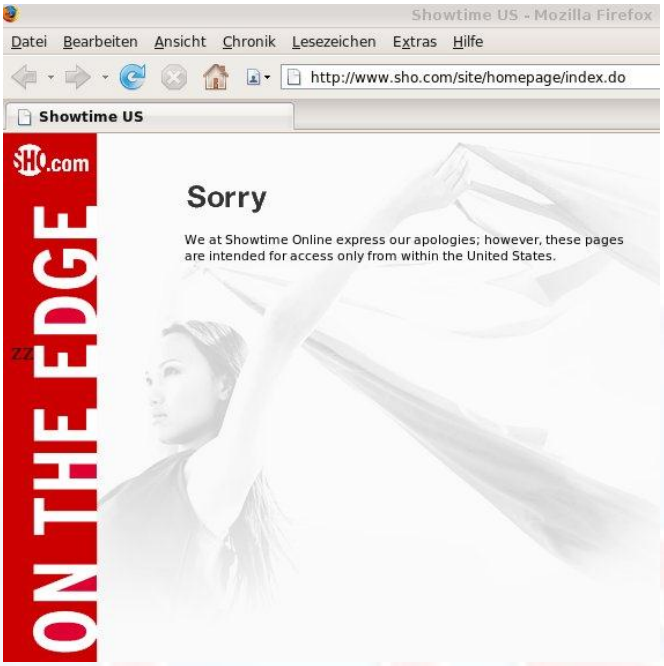
Tehnička cezura je najraširenija tip cenzure kojom se onemogućuje pristup pojedinim web stranicama. Tehnička cenzura može se izvesti na više načina:

- blokiranje IP adrese,
- DNS blokiranje i preusmjeravanje,
- URL blokiranje,
- filtriranje paketa te
- ponovno iniciranje Internetske veze.

3.1.1. Blokiranje IP adrese

Blokiranjem IP adrese (eng. *IP blocking*) sprječava se veza između web stranice tj. poslužitelja te određene IP adrese ili raspona adresa. Blokiranje IP adrese učinkovito sprječava nepoželjne veze s računala korisnika za web stranice, poslužitelje elektroničke pošte ili neke druge Internetske poslužitelje. Blokiranje IP adrese se često koristi za zaštitu od tzv. *brute force* napada. Također, blokiranje IP adrese se koristi u programima kao što

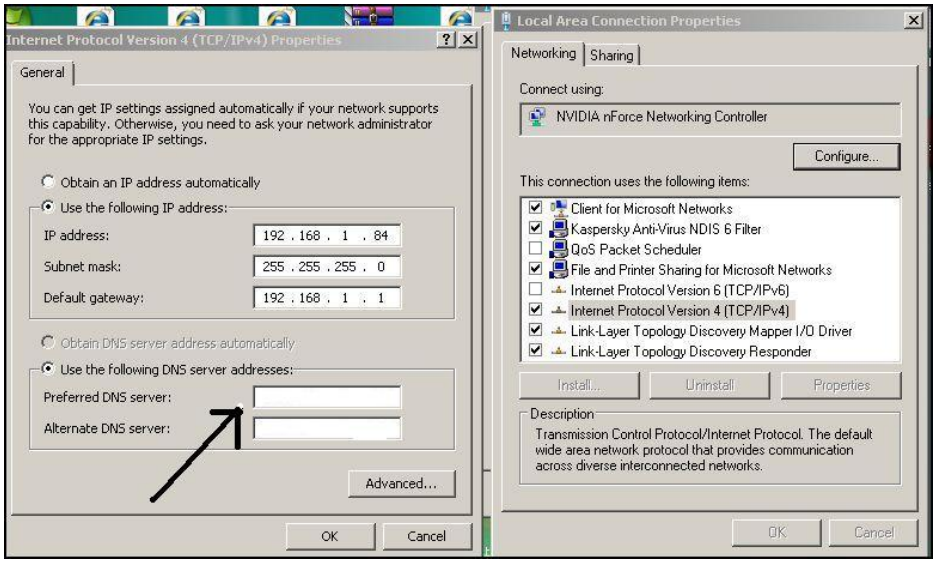
su *DenyHosts* ili *Fail2ban* za zaštitu od neovlaštenog pristupa računalu te za udaljeni pristup (eng. *Remote access*). Na Internetskim forumima i web stranicama blokiranje IP adrese se koristi za onemogućavanje određenih korisnika. Osim ovih načina korištenja, blokiranje IP adrese se učestalo koristi za cenzuru Interneta. Blokiranje IP adrese spada u tip *blacklist* cezure. Način ostvarenja cenzure pomoću blokiranja IP adrese je vrlo jednostavan. Lista sadrži IP adrese stranica kojima je onemogućen pristup. Primjer takve cenzure prikazuje Slika 3. Za zaobilaženje IP blokiranja najčešće se koriste posredničke web stranice, a više riječi o njima bit će objašnjenu u poglavlju 4.



