Sveučilište u Zagrebu

Filozofski fakultet

Odsjek za sociologiju

Diplomski rad

Kibernetička sigurnost u hrvatskim medijima: između normativnog i empirijskog

Student: Svan Hlača

Mentor: Izv. prof. dr. sc. Mirko Bilandžić

Zagreb, rujan 2018.

Sadržaj

1. UVOD

Razvoj informacijskog društva donio je prethodno nezamislivu razinu globalne povezanosti. Danas svatko ima računalo i pametni mobitel, uređaje kojima se služimo svakodnevno, kako u poslu, tako i u slobodno vrijeme. Međutim, ono što te uređaje čini posebnima je činjenica kako su cijelo vrijeme spojeni s mrežom koju dijele s više milijardi takvih uređaja s kojima mogu komunicirati u svakom trenutku. Ovakvu komunikaciju omogućila je tehnologija koja je nastala kao vojna tehnologija, ali je izašla iz okvira onoga za što je inicijalno zamišljena i postala temelj informacijskog društva.

Kako je Internet rastao i razvijao se, sve je više dolazio u ruke znanstvenika koji su željeli izgraditi utopijski sistem besplatne komunikacije za sve. Gradeći za sebe, rani Internet nisu željeli napraviti mjestom sigurnosnih propisa, već lako dostupnim mjestom namijenjenom svima. Danas je Internet potpuno otvoreni sustav na kojeg se moguće spojiti s gotovo svakim računalom ili mobitelom, a broj uređaja koji se mogu spojiti na Internet je sve veći.

Takav pristup, potpomognut globalizacijom, otvorio je put za mnoge ranjivosti u sustavu. U vrijeme kada postoji bezbroj proizvođača elektroničkih uređaja, ne postoji mogućnost stvaranja adekvatnog sustava obrane koji je u mogućnosti odvratiti napad prije no što do njega dođe. Na primjer, prijenosno se računalo sastoji od komponenata koje je proizvelo više proizvođača. Svaka od tih komponenata može u sebi imati više ranjivosti. Također, ranjivost može biti smještena i u operacijskom sustavu, ali i u bilo kojoj od bezbroj aplikacija koje se svakodnevno koriste.

Ovakvo što djeluje zastrašujuće, ali valja se zapitati je li zaista tako? Stručnjaci, mediji i ostali akteri govore o apokaliptičnim scenarijima koji samo čekaju da se dogode, međutim, nakon nešto manje od pola stoljeća od početaka razvoja Interneta, on još uvijek postoji jači no ikad.

S druge strane, pojedini autori govore o hipersekuritiziranosti ovoga pojma i tome kako stručnjaci tehnificiraju diskurs čineći ga neshvatljivim običnim korisnicima koje se primorava na poduzimanje svakodnevnih sigurnosnih praksi kako ne bi postali žrtve te time ugrozili sebe, svoje bližnje i okolinu. Tehničke sposobnosti za izvedbu takvih napada svakako postoje, ali potrebno je odrediti kolika je stvarna mogućnost da običan korisnik bude meta pomno isplaniranog napada kojeg je visoko educirana osoba pripremala više mjeseci.

Ovim se radom želi ustanoviti kako mediji u Hrvatskoj sudjeluju u stvaranju atmosfere straha pišući o mogućim prijetnjama po stanovnike. Također, analizirat će se o kakvim je tipovima prijetnji riječ, tj. kakve prijetnje mediji prikazuju. Svaka od prikazanih prijetnji će se dodatno ispitati na temelju relevantne taksonomije kako bi se ustanovilo o kojem je tipu i ozbiljnosti incidenta riječ. Svi od obrađenih incidenata biti će podijeljeni na one koji su imali izvorište ili metu napada unutar hrvatskog IP adresnog prostora te će oni koji navedeno imaju biti detaljnije analizirani. Također, na temelju relevantnih izvora biti će prikazan broj računalno-sigurnosnih incidenata u hrvatskom IP adresnom prostoru, a svaki od podtipova će biti detaljno pojašnjen na temelju relevantnih taksonomskih dokumenata.

2. INFORMACIJSKO DRUŠTVO

2.1.Što je informacijsko društvo?

Kako bi se na odgovarajući način prikazalo u kojoj je mjeri i na koji način kako kibernetička sigurnost dobivala na važnosti, valja prikazati razvoj informacijskog društva te posljedice koje je informacijska revolucija ostavila.

Informacijsko društvo nije lako definirati te postoji cijeli niz različitih pogleda na ono što ga čini. Duff (2014: 175-176), u radu koji je nastao u sklopu konferencije IADIS (*International Conference on Information Systems*), navodi da se pojam informacijskog društva može promatrati s tri različite strane te kako se, najčešće, ti različiti pogledi miješaju.

Prvi pogled temelji se na radu Daniela Bella i promatra informacijsku revoluciju kao prijelaz bogatih nacija iz proizvodnih ekonomija koje su se temeljile na proizvodnji dobara u nacije uslužnih djelatnosti koje se bave obradom i proizvodnjom informacija (Duff, 2014: 175).

Drugi pogled na informacijsko društvo svoj izvor ima u Japanu 1964[1]. godine, u nastanku pojma „johoka shakai“ (informacijsko društvo), u vrijeme kada u svijetu dolazi do eksplozije komunikacije i protoka informacija. Iako je ovaj fenomen bio globalan i svi su vjerovali kako je rast količine i protoka informacija „eksponencijalan“, u Japanu je prvi put i službeno izmjeren.

[1] Milardović navodi 1960. Međutim, usporedbom količine informacija o ovom pojmu u oba rada prednost je dana Alistairu S. Duffu.

Istraživanje je dokazalo da Japan prolazi kroz fazu „johoka“, procesa informatizacije, te postaje „joho shakai“ – informacijsko društvo. Iako se ovome ne daje veliki značaj, ostaje činjenica kako su upravo Japanci prvi izmjerili i dokazali postojanje informacijskog društva te su termin informacijsko društvo i skovali 1964. godine (Duff, 2014: 176).

Treći pogled na informacijsko društvo je i onaj najvidljiviji, a temelji se na revoluciji u informacijskoj tehnologiji koja se odigrava i danas, a koja je dubinski promijenila način na koji se informacije obrađuju i prenose te komunikaciju među ljudima.

Tehnologiju Henry Brooks objašnjava u odnosu sa znanošću na predavanju kojeg je održao na panelu “Technology and the Ecological Crisis“ što Daniel Bell (1999:118) sažima u definiciju: “tehnologija je upotreba znanstvenog znanja sa svrhom određivanja načina za obavljanje stvari na način koji se može reproducirati“. Nadalje, Castells (1998: 23, u 2000: 64) među informacijske tehnologije ubraja „konvergentni set tehnologija s područja mikroelektronike računalstva (strojevi i softver), telekomunikacija/emitiranja i optoelektronike“.

Informacijska tehnologija predstavlja jezgru za razvitak svih suvremenih tehnoloških otkrića i to na područjima razvijanja naprednih materijala, izvora energije, medicinskih primjena, proizvodnih tehnologija te transporta. Sam proces tehnološke transformacije eksponencijalno obuhvaća sve šire područje zbog sposobnosti povezivanja različitih tehnoloških područja zajedničkim digitalnim jezikom, ali i brzine napretka koja je možda najbolje sažeta u Mooreovu zakonu koji govori kako se „broj tranzistora koji se po najpovoljnijoj cijeni mogu smjestiti na čip udvostručava otprilike svake dvije godine" (Moore, 1965: 118). Naime, Castells (2010: 74) navodi kako su u 18 mjeseci, koliko je trajao period između pisanja i izdanja „Uspona umreženog društva“, mikročipovi za istu cijenu udvostručili svoju učinkovitost.

Stoga ne iznenađuje činjenica kako je pogled na razvitak informacijskog društva kroz prizmu informacijske tehnološke revolucije najdominantniji i najrašireniji, međutim, ne smije se zanemariti utjecaj što ga je ova revolucija, uz tehnološka dostignuća, imala na ekonomiju, politiku, kulturu i društvo. Duff (2014:176) zaključuje kako je nastanak informacijskog društva posljedica sinteze triju fenomena: komunikacijske eksplozije, postindustrijske ekonomije te informacijske tehnologije.

Iako temelje informacijske tehnologije možemo pronaći i prije 1940-ih godina (Bellov izum telefona, Teslin izum radija te ostali), pravi proboji u elektronici nastaju tijekom Drugog svjetskog rata i neposredno nakon njega. Razvoj tranzistora i prvog računala koje se moglo programirati predstavljaju „srce revolucije informatičke tehnologije u dvadesetom stoljeću“ (Castells, 2000: 74).

Međutim, Castells (2000: 74) napominje kako su se tek 1970-ih nove informatičke tehnologije široko rasprostranile što je ubrzalo njihov sinergijski razvoj i put prema novoj paradigmi. Naime, izumom mikroprocesora 1971. godine omogućeno je smještanje računala na čip te tim činom počinje „revolucija u revoluciji“. Inženjer Ed Roberts 1975. godine napravio je Oltar, kompjutersku kutiju čije ime potječe iz televizijske serije „Star Trek“ koja je poslužila kao temelj za razvijanje računala Apple 1 i Apple 2, prvih komercijalno uspješnih mikroračunala (Castells, 2000: 77). Sljedeći skok bilo je umrežavanje računala 1990-ih godina te dijeljenje procesorskih resursa u svrhu povećanja mogućnosti obrade podataka što je prouzrokovalo drastičan pad prosječne cijene obrade podataka.

Sposobnost umrežavanja računala omogućila je važna otkrića u telekomunikacijama tijekom 1970-ih godina, ali je tek kasnije dosegla svoj puni potencijal razvijanjem Interneta[2], javno dostupne globalne mreže koja povezuje računala i računalne mreže, tj. mreže svih mreža.

2.2.Početak i razvoj interneta

Početak Interneta možemo smjestiti u jednu od najinovativnijih istraživačkih institucija na svijetu: US Defence Department's Advanced Research Project Agency (ARPA), koja je nakon lansiranja Sputnjika, što je za američku vojsku predstavljalo značajan tehnološki udar, poduzela cijeli niz inicijativa koje su najavile informatičko doba i oblikovale svijet današnjice.

[2] U hrvatskom se jeziku vodi žustra rasprava o tome piše li se Internet velikim ili malim slovom. Iako je preporuka jezikoslovaca da se Internet u svim slučajevima piše malim slovom, akteri iza dovođenja Interneta u Hrvatsku odbijaju ovu preporuku te Internet pišu ovisno o kontekstu. Smatram kako je, u ovoj situaciji, riječ o nesporazumu i nedovoljnoj uključenosti jezikoslovaca u trenutne procese, ali i nepostojanjem želje da se zatraži mišljenje struke. U nastavku prenosim izvadak iz komunikacije s doc. dr. sc Predragom Paleom koja se odnosi na problem velikog i malog slova:
„Dozvolite samo da Vam objasnim zašto je "Internet" potrebno pisati velikim početnim slovom, bez obzira na rječnike i mišljenja jezikoslovaca. Zato jer je to ime. Naime, svaka mreža koja koristi IP protokol je "internet" s malim početnim slovom. Tako je mreža CARNet (onaj tehnički, komunikacijski dio) internet. CARNet i mnogi drugi interneti (mreze) kao što su ARNES, ACOnet, i dr. su međusobno povezani u globalnu svjetsku mrežu kojoj je ime "Internet". Dakle, kad dečki popravljaju veze u CARNet-u oni popravljaju internet, a kad Vi i ja googlamo onda pretražujemo Internet.“

U skladu s tehnološkim razvojem tijekom Hladnoga rata vrijeme pokretanja nuklearnih projektila smanjilo se s osam sati na nekolicinu minuta, ali to nije predstavljalo velike promjene zbog toga što je komunikacija između nadležnih tijela i dalje zahtijevala velike vremenske odmake. Naime, sistemi upravljanja i kontrole su i dalje bili osjetljivi za napade, a scenariji nuklearnog napada su ostavljali predsjedniku 26 sati za odgovor (Ryan, 2010: 12).

Temeljna ideja iza stvaranja Interneta bila je ideja o komunikacijskom sustavu koji je otporan na nuklearni napad, tj. sustavu koji je temeljen na komunikacijskoj tehnologiji prebacivanja paketa što je omogućavalo da mreža bude neovisna o upravnim i kontrolnim centrima zato što su paketi, jedinice poruke, sadržavale upute kako doći do primatelja te na koji način se trebaju spojiti da bi prikazale inicijalnu poruku (Castells, 2001: 10).

Prva mreža ovog tipa nazvana je ARPANET i pokrenuta je 1969. godine te je bila namijenjena za istraživače koji su radili pod okriljem Ministarstva obrane. Iako je mreža bila pod kontrolom Ministarstva obrane, znanstvenici su se njome služili za komunikaciju koju je nakon nekog vremena bilo teško razdvojiti jer se sastojala od informacija vezanih uz vojno usmjerena istraživanja, znanstvenu komunikaciju, ali i osobnu komunikaciju. ARPANET je produkt organizacije ARPA (*Advanced Research Projects Agency*) koja je, za razliku od dotadašnjih centraliziranih organizacija, djelovala kao raspršena organizacija bez vlastitog laboratorija koja je sklapala istraživačke ugovore s drugim organizacijama čime je postala središte naprednih i dugoročnih istraživačkih projekata (Ryan, 2010: 24).

Godine 1983. dolazi do razdvajanja ARPANET-a na dvije mreže. Mreža korištena za znanstvene svrhe zadržava naziv ARPANET, a mreža namijenjena vojnoj primjeni naziva se MILNET. Uz navedene, Nacionalna zaklada za znanost razvila je svoju mreže CSNET i, u suradnji s tehnološkim divom IBM, mrežu BITNET. Međutim, temelj svega bio je još uvijek ARPANET. „Mreža svih mreža“, kako se popularno naziva, oblikovana je još 1980-ih godina kao ARPA-INTERNET te je kasnije skraćena u Internet (Castells, 2001: 12).

Budući da je pri stvaranju povezane mreže računala bila riječ o raznolikim računalima potreban je bio protokol koji bi ih povezao. ARPANET je funkcionirao na temelju standardiziranog protokola NCP (engl. *Network Control Program*) koji je ostvarivao povezivanje dvaju sustava, a koji se upisivao na svako pojedinačno računalo (Abbate, 1999: 67-68).

Iako je osnova za stvaranje globalne komunikacijske mreže razvijena već tada, puni potencijal dosegnut je stvaranjem TCP/IP protokola, koji je omogućio ne samo komunikaciju putem mreže, već je omogućio šifriranje i dešifriranje podataka. Važnost TCP/IP protokola za današnji Internet je što je njegov dizajn u temelju zamišljen kako bi zadovoljio potrebe mreže otvorene arhitekture (Leiner et al., 2009: 24).

Također, TCP/IP je imao i neke dodatne prednosti kao što je činjenica kako je u danom trenutku jedini nudio neovisnost o tipu računalne opreme i operativnih sustava te o pojedinom proizvođaču. Neovisan je i o tipu mrežne opreme na fizičkoj razini i prijenosnog medija, što je omogućavalo integraciju različitih tipova mreža (Ethernet, Token Ring, X.25...). Ponudio je i jedinstveni način adresiranja koji omogućava povezivanje i komunikaciju svih uređaja koji podržavaju TCP/IP te standardizirane protokole viših razina komunikacijskih modela što je omogućilo široku primjenu mrežnih usluga (Castells, 2000: 381). Dakle, osim što je TCP/IP omogućio povezivanje različitih operacijskih sistema i računala omogućio je i povezivanje različitih mreža, te je temeljen na osnovi Interneta, otvorenoj arhitekturi, kakav je i danas (Ryan, 2010: 44).

Razvojem ovog protokola omogućeno je umrežavanje velikih razmjera za relativno nisku cijenu. Cijeli niz znanstvenika koji su radili na razvijanju Interneta, kako navodi Castells (2000: 381), ulazio je i izlazio iz institucija te je na taj način stvorena umrežena inovacijska sredina čiji su ciljevi „postali u velikoj mjeri neovisni o specifičnim zahtjevima vojne strategije ili superračunalnih linkova“. Castells (2000: 381) zaključuje: „Oni su bili tehnološki križari uvjereni da mijenjaju svijet, što su konačno i uspjeli.“

Međutim, uz napore Pentagona i onoga što Castells naziva Velike znanosti u uspostavi javno dostupne računalne mreže, u Sjedinjenim se Državama pojavila i kontrakultura koja se može povezati s odjecima pokreta 1960-ih godina, a karakterizirao ju je slobodnjački i gotovo utopijski svjetonazor. Modem je izravan rezultat rada dvojice pripadnika te kontrakulture, Warda Christensena i Randyja Suessa, koji su tehnologiju prenošenja podataka bez korištenja *host* sustava davali besplatno jer su vjerovali u koncept besplatnog i javno dostupnog komunikacijskog kanala (Castells, 2000: 381).

Uz modem, jedan od ključnih pronalazaka je i stvaranje modificirane inačice UNIX-a, višezadaćnog i višekorisničkog operativnog sustava, kojim je omogućeno povezivanje računala putem obične telefonske linije (Castells, 2000: 381).

Razvitkom povoljnog osobnog računala i javno dostupnog komunikacijskog sustava došlo je do razvijanja Bulletin Board Systema (BBS), elektroničkih oglasnih ploča koje su omogućavale svim korisnicima da slobodno komuniciraju s ostalih korisnicima mreže. Mogućnost ovog sustava prvi je put demonstrirana prilikom prosvjeda na Tian An Menu u Kini 1989. godine kada su se informacije o ovom prosvjedu širile internetom i povezale velik broj ljudi u ono što Howard Rheingold naziva „virtualnim zajednicama“ (usp. Castells, 2000: 382).

Bulletin Bord System je osnovnu ideju povezivanja računala uveo u široku populaciju čime je došlo do velikog i brzog rasta njegovih korisnika. U početku BBS je povezivao nekolicinu korisnika, te je nužan korak za povećanje broja korisnika bila nadogradnja sistema na FidoNet, globalni sistem koji je omogućavao većem broju korisnika postavljanje poruka i pozivanje istovremeno. Tri godine nakon nadogradnje, 1987. godine, BBS broji 6000 korisnika, a 1992. godine 45000 korisnika (Ryan, 2010: 69).

Castells (2000: 382) navodi „kako u njegovo vrijeme postoji tisuće takvih mikromreža koje „pokrivaju cijeli spektar ljudske komunikacije – od politike i religije, do seksa i istraživanja“. Danas se može govoriti o milijunima takvih mreža, a broj novih svakodnevno raste.

Ono što je obilježilo Internet jest činjenica kako je on oblikovan tako da bude otvoren svima i omogući širok javni pristup te otežava regulaciju prometa državnim ili komercijalnim akterima. Castells (2000: 384) zasluge za ovakav oblik vidi u činjenici kako su na razvoju radili „znanstvenici koji su htjeli postaviti novi sustav, pun tehnološke hrabrosti i svojevrstan utopijski pothvat“. Također, Castells (usp. 2000: 384) navodi kako otvorenost sustava proizlazi iz neprekidnog procesa inovacija i slobodnoga pristupa koji su potaknuli rani računalni hakeri koji su njegovali metodu „otvorenog koda“.

