Cyber terorizam: studija slučaja Anonymous

Muža, Adriana

Sveučilište u Zagrebu

Filozofski fakultet

Odsjek za sociologiju

Diplomski rad

Cyber terorizam: studija slučaja Anonymous

Student: Adriana Muža

Mentor: dr. sc. Mirko Bilandžić, red. prof.

Zagreb, 20. lipnja 2023.

Sadržaj

1. Uvod

Živimo u informatičkom dobu, kada nam je cijeli svijet dostupan na dlanu. Sve više i više ovisimo o tehnologiji i odbacujemo stare načine radi novih, jednostavnijih i bržih. Bitna stavka takvog života jest, jedan od najvećih izuma 20. stoljeća, Internet. Internet je tkivo naših života. Ako je informacijska tehnologija današnji ekvivalent električne energije u industrijskoj eri, u naše doba Internet bi se mogao usporediti i s električnom mrežom i s električnim motorom zbog njegove sposobnosti da distribuira snagu informacija kroz cijelo područje ljudske aktivnosti.

Pristup internetu kao potpuno otvorenom sustavu je danas omogućen gotovo svakome tko posjeduje neki od uređaja s tom mogućnosti, kao na primjer računalo, mobilni telefon ili tablet, a broj tih uređaja koji se mogu spojiti na Internet je sve veći. Internet se doživljavao kao novo sredstvo za komunikaciju i razmjenu podataka, bez obzira gdje su korisnici bili locirani. Trebao je biti besplatan i dostupan svima te se doživljavao kao da ima neograničeni potencijal (Caravelli i Jones, 2019: 9). No, kao i svaku tehnologiju prije, s vremenom se našao način kako koristiti Internet kao neku vrstu oružja. Sve više se raspravlja o privatnosti podataka od pojave WikiLeaks, stranice na kojoj je moguća objava povjerljivih podataka s time da je izvor uvijek zaštićen. Veliku pomutnju je napravio i Edward Snowden kada je putem WikiLeaksa objavio povjerljive datoteke CIA. Pitanje kibernetičke sigurnosti na međunarodnoj razini se postavilo i kada se otkrilo kako Rusija manipulira izborima u drugim zemljama.

Brojni pokušaji definiranja cyber terorizma nisu rezultirali općeprihvaćenim tumačenjem. O cyber terorizmu se često raspravlja u medijima, politici i sigurnosnim izvješćima, ali nažalost uz velike nedosljednosti u pogledu značenja koncepta. Široka medijska pokrivenost često je sklona zanemariti da, prema većini autora, zapravo nije uočen niti jedan jasan slučaj cyber terorizma. Posljedično, izraz se koristi za opisivanje gotovo svega, od jednostavnog hakiranja haktivizma, do fatalnih kibernetičkih napada koji uzrokuju ozbiljnu financijsku štetu i krvoproliće. Haktivizam je relativno novi fenomen koji je nastao 1980-ih iz susreta hakerskih zajednica i aktivista tehnoloških entuzijasta. Popularnost mu je porasla u kasnim 1990-ima, a posebno se proslavio pojavom kolektiva Anonymous.

Anonymous je kroz godine bio povezan s brojim događanjima u svijetu, uvijek pokušavajući podići svijest te poboljšati samu situaciju. Jedan od novijih slučajeva s kojima je Anonymous povezan jest invazija Rusije na Ukrajinu, te Anonymous-ovom objavom cyber rata ruskoj vladi i predsjedniku Vladimiru Putinu.

Ovim radom, prvo ćemo pokušati sintetizirati brojne definicije cyber terorizma s ciljem identificiranja njegovih ključnih obilježja. U drugom dijelu rada ćemo pomoću analize sadržaja elektronskih članaka sa portala vijesti sagledati napade Anonymous-a na Rusiju. Pomoću tih ključnih kriterija cyber terorizma i saznanja dobivenih iz analize sadržaja pokušat ćemo odrediti odgovor na naše istraživačko pitanje: Jesu li napadi Anonymous-a na Rusiju cyber terorizam? Ovime se nadamo otkriti je li ovo jedan od prvih pravih slučajeva cyber terorizma ili se radi o nekoj drugoj vrsti cyber napada.

2. Informacijsko društvo

Prema Hrvatskoj enciklopediji Internet se definira kao

> „svjetski sustav međusobno povezanih računalnih mreža. Zahvaljujući razvoju informacijske i komunikacijske tehnologije, postao je osnova suvremene elektroničke komunikacije, a postupno dobiva i značenje vodećega komunikacijskoga medija današnjice. Razmjena informacija među računalima različitih sustava i tehnoloških rješenja najvećim je dijelom omogućena normizacijom protoka podataka te zajedničkim sustavom adresiranja.“

Prema Castellsu (2001) Internet je tehnološka osnova za organizacijski oblik informacijskog doba: mrežu. Mreža je skup međusobno povezanih čvorova. Mreže su vrlo stari oblici ljudske prakse, ali su u naše vrijeme zaživjele novi život postavši informacijske mreže, koje pokreće Internet. Mreže imaju izvanredne prednosti kao organizacijski alati zbog svoje inherentne fleksibilnosti i prilagodljivosti, ključnih značajki za preživljavanje i napredak u okruženju koje se brzo mijenja. To je razlog zašto se mreže šire u svim domenama gospodarstva i društva, nadmašujući vertikalno organizirane korporacije i centralizirane birokracije.

U posljednjoj četvrtini dvadesetog stoljeća spojila su se tri neovisna procesa, uvodeći novu društvenu strukturu pretežno utemeljenu na mrežama: 1) potrebe gospodarstva za fleksibilnošću upravljanja i za globalizacijom kapitala, proizvodnje i trgovine; 2) zahtjevi društva u kojem su vrijednosti otvorene komunikacije i individualne slobode postale najvažnije; i 3) izvanredan napredak u telekomunikacijama i računalstvu koji je omogućila mikroelektronička revolucija. Pod tim uvjetima, Internet, opskurna tehnologija bez mnogo primjene izvan osamljenih svjetova računalnih znanstvenika, hakera i kontrakulturnih zajednica, postao je poluga za prijelaz u novi oblik društva, umrežno društvo (Castells, 2001: 2).

Webster (2006: 8-9) smatra da je moguće razlikovati pet definicija informacijskog društva, od kojih svaka predstavlja kriterije za identificiranje novog. To su: 1) tehnološka definicija koja ističe razvoj novih tehnologija, 2) ekonomska definicija koja teži novim ekonomskim mogućnostima te ističe ekonomsku važnost informacija, 3) zaposlenička definicija koja je usmjerena na promjene u području zaposlenja (deagrarizacija), 4) prostorna definicija ističe smanjenje prostornih ograničenja i mogućnosti povezivanja, te 5) kulturna definicija koja je usmjerena na razvoj virtualne stvarnosti te kako informacijsko društvo utječe na način razmišljanja i djelovanja.

Ove definicije se ne moraju međusobno isključivati, iako teoretičari naglašavaju jedan ili drugi čimbenik u predstavljanju svojih posebnih scenarija. Međutim, ono što ove definicije dijele jest uvjerenje da kvantitativne promjene u informacijama stvaraju kvalitativno novu vrstu društvenog sustava, informacijsko društvo. Na taj način svaka definicija rezonira na gotovo isti način: danas ima više informacija, stoga imamo informacijsko društvo.

Postoji šesta definicija informacijskog društva čija glavna tvrdnja nije da danas ima više informacija (očigledno ih ima), nego da je karakter informacija takav da je promijenio način na koji živimo. Sugestija je da je teorijsko znanje/informacija srž našeg ponašanja ovog vremena (Webster, 2006: 9).

Informacijsko društvo obično karakteriziraju četiri značajke. Prva jest da informacije postaju sve važnije kao ekonomski, kulturni i politički resursi na kojima su organizirana nova globalna informacijska ekonomija i informacijska društva, s većinom zanimanja koja se temelje na radu na informacijama ili znanju. Zatim, smatra se da

dinamična inovacija ICT-a[1] transformira potencijal za obradu, pohranjivanje i prijenos informacija na načine koji su prije bili nezamislivi, a ICT stoga postaje sve prisutniji u našim životima. Treća značajka jest da elektronički umrežena gospodarstva i društva iz temelja transformiraju naše koncepte vremena i prostora, omogućujući tokovima informacija da nadiđu vremenske i fizičke granice i time olakšavaju procese globalizacije i umrežavanja poduzeća. Te na kraju, informacija postaje kulturno prevladavajuća kroz multimedijske aplikacije, ali također postaje sve osporavanija i manje smislena, u svijetu natjecateljskih, kontradiktornih i stalno promjenjivih slika, znakova i poruka (Bell i suradnici, 2004: 94-95).

Koncept "informacijskog društva" pomogao je znanstvenicima da usmjere pozornost i prikupe zajedno širok raspon i raznolik niz fenomena, od promjena zanimanja, preko novih medija i digitalizacije, do razvoja u visokom obrazovanju. Unatoč tome, koncept informacijskog društva je manjkav, posebice u načinu na koji tvrdi da prikazuje nastanak novog tipa društva. Webster (2006: 263) tvrdi da je usredotočenost na informacijske trendove ključna za razumijevanje karaktera današnjeg svijeta, iako je većina scenarija informacijskog društva od male pomoći u tome.

Možemo reći kako je 21. stoljeće doba inovacija, promjena i globalizacija, koje zahtijeva stjecanje i razvoj temeljnih kompetencija u informacijskim, komunikacijskim, intelektualnim, pravnim i društvenim sferama javnog života. Načini učenja nečeg novog se mijenja iz temelja, a time i samo znanje, koje je suvremenoj osobi neophodno. Suvremeni procesi transformacije jačaju poziciju informacijskog društva u kojem ključnu ulogu imaju informacije i znanje. U današnje vrijeme informacijski resursi i znanje zauzimaju vodeće mjesto u životnim strategijama i društvenim praksama društvenih subjekata (Levchenko, Dyak, Hrytsiuk, 2021).

E. Rohovskiy (2008, prema Levchenko, Dyak, Hrytsiuk, 2021) u *SAD: Informacijsko društvo (ekonomija i politika)* tvrdi da su glavne karakteristike informacijskog društva dostupnost informacijskih resursa potrebnih za profesionalne aktivnosti ili osobne svrhe, dostupnost suvremenih informacijskih tehnologija i sredstava komunikacije, kao i stvaranje razvijene informacijske strukture koja

[1] ICT (Information And Communications Technology = Informacijska I Komunikacijska Tehnologija) obuhvaća svu digitalnu računalnu i komunikacijsku opremu. Osim računala, od poslužitelja do dlanova ili ručnih uređaja, ICT uključuje mobilne (mobilne) telefone i digitalnu televiziju (Bell i suradnici, 2004: 90).

omogućuje stalno ažuriranje informacijskih resursa potrebnih za društveni, gospodarski i znanstveno-tehnološki razvoj.

U suvremenom informacijskom društvu postoje ozbiljne proturječnosti. Konkretno, tvrdi se da tehnologija prodire u sve sfere ljudskog života. Postoji iluzija da će se mnogi ljudi uskoro riješiti mnogih tradicionalnih aktivnosti, u kojima će ih zamijeniti stroj. Čak se smatra kako se i moralni, politički i društveni problemi mogu riješiti na temelju strojne tehnologije. Pogrešivost ovog pristupa nije očita. Naravno, ne treba zaboraviti da osoba uvijek ima i imat će sposobnost osobne procjene, interpretacije informacija. Osobni dio je sastavni dio ljudskog "ja". Osim znanja koje stroj može pohraniti, čovjek ima intuiciju, vjeru, osjećaje i druga svojstva specifična samo čovjeku (Masian, 2022).

Dok se u ranijim raspravama informacijsko društvo pretežito gledalo kroz pozitivnu leću, noviji autori više razmatraju negativne posljedice informacijskog društva. Tako Masian (2022) ističe kako se staro uništava, ali nastavlja postojati, staro i novo se isprepliću, kao rezultat toga, društvena stvarnost, oštro se komplicira, a svijet nema vremena prilagoditi se. U nemogućnosti da svjetske vlasti osiguraju veću složenost upravljanja, krenuli su u suprotnom smjeru – maksimalno pojednostavljenje upravljanog sustava. To podrazumijeva uništenje mnogih institucija, struktura, grupa, tipova osobnosti i identiteta modernog društva. Između ostalog, to se odnosi na deindustrijalizaciju, uništavanje obrazovanja, „moronsku kulturu“ (debilizaciju).

2.1. Razvoj interneta

Povijesna proizvodnja određene tehnologije oblikuje njezin sadržaj i upotrebu na načine koji traju i nakon njezinog izvornog početka, a Internet nije iznimka od ovog pravila. Povijest interneta pomaže nam razumjeti staze njegovog budućeg stvaranja povijesti.

Podrijetlo Interneta nalazi se u ARPANET[2]-u, računalnoj mreži koju je postavila Agencija za napredne istraživačke projekte (ARPA) u rujnu 1969. godine. ARPA je osnovana 1958. godine od strane Ministarstva obrane Sjedinjenih Američkih Država sa

[2] ARPANET - Advanced Research Projects Agency Network, eksperimentalna računalna mreža koja je bila preteča Interneta

zadatkom mobilizacije istraživačkih resursa prema izgradnji tehnološke vojne nadmoći nad Sovjetskim Savezom nakon lansiranja prvog Sputnika 1957. (Castells, 2001: 10). Izgradnja ARPANET-a opravdana je kao način dijeljenja računalnog vremena on-line između različitih računalnih centara i istraživačkih grupa koje rade za agenciju.

Sljedeći korak bio je omogućiti povezivanje ARPANET-a s drugim računalnim mrežama, počevši od komunikacijskih mreža kojima je ARPA upravljala, PRNET[3]-a i SATNET[4]-a. Time je uveden novi koncept: mreža mreža. Godine 1973. dva računalna znanstvenika, Robert Kahn, iz ARPA-e, i Vint Cerf, tada na Sveučilištu Stanford, napisali su rad u kojem su ocrtali osnovnu arhitekturu Interneta. Da bi računalne mreže međusobno komunicirale, trebali su im standardizirani komunikacijski protokoli (Castells, 2001: 11). Godine 1978. Cerf, Postel. i Crocker, koji rade na Sveučilištu Južne Kalifornije, podijelili su protokol kontrole prijenosa (TCP[5]) na dva dijela, dodajući međumrežni protokol (IP), čime su dobili TCP/IP protokol, standard na kojem Internet i danas radi.

Castells (2001: 12) nadalje navodi kako je u veljači 1990. ARPANET, tada već tehnološki zastario, stavljen izvan upotrebe. Nakon toga, oslobodivši Internet iz svog vojnog okruženja, američka vlada zadužila je Nacionalnu znanstvenu zakladu (NSF[6]) za njegovo upravljanje. Ali NSF-ova kontrola Interneta bila je kratkog vijeka. Uz tehnologiju računalnog umrežavanja u javnoj domeni i telekomunikacije u potpunoj deregulaciji, NSF je brzo nastavio s privatizacijom Interneta. Ministarstvo obrane ranije je odlučilo komercijalizirati tehnologiju interneta, financirajući proizvođače računala u Americi da uključe TCP/IP u svoje protokole 1980-ih. Do 1990. većina računala u Americi imala je mogućnost umrežavanja, postavljajući temelj za širenje međusobnog umrežavanja.