Slika 3. Primjer blokiranja IP adrese stranice Showtime
Izvor: Wikipedia

3.1.2. DNS filtriranje i preusmjeravanje

DNS filtriranje i preusmjeravanje je relativno slab oblik cenzure. Ukoliko se želi pristupiti određenoj web stranici najčešće se upisuje URL adresa u adresnu traku. URL se tada šalje na DNS poslužitelj koji traži IP adresu za željenu URL adresu i šalje je natrag korisniku kako bi se mogla uspostaviti veza prema web stranici. Za cenzuriranu stranicu jednostavno će se u korisnički preglednik vratiti zahtjev bez IP adrese (DNS filtriranje) ili s različitom IP adresom (DNS preusmjeravanje) koja preusmjerava na sličnu, ali cenzuriranu web stranicu. To znači da web stranica kojoj se želi pristupiti postoji, ali informacije na DNS poslužitelju su promijenjene kako bi se spriječio pristup. DNS filtriranje i preusmjeravanje spada u *blacklist* tip cenzure jer DNS poslužitelj sadrži listu s cenzuriranim web stranicama. Postoje dvije mogućnosti zaobilaženja ovog načina cenzure i baš zbog toga ova cenzura nije često korištena. Prvi način je jednostavno upisivanje IP adrese željene web stranice, umjesto URL-a (Slika 4). U tu svrhu mogu se koristiti skripte koje su slobodno dostupne na Internetu, a služe za pronalaženje IP adrese URL-a. Druga metoda je promjena DNS poslužitelja kojeg računalo koristi za pretraživanje IP adrese. Primjerice, ukoliko se korisnik nalazi u Kini, a Kina je zabranila pristup na Wikipediju, umjesto korištenja kineskog DNS poslužitelja korisnik može koristiti poslužitelj od Sjedinjenih Američkih Država (koji ima informacije koje su potrebne za pristup Wikipediji). U tu svrhu koriste se alati kao što su npr. JAP, Freenet i slični. O ovim alatima će više riječi biti u nastavku.



Slika 4. Zaobilaženje DNS filtriranja upisom IP adrese DNS poslužitelja
Izvor: anonymous-proxies.org

3.1.3. URL blokiranje

URL blokiranje je najjednostavniji oblik cenzure Interneta kojeg je najjednostavnije zaobići. URL je adresa web stranice koja se unosi u adresnu traku web preglednika. Postoje razni programski alati (Slika 5) pomoću kojih se može zabraniti pristup određenim stranicama pomoću blokiranja URL adrese (npr. Website-Blocker, URLBlocker, Blue Coat). Prilikom korištenja URL (eng. *Uniform Resource Locator*) blokiranja, zahtjevi za pristup web stranici prosljeđuju se prema bazi podataka za odluku hoće li se specifičnoj URL adresi dopustiti ili uskratiti pristup. Opisani način rada ovaj tip cenzure svrstava u *blacklist* kategoriju cenzure. Ovaj sustav cenzure ima nekoliko ograničenja. Sadržaj se ne može filtrirati ili blokirati na taj način, osim ukoliko je prethodno identificiran i uključen u bazu „zabranjenih" URL adresa. URL blokiranje također ne pruža dobru prilagodbu. Na primjer, on ne može dopustiti neku web stranicu, a onemogućiti *pop-up* prozore i slične aktivne sadržaje. Također, ukoliko se umjesto upisa URL-a, upiše IP adresa, URL blokiranje neće funkcionirati.

Slika 5. Website-Blocker alat za blokiranje URL adrese
Izvor: smarthacker5.wordpress.com

3.1.4. Filtriranje paketa

U vatozidovima (eng. *Firewall*), filtriranje paketa (eng. *Packet filtering*) se izvodi programima poznatima kao paketni filtri. Paketni filtar ocjenjuje zaglavlje dolaznih paketa na temelju određenih kriterija. Na toj osnovi, on odlučuje hoće li prihvatiti ili odbiti paket. Nakon što su kriteriji, odnosno pravila za filtriranje postavljena, paketni filtar se može konfigurirati na tri načina (Slika 6).

Slika 6. Konfiguracija paketnog filtra
Izvor: all-freeware.com

Prvo, filtar se može konfigurirati za prihvaćanje paketa koji se smatraju sigurnima i automatsko neprihvaćanje ostalih paketa. Iako je to najsigurniji način, on može biti neprikladan jer blokira preveliku količinu paketa. Drugi oblik koji se može podesiti je da se odbijaju samo paketi koje filtar određuje kao neodgovarajuće uz prihvaćanje svih ostalih. Ova metoda je manje sigurna, ali smanjuje razinu neugodnosti prilikom web pregledavanja. U trećoj konfiguraciji, paket će biti u karanteni kada ga filtar presretne, a on se ne pridržava uvjeta. Tada korisnik može odrediti što treba učiniti s paketom. Paketni filtri su izvorno razvijeni na operacijskom sustavu OpenBSD, ali su preneseni i u mnoge druge. Najpoznatiji paketni filtri su ZoneAlarm, F-Secure i NeT Firewall. U svrhu cenzure na Internetu, paketni filtri se mogu koristiti tako da se konfiguriraju na način da onemogućuju pakete koji sadrže određene riječi, slike i/ili video sadržaje. Samim time, filtriranje prometa se kategorizira kao *keyword blocking* tip cenzure. Jedan od najboljih načina cenzure na Internetu je korištenje URL blokiranja u kombinaciji s filtriranjem prometa. URL filtriranje služi za početno filtriranje korisničkih zahtjeva i ono izbacuje većinu „zabranjenog“ prometa, dok filtriranje prometa odbaci povratne podatke koji nisu primjereni.

3.1.5. Ponovno uspostavljanje Internetske veze

Ponovno postavljanje Internetske veze (eng. *Connection reset*) je pojava koja se javlja prilikom pokušaja spajanja na web stranicu (Slika 7). Ukoliko je web stranica cenzurirana, filtar će blokirati (resetirati) TCP (eng. *Transmission Control Protocol*) vezu. Budući pokušaji spajanja s obje strane (dakle, bilo da korisnik ili poslužitelj pokuša inicirati vezu) će također biti blokirani u trajanju do 30 minuta. Ovisno o adresi bloka, drugim korisnicima ili web stranicama spajanje također može biti blokirano ako se komunikacija odvijala preko njih. Ova metoda spada u *blacklist* vrstu cenzure i rijetko se koristi jer je prilično radikalna. Da bi

se izbjeglo ponovno postavljanje veze razvila se tzv. metoda izbjegavanja (eng. *Circumvention method*). Metoda izbjegavanja radi tako da ignorira *reset* paket kojeg je poslao vatrozid.

Slika 7. Ponovno postavljanje Internetske veze
izvor: chinayouren-free.com

3.1.6. Usporedba tipova tehničke cenzure

Tablica 1 daje usporedbu karakteristika opisanih tipova tehničke cenzure. Prikazan je raspon svakog tipa cenzure, kao i prednosti i nedostaci. Također je naveden i način izbjegavanja pojedine cenzure.

