Haktivizam

Vukota, Katarina

SVEUČILIŠTE U RIJECI
Fakultet za menadžment u turizmu i ugostiteljstvu
Preddiplomski sveučilišni studij

KATARINA VUKOTA

Haktivizam - hakiranje u političke ili društvene svrhe

Hacktivism - Hacking for Political or Social Purposes

Završni rad

Opatija, 2024.

SVEUČILIŠTE U RIJECI
Fakultet za menadžment u turizmu i ugostiteljstvu
Preddiplomski sveučilišni studij
Poslovna ekonomija u turizmu i ugostiteljstvu
Studijski smjer: Menadžment u turizmu

Haktivizam - hakiranje u političke ili društvene svrhe

Hacktivism - Hacking for Political or Social Purposes

Završni rad

Kolegij: **Sigurnost informacijskih sustava**
Student: **Katarina Vukota**
Mentor: **izv. prof. dr. sc. Ljubica Pilepić Stifanich**
Matični broj: **25205/20**

Opatija, svibanj 2024.

SVEUČILIŠTE U RIJECI UNIVERSITY OF RIJEKA
FAKULTET ZA MENADŽMENT U TURIZMU I UGOSTITELJSTVU
FACULTY OF TOURISM AND HOSPITALITY MANAGEMENT
OPATIJA, HRVATSKA CROATIA

IZJAVA O AUTORSTVU RADA I O JAVNOJ OBJAVI OBRANJENOG ZAVRŠNOG RADA

Katarina Vukota	**25205/20**
(ime i prezime studenta)	(matični broj studenta)

Haktivizam – hakiranje u političke i društvene svrhe
(naslov rada)

Izjavljujem da sam ovaj rad samostalno izradila/o, te da su svi dijelovi rada, nalazi ili ideje koje su u radu citirane ili se temelje na drugim izvorima, bilo da su u pitanju knjige, znanstveni ili stručni članci, Internet stranice, zakoni i sl. u radu jasno označeni kao takvi, te navedeni u popisu literature.

Izjavljujem da kao student–autor završnog rada, dozvoljavam Fakultetu za menadžment u turizmu i ugostiteljstvu Sveučilišta u Rijeci da ga trajno javno objavi i besplatno učini dostupnim javnosti u cjelovitom tekstu u mrežnom digitalnom repozitoriju Fakulteta za menadžment u turizmu i ugostiteljstvu Sveučilišta u Rijeci.

U svrhu podržavanja otvorenog pristupa završnim radovima trajno objavljenim u javno dostupnom digitalnom repozitoriju Fakulteta za menadžment u turizmu i ugostiteljstvu Sveučilišta u Rijeci, ovom izjavom dajem neisključivo imovinsko pravo iskorištavanja bez sadržajnog, vremenskog i prostornog mog završnog rada kao autorskog djela pod uvjetima *Creative Commons* licencije CC BY Imenovanje, prema opisu dostupnom na http://creativecommons.org/liceses/.

U Opatiji, lipanj, 2024.

Katarina Vukota
Potpis studenta

Sažetak

U ovome radu pojam Internet aktivizma odnosno haktivizma razmatra se u širem kontektu kroz proces kombinacije starijih društveno-aktivističkih ideja i novog tehnološkog okruženja. Cilj ovog završnog rada je objasniti, opisati i analizirati pojam haktivizma te upitnost etičnosti istoga, te odgovoriti na pitanje „Jesu li haktivisti kriminalci ili ne?“.

Klasični hakeri najčešće djeluju iz osobne koristi dok haktivisti svoje aktivnosti provode kako bi skrenuli pažnju na određene probleme, društvene, ekonomske ili socijalne. Oni izražavaju svoje nezadovoljstvo te potiču promjene u društvu. Uz razne vrste hakera koji postoje, također postoje i razne vrste hakerskih napada koji postaju sve složeniji. Etičnost ovih radnji je često upitna zbog štete koju mogu prouzročiti. Smatra se da dobra namjera ne može opravdati kriminalno djelo. Najpopularnije haktivističke skupine u svojem djelovanju koriste upravo takve napade te je moguće uvidjeti kako uz takvo nešto prenose svoje poruke i ideologije.

Razni zakoni pokušavaju spriječiti rad hakera, ali time i rad haktivista te se postavlja pitanje: „Da li zakoni pomažu svima ili osobe haktiviste stavljaju u opasnost oduzimajući njihova prava. Zakoni često nisu usklađeni s brzim promjenama te postoji stalna debata o tome jeli iste zakone treba postrožiti ili ih treba učiniti fleksibilnijima kako bi se omogućila sloboda izražavanja. Na ova pitanja i niz drugih upravo ovaj rad pokušava iznaći odgovore.

Ključne riječi: haktivizam; hakiranje; privatnost na internetu; sloboda govora; građanski neposluh; moralne dileme hakiranja; etičnost haktivizma

Sadržaj

Uvod

Predmet završnog rada je pojam haktivizma odnosno hakiranja u političke i društvene svrhe. Problematika završnog rada je upitnost etičnosti haktivizma te nedovoljno istražena tematika hakiranja u etičke svrhe. Haktivizam je oblik aktivizma koji potiče nenasilnu upotrebu tehnologije, točnije smatra se da je haktivizam aktivizam koji je postao elektronički. Hakiranje postaje alat za postizanje društvenih, političkih ili ekoloških ciljeva. Kroz povijest haktivizma i hakiranja općenito moguće je uvidjeti razvoj komunikacije na internetu te interneta općenito. Osnovni ciljevi rada su sljedeći:

- objasniti razliku između tradicionalnih oblika aktivizma i fenomena haktivizma;
- identificirati etičke dileme i moralne izazove s kojima se suočavaju osobe haktivisti u opusu djelovanja;
- analizirati odnos vlasti i korporacija prema haktivizmu, te
- objasniti načine na koje se haktivisti bore protiv cenzure i ograničavanja slogode govora na internetu.

