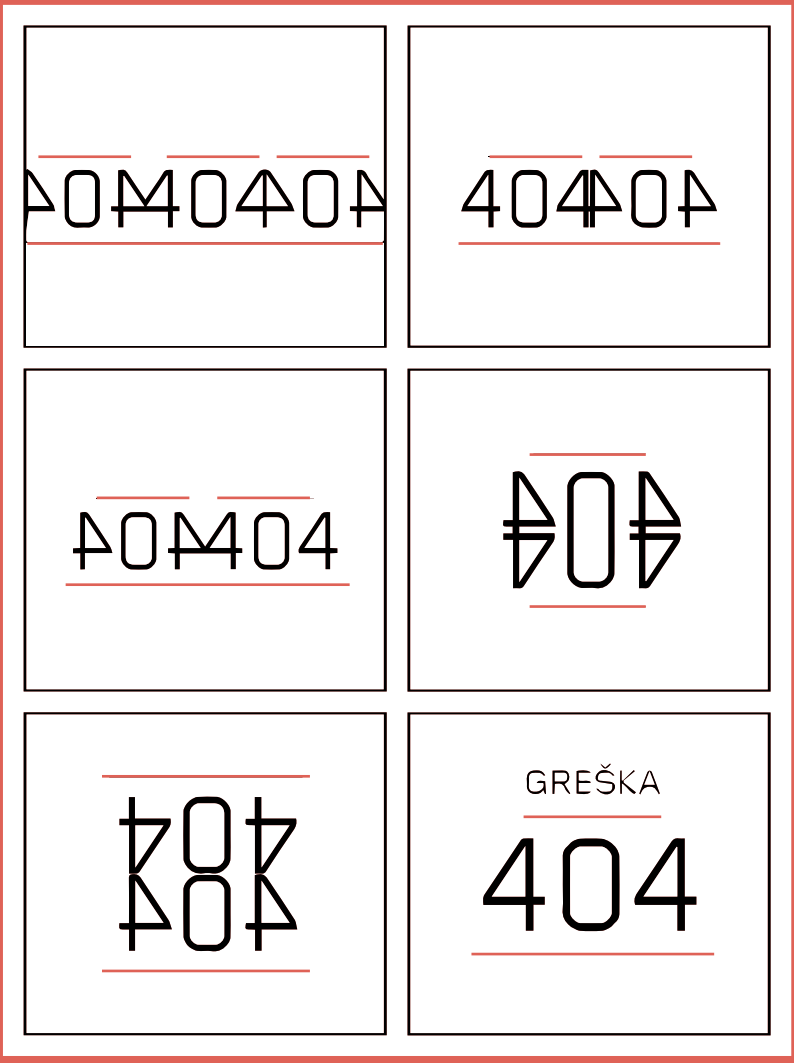
DIGITALNA PRAVA U SRBIJI

2014-2019



SHARE FOUNDATION

SADRŽAJ

Predgovor 7
O monitoringu 11
Prvih pet godina 12
Metodologija 14

Tehnički napadi 16
Hronologija 17
Specifični slučajevi 20
Svetlana Lukić 24
Branko Čečen 32
Trendovi i zaključci 38

Povrede privatnosti 40
Hronologija 41
Specifični slučajevi 44
Rodoljub Šabić 48
Trendovi i zaključci 52

Pretnje, uvrede i pritisci 54
Hronologija 55
Specifični slučajevi 58
Nedim Sejdinović 62
Sofija Todorović 68
Trendovi i zaključci 72

Manipulacije i propaganda 76
Hronologija 77
Specifični slučajevi 80
Dragana Pećo 84
Trendovi i zaključci 88

Ostale povrede 90
Hronologija 91
Specifični slučajevi 92
Trendovi i zaključci 94

PREDGOVOR

Pre samo deset godina, činilo nam se da internet ispunjava obećanje slobode. Svet se ubrzano povezivao, a pokušaji regulisanja planetarnog internet saobraćaja tretirani su kao poslednji impuls zastarelih ideja. Davne 2011. godine, SHARE je organizovao konferenciju koja je u Beograd dovela nekoliko hiljada internet entuzijasta. Bili su tu Sem Grejem-Felsen, blog-direktor prve Obamine predsedničke kampanje, Peter Sunde, osnivač portala „The Pirate Bay“, zatim Amelija Andersdoter, najmlađa poslanica Evropskog parlamenta i jedina iz redova Piratske partije, SF pisac Brus Sterling, Rafi Kaplan iz Gugla... Usledila su slična okupljanja u Novom Sadu i Rijeci, a potom u Libanu i Tunisu, poprištima borbe u kojoj se sloboda osvajala uz pomoć društvenih mreža.