Međutim, ovakva otvorena arhitektura ostavila je mrežu ranjivom na najezde sofisticiranih uljeza. Slučaj kojeg Castells izdvaja, a predstavlja kanon među hakerima i stručnjacima za kibernetičku sigurnost je svakako slučaj Kevina Mitnicka (usp. Castells, 2000: 385, Littman, 1996).

Kevin Mitnick, jedan od najpoznatijih hakera na svijetu, uhićen je 1995. godine nakon što je Tsutomu Shimomura, stručnjak za kibernetičku sigurnost, otkrio da je netko kompromitirao njegove zaštićene podatke koji se nalazili u tvrtki San Diego Supercomputer Center (Mitnick, 2012: 147). Shvativši napad kao profesionalnu uvredu, Shimomura kreće u lov na hakera te nakon nekoliko tjedana javlja FBI-u gdje se Mitnick nalazi. Castells (2000: 385) navodi kako je ovaj „javno objavljen događaj naglasio teškoću zaštite informacija na mreži". Međutim, Castells ne iznosi informaciju koja možda najbolje ocrtava položaj hakera i strah koji je ovakvo korištenje interneta utjeralo u kosti državnim akterima. Naime, sam Mitnick u više izvora često navodi kako je prilikom sudskog spora tužitelj rekao sucu kako smatra da Mitnick ne smije dobiti mogućnost plaćanja jamčevine te kako mu treba ograničiti pristup telefonu jer može nazvati NORAD (North American Aerospace Command) te fućkanjem pokrenuti lansiranje interkontinentalnih balističkih projektila. Mitnick je godinu dana proveo u samici zbog straha i nerazumijevanja tehnologije od strane državnih tijela (Current Channel, 2017)

Castells također ne izdvaja kao važnu činjenicu kako je Mitnick uhićen isključivo zato što je drugi haker odlučio pokrenuti svoju istragu. Sam Mitnick također napominje kako je svaki put kada je uhićen to bila zasluga ili suradnika koji je informacije o njemu prenio policiji ili stručnjaka poput Shimomure. Sam FBI mu nije mogao ništa (Tonton Cypher, 2017)

Upravo ovaj strah i potpuno nerazumijevanje zaslužni su za eksploziju važnosti kibernetičke sigurnosti u svijetu. Hakeri odjednom od štrebera koji vole popularnu kulturu postaju najtraženiji svjetski zločinci sposobni uzrokovati potpuno uništenje svijeta fućkanjem.

3. KIBERNETIČKI PROSTOR

3.1. Razvoj kibernetičkog prostora

Pojam kibernetika (starogrčki: kubernētikós – dobar upravljač, dobro upravljanje) prvi se put spominje u kontekstu znanosti o samoupravljanju o kojoj raspravljaju Platon i Alkibijad kako bi naznačili važnost upravljanjem ljudima. Sličan pojam, *cybernétique*, 1834. godine koristi André-Marie Ampère kako bi označio znanosti o upravljanju unutar svoje klasifikacije ljudskog znanja (Shen Tsien, 1954: 7).

Rast popularnosti ovoga pojma pripisuje se Norbertu Wieneru, jednom od pionira informacijskog društva, koji 1948. godine izdaje knjigu „Cybernetics: Or the Controland

Communication in the Animal and the Machine“ koja kibernetiku definira kao znanost o kormilarenju ili upravljanju i prijenosu informacija (Wiener, 1948: 14-19). Dvije godine kasnije, Wiener nadopunjava svoju definiciju kibernetike u knjizi „The Human Use of Human Beings“ te se ona sada odnosi na teoriju prijenosa poruke između ljudi i strojeva (prema Milardović, 2010: 91).

Godine 1950. Alan Turing, britanski matematičar, logičar i kriptograf zaslužan za, među ostalim, i dešifriranje poruka koje su šifrirane uređajem Enigma, za kojeg se slobodno može reći kako je jedan od otaca modernog računarstva, objavljuje knjigu „Computing Machinery and Intelligence“ koja postavlja temelje umjetne inteligencije. Godine 1962. Douglas Engelbart objavljuje „Augmenting Human Intellect: A Conceptual Framework“ u kojoj razmatra mogućnosti veće ljudske intelektualne učinkovitosti u pomoć računala. Milardović ovdje postavlja prekretnicu nakon koje se računalo pojavljuje kao novi medij u komunikaciji među ljudima te izdvaja knjigu „Understanding Media: The Extensions of Man“ Marshalla McLuhana iz 1964. godine u kojoj se mediji, i novi i stari razmatraju kao ljudske ekstenzije (prema Milardović, 2010: 92).

Međutim, prekretnicu u razvitku *cyber* kulture, koja se temelji na simulaciji stvarnosti i novim medijima, predstavlja *cyber punk*, pokret koji se javlja početkom 1980-ih godina kao kontrakulturni pokret koji budućnost vidi kao distopiju te kritizira tehnokratsko društvo. Sam sadržaj i odrednice *cyberpunka* snažno su obojane književnošću, filmovima i novim medijima. Valja izdvojiti Vernora Vingea koji objavljuje novelu „True Names“ u kojoj se spominju virtualni svjetovi i umjetna inteligencija. Ova novela prethodi jednom od kanonskih djela *cyber punka*, „Neuromanceru“ Williama Gibsona koji je objavljen 1984. godine, a relevantan jer je se na više mjesta spominje matrica, mreža, čip, softver, ali i zbog činjenice kako se pojam „kibernetički prostor“ izvorno pojavljuje upravo u ovom romanu (Nikodem, 2009: 112). Također, razmatra se spajanje čovjeka sa strojem, računalni virusi, umjetna inteligencija, moć velikih korporacija. Sam koncept *cyberspacea* ili kibernetičkog prostora pripisuje se Gibsonu, a odjeci ove knjige vidljivi su u kasnijim djelima *cyber punka* poput filmova kao što su Hakeri, Matrix i Ghost in the Shell, a koji predstavljaju kanonska djela *cyber punka* i *cyber* kulture općenito. Kako navodi Nikodem (2009: 110) pojam *cyber* kulture „… odnosi se na kulturna pitanja povezana sa

'cyber temama', kao što su virtualna stvarnost i kibernetički prostor, digitalna revolucija, računalno posredovana komunikacija, kiborg, cyberpunk, poslijeljudsko i sl.“.

Godine 1985. Richard Stallman objavljuje „The GNU[3] Manifesto“ (Stallman, 1985: 30-36). Ovaj manifest govori o filozofiji „slobodnog softvera“[4] i predstavlja nastojanja *cyber* pokreta za slobodnu distribuciju i korištenje softvera. S jedne strane utopijski prikazuje budućnost razvoja tehnologije, ali s druge strane upozorava na tamnu stranu tehnologije i mogućnost distopijske budućnosti. Možda ovakva razmišljanja najbolje ilustrira citat iz manifesta:

> „Zaključno, prestat će razmatranja o tome tko je vlasnik softvera i tko ima kakvu dozvolu za rad s njime. Sporazumi kojima se korisnike želi primorati da plate softver, što uključuje i licenciranje kopija, uvijek uključuju velike troškove za društvo u obliku složenih mehanizama kojima se želi odrediti koliko jedna osoba mora platiti za softver. A jedino policijska država može prisiliti sve na plaćanje. Zamislite svemirsku postaju u kojoj se zrak proizvodi mukotrpno i dugotrajno. Plaćanje zraka definitivno dolazi u obzir, međutim, nošenje maski koje broje koliko smo točno udahnuli nije moguće tolerirati čak i kada bismo svi imali dovoljno za plaćanje. K tome, video kamere nadgledaju sve kako bi vidjeli skida li netko masku. Uvijek je bolje podržati pogon za proizvodnju kisika s univerzalnim porezom bez obzira na potrošnju i baciti nepotrebne maske.“

Godine 1986. autor pod pseudonimom The Mentor objavljuje „Hacker Manifesto – The Conscience of Hacker“ (The Conscience of a Hacker, 2005). Iza pseudonima stoji američki haker i sigurnosni stručnjak Loyd Blankenship koji je bio član tada poznatih hakerskih skupina Extasy

[3] Priča oko naziva GNU je zanimljiva te ilustrira razliku između zaljubljenika koji su stvarali prve računalne sustave i oblikovali informacijsko-komunikacijske tehnologije kakve su danas te velikih korporacija i državnih službi koje su htjele ograničiti razvoj Interneta te stati na kraj politici „otvorenog koda“. Naime, GNU je računalni sustav sličan Unixu kojeg su razvili zaposlenici tvrtke AT&T u nezavisnom laboratoriju „Bell Labs“ tvrtke United States Bell System krajem 70-ih godina. Za razliku od UNIX-a, GNU, čiji je naziv rekurzivna kratica za „GNU's Not Unix“, je potpuno besplatan i javno dostupan. Također, od 1984. godine je u stalnom razvoju te je postao komponenta operativnog sustava Linux. Zanimljivo je napomenuti da je operativni sustav Linux potpuno besplatan, ali se smatra i najsigurnijim operativnim sustavom na kojem svakodnevno rade računalni stručnjaci te ga dodatno usavršavaju. Činjenica kako je Linux, kao najsigurniji operativni sustav, plod volonterskog rada zajednice, možemo reći cyber punkera, a ne velikih koorporacija ili državnih tijela govori mnogo o zajednici koja je gradila informacijsko-komunikacijski sustav današnjice.

[4] Stranica GNU.org donosi definiciju: „Slobodni softver je softver koji poštuje korisničku slobodu i zajednicu. Ugrubo, to znači da korisnik ima slobodu pokrenut, umnožiti, raspačavati, proučavati, mijenjati i poboljšavati softver. Ukratko, slobodni softver nije pitanje cijene, već slobode. U zajednici se katkad naziva i „libre software“ prema francuskom ili španjolskom kako bi se dodatno ukazalo da softver nije gratis. Sloboda omogućava korisniku da kontrolira program i radi s njime što hoće. Kada korisnik nema ovu mogućnost, govorimo o „nebesplatnom“ ili „vlasničkom“ programu. „Nebesplatni“ program upravlja korisnikom, tj. razvojni programer upravlja korisnikom, a to program čini alatom u neravnopravnoj raspodjeli moći.“

Elite i druge generacije skupine Legion of Doom. Napisan je nakon autorova uhićenja i objavljen u časopisu Phrack, a predstavlja jedan od temelja hakerske kulture. Manifest predstavlja etički kodeks hakera i naglašava kako haker treba nadjačati sebične potrebe za iskorištavanjem drugih ljudi te kako tehnologija služi za širenje horizonta i za očuvanje slobode. Manifest se također obračunava sa starim državnim garniturama koje ne razumiju hakere i njihov pogled na svijet: „Jesi li ikada, u trodijelnoj[5] psihologiji i tehnomozgu 1950-ih godina, pomislio što se nalazi iza očiju hakera?“. Manifest zaključuje proglasom:

> „Ovo je moj svijet sada… Svijet elektrona i prekidača, ljepote bauda[6]. Mi stvaramo i besplatno koristimo uslugu koja već postoji i koja bi bila jeftina da ju ne vode neumjereni profiteri koji nas nazivaju kriminalcima. Istražujemo… I zovete nas kriminalcima. Tražimo znanje… I zovete nas kriminalcima. Postojimo bez boje, nacionalnosti i religije… I zovete nas kriminalcima. Gradite atomske bombe, vodite ratove, ubijate, varate, lažete nam i želite da u to vjerujemo za svoje dobro. I opet smo mi kriminalci.
>
> Da, kriminalac sam. Moj je zločin radoznalost. Moj je zločin što sudim ljude prema onome što kažu i misle, a ne na temelju toga kako izgledaju. Moj je zločin u tome što sam pametniji od vas, a to je nešto što mi nikada nećete oprostiti.
>
> Ja sam haker i ovo je moj manifest. Možete zaustaviti ovu individuu, ali nas ne možete zaustaviti sve… Na kraju krajeva, svi smo mi isti.“

Par godina kasnije, 1996. godine, izlazi bitna deklaracija, „A Declaration of Independence of Cyberspace“ (A Declaration of the Independence of Cyberspace, 1996), koju piše John Perry Barlow, utemeljitelj organizacije Electronic Frontier Foundation, organizacije čiji je cilj zaštita slobode govora na Internetu, a koja je objavljena u gradu Davosu u Švicarskoj (Barlow, 1996: 365-7). U Deklaraciji se autor obraća vladama industrijskog svijeta, „oronulim divovima mesa i čelika“ iz *Cyberprostora*, „novog doma Uma“ i poručuje im kako oni u tom novom prostoru nemaju prava ni suvereniteta. Prema Deklaraciji, stanovnici tog novog prostora nemaju vladu, niti

[5] Uobičajeni internetski sleng. Three Piece se odnosi na trodijelno odijelo prema Collinsovu rječniku engleskog jezika, a Urban dictionary, relevantni rječnik internetskog korpusa, navodi kako se korištenje ovog frazema odnosi na „bogatog kradljivca ili prevaranta“, tj. na osobu koja se nalazi na visokoj poziciji te zloupotrebljava svoju poziciju.

[6] Baud (po prezimenu izumitelja J. M. Baudota; znak Bd), posebna jedinica za brzinu prijenosa informacije; 1 baud znači jedan znak (informacijski element) u sekundi; poseban je naziv recipročne sekunde (Bd = s–1). Pri prijenosu binarnog signala Bd = bit/s.

će je ikada imati, a autor se ostatku svijeta obraća bez autoriteta većeg od slobode. Objavljuje kako će globalni društveni prostor koji grade biti slobodan od tiranije koju im žele nametnuti te upozorava kako ne postoji metoda koje bi se stanovnici tog novog svijeta mogli bojati. Autor pojašnjava kako upravljanje izvire iz pristanka kojeg vlade nisu dobile te ga nikada ni neće dobiti: „*Cyberprostor* ne leži unutar vaših granica. Nemojte misliti da ih možete izgraditi kao nekakav javni projekt. Ne možete. On je čin prirode i raste sam kroz naše kolektivne akcije“ (Barlow, 1996).

Autor navodi da vlade nikada nisu sudjelovale u diskursu iz kojeg je Internet nastao, niti su stvarale bogatstvo na ovom novom tržištu. Zamjera im što ne razumiju njihovu kulturu, etiku i nepisana pravila koja donose više od bilo kojih propisa koje bi im željeli nametnuti. Također ih proziva zato što tvrde kako među novom zajednicom postoje problemi koje treba riješiti, a koje koriste kao izliku kako bi prikrili svoj ulazak u *cyberprostor*, iako mnogi od tih problema ne postoje. Prave konflikte ćemo sami riješiti, poručuje autor, prema društvenom ugovoru kojeg smo sami stvorili (Barlow, 1996).

Ovaj manifest, uz prethodne, jasno ocrtava položaj grupe koju možemo nazvati „*cyber* urođenicima“ spram velikih aktera poput država i korporacija koji žele kontrolirati *cyber* prostor i *cyber* kulturu. Ograničenjima koje veliki akteri žele nametnuti autor izvor vidi u strahu. Autor smatra kako zbog nemogućnosti ograničenja prostora, nije moguće ograničiti ni razvoj *cyber* kulture koja promiče, kako Milardović navodi, „antiregulacijski stav u odnosu vlada spram *cyber* prostora i *cyber* kulture.“ (Milardović, 2010: 94).

3.2. Društvo rizika i kibernetički prostor

Tehnologija, tehnika, alati i strojevi oduvijek su imali funkciju u odnosima moći između pojedinaca i društvenih skupina. Milardović navodi kako Mumford (usp. Milardović, 2010: 134) govori o tome kako svaki napredak u globalnom informacijskom društvu nosi „različite rizike kojih nismo svjesni ili ih nismo još tako duboko promislili“. Danas na vrhuncu tehnološke i strojne evolucije stoji računalo, novi mediji te ljudi koji generiraju društvo rizika zloupotrebom i instrumentalizacijom tehnologije.

Luhmann smatra da je rizik neodvojiv od odluke te kako odluke, koje mogu biti racionalne, neracionalne i iracionalne, u različitim područjima ljudskog djelovanja, mogu,

posredstvom tehnologije, generirati rizike (prema Milardović, 2010: 137). Suočavanje s rizikom podrazumijeva stvaranje prevencije i prelazak fenomena iz nepolitiziranosti u politiziranost te, na koncu, sekuritizaciju. Što, kada i na koji način postaje rizikom određuju interesne skupine koje imaju moć govornim činom nešto smjestiti u rizik, tj. sekuritizirati te na taj način učiniti rizik, kako navodi Milardović, problemskim sadržajem programa političkih stranaka, udruga civilnih društva, međunarodnih korporacija te ostalih aktera. Rizici su otvoreni za društvene procese definiranja jer ih se može umanjivati, uvećavati, sakrivati i naglašavati, a ključne društvenopolitičke pozicije koje definiraju rizik zauzimaju upravo znanost, mediji i vlast (prema Beck, 2001: 36).

Beck napominje kako je rizik neizbježna stvarnost modernizacije i napretka te kako je u korelaciji s tehnoekonomskim napretkom. Zaključuje kako se rizici ne mogu smjestiti u okvir nacionalnih država te kako danas govorimo o globalizaciji rizika i o globalnom ili svjetskom društvu rizika upravo zbog premreženosti svakog aspekta ljudskog djelovanja (Beck, 2001: 36).

Suvremeno je društvo, prema Becku, društvo rizika u kojem rizici uzrokuju izvanredno stanje, tj. društvo katastrofe i izvanrednog stanja te kao takvo zahtijeva reorganizaciju moći i vlasti te uspostavu mehanizama za upravljanje rizicima, a u kontekstu informacijskog društva ti mehanizmi moraju biti globalni (Beck, 2001: 37).

Beck nastavlja te nadopunjuje kako društvo rizika nije samo društvo katastrofe već kako je „društvo rizika u tom smislu i društvo znanosti, medija i informacija“ (Beck, 2001: 69) zato što su modernizacija te informacijska revolucija koja joj je prethodila u temelju razvitka znanosti, medija i informacija, ali u isto vrijeme izvor rizika.

Rizike modernizacije Beck vidi kao „big bussiness“ jer su nezasitni i samoproducirajući. Luhmann (1990: 230) navodi kako s rizicima privreda postaje samoreferencijalna jer je nezavisna od okruženja u kojem se zadovoljavaju ljudske potrebe. Beck zaključuje kako „s ekonomskom eksploatacijom rizika, koji se tako oslobađaju, industrijsko društvo proizvodi opasnosti i politički potencijal rizičnog društva“ (Beck, 2001: 37).

Međutim, konstatacija rizika i određivanje nečega rizičnim, je forma u kojoj, prema Becku, etika, filozofija, kultura i politika uskrsavaju unutar centara modernizacije – ekonomije, prirodnih znanosti i tehnologije. U ovoj nerazvijenoj simbiozi između prirodnih i društvenih

znanosti, nalaze se još i svakodnevne racionalnosti te racionalnosti eksperata, interesa i činjenice (usp. Beck, 2001: 44).