Iz tako postavljenog predmeta i ciljeva istraživanja modu se formulirati sljedeća istraživačka pitanja:

1. Kako se haktivizam razlikuje od tradicionalnih oblika aktivizma?
2. Koje su etičke dileme i moralni izazovi s kojima se suočavaju haktivisti?
3. Kako se vlasti i korporacije odnose prema haktivizmu?
4. Kako se haktivisti bore protiv cenzure i ograničavanja slobode govora na internetu?

Pri izradi ovog rada korištene su metode deskripcije, analize, sinteze, indukcije i dedukcije. Također je korištena metoda kompilacije.

Rad osim uvoda i zaključka sadrži sedam međusobno povezanih dijelova. U uvodu je objašnjen predmet i problem istraživanja te se navode osnovni ciljevi rada. Nadalje su definirana istraživačka pitanja i opisana metodologija istraživanja. Uvod završava kratkim prikazom osnovne strukture rada. Prvi dio rada pod nazivom „Haktivizam – isticanje nepravde i zalaganje za promjenu“ daje

fokus na aktivizam, odnosno odgovara na pitanja „Što je aktivizam?“, „Tko su aktivisti?“ te na pitanje „Koje vrste aktivizma postoje?“. Sljedeći dio rada nosi naslov „Hakiranje“. U ovom dijelu rada spominje se i objašnjava pojam hakiranja, objašnjava se problematika sa nazivom „haker“, spominju se vrste hakera te opisuju klasični napadi koji su najčešći rezultati njihova djelovanja. Nadalje, u istom poglavlju se navode najpoznatiji hakeri u povijesti hakiranja te njihova djela. Treći dio rada govori o haktivizmu te o razlici između klasičnog hakiranja i haktivizma. Za analizu haktivizma kao oblika protesta, potrebno je raspravljati i analizirati načine na koje haktivisti hakiraju te koje tehnike koriste. Nakon toga, u radu se spominje povijest haktivizma, od samih početaka pa do danas te ukazuje na činjenicu koliko se haktivizam proširio globalno. Nadalje, spominju se najpopularnije haktivističke grupe; Anonymous, The Jester, LuLzSec, WikiLeaks i Telecomix; koje imaju najviše utjecaja i pomoću kojih je moguće uvidjeti kako je haktivizam vrsta prosvjeda unutar kibernetičkog prostora koji pomalo počinje gubiti granice. Slijedeći dio rada se odnosi na pitanje etičnosti i moralnosti hakiranja te navodi određene argumente kojima se hakeri vode da opravdaju svoja djela. Vezano za pitanje etičnosti, u radu se daje usporedba haktivizma kao oblika građanskog neposluha te argumenata kada je to moralno i etično. Za kraj, zadnji dio rada se dotiče pravnih regulativa, zakona i prijedloga zakona za koje haktivisti smatraju da ugrožavaju ne samo njih, već i sve ostale korisnike interneta. Zaključak ovoga rada iznosi osnovne nalaze ovog istraživanja do kojih je autorica došla te odgovara na postavljena istraživačka pitanja.

1. Aktivizam- isticanje nepravde i zalaganje za promjenu

Kada ljudi promatraju postupke koji ne uzrokuju dobrobit , često se osjećaju obveznima progovoriti i suprotstaviti se istome. Bilo da se radi o izgaranju fosilnih goriva, zlostavljanju životinja ili o lošem postupanju prema ljudima, kada se veći broj ljudi ujedini i zahtijeva promjene, imaju moć stvoriti drugačiji, „bolji“, svijet. Moguće je aktivizam definirati kao akciju koja izaziva osobe na vlasti da dovedu do promjene i da doprinesu općem dobru.

Ne postoji samo jedan način aktivizma. Naime, svaka akcija koja skreće pozornost na neki problem predstavlja aktivizam. U svojoj biti, aktivizam je najjednostavnije isticanje nepravde i zalaganje za bolju budućnost i promjenu. Tradicionalni oblici aktivizma uključuju prosvjede i demonstracije, no ako se napori aktivista zanemare, oni se okreću nekonvencionalnim oblicima aktivizma.[1]

Ovo poglavlje daje uvid u oblike aktivizma, odgovara na pitanja tko su aktivisti i koje su njihove uloge te kako aktivizam utječe na društvo.

1.1. Oblici aktivizma

1.1.1. Demonstracije i protesti

Vlada prima snažnu poruku kada se ljudi udruže i okupljaju oko jedinstvenog cilja. Javnost daje očigledan znak da postoji neki problem. Demonstracije se pojavljuju u raznim oblicima, kao marširanje na ulicama, javni prosvjedi i slično. Oni koji sudjeluju na prosvjedima često koriste šokantne taktike za privlačenje pažnje i povećanje pritiska. Neki od primjera su prosvjednici koji prosvjeduju goli.

[1] Brooks, E. (2023). What Is Activism: Definition, Types, Role, Examples, Importance, LIBERTIES, Creative Commons, https://www.liberties.eu/en/stories/activism/44871 (pristupljeno: 3.4.2024.)

1.1.2. Štrajk

Štrajk je oblik aktivizma u kojem zaposlenici odbijaju obavljati svoj posao u znak protesta. To je postao popularan oblik prosvjeda tijekom i nakon industrijske revolucije, kada su pripadnici industrijske radničke klase, od rudara ugljena do radnika u tvornicama, odložili svoj alat i zahtijevali bolje plaće i uvjete rada. 40-satni radni tjedan bio je rezultat dugotrajnog pokreta za reformu rada u Američkim Sjedinjenim Državama čija je strategija aktivizma uključivala nacionalne štrajkove.