Izgledalo nam je da će internet spasiti svet.

Malo ko se osvrtao na mračnu stranu tehnologije, a priče o zloupotrebama otpisivane su kao teorije zavere – sve dok 2013. Edvard Snouden, kompjuterski tehničar pod ugovorom u američkoj Nacionalnoj bezbednosnoj službi, nije otkrio da svet već uveliko nije onakav kakvom smo mu se nadali u digitalnoj eri.

Godinu dana kasnije, u Srbiji je disruptivni atak na internet bio izazvan prirodnim nepogodama – u februaru je zavejan Feketić, a u maju se čitav region našao pod vodom, uz velike ljudske i materijalne žrtve. Komentari događaja u zavejanom vojvođanskom selu i informacije o poplavama iznenada su nestajali sa interneta, nekad silom, nekad telefonskim pozivom. Neko je organizovano i planski pokušavao da briše memoriju iz digitalnog okruženja koje sve zauvek pamti.

Kako bismo uhvatili korak sa sve mračnijim izgledima budućnosti, SHARE Fondacija se transformisala u organizaciju kojoj je osnovni cilj bio da istraži nepoznato, brani ljudska prava na internetu, akumulira znanje u ovoj oblasti i uspostavi mrežu saboraca.

Uz tehnološki razvoj, ubrzavao se i razvoj alata za zloupotrebe. Države, korporacije, političke organizacije, svi su se uključili u trku za kontrolu naše svakodnevice: šta gledamo, slušamo, kupujemo, s kim se družimo, o čemu razgovaramo a šta prećutkujemo, za koga glasamo i kome doniramo - informacije o nama i našem ponašanju na internetu postale su pogonsko gorivo nove industrije, ali i strateški resurs stare politike. Afera Kembridž analitike i Fejsbuka pokazala je razmere uticaja novih tehnologija na temelje političke zajednice; pod

razornim uticajem nano-marketinga i digitalne manipulacije, građani Ujedinjenog Kraljevstva glasali su za izlazak iz Evropske unije, a građani SAD izabrali su Donalda Trampa za predsednika. Alternativne činjenice zavladale su svetom u eri post-istine, kojoj globalna povezanost samo ide na ruku.

Korak ka zauzdavanju industrije podataka preduzela je Evropska unija, najveće tržište na svetu, usvajanjem Opšte uredbe o zaštiti podataka čiji se efekti na zaštitu prava građana sa jedne, i preduzetnički duh internet inovacija s druge strane, još uvek odmeravaju.

Algoritamsko odlučivanje, veštačka inteligencija i neuralne mreže danas su novi horizont razvoja internet tehnologija. Ovog puta, prati ih daleko veći oprez korisnika, programera i javnih politika.

U međuvremenu, pravnici, umetnici, tehnički forenzičari, novinari, aktivisti i mnogi drugi, okupljeni oko vrednosti SHARE Fondacije, nastavljaju da grade slobodnu bazu znanja, uz učešće u različitim evropskim i svetskim forumima o budućnosti interneta. Sprovodimo istraživanja o infrastrukturi interneta, Fejsbukovoj algoritamskoj fabrici, pratimo globalni razvoj alata za državni nadzor građana i njihovu primenu u Srbiji. Aktivno učestvujemo u zagovaranju novih i kritičkoj analizi postojećih zakonskih predloga koji se tiču regulisanja našeg života na internetu. Upozoravamo i mobilišemo javnost u slučajevima povreda prava i sloboda građana.