Početkom 1990-ih brojni pružatelji internetskih usluga izgradili su vlastite mreže i postavili vlastite pristupnike na komercijalnoj osnovi. Nakon toga, Internet je brzo rastao kao globalna mreža računalnih mreža. To je omogućeno originalnim dizajnom ARPANET-a, koji se temelji na višeslojnoj, decentraliziranoj arhitekturi i otvorenim komunikacijskim protokolima.

[3] PRNET - The Packet Radio Network
[4] SATNET - Atlantic Packet Satellite Network
[5] TCP - Transmission Control Protocol
[6] NSF - National Science Fondation

Ono što je omogućilo Internetu da zagrli cijeli svijet bio je razvoj svjetske mreže (World Wide Web - WWW). To je sistem za razmjenu informacija koju je 1990. razvio engleski programer Tim Berners-Lee koji radi u CERN[7]-u, europskom istraživačkom centru za fiziku visokih energija sa sjedištem u Ženevi. Definirao je i implementirao softver koji je omogućio dohvaćanje i doprinos informacijama s i na bilo koje računalo povezano putem interneta: HTTP[8], HTML[9] i URI[10] (kasnije nazvan URL[11]) (Castells, 2001: 15).

Do sredine 1990-ih Internet je bio privatiziran, njegova otvorenost omogućila je umrežavanje svih računalnih mreža bilo gdje u svijetu, svjetska mreža je mogla funkcionirati na odgovarajućem softveru, a javnosti je bilo dostupno nekoliko preglednika prilagođenih korisniku. Dok je internet nastao u glavama računalnih znanstvenika ranih 1960-ih, računalna komunikacijska mreža uspostavljena je 1969., a distribuirano računalstvo, interaktivne zajednice znanstvenika i hakera pojavile su se kasnih 1970-ih, za većinu ljudi, Internet je rođen 1995.

3. Kibernetički prostor

Kibernetički prostor je virtualni svemir. Definicije se razlikuju, ali pojam kibernetički prostor obično uključuje čitav niz usluga, uključujući mrežne igre, razmjenu trenutnih poruka i fizičke uređaje koji se koriste za pohranu podataka. Internet djeluje kao osnova za kibernetički prostor jer je javno dostupan i može se proširiti beskonačnim podatkovnim mrežama (Vuković, 2012). Kibernetički prostor postoji u perspektivi ljudi, ne poznaje granice država, odnosno ne postoji u geografskom smislu prostora.

David Bell i suradnici (2004: 41) objašnjavaju kibernetički prostor kao

> „izraz koji se koristi za opisivanje prostora stvorenog spajanjem elektroničkih komunikacijskih mreža kao što je Internet koji omogućuje komunikaciju posredovanu računalom (CMC) između bilo kojeg broja

[7] CERN - The European Organization for Nuclear Research
[8] HTTP - The Hypertext Transfer Protocol
[9] HTML - HyperText Markup Language
[10] URI - Uniform Resource Identifier
[11] URL - Uniform Resource Locator

> ljudi koji mogu biti geografski raspršeni diljem svijeta. To je javni prostor gdje se pojedinci mogu sastajati, razmjenjivati ideje, dijeliti informacije, pružati društvenu podršku, poslovati, stvarati umjetničke medije, igrati simulacijske igre ili sudjelovati u političkim raspravama. Takva ljudska interakcija ne zahtijeva zajedničku fizičku ili tjelesnu prisutnost, već ju karakterizira međusobno povezivanje milijuna ljudi diljem svijeta koji komuniciraju putem e-pošte, sustava oglasnih ploča i soba za čavrljanje.“

Pojam *Kibernetički prostor* stvorio je pisac William Gibson u cyberpunk romanu Neuromancer (1984). Gibson (1984: 67, prema Bell, 2006: 2) opisuje kibernetički prostor kao

> „Konsenzualna halucinacija koju svakodnevno doživljavaju milijuni legitimnih operatera. … Grafički prikaz podataka izvučenih iz banaka svakog računala u ljudskom sustavu. Nezamisliva kompleksnost. Svjetlosne linije nizale su se u neprostoru uma, nakupinama i konstelacijama podataka. Kao gradska svjetla, koja se povlače.“

Deklaracija o neovisnosti kiberprostora (1996) Johna Perryja Barlowa jedan je od mnogih dokumenata koji pokušavaju odjednom definirati i razgraničiti arenu elektroničke interakcije, trgovine i informacija kibernetičkog prostora. Čineći to, tekst konstruira stil utopije, svijet koji je, Barlowovim riječima, „posvuda i nigdje“ (1996: 366), svijet u kojem se pretpostavlja da je revolucionarna politika imanentna strojevima koji ju strukturiraju i omogućuju. Utopijski scenarij koji se nudi u *Deklaraciji* književne je prirode, ali političke težnje. Barlow piše: "Mi stvaramo vlastiti društveni ugovor jer je naš svijet drugačiji" (1996: 366).

Kibernetički prostor je sastavni dio modernog društva. On je vrlo učinkovit alat i pokretač aktivnosti. Utječe ili je integriran (vidljivo i neprimjetno) u sve aspekte svakodnevnog života većine ljudi i digitalno prenesenih aktivnosti. Sastavljen od ICT-a, postao je dio kritične infrastrukture koja podupire socioekonomski rast, upravljanje nacijama i pod-društvima, vođenje poslovanja i ostvarivanje ljudskih prava i sloboda. Kao dio svojih poželjnih i očekivanih posljedica, omogućio je tvrtkama i vladama stvaranje prihoda i zapošljavanja, omogućio pristup poslovanju i informacijama, omogućio e-učenje i olakšao vladine aktivnosti. Kao takvi, Internet i ICT postali su

nezamjenjivi i omogućili mnoge pozitivne aspekte suvremenog načina života. Međutim, obrnuto, prihvaćanje ovih tehnologija od strane korisnika također je omogućilo manje poželjnim aktivnostima, rizicima i prijetnjama kao što su izloženost informacijama, kriminal, špijunaža, terorizam i ratovanje da iskoriste tu istu infrastrukturu (Reid &Van Niekerk, 2014). Upravo zbog toga se pojavila potreba za kontroliranjem i zaštitom kibernetičkog prostora te se sve više govori o kibernetičkoj sigurnosti.

3.1. Kibernetička sigurnost

U svojoj knjizi Nacionalna sigurnost: prognoza ugroze, Mirko Bilandžić (2019: 6) navodi kako je sigurnost neophodan element svakog društva te da ju treba shvatiti kao „javno dobro“. Ona proizlazi iz društvenih procesa te je razumljiva samo kao povezan koncept, tj ona uvijek povezuje konkretan referentni okvir, sektor djelatnosti i poseban način razmišljanja o politici. Generalno, sigurnost možemo definirati kao nedostatak ugroze ili odsutnost straha.

Kibernetička sigurnost se odnosi na skup tehnika koje se koriste za zaštitu integriteta mreža, programa i podataka od napada, oštećenja ili neovlaštenog pristupa. Može se promatrati kao skup mehanizama koji štite od unutarnjih i vanjskih prijetnji. Interne prijetnje mogu biti nedostaci u softverskom programu ili operativnom sustavu, dok su vanjske prijetnje neovlašteni pristup ili ljudske pogreške (Bihari, 2019).

Vuković (2012) kibernetičku sigurnost definira kao „primjenu tehnologija, procesa i kontrola za zaštitu sustava, mreža, programa, uređaja i podataka od kibernetičkih napada. Cilj joj je smanjiti rizik od kibernetičkih napada i zaštititi od neovlaštenog iskorištavanja sustava, mreža i tehnologija“.

Rječnik Merriam-Webster kibernetičku sigurnost definira kao "mjere poduzete za zaštitu računala ili računalnog sustava (kao na internetu) od neovlaštenog pristupa ili napada" (Merriam-Webster, 2020, prema Cains et. al., 2021).

Međunarodna telekomunikacijska unija (ITU) definira kibernetičku sigurnost kao "skup alata, politika, sigurnosnih koncepata, sigurnosnih mjera zaštite, smjernica, pristupa upravljanju rizikom, radnji, obuke, najboljih praksi, osiguranja i tehnologija koje se mogu koristiti za zaštitu kibernetičkog okruženja te organizacija i imovina

korisnika" unutar ciljeva cyber sigurnosti fokusa povjerljivosti, dostupnosti i integriteta (CIA - confidentiality, availability, and integrity) (ITU, 2008, prema Cains et. al., 2021).

Bihari (2019) ovim ciljevima dodaje i ranjivost te ih naziva mehanizmima kibernetičke sigurnosti. Opisuje povjerljivost kao načelo da se informacije ne otkrivaju ako to nije namjera. Integritet je osiguranje točnosti i potpunosti podataka tijekom cijelog životnog ciklusa što znači da se podaci ne mogu mijenjati na neovlašteni način. Kako bi bilo koji informacijski sustav služio svojoj svrsi, pohranjeni podaci moraju biti dostupni kada su potrebni, stoga su sustavi visoke dostupnosti dizajnirani da ostanu dostupni cijelo vrijeme izbjegavajući prekide usluge zbog nestanka struje, kvarova hardvera i nadogradnji sustava. Ranjivost je osjetljivost sustava ili greška u dizajnu hardvera ili softvera i može se iskoristiti za dobivanje neovlaštenog pristupa. Stolno računalo suočava se s drugačijim prijetnjama u usporedbi s računalom koje se koristi u vladinoj ili vojnoj mreži.

Iako ove definicije izražavaju potrebu zaštite imovine, one su usmjerene na hardver i softver i ne uzimaju u obzir ljudske aspekte kibernetičke sigurnosti. Nadalje, na definiranje kibernetičke sigurnost utječe multidisciplinarnost pojma. Komponente fizičkog okruženja i ljudskih, odnosno društvenih interakcija izostavljene su iz ovih definicija što ometa sposobnost cyber istraživača i analitičara rizika da holistički procijene rizik koji predstavlja sustave, mreže i korisnike u cyber domeni. Pristup koji uključuje čovjeka dovodi u pitanje trenutne definicije kibernetičke sigurnosti usmjerenu na stroj jer uključuje polja kao što su sociologija, psihologija, znanost o riziku i odlučivanju kao i mnoga druga (Cains, et.al, 2021).

Hakiranje, krađa, cyber uhođenje, krađa identiteta, zlonamjerni softver, navođenje i zlostavljanje djece samo su neki od cyber zločina u ovom području. Cyber sigurnost bavi se sigurnošću kibernetičkog prostora od kibernetičkih kriminalaca. Važno je učinkovito implementirati kibernetičku sigurnost kako bi zaštitili internetski sustav i povjerenje ljudi u ovom sustavu od raznih kibernetičkih napada (Bihari, 2019).

Kibernetički kriminal kombinacija je informacijskih, financijskih i osobnih sigurnosnih prijetnji. Kibernetički alati za zločin smatraju se Internetom, e-poštom i društvenim mrežama, ali popis postaje sve duži godinu po godinu. Dakle, jednostavniji život u društvenoj sferi je na scenu donio nove tehnologije zbog čega su se pokrenuli i neki sigurnosni problemi i otvorila su se vrata za kibernetičke kriminalce da uđu i

napadnu unutar kibernetičkog prostora s manje napora (Burden i Palmer, 2003). Caravelli i Jones (2019: 7) tako navode neke primjere zloupotrebe kibernetičkog prostora. Jedan od tih primjera je primjer društvenih mreža koje same po sebi čine baze podataka. Britanska konzultantska tvrtka Cambridge Analytica je uvidjela tu priliku preuzevši osobne podatke milijuna korisnika Facebook-a. Cambridge Analytica stvorila je aplikaciju "This Is Your Digital Life", te je tada organizirala postupak informirane suglasnosti za istraživanje u kojem bi se nekoliko stotina tisuća korisnika Facebook-a složilo ispuniti anketu za plaćanje koja je bila samo za akademsku upotrebu. Međutim, Facebook je ovoj aplikaciji omogućio ne samo prikupljanje osobnih podataka od ispitanika u anketi, već i od njihovih prijatelja na Facebooku. Ti podaci su se koristili za razne političke kampanje, između ostalog i onu Donalda Trumpa. No ovakva zloupotreba kibernetičkog prostora se ne koristi samo u korporacijskom svijetu. Susrećemo i nacije poput Rusije koja hakiranjem remeti demokratske procese i utječe na izbore, ne samo u Sjedinjenim Američkim Državama već i u Ujedinjenom Kraljevstvu i drugim glavnim europskim narodima. U isto vrijeme, Kina je stvorila umjetnički oblik krađe obilnih količina tajnih vojnih i kadrovskih podataka vlada koje smatra protivnicima kao i podjednako velike količine zaštićenih informacija zapadnih korporacija (Caravelli i Jones, 2019: 8).

Burden i Palmer (2003) razlikuju dvije vrste kibernetičkog kriminala: „Istinski“ kibernetički kriminal (tj. neiskrena ili zlonamjerna djela koja ne bi postojala izvan internetske mreže okoliša, ili barem ne u istom oblik ili sa sličnim utjecajem), i kriminal koji je jednostavno "e-omogućen" (tj. kriminalno djelo poznato svijetu prije pojave svjetske mreži, ali koja je sada sve više prisutna preko Interneta).

Pod „Istinske“ kibernetičke zločine podrazumijevaju hakiranje, kibernetički vandalizam, širenje virusa, napade uskraćivanja usluga te otmicu domena imena.

Hakiranje je u mnogo čemu arhetipski kriminal 21. stoljeća, koristeći tehnologiju kao sredstvo stjecanje neovlaštenog pristupa privatnom računalnom sustavu, često u svrhu dobivanja povjerljive informacije ili počinjenje neke vrste prijevare. Bilo ono hakiranje "iz zabave" (tj. bez namjere nanošenja štete ili krađe podataka ili novca) ili kada je motiv za hakiranje aktivna namjera izvršiti daljnje kazneno djelo kao što je prijevara, zločin iz nepoštenje (npr. za krađu povjerljivih podatkovnih datoteka i prodati

ih trećoj strani ili koristiti podatke sadržane u njima za privatnu korist, uključujući ucjena) ili, na primjer, terorizam, ono je uvijek kazneno djelo (Burden i Palmer, 2003).

Kibernetički vandalizam obično je usmjeren na web stranice, koje su prvo hakirane, a zatim izmijenjene na način koji se ponekad može činiti šaljiv, ali će jednako često biti zlonamjeran ili čak i politički motivirani.

Većina nas je upoznata s problemom virusa, tj. kodom koji se obično širi e-poštom i zbog čega računala obavljaju određene funkcije, neke bezopasne (npr. učiniti da se odskočne ovce pojave na zaslon), drugi manje (npr. Brisanje podataka iz baza podataka ili prosljeđivanje pornografske poruke svima u adresaru e-pošte primatelja).