1.1.3. Bojkot

Bojkot je oblik nenasilnog prosvjeda u kojem ljudi kolektivno odlučuju ne sudjelovati u aktivnosti, događaju, i organizaciji. Primjer je BDS (Boycott, Divestment, Sanction), pokret koji je predvođen Palestincima koji poziva građane, organizacije, institucije i vlade na globalnoj razini da izvrše ekonomski pritisak na Izrael kako bi prestao sa ugnjetavanjem Palestine povlačenjem komercijalne i društvene potpore. Bojkot je vrsta aktivizma koju može prakticirati svaka osoba svakodnevno pri obavljanju kupovine.

1.1.4. Online kampanje

Slanje e-pošte, objavljivanje na društvenim medijima i potpisivanje peticija pokazuje javnim dužnosnicima, korporacijama i drugim moćnicima da su ljudi uloženi u cilj i šalje poruku da će njihova popularnost biti ugrožena ako ne obrate pažnju. Ovo je oblik izgradnje mandata, jer pokazuje da javnost podržava određeni smjer djelovanja i legitimizira zahtjev za reformom. Što je više angažmana, to je pritisak jači.

1.1.5. Građanski neposluh

Građanski neposluh je oblik prosvjeda s dugom tradicijom u kojem prosvjednici namjerno krše zakon kako bi istaknuli neke nepravde ili doveli do promjene zakona ili politike. Oni prosvjednici koji se upuštaju u ovu vrstu aktivizma, svojevoljno i svjesno riskiraju suočavanje s određenim posljedicama kao što su novčane kazne ili uhićenja kao sredstvo pokazivanja svoje predanosti cilju. Posljednjih su godina ekološki pokreti kao što su The Extinction Rebellion ili Just Stop Oil privukli pozornost javnosti svojim nekonvencionalnim prosvjedima koji uključuju blokiranje prometa, ometanje sportskih događaja visokog profila i bacanje hrane na poznata umjetnička djela.

1.1.6. Protestna umjetnost

Umjetnici često koriste svoje radove kako bi potaknuli rasprave o važnim društvenim i političkim temama, osobito ako im slava daje platformu za dopiranje do masa. Primjer je Keith Haring koji je dizajnirao plakate koji su korišteni na prosvjedima protiv nuklearnog oružja i apartheida.

1.2. Aktivisti i njihove uloge

Aktivistom se smatra svaka osoba kojoj je stalo do određenog cilja i koja sudjeluje u kolektivnoj akciji za postizanje određene promjene. Unutar pokreta postoje razne uloge koje aktivisti mogu preuzeti kako bi bili učinkoviti u postizanju svoje misije.

Prva i najčešća uloga je uloga građana. Građani koji se bave aktivizmom igraju važnu ulogu jer utjelovljuju demokratske vrijednosti prema kojima bi obični građani trebali biti aktivno uključeni u donošenje političkih odluka.

Nadalje, reformator je tipično osoba koja će pokušati stvoriti promjenu iznutra koristeći postojeće institucije za postizanje ciljeva svog pokreta. Lobiranje, javno zagovaranje, referendumi i skupovi su preferirani načini na koji reformatori provode aktivizam.

S druge strane, buntovnik radi van sustava. Oni iznose pitanja u javnost a njihovi reformski zahtjevi ciljaju na nositelje moći kao što su vlade i institucije.

Na kraju, nositelj promjena je aktivist odgovoran za educiranje javnosti o društvenim pitanjima i uključivanje običnih građana u proces donošenja promjena.[2]

[2] Brooks, E. (2023). What Is Activism: Definition, Types, Role, Examples, Importance, LIBERTIES, Creative Commons, https://www.liberties.eu/en/stories/activism/44871 (pristupljeno 3.4.2024.)

1.3. Utjecaj aktivizma na društvo

Mnoge od najvažnijih društvenih i političkih revolucija koje su se dogodile u povijesti rezultat su aktivizma. Od ukidanja ropstva, dobivanja jednakih prava žena do rušenja diktatura, promjena koja je u jednim trenutku bila nezamisliva, postala je stvarnost zahvaljujući hrabrosti, viziji i predanosti aktivista.

Budući da obično djeluju izvan sustava moći, aktivisti kontroliraju moćnike. Njihova je uloga osigurati da vlade, korporacije i moćni pojedinci djeluju u najboljem interesu većine, a ne nekolicine elita. Pokret za klimatske promjene snažan je primjer aktivista koji drže političke vođe i tvrtke odgovornima za njihov štetan utjecaj na društvo i vrše pritisak na njih da dobrobit ljudi i planeta stave ispred profita.

2. Hakiranje

Postoje mnogobrojne definicije „hakera“. Kada se sve one zajedno kombiniraju, na kraju dobijamo računalnog entuzijasta koji uživa u učenju programskih jezika i računalnih sustava i često se može smatrati stručnjakom za tu temu, koji je ovladao umjetnošću i znanošću izrade računala i softvera te su sposobni učinit puno više nego što su izvorni dizajneri planirali. [3]

Haker je eventualno postao negativan naziv koji opisuje osobe koje bez dopuštenja „provaljuju“ u tuđe računalo te namjerno nanose štetu.

Ovo poglavlje daje uvid u same početke hakiranja te povijest samog naziva te kako se definicija s vremenom promijenila. Nadalje, u poglavlju se objašnjavaju vrste hakera te se navode najpoznatiji hakeri svih vremena.