Način cenzure	Raspon cenzure	Prednosti	Nedostaci	Izbjegavanje
Blokiranje IP adrese	IP zasnovano (*IP-based*)	Vrlo jaka cenzura ukoliko je dobra crna lista	Točnost cenzure ovisi o listi, IP adrese su promjenjive	Posrednički poslužitelji
DNS filtriranje i preusmjeravanje	IP zasnovano (*IP-based*)	Ne ovisi o promjenama IP adrese, teško izbjegavanje cenzure		Pronaći drugi DNS poslužitelj, na drugi način odrediti IP adresu
URL blokiranje	HTTP	Jednostavna, ne ovisi o imenima domena (DNS)	Točnost cenzure ovisi o listi	VPN mreža
Filtriranje paketa	TCP zasnovano (*TCP-based*)	Fokus na pakete	Pogrešno odbacivanje podataka	VPN, smanjivanje količine teksta u paketu
Ponovno postavljanje Internetske veze	TCP zasnovano (*TCP-based*)	Pruže veću kaznu od ostalih cenzura	Samo dodatak ostalim cezurama	Ignoriranje *reset* paketa

Tablica 1. Svojstva tipova tehničke cenzure

3.2. „Brute-force“ cenzura

„*Brute-force*“ cenzura bi u prijevodu značila cenzura „silom“, a u današnje vrijeme se jako rijetko susreće. Dijeli se na potpuno blokiranje i uklanjanje rezultata pretraživanja.

Potpuno blokiranje (eng. *Full block*) je tehnički najjednostavniji način cenzure na Internetu. Pod potpunim blokiranjem smatra se odsijecanje svih mrežnih uređaja, bilo programski ili isključivanjem strojeva, čupanjem kablova i slično. Primjer cenzure potpunim blokiranjem je slučaj egipatskih prosvjeda 27. siječnja 2011. Tada je oko 3500 BGP (eng. *Border Gateway Protocol*) mrežnih ruta zatvoreno od oko 22:10 do 22:35 UTC. BGP rute su tada ugašene rezanjem interkontinentalnih (europsko-azijskih) optičkih veza.

Uklanjanje rezultata pretraživanja (eng. *Search result removal*) drugi je tip „*Brute-force*“ cenzure. Temelji se, kako samo ime kaže, na potpunom uklanjanju rezultata koje neki Internetski pretraživač pronađe. Ovakav tip cenzure se često nalazi u poduzećima gdje je cilj što veća produktivnost njihovih zaposlenika pa im se pokušavaju ukloniti sve web stranice koje bi ih mogle ometati. Drugi primjer ovakve cenzure je Kina, u kojoj vlasti reguliraju informacije na Internetu. Tako se, na primjer, s kineskih poslužitelja ne mogu pronaći razni podaci za koje se smatra da nisu primjereni i politički korektni. Iz tog razloga zabranjen je pristup YouTube-u, Wikipediji, itd. Također, nije moguće pristupiti stranicama tipa Flickr, Myspace, Twitter i Facebook jer je na njima moguće izraziti vlastito mišljenje, a u rezultatima pretraživanja se neće pojaviti podaci s tih stranica.

3.3. Netehnička cenzura

Netehnička (eng. *Non-technical censorship*) cenzura je ona koju korisnik regulira samo za sebe, dakle nije cijela korisnikova mreža cenzurirana. Netehnička cenzura se dijeli na „*by-catch*“ cenzuru i samocenzuriranje (eng. *Self-censorship*).

„*By-catch*“ cenzura je vezana uz tzv. „*Scunthorpe*“ problem. „*Scunthorpe*“ problem nastaje kada filtar za cenzuru ili pretraživač ukloni neke rezultate jer njihov tekst sadrži niz slova koja su zajednička s opscenim riječima. Dok računala mogu lako identificirati nizove teksta u dokumentu, široka pravila blokiranja mogu rezultirati lažno pozitivnim rezultatima blokiranja. Rješenje „*Scunthorpe*“ problema je „*by-catch*“ cenzura kojom se rezultati cenzuriraju, ali se za njih može odrediti da ih se u budućnosti ne cenzurira (definira se iznimka), a o tome odlučuje korisnik.

Samocenzura (Slika 8) s druge strane radi potpuno suprotno. Korisnik može za sebe odlučiti koje će se riječi ili cijele web stranice cenzurirati. Razlika između samocenzure i URL blokiranja je u tome što samocenzura može cenzurirati samo neke riječi, a ne cijele web stranice (URL-ove). Dodatno, samocenzura omogućuje prikaz cenzuriranog sadržaja ukoliko korisnik to želi.

Slika 8. Primjer blokiranja sadržaja na temelju samocenzure
Izvor: otterzen.blogspot.com

4. Načini zaobilaženja cenzure na Internetu

Postoji niz resursa i načina koji omogućuju korisnicima zaobilaženje tehničkih aspekata cenzure Interneta. Svaki način ima različitu jednostavnost, brzinu i sigurnost korištenja. Većina se, međutim, oslanja na dobivanje pristupa na mrežnu vezu koja ne podliježe filtriranju, često u različitim nadležnostima koje ne podliježu istim zakonima cenzure. Ovo je svojstven problem cenzure Interneta. Dakle, tako dugo dok postoji i jedan javno dostupan sustav za pristup informacijama u svijetu bez cenzure, i dalje će postojati mogućnost da korisnici imaju pristup cenzuriranom materijalu. Najpoznatiji načini zaobilaženja cenzure na Internetu su:

- posredničke web stranice (eng. *Proxy Websites*),
- programska rješenja (eng. *Software Solutions*) te
- virtualne privatne mreže (eng. *Virtual Private Network*, VPN).