Kao e-omogućene zločine Burden i Palmer (2003) podrazumijevaju zlouporaba kreditnih kartica, krađu podataka, klevetu, ucjenu, pornografiju, Web stranice mržnje, pranje novca, kršenje autorskih prava, kibernetički terorizam i šifriranje.

Zlouporaba podataka koji su povjerljivi određenoj organizaciji ili osobi datira davno prije pojave Interneta, ali što to transformira u internetskom kontekstu je volumen i brzina kojom takve informacije mogu biti prisvojene, cijele knjižnice se prenose u nekoliko sekundi.

Nakon 11. rujna bilo je vidljiv potencijal Interneta kao alata za terorizam, ne samo kao sredstvo širenja informacija, ali i kao oružje. Caravelli i Jones (2019: 13) definiraju kibernetički terorizam kao unaprijed smišljene, politički motivirane napade protiv informacija, računalnih sustava, računalnih programa i baza podataka koje rezultiraju nasiljem nad vladama, poduzećima i pojedincima. Autori također dodaju još jednu dimenziju, napominjući kritičnu važnost Interneta u regrutiranju i raznim propagandni ciljevima.

4. Terorizam

Terorizam se, u različitim oblicima, prakticira kroz povijest i kroz široku paletu političkih ideologija. Postoji toliko definicija za riječ terorizam koliko postoji i metoda za njegovo izvršavanje. Izraz znači različite stvari za različite ljude, a pokušaj definiranja ili klasificiranja terorizma pokazuje se nemogućim. Međutim, većina

definicija terorizma ovisi o tri faktora: metoda (nasilje), meta (civilna ili vlada) i svrhu (usaditi strah i prisiliti političke ili društvene promjene) (Kushner, 2003: 378).

Uobičajeni element terorizma je upotreba nasilja, često, ali ne uvijek mu prethodi prijetnja nasiljem. Postoji neslaganje oko toga treba li to nasilje biti fizičko. Jesu li različiti oblici mentalne okrutnosti, na primjer, oblik terorizma? Namjera stvaranja straha je drugi uobičajeni element koji razlikuje teroristično nasilje od drugih oblika nasilja. Ovaj element predstavlja ideju kako je terorizam u konačnici oblik psiholoških operacija. Ova psihološka komponenta nastojanja stvaranja straha kao primarnog cilja, bilo u pojedincu, zajednici, državi ili korporaciji, bitna je za koncept terorizma. Još jedan element terorizma kao svrhovito djelovanje jest to da je teroristički čin oblik komunikacije koji ima za cilj poslati poruku straha i zastrašivanja, ne samo neposrednim žrtvama, već i široj publici (Anderson i Sloan, 2009).

Čini se da višestruke definicije terorizma kao fenomena ne doprinose našem razumijevanju onoga što se događa, tko je odgovoran za to, te kako se suprotstaviti i spriječiti ili, općenito, odgovoriti na ono što mnogi doživljavaju kao egzistencijalnu prijetnju svijetu koji poznajemo. Tijekom proteklih nekoliko desetljeća, ali intenzivnije od događaja 11. rujna 2001., znanstvenici, političari, vojni čelnici i praktički svaka upućena ili zainteresirana strana izašli su s nekom vrstom sveobuhvatne i ispravne definicije o tome što predstavlja teroristički čin ili u koje aktivnosti netko mora biti uključen da bi bio označen kao terorist. Ovo obilje riječi nije od velike pomoći u našem individualnom ili kolektivnom razumijevanju terorizma i netko bi mogao tvrditi da je kontraproduktivno da se uopće približimo razumijevanju s kim imamo posla (Haberfeld i von Hassell, 2009).

Ujedinjeni narodi (UN) definirali su terorizam tako da bi njegovi počinitelji i podržavatelji mogli biti stigmatizirani, izolirani i sankcionirani. Srž definicije - korištenje bilo kojeg sredstva da se „nezakonito i namjerno . . . nanosi smrt, ozljeda ili teška tjelesna ozljeda civilu ili bilo kojoj drugoj osobi koja ne sudjeluje aktivno u neprijateljstvima u situaciji oružanog sukoba, kada je svrha takvog djela, po svojoj prirodi ili kontekstu, zastrašivanje stanovništva, ili prisiliti vladu ili međunarodnu organizaciju da poduzmu ili se suzdrže od poduzimanja bilo koje radnje" - učinkovito je dogovorena barem od 1990-ih i korištena je u konvenciji UN-a za borbu protiv financiranja terorizma (Law, 2015: 4).

Bilandžić u svojoj knjizi *Sjeme zla: uvod u studije terorizma* (2014) navodi neke od razloga ponuđenih od strane izvršnog direktora *International Institute for Counter-Terrorism*, Boaz Ganora, zašto je teško doći do jedinstvene definicije terorizma:

> „pravno i političko poimanje prijepornog pojma terorizma, kao i ono društvenih znanosti i javnosti je divergentno; definicija terorizma je povezana s procesima (de)legitimacije i kriminalizacije; postoje mnogi tipovi terorizma s različitim formama i manifestacijama; u dva stoljeća postojanja značenje terorizma se mijenjalo; granice terorizma i ostalih oblika političkog nasilja nisu čvrsto jasne“ (2014: 73).

Wayman Mullins (1997:15; prema Bilandžić, 2014: 83) nudi kriterije, odnosno pet elemenata, koje bi trebala sadržavati jedinstvena definicija terorizma. 1) nasilje nije krajnji cilj, već sredstvo za njegovo ostvarivanje; 2) prijetnja je prvenstveni cilj nasilja u terorizmu, nasilje se koristi samo do one granice kada je prijetnja podržana; 3) psihološki utjecaj, odnosno strah je važan za ostvarivanje političke promjene. Strah u široj populaciji ima veći učinak na političke promjene nego nasilje upućeno prema vladi; 4) ciljane žrtve nisu one koje stradaju direktno od nasilja već one koje mu svjedoče; 5) konačni cilj terorizma jest politička promjena, bez obzira na postojanje drugih motiva i ciljeva, politička promjena je uvijek srž terorizma.

S obzirom na kompleksnost i promjenjivost pojma terorizam, kao i na neslaganje oko njegovog definiranja, možda bismo se trebali usredotočiti odgovaraju li događaji koje nazivamo terorizmom određenim kriterijima (primjerice gore navedenim), umjesto beskrajno pokušavati ostvariti nemoguće. Zapravo, možda bismo se trebali baviti puno važnijim pitanjima unutar studije terorizma umjesto bavljenjem pitanjem koje nikada neće dobiti svoj odgovor zbog ničeg drugog nego politike.

4.1. Povijest terorizma

U dugoj povijesti terorizma, imena određenih skupina više puta se pojavljuju, te one dijele tendenciju korištenja nasilja za promicanje i provođenje svojih političkih (ili vjerskih) uvjerenja. Kao začetak terorizma možemo smatrati Zelote još u 1. stoljeću. Zeloti su bili vjerski nacionalisti, radikalne grupe židovskih domoljuba, iz prvog stoljeća koji su se pobunili protiv rimske okupacije (Bilandžić, 2014: 53). Skriveni u

gužvi, uboli bi svjetovne službenike, svećenike i vojnike svojim bodežima (sicarii), a zatim pobjegli stapajući se u gužve. Njihovi su postupci stvorili okruženje straha u kojem se nikome nije moglo vjerovati i svi su se bojali. Zeloti su pokrenuli tehnike čistog terora koje su bile korištene u budućim generacijama „istinskih vjernika“ (Anderson i Sloan, 2009: 57).

Riječ *Asasin* došla je iz druge vjersko-političke skupine. U 11. i 12. stoljeću, Ismailiti su bili aktivisti u jugozapadnoj Aziji organizirani u trupe ubojica, poznate kao Fedayeen, doslovno "samožrtvovnici" (Anderson i Sloan, 2009: 58). Asasini su bili voljni poduzeti napade na sunitske vladare unatoč izvjesnosti vlastite smrti ili zarobljavanja, budući da im je bilo osigurano mjesto na nebu ako padnu kao mučenici boreći se na Božjem putu. Kao i kod suvremenih bombaša samoubojica, bijeg se nikada nije planirao niti pokušavao jer se vjerovalo kako se žrtvuju za veće dobro. Naziv Asasini proizašao je iz riječi *hašašini*, kako su ih nazivali zbog korištenja hašiša prije izvođenja atentata (Bilandžić, 2014: 55).

Pojam *teror* kao središnji koncept terorizma, pojavljuje se prvo u francuskom jeziku u 14. stoljeću, a potom u engleskom u 16. stoljeću. Pojam dolazi od latinske riječi terrere, terreo, što znači „dovesti nekoga do strepnje posredstvom velikog straha“ (Bilandžić, 2014: 56).

Moderni terorizam nastao je tijekom Francuske revolucije i reakcije koja je uslijedila. Pod Građaninom Maximilien Robespierreom i njegovim Odborom za javnu sigurnost, *Veliki teror* bio je usmjeren protiv stvarnih i izmišljenih neprijatelja revolucije (Anderson i Sloan, 2009: 58). Robespierre je 5. veljače 1794. godine definirao što je mislio pod *terorom*. To nije bio politički program ili ideologija, već sredstvo za postizanje cilja: trijumf republikanske demokracije nad njezinim brojnim neprijateljima. Revolucionari su tek kasnije upotrijebili precizne izraze *terorist, terorizam* ili *teror*, na neprijateljski, retrospektivan način, kada su se distancirali od sustava kakav je funkcionirao u Francuskoj 1793-4. Riječ *teror* već je imala mnogo upotreba, ali ideju da je Francuska pretrpjela *sustav terora* prvi je izrazio pokajnički jakobinac, Bertrand Barère, 29. srpnja 1794. dan nakon što je njegov nekadašnji kolega Robespierre giljotiniran. Rječnik Académie française iz 1798. definirao je terorizam kao sustav ili režim terora, a teroriste kao agenta ili pristašu terora koji je nastao zloporabom revolucionarnih mjera (Rapport, 2015: 63).

Teror je užasnuo europsku maštu i bacio sjenu na revolucionarne pokrete u sljedećim generacijama. U razdoblju između pada Napoleona Bonapartea i revolucija 1848., europski revolucionari uključivali su spektar od liberalnih, ustavnih monarhista do ranih revolucionarnih socijalista, koji su se svi u različitim stupnjevima protivili autoritarnom poretku koji se pojavio 1815. godine. Za većinu, državni teror 1793.–4. bio je upozorenje koje je trebalo poslušati. Bilo je više nego simbolično važno da je, kada je Druga republika proglašena na ruševinama posljednje francuske monarhije 1848. godine, jedan od prvih dekreta privremene vlade bio proglasiti ukidanje smrtne kazne za političke zločine (Rapport, 2015: 71).

Drugom polovicom 19. stoljeća teroristi počinju češće koristiti atentat kao sredstvo za ostvarenje ciljeva. Počinje cijelim nizom atentata na američke predsjednike Abraham Lincoln, 16. američki predsjednik, ubijen 1865. godine u nadi kako će njegova smrt pomoći jugu u građanskom ratu. James Abram Garfield, 20. američki predsjednik, 1881. godine, zatim William McKinley, 25. američki predsjednik ubijen je 1901. godine. No ni Europa nije izbjegla trend atentata, primjerice: ubojstvo austrougarske carice Elizabete 1898., talijanskog kralja Umberta I 1900., nekoliko pokušaja atentata na njemačkog državnika Otto von Bismarcka te još nekoliko uspješnih atentata diljem Europe (Bilandžić, 2014: 59).

Tijekom tog razdoblja razvile su se i moderne terorističke taktike. Organizacija Narodnaya Volya (Narodna volja) koristila je dinamit i bombe u svojim atentatima na dužnosnike carskog režima. U tom su razdoblju sljedbenici anarhizma dalje razvijali terorizam kao oružje propagande i komunikacije (Anderson i Sloan, 2009: 59).

Konstantna prijetnja anarhističkog terorizma nacionalnim državama ali i međunarodnom poretku prisilila je 1898. velike sile da se sastanu u Rimu, što možemo smatrati prvom međunarodnom konferencijom o protuterorizmu. No države nisu razmatrale uzroke ili njihovu moguću odgovornost za probleme na koje se odgovara nasiljem (Bilandžić, 2014: 60-61). Jedini cilj jest bio na anarhiste nalijepiti etiketu luđaka.

Vladavinu terora koju je započela Francuska revolucija Staljin je ubilačkom učinkovitošću proširio masovnim čistkama i pokaznim suđenjima 1920-ih i 1930-ih, a dosegla je svoj vrhunac u genocidu koji je pokušan pod Trećim Reichom sa svojim koncentracijskim logorima i krematorijima. Ova ubojita kombinacija tehnologije i

pratećih organizacijskih sposobnosti dovela je do sazrijevanja terorizma odozgo. U 1960-ima, "teror odozdo" se nastavio kao nova generacija u kojoj su revolucionari pokušali svrgnuti ono što su smatrali represivnim režimima. U Latinskoj Americi je korištenje terora kao dijela pobunjeničkih pokreta ubrzala kubanska revolucija i pokušaj njezina izvoza u Srednju i Južnu Ameriku. Ernesto Che Guevara možda je najbolje utjelovio mističnost koja je okruživala nove revolucionare. Guevara je naglašavao potrebu za primjenom taktike terora u gerilskom ratu koji je u osnovi ruralan. Naglasio je važnost focoa — male, tajne skupine pobunjenika koji bi mogli zapaliti vatru revolucije (Anderson i Sloan, 2009: 60).

U 1980-ima države su sve više podržavale razne terorističke skupine u ostvarivanju svojih vanjskopolitičkih ciljeva. Državno sponzorirani terorizam od strane Sovjetskog Saveza, Sjedinjenih Američkih Država, Irana, Iraka, Sirije, Sjeverne Koreje i drugih vlada omogućio je teroristima razinu financijske, logističke i taktičke podrške koja im u prošlosti nije bila dostupna. O vezama između raznih terorističkih skupina i njihovih državnih sponzora žestoko se raspravljalo, posebice od strane Sjedinjenih Američkih Država, koje su nastojale provjeriti stupanj upletenosti Moskve u teroriste u posljednjim danima hladnog rata. Državno pokroviteljstvo, osobito na Bliskom istoku, nastavlja povećavati sposobnost raznih terorističkih skupina da slijede svoje ciljeve i za države pokrovitelje da slijede svoje geopolitičke ciljeve kroz posredničko ratovanje (Anderson i Sloan, 2009: 61).

Krajem 20. i početkom 21. stoljeća ponovno jača terorizam s vjerskom dimenzijom. Najizraženija je skupina Al Qa´ida, zbog koje terorizam postaje središnja sigurnosna prijetnja međunarodnog poretka te postaje izazov suvremenog svijeta. Bez obzira na vjersku dimenziju ovaj terorizam jest i dalje politički motiviran. Ovaj oblik terorizma ustvari instrumentalizira religiju, koristi njenu ekstremizaciju te ju militarizira (Bilandžić, 2014: 69-70).