Upravo ovakav oblik simbioze pretpostavlja usuglašeno djelovanje različitih i raznorodnih disciplina, skupina građana, poslovnog sektora, administracije i politike, ali je vjerojatnije, kako Beck zaključuje, da se u međudjelovanju konstatacije rizika dezintegriraju u proturječne definicije i sukobe oko pojmovnog određivanja (Beck, 2001: 44).

Posljedica ovakvog procesa jest rušenje monopola što ga znanost ima nad racionalnošću. Upravo je znanost, baveći se civilizacijskim rizicima, napuštala svoju osnovu eksperimentalne logike i ulazila u „poligamski brak s privredom, politikom i etikom ili preciznije: 'one žive s njima u nekoj vrsti „trajnog braka bez vjenčanog lista'" (Beck, 2001: 45).

Iz ovakvog uređenja proizlazi, prema Becku (2001: 49), kako društveni efekt definicije rizika ne ovisi od njihove znanstvene održivosti već o „dobrim" argumentima ili argumentima koji mogu „proći" u javnosti. Međutim, ovakvo uređenje onemogućava izdvajanje pojedinačnih uzroka i odgovornosti zbog sustavne međuovisnosti visokospecijaliziranih aktera modernizacije u privredi, pravu i politici.

Također, Beck ističe kako se rizici ne iscrpljuju u efektima i oštećenjima što su već nastupila. Rizici dolaze s budućom komponentom koja se temelji na produžavanju trenutno sagledivih oštećenja u budućnosti, a dijelom na općem gubitku povjerenja ili na pretpostavljenim „pojačivačima rizika"(Beck, 2001: 50). Centar svijesti o riziku ne nalazi se više u sadašnjosti nego u budućnosti. Prošlost gubi snagu koju je imala i koja joj je dozvoljavala da odredi sadašnjost te na njeno mjesto dolazi budućnosti. Dolaskom budućnosti na poziciju s koje može određivati sadašnjosti dolazi i, kako Beck navodi, nešto nepostojeće, iskonstruirano, fiktivno, nastalo kao posljedica sadašnjeg iskustva i aktivnosti (Beck, 2001: 51).

Čovjek djeluje danas kako bi proaktivnim i preventivnim djelovanjem spriječio, ublažio i otklonio probleme i krize sutrašnjice. Međutim, Beck tvrdi kako u raspravama što ih vodimo oko budućnosti imamo posla „s jednom „projektiranom promjenom" s „projektiranim uzrokom" trenutnog, osobnog ili političkog, rada. Ovakav pristup podrazumijeva rast relevantnosti i značaja ovih promjena zajedno s njihovom nepredvidljivošću i opasnošću te nalaže planiranje kojim valja odrediti i organizirati sadašnje aktivnosti" (Beck, 2001: 51).

Kako su rizici dobra čije se nepostojanje pretpostavlja sve dok se ne opozovu, u skladu s motom „in dubio pro progres“, nema potrebe za procesom društvenog priznavanja, odnosno, rizici se mogu legitimirati time što se njihova proizvodnja nije vidjela ni željela. U svijetu kibernetičke sigurnosti ovo izvrsno predstavlja ranjivost nultog dana ili „zero-day“ ranjivost. Ova ranjivost je ranjivost u softverskom paketu koja nije poznata onima koji su softverski paket razvili, od „freelance“ razvojnih programera do globalnih korporacija kakve su Microsoft, Alphabet, Oracle, Adobe i Apple. Kada se za ovu ranjivost sazna, korporacija objavi zakrpu kojom korisnici otklanjaju ranjivost koja se nalazi u njihovom sustavu i koja omogućava kompromitaciju istog. Na primjer, korporacija Oracle jasno navodi kako neće pružati dodatne informacije o poznatim ranjivostima osim osnovnih informacija koje dolaze uz zakrpe, upozorenja, razne poruke i zakonske spise. Također, Oracle će svim korisnicima pružiti jednake informacije kako bi ih jednako zaštitio. Na kraju, Oracle navodi kako neće pružati informacije o napretku otklanjanja ranjivosti pojedinačnim korisnicima te kako ne razvija niti ne distribuira aktivne ranjivost za njihove proizvode (Oracle, 2018). Svakako valja izdvojiti kako uz proizvod dolazi i podrška za sve ranjivosti koje će se moći iskoristiti u budućnosti, ali kako odgovornost za nastalu štetu nikako nije na korporaciji.

Kao što je pokazano u slučaju s tvrtkom Oracle, rizici u modernizaciji, prema Becku, razvijaju i jedan izjednačavajući efekt unutar svog dometa i među onima koje pogađaju te ovdje Beck nalazi njihovu političku snagu. „Rizična društva nisu klasna društva, a rizični položaji pojedinca ne mogu se shvatiti kao klasni položaji, niti se njihovi konflikti mogu shvatiti kao klasni konflikti“ (Beck, 2001: 55).

Ovaj je fenomen puno razvidniji kada se predoči poseban model raspodjele rizika modernizacije. Naime, rizici „posjeduju imanentnu tendenciju k globalizaciji“ (Beck, 2001: 55), a to je posebno točno za informacijsko društvo kojim upravlja malen broj tehnoloških divova koji su, u svom dosegu, globalni.

Na ovome tragu, operativni sustav Android koriste jednako uređaji od 50 američkih dolara i oni mnogo skuplji, a on čini 85,9% globalnog tržišta mobilnih uređaja. U 2017. godini krajnjim je korisnicima prodano 1,54 milijarde novih uređaja, a Google je iste godine objavio kako, na mjesečnoj razini, ima 2 milijarde aktivnih uređaja koji koriste neku od inačica operativnog sustava Android (Statista, 2018). Rizik u dobu refleksivne modernosti ovisi o srži

odluke, a rizik postaje rizičan u trenutku kada se o njemu odlučuje. Pokušaji upravljanja rizikom, koji prate odluku o riziku, na koncu vode do gubitka kontrole nad mogućnostima upravljanja rizikom (Williams, 2008: 63). Umanjivanje jednog rizika mehanizmima kontrole može voditi u potpuno novi rizik koji inicijalno nije bio predviđen, a sam po sebi može imati veće posljedice od rizika iz kojeg je nastao (Williams, 2008: 63).

Efekt bumeranga po kojem sami akteri modernizacije zapadaju izrazito i konkretno u vrtlog opasnosti koje oni sami stvaraju i od kojih profitiraju, o kojem govori Beck, nije toliko vidljiv u kontekstu informacijske sigurnosti, ali je vidljiv u informacijskom društvu (usp. Beck, 2001: 55). Slučaj baterija sklonih eksploziji svakako nije koristio Samsungu te je ovaj slučaj uvelike utjecao na popularnost njihovog proizvoda u svijetu. Doduše, kriza nije dugo trajala te je gotovo i zaboravljena, a Samsung nastavlja s izbacivanjem novih uređaja na svjetsko tržište (Tsukayama, H., 2018).

Štoviše, katkad se nastali incidenti koriste kako bi se progurala neka inovacija ili postavio novi sigurnosni standard, čak i u slučajevima kada incidenti nemaju veze s npr. zastarjelim operativnim sustavom. U trenutku pisanja rada pojavila se vijest (Ž. L., 2018) o tome kako je Microsoft objavio kako su Rusi izveli hakerski napad na američki Senat te kako pokreće novu specijaliziranu uslugu za zaštitu i *cyber*-sigurnost, nazvanu AccountGuard koju će ponuditi organizacijama koje koriste uslugu Microsoft Office365 u sklopu svog programa „Defending Democracy“, bez dodatnih naknada.

Uvidom u opis incidenata i tehnika koje su korištene prilikom napada, jasno se da zaključiti kako je riječ o podtipu socijalnog inženjeringa koji se zove *spear-phishing*[7] i koji ovisi o tome da žrtva povjeruje napadaču koji se izdaje kao legitimna osoba. Umjesto programa osvještavanja o riziku što ga informacijski sustavi i povezane usluge nose, Microsoft je ponudio uslugu čija su tri glavna cilja prikupljanje velike količine informacija kako bi sagledali „veliku sliku“, obavještavanje političke organizacije u slučaju da njihov član bude metom državno potpomognutog napada i rad s organizacijama koje su najosjetljivije na državno potpomognute napade (Burt, T., 2018).

[7] *Phishing* – prema nekim izvorima iz engleskog izvornika *fishing* – pecanje. Utjecaj *cyberpunka* vidljiv je u zamjeni slova f slovima ph. Riječ je o uobičajenoj praksi *cyberpunka* te su neki od utemeljitelja na sličan način pisali svoje aliase npr. Phiber Optik.

Iako je njihov servis korišten u napadu, nisu osviješteni rizici neodgovornog korištenja tog servisa, već se nude dodatne usluge koje će umanjiti postojeće i dokazane rizike koje taj servis nosi. Ove nove usluge prikazuju se kao inovacija i dodatan korak u sigurnosti informacijskih sustava, ali premještaju naglasak s činjenice da je meta uvijek stvarni čovjek, bez obzira na to koliko se sigurnosnih mehanizama i vatrenih zidova nalazilo između njega i napadača.

Kako Beck (2001: 68) navodi, u negiranju i neopažanju nastaje „objektivno zajedništvo globalnog položaja ugroženosti“. Stvarnost rizika koji više ne poznaje društvene i nacionalne razlike i granice raste, međutim, sakrivena je iza mnogih interesa. Rizik je, u razvijenom tržišnom društvu, dvojak. On predstavlja rizik, ali i tržišnu šansu. Razvitkom rizičnog društva produbljuje se jaz između onih koji su pogođeni rizicima i onih koji od rizika profitiraju (Beck, 2001: 69).

„Na sličan način raste i društveni i politički značaj znanja, a s njim i mogućnost medija da se znanje oblikuje znanošću i istraživanjem te da se širi masovnim medijima... Rizično društvo postaje društvo znanosti, medija i informacija te stvara antagonizme između onih koji stvaraju definicije rizika i onih koji ih konzumiraju.“ (Beck, 2001: 69).

Oni koji rizike konzumiraju postaju ovisni o eksternom znanju onih koji stvaraju definicije rizika tj. pogođeni rizicima postaju nekompetentni za stvari koje se tiču njihove vlastite pogođenosti. Na ovaj način, kako Beck zaključuje, gube bitan dio svoje kognitivne suverenosti (usp. Beck, 2001: 79).

Štetno se nalazi svuda oko nas i stalno vreba, a oni koji su najsnažnije pogođeni rizikom, nemaju vlastite sposobnosti prosuđivanja je li nešto neprijateljsko ili prijateljsko te ovise o pretpostavkama i metodama producenata eksternog znanja, postaju ranjivi. Kako navodi Furedi (2008:108), svijet postaje daleko opasniji ako se jastvo doživljava kao bespomoćno i ranjivo, tj. nesposobno za vlastito prosuđivanje.

Beck zaključuje „kako se u rizičnim položajima stvari iz svakodnevnog života mogu, takoreći preko noći, pretvoriti u 'trojanske konje' iz kojih iskaču opasnosti, a s njima i eksperti za rizike koji u svađi jednih s drugima objavljuju čega se treba plašiti, a čega ne“ (Beck, 2001: 79).

Furedi (2008: 107) navodi kako se kognitivna suverenost onih koji rizike konzumiraju gubi na temelju vjerovanja kako je pokušaj ljudi da preuzmu vlastitu sudbinu u svoje ruke

nerealan i vrlo opasan. Takvi postupci, oblici ponašanja i vrijednosti, koji su povezani s preuzimanjem rizika, eksperimentiranjem ili pokušajem ovladavanja svojom sudbinom, izvrgavaju se kritici kao negativni oblici ponašanja. Kulturu straha, kako piše Furedi (2008: 171), prožima duboki osjećaj bespomoćnosti, osjećaj smanjene mogućnosti djelovanja koja ljude nagoni da postanu pasivni subjekti koje ne mogu činiti ništa drugo osim žaliti se i reći „bojimo se“.

„Kada bi ljudi samo znali ono što znaju tehnički stručnjaci i kako oni misle, umirili bi se – inače su upravo beznadno iracionalni“ (Beck, 2001: 85), govori Beck i ovakvo shvaćanje označava kao pogrešno jer odvaja eksperte i ne-eksperte. Eksperti vide ostatak svijeta očima tehnološke elite koja gleda „studenta tehničkog fakulteta u prvom semestru“ (Beck, 2001: 84). Dobre je volje, trudi se, ali nema pojma i, kako bi Furedi rekao, predstavlja ranjivost. Kada bi posjedovao dovoljno znanja, priključio bi se gledištu i procjeni eksperata te bi i sam zauzeo takav stav.

Međutim, nedostatak znanja i naslućivanje kako spoznaja, tj. ovladavanje znanjem što ga eksperti imaju, nije moguća slabe ljudsku sposobnost za eksperimentiranjem i inicijativom. Takva klima, prouzročena neizvjesnošću posljedica djelovanja, neeksperte potiče na stav kako su znanje i njegovi proizvodi riskantni i opasni, a opasnost s kojom se suočavaju teško shvatljiva (usp. Furedi, 2008: 110). Činjenica je kako se prosječan korisnik ne može othrvati naletu digitalizacije te kako ona postaje neodvojiv dio njegovog svakodnevnog života. U Republici Hrvatskoj sve se više javnih servisa okreće digitalizaciji te se korisnike primorava da se njima koriste kako bi mogli ravnopravno sudjelovati u svakodnevici iako im se ne nudi valjana edukacija o tome kakva im ugroza prijeti. Može se zaključiti kako neeksperti žive u stalnom stanju straha od potpuno nejasne i nepoznate ugroze te kako si nikako u tome ne mogu pomoći.

3.3. Sekuritizacija kibernetičkog prostora

Sekuritizacija se odnosi na diskurzivnu konstrukciju prijetnje. Točnije, sekuritizacija se može definirati kao proces u kojem akter proglašava pojedini fenomen, odnos ili aktera egzistencijalnom prijetnjom po određeni referentni objekt. Ako relevantna publika prihvati stav kako nešto valja sekuritizirati, dolazi do suspenzije „uobičajenih“ političkih procesa i uspostave izvanrednih mjera kojima se odgovara na prikazanu prijetnju (Buzan, Wæver, de Wilde, 1998: 25)

Sigurnost, u ovom smislu, predstavlja polje pregovora između govornika i publike koje je uvjetovano, u velikoj mjeri, pozicijom moći što ju govornik zauzima unutar određene grupe. Wæver zaključuje kako uspješna sekuritizacija uključuje artikulaciju prijetnje s „određenog mjesta, institucionalnim glasom, od elita“ (Weaver prema McDonald, 2008: 69).

Artikulacija same prijetnje dolazi u obliku „govornog čina“, pojma često korištenog u Austinovoj teoriji jezika (Austin, 1962), a koji označava formu reprezentacije koja nije samo opis preferencija ili pogleda na vanjsku stvarnost. Prijetnja prolazi tri stadija, tj. iz polja nepolitiziranosti ulazi u polje politiziranosti te potom u polje sekuritizacije.

Sekuritizacija je nastavak rada Kopenhaške škole, skupine akademika okupljenih oko Barrija Buzana i Olea Wævera koji su u to vrijeme radili na Centru za istraživanje mira u Kopenhagenu. Jedan od prvih koncepata bilo je promatranje sigurnosti kroz prizmu različitih sektora. Nastavno na rad Barrija Buzzana, sektori su definirani kao arene koje uključuju određene tipove sigurnosnih odnosa te mogu biti vojni, politički, ekonomski, društveni i ekološki (Williams, 2008: 3).

Međutim, ulaskom informacijsko-komunikacijskih tehnologija u svakodnevni život, ne možemo govoriti o odvojenim sektorima sigurnosti jer je danas svaki aspekt ljudskog života i djelovanja premrežen. Vojna sigurnost uvelike ovisi o kibernetičkoj sigurnosti, kako u obliku šifrirane komunikacije, tako i u obliku potencijalnih kibernetičkih napada na postrojenja s interkontinentalnim balističkim projektilima i obavještajnih CYBINT/DNINT operacija. Politička sigurnost također snažno ovisi o kibernetičkoj sigurnosti čega smo svjedoci bili za vrijeme predsjedničke kampanje u Sjedinjenim Američkim Državama (Wired, 2018). Ekonomska sigurnost je dugo bila najsnažnije vezana uz kibernetičku sigurnost zbog snažnog poslovnog sektora koji je brzo prihvatio blagodati informacijsko-komunikacijskih tehnologija, a uz njih i nedostatke. Društvena sigurnost je također značajno određena novim tehnologijama, pogotovo kroz sveprodirajuće društvene mreže koje omogućavaju grupiranje i prethodno nezamisliv doseg. Ekološka sigurnost je posljednji od sektora koji ovise o kibernetičkoj sigurnosti zbog činjenice kako jedan uspješno izveden napad može prouzrokovati ekološku katastrofu ogromnih razmjera.

Kibernetička sigurnost više nije samo sigurnost informacijsko-komunikacijskih sustava, već predstavlja temeljnu sastavnicu sigurnosti cjelokupnog opsega ljudskih djelatnosti u informacijskom društvu.

Možda najbolje uključenost informacijsko-komunikacijskih tehnologija u današnje društvo ilustrira broj IoT[8] uređaja u 2017. godini. Naime, na globalnoj razini, trenutno je umreženo više od 20 milijardi uređaja, a taj broj bi do 2025. godine trebao narasti na više 75 milijardi umreženih uređaja. Sagledamo li te brojke iz nama bliže perspektive, danas svaki kućanski stroj postoji i u verziji koja ima mogućnost spajanja na Internet te mogućnost udaljenog pristupa. Od klima, perilica za rublje, usisavača do automobila, bicikala i televizora, ali i opreme za centrifugiranje[9].

O sekuritizaciji *cyber* prostora, tj. o kibernetičkoj sigurnosti počelo se govoriti nakon Hladnog rata kao odgovor na cijeli niz tehnoloških inovacija i promjena u geopolitičkom krajobrazu. Ranih 90-ih godina 20. stoljeća pojam kibernetička sigurnost koristili su znanstvenici kako bi označili cijeli niz nesigurnosti vezanih uz umrežena računala, međutim, pojam je dobio šire značenje nakon što je ustanovljeno kako prijetnje što izviru iz digitalnih tehnologija mogu imati drastične posljedice po cjelokupno društvo (Hansen i Nissenbaum, 2009: 1).

Sigurnost se u kontekstu informacijsko-komunikacijskih tehnologija spominje, vjerojatno po prvi put, u izvještaju Odbora za informatiku i telekomunikacije (engl. C*omputer Science and Telecommunications Bord* – CSTB) iz 1991. godine naslovljenom *Računala pod rizikom: Sigurno računanje u informacijskom dobu* (engl. *Computers at Risk: Safe Computing in the Information Age*) (Hansen i Nissenbaum, 2009: 6).