Snimili smo obrazovni serijal od deset epizoda, emitovan na nekoliko televizija u zemlji i regionu. Objavljujemo priručnike o bezbednosti na internetu za istraživačke novinare, pomažemo onlajn medijima kada trpe pritiske zbog svog rada i u odbrani od sajber napada. Osnovali smo prvi poseban Centar za prevenciju bezbednosnih rizika u informacionim sistemima za onlajn medije, organizacije civilnog društva i aktiviste u Srbiji - SHARE CERT.

Uspostavili smo stalni monitoring prava i sloboda građana u digitalnom okruženju, uz redovne godišnje izveštaje o nalazima i trendovima. Publikacija pred vama upravo predstavlja presek prilika na internetu u Srbiji u prethodnih pet godina. Značaj dokumentovanja povreda digitalnih prava prepoznat je i u regionu pa od septembra ove godine, u saradnji sa istraživačkom mrežom BIRN, pratimo stanje u Bosni i Hercegovini, Hrvatskoj, Mađarskoj, Rumuniji i Severnoj Makedoniji.

Najveća zasluga za dokumentovanje 500 slučajeva povreda prava i sloboda na internetu u Srbiji, pripada našem kolegi Bojanu Perkovu koji je tokom pet

godina svakodnevno pratio najznačajnije incidente.

SHARE ne bi postojao bez svojih saradnika, široke mreže organizacija, stručnjaka i aktivista koji ulažu u znanje kao javno dobro.

Posebnu zahvalnost dugujemo Svetlani Lukić, Sofiji Todorović, Dragani Pećo, Branku Čečenu, Rodoljubu Šabiću i Nedimu Sejdinoviću na ličnom učešću u nastanku ove publikacije. Veličina njihovog doprinosa javnom dobru u Srbiji se ne može opisati rečima.

Hvala.

Danilo Krivokapić i Andrej Petrovski
Beograd, oktobar 2019.

TEHNIČKI NAPADI

HRONOLOGIJA

2014

Učestali problemi sa pristupom onlajn sadržajima primećeni su za vreme velikih poplava u maju 2014. godine, što je na neki način i podstaklo monitoring digitalnih prava i sloboda. U početku su problemima najčešće bili izloženi slabije posećeni portali, posebno oni iz manjih sredina, koji su objavljivali kritike postupaka državnih službi i javnih funkcionera tokom poplava. Tokom te godine dokumentovano je 13 slučajeva tehničkih napada na integritet onlajn sadržaja i narušavanja informacione bezbednosti. U čak 11 slučajeva mete su bili onlajn mediji, dok su napadači uglavnom nepoznati. Onesposobljavanje usluge bilo je najčešće primenjeno sredstvo tehničkih napada, i to devet puta, što odgovara najbrojnijoj potkategoriji povreda u 2014. godini, činjenje sadržaja nedostupnim putem tehničkih metoda. Uočeno je da su tehnički napadi sa ciljem onemogućavanja ili otežavanja pristupa sadržaju, često bili povezani sa konkretnim društvenim događajima, slično kao u vreme poplava. Tako su u oktobru iste godine zabeleženi napadi na srpske i albanske sajtove posle fudbalske utakmice Srbija - Albanija koja je prekinuta posle pojave drona na stadionu. Pored činjenja sadržaja nedostupnim, zabeležena su i dva primera iz potkategorije neovlašćenih izmena i postavljanja sadržaja.

2015

Tehnički napadi na onlajn medije nastavljaju se i tokom 2015. godine, kada su bili mete u 12 od ukupno 19 slučajeva, od čega pojedini i u više navrata. Mada su većinom tehnički napadi izvođeni da bi se sadržaj učinio nedostupnim, čak 14 puta, među udarima na informacionu bezbednost onlajn medija bilo je i slučajeva neovlašćenog pristupa; zabeleženo ih je šest. U jednom od tih incidenata nepoznati počinioci su ubacili diskreditujuće tekstove na sajtove dva medija. Takođe, tokom 2015. godine i nekoliko lokalnih medija našlo se na meti tehničkih napada. Tehnički pritisci su dodatni problem za medije iz manjih sredina, koji nemaju sredstava za unapređenje odbrane. Najupečatljiviji napad u toku 2015. dogodio se u aprilu, kada je potpuno onesposobljen portal „Teleprompter“, tada već izložen čestim pritiscima. Iste godine su po prvi put zabeležena dva napada iz potkategorije uništavanja i krađe podataka i programa: jednom je na meti bio onlajn medij, a drugi put istraživački novinari, kojima je bila oduzeta oprema a snimci sa nje su obrisani.