Razvijanjem tehnologije, pogotovo računala i interneta, pojavljuje se novi, lakši način širenja informacija i ideja. No, te ideje i podaci koji se šire putem interneta nisu uvijek korišteni u pozitivne svrhe, a Internet olakšava drugima ulazak u našu privatnost i pristup osobnim podacima. S pojavom sigurnosnih pitanja vezanih uz kibernetički prostor, pojavljuje se i novi oblik terorizma, cyber terorizam.

4.2. Cyber terorizam

Iako uobičajeni elementi nasilja, političke motivacije, prijetnje i straha gore opisani daju liniju kontinuiteta koji prolaze kroz dugu i složenu povijest terorizma, treba uzeti u obzir i da je tehnološka inovacija stvorila novi oblik terorizma.

Sigurno je da internet teroristima pruža sve veću mogućnost širenja svojih uvjerenja i ciljeva bez opasnosti da ih se uhvati. Web stranica, na primjer, daje terorističkoj skupini mogućnost da objavi svoj manifest kroz anonimnost kibernetičkog prostora. Što je možda još značajnije, internet pruža sredstva pomoću kojih razne terorističke skupine mogu održavati svoju sigurnost putem anonimnosti kibernetičkog prostora, ali sve više imaju sposobnost i prilike koordinirati operacije s vrlo različitim skupinama koje mogu dijeliti opći strateški cilj destabiliziranja grada, države ili regije. Zbog toga se sada razvijaju u samostalne, slobodne ćelije koje se mogu uključiti u usklađene napade, ali koje mogu ostati oslobođene potrebe za vanjskom potporom, bilo državnom ili nedržavnom. Kao takve, grupe će biti sve teže identificirati, jer se radi o manjim skupinama. Zbog toga će biti teže i suzbiti njihovo djelovanje budući da nisu dio veće organizacije koja se može staviti pod nadzor tehničkih obavještajnih službi ili infiltrirati od strane neprijateljske obavještajne službe.

Od posebne važnosti bilo je sigurno korištenje interneta, kako bi se zadržala ta anonimnost. To je postignuto korištenjem Dark Weba, dijela interneta kojem ne pristupaju popularne tražilice poput Google-a ili Yahoo-a. Neki stručnjaci tvrde da se čak 90 posto informacija sadržanih na internetu ne može pristupiti putem konvencionalnih tražilica. Često "nevidljive" informacije nalaze se kroz ono što je označeno kao *Dark Web*. Najjednostavnije rečeno, Dark Web se sastoji od web stranica koje postoje na šifriranim mrežama. Mnogi od njih, zbog svoje anonimnosti, promiču ilegalne aktivnosti poput prodaje droge ili kupnje vatrenog oružja (Caravelli i Jones, 2019: 14).

Jedan od prvih prijavljenih incidenata koji je sadržavao aktivnosti slične onome što bi mogli biti elementi cyber terorizma dogodio se 1997. kada su etnički tamilski gerilci navodno preplavili veleposlanstva Šri Lanke tisućama elektroničkih poruka. Poruke e-pošte glase „Mi smo internetski crni tigrovi i ovo radimo kako bismo ometali vašu komunikaciju“. Bombardiranje elektroničkom poštom s oko 800 elektroničkih poruka trajalo je otprilike dva tjedna i navodno je imalo željeni učinak stvaranja straha u

veleposlanstvima. Napad se smatra prvim poznatim napadom terorista na računalne sustave neke zemlje, ali još uvijek nije klasificiran kao jasan slučaj cyber terorizma (Denning, 2001).

Neki (Anderson i Sloan, 2009: 271) smatraju kako je pojam cyber terorizam još teže definirati od samog terorizma iz razloga što mu u većini slučajeva nedostaje bitan element terorizma, tj. prijetnja ili uporaba nasilja. Prema tome, koliko god hakiranje moglo ometati bazu podataka ili bankovni sustav, ono se ne bi smatralo terorizmom osim ako namjeravani rezultati takvog ometanja mogu ili jesu doveli do fizičkog nasilja nad ljudima. Stoga, poremećaj reda letenja sam po sebi nije terorizam, ali poremećaj sustava kontrole zračnog prometa s namjeravanim učincima smrti putnika doista bi bio oblik terorizma.

Kushner (2003: 104) pak navodi kako neki vjeruju da će se hakiranje koristiti kao oružje za masovni poremećaj u kombinaciji s tradicionalnim terorističkim napadima, dok drugi tvrde da cyber teror malo nudi tradicionalnim teroristima, zbog nedostatka drame i male vjerojatnosti značajnih ozljeda ili smrti, ali i jer su tradicionalni teroristički alati, poput bombaša samoubojica, još uvijek prilično učinkoviti. Unatoč tome, koordinirani kibernetički napad na određene infrastrukture, poput računala koja kontroliraju i koordiniraju zrakoplove ili onih koji upravljaju burzom, mogao bi izazvati značajan kaos.

Većini slučajeva kojima se pripisuje termin cyber terorizma nedostaje neki od ključnih elemenata terorizma. Uglavnom je riječ o, već spomenutom, nedostatku prijetnje ili uporabe nasilja, no često nedostaje i politički motiv hakera. Kako onda odrediti što čini cyber napadom terorizmom? Kako odrediti što cyber terorizam jest?

4.2.1. Definiranje cyber terorizma

Pojam cyber terorizam odnosi se na konvergenciju terorizma i kibernetičkog prostora, odnosno politički motiviranu sabotažu informacijskih sustava. Od 1990-ih, incidenti hakiranja, kibernetičkog kriminala i vrlo destruktivnih računalnih virusa bili su rašireni, ali mnogi vjeruju da pravi cyber terorizam ostaje više prijetnja, iako možda neizbježna, nego stvarnost.

Prema Kushneru (2003: 103) Barry Collin, s Instituta za sigurnost i obavještajne poslove u Kaliforniji, skovao je pojam cyber terorizam 1980-ih. U radu iz 1997. Collin je opisao moguće scenarije cyber terora. U jednom, cyber terorist hakira računalni sustav proizvođača žitarica i podiže razinu željeza u svakoj kutiji, uzrokujući da se nebrojena djeca razbole i umru. U drugom scenariju, cyber teroristi destabiliziraju cijelu zemlju masovnim napadima na financijske institucije i burze. Collinov treći scenarij, u kojem cyber terorist hakira sustav kontrole zračnog prometa, približio se stvarnosti kada je 1997. tinejdžer dobio pristup telefonskom prekidaču u maloj zračnoj luci u Massachusettsu i slučajno prekinuo sve komunikacije kontrolnog tornja na nekoliko sati. Bez obzira na to što je bio alarmantan, incident se više smatrao hakiranjem koje je pošlo po zlu nego cyber terorom jer u slučaju nije bilo političke motivacije. Do danas je to često slučaj, hakeri s alatima za onesposobljavanje ključnih državnih ili korporativnih računalnih sustava nemaju političku motivaciju da to učine, dok teroristi koji imaju motivaciju urušiti informacijske sustave kako bi izazvali kaos nemaju potrebne računalne vještine.

Kao odgovor na sve veći broj politički motiviranih hakiranja i kibernetičkih napada, izvješće Centra za strateške i međunarodne studije iz 1998. iznijelo je jednu od prvih često spominjanih definicija „Cyber terorizam znači unaprijed smišljene, politički motivirane napade podnacionalnih skupina ili tajnih agenata ili pojedinaca na informacijske i računalne sustave, računalne programe i podatke koji rezultiraju nasiljem nad neborbenim ciljevima“ (Centar za strateške i međunarodne studije, prema Taliha¨rm, 2010) .

Nekoliko godina kasnije, 2001., profesorica Dorothy E. Denning precizirala je definiciju Centra za strateške i međunarodne studije opisujući kako cyber terorizam

> „se općenito shvaća kao nezakoniti napadi i prijetnje napadima na računala, mreže i informacije pohranjene u njima kada su učinjeni radi zastrašivanja ili prisile na vladu ili njezine ljude u svrhu postizanja političkih ili društvenih ciljeva. Nadalje, da bi se kvalificirao kao cyber terorizam, napad bi trebao rezultirati nasiljem protiv osoba ili imovine, ili barem uzrokovati dovoljno štete da stvori strah. Napadi koji dovode do smrti ili tjelesnih ozljeda, eksplozija, pada zrakoplova, kontaminacije vode ili veliki ekonomski gubitak bili bi primjeri. Ozbiljni napadi na

> kritične infrastrukture mogli bi biti činovi cyber terorizma, ovisno o njihovom učinku. Napadi koji ometaju nebitne usluge ili koji uglavnom imaju visoke troškovi ne bi“ (Denning 2001, prema Taliha¨rm 2010).

Taliha¨rm (2010) pravi razliku između ciljano orijentiranih (uskih) i alatno orijentiranih (širokih) razumijevanja: Prvi identificira cyber terorizam kao sve politički ili društveno motivirane napade na računala, mreže i informacije, bilo da se izvode preko drugih računala ili fizički, kada uzrokuju ozljede, krvoproliće ili ozbiljnu štetu ili strah. Drugi označava sve radnje koje koriste internet ili računala za organiziranje i dovršetak terorističkih akcija kao cyber terorizam.

Plotnek i Slay (2019) su svojom taksonomijom pojma cyber terorizma razvili 6 elemenata (akter, motiv, namjera, sredstvo učinak, meta) te im dodali odgovarajuće elemente. Prilikom tog postupka dobili su rezultate: 1) akter: s predumišljajem i nedržavni, 2) motiv: ideološki i socijalni, 3) namjera: izazvati strah ili prisiliti, 4) sredstva: napad ili prijetnja napadom koji potječu iz kibernetičkog prostora, 5) učinak: posljedica koja se događa izvan kibernetičkog prostora (npr. psihološki, društveni, politički, fizički, ekonomski, ekološki) te 6) meta: civili, državne ili nedržavne. Plotnek i Slay (2019) nadalje ističu kako nakon identificiranja kritičnih atributa koji proizlaze iz postojećih definicija u literaturi, usklađenih s novopredloženom taksonomijom cyber terorizma, mogu predložiti novu definiciju kao što je:

> „Cyber terorizam je napad s predumišljajem ili prijetnja napadom od strane nedržavnih aktera s namjerom korištenja kibernetičkog prostora za izazivanje posljedica u stvarnom svijetu kako bi se izazvalo strah ili prisililo civilne, vladine ili nevladine mete u potrazi za društvenim ili ideološkim ciljevima. Posljedice u stvarnom svijetu uključuju fizičke, psihosocijalne, političke, ekonomske, ekološke ili druge posljedice koje se događaju izvan kibernetičkog prostora” (Plotnek i Slay, 2019).

Je li cyber terorizam poseban fenomen sa svojim karakteristikama ili podvrsta terorizma kao široke i raznolike kategorije nasilja? Prema nalazim Jarvis i McDonald (2015) neki cyber terorizam smatraju podvrstom terorizma, pri čemu se napad može kvalificirati kao cyber teroristički tek nakon što su sve komponente definicije terorizma ispravno zadovoljene. Stoga oni smatraju fizičko nasilje nad ljudima ili imovinom važnim elementom cyber terorizma. Međutim, to nije bio stav većine u njihovom

istraživanju. To što ovdje postoji, kao takav, kontrast s razumijevanjem terorizma *per se* postavlja pitanje postoje li kvalitativne razlike između terorizma i cyber terorizma. Ovo gledište cyber terorizam tretira kao podvrstu šire kategorije terorizma, ali istodobno priznaje da postoje kvalitativne razlike između to dvoje. Dodavanje kvalitativno različite potkategorije već postojećem konceptu ima potencijal imati važne naknadne učinke. U tom smislu, njihovi nalazi sugeriraju da je neslaganje oko koncepta cyber terorizma važno ne samo u procjeni i odgovoru na ovu konkretnu prijetnju. Ali, osim toga, ovo neslaganje također potiče znanstvenike da preispitaju, možda čak i promijene, svoje razumijevanje samog terorizma.

Prema definiciji Dorothy Denning (2001), kibernetički napadi koji bi se kvalificirali kao kibernetički terorizam trebali bi, osim što imaju političku ili društvenu motivaciju, donijeti dovoljan stupanj razaranja i poremećaja kako bi generirali onoliko straha i kaosa koliko i tradicionalni (fizički) teroristički činovi. Napadi na kritičnu infrastrukturu, kao što su elektroenergetika, telekomunikacije, vodoopskrba, nafta i plin te financijske institucije, koji rezultiraju ozbiljnom štetom mogu se smatrati cyber terorizmom. S druge strane, kibernetički napadi koji su pokrenuti protiv banaka i burzi i rezultiraju milijunima dolara štete, ali ne uključuju element društvene i političke motivacije, ne bi se smjeli označavati cyber terorizmom (Taliha¨rm, 2010).

4. 2. 2. Haktivizam i cyber terorizam

U posljednjih 30 godina, uspon interneta i njegovih tehnologija duboko je utjecao na sva područja društva, od ekonomije do tehnologije i od psihologije do politike. Aktivizam, kao društveni fenomen, nije izbjegao ovu evoluciju. Usvojio je nove metode prosvjeda i razvio nove ideologije na koje su uvelike utjecali infrastruktura kibernetičkog prostora, njegovi korisnici i alati (Denning 2015). Od ranih 1990-ih internetska zajednica svjedoči posebnom rastu novog fenomena koji je odigrao značajnu ulogu u pokazivanju kako sam internet može postati raskošno i vrijedno mjesto za političke borbe, građanski angažman i društvene prosvjede. Ovaj fenomen, koji kombinira tipične aspekte hakiranja sa sociopolitičkim vrijednostima i ideologijama preuzetim iz tradicionalnih oblika aktivizma, poznat je kao *haktivizam* (Denning, 2015).

Haktivizam je konvergencija hakiranja s aktivizmom, gdje se hakiranje ovdje koristi za označavanje operacija koje iskorištavaju računala na načine koji su neuobičajeni i često nezakoniti, obično uz pomoć posebnog softvera (hakerski alati). Haktivizam uključuje elektronički građanski neposluh, koji donosi metode građanskog neposluha u kibernetički prostor (Denning, 2001).

Haktivizmom se bavilo u različitim sektorima industrije kibernetičke sigurnost i akademske zajednice, uglavnom u području političkih znanosti, prava, sociologije, sigurnosnih studija i upravljanja. Akademska zajednica posebno se usredotočila na podrijetlo i evoluciju haktivizma, karakteristike specifičnih grupa kao što su Anonymous, veza između haktivizma kao novog oblika građanskog neposluha i tradicionalnijih društvenih prosvjeda, konfliktna pravna i etička pozicija haktivizma, te specifične tehnike koje koriste haktivisti (Romagna, 2019).