U spomenutom izvještaju sigurnost se definira kao „zaštita od neželjene objave i prilagodbe te od neželjenog uništenja podataka u sustavu, ali i zaštita samog sustava. Također, sigurnost sadrži i tehnički i ljudski aspekt te ima „značajan broj proceduralnih, administrativnih, fizičkih i ljudskih komponenata“ (Hansen i Nissenbaum, 2009: 6).

Ono što je od presudne važnosti kada je riječ o kibernetičkoj sigurnosti jest činjenica kako prijetnje ne dolaze isključivo namjerom agenata, već mogu biti sistemske prijetnje. Hundley i Anderson smatraju, kako Hansen i Nissenbaum prenose, da „kibernetička sigurnost ovisi o inherentnim nepredvidljivostima računala i informacijskih sustava koji, sami po sebi, stvaraju

[8] engl. *Internet of Things*
[9] Detaljnije na: https://www.csoonline.com/article/3218104/malware/what-is-stuxnet-who-created-it-and-how-does-it-work.html (pristupano: 15.9.2018.)

neželjenu, potencijalnu ili aktualnu, opasnu situaciju po sebe ili po fizički i ljudski okoliš u koji su ugrađeni“ (Hansen i Nissenbaum, 2009: 7).

Prijetnje mogu proizaći iz grešaka kako u programskoj podršci (engl. *software*) tako i u računalnoj sklopovskoj podršci (engl. *hardware*) i ne mogu biti otklonjene usavršavanjem digitalne tehnologije i programiranja. Edwards i Denning, prema Hansen i Nissenbaum, zaključuju kako unutar računalnih sistema postoji inherentna ontološka nesigurnost (Hansen i Nissenbaum, 2009: 6).

Spomenuti slučaj s Mitnickom i sudnjim danom pokrenutim fućkanjem ilustrira kakav je stav bio prema kibernetičkoj sigurnosti krajem 20. stoljeća. Tijekom 1990-ih upozorenja su davali istaknuti američki političari, privatne korporacije i mediji koji su govorili o „elektroničkim Pearl Harborima“ i „oružjima masovnog ometanja“ (engl. *weapons of mass disruption*) i tako najavljivali tamnu budućnost zapadnom svijetu (Hansen i Nissenbaum, 2009: 1; Gartzke, 2012: 2).

Događaji koji su obilježili početak 21. stoljeća poput napada na Svjetski trgovački centar potaknuli su nova razmatranja informacijsko-komunikacijskih tehnologija i sigurnosti, ali i zaštite digitalne infrastrukture, elektronskog nadgledanja, korištenja tehnologije od terorista i Interneta kao platforme za komunikaciju unutar i preko granica države.

Također, incident iz 2007. godine koji je uključivao DDoS[10] napad na estonske javne i privatne institucije, a koji je označen kao odgovor na micanje skulpture iz Drugog svjetskog rata, nazvan je prvim ratom u kibernetičkom prostoru i rezultirao je deklaracijom NATO-a koja je informacijsko-komunikacijske sustave definirala kao ključne sastavnice sigurnosti (Hansen i Nissenbaum, 2009: 2). Uz navedeni incident, kao primjer cyber-rata Clarke i Knake navode izraelski zračni napad na sirijska nuklearna postrojenja Dei rez-Zor iz 2007. godine (prema Kovačević, 2013: 92). Uz njih, Steinnon početak cyber-rata vidi u višednevnom DDoS napadu na ured gruzijskog predsjednika i niz vladinih institucija (prema Kovačević, 2013: 923).

[10] DDoS ili distibuted denial of service napad je napad uskraćivanja usluga koji se izvodi namjernim generiranjem velike količine mrežnog prometa kako bi se iskoristili svi raspoloživi resursi, onemogućavajući pri tome uobičajeni rad napadnutog računala.

Međutim, Hansen i Nissenbaum navode kako su kibernetičku sigurnost obilježila tri specifična koncepta koji su uz nju snažno vezani te ju, odnosima između sebe, definiraju (Hansen i Nissenbaum, 2009: 9). Svaki od ova tri koncepta snažno određuje odnos između sigurnosnih stručnjaka i aktera sekuritizacije s korisnicima informacijsko-komunikacijskih tehnologija te dodatno produbljuje jaz između ove dvije skupine čime onemogućuje podizanje razine kibernetičke sigurnosti.

3.3.1. Hipersekuritizacija

Prvi koncept, hipersekuritizaciju, predstavlja Buzan (prema Hansen i Nissenbaum, 2009: 9) te ju opisuje kao „proširenje sekuritizacije van normalne razine prijetnji i opasnosti pomoću tendencije da se pretjeruje u prikazu prijetnji te uspostavlja velik broj protumjera“. Uspjeh hipersekuritizacije određuje je li ona okarakterizirana kao pretjerivanje ili nije, tj. uspješna hipersekuritizacija ne smije biti okarakterizirana kao pretjerivanje.

Također, svi procesi sekuritizacije uključuju element hipotetskog u tome što stvaraju prijetnju na koju treba odgovoriti te na taj način „mobiliziraju ako-onda logiku“ (Hansen i Nissenbaum, 2009: 10). Za razliku od sekuritizacije, hipersekuritizacija podrazumijeva trenutne i međusobno povezane efekte. Na primjer, dok sekuritizacija mreže govori isključivo o mreži kao takvoj, hipersekuritizacija prikazuje na koji način prijetnja mreži prijeti društvenom, financijskom i vojnom sektoru. Također, sekuritizacija uvijek promatra budućnost, ali zaključke temelji i na referencama iz prošlosti kao što su npr. Hirošima i Nagasaki. U kontekstu kibernetičke sigurnosti, hipersekuritizacija nema tu mogućnost zato što ne postoje povijesne reference što kao posljedicu ima preuveličavanje prijetnje zbog činjenice kako ne postoji referentni okvir (Hansen i Nissenbaum, 2009: 10).

3.3.2. Svakodnevne sigurnosne prakse

Drugi koncept koji snažno oblikuje kibernetičku sigurnost su svakodnevne sigurnosne prakse koje uspostavljaju akteri u sekuritizaciji, državna tijela, privatne organizacije i tvrtke. Svakodnevnim se sigurnosnosnim praksama želi „mobilizirati“ pojedince na dva načina: osiguravanjem partnerskog odnosa pojedinca prema akterima sekuritizacije i suglasnosti u održavanju visoke razine kibernetičke sigurnosti te činjenjem hipersekuritiziranih scenarija plauzibilnijima povezivanjem elemenata scenarija katastrofe sa svakodnevnim iskustvima

običnih korisnika. Uspjeh sekuritizacije uvelike ovisi o sposobnosti aktera sekuritizacije da poveže osjećaj straha i prijetnje s osjećajima, potrebama i interesima običnih korisnika te činjenicom kako dovodi iste u opasnost ne pridržavajući se svakodnevnih sigurnosnih praksi (Hansen i Nissenbaum, 2009: 11).

Cyber sekuritizacija svakodnevnog života dodatno naglašava ulogu pojedinca kao partnera u borbi protiv nesigurnosti, ali i naglašava ulogu pojedinca kao izvora nesigurnosti, prijetnju ili, kako govori Furedi, ranjivost. Naglašavanjem činjenice kako se odbijanjem praćenja svakodnevnih sigurnosnih praksi narušava sigurnost cijelog sustava, u običnog se korisnika ugrađuje moralna odgovornost prema održavanju vlastite sigurnosti i, na koncu, sigurnosti cijelog sustava (Hansen i Nissenbaum, 2009: 12).

3.3.3. Tehnifikacija diskursa

Treći koncept koji obilježava kibernetičku sigurnost je tehnifikacija diskursa. Snažan naglasak na hipotetskim situacijama otvara prostor za tehnički, ekspertni diskurs. Kako Nissebaum naglašava (prema Hansen i Nissenbaum, 2009: 13), znanje potrebno da bi se obuhvatilo cijelo polje kibernetičke sigurnost je impozantno te često nije dostupno široj javnosti. Ubrzani napredak razvoja tehnologije sa sobom donosi i nove metode napada što dodatno potvrđuje privilegiranu poziciju stručnjaka za kibernetičku sigurnost. Pridavanje ovakve privilegirane pozicije stručnjacima za kibernetičku sigurnost izvire upravo iz logike sekuritizacije: „ako je kibernetička sigurnost toliko važna ne može biti prepuštana amaterima“ (Hansen i Nissenbaum, 2009: 13). Upravo tehnifikacija diskursa u sekuritizaciji dopušta određivanje tehničkog kao domene koja zahtijeva stručnost koju javnost i većina političara nema. Na taj način, stručnjaci postaju akteri sekuritizacije bez „politike“ s potpunim legitimitetom i bez mogućnosti da budu izazvani ili da njihova procjena bude dovedena u pitanje (Hansen i Nissenbaum, 2009: 14).

4. PRIKAZ RAČUNALNO-SIGURNOSNIH INCIDENATA U MEDIJIMA

4.1.Metodologija

U radu su korištene dvije metode iz korpusa kvalitativnih metoda društvenih znanosti. U prvom je koraku korištena analiza sadržaja članaka na najčitanijim hrvatskim internetskim portalima koje, prema popisu tvrtke Gemius, čine portali 24sata.hr, dnevnik.hr, vecernji.hr,

tportal.hr i index.hr[11]. Popisu je dodan i portal index.hr koji nije uvršten na popis tvrtke Gemius vlastitom zahtjevom, ali pripada najčitanijim portalima u Hrvatskoj.

Pretraga navedenih portala vršena je prema ključnim riječima „cyber“, „kibernetička“, „računalna“, „haker“ i „hakeri“ i obuhvatila je sve članke koji su objavljeni u 2017. godini. Na ovaj je način izdvojeno 1335 rezultata, međutim, zbog preklapanja u ključnim riječima, izdvojeno je 607 članaka.

Ključne riječi su odabrane na temelju više različitih kriterija. Na početku stoljeća terminologija koja se koristila u kontekstu onoga što se danas naziva kibernetička sigurnost sastojala se od više različitih pojmova kao što su „računalna sigurnost“ (engl. *Computer Security*), „IT sigurnost“ (engl. *IT Security*) te „informacijska sigurnost“ (engl. *Information Security*) (Schatz, Bashroush, Wall, 2017: 53). Međutim, krajem prvog desetljeća pojam „kibernetička sigurnost“ (engl. *Cyber Security*) počinje jačati te se sve češće spominje, a pravi uzlet doživljava 2009. godine kada predsjednik SAD-a, Barack Obama, poziva građane na prepoznavanje kibernetičke sigurnosti kao važne sastavnice nacionalne otpornosti i sigurnosti. Od tada, pojmovi „računalna sigurnost“, „informacijska sigurnost“ i „IT sigurnost“ gube na značaju dok „kibernetička sigurnost“ sve više jača (Schatz, Bashroush, Wall, 2017: 54). U Republici Hrvatskoj, pojam „kibernetički“ uveden je u pravni poredak ratifikacijom Konvencije o kibernetičkom kriminalu 2002. godine (Vojković, Štambuk-Sunjić, 2005: 124) te predstavlja prilagodbu engleskog prefiksa *cyber-* hrvatskom jeziku. Govoreći o ratifikaciji Konvencije, Vojković navodi kako je pojam „računalni kriminal“, koji je do tada bio u Hrvatskoj najrazumljiviji i opće prihvaćeni termin, zamijenjen, i to prema njegovu mišljenju pogrešno, terminom „kibernetički kriminal“ (Vojković, Štambuk-Sunjić, 2005: 125). Praksa prevođenja prefiksa *cyber-* u pridjev „kibernetički“, a ne „kiber“, karakteristična je za slavenske jezike kao što su slovenski i češki jezik (*kibernetska varnost, kybernetická bezpečnost*) te se odrazila i na zakonodavstvo u Hrvatskoj. Međutim, zbog globalnog dosega prefiksa *cyber-*, ali i njegove uloge u popularnoj kulturi te cyberpunk pokretu, on se i dalje koristi u hrvatskom jeziku. Dakle, termin „kibernetička sigurnost“ je danas zakonski određen, prefiks *cyber-* predstavlja oblik iz kojeg je izveden termin „kibernetički“, a „računalni“ je zamijenjen terminom „kibernetički“ 2002. godine

[11] 24sata.hr (https://www.24sata.hr/), dnevnik.hr (https://dnevnik.hr/), vecernji.hr (https://www.vecernji.hr/), tportal.hr (https://www.tportal.hr/) i index.hr (https://www.index.hr/)

ratifikacijom Konvencije, ali je još uvijek ostao snažno prisutan u hrvatskom jeziku kao izravan prijevod pojma „computer security“ čija je popularnost krenula padati tek 2009. godine (Schatz, Bashroush, Wall, 2017: 54). Pojam „haker“ korišten je u oba oblika, jednini i množini, zbog različitih rezultata koje je pretraga po ovim ključnim riječima davala. Na primjer, portal vecernji.hr pretragom po ključnoj riječi „haker“ daje svega 6 rezultata, dok „hakeri“ daje 91 rezultat. Portal 24sata.hr pretragom po ključnoj riječi „haker“ daje 15, a „hakeri“ 89 rezultata. Slično nastavlja i tportal.hr, koji pretragom po ključnoj riječi „haker“ daje 15, a „hakeri“ 104 rezultata. Dnevnik.hr pretragom po ključnoj riječi „haker“ daje 5, a „hakeri“ 27 rezultata. Najmanju razliku pokazuje portal index.hr koji pretragom po ključnoj riječi „haker“ daje 192 rezultata, dok ključna riječ „hakeri“ daje 202 rezultata.

Iz na ovaj način prikupljenih članaka izdvojeno je deset članaka koji se odnose na sedam računalno-sigurnosnih incidenata čije je izvorište ili objekt napada u hrvatskom IP adresnom prostoru te se u daljnjoj analizi koristi metoda studije slučaja, tj. analiza svih računalno-sigurnosnih incidenata u Republici Hrvatskoj u 2017. godini kroz njihove opise u medijskom prostoru.

Studija slučaja je kvalitativna istraživačka metoda koja se često definira kao „studija malog broja slučajeva ili jednog slučaja u opreci sa studijama velikog broja slučajeva“ (Jožanc, 2015: 38). Budući da je ustanovljeno kako se vrlo malen broj članaka odnosi na incidente koji su imali izvorište ili objekt napada u hrvatskom IP adresnom prostoru, studijom slučaja je opisan svaki od promatranih incidenata, ali je i klasificiran na temelju VOUND taksonomije te napadom prouzročene materijalne štete. Također, Schramm, prema Yinu, navodi kako je „esencija studije slučaja, centralna tendencija svih tipova studije slučaja, osvjetljavanje odluke ili niza odluka: zašto su donesene, kako su implementirane i s kojim rezultatom“ (Yin, 1984:12), što, u kontekstu prikaza računalno-sigurnosnih incidenata, omogućava sagledavanje šire slike te detaljniju obradu manjeg broja slučajeva što dalje omogućava analizu odnosa između empirijskog i normativnog u kontekstu računalno-sigurnosnih incidenata.

Uz navedeno, posebno je obrađen i slučaj značajnog incidenta zaraze zlonamjernim *ransomware*[12] sadržajem WannaCry koji je odjeknuo u svijetu, ali i u Hrvatskoj. Prikazano je što je prethodilo napadu, na koji način je izveden, koji je doseg imao te koji je trag ostavio u Hrvatskoj.

Sav medijski sadržaj, vezan uz računalno-sigurnosne incidente u Republici Hrvatskoj, podijeljen je s obzirom na izvorište računalno-sigurnosnog incidenta, opseg napada i vrstu napada po uzoru na klasifikacijsku shemu Nacionalne taksonomije računalno-sigurnosnih incidenata koja sigurnosno-računalne incidente dijeli prema:

1) Vektoru napada,

2) Operativnom učinku napada,

3) Učinku napada na informacije,

4) Objektu napada,

5) Dosegnutoj fazi napada.

Uz navedeni kriterij, medijski sadržaj je kategoriziran prema dosegnutom broju žrtava te uzrokovanoj materijalnoj šteti.

Komparativnom analizom utvrđena je i razlika medijskog prikaza računalno-sigurnosnih incidenata i službene evidencije istih koja se nalazi u okviru Statističkog pregleda temeljnih sigurnosnih pokazatelja i rezultata rada u 2017. godini Ministarstva unutarnjih poslova te Godišnjeg izvještaja rada Nacionalnog CERT-a[13] za 2017. godinu.

Analizom su obuhvaćene sve kategorije računalno-sigurnosnih incidenata Godišnjeg izvještaja rada Nacionalnog CERT-a te samo one kategorije koje se odnose na kibernetičku sigurnost u ostalim izvorima. Pod tim se kategorijama podrazumijeva: neovlašteni pristup, ometanje rada računalnog sustava, oštećenje računalnih podataka, neovlašteno presretanje računalnih podataka, računalno krivotvorenje i računalna prijevara.

[12] Ransomware je naziv za skup zlonamjernih programa koji korisniku onemogućuju korištenje računala. Nakon zaraze ransomware može šifrirati datoteke ili onemogućiti korištenje tako da se pojavi početni ekran s određenom porukom koju nije moguće maknuti. Od korisnika čije je računalo zaraženo traži se otkupnina u zamjenu za daljnje normalno korištenje računala.

[13] Engl. *Computer Emergency Response Team*

Komparativna analiza pokazala je o koliko je računalno-sigurnosnih incidenata, prema službenim izvještajima nadležnih tijela, u 2017. godini riječ, prati li broj i sastav medijskih članaka te brojke, u kojoj se mjeri računalno-sigurnosni incidenti obrađeni u medijima odnose na računalno-sigurnosne incidente krajnjeg korisnika te koja je uloga prosječnog korisnika u incidentu.

Ovom se analizom nastojalo odgovoriti u kojem odnosu stoji stvarna situacija računalno-sigurnosnih incidenata krajnjih korisnika te prikaz računalno-sigurnosnih incidenata u medijima te se nastojalo odgovoriti na pitanje može li se govoriti o hipersekuritiziranosti ove teme u Hrvatskoj.

Analizom sadržaja medijskih prikaza odabranih slučajeva članaka koji se odnose na incidente koji su imali cilj ili izvorište napada unutar hrvatskog IP adresnog prostora istraženo je na koji način mediji, kao glavni izvor informacija o sigurnosnim incidentima, ali i jedan od aktera na društvenopolitičkoj poziciji koja definira rizik, sudjeluju u definiranju računalno-sigurnosnog incidenta, kako te incidente prikazuju te na koji je način i u kojem kontekstu prikazan ljudski faktor, tj. na koji je način čovjek utjecao na ranjivost sustava te je li i na koji način zaslužan za sigurnosni incident. Također, odgovoreno je na pitanje vladaju li diskursom sigurnosni stručnjaci i je li on pretjerano "tehnificiran" te na koji način akteri uvjetuju korisnika obvezujući ga na prihvaćanje svakodnevnih sigurnosnih praksi. Istraživanjem se nastojalo odgovoriti i na pitanje tretira li se korisnika kao najveću ranjivost sustava te postoji li za to temelj kada govorimo o stanju kibernetičke sigurnosti u Hrvatskoj.