2.1. Povijest hakiranja

Na samim početcima upotrebe računala, hakeri su bile osobe koje su znale kodni jezik i koje su bile sposobne raditi s računalima. Hakeri su bili stručnjaci za računala te njihovo ime nije negativnog značenja. Oni koji su svoje znanje i vještine zloupotrijebili se zvali „krakeri“. "Krakiranje" se obično odnosi na nezakonito provaljivanje u tuđe računalo nizom tehnika, kao što je iskorištavanje tehničkih grešaka. Eventualno, pojmovi hakiranje i krakiranje se izjednačavaju. [4]

U kolovozu 2014. hackerspaces u Nizozemskoj izdao je otvoreno pismo nizozemskom javnom tužiteljstvu (PPS): U ovom dokumentu članovi hakerskih zajednica iz Amsterdama, Heerlena, Utrechta i drugih gradova pozvali su vladinu instituciju da prepravi definiciju ' hakiranje' kako je predstavljeno na njihovoj web stranici .Dok je PPS to opisao kao "provaljivanje u računala bez dopuštenja", članovi hackerspacea istaknuli su da se hakiranje odnosi na kreativno bavljenje

[3] Sukhai, N (2004). Hacking and cybercrime. In Proceedings of the 1st annual conference on Information security curriculum development (InfoSecCD '04). Association for Computing Machinery, New York, NY, USA, 130.
[4]Devitt, M. (2001). A brief history of computer hacking. // Dynamic Chiropractic 19, 13. https://www.dynamicchiropractic.com/mpacms/dc/article.php?id=18078 (preuzeto 04.03.2024.)

tehnologijama. Protiveći se svođenju hakiranja na ilegalne aktivnosti, hakiranje su opisali kao istraživanje tehnoloških mogućnosti i granica na nepredviđene, inovativne načine.[5]

Na primjer, hakeri su postali poznati po tome što su provalili u sustave i zatim govorili kontrolorima tih sustava kako su to učinili i davali (obično neželjene) savjete kako popraviti stvari.[6]

Prvi oblici hakiranja zapravo uopće nisu započeli na računalima. U 1960-ima, jedan od prvih populariziranih hakiranja, povezan s telefonima, bio je poznat kao phreaking. Phreaking je kada pojedinac koristi zviždaljku ili drugu visoku buku kako bi prevario telefon da primi operativne naredbe i tako promijeni ponašanje telefonskog sustava.

Otprilike 1965. John Draper, koji je postao poznat kao Cap'n Crunch zbog svojih tehnika phreakinga, shvatio je da može koristiti igračku zviždaljku za iskorištavanje telefonskih poziva. Zviždaljku je pronašao u kutiji sa žitaricama, otuda i njegov nadimak. Uz pomoć zviždaljke i prave frekvencije buke, uspio je obaviti besplatne međugradske telefonske razgovore.

Svijet hakiranja kakav poznajemo danas započeo je ranih 1970-ih, nakon popularizacije ranih računala. S vladinim agencijama koje su koristile ove nove tehnologije, Zračne snage su 1971. naručile prvi pentest svojih sustava. Ti timovi visoko tehničkih stručnjaka postali su poznati kao "Tiger teams" i bili su jedna od najranijih vrsta hakera. Nakon uspona Tiger Teamsa 1970-ih, mogu se vidjeti i drugi primjeri hakiranja u tradicionalnijem smislu, kao što je izum prvog računalnog crva na svijetu i antivirusa koji je uslijedio.

Kako je vrijeme odmicalo, sve je više agencija počelo testirati svoju mrežnu sigurnost kao odgovor na neke od najranijih oblika računalnog hakiranja. Do 1980-ih, svijet hakiranja dovoljno je napredovao da je Kongres poduzeo akciju donošenjem Zakona o računalnim prijevarama i zlouporabi, koji je do danas ostao tema rasprave.

[5] Richterich, A. & Wenz, K. (2017). Introduction. Making and Hacking. Digital Culture & Society, 3(1), 20.
[6] Jordan, T. (2016). A genealogy of hacking. Convergence: The International Journal of Research into New Media Technologies, 23(5), 531.

2.2. Vrste hakera

Hakere je moguće podijeliti u 3 skupine, točnije 3 šešira: crni šeširi, bijeli šeširi i sivi šeširi. Izrazi potječu iz sheme kodiranja boja koja se nalazi u vesternima iz 1950-ih, gdje su loši likovi nosili crne šešire, a dobri likovi bijele ili druge šešire svijetlije boje.

2.2.1. Crni šeširi

Hakeri koji spadaju pod crni šešir su kriminalci koji provaljuju u računalne mreže sa zlom namjerom. Objavljuju zlonamjerne softvere koji uništavaju datoteke, kradu lozinke, brojeve kreditnih kartica i druge osobne podatke. Hakiranje jest postalo glavno oružje za prikupljanje obavještajnih podataka za vlade ali crni šeširi ipak češće rade sami ili s organizacijama organiziranog kriminala za laku zaradu. [7]

2.2.2. Bijeli šeširi

Hakeri koji spadaju pod bijeli šešir koriste svoje sposobnosti da oštete organizaciju- ali samo hipotetski. Prava svrha hakera bijelog šešira je zapravo otkrivanje sigurnosnih propusta u sustavu kako bi pomogli pri zaštiti poslovanja od opasnih hakera. Tvrtke angažiraju Bijele šešire da testiraju svoje informacijske sustave. Oni provode detaljno i dubinsko skeniranje mreža u potrazi za zlonamjernim softverima koristeći metode koje koriste i Crni šeširi, čak testiraju i osoblje tako da ih navedu da kliknu na poveznice koje vode do zaraze zlonamjernim softverom. Bijeli šeširi su jedan od razloga zašto velike organizacije obično imaju manje zastoja i imaju manje problema sa svojim web stranicama. Hakeri iz tog razloga često lakše ulaze u sustave malih tvrtki, jer znaju da male tvrtke nemaju resursa da si priušte testiranje od strane Bijelog šešira. [8]