Denning (2001) naglašava razlike između aktivizma, haktivizma i kibernetičkog terorizma, ali se slaže da su granice između njih pomalo nejasne. Prema Denning, haktivisti obično imaju četiri glavna oružja: 1) virtualna sjedišta i blokade (haktivisti stvaraju toliko prometa na odabranoj web stranici da se ona zaglavi i ne može ispravno funkcionirati), 2) napadi e-poštom (poslužitelj e-pošte je napadnut tisućama e-pošte i radnja, opet, prekida normalno funkcioniranje), 3) hakiranje i provale u računala (npr. provala u web stranicu radi promjene informacija, oštećenje), i 4) računalni virusi i crvi.

U pravilu, haktivizam je politički prosvjed koji koristi virtualne metode i ne nastoji izazvati veliku financijsku štetu ili ozlijediti ljude, stoga ga ne treba kvalificirati kao cyber terorizam. Međutim, haktivizam nam daje uvid u ono što bi cyber teroristi mogli učiniti u većem opsegu budući da bi teroristi mogli upotrijebiti bilo koju od gore navedenih taktika za postizanje svojih politički motiviranih ciljeva. Virusi, posebno oni koji nose destruktivne posljedice, potencijalno su snažno oruđe u rukama cyber terorista. Drugi alati haktivizma, uključujući napade na računalne mreže, također bi se mogli iskoristiti za vrlo destruktivne ciljeve (Denning, 2001).

Oblici cyber terorizma s kojima se susrećemo uglavnom su povezani s internetskom propagandom, regrutiranjem i dobivanjem financijske potpore. S obzirom na ova razmatranja, razliku između haktivizma i cyber terorizma treba istražiti u kombinaciji tri elementa koji razlikuju ta dva fenomena: 1) postojanje/nedostatak fizičke štete ili barem ozbiljnog poremećaja vitalne infrastrukture, 2)

prisutnost/odsutnost straha kod žrtve napada i kod drugih pojedinaca ili organizacija koje bi mogle biti pod njegovim utjecajem i 3) različita upotreba unaprijed postavljene oznake za prepoznavanje prirode radnje (Romagna, 2019).

Za početak, nije vrsta tehnike koja se koristi za operaciju ono što povlači granicu između cyberterorizma i haktivizma, već prije učinci povezani s njezinom upotrebom. Hampson (2012., str. 539; prema Romagna, 2019) naglašava kako bi „dopušteni oblici haktivizma trebali imati kao svoju primarnu svrhu nenasilnu komunikaciju koherentne poruke, dok je oblike haktivizma koji predstavljaju prijetnju fizičkim ozljedama ili nasiljem [. . .] bolje opisati kao cyber kriminal ili cyber terorizam". Ukoliko bi osoba koristila zlonamjerni softver za pokretanje prosvjeda, te ako bi zlonamjerni softver izravno ili neizravno fizički ozlijedio drugu osobu, tada bi se napustila oznaka haktivizma, a ovisno o konačnom cilju, primijenila bi se oznaka kibernetičkog kriminala ili terorizma. Unatoč tome, Holt (2012) tvrdi da s obzirom na kibernetički prostor fizička ozljeda ne bi bila nužna za identifikaciju terorističke akcije. Poremećaj koji može ozbiljno onemogućiti, spriječiti ili osakatiti financijske usluga, elektroenergetske mreže ili bilo koje druge kritične infrastrukture vjerojatno bi završio pod oznakom terorizma, osobito ako stvara paniku ili strah kod svojih meta.

Strah je suštinski terorizmu. Teroristi traže političku promjenu prisiljavajući društvo i javne institucije prijetnjama i stvarajući strah i/ili štetu nasilnim radnjama (Holt, 2012). Haktivisti, umjesto toga, odbijaju korištenje fizičkog nasilja i nemaju za cilj stvoriti strah kod svojih meta, a neki od njih čak tvrde da se bilo kakav oblik ometanja ne bi trebao tolerirati (Romagna, 2019).

Posljednja točka je spornija, jer spaja proces etiketiranja, samopercepcije i političke poglede. Vegh (2003; prema Romagna, 2019) kritizira činjenicu da je razlika između haktivizma i cyber terorizma postala nejasnija zbog interesa medija i vlada. Pokušali su gurnuti haktivizam u polje terorizma kako bi imali više moći i sposobnosti odgovoriti na bilo koju vrstu ilegalnih cyber akcija. Na pitanje percepcije uvelike utječe politička situacija u zemlji. U očima haktivista, te se operacije vide kao legitimni oblici prosvjeda, dok su u pogledu osuđivača, što je najčešće vlada, to nepravedni i neopravdani oblici kriminalne aktivnosti ili terorizam.

5. Anonymous

Anonymous hakeri slabo su organizirana internetska skupina političkih aktivista koji se bave haktivizmom. Priča o podrijetlu Anonymous-a počinje na forumu za online poruke 4chana, web stranica anonimne društvene zajednice osnovana 2003. godine. Čak i danas, postovi na 4chanu od korisnika koji ne navedu korisničko ime označeni su kao da su ih napisali *Anonimni* (Huddleston, 2022). Općenito, Anonymous se protivi vladama i korporacijama za koje smatra da sudjeluju u cenzuri ili promiču nejednakost. Budući da je grupa decentralizirana, nema stvarnu strukturu ili hijerarhiju, tako da često postoji mnogo internih rasprava o tome koje ideje ili ciljeve podržati.

Njihove su mete u prošlosti uključivale CIA-u, Scijentološku crkvu i Islamsku državu, a iako je kolektiv ostao uznemiren brojnim uhićenjima u SAD-u početkom 2010-ih, obnovio je aktivnosti nakon ubojstva Georgea Floyda. Jedan bivši član Anonymousa opisao je njihovo vodeće načelo kao "anti-ugnjetavanje"(Milmo, 2022).

U trenutku pisanja prve verzije ovog rada (ožujak, 2023. godine) Anonymous ima tri aktivne operacije: OpRussia, OpIran i OpSerbia. OpIran služi kao podrška hakerskom kolektivu za prosvjede protiv smrti Mahse Aminija. Ova 22-godišnja žena umrla je dok ju je držala policija za moral zbog navodnog kršenja strogih islamskih kodeksa odijevanja u Iranu noseći previše labavu maramu, što je natjeralo žene diljem zemlje da uklone ili čak spale svoje obavezne marame. U poruci objavljenoj na kanalima društvenih medija povezanih s Anonymousima nakon početka ovih prosvjeda, hakerska skupina je rekla da je Aminijina smrt bila "posljednja kap" i da je pokrenula OpIran protiv iranske države (Cuthbertson, 2022).

Anonymous optužuje srbijanskog predsjednika Aleksandra Vučića da se ponaša kao "Putinova marioneta" dok Srbija raspiruje sukob s Kosovom, činom za koji se Rusija nada da bi mogao odvratiti Zapad od Ukrajine. Sukladno s tim, Anonymous početkom 2023. godine vrši bezbroj napada na srpske državne web stranice i baze podataka u sklopu OpSerbia (Aitken, 2023).

OpRussia su napadi Anonymous-a na Rusiju i njene saveznike kao reakcija na invaziju na Ukrajinu. Ovi napadi su tema ovog rada, stoga ćemo o njima detaljnije u kasnijim dijelovima rada.

Suosnivač tvrtke za kibernetičku sigurnost Security Discovery, Jeremiah Fowler, rekao je za CNBC da pristaše Anonymous-a vjerojatno gledaju na grupu kao na neku vrstu "cyber Robin Hooda", koji cilja na moćne vlade i korporacije u ime popularnih ciljeva. Ali Anonymous definitivno ima kritičare. Mnogi vjeruju da je taktika opreza grupe ekstremna i potencijalno opasna. Godine 2012. Američka Nacionalna sigurnosna agencija (NSA) Anonymous je ocijenila prijetnjom nacionalnoj sigurnosti (Huddleston, 2022).

S obzirom na manjak strukture i hijerarhije unutar skupine također nema ni službenog pripadništva skupini ili jedinstvenog glasnogovornika skupine. Tako bilo koja individua može tvrditi da je član Anonymous skupine te da su njihovi postupci u ime Anonymous ideologije.

5.1. Kontekst napada

Ne možemo u potpunosti razumjeti detalje napada Anonymous-a na Rusiju bez da razmotrimo pozadinu svih događanja. Za početak treba spomenuti rusko-ukrajinski sukob, koji je započeo u ožujku 2014. (iako temeljne napetosti datiraju stotinama godina unatrag) (Geers, 2015). Građanski nemiri, potaknuti proruskim snagama i potpomognuti ruskom vojskom, eskalirali su u oružani sukob u regiji Donbas. Sudionici su bili ruska vojska, proruski militanti, paravojske i dobrovoljačke milicije.

Početkom veljače 2015. Francuska, Njemačka, Rusija i Ukrajina pokušale su pokrenuti pregovore o okončanju nasilja putem sporazuma iz Minska. Okvir sporazuma uključivao je odredbe za prekid vatre, povlačenje teškog naoružanja i punu kontrolu ukrajinske vlade u cijeloj zoni sukoba. Međutim, pokušaji da se postigne diplomatsko rješenje i zadovoljavajuće rješenje uglavnom su bili neuspješni (Center for Preventive Action, 2022).

Ruske snage izvršile su invaziju 24. veljače 2022. na većinom nepripremljenu Ukrajinu nakon što je ruski predsjednik Vladimir Putin odobrio "specijalnu vojnu operaciju" protiv zemlje. Putin je u svojoj izjavi ustvrdio da je cilj operacije demilitarizacija i denacifikacija Ukrajine te okončanje navodnog genocida nad Rusima na ukrajinskom teritoriju (Center for Preventive Action, 2022).

Ovaj sukob je specifičan zbog toga što se vodi u kibernetičkom prostoru kao i na bojištu. Cyber aktivnost protiv Ukrajine u početku je bila prigušena, unatoč raširenim predviđanjima da će ruski vojni napad na zemlju biti kombiniran s digitalnim šokom i strahopoštovanjem. Ukrajinske web stranice bile su pogođene DDoS[12] napadima prije ofenzive, uključujući ukrajinsko ministarstvo obrane i PrivatBank, najveću ukrajinsku komercijalnu banku, ali nije bilo napada u razmjerima slučaja NotPetya 2017. – kada je razorni napad malwarea koji se pripisuje Rusiji uništio računala u Ukrajini i širom svijeta (Milmo, 2022). U veljači 2022. web stranice ukrajinske vlade, uključujući ministarstva obrane i unutarnjih poslova, bankarske stranice i druge povezane organizacije bile su meta distribuiranih napada uskraćivanjem usluge usporedo s ruskom invazijom (Center for Preventive Action, 2022).

Taktike kibernetičkog ratovanja započele su prekidom ukrajinskih medijskih i telekomunikacijskih mreža od strane proruskih hakera, dovodeći u pitanje komunikacijske sposobnosti ukrajinske vlade i mogućnosti odgovora sličnim kibernetičkim napadima.

Aktivnosti cyber ratovanja proširene su na: cyber špijunažu i propagandne kampanje, DDoS napade na ukrajinske medije i vladine organizacije, narušavanja web stranica, ometanje komunikacije ukrajinskih političara, manipulaciju informacijama i video zapisima, kampanju korumpiranog glasačkog procesa u Ukrajini, curenje povjerljive e-pošte, telefonskih poziva i dokumenata, i poremećaja mreža i informacijskih sustava. Međutim, izostali su napadi na obrambene sustave, a predložene su različite teorije o tome zašto je to bio slučaj. To se promijenilo u prosincu 2015. kada je sofisticirani cyber napad isključio desetke trafostanica ostavljajući više od 230 000 stanovnika bez struje do 6 sati (Zetter, 2016).

[12] Distribuirani napad uskraćivanja usluge (DDoS) zlonamjeran je pokušaj prekida normalnog prometa ciljanog poslužitelja, usluge ili mreže preplavljivanjem cilja ili njegove okolne infrastrukture poplavom internetskog prometa. DDoS napadi postižu učinkovitost korištenjem više kompromitiranih računalnih sustava kao izvora prometa napada.
DDoS napad je poput neočekivane prometne gužve koja začepljuje autocestu, sprječavajući redoviti promet da stigne na svoje odredište. (https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/)

6. Cyber napadi Anonymousa na Rusiju

Nakon što je Rusija napala Ukrajinu 24. veljače 2022. godine, Twitter račun sa 7,9 milijuna sljedbenika pod nazivom *Anonymous* objavio je cyber rat protiv Rusije i njenog predsjednika Vladimira Putina (Huddleston, 2022). Od tada je grupa preuzela odgovornost za razne kibernetičke napade koji su onesposobili web stranice i procurili podatke iz ruskih vladinih agencija, kao i državnih novinskih kuća i korporacija.

6. 1. Metodologija

Za potrebe ovog istraživanja koristile su se dvije kvalitativne metode istraživanja, metoda analize sadržaja i studija slučaja. Analiza sadržaja istraživačka je tehnika kojom se želi izgraditi sistematska iskustvena evidencija o simboličkom komuniciranju, kao jednom od najvažnijih aspekata društvenog života (Halmi, 1996: 275). Schreier (2012: 20) definira analizu sadržaja kao sistematsku i fleksibilnu metodu analize kvalitativnih podataka koja smanjuje i sažima materijale. Analiza sadržaja stječe popularnost sredinom prošlog stoljeća i nazvana je „Konstantna usporedna metoda kvalitativne analize“. Od 1980-tih ona postaje neizostavan alat za mjerenje medijskih profila, a osim za utvrđivanje postojećega stanja, koristi se i za definiranje i predviđanje trendova. Analiza sadržaja se često koristi za analizu masovnih medija. U prošlosti je uglavnom bila fokusirana na pisani materijal, dok se u novije vrijeme primjenjuje na verbalne, slikovne i filmske materijale kao i na sve druge kvalitativne sadržaje (Halmi, 2003: 361). Za kvalitativnu analizu sadržaja važan je kontekst te je više usmjerena zaključivanju o samom kontekstu, autoru i primatelju, a samo djelomično se usmjeruje na same podatke (Schreier, 2012).

Uzorak na kojem se provelo ovo istraživanje su članci portala vijesti koji se odnose na cyber napada od strane Anonymous-a na Rusiju. Pregledom web-stranica došli smo do popisa 14 najpopularnijih portala vijesti na svijetu. Od tih 14, u prvom krugu smo izbacili portale *New York Times* i *USA Today* zbog nedostatka besplatnog pristupa. Pretraživanje je izvršeno na sljedećih 12 portala: *CNN, BBC, The Guardian, Daily Mail, The Washington Post, Indiatimes, Huffington Post, Fox News, NBC, ABC, CNBC, The Independent*. Ove portale pretražili smo pomoću ključnih riječi: *Anonymous, Russia, Cyber war, Cyber attack*. Ključne riječi su na engleskom zbog toga

što su i portali na istom jeziku. Koristim izraze *cyber rat* i *cyber napad* iz dva razloga. Prvi jest taj što mediji Anonymous od početka ovog sukoba predstavljaju u pozitivnom svijetlu te se nikada ne koriste pojmovi s negativnim konotacijama, kao terorizam, u opisu njihovih napada. Drugi razlog za korištenje ovih pojmova jest taj što i Anonymous u svojim objavama na društvenim mrežama govori o objavi cyber rata ili o novim izvršenim cyber napadima.