4.2.Istraživanje

Kada govorimo o računalno-sigurnosnim incidentima u Republici Hrvatskoj u 2017. godine, potrebno je navesti što se pod računalno-sigurnosnim incidentom podrazumijeva. Prema „Nacionalnoj taksonomiji računalno-sigurnosnih incidenata“ iz 2018. godine nastaloj temeljem Akcijskog plana za provedbu Nacionalne strategije kibernetičke sigurnosti, računalno-sigurnosni incident podrazumijeva „jedan ili više računalno-sigurnosnih događaja koji su narušili odnosno narušavaju sigurnost informacijskog sustava ili računalne mreže, te ugrožavaju povjerljivost,

cjelovitost i dostupnost informacija[14] koje se korištenjem informacijskog sustava ili računalne mreže kreiraju, obrađuju, pohranjuju ili prenose. Uz računalno-sigurnosni incident, definira se i značajan incident, tj. „računalno-sigurnosni incident koji utječe na kritične podatke (neklasificirane i klasificirane) i/ili informacijske sustave i računalne mreže u javnom i privatnom sektoru, posebice na sustave koji su dio nacionalne kritične infrastrukture, na kojima se ti podaci obrađuju i koje se prenose te koji može ostvariti i/ili ostvaruje negativan utjecaj na svakodnevni život velikog broja građana, nacionalnu ekonomiju i nacionalnu sigurnost u cjelini. Ova taksonomija predstavlja ostvarenje cilja G.11 Akcijskog plana za provedbu Nacionalne strategije kibernetičke sigurnosti kojom se nastoji "definirati taksonomije, uključujući pojam značajnog incidenta, definirati protokole za razmjenu anonimiziranih podataka o značajnim sigurnosnim incidentima, te uspostaviti platformu ili tehnologiju za razmjenu podataka" (Akcijski plan za provedbu Nacionalne strategije kibernetičke sigurnosti, 2015), a prethodno spomenuta definicija računalno-sigurnosnog incidenta predstavlja napredak na polju usuglašavanja kriterija pri klasifikaciji događaja svih dionika na području informacijske i kibernetičke sigurnosti.

Prema službenim podacima nadležnih tijela, Nacionalnog CERT-a i Ministarstva unutarnjih poslova, u Republici Hrvatskoj su u 2017. godini ukupno zabilježena 732 incidenta u nadležnosti Nacionalnog CERT-a te 755 incidenata u nadležnosti Ministarstva unutarnjih poslova, a koji su imali izvorište ili objekt napada unutar hrvatskog IP adresnog prostora ili .hr domene

Od računalno-sigurnosnih incidenata pod nadležnošću Nacionalnog CERT-a u 2017. godini, riječ je bilo o 370 slučajeva *web defacementa*, incidenata koji podrazumijevaju kompromitiran *web* poslužitelj s izmijenjenim izgledom i sadržajem *web* stranice, 127 slučajeva *phishing* URL-ova, incidenata koji podrazumijevaju kompromitiran web poslužitelj s postavljenom lažiranom stranicom čija je svrha krađa podataka, 59 slučajeva *phishinga*, incidenata koji podrazumijevaju navođenje korisnika na odavanje podataka putem raznih komunikacijskih kanala (najčešće elektroničke pošte), 42 slučaja *malware* URL-a, incidenata koji podrazumijevaju kompromitiran web poslužitelj s postavljenim zlonamjernim kodom, 29 slučaja *spamova*, incidenata koji podrazumijevaju slanje neželjene elektroničku poruku reklamnog

[14] Odnosi se na jedan od najpoznatiji sigurnosnih modela u kibernetičkoj sigurnosti poznat i pod nazivom „CIA principle" (Confidentiality, Integrity and Availability).

sadržaja, 28 slučaja nedozvoljenih mrežnih aktivnosti, incidenata koji podrazumijevaju neovlašteno automatizirano prikupljanje informacija o računalnim mrežama i sustavima, 28 slučaja *spam* URL-ova, incidenata koji podrazumijevaju kompromitiran *web* poslužitelj s neovlašteno postavljenim reklamnim sadržajem, 20 slučaja *botova*, incidenata koji podrazumijevaju računalo ili neku drugi uređaj zaražen zlonamjernim kodom, a koji djeluje kao *bot* unutar *botnet* mreže, 12 slučajeva ostalih vrsta napada i zlouporaba za koje korisnik smatra da je riječ o računalno-sigurnosnom incidentu, 10 DoS-ova (engl. *Denial-of-Service*), incidenata koji podrazumijevaju volumetrički napad koje se izvodi slanjem velikog broja IP paketa s ciljem zagušenja mrežne propusnosti, 4 *malware* domene, incidenata koji podrazumijevaju kompromitirano web sjedište s postavljenim zlonamjernim kodom, 3 kompromitirana računala te 2 slučaja C&C poslužitelja, incidenata koji podrazumijevaju kontrolni poslužitelj za nadzor i upravljanje računalima koja su dio *botnet* mreže.

Od računalno-sigurnosnih incidenata pod nadležnošću Ministarstva unutarnjih poslova u 2017. godini, riječ je bilo o 5 slučajeva neovlaštenog pristupa, incidenata koji podrazumijevaju ili višestruko pogađanje zaporki ili iskorištavanje ranjivosti kako bi se ostvario neovlašteni pristup računalu, 11 slučajeva ometanja rada računalnog sustava, incidenata koji podrazumijevaju uskraćivanje dostupnosti računalnog sustava, 7 slučajeva oštećivanja računalnih podataka, 1 slučaj neovlaštenog presretanja računalnih podataka, incidenata koji podrazumijevaju prikupljanje informacija *sniffing*[15] metodom, 10 slučajeva računalnog krivotvorenja te 721 slučaj računalne prijevare, incidenata koji podrazumijevaju razne vrste prijevara na internetu, od lažnog predstavljanja, prijevara prilikom trgovine na internetu i slično.

Kada je riječ o značajnim incidentima u 2017. godini, valja izdvojiti zlonamjerni *ransomware* sadržaj WannaCry koji je dostigao razinu globalnog incidenta 12. svibnja 2017. godine, prvog ovakvog intenziteta u kojem je zlonamjernim *ransomware* sadržajem WannaCry pogođeno više od 400 000 računala u 150 zemalja diljem svijeta. Prema navedenome na stranicama Ureda vijeća za nacionalnu sigurnost, u Republici Hrvatskoj je zabilježeno 205 slučajeva zaraženih računala zlonamjernim *ransomware* sadržajem WannaCry.

[15] Presretanje mrežnog prometa *snifferom*, posebno razvijenom aplikacijom koja presreće mrežne pakete.

S druge strane, kada je riječ o računalno-sigurnosnim incidentima koji su imali ili izvorište ili objekt napada u hrvatskom IP adresnom prostoru ili .hr domeni, mediji pokazuju značajno drugačiju sliku što pokazuje analiza relevantnih članaka objavljenih na najčitanijim internetskim portalima, koje, prema popisu tvrtke Gemius, čine portali 24sata.hr, dnevnik.hr, vecernji.hr, tportal.hr te index.hr.

Pretraga članaka napisanih u 2017. godini povezanih s ključnim riječima „cyber", „kibernetička", „računalna", „haker" i „hakeri" dala je mnoštvo rezultata, ali i različite rezultate za svaki portal. Portal index.hr najviše članaka, njih 202, prikazuje pretragom pojma „haker". Portal 24sata.hr najviše članaka, njih 89, prikazuje pretragom pojma „hakeri". Portal dnevnik.hr najviše članaka, njih 30, prikazuje pretragom pojma „cyber". Portal vecernji.hr, najviše članaka, njih 91, prikazuje pretragom pojmova „hakeri" i „cyber". Portal tportal.hr, najviše članaka, njih 166, prikazuje pretragom pojma „računalna".

Kada se od navedenih članaka izdvoje oni koji se odnose na konkretan računalno-sigurnosni incident koji je imao ili izvorište ili objekt napada u hrvatskom IP adresnom prostoru ili .hr domeni, tj. članaka koji govore o stvarnom slučaju računalno-sigurnosnog incidenta koji se dogodio u Republici Hrvatskoj, a ne o potencijalnim prijetnjama koje bi mogle pogoditi Republiku Hrvatsku i njene stanovnike, broj povezanih članaka drastično pada. Svaki od relevantnih računalno-sigurnosnih incidenata obrađen je prema VOUND taksonomiji kako bi se utvrdilo u koju skupinu spomenuti incidenti spada te o kojoj je razini prijetnje riječ te su na temelju tih podataka incidenti kasnije i analizirani.

Naime, od svih relevantnih članaka u 2017. godini konkretnim primjerima računalno-sigurnosnih incidenata koji su imali ili izvorište ili objekt napada u hrvatskom IP adresnom prostoru ili .hr domeni posvećuje se svega 10 članaka ne računajući WannaCry[16] koji je zasebno obrađen zbog velikog broja članaka u kojima se o njemu piše.

Analizom opisanih računalno-sigurnosnih incidenata u člancima ustanovljeno je kako se u dva članka, „Kriminalci u akciji: Kako ćete zaštititi svoju karticu od krađe" objavljenom 27.studenog 2017. godine na portalu 24sata.hr i „Lopovi imaju sve naprednije metode za varanje građana, ali zaštititi se možete na prilično jednostavan način", objavljenom 2. studenog 2017.

[16] Detaljnije na: https://www.cert.hr/wp-content/uploads/2018/02/WannaCry.pdf (pristupano: 10..2018.).

godine na portalu Dnevnik.hr, piše o različitim slučajevima iste vrste računalno-sigurnosnog incidenta, krađe povjerljivih bankovnih podataka, tj. *skimming* napada. Prema VOUND taksonomiji, vektor napada je fizički napad jer je riječ o instalaciji zlonamjernog uređaja na fizički izložen uređaj, u ovom slučaju bankomat. Operativni učinak napada u ovom slučaju je prikupljanje informacija, točnije skeniranje koje podrazumijeva neovlašteno i automatizirano prikupljanje informacija o povjerljivim korisničkim podacima. Učinak napada na informacije je otkrivanje informacije jer napadač prikuplja podatke s magnetne trake bankovne kartice te PIN-ove. Objekt napada je za ove incidente sam korisnik jer je cilj napada prikupljanje korisnikovih osobnih informacija. Dosegnuta faza napada je potpuna kompromitacija jer je napadač ostvario svoj cilj i motivaciju za napad. Prema navedenom u članku „Kriminalci u akciji: Kako ćete zaštititi svoju karticu od krađe" u tom je sigurnosnom incidentu materijalna šteta ukupno bila manja od 10 000 kuna, a drugi članak, „Lopovi imaju sve naprednije metode za varanje građana, ali zaštititi se možete na prilično jednostavan način", takvu informaciju ne navodi.

Članci „Nova prijetnja: Poruke iz lažne Porezne žele do vaših podataka" i „Ne nasjedajte na ovaj lažni mail iz porezne, mogli biste ostati bez podataka" objavljeni su istog dana, 1. prosinca 2017. godine na portalu 24.sata, odnosno portalu Tportal.hr. Analizom je ustanovljeno kako je riječ o računalno-sigurnosnom incidentu koji podrazumijeva *phishing* kampanju. Prema VOUND taksonomiji vektor napada je socijalni inženjering[17] jer je riječ o *phishing* poruci u kojoj se korisniku savjetovalo preuzimanje zlonamjernog sadržaja s *phishing* URL-a koji se nalazio na lažnoj domeni porezna-uprava.net. Prema operativnom učinku napada, ovaj incident pripada kompromitaciji i to *phishing* URL tipu kompromitacije. Učinak napada na informacije je otkrivanje jer preuzimanjem zlonamjernog sadržaja na računalo žrtva omogućava napadaču pristup računalu i povjerljivim informacijama. Objekt napada je u ovom slučaju lokalno računalo jer je riječ o napadu u kojem dolazi do kompromitacije lokalnog računala pojedinačnog korisnika preuzimanje zlonamjernog sadržaja. Prema dosegnutoj fazi napada riječ je o fazi isporuke, a do ostvarivanja pristupa nije došlo zbog pravovremene reakcije nadležnih službi koje su onemogućile vezu s kompromitiranog računala s napadačem. Ni u jednom se članku ne otkriva koliko je pojedinaca pogođeno niti kolika je materijalna šteta uzrokovana ovim incidentom,

[17] Socijalni je inženjering niz tehnika pomoću kojih pojedinac, iskorištavanjem ljudskih pogrešaka i slabosti, utječe na drugog pojedinca kako bi ga naveo da učini nešto što nije u njegovom interesu.

međutim, zbog brzog djelovanja nadležnih službi koje su prijetnju u veoma kratkom roku otklonile, može se pretpostaviti kako je riječ o neznačajnoj šteti, tj. ni uređaji ni podaci nisu oštećeni u napadu, a sanacija podrazumijeva instalaciju antivirusnog programa.

Sljedeći incident opisan je u člancima „Hakeri srušili sustav KBC-a Sestara milosrdnica, pacijenti ostali bez snimaka lomova“ objavljenom na portalu Vecernji.hr 12. siječnja 2017. godine te „Hakeri napali Traumatologiju: Srušio se sustav s podacima“ objavljenom na portalu 24sata.hr istog dana. Prema vektoru napada ovaj se incident svrstava u skupinu napada na dostupnu mrežnu i računalnu opremu, napada koji iskorištavaju ranjivosti računalnih mreža, ranjivih mrežnih uređaja te javno dostupnih poslužitelja ili računala. Operativni učinak napada je sustav zaražen zlonamjernim kodom, a učinak napada na informacije je uništenje informacija. Objekt napada je u ovom slučaju upravljačka infrastruktura jer je riječ o napadu na kritične dijelove sustava koji koordiniraju aktivnosti i upravljaju resursima informacijskog sustava. Dosegnuta faza napada je potpuna kompromitacija jer je došlo do uništenja podataka te privremenog uskraćivanja usluge. U člancima se ne navodi o kojem je broju pogođenih korisnika riječ, ni koja je materijalna šteta. Međutim, kako u članku stoji da su se svi podaci vraćeni iz sigurnosne kopije te smješteni na novi poslužitelj, može se pretpostaviti kako je materijalna šteta u ovom slučaju gotovo zanemariva.

Sljedeći članak „Lažni bankar prevario dvije žene, uzeo im 3 900 kuna za klađenje“ objavljen je na portalu Index.hr 8. travnja 2017. godine. Vektor ovog napada je socijalni inženjering jer je napadač naveo žrtve na kršenje uobičajenih, sigurnosnih procedura, tj. lažnim predstavljanjem je došao do povjerljivih informacija. Operativni učinak ovog napada je prijevara, a učinak napada na informacije je otkrivanje jer je napadač ostvario pristup informacijama kojima u normalnim okolnostima ne bi imao pravo pristupa. Objekt napada su u ovom slučaju korisnice jer su napadom prikupljane korisnikove osobne informacije, a dosegnuta faza napada je potpuna kompromitacija jer je došlo do ostvarivanja ciljeva i motivacije za napad , tj. došlo je do krađe novčanih sredstava s računa žrtava. Ovim su napadom zahvaćene dvije osobe koje su oštećene za 3 900 kuna.

Članak „Hakeri od Cro Copa tražili otkupninu: "Bolje mu je da ga ne nađu, ako ga nađe policija - jadna mu majka“ objavljen je 28. travnja 2017. godine na portalu Index.hr. Vektor napada nije opisan, međutim, može se pretpostaviti kako je riječ ili o socijalnom inženjeringu ili

o napadu na web tehnologije koje podrazumijevaju *brute force* napade na autentifikacijske mehanizme web aplikacija kao što su zaporke. Prema operativnom učinku napada postoje dvije mogućnosti, kompromitacija korisničkog računa na temelju podataka prikupljenih socijalnim inženjeringom ili je riječ o pokušaju neovlaštenog pristupa koji podrazumijeva višestruko pogađanje lozinke za pristup. Učinak napada na informacije je uništenje jer napad za konačni cilj ima uklanjanje pristupnih prava žrtvi. Objekt napada je korisnik, a dosegnuta je faza napada potpuna kompromitacija. U članku se navodi kako je pogođena samo jedna žrtva, a materijalne štete nije bilo jer žrtva nije platila traženu otkupninu za povrat korisničkog računa, već joj je nadležna služba, nakon prijave incidenta, vratila pristup korisničkom računu.

Dana 26. svibnja 2017. godine, na portalu Index.hr, objavljen je članak „OPREZ Nova prijevara putem maila na bizarno jednostavan način izvlači novac od naivnih ljudi“. U ovom je članku riječ o dvije tvrtke s područja Karlovca koje se razlikuju po tome što je iz jedne uplaćen novac napadaču, a iz druge nije. Vektor napada je socijalni inženjering jer se napadač predstavio kao direktor obje pogođene tvrtke te je tražio da mu se isplati novac na privatan račun u Španjolskoj. Operativni učinak napada je prijevara, a učinak napada na informacije nije zabilježen, tj. nema ga. Objekt napada je u oba slučaja bio korisnik, tj. djelatnica u tvrtki. Dosegnuta faza napada je dvojaka. Naime, u slučaju tvrtke koja nije isplatila novac se može govoriti o fazi isporuke iza koje nije slijedila faza ostvarivanja pristupa i kompromitacije. S druge strane, u slučaju tvrtke koja je isplatila novac riječ je o potpunoj kompromitaciji. Napadom su pogođene dvije tvrtke, a materijalna šteta, koja nije navedena u članku, prouzrokovana je u samo jednoj.

Članak „Oprez na društvenim mrežama: Lažni general ženu iz Gruda koštao 20 000 kuna“ objavljen je na portalu Tportal.hr 6. rujna 2017. godine. Prema vektoru napada riječ je socijalnom inženjeringu jer je lažnim predstavljanjem napadač na društvenoj mreži Facebook nagnao žrtvu na isplatu veće količine novaca. Operativni učinak napada je prijevara jer je riječ o lažnom predstavljanju napadača. Učinak napada na informacije nije zabilježen, tj. nema ga. Objekt napada je u ovom slučaju korisnik, a dosegnuta faza napada je potpuno kompromitacija jer je došlo do uplate na račun napadača Ovom je prijevarom pogođen jedan korisnik, a materijalna šteta iznosi 20 000 kuna.

4.2. Analiza

Iako su u 2017. godini nadležne službe zabilježile 1487 računalno-sigurnosnih incidenata u hrvatskom IP adresnom prostoru ili .hr domeni, mediji su se u Hrvatskoj osvrnuli samo na njih sedam i to u svega deset članaka. Četiri članka navode kako postoji izravna materijalna šteta u obliku novca kojeg je napadač stekao prijevarom ili krađom, dok se u ostalima ne spominje materijalna šteta koja je uzrokovana izravnim akcijama napadača.