4.1. Posredničke web stranice

Posredničke web stranice su često najjednostavniji i najbrži način za pristup zabranjenim web stranicama u zemljama s cenzurom Interneta. Kako je njima dozvoljen pristup stranicama za koje neki korisnik nema prava pristupa, služe kao posrednik između (djelomično) blokiranih web odredišta i korisnika (kojem je pristup tom odredištu zabranjen). To se obično postiže tako da posrednički poslužitelj dohvaća željenu stranicu umjesto korisnika te mu unutar vlastite web stranice (u obliku neke forme, tj. podstranice) prikazuje zabranjeni sadržaj (Slika 9). Preporuča se korištenje HTTPS (eng. *Hypertext Transfer Protocol Secure*) protokola, budući da je šifriran i teže ga je blokirati ili cenzurirati. U državama s izraženom cenzurom Interneta često se zabranjuju i posredničke web stranice. Popis posredničkih web stranica se lako može pronaći na više mjesta na Internetu, a jedan od popularnijih nalazi se na:

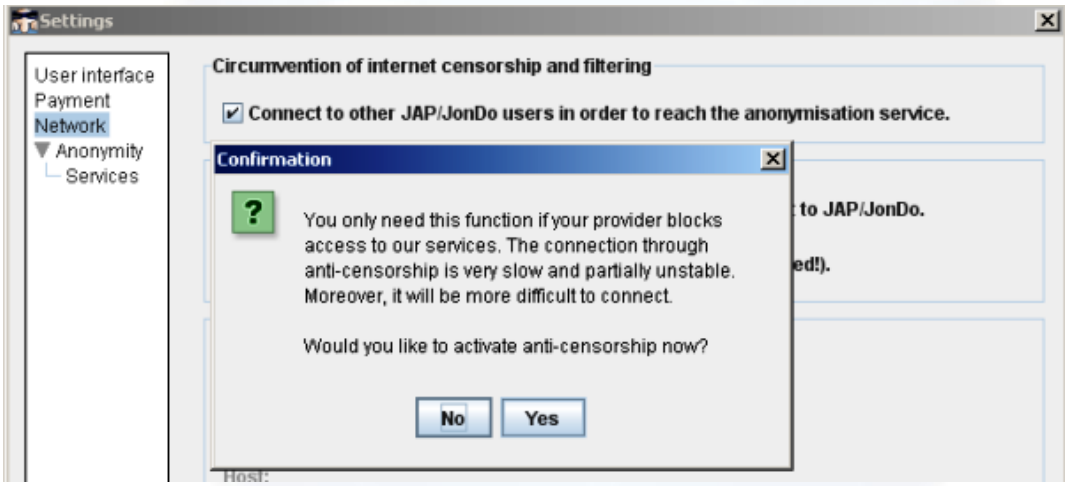
http://www.proxywebsites.biz/

Slika 9. Pristup cenzuriranim web stranicama pomoću proxy web stranica
Izvor: linglom.com

4.2. Programska rješenja

Cenzuru na Internetu moguće je zaobići korištenjem raznih programskih alata za zaobilaženje cenzure i blokiranja na mreži. Poznatiji alati su *Java Anon Proxy, JonDos, Psiphon, Freene, I2P* i *Tor*.

Jedan od raširenijih i češće korištenih programskih rješenja za zaobilaženje cenzure na Internetu je *Java Anon Proxy* (JAP). Radi se o besplatnom alatu otvorenog koda dostupnom za sve operacijske sustave. Od 2004. godine on također uključuje i funkcionalnost koja omogućuje korisnicima zaobilaženje blokade cenzure. *Java Anon Proxy* je prvenstveno napravljen da korisnicima omogući anonimno pretraživanje Interneta. Napravljen je u suradnji tehničkog sveučilišta u Dresdenu (njem. *Technische Universität Dresden*) i sveučilišta u Regensburgu (njem. *Universität Regensburg*). Koristi se iz nekoliko razloga: sigurnost, anonimnost korisnika, balansiranje opterećenja, hvatanje i filtriranje mrežnog prometa s ciljem smanjenja zahtjeva za propusnost te zaobilaženje cenzure ili blokiranja. Filtriranje programom *Java Anon Proxy* može izolirati neprihvatljive sadržaje web stranica kao što su kolačići (eng. *cookies*), *pop-up* reklame i slično. Alat također šifrira web komunikaciju, štiteći korisnika od rutinskog praćenja ili čak posvećenog nadzora (praćenje rada računala koja su uključena u prijenos i obradu informacija putem Interneta i uvid u prijenos informacija satelitskim i zemaljskim telekomunikacijskim sustavima). *Java Anon Proxy* sadrži naredbu „*Connect to other JAP users in order to reach the anonymization service*“ (Slika 10) koja korisnicima omogućuje prikaz cenzuriranog sadržaja na webu. Ukoliko je sadržaj web stranice cenzuriran, *Java Anon Proxy* automatski pronalazi drugu IP adresu stranice na kojoj je moguće pregledati sadržaj.



Slika 10. Zaobilaženje cenzure pomoću programa Java Anon Proxy
Izvor: flossmanuals.net