2.2.3. Sivi šeširi

Između Bijelog i Crnog šešira se nalaze Sivi šešir hakeri. Oni provode smjesu aktivnosti i crnog i bijelog šešira. Sivi šeširi traže rupe i ranjivosti u sustavu ali bez dopuštenja i znanja vlasnika. Ako pronađu probleme, prijaviti će ih vlasniku, no također će tražiti i mali naknadu za rješavanje

[7] What is a Black-Hat hacker? kaspersky. https://www.kaspersky.com/resource-center/threats/black-hat-hacker (pristupljeno: 02.04.2024)
[8] White Hat Hackers: The Good, the Bad, or the Ugly? kaspersky. https://www.kaspersky.com/resource-center/definitions/white-hat-hackers (pristupljeno: 02.04.2024.)

problema. Sivi šeširi vjeruju da rade nešto dobro kada hakiraju i napadaju web stranice od tvrtki bez njihovog dopuštenja. No vlasnici tvrtki jako rijetko cijene takve neovlaštene upade u njihovu informacijsku infrastrukturu. Stvarna namjera Sivog šešira je hvalisanje svojim vještinama o dobivanje publiciteta jer oni smatraju da svojim dijelima pridonose kibernetičkoj sigurnosti. [9]

2.3. Najpoznatiji hakeri

2.3.1. Aron Swartz

Aaron Swartz je slavno pomogao pokrenuti popularnu online društvenu mrežu Reddit i izazvao niz pozornosti tijekom svog vremena kao haktivist. Godine 2011. vlada je uhitila i optužila Swartza za hakiranje mreže MIT-a radi preuzimanja goleme predmemorije JSTOR akademskih podataka. Ove su optužbe na kraju prerasle u dvije savezne točke optužnice za prijevaru putem interneta i gotovo desetak kršenja Zakona o računalnim prijevarama i zlouporabi s maksimalnom kaznom od milijun dolara i 35 godina zatvora.

Kroz proces nagodbe, u kojem je Swartz odbio sudjelovati, tragično je počinio samoubojstvo. Nekoliko godina nakon njegove smrti, Internetska kuća slavnih uvrstila je Swartza zbog njegovog rada na osnivanju online grupa kao što je Demand Progress i njihove kampanje protiv Zakona o privatnosti na internetu.[10]

2.3.2. Kevin Poulsen

Počevši kao tinejdžer, Kevin je hakirao ARPANET, Pentagonovu računalnu mrežu. Napad je brzo otkriven, što je dovelo do uhićenja gospodina Poulsena. Unatoč tome što je uhvaćen, vlada je mladog gospodina Poulsena pustila uz upozorenje. Do kraja desetljeća, 1988., još jedan hak koji je izveo gospodin Poulsen doveo ga je u sukob s vladom. Kako bi izbjegao uhićenje, otišao je u ilegalu i nastavio hakirati vladine tajne.

[9] Black hat, White hat, and Gray hat hackers – Definition and Explanation. kaspersky. https://www.kaspersky.com/resource-center/definitions/hacker-hat-types (pristupljeno: 02.04.2024.)
[10] Martini, M. (2017). Mourning for a hacktivist: grieving the death of Aaron Swartz on a digital memorial. Media, Culture & Society, 40(2), 235.

Do 1990. proslavio se provalom u radio postaju kako bi osigurao natjecanje za potpuno novi Porsche, odmor i 20.000 dolara. Od tada je uhićen i tri godine mu je zabranjeno korištenje računala kao oblik kazne. Danas Poulsen radi kao haker s bijelim šeširom i novinar, pišući za popularne publikacije kao što su Wired i The Daily Beast.[11]

2.3.3. Michael Calce zvani MafiaBoy

Michael je postao poznat po nizu napada (DDoS) na razne korporativne mreže. Prvo, g. Calce je iskoristio mrežu sveučilišnih računala kako bi srušio vodeću tražilicu u to vrijeme, Yahoo.

Ubrzo nakon toga, napao je Dell, eBay, CNN i Amazon koristeći svoj sada zloglasni DDoS napad. Ovaj je napad donio iznenađujuću realizaciju korporativnoj Americi, šokiranoj što su se tvrtke vrijedne milijarde dolara tako lako zatvorile. Briga za korporativne interese dovela je do niza zakonskih promjena usmjerenih na kibernetički kriminal. Danas Miachael radi kao haker s bijelim šeširom koji promiče testiranje kibernetičke sigurnosti i treninge za podizanje svijesti kako bi se tvrtke zaštitile od internetskih prijetnji.[12]

2.3.4. Jeanson James Ancheta

Jeanson je zauzeo jedinstveni pristup hakiranju u usporedbi s drugima svojom znatiželjom o "botnetovima". Ovi botnetovi sastojali su se od softverskih napada koji su probili kontrolu nad računalnim sustavom.

Do 2005. Jeanson je uspješno kompromitirao gotovo pola milijuna strojeva. Kao što je navedeno od strane Ars Technica, g. Ancheta je koristio ovu mrežu da profitira prodajom pristupa tvrtkama za oglašavanje i drugim hakerima. Zbog ovih ludorija i posebno zbog kršenja Zakona o zlouporabi računalnih prijevara, vlada ga je optužila za zločin. Njegova bi kazna bila 57 mjeseci zatvora i novčana kazna od 75.000 dolara, što bi označilo prvi put da je haker dobio zatvorsku kaznu zbog korištenja botneta.[13]

---

[11] Prasad Tulasi, S. (2014.). Ethical Hacking and Types of Hackers, International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE), 11(2), 25.
[12] Deshmukh, R. V., & Devadkar, K. K. (2015). Understanding DDoS Attack & its Effect in Cloud Environment. Procedia Computer Science, 49, 208.
[13] Fox, J. (2021). Top 10 famous hackers, https://www.cobalt.io/blog/top-ten-famous-hackers, (pristupljeno: 30.05.2024.)