Incidenti su opisani u člancima „Kriminalci u akciji: Kako ćete zaštititi svoju karticu od krađe“ i „Lopovi imaju sve naprednije metode za varanje građana, ali zaštititi se možete na prilično jednostavan način“ u kojima je navedeno na koji je način krađa bankovnih podataka žrtava izvedena, koliko je novca ukradeno, a oba članka nude sigurnosne savjete tj. svakodnevne sigurnosne prakse kojih bi se trebali držati prilikom rukovanja bankomatom. Oba članka savjetuju korisnicima da naprave vanjski pregled uređaja kako bi ustanovili „ima li možda na njemu nešto nalijepljeno“ te „kod dolaska na bankomat svakako treba vidjeti ako išta djeluje sumnjivo“. Također, savjetuje se prekrivanje tipkovnice rukom prilikom upisivanja PIN-a te praćenje vlastitog bankovnog računa. Članak „Kriminalci u akciji: Kako ćete zaštititi svoju karticu od krađe“ navodi kako su napadači krivotvorili više od 100 bankovnih kartica, međutim, uspjeli su izvesti transakcije s karticama samo triju žrtava, u ukupnom iznosu od 10 000 kuna, prije no što je sigurnosni sustav pogođenih banaka reagirao. Sav novac je vraćen žrtvama čime je sanirana sva šteta, a sam sustav nije pretrpio nikakav značajan udar.

Članci „Nova prijetnja: Poruke iz lažne Porezne žele do vaših podataka“ i „Ne nasjedajte na ovaj lažni mail iz porezne, mogli biste ostati bez podataka“ govore o *phishing* kampanji koja je trajala gotovo dva tjedna te je jedan od 127 računalno-sigurnosnih *phishing* URL incidenata koje je Nacionalni CERT zabilježio tijekom cijele 2017. godine. Sam članak je objavljen nakon što je prijetnja otklonjena, ne govori o tome kolika je šteta uzrokovana, niti koliko je žrtava bilo, međutim, donosi savjete običnim korisnicima kako se od navedenog napada, iako više ne predstavlja stvarnu prijetnju, zaštititi. U službenom upozorenju koje je preneseno na oba portala piše kako se:

> „u slučaju pokretanja preuzete maliciozne datoteke, ista komunicira s upravljačkim poslužiteljem (C&C) na IP adresi 81.4.125.50 na sljedećim domenama: consaltingsolutionshere.com, kimdotcomfriends.com, bestfriendsroot.com. Zbog toga savjetuju korisnicima da se blokira promet prema navedenim domenama te da istovremeno

> obave provjeru ima li pokazatelja o zabilježenim konekcijama prema zlonamjernim domenama. Također jedan od indikatora provjere kompromitacije računala je i utvrđivanje postojanja aktivnih procesa na sustavu naziva weather.exe i serk.exe“.

Ni jedan ni drugi članak ne navode kako sam tekst poruke nije usklađen s hrvatskim jezikom, a u kojem, primjerice, stoji „Ukoliko mislite da ste ovaj email dobili greškom prosljedite ga Vašem šefu računovodstva“. Također, umjesto dokument stoji „document“, a umjesto preuzmi datoteku stoji „preuzmite fajl“. Autori članaka preuzeli su službeno upozorenje sa stranica portala Nacionalnog CERT-a, koji je, zbog prirode djelatnosti kojom se bavi, a i publike koja ga prati, pisan jezikom struke koji razumiju stručnjaci na području informacijskih tehnologija. Može se zaključiti da pojedinac koji je „nasjeo“ na ovako jednostavnu *phishing* poruku ni na koji način ne može poduzeti adekvatne mjere otklanjanja prijetnje te jedino može potražiti pomoć stručnjaka. Zanimljivo je što se nigdje ne navodi kako je vektor napada socijalni inženjering, od kojeg se ne može obraniti prateći neke jasno propisane sigurnosne prakse, već ovisi o „zdravom razumu“ žrtve koja će moći prepoznati kako nešto nije u redu u poruci ili zahtjevu što ga je dobila.

Štoviše, naslovi ovih dvaju članaka mnogo govore o razumijevanju medija kada je riječ o računalno-sigurnosnim incidentima. Iako se u službenim upozorenjima nigdje ne navodi kako žrtve ostaju bez podataka, već stoji kako će doći do kompromitacije računala, oba članka svode ova dva odvojena pojma na isto. Naime, kompromitacija računala ne mora značiti da će žrtva ostati bez podataka, a poneke računalno-sigurnosne ugroze nisu ni vidljive prosječnim korisnicima. Kompromitacija računala preuzimanjem zlonamjernog sadržaja bi mogla označavati, na primjer, uključenje računala u *botnet* mrežu, mrežu tzv. zombi računala, kojima upravlja napadač i pomoću kojih izvodi volumetričke DoS i DDoS napade. Žrtva se može najnormalnije nastaviti služiti računalom bez ikakvih pokazatelja kako je do kompromitacije došlo, dok ono, primjerice, u isto vrijeme onemogućava rad servera u Južnoj Koreji.

Sljedeći incident je opisan u člancima „Hakeri srušili sustav KBC-a Sestara milosrdnica, pacijenti ostali bez snimaka lomova“ i „Hakeri napali Traumatologiju: Srušio se sustav s podacima. Prema navedenom u članku, ravnatelj KBC-a Sestre milosrdnice doc. dr. sc. Mario Zovak, dr.med. govori:

> „Istina je da smo imali problem kad nam je pao sustav na starom serveru, gdje su se pohranjivali radiološki podaci, jer su nas napali hakeri. Svi podaci su spašeni iz backupa i

prebačeni na novi server. Nakon što je ustanovljen napad, slučaj smo prijavili policiji koja će utvrditi način kako su hakeri upali virusom u sustav da bismo se ubuduće od istoga zaštitili.“.

Iz navedene izjave se može zaključiti kako je ranjivost u sustavu predstavljala stara i neodržavana oprema na kojoj su bili pohranjeni podaci. Također, članak pokazuje kako nikakva šteta, osim zamjene dotrajale opreme, nije prouzrokovana, te da su svi podaci uspješno vraćeni iz sigurnosne kopije. Dakle, osoba koja je radila na održavanju sustava je, prema svim pokazateljima, bila svjesna rizika, poduzela je sve zaštitne mjere kako šteta ne bi eskalirala te je dotrajalu opremu, nakon što je više nije bilo moguće zaštititi na softverskoj razini, zamijenila novom i sigurnijom. Iako u članku nije navedeno zašto je upravo taj sustav bio metom napadača, a u trenutku objave ista informacija nije bila poznata ni nadležnoj službi, autori zaključuju kako su hakeri „bešćutni“. Međutim, jednako je moguće da je napadač razvio aplikaciju koja skenira mrežne uređaje tražeći one s postojećim ranjivostima koje napadač lako iskorištava za kompromitaciju sustava. Ukratko, postoji mogućnost da je ovaj napad izveden samo zato što je zastarjela oprema to dopuštala i da ne postoji nikakvo dublje značenje ovog napada, ali autori članka su takvo što propustili napomenuti.

Incident opisan u članku „Lažni bankar prevario dvije žene, uzeo im 3 900 kuna za klađenje“ govori o klasičnom tipu socijalnog inženjeringa, *phishingu*, koji je prethodno spomenut kao jedan od češćih vektora napada. Međutim, ovdje je riječ o klasičnoj prijevari, koja ne uključuje neke složene tehničke pothvate kako bi se uspješno izvela. Žrtve su napadaču odale informacije, najvjerojatnije u želji za zaradom, jer su pohlepa i neznanje, uz ostalo, ono na što napadač kod socijalnog inženjeringa računa. Doduše, može se reći kako je ovaj incident samo rubno računalno-sigurnosni jer se jednako tako mogao odviti na ulici ili ispred žrtvinih vrata. Iako ne piše na koji je način komunikacija sa žrtvama ostvarena, je li riječ bila o kontaktu putem društvenih mreža, putem lažne internetske forme za unos podataka ili putem lažne adrese elektroničke pošte, moguće je pretpostaviti kako je riječ o slučajevima koji su, sadržajem, uobičajeni u Hrvatskoj kada se u obzir uzme činjenica da je u 2017. godini MUP zabilježio 721 pokušaj računalne prijevare. Zašto je baš ovaj od svih slučajeva izdvojen, nije jasno.

O sličnom tipu računalno-sigurnosnog incidenta govori i članak „OPREZ Nova prijevara putem maila na bizarno jednostavan način izvlači novac od naivnih ljudi“. U izvođenju ovog napada također je korišten socijalni inženjering, točnije metoda *phishing* kako bi se djelatnicu

jedne od dvije pogođene tvrtke nagnalo da uplati novac na napadačev račun u Španjolskoj. Dodatne informacije o tehničkom dijelu samog napada u članku nisu navedene, međutim, sam članak sugerira kako nije riječ o tehnički veoma složenom napadu, već se može zaključiti kako je riječ o klasičnoj *CEO Fraud*[18] prijevari. Kako je sporna poruka elektroničke pošte pristigla na adrese dviju tvrtki, a samo u jednoj od njih je prepoznato da je riječ o prijevari, može se reći kako je ovaj incident uspješno izveden zbog nedovoljne edukacije djelatnika tvrtke koja je bila metom prijevare. Autori prenose upozorenje policije u kojem se korisnike upozorava da provjere istinitost primljenih poruka elektroničke pošte bez dodatnih objašnjenja na koji način bi trebali prepoznati da je riječ o pokušaju prijevare. Od dodatnih informacija se navodi kako je riječ o obliku računalne prijevare koji je usmjeren na računovodstvene servise državne vlasti i pravnih osoba.

Članak „Oprez na društvenim mrežama: Lažni general ženu iz Gruda koštao 20 000 kuna" nastavlja na istom tragu kao i prethodni članak te opisuje incident koji je također primjer socijalnog inženjeringa. Napadač se predstavljao kao visoki vojni dužnosnik američke vojske koji je žrtvi pristupio putem društvene mreže Facebook te joj kazao kako želi kupiti nekretninu na području Dubrovačko-neretvanske županije. Kazao joj je kako mu treba pomoć za prijenos novca te kako će joj on, ako pomogne, dati novčanu naknadu. Žrtva je na to uplatila napadaču 20 000 kuna na račun u Indoneziji. Kako je preneseno u članku, nakon ponovljenih zahtjeva za novčanim uplatama žrtva je shvatila da je riječ o prijevari i prijavila incident policiji. Autori prenose upozorenje policije:

> „Upozoravamo građane na još jedan pojavni oblik internetske prijevare koji je zabilježen na području Policijske uprave dubrovačko-neretvanske, a radi se o prijevari putem profila društvene mreže. Naime, osoba zaprimi zahtjev za prijateljstvom od osobe, stranog državljanina, koji se predstavlja kao visoki politički ili vojni dužnosnik koji ima namjeru kupiti nekretninu na našem području. Zbog problema oko transfera novčanih sredstava, osoba od vas zatraži pomoć u vidu uplate određenog novčanog iznosa uz obećanje primamljive novčane naknade. No, transfera novca ustvari nema, a žrtve se navuku da u ime taksi ili sličnih davanja plaćaju znatne iznose kako bi se olakšalo isplaćivanje spomenute naknade".

[18] CEO Fraud je tip prijevare u kojoj napadač šalje zlonamjernu poruku elektroničke pošte s lažirane adrese u kojoj se predstavlja kao visoko pozicionirani djelatnik tvrtke u kojoj se nalazi meta

Autor članak zaključuje savjetom „Najbolji način zaštite od ovakve vrste prijevare je neprihvaćanje zahtjeva za prijateljstvo od nepoznatih stranih osoba“ koji se može povezati sa savjetom koji se često daje djeci, „nemoj otvarati vrata nepoznatim ljudima“. Iako je u ovom slučaju riječ o generalu američke vojske, puno je poznatiji nigerijski princ[19], a ovakvi tipovi prijevara spominju se i u 19. stoljeću kada su se prevaranti predstavljali kao bogate osobe zatočene u španjolskom zatvoru (Gillespie, 2017).

Posljednji analizirani članak „Hakeri od Cro Copa tražili otkupninu: "Bolje mu je da ga ne nađu, ako ga nađe policija - jadna mu majka“ prikazuje specifičan incident u kojem je poznatom MMA borcu napadač došao do korisničkih podataka za prijavu na društvene mreže. Ovaj incident je izdvojen samo zato što je riječ o popularnoj osobi, a podaci društvene mreže Facebook govore kako je u 2011. godini od milijardu prijava 0,06% svih bilo kompromitirano. Točnije, u 2011. godini se dnevno kompromitiralo 600 000 računa. Kako i zašto je do kompromitacije došlo, u članku nije navedeno, ali imajući na umu da postoji niz sigurnosnih mehanizama koje valja zaobići kako bi se ostvario pristup ovoj društvenoj mreži, može se zaključiti kako je riječ o propustu žrtve.

Značajni incident zaraze zlonamjerni *ransomware* sadržajem WannaCry

U 2017. godini promatrani su portali zlonamjernom *ransomware* sadržaju posvetili niz članaka što je i očekivano s obzirom na to da je riječ o najvećem računalno-sigurnosnom incidentu u povijesti. Prema VOUND taksonomiji, kod zlonamjernog *ransomware* sadržaja WannaCry vektor napada je socijalni inženjering u prvoj fazi napada, operativni učinak je kompromitacija/sustav zaražen zlonamjernim kodom u prvoj te pokušaj neovlaštenog pristupa iskorištavanjem ranjivosti u programskom paketu drugoj fazi, učinak napada na informacije je uništenje, objekt napada je lokalno računalo, a dosegnuta faza napada potpuna kompromitacija. Ukratko, zlonamjerni je sadržaj isporučen korištenjem socijalnog inženjeringa kako bi se žrtvu nagnalo da preuzme i pokrene zlonamjerni kod, operativni učinak je preuzimanje zlonamjernog *ransomware* sadržaja WannaCry na računalo, ali i širenje istog na računala unutar lokalne mreže

[19] Detaljnije na: https://www.fbi.gov/scams-and-safety/common-fraud-schemes/nigerian-letter-or-419-fraud (pristupano: 12.9.2018.)

bez potrebe za interakcijom žrtve, napadom se informacije na uređaju, koji je lokalno računalo, uništavaju, a sam je napad, iz perspektive napadača, dosegnuo završnu fazu u kojoj se ostvaruju ciljevi i motivacija za napad. Kao što je već navedeno, u Republici Hrvatskoj je zabilježeno 205 slučajeva zaraze zlonamjernim sadržajem WannaCry što, kada se u obzir uzme činjenica kako je bila riječ o globalnoj kampanji, veoma malen broj.

Zlonamjerni *ransomware* sadržaj WannaCry pojavljuje se prvi put, u inačici 1.0., u veljači i ožujke 2017. godine. Iako su slučajevi zaraze zabilježeni mnogo prije no što je WannaCry postao globalna prijetnja, tek inačica 2.0 predstavlja značajnu prijetnju. Naime, toj je inačici dodana mogućnost automatskog širenja zaraze te WannaCry poprima karakteristike računalnog crva. Prvog dana napada, 12. svibnja 2017. godine WannaCry 2.0 zarazio je 75 000 računala, a između ostalog i National Health Service, Deutche Bahn, Telefónica, FedEx i Ministarstvo unutarnjih poslova Ruske Federacije. Napad se nastavio i nakon 12. svibnja te je WannaCry sveukupno pogodio više od 400 000[20] žrtava u 150 zemalja[21].

WannaCry je koristio dvije ranjivosti, EternalBlue[22] i DoublePulsar[23], koje su napadaču omogućavale udaljeno preuzimanje kontrole nad računalima s operativnim sustavom Windows iskorištavanjem ranjivosti u implementaciji SMB protokola[24]. Ranjivost EternalBlue posebno je opasna iz više razloga. Iskorištavanjem ove ranjivosti moguće je napasti računala udaljeno, preko mreže. Također, za iskorištavanje ove ranjivosti nije potrebno znati nikakvo korisničko ime ili lozinku, a uspješno iskorištavanje napadaču daje potpunu kontrolu nad računalom jer je riječ o ranjivosti koja se nalazi u jezgri operativnog sustava (eng. *kernel*), tzv. nultom prstenu (engl. *ring 0*).

Navedene ranjivosti su postale javno dostupne nakon što je hakerska skupina Shadow Brokers[25] u kolovozu 2016. godine pokrenula aukciju za njihovu prodaju. Naime, saznanja o

[20] Službeni podaci se razlikuju pa tako MalwareTech, sigurnosni stručnjak zaslužan za prekid kampanje, navodi kako je do 19. svibnja 2017. godine zabilježeno 416,989 jedinstvenih IP adresa.
[21] Detaljnije na: https://www.zdnet.com/article/wannacry-ransomware-crisis-one-year-on-are-we-ready-for-the-next-global-cyber-attack/ (pristupano: 15.9.2018.)
[22] Detaljnije na: https://www.cvedetails.com/cve/CVE-2017-0143/ (pristupano 15.9.2018.)
[23] Detaljnije na: https://www.cvedetails.com/cve/CVE-2017-0145/ (pristupano: 15.9.2018.)
[24] Detaljnije na: https://docs.microsoft.com/en-us/windows/desktop/fileio/microsoft-smb-protocol-and-cifs-protocol-overview (pristupano: 15.9.2018.)
[25] Detaljnije na: https://www.theatlantic.com/technology/archive/2017/05/shadow-brokers/527778/ (pristupano: 15.9.2018.)

ranjivostima ukradena su iz Equation grupe, napredne „hakerske“ grupe koja djeluje u okviru TAO-a (engl. *Office of Tailored Access Operations*) koji je, navodno, tajni odjel NSA-a koji aktivno napada računalne sustave i mreže te na taj način prikuplja informacije[26]. Nakon niza objava kojima oglašavaju i prodaju ukradeno, grupa Shadow Brokers 14. travnja 2017. godine objavljuje niz moćnih alata za kompromitaciju računala, od kojih su najznačaniji EternalBlue i DoublePulsar. Zanimljivo je kako je mjesec dana prije same objave, 14. ožujka 2017. godine Microsoft objavio sigurnosnu nadogradnju MS17-010 u kojoj se nalazila i sigurnosna zakrpa za ranjivost EternalBlue. Dakle, mjesec dana prije objave ranjivosti na stranici Wikileaks u događaju nazvanom „Year Zero“[27], ažurirana računala su bila zaštićena od napada, a sva ona računala koja nisu napravila sigurnosnu nadogradnju sustava bila su potencijalne mete za zlonamjerni sadržaj WannaCry[28].

Točan identitet napadača nije poznat, no sigurnosni stručnjaci iz tvrtke Symantec tvrde kako postoje snažne veze s Lazarus grupom[29], koja je, između ostalog, povezana s velikim napadom na Sony Pictures Entertainment u 2014. godini te krađom 80 milijuna dolara iz Centralne Banke Bangladeša u 2016. godini. Lazarus grupu se povezuje sa Sjevernom Korejom, međutim, ne postoje još konkretni dokazi za takvu tvrdnju i teško da će, osim ako ne preuzmu zasluge za napad, postojati.