U 2016. godini, slučajevi neovlašćenog pristupa informacionim sistemima, kojih je zabeleženo osam, izjednačavaju se po broju sa incidentima u kojima je sadržaj učinjen nedostupnim. Budući da su te godine u Srbiji organizovani

2016

vanredni parlamentarni izbori, prvi put su dokumentovani napadi na političke aktere, i to iz opozicije. Medijski sajtovi su ponovo bili najčešće mete napada, tačnije u 50 posto slučajeva, dok su u dva navrata mete napada bili sajtovi organa vlasti, tačnije sajtovi predsednika Republike i Grada Beograda. Među značajnim incidentima koji su obeležili 2016. godinu izdvaja se blokiranje Tviter naloga novinara kada je nepoznat napadač pokušao da mu kompromituje nalog. Zabeležena su i dva slučaja računarskih prevara u kojima su bili targetirani građani.

2017

Tokom 2017. godine učestali su pritisci na onlajn medije kroz tehničke napade na njihove informacione sisteme: od ukupno 15 zabeleženih slučajeva iz ove kategorije, onlajn mediji su bili mete sedam puta. Jedan od zanimljivijih slučajeva tehničkih napada obrađen je kada su nepoznati napadači ubacili afirmativne tekstove u baze sajtova medija. Takođe su primećeni slučajevi računarskih prevara većih razmera, kojih je bilo četiri, a kojima su targetirani građani i državni organi, poput Narodne banke Srbije. U sva četiri incidenta korišćene su lažne imejl poruke. Upad u sistem koji je mogao da ima ozbiljne posledice po građane dogodio se u avgustu 2017, kada je meta bio server na kome su čuvane kontakt informacije i lični podaci korisnika usluga švedske kompanije koja hostuje veliki broj srpskih sajtova.

2018

Narušavanje informacione bezbednosti u 2018. godini zabeleženo je u 13 slučajeva. Mete napada bili su građani, organizacije civilnog društva, novinari i onlajn mediji. Te godine je prvi put primećen veći broj napada na organizacije civilnog društva. Kao i prethodnih godina, napadači su najčešće ostali nepoznati. Kao sredstvo napada pet puta je onesposobljen servis, a četiri puta je došlo do upada u sistem. Najviše narušavanja informacione bezbednosti svrstano je u potkategorije računarske prevare i činjenja sadržaja nedostupnim putem tehničkih metoda, po pet. Za njima slede napadi iz potkategorije neovlašćene izmene i postavljanje sadržaja, četiri puta, te onemogućavanje kontrole nad nalogom ili sadržajem, zabeležene u tri slučaja.

2019

U periodu do septembra 2019. godine značajno je smanjen broj dokumentovanih tehničkih napada. Zabeležena su svega tri incidenta, od čega su dva napadi na onlajn medije, a jedan na privatnu kompaniju. Po jedan slučaj svrstan je u kategorije neovlašćenog pristupa i činjenja sadržaja nedostupnim putem tehničkih metoda, a jedan napad obuhvatio je obe ove potkategorije.

SPECIFIČNI SLUČAJEVI

Sve korisnike interneta koji su 8. decembra 2013. godine hteli da pročitaju važnu vest na novosadskom portalu Radio 021, sačekala je ista poruka: HTTP Error 404. Takođe poznata kao '404 Not Found', ova poruka govori da traženi sadržaj ne postoji na toj adresi, ili je nekada postojao, ali je uklonjen. To se ponekad dešava sa zastarelim linkovima i stranicama koje nisu aktivne. Međutim, na ovoj adresi se nekoliko sati ranije nalazio tekst o privilegijama za kćerku guvernerke Narodne banke Srbije, Jorgovanke Tabaković.