Vremensko ograničenje prikupljanja članaka jest od 24. veljače 2022. (dan objave rata) do 11. siječnja 2023. (dan prikupljanja članaka). Ključni kriterij koji su članci morali ispunjavati jest da oni uistinu govore o napadima pripadnika kolektiva Anonymous na Rusiju.

Kao istraživačka strategija, studija slučaja se koristi u mnogim situacijama kako bi doprinijela našem znanju o pojedinačnim, grupnim, organizacijskim, društvenim, političkim i srodnim fenomenima. Definicije studija slučaja koje se najčešće susreću samo su ponavljale vrste tema na koje su studije slučaja primijenjene. Na primjer, prema riječima jednog promatrača „Bit studije slučaja, središnje tendencije među svim vrstama studija slučaja, jest da pokušava rasvijetliti odluku ili skup odluka: zašto su donesene, kako su provedene i s kojim rezultatom“ (Schramm, 1971, prema Yin, 2003: 12). Kvalitativno istraživanje uvijek polazi od proučavanja pojedinačnog slučaja (ili skupine slučajeva istog fenomena) kako bi formuliralo hipoteze i opće teorije o proučavanom fenomenu. Osnovni postupak studije slučaja sastoji se u sagledavanju svih važnijih aspekata nekog fenomena ili situacije uzimajući kao jedinicu analize pojedinačnog subjekta, skupinu, zajednicu ili kulturu. Svaka od tih jedinica analize se smatra zasebnom cjelinom koja može ali i ne mora biti u relaciji s drugim cjelinama ili pojedincima (Halmi i Crnoja, 2003).

Lune i Berg (2017) kod upotrebe i značenja pristupa studije slučaja otkrivaju dva bitna elementa. Prvi jest da studije slučaja zahtijevaju više metoda i/ili izvora podataka pomoću kojih stvaramo potpuno i duboko ispitivanje slučaja. Koje ćemo točno metode koristiti i kako ćemo ih točno kombinirati ovisit će o samom slučaju, iako potreba za dubinom i kontekstom u jednom okruženju svakako daje prednost kvalitativnom istraživanju u odnosu na kvantitativno istraživanje. Drugi element glasi: da bi određeno istraživanje mogli nazvati studijom slučaja znači da postoji neka šira kategorija

događaja (ili okruženja, grupa, subjekata itd.) od kojih je ova studija jedan slučaj. Pitanje koje postavljamo jest: Čega je ovo slučaj?

6.1. Rezultati

Kao što smo ranije istaknuli, pretraživanje je izvršeno na 12 portala (*CNN, BBC, The Guardian, Daily Mail, The Washington Post, Indiatimes, Huffington Post, Fox News, NBC, ABC, CNBC, The Independent*) pomoću ključnih riječi: *Anonymous, Russia, Cyber war, Cyber attack*. Postavljeno vremensko ograničenje za članke je od 24. veljače 2022. (dan objave rata) do 11. siječnja 2023. (dan prikupljanja članaka). Prilikom pretraživanja, portali *CNN, The Washington Post, NBC* te *ABC* nisu pružili nijedan članak koji bi zadovoljavao uvijete našeg istraživanja. Na preostalih 8 portala vijesti pronašli smo ukupno 26 članaka koji zadovoljavaju kriterije za naše istraživanje. Tijekom detaljnijeg pregleda članaka odlučili smo izbaciti još 4 članka iz analize. Razlog za isključivanje ovih članaka jest što ne govore o specifičnim napadima Anonymous-a na Rusiju već dva od njih govore o objavi rata Anonymous-a Putinu dok druga dva članka govore o taktikama koje su korištene u ovim napadima.

Tako na kraju raspolažemo s ukupno 22 članka za analizu (*BBC* 1 članak, *The Guardian* 1 članak, *Daily Mail* 4 članka, *Indiatimes* 1 članak, *Huffington Post* 2 članka, *Fox News* 1 članak, *CNBC* 3 članka, *The Independent* 9 članaka). Iako je vremensko ograničenje bilo do 11. siječnja 2023. godine, posljednji članak jest napisan 28. srpnja 2022.

Jeremiah Fowler, (Pitrelli, 2022a) suosnivač tvrtke za kibernetičku sigurnost Security Discovery, koji prati hakerski kolektiv otkako je objavio "kibernetički rat" Rusiji zbog invazije na Ukrajinu, podijelio je napade Anonymous-a u šest kategorija te ih rangirao prema efikasnosti:

- Hakiranje u baze podataka
- Ciljanje tvrtki koje nastavljaju poslovati u Rusiji
- Blokiranje stranica
- Treniranje regruta
- Otimanje medija i stream platformi
- Direktno obraćanje rusima

Slučajeve zasebnih cyber napada koji su prikazani u člancima koje smo analizirali, podijelili smo prema toj klasifikaciji samo što smo mi poredali kategorije po njihovoj medijskoj popularnosti.

Prije nego što krenemo u detaljniju analizu smatramo potrebnim napomenuti kako su analizirani članci manjkavi s informacijama te često nedostaje konkretan datum i vrijeme izvršenog napada kao i neke ostale ključne informacije o istome. Iz ovog razloga je često nemoguće odrediti govore li neki članci o istim napadima ili svaki o različitim napadima. Zbog toga smo podijelili članke u kategorije te ćemo pretežito govoriti o skupini napada češće nego o jednom specifičnom napadu. No, o ovim nedostacima ćemo više u raspravi.

Najčešće se u analiziranim člancima spominju napadi koji se donose na otimanje medija i stream platformi. Od ukupno 22 članka u analizi, ovaj tip napada se spominje čak u njih 15. U ovu kategoriju uključujemo napade preuzimanja kontrole nad službenim ruskim televizijskim kanalima (Russia 24, Channel One, Moscow 24), nad stream platformama (Wink, Ivi), te nad portalima vijesti (Tass, Kommersant, Fontanka, Izvestia)[13]. Preuzimanja kontrole televizijskih kanala i stream platformi se najčešće izvodilo zajedno, te je uključivalo prikazivanje snimki iz Ukrajine. Ove snimke su sadržavale prikaze ukrajinskih gradova nakon bombandiranja, ljude na ulici okružene ruševinama te obraćanja ukrajinskih vojnika. U jednom slučaju takvog napada, video je sadržavao poruku na kraju, u kojoj stoji da su „obični Rusi protiv rata“ (Mishra, 2022) i pozivaju Ruse da se suprotstave napadu na Ukrajinu. U drugim slučajevima bi se prikazivali videi s ukrajinskim narodnim simbolima i narodnim pjesmama. U jednom slučaju su nazive programa na stranici rasporeda zamijenjeni s natpisima: „Krv tisuća Ukrajinaca i stotine njihove ubijene djece je na vašim rukama“ i „TV i vlasti lažu. Ne ratu.“ (James, 2022).

U kategoriju otimanja medija smo svrstali i otimanje portala vijesti. Tokom ovog tipa napada uobičajena početna stranica portala je zamijenjena nekom porukom

[13] TASS - novinska agencija u državnom vlasništvu

Kommersant - ruske nacionalne novine

Izvestija - dnevne novine, koje su osnovane u St. Petersburgu tijekom ruske revolucije i bile su jedno od glavnih medijskih izdanja u Sovjetskom Savezu

potpisanom Anonymous. Tako je u jednom od ovih napada početna stranica portala *Fontanka, Kommersant* i *Izvestia* zamijenjena porukom:

> „Poštovani građani. Pozivamo vas da zaustavite ovo ludilo, ne šaljite svoje sinove i muževe u sigurnu smrt. Putin nas tjera da lažemo i dovodi nas u opasnost. Bili smo izolirani od cijelog svijeta, prestali su kupovati naftu i plin. Za nekoliko godina živjet ćemo kao u Sjevernoj Koreji. Što je to za nas? Putina staviti u udžbenike? Ovo nije naš rat, zaustavimo ga!
>
> Ova poruka će biti izbrisana, a neki od nas će biti otpušteni ili čak u zatvoru. Ali ne možemo više.
>
> Ravnodušni novinari Rusije“ (Dennet, 2022).

Uz ovu poruku prikazan je i nadgrobni spomenik s brojem 5,300 što je navodno broj ruskih vojnika koje su ukrajinske snage ubile do dana ovog napada, odnosno do 28. veljače 2022. godine.

Druga kategorija napada po učestalosti pojavljivanja u analiziranim člancima, koja se spominje u 8 od 22 članka, jest blokiranje stranica. Ova vrsta napada se najčešće obavlja pomoću DDoS napada, odnosno, distribuirani napad uskraćivanja usluga. Najjednostavnije objašnjeno, DDoS napad se provodi poplavljujući web stranicu sa što više prometa i zahtjeva dok ne dođe do, takozvanog, rušenja stranice. Nakon što dođe do rušenja web stranice ona više nije u funkciji te je potrebno neko vrijeme kao bi se popravila nastala šteta.

Prema analiziranim člancima, Anonymous na svojim twitter računima tvrdi kako su brojne stranice bile žrtve ovog tipa napada, te stranice su: službena stranica Kremlina, stranica ruske Federalne sigurnosne službe (FSB), Analitički centar Vlade Ruske Federacije, Ministarstvo sporta Ruske Federacije, Ministarstvo vanjskih poslova, Ministarstvo obrane, Ministarstvo unutarnjih poslova, Služba sigurnosti, Kabinet ministara, Moscow.ru[14], Gazprom[15], Russia Today[16], Gazregion[17], Technotec[18], Tetraedr[19].

[14] Službena stranica grada Moskva

[15] Naftna kompanija, najveći eksploatator zemnog plina na svijetu

[16] Russia Today je globalna televizija osnovana od strane Ruske vlade. Iako je u pitanju medij, nije spomenut napad otimanja programa već samo DDoS napad na službenu stranicu ove televizije.

Napadi iz ove kategorije se u analiziranim člancima uglavnom samo spomenu no ne pružaju nam se ikakve informacije osim potvrde da određene web stranice nisu bile u funkciji neko vrijeme.

Treća najčešće spomenuta kategorija napada su napadi na baze podataka, ovaj tip napada se spominje u 7 od ukupno 22 analizirana članka. Osim dolje raspisanih napada, Anonymous je preuzeo odgovornost i za napade na baze podataka ruskog Ministarstva obrane i ruske Središnje banke.

Najpoznatiji slučaj u ovoj kategoriji jest napad na Roskomnadzor, rusku agenciju medijske cenzure. Neposredno prije invazije agencija je ograničila pristup Facebooku i Twitteru prije nego što ih je blokirao, a također je zaprijetila da će prekinuti pristup Wikipediji, zbog članka o invaziji. Agencija je 24. veljače naredila svim medijskim kućama da koriste samo službene, državno odobrene izvore informacija ili će se suočiti sa oštrom kaznom za širenje „lažnih vijesti“[20]. Riječi *rat, invazija* i *napad* bile su zabranjene za upotrebu kada se opisuju ruske vojne akcije u Ukrajini. Kao odgovor na to Anonymous-i su

> „hakirali rusku agenciju za cenzuru medija i objavili 340.000 datoteka iz savezne agencije Roskomnadzor, ukravši povjerljive dokumente koje su potom proslijedili organizaciji za transparentnost Distributed Denial of Secrets (DDoSecrets), koja ih je objavila na internetu.
>
> Skup od 820 gigabajta e-pošte i privitaka, od kojih su neki datirani čak 5. ožujka, pokazuju kako Kremlj cenzurira sve što se odnosi na njihovu brutalnu invaziju na Ukrajinu, koju Moskva umjesto toga naziva 'specijalnom vojnom operacijom“ (May i Newman, 2022).

Još jedan ovaj tip napada za koji smo dobili nešto više informacija jest i slučaj hakiranja u bazu podataka o pomorskom praćenju. Anonymous su preimenovali jahtu

[17] Tvrtka specijalizirana za izgradnju magistralnih plinovoda, kompresorskih stanica, objekata za distribuciju plina

[18] Proizvodnja i isporuka opreme za naftna polja

[19] Bjeloruski proizvođač oružja

[20] U vezi s novim ruskim zakonom o lažnim vijestima. Bilo koje informacije o invaziji Ukrajine u medijima koje ruska vlada smatra neistinitim ili neprihvaćenim se smatraju lažnim vijestima te prema ovom zakonu osobu čeka zatvorska kazna do čak 15 godina.

ruskog predsjednika Vladamira Putina u „FCKPTN“ vandalizirajući podatke praćenja plovidbe. Njemački ogranak skupine Anonymous preimenovao je Putinovo luksuzno plovilo iz „Graceful“ i promijenio podatke o njegovoj lokaciji kako bi izgledalo da se srušio na Zmijski otok u Ukrajini. Hakeri su zatim preimenovali njegovo odredište u *anonymous* i *anonleaks*, prije nego što su se konačno odlučili za *pakao* (Smith, 2022a).

Četvrta i peta kategorija se pojavljuju svaka u 2 analizirana članka, a kategorije su ciljanje tvrtki koje nastavljaju poslovati u Rusiji i direktno obraćanje Rusima. Ciljanje tvrtki koje nastavljaju poslovati u Rusiji je pretežito usmjereno na tvrtke Zapadnog svijeta. Jedan od Twitter računa Anonymous-a (@YourAnonTV) 21. ožujka objavljuje poruku: "Pozivamo sve tvrtke koje nastavljaju poslovati u Rusiji plaćajući poreze proračunu kriminalnog režima Kremlja: Povucite se iz Rusije!" (Pitrelli, 2022b). Ova objava je sadržavala i sliku od 40 loga tvrtki, šaljući jasnu poruku da imaju 48 sati da prekinu suradnju s Rusijom. Nekoliko tih tvrtki je već ranije prekinulo poslovanje u svim ruskim podružnicama, neke (Dunkin i Bridgestone Tires) su odgovorile direktno na ovu objavu te objavile kako pokreću proces obustave poslovanja. Isti Twitter račun od Anonymous-a 24. ožujka objavljuje još jedan popis tvrtki s istom porukom. Anonymous-i su preuzeli zasluge za zatvaranje ruske web stranice Decathlon-a, zajedno sa stranicama za Leroy Merlin i francusku tvrtku supermarketa Auchan. Također su tvrdili kako su hakirali i Švicarsku poznatu tvrtku Nestle, no nikada nije potvrđeno da je uopće došlo do hakiranja ove tvrtke te Nestle negira da je došlo do ikakvog oblika cyber napada, iako su ubrzo nakon ove tvrdnje i oni prekinuli poslovanje u Rusiji.

Kada je riječ o direktnom obraćanju Rusima, spominje se samo jedan određeni način tog komuniciranja, a to je pomoću hakiranja printera. U jednoj od svojih Twitter objava pišu: “Tiskali smo antipropagande i upute za instalaciju Tor[21]-a tiskarima diljem [Rusije] 2 sata i do sada smo ispisali više od 100.000 primjeraka. 15 ljudi radi na ovoj operaciji" (Sankaran, 2022).