Kada govorimo o Republici Hrvatskoj i zarazi zlonamjernim *ransomware* sadržajem WannaCry, kao što je već navedeno, u Hrvatskoj je zaraženo svega 205 računala. S druge strane, mediji tu brojku, iako je javno dostupna, nisu objavili, a sadržaj WannaCry se spominje u 12 članaka na portalu tportal.hr, 1 na portalu dnevnik.hr, 12 na portalu Vecernji.hr, 15 na portalu Index.hr te 4 na portalu 24sata.hr. Ukupno, riječ je o 44 članka u kojima se spominje WannaCry, zlonamjerni sadržaj koji je u Hrvatskoj ostavio gotovo nezamjetan trag. Ured vijeća za nacionalnu sigurnost navodi kako „mjesec dana kasnije možemo ocijeniti kako WannaCry nije nanio znatniju štetu u Hrvatskoj“, a šteta se sanirala ponovnom instalacijom operativnog sustava, iako je u većini slučajeva zaraza uklonjena bez toga (Ured Vijeća za nacionalnu sigurnost, 2018.)

[26] Detaljnije na: https://securityscorecard.com/blog/what-is-equation-group-shadow-brokers (pristupano: 15.9.2018.)
[27] Detaljnije na: https://wikileaks.org/ciav7p1/ (pristupano: 15.9.2018.)
[28] Detaljnije na: https://technet.microsoft.com/en-us/library/security/ms17-010.aspx (pristupano: 15.9.2018.)
[29] Detaljnije na: https://www.symantec.com/connect/blogs/wannacry-ransomware-attacks-show-strong-links-lazarus-group (pristupano: 15.9.2018.)

Članci koji su obrađivali ovu temu na različite su načine prikazivali WannaCry. Članak objavljen 15.svibnja 2017. godine na portalu 24sata.hr naslovljen „Više nitko nije siguran: Hakeri su „srušili“ i hrvatsku policiju?“ govori o tome kako se redakciji obratila čitateljica koja nije mogla registrirati automobil jer je informacijski sustav MUP-a bio blokiran. MUP je naveo da su „evidentirane određene smetnje u internetskom sustavu te stručne službe otklanjaju navedeno“ te kako im „informacijski sustav pritom nije bio ugrožen te kako normalno funkcionira“. U objavi MUP-a nigdje nije naveden WannaCry te iz portala 24sata.hr zaključuju kako nije poznato je li poteškoća uzrokovana zlonamjernim sadržajem.

Portal Tportal.hr 18. svibnja 2017. godine objavljuje članak naslovljen „Ako nisu ugroženi životi – ne započinjite razgovor s hakerima i ne plaćajte otkupninu“ u kojem se ne navodi o koliko je slučaja zaraze u Hrvatskoj riječ te se u kojem savjetuje niz sigurnosnih praksi kojima se može izbjeći zaraza te posebno ističe da „ako ne postoji prijetnja ljudskim životima – ne započinjati razgovor s napadačima i ne plaćati otkupninu“. Članak objavljen na istom portalu naslova „Šest pitanja o hakerskom napadu koji je uzdrmao svijet“ na pitanje „Treba li vas biti strah?“ odgovara kako se može dogoditi da korisnik ostane bez svega što drži na računalu te korisnicima savjetuje prihvaćanje svakodnevnih korisničkih praksi koje moraju poštovati jer inače ne poštuju ni osnovne sigurnosne standarde.

Svi portali nude složene sigurnosne savjete kako se zaštititi od zaraze koji podrazumijevaju napredno znanje o kibernetičkoj sigurnosti, računalnim sustavima i podešavanju računalnih mreža što nikako ne spada u znanje kojim barata osnovni korisnik. Analiza navedenih portala pokazala je kako savjete i svakodnevne sigurnosne prakse nudi 18 članaka na portalu Index.hr, 2 članka na portalu Dnevnik.hr, 10 članaka na portalu Vecernji.hr, 20 članaka na portalu 24sata.hr te čak 71 članak na portalu Tportal.hr. Primjera radi, u vrijeme kada je WannaCry bio na vrhuncu, svi su portali prenijeli isto tehnički pisano upozorenje MUP-a i ZSIS-a koje je naprosto kopirano u tekst članka bez prilagodbe teksta čitatelju. Savjeti poput „Ako primjena zakrpe nije moguća, onemogućiti SMBv1 protokol prateći sljedeću proceduru (ovisno o inačici operativnog sustava): Windows Vista, Windows Server 2008, Windows 7, Windows Server 2008 R2, Windows 8 i Windows Server 2012: 1. sc.exe config lanmanworkstation depend=bowser/mrxsmb20/nsi“ ni na koji način ne pomažu krajnjem korisniku te dodatno tehnificiraju diskurs koji je sam po sebi nerazumljiv.

4.3. Rasprava

Analizom te usporedbom računalno-sigurnosnih incidenata koji su imali izvorište ili objekt napada u hrvatskom IP adresnom prostoru ili .hr domeni, a o kojima su vijesti prenijeli hrvatski mediji te smještanjem tih incidenata u kontekst cjelokupnog broja sličnih incidenata u Hrvatskoj, jasno se može zaključiti kako incidenti, da bi ih se prikazalo u medijima, moraju uključivati značajnu novčanu štetu, moraju rezultirati prestankom rada nekog vitalnog sustava ili moraju biti povezani sa stvarnom osobom koja je žrtva. Podaci nadležnih službi pokazuju potpuno drugačiju situaciju i mediji jednostavno cijeli jedan vid računalnih ugroza ne prikazuju. Od 370 slučaja *web defacementa*, najpopularnije vrste računalno-sigurnosnog incidenta, se ne spominje ni jedan.

Doduše, incidenti ovog tipa ne uzrokuju gotovo nikakvu materijalnu štetu, napadaju ranjive i zastarjele internetske stranice te ih, obično, izvode mladi hakeri željni uzbuđenja. Najčešće je riječ o upozorenjima poput „We are anonymous“ i „You have been hacked“ koja hakerima služe kako bi se pokazali svoje znanje i umješnost te postavili dokaze o kompromitaciji na servisu pastebin.com što je svojevrsna oglasna ploča na kojoj zlonamjerni hakeri opisuju napade koje su izveli. Incidenti koji uključuju slanje *phishing* URL-ova je 127, a o njima govore dva članka koji se odnose na isti incident. Štoviše, članci pružaju savjete za obranu od navedene prijetnje nakon što je ona bila otklonjena. Može se zaključiti kako je vijest prenesena zato što je označena kao važna od strane nadležnih službi koje su putem svojih komunikacijskih kanala upozorile korisnike te zato što je riječ o incidentu u kojem se napadač predstavljao kao upravna organizacija Ministarstva financija. Može se pretpostaviti da je šteta, iako nije službeno objavljena, bila zanemariva. Iz navedenog se može zaključiti kako računalno-sigurnosni incidenti u Hrvatskoj nisu dovoljno zanimljivi da bi ih mediji prikazivali u istoj mjeri u kojoj su zastupljeni u pokazateljima nadležnih službi.

Iako je relativno velik broj članaka povezan s kibernetičkom sigurnošću, o incidentima u Hrvatskoj se govori veoma malo. Sagledaju li se ostali članci može se zaključiti kako prevladava diskurs koji govori o mogućnostima, tj. potencijalnim prijetnjama koje se kriju u svijetu oko nas. Naslovi poput „Roditelji, ako ste djeci kupili ovu lutku, odmah ju uništite!“ i „Avione više ne rušimo kao nekad, dovoljan nam je iPad“ običnom korisniku stvaraju strah, međutim, nekome tko svakodnevno prati vijesti iz kibernetičke sigurnosti ovakve vijesti ne predstavljaju ništa novo.

Usporedbe radi, dok portal 24sata.hr govori o špijunskoj lutki, relevantni sigurnosni portali govore o prijenosu signala putem zvuka što ga proizvodi računalni ventilator (Greenberg, A., 2018), očitavanju raspoloženja korisnika pomoću WiFi signala (Murnane, K., 2016) te hakiranju *pacemakera* (CERT, 2017). Međutim, veoma je važno napomenuti, a to je ono što mediji propuštaju napomenuti, kako je riječ o teoretskim konceptima (engl. *Proof of Concept*) koje razvijaju vrhunski sigurnosni stručnjaci u kontroliranim okruženjima s jasnim ciljem osmišljavanja novih tehnika napada.

Možda najbolje glad medija za stvarnim računalno-sigurnosnim prijetnjama pokazuje situacija oko kampanje zlonamjernim *ransomware* sadržajem WannaCry. Službeni računi napadača koji je izveo napad javno su dostupni te prikazuju kako je u cijeloj kampanji zarađeno svega 49.96959529 bitcoina (Collins, K., 2017) što je u to vrijeme iznosilo 120 055,58 američka dolara, a podaci govore kako je zaraženo više od 400 000 računala. Također, Kaspersky navodi kako je 98% računala koristilo operativni sustav Windows 7 koji je prvi put pušten u javnost 2009. godine (Perekalin, A., 2017). Valja ponovno napomenuti kako je zakrpa koja je onemogućavala napad bila objavljena 91 dan prije globalne zaraze, a da je u objavi ranjivosti koja su omogućila izvedbu ovog napada na stranici Wikileaks Juliana Assangea kazao:

> „Postoji ekstremno visok rizik proliferacije kada govorimo o razvoju kibernetičkih oružja. Usporedbe se mogu vući između nekontrolirane proliferacije takvih oružja, koje su posljedica nemogućnost da ih se ograniči te visoke cijene što je postižu na globalnom tržištu oružja. Značaj događaja „Year Zero“ nadilazi izbor između kibernetičkog rata i mira. Ova objava je izvanredna iz političke, pravne i forenzičke perspektive“ (Wikileaks, 2017).

Međutim, iako je WannaCry bio idealan kandidat za izvedbu kibernetičkog Pearl Harbora, zapravo je, u svom dosegu i posljedicama, podbacio. Nekako je za očekivati od tajnih kibernetičkih oružja razvijenih od strane američkih tajnih službi da uzrokuju padove aviona i eksplozije nuklearnih elektrana, a ne onemogućavanje pristupa liječničkim kartonima pacijenata i prekid prikazivanja voznog reda njemačke željeznice na kolodvorskim zaslonima. Napad je prekinuo ranije spomenuti dvadesetdvogodišnji britanski stručnjak za kibernetičku sigurnost MalwareTech koji je veoma povoljno kupio domenu koja je unutar koda samog sadržaja bila postavljena kao „kill switch“ ili prekidač te time uzrokovao prestanak širenja zaraze. Takvo što ne može biti vezano uz globalnu prijetnju.

Hrvatski su se mediji također prihvatili zlonamjernog *ransomware* sadržaja WannaCry kao globalne prijetnje iako je u Hrvatskoj zabilježeno svega 205 slučajeva zaraze. Štoviše, kako je već navedeno, iz UVNS-a je kazano kako WannaCry nije bila ozbiljna prijetnja. Međutim, o ovom su incidentu generirana 44 članka na 5 najvećih portala, a i televizijske su se kuće borile kako bi došle do izjava stručnjaka koji će pojasniti o čemu je točno riječ, zašto se trebamo bojati te na koji način se zaštititi. Iako su prenošene složene upute za zaštitu računala, zapravo je potrebno bilo napraviti redovnu nadogradnju operativnog sustava kako bi se zaraza onemogućila. Mjesec dana kasnije se odvila slična kampanja zlonamjernim *ransomware* sadržajem NotPetya koju su mediji ponovno proglasili globalnim kibernetičkim napadom, a Index.hr je čak objavio naslov „NOVI VELIKI CYBER NAPAD Hakirane tvrtke diljem svijeta, napadnut i Černobil". Podaci pokazuju kako je napadom pogođeno svega 16 500 uređaja, a u Černobilu je pogođen sustav za nadzor radijacije, međutim straha od radijacije nije bilo. Napad je iskorištavao potpuno iste ranjivosti kao i WannaCry, koje su bile zakrpane gotovo 4 mjeseca prije napada.

Uzme li se sve u obzir, možemo govoriti o tome kako je kibernetička sigurnost hipersekuritizirana, tj. da se naglašava mogućnost „Cyber Pearl Harbora", iako dosadašnji podaci i slučajevi to ne pokazuju. Mediji, u Hrvatskoj, najčešće o kibernetičkoj sigurnosti govore kao izvoru velikih prijetnji, prenaglašavajući činjenicu kako je riječ o globalnom problemu pa tako svaku potencijalnu prijetnju prikazuju kao prijetnju koja može poremetiti život u Hrvatskoj. Međutim, činjenica je kako je stvarna situacija zapravo medijski nezanimljiva, a mediji koriste svaku situaciju kako bi prijetnju uvećali do krajnjih granica te uzrokovali dodatan strah među korisnicima koji potom grozničavo prolaze kroz savjete koje ti isti mediji objavljuju kako bi se osjećali barem malo sigurnije.

Ti savjeti se sastoje od svakodnevnih praksi koje bi korisnik trebao poduzimati prilikom rada na računalu ili bilo kakvom elektroničkom uređaju, a mogu se odnositi na dodatnu provjeru identiteta osobe s kojom komuniciramo, nadogradnje antivirusnog programa, vanjske provjere uređaja poput bankomata, provjere adresa kojima pristupamo, provjere protokola koje koristimo, provjere adresa elektroničke pošte, ali ne više u polju pošiljatelja nego u tijelu zaglavlja jer se polje pošiljatelja može lako lažirati. Ono što izbjegavaju napomenuti, a čini srž kvalitetne zaštite od kibernetičkih ugroza je zdrav razum.

Dvije su stvari sigurne kod kibernetičke sigurnosti. Zdrav razum je najbolji oblik zaštite jer korisniku omogućava da na temelju dosadašnjih saznanja djeluje u novim situacijama te prepozna rizičnu situaciju. Rječnikom teoretičara učenja, savjeti koje prenose mediji spadaju u pasivno učenje tj. izravan transfer znanja što je karakteristično za bihevioriste. S druge strane, kognitivisti učenje promatraju kao stvaranje kognitivnih struktura koje nam omogućavaju obradu novih informacija na temelju postojećih saznanja te internalizaciju znanja kao aktivan proces. Ukratko, ne postoji popis koraka koje će netko moći poduzeti kako bi prepoznao kibernetičku prijetnju, ali postoji mogućnost razvijanja prepoznavanja rizičnih situacija što podrazumijeva mnogo više truda i ulaganja, ali i puno veću fleksibilnost i na koncu sposobnost obrane od ugroza. Christopher Hadnagy, jedan od najpoznatijih sigurnosnih stručnjaka, utemeljitelj SECTF-a na DEFCON-u, piše kako kvalitetan sigurnosni program ne čini objašnjavanje što je to dobra lozinka i od koliko bi se ona znakova trebala sastojati, već demonstracija koliko je brzo hakeru potrebno da probije neku slabu lozinku kako bi se osvijestila važnost pravilnog, odgovornog i opreznog, ali ne prestrašenog pristupa (Hadnagy, 2011: 343).

Krajnji korisnik bi trebao konzumirati tako definiran rizik te svoju kognitivnu suverenost, kako je naziva Beck (2001: 79), prepustiti stručnjacima zbog vjerovanja kako je preuzimanje vlastite sudbine u svoje ruke nerealan i vrlo opasan potez (Furedi, 2008: 107). Nepraćenje tih koraka predstavlja opasnost ne samo za njega, nego za cijeli sustav oko njega, a pritisak se na njega vrši navođenjem najstrašnijeg scenarija uspješno izvedenog kibernetičkog napada.

Rizik svakako postoji, ali treba osvijestiti kako običan korisnik jednostavno nije dovoljno atraktivna meta za potpunu demonstraciju moći kvalitetno izvedenog kibernetičkog napada. Stuxnet je, između niza ostalih primjera, pokazao koliko kibernetički napad zapravo može te je pokazao kako ne postoji zaštita protiv kvalitetno izvedenog kibernetičkog napada. S druge strane, Stuxnet je plod rada najviše razine sigurnosnih stručnjaka s gotovo neograničenim budžetom te ne bi bilo racionalno koristiti ga za iznuđivanje novaca ili krađu fotografija s računala.

Kada je riječ o sigurnosnim stručnjacima, svakako treba napomenuti kako oni snažno utječu na tehnifikaciju diskursa te ga čine udaljenijim i nerazumljivijim običnom korisniku kao što je vidljivo na temelju savjeta za zaštitu od računalno-sigurnosnih ugroza objavljenih od strane nadležnih službi. Štoviše, oni postoje gotovo odvojeni od običnog korisnika potpuno nedotaknuti njegovim potrebama. Koriste besplatan operativni sustav kojeg razvija sama zajednica računalnih

stručnjaka, Linux, a koji je nemjerljivo manje podložan kibernetičkim napadima od proizvoda tvrtke Microsoft. Također, kao što je već navedeno, sigurnosni stručnjaci obične korisnike promatraju očima tehnološke elite koja im pruža najosnovnije upute o tome kako se donekle zaštititi od najučestalijih napada koji su trenutno aktivni.

Razliku između računalno-sigurnosnih stručnjaka i običnog korisnika izvrsno ilustrira jedna situacija kojoj je autor prisustvovao u okviru sigurnosne konferencije FSeC u Varaždinu 2017. godine. Konferencija je bila podijeljena na izlagački dio i dio službenih predavanja i radionica. Predstavljajući Nacionalni CERT, pokušalo se podijeliti promotivni materijal u obliku zapakirane USB memorije. Veoma brzo je primijećeno kako posjetitelji uzimaju sve promotivne materijale osim USB-ova. Kada je jedan od sigurnosnih stručnjaka posjetitelja upitan zašto je tome tako, odgovorio je: „Nikad ne uzimam nepoznat USB. Religija mi brani. Tko zna što se na njemu nalazi?“.

5. ZAKLJUČAK

Kibernetička sigurnost svakako predstavlja značajan aspekt svakodnevnog života u informacijskom društvu, međutim, važno je razlikovati svakodnevne slučajeve i dosege „uobičajenih dnevnih aktivnosti napadača“ od korištenja posebno razvijenih kibernetičkih oružja koja se temelje na tajnim ranjivostima. Iako postoji mogućnost da kupac nekog pametnog televizora bude prisluškivan te da se prikupljaju podaci o njemu, valja se zapitati kome bi bilo u interesu da takvo što napravi. Računalne prijevare se ne razlikuju, osim po mediju provedbe, od običnih prijevara, a napadač računa na lakovjernost i pohlepu žrtve koje se ne mogu anulirati doslovnim praćenjem općenito napisanih sigurnosnih praksi. Slučajevi pokazuju kako kibernetičko oružje posjeduje stvaran potencijal za narušavanje sigurnosti, međutim, takvi slučajevi su još uvijek rijetkost u svijetu, a pogotovo u Hrvatskoj. Mediji, s druge strane svaku moguću prijetnju prikazuju kao hipersekuritiziranu, pretjeranu, odnoseći se samo na krajnje posljedice uspješno izvedenog napada. WannaCry je, zbog 205 slučajeva, dobio čak 44 članka, dok su se svi ostali računalno-sigurnosni incidenti u 2017. godini raspodijelili na preostalih 10.

Dobar je pokazatelj i broj registriranih *botova* u Republici Hrvatskoj, podatku koji se temelji na vanjskim izvorima koji dostavljaju informacije Nacionalnom CERT-u te prikazuju okvir stvarnog stanja. Riječ je o broju zaraženih računala u Republici Hrvatskoj, a koja su dio neke *botnet* mreže kojom upravlja zlonamjerni korisnik kako bi izvodio DDoS i DoS napade.