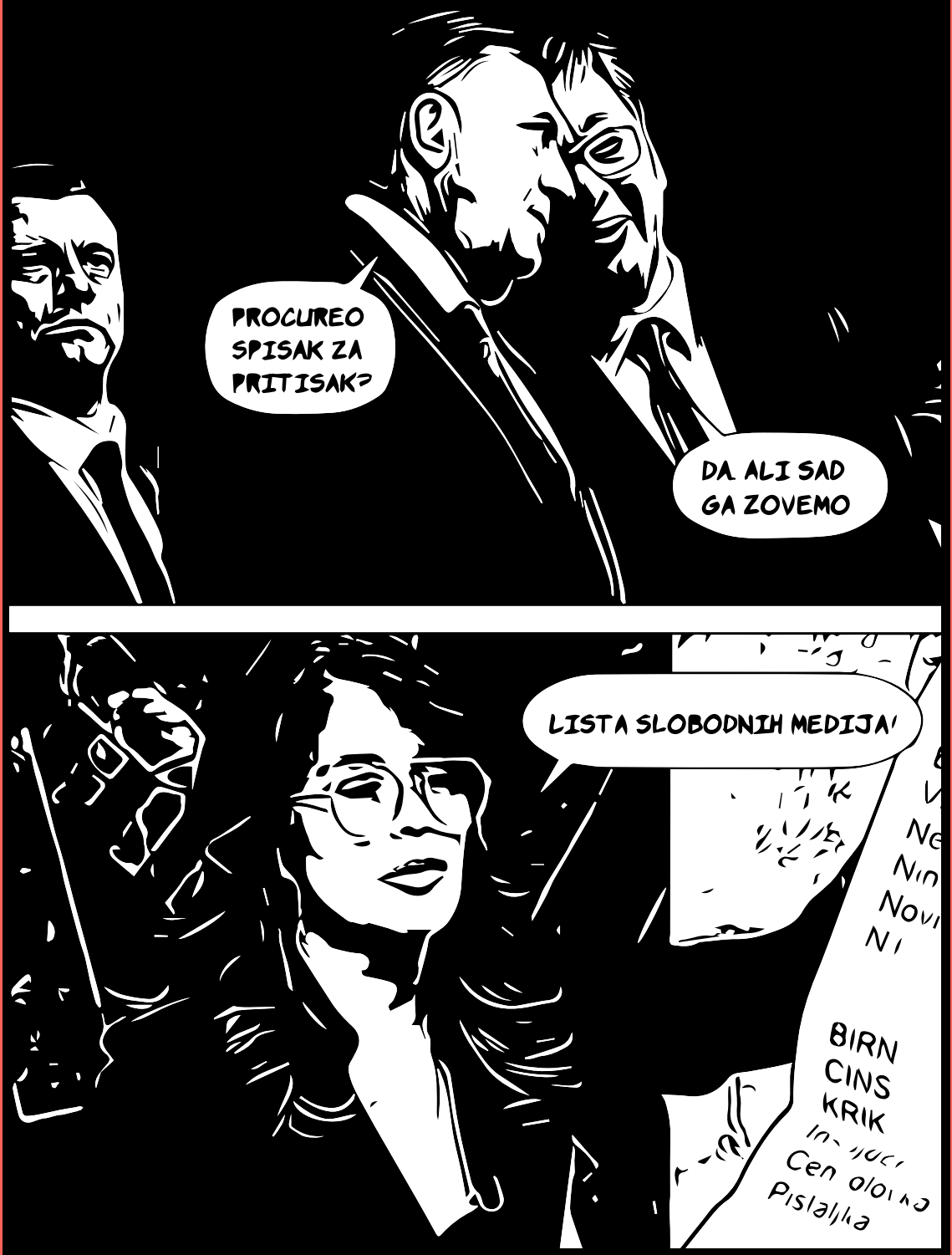
Osim na portalu 021.rs, greška 404 je umesto iste vesti korisnike čekala i na stranici alo.rs. Ispostavilo se da su ovo bili slučajevi redakcijske cenzure. Očigledna manipulacija informacijama od javnog značaja razljutila je deo onlajn zajednice i javnosti, dok se tekst viralno množio po ličnim profilima, blogovima i sajtovima nezavisnih medija. Nepoznatim nalogodavcima cenzure postalo je jasno da je potrebno pronaći neke manje direktne oblike pritiska na one koji objavljuju nepoželjne vesti.