U nijednom od 22 analizirana članka se ne spominje treniranje regruta, te je ovo posljednja od šest kategorija napada kojima se koristi grupa Anonymous u napadima na Rusiju. Valja napomenuti kako ima i napada od strane Anonymousa koje nismo mogli

[21] Tor Browser izolira svaku web stranicu koju posjetite tako da vas treća strana za praćenje i oglase ne može pratiti. Svi kolačići automatski se brišu kada završite s pregledavanjem. Također omogućava Anonymousu da komunicira s ruskim narodom.

svrstati u ijednu od gore navedenih kategorija. Tako treba spomenuti slučaj gdje Anonymous-i preuzimaju odgovornost za hakiranje ruskih nadzornih kamera i postavljanje poruka poput "Putin ubija djecu" na scene s kamera. Prijenosi kamera emitirani su uživo na web stranici Behind Enemy Lines (Papenfuss, 2022). Drugi slučaj koji nismo mogli svrstati u jednu od ovih kategorija jest hakiranje ruskog vojnog radija radi postavljanja slike poznatog *troll face* meme-a (Smith, 2022b).

Adam Smith u istom tom članku, *Anonymous claims hack on Russia's Central Bank and will 'release secret agreements in 48 hours'*, iznosi i podatak kako su Anonymous-i preuzeli odgovornost za čak 2,500 cyber napada koji uključuju napade na rusku i bjelorusku vladu, državne televizije, banke, bolnice, aerodrome i kompanije. Ovaj članak je objavljen 24. ožujka 2022., točno mjesec dana od početka ruske invazije i Anonymous-ove objave rata Putinu.

7. Rasprava

Ranije smo već spomenuli kako je etiketiranje nečega terorizmom vrlo sklisko područje jer je određivanje je li nešto terorizam ili ne uvelike uvjetovano političkim gledištem. U cijeloj toj priči ulogu imaju i vrijednosti osobe koja etiketira nešto kao takvim, te je nerijetko teško ostati objektivan i izbjeći utjecaj osobnih uvjerenja na odluku treba li neki slučaj dobiti tu etiketu ili ne. Netko tko je jednoj osobi terorist, drugoj može biti heroj i vice versa. Upravo iz tog razloga jest potrebno što jasnije definirati ovakve pojmove ili, u najmanju ruku, odrediti jasne kriterije koje neki slučaj mora zadovoljavati kako bi se mogao etiketirati pod tim pojmom.

Preostaje nam pitanje, jesi li ovi napadi Anonymous-a na Rusiju cyber terorizam? Odgovor na ovo pitanje je dakako kompliciranije od jednostavnog da ili ne, kao i svako drugo pitanje u sociologiji, no ne preostaje nam ništa drugo nego pokušati dati što objektivniji odgovor na temelju informacija koje imamo.

Prvi korak do dobivanja odgovora na naše pitanje jest odrediti što cyber terorizam zapravo jest. Pogled na definiranje ovog pojma može uvelike utjecati na krajnji zaključak. Dakako najstroži pogled jest onaj koji cyber terorizam vidi samo kao podvrstu terorizma, što znači kako je aspekt kibernetičkog prostora samo dodan na već postojeće kriterije terorizma. Ranije smo već naveli ove kriterije koje nudi Wayman

Mullins (1997:15; prema Bilandžić, 2014: 83), a oni su: 1) nasilje nije krajnji cilj, već sredstvo za njegovo ostvarivanje; 2) prijetnja je prvenstveni cilj nasilja u terorizmu, nasilje se koristi samo do one granice kada je prijetnja podupreta; 3) psihološki utjecaj, odnosno strah je važan za ostvarivanje političke promjene. Strah u široj populaciji ima veći učinak na političke promjene nego nasilje upućeno prema vladi; 4) ciljane žrtve nisu one koje stradaju direktno od nasilja već one koje mu svjedoče; 5) konačni cilj terorizma jest politička promjena, bez obzira na postojanje drugih motiva i ciljeva, politička promjena je uvijek srž terorizma. Dorothy Denning (2001) ima slično gledište, jasno ističući kako se nijedan napad ne može smatrati cyber terorizmom bez određenog stupnja razaranja, straha i kaosa kojim smo upoznati kroz ostale vrste terorizma.

Gledajući ove napade kroz leću ovakvog strogog shvaćanje cyber terorizma možemo sa sigurnošću reći kako se u ovom slučaju ne radi o cyber terorizmu. Prvenstveno nam nedostaje stavka terora i nasilja iako imamo element prisile. Element izazivanja strah bismo mogli reći kako je bio prisutan u napadima zapadnih tvrtki koje su u tom trenutku i dalje poslovale u Rusiji. S obzirom da su tvrtke uključene u tim napadima dobile javno upozorenje te rok od 48 sati da postupe po njihovoj želi ili će njihovi podaci biti kompromitirani. Znamo i kako ovi napadi zadovoljavaju i kriterij političke motiviranosti.

No pogledamo li taksonomiju Plotnek i Slay-a (2019), napadi u analiziranim člancima ispunjavaju više kriterija. Radi se o 6 kriterija: 1) akter: s predumišljajem i nedržavni, 2) motiv: ideološki i socijalni, 3) namjera: izazvati strah ili prisiliti, 4) sredstva: napad ili prijetnja napadom koji potječu iz kibernetičkog prostora, 5) učinak: posljedica koja se događa izvan kibernetičkog prostora (npr. psihološki, društveni, politički, fizički, ekonomski, ekološki) te 6) meta: civili, državne ili nedržavne.

Kao prvo, znamo kako se radi o nedržavnom akteru, prisutnom u cijelom svijetu, te znamo kako se ovakvi masovni napadi moraju unaprijed osmisliti i organizirati. Pogotovo kada je riječ o masovnim DDoS napadima koji su najdraže oružje Anonymous-a. Zatim, znamo i kako su svi napadi za koje Anonymous preuzima odgovornost ideološki motivirani. Možemo sa sigurnošću reći i kako se svi njihovi napadi odvijaju u kibernetičkom prostoru. Također znamo i kako je u slučaju ovih napada, sa iznimkom napada na Zapadne tvrtke, meta svih napada bila državna.

O samome učinku izvan kibernetičkog prostora možemo reći da postoji samim time što imamo saznanje o ovim napadima. Upoznati smo sa ruskom praksom cenzure medija i zataškavanja činjenica koje ne idu u korist ruskoj vlasti. S tim saznanjem, za očekivati je kako bi ovakve napade pokušali zadržati tajnima no usprkos toga vijesti su se brzo pročule po cijelome svijetu. Učinke možemo vidjeti i po tome što su pojedini ruski građani snimali neke od gore navedenih napada (preuzimanje kontrole nad televizijskim kanalima) te slali snimke pojedincima van Rusije kako bi ih oni objavili na društvenim mrežama. Tim postupkom se proširila vijest o napadima dajući im još veću pažnju. Iako nemamo točne informacije o učinku prekida poslovanja zapadnih tvrtki u Rusiji, znamo da takav masovni prekid ekonomske transakcije u nekoj zemlji ostavlja posljedice na njeno gospodarstvo, pa i na državni proračun.

Preostao nam je još kriterij namjere, koja bi trebala uključivati strah ili neki oblik prisile. Prilikom upozorenja koja su uputili zapadnim tvrtkama koje su i dalje poslovale u Rusiji bilo je elementa prisile. Prestanite poslovati s Rusijom ili ćete postati naša sljedeća meta. U slučaju preuzimanje podataka iz baze podataka Središnje banke, Anonymous je objavio kako posjeduju te podatke te da će ih objaviti u roku 48 sati od te objave. Ovakvo djelovanje možemo shvatiti kao pokušaj izazivanja straha, znamo nešto za što ne želite da javnost zna, a mi ćemo im to reći. Možemo reći kako je cijeli taj cyber rat pokušaj prisile ruske vlade da zaustavi invaziju, no je li to dovoljno da bismo rekli kako se ovdje radi o cyber terorizmu? Strogo gledajući po taksonomiji Plotnek i Slay-a neke napada, same po sebi, bismo mogli smatrati cyber terorizmom, primjerice napadi na zapadne tvrtke te hakiranje Središnje banke. Ostali napadi sami po sebi ne zadovoljavaju kriterij namjere, iako možemo reći da u cijelosti, OpRussia služi kao pokušaj prisile ruske vlade da zaustavi invaziju. Zbog toga dolazimo do zaključka kako u ovim napadima imamo element prisile kao kriterij namjere.

Prije nego što odgovorimo na naše pitanje, želimo slučajeve ovih napada provući kroz još jednu grupu elemenata. S obzirom kako se Anonymous još od svog osnutka često etiketira pojmom haktivističke grupe, smatramo potrebnim ove slučajeve provući kroz tri elementa, koji razlikuju haktivizam i cyber terorizam: 1) postojanje/nedostatak fizičke štete ili barem ozbiljnog poremećaja vitalne infrastrukture, 2) prisutnost/odsutnost straha kod žrtve napada i kod drugih pojedinaca ili organizacija koje bi mogle biti pod njegovim utjecajem i 3) različita upotreba unaprijed postavljene oznake za prepoznavanje prirode radnje (Romagna, 2019).

Već smo utvrdili kako nijedan od ovih napada nije uzrokovao fizičku štetu, no preuzimanje kontrole nad medijima koji su u Rusiji uvelike cenzurirani i kontrolirani se smatra poremećajem vitalne infrastrukture. Također, tjeranjem velikih tvrtki da prekinu poslovanje u određenoj državi donosi poremećaj u gospodarstvu te države. Jedini slučaj napada za koji zasigurno možemo reći da je prisutan element straha su napadi na zapadne tvrtke. Posljednji element je najteži za odrediti iz razloga koje smo naveli na samom početku rasprave. Radi se o procesu etiketiranja, o osobnoj percepciji i političkoj situaciji. Iz perspektive ruske vlade i njihovih saveznika Anonymous-i su bez sumnje cyber teroristi ili u najmanju ruku kriminalci koje treba zaustaviti. No iz perspektive Ukrajine i njihovih saveznika, oni su heroji, borci za pravdu, (h)aktivisti.

Nakon godina slabe haktivističke aktivnosti, 2022. godine je ponovno zaživio u velikim razmjerima. Ruska sveobuhvatna invazija na Ukrajinu iznjedrila je mnoštvo haktivističkih skupina na obje strane sukoba, dok u Iranu i Izraelu takozvane haktivističke skupine pokreću sve destruktivnije napade. Ovaj novi val haktivizma, koji se razlikuje od skupine do zemlje, dolazi s novim taktikama i pristupima i, sve više, briše granice između haktivizma i napada koje sponzorira vlada.

S jedne strane ovog sukoba, Anonymous i ukrajinska IT vojska, odnosno dobrovoljna skupina hakera iz cijelog svijeta, kontinuirano su pokretali brojne napade protiv ruskih ciljeva. Druge skupine povezane s haktivistima pokrenule su goleme operacije hakiranja i curenja podataka protiv ruskih entiteta, što je rezultiralo objavljivanjem stotina gigabajta podataka iz Rusije na internetu. S druge strane sukoba četiri su glavne proruske haktivističke skupine: Killnet, NoName 057, From Russia With Love i Anonymous Russia. Killnet je vjerojatno najaktivnija od ovih grupa. Njihove su mete, poput Europskog parlamenta, uglavnom bile zemlje koje se protive Rusiji. Grupa, koja uglavnom koristi DDoS napade, prijateljski je naklonjena medijima i obraća se govornicima ruskog jezika.

Prije samog zaključka istraživanja želimo raspraviti još nekoliko zapažanja tokom istraživanja. Jedno od najvećih iznenađenja prilikom ovog istraživanja je manjak interesa medija za ovaj slučaj. Pri tome ne govorim samo o malome broju članaka o samim napadima već i o brzini kojom se interes izgubio. Iako je posljednji članak iz analize napisan krajem srpnja 2022. godine, svega tri članka je napisano i objavljeno nakon ožujka iste godine. Prema tome, medijska zastupljenost napada Anonymous-a na

Rusiju je pretežito prisutna samo u prvih mjesec dana napada. Kada bismo gledali samo po medijima rekli bismo kako je ovo gotova priča, da su Anonymous-i odustali od svoje misije i obustavili napade na rusku vladu. No kada pogledamo najpoznatije twitter račune koji se predstavljaju kao Anonymous (*@YourAnonTV, @AnonOpsSE, @YourAnonOne, @YourAnonNews*) ti napadi se i dalje vrše više od godinu dana nakon početka, samo što medijima više nije zanimljivo baviti se ovom pričom.

Prilikom pretraživanja portala i pregledavanja članaka u potrazi za člancima koji se bave napadima Anonymous-a na Rusiju primijetila smo nekoliko zanimljivosti. Pri pretraživanju pod ključnom riječju Anonymous, većina dobivenih članaka su bili usmjereni na cyber napade na Donalda Trump, bivšeg američkog predsjednika, još 2020. godine. Zanimljivo je kako je medijski najzastupljeniji baš taj slučaj, umjesto recimo njihovih aktualnih operacija kao OpRussia ili OpIran, ili recimo slučaj Crkve Scijentologije, što je jedan od najpoznatijih slučaja Anonymous-a te slučaj kojih ih je učinio poznatima u široj populaciji.

Također je potrebno istaknuti kako su se, zbog specifične strukture kolektiva, našli zasebni ogranci Anonymous-a na suprotnim stranama. Dok je većinsko djelovanje Anonymous kolektiva bilo u korist Ukrajine, jedan ogranak se odvojio te djelovao u korist Ruske vlade. Smatramo kako je ovakva podjela moguća samo zbog manjka strukture i hijerarhije unutar kolektiva, jer takav slobodan pristup organizaciji je upravo ono što omogućava svakome da djeluje u ime kolektiva.

Primijetila sam i kako niti jedan od pretraživanih portala ne koristi pojam Cyber terorizam u slučaju ovih napada. Uvijek se koriste pojmovi cyber napad ili cyber rat. To može biti iz razloga što Anonymous, u svojim twitter objavama, ove napade sam predstavlja kao napade u sklopu cyber rata. No treba uzeti u obzir i gdje se nalaze središnje redakcije ovih portala vijesti, kao i službeno stajalište tih država o Ukrajinsko-Ruskom ratu. Sa izuzetkom Indiatimes, radi se o portalima sa središtima u Velikoj Britaniji ili Sjedinjenim Američkim Državama. Te dvije države su javno iskazale svoju podršku Ukrajini te redovito šalju nekakav oblik pomoći. Time se ponovno vraćamo na proces etiketiranja i političkog utjecaja kod definiranja nečega terorizmom. Stoga smatramo kako je i politička pozadina tih država, pa posljedično i portala, imala utjecaj na izbor riječi koje su se koristile za opis ovih napada. To je dakako zanimljiva misao koja bi se mogla istražiti u nekoj drugoj analizi i stvoriti još jedno istraživanje.