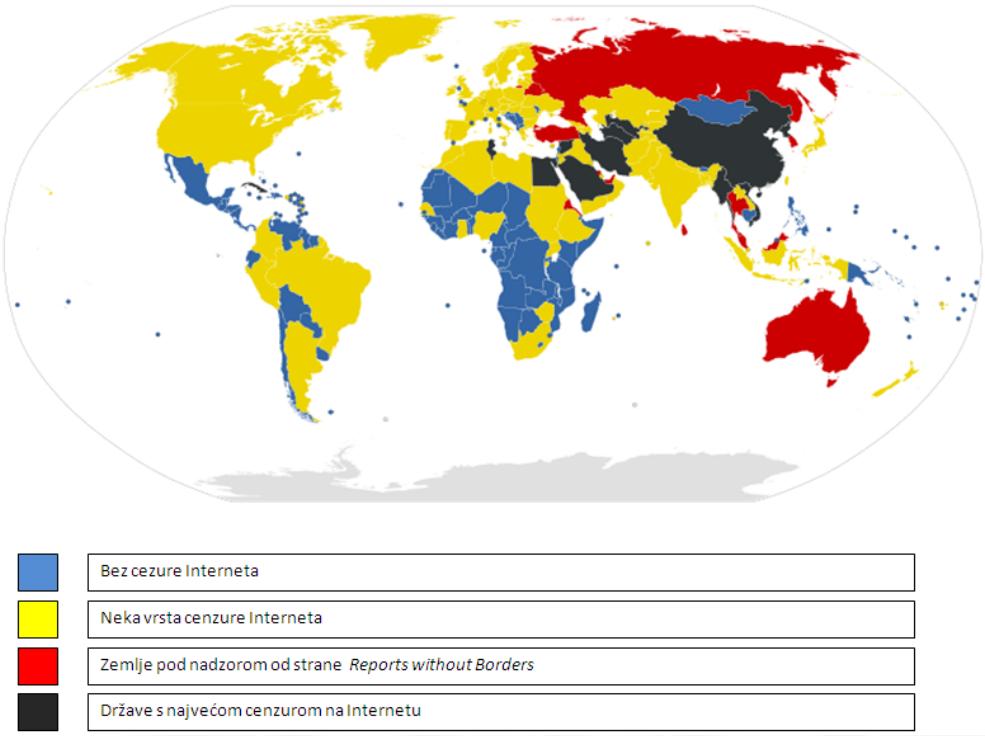
4.3. Virtualne privatne mreže

U posljednje vrijeme u zemljama s izraženom cenzurom Interneta sve se više koriste virtualne privatne mreže. VPN mreže omogućuju pojedincima i tvrtkama razmjenu i pristup informacijama s bilo kojeg računala u svijetu. Mreže su privatne, jer im je pristup ograničen samo na određene korisnike. VPN-ovi se smatraju virtualnim mrežama jer za povezivanje koriste druge mreže i korisnike, a ne izravnu vezu. VPN mreže postaju sve popularnije i sigurnije, a njihove brojne prednosti postaju sve očitije. VPN-om je moguće zaobići geografska ograničenja Interneta, ali i izbjeći stalno praćenje korisničkih aktivnosti. Korištenjem VPN-a korisnik je u mogućnosti sam odrediti hoće li cenzuru, kao i kakva će ona biti. Osim toga, korisnik je zaštićen od svih praćenja njegovih aktivnosti, njegovog lociranja i zlonamjernih napadača. Postoji više od 150 dostupnih pružatelja VPN usluga i njihov broj još uvijek raste. Korištenje ovih VPN servisa najčešće se plaća, ali korisnik može i sam složiti svoj VPN servis. Popis dostupnih pružatelja VPN usluga može se naći na adresi:

http://www.bestvpnservice.com/

5. Primjeri cenzure na Internetu

Kao što je već rečeno, neke države u svijetu imaju jaku cenzuru Interneta, dok je druge gotovo i nemaju. Slika 11 prikazuje izraženost cenzure u svijetu. U nastavku teksta dan je primjer Sjedinjenih Američkih Država koje imaju optimalnu i vrlo razrađenu cenzuru Interneta te primjer Narodne Republike Kine koja je ekstremna po pitanju cenzure Interneta.



Slika 11. Cenzura u svijetu
Izvor: Wikipedia

5.1. Sjedinjene Američke Države

Jaka zaštita slobode govora i izražavanja je ukorijenila cenzuru u Prvi amandman u Ustavu Sjedinjenih Američkih Država. Ta se zaštita proširila na Internet, i kao rezultat toga je da vlada SAD-a dozvoljava vrlo malo tehničkog filtriranje Interneta u SAD-u. Ipak, Internet je u SAD-u reguliran od strane države i on predstavlja složen skup pravno obvezujućih i privatno posredovanih mehanizama. Nakon desetljeća i pol rasprave o spornim sadržajima regulacije, zemlja je još uvijek vrlo daleko od postizanja političkog konsenzusa o prihvatljivim granicama slobode govora i o najboljem sredstvu zaštite maloljetnika od ilegalne aktivnosti na Internetu. Kockanje, kibernetička sigurnost (eng. *Cyber security*) i opasnosti za djecu izvor su čestih rasprava u SAD-u. Značajan javni otpor na predložena pravila i ograničenja sadržaja spriječili su ekstremnije mjere cenzure Interneta koje se rabe u nekim drugim državama svijeta. Javne rasprave te rasprava zakonodavne i sudske vlasti proizveli su strategiju filtriranja i cenzuriranja Interneta u SAD-u koja je drugačija od onih u većini ostalih država svijeta. Mnoge vlade pokušavaju regulirati sadržaj koji je zabranjen na temelju Prvog amandmana, često nakon dugotrajnih pravnih bitaka. Vlada je u mogućnosti izvršavati pritisak neizravno gdje se ne može izravno cenzurirati. S izuzetkom dječje pornografije, sadržaj ograničenja obično se više oslanja na uklanjanje sadržaja od blokiranja. Za razliku od većeg dijela ostatka svijeta, gdje cenzuru Interneta regulira država i pružatelji Internetskih usluga, u SAD-u se većina sadržaja cenzurira na privatnoj ili dobrovoljnoj razini.

Prvi val mjera cenzure u 1990-im godinama u Sjedinjenim Američkim Državama nastao je kao odgovor na obilje seksualno eksplicitnog materijala dostupnog maloljetnicima na Internetu. Od tog vremena postojalo je nekoliko zakonodavnih pokušaja stvaranja obveznog sustava provjere sadržaja. U SAD-u se tada uspjelo proizvesti sveobuhvatno rješenje za strože provjere Interneta. Istovremeno, dok se zakonski pokušavala nadzirati distribucija društveno neprihvatljivog materijala na Internetu, u SAD-u je nastao robustan sustav koji ograničava odgovornost nad sadržajem za Internet posrednike, kao što su davatelji internetskih usluga (ISP) i *hosting* tvrtke. Zabrinutost za nacionalnu sigurnost potaknula je napore proširivanja nadzora digitalnih komunikacija i bolje praćenje mrežne komunikacije. Danas u SAD-u ima više zakona vezanih uz cenzuru na Internetu, i oni su:

- *Communications Decency Act* (CDA) – zabranjuje nepristojnost i opscenost na Internetu,
- *Child Online Protection Act* (COPA) – zabranjuje golotinju i seksualne radnje na mreži,
- *Digital Millennium Copyright Act* (DMCA) – štiti privatnost i sigurnost djece na Internetu,
- *Children's Online Privacy Protection Act* (COPPA) – štiti privatnost djece na Internetu,
- *Children's Internet Protection Act* (CIPA) - štiti djecu od štetnih *online* sadržaja.