2.3.5. Matthew Bevan i Richard Pryce

Kao tim britanskih hakera, Bevan i Pryce postali su poznati po hakiranju vojnih mreža tijekom kasnih 1990-ih. Njih su dvojica zamalo započeli globalni sukob kada su Korejskom institutu za atomska istraživanja procurili podaci o američkom vojnom sustavu. Iako je Bevan tvrdio da je tražio informacije o NLO-ima, napadi na napredne vojne mreže pokazali su ranjivost tih visoko povjerljivih mreža.[14]

2.3.6. Albert Gonzalez

Prema NY Daily Newsu, g. Gonzalez je pokazao rane znakove vodstva tijekom srednje škole gdje je vodio „čopor problematičnih računalnih štrebera.“ U dobi od 22 godine vlada je uhitila g. Gonzaleza zbog optužbi povezanih s prijevarom u vezi s njegovom aktivnošću krađe podataka o debitnoj kartici. To je dovelo do njegove suradnje s vladom i na kraju do suradnje s tajnom službom.[15]

Iako je tijekom svog vremena radio s vladom na hvatanju hakera, nastavio je raditi crni hakerski posao. Do 2005. pomogao je organizirati napad na TJX s osnovnom SQL injekcijom, što je dovelo do procijenjenih 256 milijuna dolara. Godine 2015., tijekom izricanja presude za hakiranje TJX-a, tužitelji su njegove cyber napade i štetu koju su oni prouzročili nazvali "neusporedivim".[16]

2.3.7. Adrian Lamo

Adrian je došao u središte pozornosti javnosti zbog svojih hakerskih aktivnosti probijanjem sustava za upravljanje sadržajem i dodavanjem lažnog citata državnog odvjetnika Johna Ashcrofta. Lamo je postao ozloglašen zbog svojih djela kako za medije tako i za žrtve njegovih hakiranja. Do ove točke, Lamo je sa svojim hakiranjem otišao predaleko 2002. kada je provalio u mrežu The New York Timesa. To je dovelo do kazne od dvije godine uvjetne i novčane kazne od gotovo 65.000 dolara.[17]

[14] Phillips, Peter J. and Pohl, Gabriela, (2022) The Economics of Information and Human Factors in Cybersecurity
[15] Lu, Y., Luo, X., Polgar, M., & Cao, Y. (2010). Social Network Analysis of a Criminal Hacker Community. Journal of Computer Information Systems, 51(2), 32
[16] Pogrebna, G. & Skilton, M. (2019). A Sneak Peek into the Motivation of a Cybercriminal. Navigating New Cyber Risks, 43.
[17] Bradbury, D. (2011). The World’s Dumbest Hackers. Infosecurity, 8(2), 17

2.3.8. Gary McKinnon

Godine 2002. Gary je postao poznat u svijetu računalnog hakiranja počinivši "najveći vojni računalni hak svih vremena". G. McKinnon je izrazio iskrenu namjeru probijanja tih vojnih mreža kako bi potražio informacije o NLO-ima i drugim tehnologijama korisnim za javno dobro. Unatoč svemu tome, nikada nije osuđen za zločin jer je Ujedinjeno Kraljevstvo blokiralo njegovo izručenje Sjedinjenim Državama kako bi se suočio s kaznenim optužbama do 70 godina zatvora.[18]

2.3.9. Julian Assanage

Jedan od najpoznatijih hakera na svijetu zbog svoje međunarodne prisutnosti u medijima, Julian Assange nudi suvremeni primjer koliki utjecaj na svijet pojedinac može imati kroz hakiranje.

Budući da je bio na Interpolovom popisu najtraženijih, mnogi u svijetu bi Assangea spremno identificirali kao jednog od najvećih hakera na svijetu uzimajući u obzir otkrića utjecaja koje je njegova organizacija, Wikileaks, objavila svijetu. Kroz sve to, Assange čeka izručenje Sjedinjenim Državama kako bi se suočio s optužbama za svoju umiješanost u organizaciju Wikileaks.

Od siječnja 2021. Ujedinjeno Kraljevstvo je službeno blokiralo izručenje Juliana Assnagea kako bi se suočio s optužbom u Sjedinjenim Državama.[19]

2.3.10. Kevin Mitnick

Kevin Mitnick počeo je hakirati u ranoj dobi. U središte pozornosti javnosti dospio je 1980-ih nakon što je hakirao Zapovjedništvo obrane Sjeverne Amerike (NORAD). Ti bi događaji inspirirali film Ratne igre.

Dva druga slučaja hakiranja dovela su Mitnicka do mjesta hakera broj jedan svih vremena. Prvo je 1989. hakirao Digital Equipment Corporation (DEC) kako bi napravio kopije njihovog softvera. Hakiranje DEC-a dovelo je do njegovog uhićenja od strane FBI-a i osude. Unatoč ovom visokoprofilnom uhićenju, dok je bio na slobodi, Mitnick je slavno hakirao Pacific Bellov sustav govorne pošte, samo kako bi dokazao da može.

[18] Arnell, P. & Reid, A. (2009). Hackers beware: the cautionary story of Gary McKinnon. Information & Communications Technology Law, 18(1), 5.
[19] Anderson, P. D. (2020). Privacy for the weak, transparency for the powerful: the cypherpunk ethics of Julian Assange. Ethics and Information Technology.

Posljednjih godina, Mitnick je držao granicu između hakera s bijelim i crnim šeširom sa svojom tvrtkom za cyber-sigurnost i uslugama savjetovanja za sigurnost kao što je "Mitnick's Absolute Zero Day Exploit Exchange". Kroz svoje dugogodišnje iskustvo postao je poznat kao jedan od najpoznatijih i najboljih hakera na svijetu.[20]

[20] Prasad Tulasi, S. (2014.). Ethical Hacking and Types of Hackers, International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE), 11(2), 26.