8. Zaključak

Napadi Anonymous-a na Rusiju su zasigurno njihov najveći i najorganiziraniji pothvat do sada te su njime dokazali kako nisu skupina kojoj se itko želi naći na putu. Ovi napadi su zasigurno otvorili vrata za nove rasprave i nova pitanja cyber sigurnosti diljem svijeta, dokazavši da čak ni Rusija, koja je dosada uvijek bila vršitelj cyber napada, nije nedodirljiva i zaštićena koliko se smatralo.

Unutar pokrenute rasprave o cyber sigurnosti ponovno se pokrenula i rasprava o cyber terorizmu, njegovom postojanju i definiranju. Cyber terorizam bismo najbolje mogli definirati kao politički motiviran kibernetički napad koji ima za cilj nanijeti štetu prijetnjom ili bitnim poremećajem vitalne infrastrukture, kao i bilo kojim drugim tipom napada na računala ili informacije pohranjene na njima u svrhu prisile ili izazivanja straha bilo kojoj osobi, grupi, organizaciji, tvrtki ili državi.

S time je došlo i vrijeme da napokon odgovorimo na naše pitanje: jesi li ovi napadi Anonymous-a na Rusiju cyber terorizam? Na temelju informacija koje imamo možemo zaključiti kako su napadi unutar OpRussia politički motivirani, odnosno motivirani ratnim sukobom Rusije i Ukrajine. Kao odgovor na Rusku invaziju, kolektiv Anonymous je ilegalno preuzimao informacije iz ruskih bazi podataka, remetio rad brojnih medija, preuzimao kontrolu pojedinih uređaja spojenih na internetsku mrežu te prijetio remećenjem poslovanja određenim tvrtkama. Sve to sa svrhom prisile Ruske vlade kako bi obustavile svoje ratne pohode te time prekinula ratni sukob u Ukrajini. Sagledavši sve prikupljene informacije o OpRussia možemo zaključiti kako se ovdje radi o cyber terorizmu. Iako bi neki vjerojatno tvrdili kako je riječ o haktivizmu, ranije smo već istaknuli kako ostavljanje negativnog učinka na metu napada čini bitnu distinkciju između haktivizma i cyber terorizma.

Dakako treba istaknuti kako je ovo istraživanje imalo i svojih nedostataka. Za početak, članci koje smo analizirali ne sadrže puno informacija o samim napadima, kao što smo ranije i istaknuli. Većina članaka pretežito samo nabraja sve stranice ili baze podataka na koje se izvršio napad.

Još jedan od nedostataka jest i činjenica kako su analizirani članci došli od portala iz dvije velike, razvijene, zapadne zemlje i jednog Indijskog portala koji je poprilično vesterniziran. Portali iz drugih krajeva svijeta bi možda prikazivali ove

napade u drugačijem svijetlu, što bi potencijalno moglo utjecati na rezultate ovog istraživanja.

Za kraj ne treba ni odbaciti mogućnost ljudske pogreške. Iako smatramo kako sam donijeli zaključak isključivo na temelju informacija koje su nam pružene, ne možemo odbaciti mogućnost da nismo uspjeli ostati objektivni tokom analize te da je rezultat uvjetovan našim osobnim stajalištima o cijeloj situaciji. Na kraju krajeva, nekoliko puta tokom rada ističem upravu tu opasnost.

9. Literatura

Knjige

Anderson, S., i Sloan, S. (2009). Historical dictionary of terrorism (3rd ed.). Lanham, Maryland: Scarecrow Press

Barlow, J.P. (1996). A Declaration of the Independence of Cyberspace. Davos: Electronic Frontier Foundation

Bell, D., Loader, B.D., Pleace, N., & Schuler, D. (2004). Cyberculture: The Key Concepts (1st ed.). Routledge. https://doi.org/10.4324/9780203647059

Bell, D. (2006). Cyberculture Theorists: Manuel Castells and Donna Haraway (1st ed.). Routledge. https://doi.org/10.4324/9780203357019

Bilandžić, M. (2014). Sjeme zla: Elementi sociologije terorizma. Zagreb: Plejada

Bilandžić, M. (2019). ' Nacionalna sigurnost : prognoziranje ugroza', Despot Infinitus: Zagreb

Caravelli, J. i Jones, N. (2019). 'Cyber Security: Threats and Responses for Government and Business', Praeger Security International: Santa Barbara

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

Halmi, A. (2003). 'Strategije kvalitativnih istraživanja u primjenjenim društvenim znanostima', Naklada Slap: Zagreb

Halmi, A. (1996). ' Kvalitativna metodologija u društvenim znanostima', A. G. Matoš: Zagreb

Kushner, H. (2003). Encyclopedia of terrorism, Sage Publications

Law, D. (2015). The Routledge History of Terrorism (1st ed.). Taylor and Francis Group. Preuzeto s: https://books.google.hr/books?id=3ZCsBwAAQBAJ&printsec=frontcover&hl=hr&source=gbs_book_other_versions#v=onepage&q&f=false

Lune, H. i Berg, B.L. (2017). Qualitative Research Methods for the Social Sciences. Pearson Education Limited: Harlow, Preuzeto: http://law.gtu.ge/wp-

content/uploads/2017/02/Berg-B.-Lune-H.-2012.-Qualitative-Research-Methods-for-the-Social-Sciences.pdf

Rapport, M. (2015). The Routledge History of Terrorism (1st ed.). Taylor and Francis Group. Preuzeto s: https://books.google.hr/books?id=3ZCsBwAAQBAJ&printsec=frontcover&hl=hr&source=gbs_book_other_versions#v=onepage&q&f=false

Schreier, M. (2012). ' Qualitative Content Analysis in Practice', SAGE Publications: Bremen

Webster, F. (2006). Theories of the Information Society (1st ed.). Routledge. https://doi.org/10.4324/9780203962824

Stručni radovi

Bihari, S. (2019). Cyber Security as an Academic Discipline: Challenges and Opportunities, International Journal of Research and Analytical Reviews. March 2019, 6 (1).

Burden, K., Palmer, C. (2003). 'Internet crime: Cyber Crime — A new breed of criminal?', Computer Law & Security Review 19 (3), Preuzeto s: https://booksc.org/book/4619355/d45b6a (Datum pristupa: 27.06.2021.)

Cains, M.G. i Flora, L. i Taber, D. i King, Z. i Henshel, D. (2021). Defining Cyber Security and Cyber Security Risk within a Multidisciplinary Context using Expert Elicitation. ResearchGate DOI: 10.1111/risa.13687

Denning, D.E. (2001). "Activism, Hacktivism, and Cyberterrorism: the Internet As a Tool for Influencing Foreign Policy". In Arquilla, J. & Ronfeldt, D. (Eds.), Networks and netwars. The future of terror, crime and militancy, Chapter eight, 239-288. Santa Monica: RAND Corporation.

Denning, D. (2015). The Rise of Hacktivism. Georgetown Journal of International Affairs, 8 September 2015.

Geers, K. (2015). Cyber War in Perspective: Russian Aggression Against Ukraine. NATO Cooperative Cyber Defence Centre for Excellence. Publications: Tallinn.

Retrieved from https://ccdcoe.org/multimedia/cyber-war-perspective-russian-aggression-against-ukraine.html

Haberfeld, M.R., von Hassell, A. (2009). A New Understanding of Terrorism: Case Studies, Trajectories and Lessons Learned. Springer

Halmi, A. i Crnoja, J. (2003). QUALITATIVE RESEARCH IN SOCIAL SCIENCES AND HUMAN ECOLOGY. Socijalna ekologija, 12 (3-4), 195-210. Preuzeto s https://hrcak.srce.hr/47897

Holt, T. J. (2012). Exploring the Intersections of Technology, Crime, and Terror. Terrorism and Political Violence, 24(2), 337-354. doi:10.1080/09546553.2011.648350

Jarvis, L.; Macdonald, S. (2015). What Is Cyberterrorism? Findings From a Survey of Researchers, Terrorism and Political Violence, 27:4, 657-678, DOI: 10.1080/09546553.2013.847827

Levchenko, O., Dyak, T., Hrytsiuk, Y. (2021). The elite of the information society: challenges of modern world. EUROPEAN HUMANITIES STUDIES: State and Society. DOI: 10.38014/ehs-ss.2021.2.06

Masian, A. (2022). Information Society and Global Modern Problems. Fìlosofsʹkì ta metodologìčnì problemi prava. doi: https://doi.org/10.33270/01222302.44

Plotnek, J.J. i Slay, J. (2020). Cyber Terrorism: A Homogenized Taxonomy and Definition. Elsevier

Rein, R. i Van Niekerk, J. (2014). From Information Security to Cyber Security Cultures. Research gate https://www.researchgate.net/publication/281107085_From_Information_Security_to_Cyber_Security_Cultures_Organizations_to_Societies

Romagna, M. (2019). Hacktivism: Conceptualization, Techniques, and Historical View. Springer https://doi.org/10.1007/978-3-319-90307-1_34-1

Talih¨arm, A.-M. (2010). Cyberterrorism: in theory or in practice? Defence Against Terrorism Review, 3(2):59–74.

Vuković, H. (2012). 'Kibernetska sigurnost i sustav borbe protiv kibernetskih prijetnji u Republici Hrvatskoj', National security and the future, 13(3), str. 12-31. Preuzeto s: https://hrcak.srce.hr/100728

Zetter, K. (2016, March 3). Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid. WIRED. Retrieved from https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid

Web stranice

Center for Preventive Action. (8. studeni 2022). Conflict in Ukraine. *Global Conflict Tracker*. Preuzeto 16. veljače 2023. s https://www.cfr.org/global-conflict-tracker/conflict/conflict-ukraine

Elektronski članci vijesti

Aitken, P. (5. siječnja 2023). Anonymous claims Serbia is 'Putin's puppet,' Russia looks to expand war in Europe and 'distract the West'. *FoxNews*. Preuzeto: 28. ožujka 2023., s https://www.foxnews.com/world/anonymous-claims-serbia-putins-puppet-russia-expand-war-europe-distract-west

Cuthbertson, A. (21. rujna 2022). 'Anonymous' hackers knock Iran state websites offline amid nationwide protests. *Independent*. Preuzeto: 28. ožujka 2023., s https://www.independent.co.uk/independentpremium/world/anonymous-iran-hack-protests-cyber-attack-amini-b2173181.html

Dennett, K. (28. veljače 2022). Anonymous collective hack THREE state news agencies urging Russians to 'stop this madness' after Moscow painted Ukrainian troops as Nazis and banned its media from calling attack an 'assault, invasion or war'. Dailymail. Preuzeto: 20. prosinca 2022., s https://www.dailymail.co.uk/news/article-10560131/Anonymous-collective-THREE-Russian-news-agency-websites.html

Huddleston, T. (25. ožujka 2022). What is Anonymous? How the infamous 'hacktivist' group went from 4chan trolling to launching cyberattacks on Russia. CNBC. Preuzeto: , s https://www.cnbc.com/2022/03/25/what-is-anonymous-the-group-went-from-4chan-to-cyberattacks-on-russia.html?&qsearchterm=anonymous%20russian

Milmo, D. (27. veljače 2022). Anonymous: the hacker collective that has declared cyberwar on Russia. The Guardian. Preuzeto: 20. prosinca 2022., s

https://www.theguardian.com/world/2022/feb/27/anonymous-the-hacker-collective-that-has-declared-cyberwar-on-russia

Mishra, S. (7. ožujka 2022). Anonymous hacks Russian state TV with Ukraine footage. Independent. Preuzeto: 11. siječnja 2023., s https://www.independent.co.uk/news/world/europe/anonymous-wink-ivi-russia-24-channel-1-moscow-24-b2029915.html

Newman, J. i May, L. (15. ožujka 2022). Anonymous claims it has successfully carried out new cyberattack on Russian government websites including the FSB. Dailymail. Preuzeto: 20. prosinca 2022., s https://www.dailymail.co.uk/news/article-10615799/Anonymous-claims-successfully-carried-new-cyberattack-Russian-government-websites.html

Papenfuss, M. (18. ožujak 2022). Hackers Help Channel Millions Of Anti-War Texts To Russian People. Huffington post. Preuzeto: 20. prosinca 2022., s https://www.huffpost.com/entry/squad303-anti-war-texts-to-russians_n_6233e78fe4b0f1e82c479d94

Pitrelli, M. (28. srpanj 2022a). Hacktivist group Anonymous is using six top techniques to 'embarrass' Russia. CNBC. Preuzeto: 20. prosinca 2022., s https://www.cnbc.com/2022/07/28/how-is-anonymous-attacking-russia-the-top-six-ways-ranked-.html?&qsearchterm=anonymous%20russian

Pitrelli, M (31. ožujka 2022b). Anonymous' next cyber target: Western companies still doing business in Russia. CNBC. Preuzeto: 20. prosinca 2022., s https://www.cnbc.com/2022/04/01/which-companies-are-being-targeted-by-anonymous-see-their-responses.html?&qsearchterm=anonymous%20russian

Sankaran, V. (22. ožujka 2022). Anonymous says it has hacked printers 'all across Russia' to spread anti-propaganda messages. Independent. Preuzeto: 11. siječnja 2023., s https://www.independent.co.uk/tech/anonymous-russia-printers-hacked-ukraine-invasion-b2041031.html

Smith, A. (28. veljače 2022a). Anonymous trolls Putin by renaming yacht 'FCKPTN' and sending it to 'Hell' by hacking maritime dana. Independent. Preuzeto: 20. prosinca 2022., s https://www.independent.co.uk/tech/anonymous-vladimir-putin-yacht-fckptn-b2024780.html

Smith, A. (24. ožujka 2022b). Anonymous claims hack on Russia's Central Bank and will 'release secret agreements in 48 hours'. Independent. Preuzeto: 11. siječnja 2023., s https://www.independent.co.uk/tech/anonymous-hack-russia-central-bank-b2043212.html

Sažetak

U ovom radu analiziramo jesu li napadi Anonymous-a na Rusiju cyber terorizam. Analizom sadržaja članaka sa svjetskih najpopularnijih portala vijesti utvrdit ćemo odgovor na to pitanje. Kako bismo bolje razumjeli koncept cyber terorizma dotaknuti ćemo se i pojmova informacijskog društva, kibernetičkog prostora, kibernetičke sigurnost i terorizma. Također se moramo pozabaviti i kontekstom samih napada te pozadinskom pričom Anonymous-a.

Ključne riječi: cyber terorizam, Anonymous, kibernetička sigurnost, haktivizam, OpRussia

Abstract

In this paper, we analyze whether Anonymous' attacks on Russia are cyber terrorism. By analyzing the content of articles from the world's most popular news portals, we will determine the answer to that question. In order to better understand the concept of cyber terrorism, we will also touch on the concepts of information society, cyber space, cyber security and terrorism. We also need to address the context of the attacks themselves and the background story of Anonymous.

Keywords: cyber terrorism, Anonymous, cyber security, hacktivism, OpRussia