5.2. Narodna Republika Kina

Cenzura Interneta u Narodnoj Republici Kini provodi se na temelju različitih zakona i upravnih propisa. Ne postoje posebni zakoni ili propisi koje cenzura Interneta slijedi. U skladu s time, vlast Narodne Republike Kine je napravila više od šezdeset različitih propisa o cenzuri na Internetu. Cenzuru energično provode pokrajinske podružnice u vlasništvu državnih pružatelja mrežnih usluga (eng. *Internet Service Provider*, ISP), poslovnih tvrtki i organizacija. Takva cenzura se ne primjenjuje na Hong Kong i Macau jer su one posebne ovlasti koje s priznatim međunarodnim ugovorom imaju neovisne sudbene vlasti i ne podliježu većini zakona iz Kine, uključujući i one koji zahtijevaju ograničavanje slobodnog protoka informacija. Rigorozniji stav vlade u nastojanju da neutralizira kritičko *online* mišljenje pojavilo se nakon niza velikih anti-Japanskih, anti-polucijskih te anti-korupcijskih prosvjeda i etničkih pobuna, od kojih su mnogi bili organizirani ili publicitet stekli pomoću poruka elektroničke pošte, soba za razgovor i SMS (eng. *Short Message Service*) poruka. Procjenjuje se da „Internet policija“ u Kini broji više od 30.000 ljudi. Kritički komentari koji se pojavljuju na Internetskim forumima, blogovima i glavnim portalima kao što su Sohu i Sina obično se brišu u roku od nekoliko minuta. Cenzura Interneta u Kini se smatra opsežnijom i naprednijom od bilo koje druge zemlje u svijetu. Državna vlast ne samo da blokira web stranice sa sadržajem, već i nadzire pristup pojedinaca Internetu. Amnesty International navodi da je u Kini najveći zabilježen broj zatočenih novinara i *cyber* disidenata u svijetu. Djela za koja su optuženi uključuju komuniciranje sa skupinama u inozemstvu, suprotstavljanje progonu Falun Gonga, potpisivanje *online* peticija te pozivanje na reformu i kraj korupcije. Pojedinac u Kini ne smije koristiti Internet za stvaranje, repliciranje, preuzimanje ili prenošenje sljedećih vrsta informacija:

- Poticanje odupiranju ili razbijanju Ustava, zakona ili provedbe administrativnih propisa.
- Poticanje na svrgavanje vlade ili socijalističkog sustava.
- Poticanje na podjelu zemlje te oštećivanje nacionalnog ujedinjenja.
- Poticanje mržnje ili diskriminacije između nacionalnosti ili oštećivanje jedinstva naroda.
- Promicanje neistine ili iskrivljene istine, širenje glasina ili uništavanje poretka društva.
- Promicanje praznovjerja, seksualno sugestivnog materijala, kockanja, nasilja ili ubojstva.
- Terorizam ili poticanje drugih kriminalnih aktivnosti, otvoreno vrijeđanje drugih ljudi ili klevete o drugim ljudima.
- Povređivanje ugleda državnih organizacija.
- Ostale aktivnosti protiv Ustava, zakona i upravnih propisa.

Lista cenzuriranih web stranica u Narodnoj Republici Kini je podugačka, a uključuje i stranice kao što su YouTube, Flickr, Wikipedia, Myspace, Twitter i Facebook. Više o listi zabranjenih web stranica se može naći na web adresi:

http://en.wikipedia.org/wiki/List_of_websites_blocked_in_the_People%27s_Republic_of_China

6. Zakonske osnove cenzure u Republici Hrvatskoj

Prema Ustavu Republike Hrvatske osobne i političke slobode i prava uključuju:

- Slobodu mišljenja i izražavanja misli. Sloboda izražavanja misli obuhvaća osobito slobodu tiska i drugih sredstava priopćavanja, slobodu govora i javnog nastupa i slobodno osnivanje svih ustanova javnog priopćavanja. Zabranjuje se cenzura. (čl. 38.)
- Sloboda i tajnost dopisivanja i svih drugih oblika općenja zajamčena je i nepovrediva. Samo se zakonom mogu propisati ograničenja nužna za zaštitu sigurnosti države ili provedbu kaznenog postupka. (čl. 36.)
- Zabranjeno je i kažnjivo svako pozivanje ili poticanje na rat ili uporabu nasilja, na nacionalnu, rasnu ili vjersku mržnju ili bilo koji oblik nesnošljivosti. (čl. 39.)

Slobode medija iz Zakona o medijima opisane su u članku 3:

- Sloboda medija obuhvaća osobito: slobodu izražavanja mišljenja, neovisnost medija, slobodu prikupljanja, istraživanja, objavljivanja i raspačavanja informacija u cilju informiranja javnosti; pluralizam i raznovrsnost medija, slobodu protoka informacija i otvorenosti medija za različita mišljenja, uvjerenja i za raznolike sadržaje, dostupnost javnim informacijama, uvažavanje zaštite ljudske osobnosti, privatnosti i dostojanstva, slobodu osnivanja pravnih osoba za obavljanje djelatnosti javnoga informiranja, tiskanja i raspačavanja tiska i drugih medija iz zemlje i inozemstva, proizvodnju i objavljivanje radijskog i televizijskog programa, kao i drugih elektroničkih medija, autonomnost urednika, novinara i ostalih autora programskih sadržaja u skladu s pravilima struke.
- Slobode medija dopušteno je ograničiti samo kada je i koliko je to nužno u demokratskom društvu radi interesa nacionalne sigurnosti, teritorijalne cjelovitosti ili javnoga reda i mira, sprječavanja nereda ili kažnjivih djela, zaštite zdravlja i morala, zaštite ugleda ili prava drugih, sprječavanja odavanja povjerljivih informacija ili radi očuvanja autoriteta i nepristranosti sudbene vlasti samo na način propisan zakonom.
- Zabranjeno je prenošenjem programskih sadržaja u medijima poticati ili veličati nacionalnu, rasnu, vjersku, spolnu ili drugu neravnopravnost, kao i ideološke i državne tvorevine nastale na takvim osnovama, te izazivati nacionalno, rasno, vjersko, spolno ili drugo neprijateljstvo ili nesnošljivost, poticati nasilje i rat.