3. Haktivizam- elektronički aktivizam

Politički protesti su česta pojava u gotovo svim zajednicama, nebitno jesu li to demonstracije na ulici ili su to sastanci političara. Ljudi žele utjecati i kontrolirati prostore u kojima žive i danas je to čak prešlo u virtualni svijet i ljudi također žele kontrolirati kibernetički prostor. Pojam haktivizam je moguće definirati kao nenasilna upotreba hakiranja, točnije ilegalnih ili pravno dvosmislenih alata, u političke svrhe. Također bi se moglo reći da je haktivizam kombinacija političkog prosvjeda i računalnog hakiranja. Primjeri tih ilegalnih alata su kvarenje web stranica, krađa informacija, parodije na web stranice, DoS napadi i virtualne sabotaže. (Denial-of-Service (DoS) napad je napad namijenjen gašenju stroja ili mreže, čineći ga nedostupnim korisnicima kojima je namijenjen. DoS napadi to postižu preplavljivanjem mete prometom ili slanjem informacija koje pokreću rušenje.) [21]

Ovo poglavlje naglašava bitne razlike i sličnosti između hakiranja i haktivizma te objašnjava forme, točnije postupke kojima se haktivisti koriste.

3.1. Sličnosti i razlike hakiranja i haktivizma

Razvijanjem Interneta dolazi i do razvijanja alata koje koriste haktivisti za postizanje svojih ideoloških ciljeva. Cilj i gledište pojedinca će vjerojatno odrediti sami oblik haktivizma. Haktivisti djeluju unutar kibernetičkog prostora no njihov utjecaj se osjeti i u izvan mrežnom okruženju. Najjednostavnije rečeno, haktivizam je aktivizam koji je postao elektronički.

Haktivizam koristi računalne tehnike posuđene od već postojeće hakerske zajednice te je zbog toga teško točno odrediti gdje prestaje hakiranje a započinje haktivizam. Hakiranje i haktivizam imaju različite motive: motiv hakiranja je najčešće osobni interes, dok je motiv haktivizma postizanje nekog društvenog ili političkog cilja. Pojam hakiranja nije oduvijek korišten za opisivanje

[21] What is a denial of service attack (DoS) ? Paloalto Networks. https://www.paloaltonetworks.com/cyberpedia/what-is-a-denial-of-service-attack-dos (pristupljeno: 15.04.2024.)

kibernetičkog kriminala. Hakiranje je izvorno opisano kao inovativno korištenje tehnologije za rješavanje određenog problema. Nadalje, hakiranje se često koristi u obrani ili promicanju skupa normi koje su se razvile kao dio internetske kulture. Ali danas, hakiranje se razlikuje od haktivizma jer hakiranju nedostaju politički ciljevi. Veliki dio hakiranja je motiviran prijevarnim ciljevima. Hakeri su odgovorni za krađu identiteta, prijevare, špijunažu i razne druge zločine s godišnjim troškovima u trilijunima dolara[22]. FBI je kibernetički kriminal proglasio najznačajnijim kriminalom, naime u SAD-u je borba protiv kibernetičkog kriminala glavni prioritet, odmah nakon protuterorizma i protuobavještajne službe. Globalni prostor kibernetičke sigurnosti je posljednjih godina doživio povećane prijetnje. Tijekom pandemije Covid- 19, 2020. godine, napadi zlonamjernim softverom porasli su za 358% u usporedbi s 2019. [23]

U suprotnosti sa hakiranjem, haktivizam je uglavnom motiviran političkim interesima koji su barem djelomično usmjereni na „offline" probleme. Angažiran je prvenstveno s komunikacijskim a ne destruktivnim ciljevima. Najbolji primjer je napad na web stranicu DOJ-a. DOJ (Department of Justice) je američko ministarstvo pravosuđa koje provodi federalne zakone, traži pravednu kaznu za krivce i osigurava pošteno i nepristrano provođenje pravde. Haktivisti su napali njihovu službenu stranicu u znak protesta protiv Zakona o pristojnosti u komunikaciji iz 1996. Haktivisti su izjasnili svoju zabrinutost da bi se implicirano zakonodavstvo uplelo i degradiralo kulturu i vrijednost Interneta kroz cenzuru. Ovaj napad također odražava komunikativni element haktivizma jer je web stranica DOJ-a ostala djelomično u funkciji tijekom i nakon napada, a trošak popravka oštećenja je bio minimalan.[24]

[22] Hampson, N.C.N. (2012). Hacktivism: A New Breed of Protest in a Networked World, Boston College International and Comparative Law Review, 35(2), 529
[23] Griffiths, C. (2022). The Latest 2022 Cyber Crime Statistics (updated November 2022). AAG. https://aag-it.com/the-latest-2022-cyber-crime-statistics/ (pristupljeno: 29.03.2024.)
[24] U.S. Department of Justice. US.GOV. https://www.usa.gov/federal-agencies/u-s-department-of-justice (pristupljeno: 29.03.2024.)

3.2. Forme haktivizma

Za analizu haktivizma kao oblika protesta, potrebno je raspravljati i analizirati načine na koje haktivisti hakiraju te koje tehnike koriste. Međutim, razvijanjem tehnologije, dolazi i do razvijanja oblika haktivizma. Sljedeće opisane metode su samo najpopularniji primjeri haktivizma u nedavnoj prošlosti; te najpopularnije metode bi mogle biti u potpunosti drugačije u bliskoj budućnosti.