Specifično je za ovaj tip zlonamjernog sadržaja to što ne ostavlja tragove na računalu te djeluje u pozadini ni na koji način mijenjajući iskustvo korisnika na računalu.

U 2017. godini u Hrvatskoj je nekom vrstom zlonamjernog *botnet* sadržaja bilo zaraženo približno 320 000 uređaja, a koji su se koristili u izvedbi složenih napada. Međutim, zbog činjenice kako ne postoji šteta za korisnika te kako je riječ o samo jednom uređaju koji čini milijunsku *bot* mrežu, ovakav podatak jednostavno nije dovoljno atraktivan da bi bio prikazan i u jednom od promatranih članaka.

Činjenica je kako je uređaja sve više i kako s njima dolazi sve veći broj potencijalnih prijetnji koje mogu biti ostvarene iskorištavanjem velikog broja ranjivosti. Međutim, to što ranjivosti, a s njima i mogućnosti postoje, ne znači kako će netko stvarno te ranjivosti i iskoristiti.

Nažalost, mediji stvaraju sliku u kojoj prijetnje izlaze iz svakog elektroničkog uređaja, ali se može zaključiti, na temelju analize medijskog prostora, da takvo što nije empirijski utemeljeno.

6. LITERATURA

Knjige i članci

Abbate, J. (1999). Inventing the Internet. Camridge-Massachusetts-London-England: The MIT Press

Austin, J. L. (1962). How To Do Things With Words. Oxford: Clarendon Press

Barlow, J.P. (1996) „A Declaration of the Independence of Cyberspace“. U J. Casimir (ur.) *Postcards from the Net: An Intrepid Guide to the Wired World,* str. 365–7

Beck, U. (2001). Rizično društvo: U susret novoj moderni. Beograd: Filip Višnjić

Bell, D. (1999). The coming of post-industrial society: A venture in social forecasting. New York: Basic Books

Buzan, B., Wæver, O., de Wilde, J. 1998. Security: A new framework for analysis. Bolder – London: Lynne Rienner Publishers

Castells, M. (2000) Uspon umreženog društva. Informacijsko doba: Ekonomija, društvo i kultura. Svezak 1. Zagreb: Golden marketing

Castells, M. (2001). The Internet Galaxy: Reflexions on the Internet, Business, and Society. Oxford: Oxford University Press

Duff, A. (2014) Key principles of the good information society. U Kommers, P. & Isaias, P. (ur.) *Proceedings of 13th IADIS International Conference on e-Society*, 175-182

Furedi, F. (2008) Politika straha: S onu stranu ljevice i desnice. Zagreb: Izdanja Antibarbarus

Gartzke, E. 2013. The Myth of Cyberwar. Bringing War on the Internet Back Down to Earth. *International Security , 38(2),* str. 41-73

Hadnagy, C. 2011. Social Engineering: The Art of Human Hacking. Indianapolis: Wiley Publishing Inc.

Hansen, L. i Nissenbaum, H. 2009. Digital Disaster, Cyber Security, and the Copenhagen School. U *International Studies Quarterly, 53(4),* str. 1155-1175.

Jožanc, N. (2015). Studija slučaja u komparativnoj politici. U: *Politička misao 52 (3),* str. 35-58

Kovačević, B. (2014). Cyberwar – Američka izlika za novi rat? U: *Polemos: časopis za interdisciplinarna istraživanja rata i mira 16 (32),* str. 91-110

Leiner, B. M., 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“. U: *ACM SIGCOMM Computer Communication Review 39 (5),* str. 22-31

Littman, J. (1996). The fugitive game: Online with Kevin Mitnick: The inside story of the great cyberchase. New York: Little Brown & Co.

Luhmann, N. (1990). Essays on self-reference. New York-Oxford: Columbia University Press Gillespie, A. A. (2017). The Electronic Spanish Prisoner: Romance Frauds on the Internet. U: *The Journal of Criminal Law 81 (3)*, str. 217-231

McDonald, M. 2008 Constructivism. U Williams, P. D. (ur.) *Security studies: An introduction.* London and New York: Routledge, str. 152-169.

Milardović, A. 2010. Globalno selo. Sociologija informacijskog društva i cyber kulture. Zagreb: Centar za politološka istraživanja

Moore, G. E. (1965). "Cramming more components onto integrated circuits". U: *Electronics, 38 (8),* str. 114-117

Nikodem, K. (2009). Kiborzi i „djeca po narudžbi“. Prilog sociološkom istraživanju osnova cyber kulture. U: *Socijalna ekologija: časopis za ekološku misao i sociologijska istraživanja okoline 18 (2),* str. 107-129

Ryan, J. (2010). A history of the Internet and the digital future. London: Reaktion Books

Schatz, D., Bashroush, R., Wall, J. (2017). „Towards a more representative definition of cyber security“. U: *The journal of digital forensics, security and law* 12(2), str 53-74

Shen Tsien, H. (1954). Engineering cybernetics. New York-Toronto-London: McGraw-Hill Book Company

Stallman, R. (1985). The GNU Manifesto. U: *Dr. Dobb's Journal of Software Tools 10 (3)*

Vojković, G. i Štambuk-Sunjić, M. (2016). „Konvencija o kibernetičkom kriminalu i kazneni zakon Republike Hrvatske“. U: *Zbornik radova Pravnog fakulteta u Splitu* 43(1), str. 123-136

Wiener, N. (1948). „Cybernetics“. U: *Scientific American 179 (5)*, str. 14-19

Williams, M. J. (2008). Cooperation and conflict. U: *Security studies, reflexive modernization and the risk society 43 (1),* str. 57-79

Williams, P. D. 2008. Security studies: An introduction. U Williams, P. D. (ur.) *Security studies: An introduction.* London and New York: Routledge, str. 1-13

Yin, R. K. (1994). Case study research: Design and methods. Thousand Oaks: Sage Publications

Internetski izvori

Akcijski plan za provedbu nacionalne strategije kibernetičke sigurnosti (2015). URL: https://www.uvns.hr/hr/aktualnosti-i-obavijesti/nacionalna-strategija-kiberneticke-sigurnosti (pristupano 5.12.2018.)

Analiza WannaCry Ransomwarea (2018). URL: https://www.cert.hr/wp-content/uploads/2018/02/WannaCry.pdf (pristupano 20.8.2018.)

B. S. (1.12.2017) „Ne nasjedajte na ovaj lažni mail iz porezne, mogli biste ostati bez podataka“. URL: https://www.tportal.hr/tehno/clanak/ne-nasjedajte-na-ovaj-lazni-mail-iz-porezne-mogli-biste-ostati-bez-podataka-20171201 (pristupano 5.9.2018.)

B. S. (6.9.2017) „Oprez na društvenim mrežama: Lažni general ženu iz Gruda koštao 20.000 kuna“. URL: https://www.tportal.hr/tehno/clanak/oprez-na-drustvenim-mrezama-lazni-general-zenu-iz-gruda-kostao-20-000-kuna-20170906 (pristupano 5.9.2018.)

Barlow, J. P. (2016) „A Declaration of the Independence of Cyberspace“. URL: https://www.eff.org/cyberspace-independence (pristupano 6.9.2018.)

Burt, T. (2018) „Protecting democracy with Microsoft AccountGuard“. URL: https://blogs.microsoft.com/on-the-issues/2018/08/20/protecting-democracy-withmicrosoft-accountguard/ (pristupano 20.8.2018.)

Collins, K. (3.8.2017.) „The hackers behind the WannaCry ransomware attack have finally cashed out“. URL: https://qz.com/1045270/wannacry-update-the-hackers-behind-ransomware-attack-finally-cashed-out-about-140000-in-bitcoin/ (pristupano 1.9.2018.)

CVE Details (2017). URL: https://www.cvedetails.com/cve/CVE-2017-0143/ (pristupano 1.9.2018.)

CVE Details (2017). URL: https://www.cvedetails.com/cve/CVE-2017-0145/ (pristupano 1.9.2018.)

D. M. (8.4.2017) „Lažni bankar prevario dvije žene, uzeo im 3.900 kuna za klađenje“. URL: https://www.index.hr/vijesti/clanak/lazni-bankar-prevario-dvije-zene-uzeo-im-3900-kuna-za-kladjenje/962246.aspx (pristupano 7.9.2018.)

Gaščić, D. (15.5.2017) „Više nitko nije siguran: Hakeri su „srušili“ i hrvatsku policiju?“ URL: https://www.24sata.hr/tech/vise-nitko-nije-siguran-hakeri-su-srusili-i-hrvatsku-policiju-524554 (pristupano 6.9.2018.)

Godišnji izvještaj rada Nacionalnog CERT-a u 2017. godini (1.3.2018.) URL: https://www.cert.hr/godisnji-izvjestaj-rada-nacionalnog-cert-a-za-2017-godinu/ (pristupano 7.9.2018.)

Greenberg, A. (2.7.2018.) „Mind the gap: This researcher steals datawith noise, light and magnets“. URL: https://www.wired.com/story/air-gap-researcher-mordechai-guri/ (pristupano 28.8.2018.)

Hruškovec, I. (12.1.2017.) „Nova prijetnja: Poruke iz lažne Porezne žele do vaših podataka“. URL: https://www.24sata.hr/tech/nova-prijetnja-poruke-iz-lazne-porezne-zele-do-vasih-podataka-550701 (pristupano 6.9.2018.)

Hruškovec, I. (27.10.2017.) „Kriminalci u akciji: Kako ćete zaštititi svoju karticu od krađe“. URL: https://www.24sata.hr/tech/kriminalci-u-akciji-kako-cete-zastititi-svoju-karticu-od-kra-e-545891 (pristupano 6.9.2018.)

I. G. (28.4.2017.)“Hakeri od Cro Copa tražili otkupninu: 'Bolje mu je da ga ne nađu, ako ga nađe policija - jadna mu majka'“. URL: https://www.index.hr/sport/clanak/hakeri-od-cro-copa-trazili-otkupninu-bolje-mu-je-da-ga-ne-nadju-ako-ga-nadje-policija-jadna-mu-majka/966418.aspx (pristupano 7.9.2018.)

Jurić, M. (2.10.2017.) „Lopovi imaju sve naprednije metode za varanje građana, ali zaštititi se možete na prilično jednostavan način“. URL: https://dnevnik.hr/vijesti/hrvatska/iako-su-pokusaji-

prijevara-sve-napredniji-svijest-gradjana-jos-je-uvijek-jako-niska---494631.html (pristupano 5.9.2018.)

M. V. (26. 5.2017.) „OPREZ Nova prijevara putem maila na bizarno jednostavan način izvlači novac od naivnih ljudi“. URL: https://www.index.hr/vijesti/clanak/oprez-nova-prijevara-putem-maila-na-bizarno-jednostavan-nacin-izvlaci-novac-od-naivnih-ljudi/972860.aspx (pristupano 6.9.2018.)

Microsoft SMB Protocol and CIFS Protocol Overview (31.5.2018.) URL: https://docs.microsoft.com/en-us/windows/desktop/fileio/microsoft-smb-protocol-and-cifs-protocol-overview?fbclid=IwAR0Zmo5mPQbdxvkffm8XP--e57mGoOgtYIOHUVjvmN6xv3g3xqjL1RKsDOk (pristupano 12.9.2018.)

Murnane, K. (2016) „Scientists Can Use WiFi To Read Your Emotions“. URL: https://www.forbes.com/sites/kevinmurnane/2016/09/20/mits-csail-lab-creates-a-system-that-identifies-peoples-emotions-using-wireless-signals/#4ee06c866b53 (pristupano 1.9.2018.)

Negovetić L., Blotnej, B. (12.1.2017.) „Hakeri napali Traumatologiju: Srušio se sustav s podacima“. URL: https://www.24sata.hr/news/hakeri-napali-traumatologiju-srusio-se-sustav-s-podacima-506981 (pristupano 7.9.2018.)

Nigerian Letter or '419' Fraud (2018). URL: https://www.fbi.gov/scams-and-safety/common-fraud-schemes/nigerian-letter-or-419-fraud?fbclid=IwAR1cOCRJrE817d7TlavX0EjlGRvwjl6w72snAjrJ7X-yiRho9Rqrgo34qO8 (pristupano 15.10.2018.)

Oracle Security Vulnerability Disclosure Policies“ (2018). URL: https://www.oracle.com/corporate/security-practices/assurance/vulnerability/disclosure.html (pristupano 5.12.2018.)

Palmer, D. (11.5.2018) „WannaCry ransomware crisis, one year on: Are we ready for the next global cyber attack?“.URL: https://www.zdnet.com/article/wannacry-ransomware-crisis-one-year-on-are-we-ready-for-the-next-global-cyber-attack/(pristupano 2.9.2018.)

Perekalin, A. (2017) „WannaCry: Are you safe?“. URL: https://www.kaspersky.com/blog/wannacry-ransomware/16518/ (pristupano 10.9.2018.)

Pronađene mnoge ranjivosti u pacemaker uređajima (2017). URL: https://www.cert.hr/31250/ (pristupano 10.9.2018.)

Schneier, B. (23.5.2017) „Who Are the Shadow Brokers?“. URL: https://www.theatlantic.com/technology/archive/2017/05/shadow-brokers/527778/ (pristupano 1.9.2018.)

Security. (2018) URL: https://technet.microsoft.com./en-us/library/security/ms17-010.aspx. (pristupano 5.5.2018.)

Smartphones industry: Statistics & Facts (2018). URL: https://www.statista.com/topics/840/smartphones/ (pristupano 21.8.2018.)

Symantec Security Response. (22.5.2018.). URL: https://www.symantec.com/connect/blogs/wannacry-ransomware-attacks-show-strong-links-lazarus-group (pristupano 1.9.2018.)

The Cambridge Analytica Story, Explained (2018). URL: https://www.wired.com/amp-stories/cambridge-analytica-explainer/ (pristupano 5.12.2018.)

The Mentor (2005) „The Conscience of a Hacker“. URL: https://archive.org/stream/The_Conscience_of_a_Hacker/hackersmanifesto.txt (pristupano 5.9.2018.)

Tonton Cypher (2017) „Kevin Mitnick [Hacker Documentary]“. URL: https://www.youtube.com/watch?v=tIVAjgiatqM (pristupano 4.12.2018.)

Tsukayama, H. (2018) How Samsung moved beyond its exploding phones. URL: https://www.washingtonpost.com/business/how-samsung-moved-beyond-its-exploding-phones/2018/02/23/5675632c-182f-11e8-b681-2d4d462a1921_story.html?noredirect=on&utm_term=.46d008b29dd4 (pristupano 2.9.2018.)

V. L. (12.1.2017.) „Hakeri srušili sustav KBC-a Sestara milosrdnica, pacijenti ostali bez snimaka lomova“. URL: https://www.vecernji.hr/vijesti/hakeri-sruseli-sustav-kbc-a-sestara-milosrdnica-pacijenit-ostali-bez-snimaka-lomova-1141823 (pristupano 5.9.2018.)

Vault 7: CIA Hacking Tools Revealed (2017). URL: https://wikileaks.org/ciav7p1 (pristupano 20.9.2018.)

WannaCry kampanja u RH. URL: https://www.uvns.hr/hr/aktualnosti-i-obavijesti/wannacry-kampanja-u-rh (pristupano 5.12.2018.)

WannaCry: Are you safe? (13.5.2017.). URL: https://www.kaspersky.com/blog/wannacry-ransomware/16518/ (pristupano 10.9.2018.)

What is free software? (13.8.2018.). URL: https://www.gnu.org/philosophy/free-sw.html (pristupano 10.9.2018.)

What is the Equation Group & who are the Shadow Brokers? (11.05.2017.). URL: https://securityscorecard.com/blog/what-is-equation-group-shadow-brokers (pristupano 1.9.2018.)

Wikileaks. URL: https://wikileaks.org/ciav7p1/ (pristupano 10.8.2018.)

Wranka, M. (15.5.2017.) „Šest pitanja o hakerskom napadu koji je uzdrmao svijet“. URL: https://www.tportal.hr/tehno/clanak/sest-pitanja-o-hakerskom-napadu-koji-je-uzdrmao-svijet-20170515 (pristupano 5.9.2018.)

Wranka, M. (18.5.2017.) „Ako nisu ugroženi životi – ne započinjite razgovor s hakerima i ne plaćajte otkupninu“. URL: https://www.tportal.hr/tehno/clanak/ako-nisu-ugrozeni-zivoti-ne-zapocinjite-razgovor-s-hakerima-i-ne-placajte-otkupninu-20170517 (pristupano 5.9.2018.)

Ž. L. (2018) „Microsoft: Rusi su izveli hakerski napad na američki Senat“. URL: https://www.index.hr/vijesti/clanak/microsoft-rusi-su-izveli-hakerski-napad-na-americki-senat/2018854.aspx (pristupano 5.12.2018.)

Dokumenti

Nacionalna taksonomija računalno-sigurnosnih incidenata - https://www.cert.hr/wp-content/uploads/2018/06/Nacionalna-taksonomija-ra%C4%8Dunalno-sigurnosnih-incidenata.pdf

Statistički pregled temeljnih sigurnosnih pokazatelja i rezultata rada u 2017. godini Ministarstva unutarnjih poslova. Zagreb, siječanj 2018.

Godišnji izvještaj rada Nacionalnog CERT-a u 2017. godini

Sažetak

U ovom je radu analizirano stanje kibernetičke sigurnosti u Republici Hrvatskoj s posebnim težištem na prikazu računalno-sigurnosnih incidenata koji su imali izvorište ili metu unutar hrvatskog IP adresnog prostora ili .hr domene. Analizom internetskih članaka pet najpopularnijih portala u Republici Hrvatskoj, utvrdit će se u kojem odnosu stoje sa stvarnim brojem računalno-sigurnosnih incidenata. Također, kako bi se opisao razvoj kibernetičke sigurnosti, riječi će biti o razvoju Interneta, cyber kulture te kibernetičkog prostora. Konceptima sekuritizacije, ali i hipersekuritizacije, svakodnevnenih sigurnosnih praksi te tehnifikacije prikazat će se na koji se način stvara slika o kibernetičkoj sigurnosti u javnosti te kakvu poziciju akteri sekuritizacije predviđaju običnom korisniku.

Ključne riječi: Kibernetička sigurnost, sigurnost, sekuritizacija, incidenti, hakeri

Abstract

This master thesis gives an overview of cyber security in Republic of Croatia with special focus on cyber security incidents that had their point of origin or target in Croatian IP space or .hr domain. Analysis of relevant Internet articles of five most popular Croatian news portals will show in what relation does it stand to number of cyber security incidents. Furthermore, to describe progress of cyber security, evolution of Internet, cyber culture and cyber space will be shown. By concepts of securitization and especially hypersecuritization, everyday security practices and discourse techification, the of picture of cyber security in public will be shown as will be the position of that actors of securitization predict for basic users.

Key words: Cyber security, security, securitization, incidents, hackers