Na temelju Ustava i Zakona o medijima zaključuje se o potrebi provjere sadržaja na Internetu, ali i o potrebi da se provjera provodi vrlo precizno, tako da se ne naruše temeljna prava na slobodu mišljenja i pristupa informacijama. Budući da je trenutno nemoguće takvu provjeru na Internetu provoditi zaista kvalitetno, u Hrvatskoj ne postoje zakoni koji bi dopuštali filtriranje web sadržaja javnim mrežama. Zakon o telekomunikacijama nalaže javnim operaterima (pravnim osobama koje raspolažu telekomunikacijskom mrežom) sa znatnijom tržišnom snagom pružanje otvorenog pristupa mreži (čl. 52). Pristup se prema članku 58. može ograničiti samo iznimno radi:

- sigurnosti rada telekomunikacijske mreže,
- održavanja cjelovitosti telekomunikacijske mreže,
- sposobnosti međusobnog funkcioniranja telekomunikacijskih usluga ili
- zaštite podataka.

Ovaj zakon se ne odnosi na privatne mreže poput poslovnih mreža ili akademskih mreža, kao što je CARNet, koje omogućuju pristup samo određenoj skupini korisnika. Takva privatna mreža može ograničiti pristup Internetu u skladu s vlastitim i interesima svojih korisnika.

7. Budućnost cenzure na Internetu

Internet je najveće i najraširenije sredstvo koje omogućuje slobodno izražavanje mišljenja svakog pojedinca. Sloboda govora je jedno od ključnih prava svakog čovjeka u demokratski uređenom društvu. Prema tome, postavlja se pitanje zašto vlade pojedinih država cenzuriraju sadržaj na Internetu.

Razlozi uvođenja cenzure na Internetu su zaista brojni, ali većinom su usmjereni na zaštitu samih korisnika. Cenzurirane stranice obično sadrže neki oblik neprikladnog sadržaja poput klevetanja, rasne diskriminacije, dječje pornografije i sl. Osim toga, tu su i drugi primjeri sadržaja koje bi svakako trebalo blokirati poput lažnog oglašavanja, navođenja na financijske prijevare te prijetnja. Na Internetu je sve moguće. Svaki korisnik koji ima pristup može postaviti ili pronaći određene informacije, fotografije ili video isječke. Uzimajući u obzir sve navedeno, cenzura sadržaja na Internetu se ne čini kao loša opcije uvođenja bar neke kontrole nad tim nevjerojatnim medijem.

Međutim, problem se javlja kod postavljanja granica između onoga što treba blokirati, a što ne. Većinom se cenzura ne zadržava samo na sadržaju koju je zaista neprikladan nego se proširuje na sav materijal koji vlade određenih država smatraju nepoželjnim. Blokiranje takvih informacija moglo bi biti sve više izraženo u budućnosti pa i popraćeno s visokim novčanim ili zatvorskim kaznama.

Dodatni problem je pitanje kome treba povjeriti donošenje odluke o blokiranju nekog sadržaja i provođenje cenzure. U prošlosti je cenzura Interneta bila vrlo izravna – vlade bi blokirale web stranice, manipulirale tražilicama i kažnjavale autore neprimjerenih sadržaja. Međutim, povećan broj web stranica i korisnika Internet usluga učinio je ovakve metode neefikasnima. Danas blokiranje neke web stranice rezultira privlačenjem pažnje šire javnosti i rastom popularnosti takve stranice što korisnike navodi na pronalaženje zaobilaznih rješenja za pristup blokiranoj stranici. Također, vlade više nisu u mogućnosti dovoljno brzo blokirati sve web stranice kojima se informacije danas mogu širiti. Prema tome, potrebno je pronaći nove načine kontrole Internetskog sadržaja. Čak i metode temeljene na DNS filtriranju i filtriranju samog sadržaja ne mogu dati dovoljno pouzdane rezultate. Ovi problemi bit će sve istaknutiji u budućnosti jer su korisnici sve više svjesni prava slobodnog izražavanja i spremni boriti se za slobodu na Internetu. Čak i u vrlo zatvorenim, konzervativnim državama, društvo sve više postaje svjesno količine kontrole koju uvodi vlada pod izlikom da štiti svoje građane od neprimjerenih sadržaja.

8. Zaključak

Štetni sadržaji na Internetu prisutni su u različitim oblicima, kao programi kojima je cilj narušiti rad računala ili ukrasti podatke, kao zlonamjerno oblikovane web stranice, poruke elektroničke pošte, IM poruke, neprikladni slikovni, video ili tekstualni sadržaji itd. Jedan od štetnih sadržaja na Internetu jesu i stranice koje promiču mržnju, pedofiliju, terorizam i slično. U određenim uvjetima (škole, tvrtke) koriste se filtri web stranica kako bi se spriječio pristup neprihvatljivim web stranicama. Takve usluge mogu koristiti i roditelji zabrinuti za sigurnost svoje djece.