Nekoliko hiljada inficiranih računara istovremeno je napalo servere na kojima su se nalazile stranice cins.rs i autonomija.info, a koji su takođe preneli ovu vest. Svim korisnicima interneta koji su u tom trenutku hteli da je pročitaju, pojavljivala se nešto drugačija poruka: HTTP Error 503. Karakteristična za DDoS napade, greška 503 govori da je u pitanju privremeni problem tehničke prirode, na primer da je server zbog nečega nedostupan. Za ovakve napade nisu potrebni veliki resursi i politička moć, a njihov cilj je čisto maltretiranje; sprovode se isključivo u mraku, skrivenim kanalima interneta, računajući na odsustvo odgovornosti.

Mada je u to vreme bio prilično popularan, DDoS je ubrzo pao u senku sofisticiranijih tehnika onlajn napada. Sa portala Centra za istraživačko novinarstvo Srbije (CINS) tekst o cenzuri na 021.rs konačno je uklonjen ručno, neovlašćenim i neopaženim pristupom njihovom sistemu. Par meseci kasnije, pošto je CINS objavio istraživanje o kockarnicama, otkriveni su neovlašćeni pristupi serveru, svim podacima i komunikacijama zaposlenih tokom perioda od 10 dana. Incidenti su vremenom postajali kompleksniji i teži.

Urednika portala Teleprompter su jednog jutra probudile brojne SMS poruke sa kodovima i notifikacije o promenjenim šiframa na imejl nalozima vezanim za sve privatne i poslovne servise. Obrisani su svi sadržaji na sajtu, kao i nalozi na društvenim mrežama. Analiza slučaja pokazala je da su svi dostupni sistemi zaštite bili na mestu (kompleksne šifre, multifaktorska autentifikacija i drugo), pa je sumnja usmerena ka neovlašćenom pristupu SMS-u (verovatno preko kompromitovanih službenika operatora) ili instaliranom malveru (zlonamernom softveru) u telefonu vlasnika koji bi napadaču prosleđivao poruke sa kodovima. Na sumnjama koje je nemoguće proveriti bez nadležnih organa, ostali su i mnogi drugi, misteriozni slučajevi neovlašćenih pristupa, uništavanja i krađe podataka, onemogućavanja kontrole nad nalozima i sadržajima. Dodatno, slučajevi su nepogrešivo koincidirali sa aktuelnim društveno-političkim aferama. Privatna mejl prepiska naučnice Miljane Radivojević, koja je otkrila da doktorat rektora Megatrend univerziteta ne postoji, dostavljena je medijima i objavljena uživo u programu nacionalne televizije. Nakon objavljivanja teksta „Glavni fantom iz Savamale“ Tviter nalog Nikole Tomića, urednika u nedeljniku NIN, blokiran je zbog pokušaja kompromitovanja.

Kontekst ovih incidenata jedini je putokaz u utvrđivanju motiva, a time i mogućih strana zainteresovanih da se napadi izvedu. Nedvosmislenih dokaza o nalogodavcima i napadačima nema, dok priroda tih napada i sama struktura interneta čine da nezavisni istraživači veoma teško mogu ući u trag napadačima, dobro sakrivenim iza anonimnih mreža i višestrukih IP adresa, obično kroz virtuelne privatne tunele. Istovremeno, na izabranim adresama sprskog interneta svako malo se desi možda i najpopularniji, ali i najbenigniji primer tehničkih napada u popularnoj kulturi - neovlašćena izmena naslovnih stranica (defacing). Tako se na zvaničnom sajtu Grada Beograda pojavila zastava Republike Hrvatske, na sajtu CINS-a grb OVK, a na portalu Tanjuga poruka lokalnih haktivista: „Nažalost, nismo dovoljno profesionalni da bi preneli vesti takve kakve jesu, nego moramo da izmenimo po neki video zbog hleba i igara“.


PROCUREO SPISAK ZA PRITISAK?
DA, ALI SAD GA ZOVEMO
LISTA SLOBODNIH MEDIJA!
BIRN
CINS
KRIK

2019