Sloboda pružatelja usluga pristupa Internetu na uvođenje ograničenja na Internetsku komunikaciju dosta je kontroverzna ideja koja ima brojne protivnike. Problem je što bi se na taj način bitno promijenio smisao Interneta kao slobodne mreže. Osim toga, otvorio bi se prostor za zlouporabe i uvođenje cenzure. Osim automatske zaštite računala, od iznimne je važnosti informirati se o opasnostima i dobrom korisničkom ponašanju na Internetu.

Svaki korisnik Interneta treba biti sposoban prepoznati i izbjeći sumnjive sadržaje te znati kako postupiti kada dođe u kontakt s njima. S obzirom na raširenost i ulogu Interneta u svijetu, razumijevanje njegovog funkcioniranja nije više dovoljno ostaviti stručnjacima (informatičarima). Internet ulazi u svijet i svijet postaje Internet, sve važne informacije kruže Internetom i na njemu se nalaze razni povjerljivi podaci. Iz tog razloga opasnosti koje ondje vrebaju nisu samo virtualne, već su stvarne.

Razumijevanje Interneta, svijest o postojećim opasnostima, odgovorno ponašanje i korištenje računalne zaštite nužni su kako bi ovu nesigurnu mrežu, svaki korisnik za sebe učinio sigurnim mjestom. Cenzura Interneta je razumna opcija ukoliko se ona izvodi na razuman način. Krajnji cilj cenzure na Internetu trebao bi biti potpuno uklanjanje stranica društveno neprimjerenog sadržaja, ali bi s druge strane Internet uvijek trebao ostati transparentno mjesto na kojem svi korisnici mogu naći primjerene i točne informacije.

9. Leksikon pojmova

TCP (*Transmission Control Protocol*)

Jedan od dva protokola usmjeravanja koja se koriste u Internetu, uspostavlja logičku vezu između krajnjih računala i osigurava pouzdani prijenos. TCP se nalazi na transportnom sloju OSI modela. http://www.webopedia.com/TERM/T/TCP.html

IP protokol (*Internet Protocol*)

IP je jedan od glavnih protokola u Internetu, a koristi se za usmjeravanja paketa kroz Internet. U tu namjenu, dodjeljuje IP adrese izvora paketa i njegovog odredišta na temelju kojih će se paketi usmjeravati kroz nekoliko računalnih mreža.

http://compnetworking.about.com/od/networkprotocolsip/g/ip_protocol.htm

URL (*Uniform Resource Locator)*

URL predstavlja adresu određenog resursa na Internetu. Resurs na koji pokazuje URL adresa može biti HTML dokument, slika, datoteka ili bilo koja datoteka koja se nalazi na određenom web poslužitelju.
http://searchnetworking.techtarget.com/definition/URL

HTTP protokol (*HyperText Transfer Protocol*)

Osnovna i najčešća metoda prijenosa informacija na webu. Predstavlja protokol na aplikacijskom sloju OSI modela, a osnovna namjena je prijenos HTML dokumenata (tj. web stranica). HTTP je *request/response* protokol za komunikaciju između poslužitelja i klijenta. HTTP klijent, kao što je web preglednik najčešće inicira prijenos podataka nakon što uspostavi TCP vezu s udaljenim web poslužiteljem na određenom priključku. Poslužitelj neprekidno osluškuje zahtjeve na određenom mrežnom komunikacijskom priključku (tipično priključak 80), čekajući da klijent inicira komunikaciju. - http://hr.wikipedia.org/wiki/HTTP

http://www.w3.org/Protocols/

Sigurnosna stijena (*Firewall*)

Sigurnosna stijena (engl. *Firewall*) je skup komunikacijskih nakupina koji služe kako bi odvojili privatnu mrežu od javne. Sastoje se od programa koji služe kako bi pratili i upravljali promet između računala i mreža. Sigurnosne stijene mogu propuštati, blokirati, šifrirati promet na temelju pravila koja korisnik postavlja.

http://searchsecurity.techtarget.com/definition/firewall

DNS (*Domain Name System*)

Domain Name System (DNS) je hijerarhijski sustav imenovanja izgrađen na distribuiranim bazama podataka za računala, usluge ili bilo koji resurs spojen na Internet ili privatnu mrežu.

http://www.kb.iu.edu/data/adns.html

10. Reference

[1] Wikipedia: Internet censorship,
http://en.wikipedia.org/wiki/Internet_censorship, kolovoz 2008.

[2] Reuters: Government control of Internet failing,
http://www.reuters.com/article/2007/11/14/us-internet-cerf-idUSN1420689320071114?sp=true, studeni 2007.

[3] Wikipedia: Internet censorship in the United States,
http://en.wikipedia.org/wiki/Internet_censorship_in_the_United_States, svibanj 2011.

[4] Ustav Republike Hrvatske,
http://narodne-novine.nn.hr/clanci/sluzbeni/232289.html, siječanj 2009.

[5] Wikipedia: Internet censorship in the People's Republic of China,
http://en.wikipedia.org/wiki/Internet_censorship_in_the_People%27s_Republic_of_China, svibanj 2011.

[6] Jonathan Strickland: How Internet Censorship Works,
http://computer.howstuffworks.com/internet-censorship.htm, travanj, 2011.

[7] Wayne Madsen: Internet censorship,
http://www.rense.com/general69/intercens.htm, rujan 2005.

[8] Jonathan Zittrain, Benjamin Edelman: Empirical Analysis of Internet Filtering in China,
http://cyber.law.harvard.edu/filtering/china/, ožujak 2003.

[9] Spam Laws: Glosary,
http://glossary.spamlaws.com/definition/c/, lipanj 2011.

[10] Libraryspot: Internet filters,
http://www.libraryspot.com/features/internetfilters.htm, lipanj 2011.

[11] Flossmanuals: How to Bypass Internet Censorship,
http://booki.flossmanuals.net/bypassing-censorship/_v/1.0/using-jon-do/, veljača 2011.

[12] The Kassandra Project: Internet censorship: the list of countries with no press freedom,
http://kassandraproject.wordpress.com/2008/01/29/internet-censorship-the-list-of-countries-with-no-press-freedom/, siječanj 2008.