3.2.1. DoS napadi (Denial of Service)

Kao što je već spomenuto DoS napadi su namijenjeni gašenju stroja ili mreže, čineći ga nedostupnim korisnicima kojima je namijenjen. DoS napadi to postižu preplavljivanjem mete prometom ili slanjem informacija koje pokreću rušenje. Popularna iteracija DoS napada je DDoS napad, koji se razlikuje od DoS napada korištenjem mreže višestrukih napadajućih računala. Tijekom DDoS napada, inicijator aktivira moć napada a mreža računala pod kontrolom inicijatora, botnet, umnožava tu moć prema ciljnom poslužitelju. Botneti su postali jako rašireni i brojni. Izvješća pokazuju da je ponuda botneta puno veća od potražnje za istima, što je dovelo do pada cijene. Posljedično, DDoS napadi su se značajno povećali u proteklih nekoliko godina. Softver koji je bio korišten tijekom napada na WikiLeaks je nazvan „Low Orbit Ion Cannon“ (LOIC). Taj softver je čak i početnicima omogućio da se pridruže DDoS napadu. Sudjelovanje je bilo relativno jednostavno; LOIC je dopuštao sudjelovanje na dva načina: izravno, utipkavajući IP adresi mete te klikom na gumb „FIRE“ (ispali). Drugi je bio alternativni način: žrtvujući svoja računala ili mreže na takozvani „LOIC Hivemind“ i time dopuštajući drugim korisnicima da usmjeravaju napade iz predanog sustava. Za razliku od članova nenamjernih botneta, korisnici LOIC-a zadržavaju mogućnost dodavanja ili uklanjanja svojih računala iz napadačke mreže.

DDoS napadi često krše zakone više nacija. Inicijator koji se nalazi u zemlji A može kontrolirati mrežu računala koja se nalaze u zemljama B, C i D da napadne web stranicu smještenu na poslužitelju koji se nalazi u zemlji E. To znači da se žrtva, dokazi i počinitelji mogu nalaziti na različitim mjestima, točnije u različitim zemljama, od kojih mnoge vjerojatno imaju različite režime kibernetičke sigurnosti, ili još gore, nikakav režim.

3.2.2. Oštećenja web stranica

Vjeruje se da je narušavanje web stranica, poput onog napada na DOJ, najčešći oblik haktivizma. Pod oštećenje web stranice se smatra dobivanje neovlaštenog pristupa web poslužitelju i zamjena ili mijenjanje web stranice s novim sadržajem koji prenosi neku određenu poruku. Oštećenja mogu biti ograničena na jedno mjesto ili se mogu dogoditi u enormnim količinama na tisućama stranica. Iako haktivisti ovim postupkom učinkovito preuzmu ciljanu stranicu kako bi prenijeli neku poruku, narušavanje ne mora nužno oštetiti cijelu stranicu. Oštećenjem web stranice se obično koriste kao sredstvo za prenošenje poruke ali također tim činom pokazuju svoju moć te privlače pažnju.

3.2.3. Preusmjeravanje stranice

Kao što sami naziv sugerira, haktivisti preusmjeravanjem šalju korisnike na drugačiju stranicu umjesto na onu koja je naznačena web adresom. Dobivanjem neovlaštenog pristupa web poslužitelju i podešavanjem postavki adrese, počinitelj navodi potencijalne korisnike da dođu do alternativnog mjesta. Ovom metodom haktivist otima pristup stranici koja je ciljana i preuzima kontrolu nad sadržajem koji se prikazuje kada korisnik interneta koristi web adresu za ciljanu stranicu.

3.2.4. Virtualni Sit-in

Virtualni Sit-in je vrsta elektroničkog građanskog neposluha gdje aktivisti i prosvjednici izražavaju svoja mišljenja istovremeno. Pristupaju web stranici više puta te tim činom stvaraju prekid rada ciljane web stranice. Naziv izraza je izveden iz popularnog nenasilnog oblika prosvjeda koji je bio popularan tijekom Pokreta za građanska prava u Sjedinjenim Američkim Državama tijekom 1950-ih i 1960-ih. Virtualni Sit-in je također poznat kao virtualna blokada. [25]

Kao forma haktivizma, moguće ga je usporediti sa DDoS. Cilj obje metode je usporiti ili srušiti ciljani poslužitelj pretrpavajući ga zahtjevima za informacija. Ključna razlika je u tome što umjesto da mrežom zapovijedaju botneti, Virtualni Sit-ins uključuju pojedince koji ponovno učitavaju web stranice. Određeni jednostavno ručno ponovno učitavaju stranice a drugi preuzimaju određeni kod koji im dopušta automatsko i ponovno učitavanje ciljane stranice. Virtualni Sit-ins se smatra „masovnim oblikom haktivizma“ i „demokratskim ili reprezentativnim oblikom haktivizma.“

[25] Virtual Sit-In. techopedia. https://www.techopedia.com/definition/29626/virtual-sit-in (pristupljeno: 03.04.2024.)

3.2.5. Krađa informacija

Krađa informacija je metoda haktivizma koja se u jednu ruku ne može razlikovati od obične provale. Uključuje neovlašteno stjecanje pristupa računalu ili mreži te krađu privatnih podataka. Iako je krađa informacija ne dvosmisleno nezakonita, ova metoda je iznenađujuće najviše prihvaćena od strane haktivista.

4. Povijest haktivizma

Hakiranje datira još iz 1950.-ih godina, kada su studenti Tehnološkog fakulteta u Massachusettsu počeli eksperimentirati sa strujnim krugovima, no tek u listopadu 1989. godine se dogodila prva haktivistička akcija. Tada se zlonamjerni crv uvukao u računala NASA-e i Ministarstva energetike SAD-a te je promijenio zaslone za prijavu zaraženih računala. Na zaslonima je pisalo „Crvi protiv nuklearnih ubojica“. To je bio dio anti nuklearnog pokreta. Iako je ovaj napad bio izveden online, bio je izazvan i namjera je bila utjecaj na fizički svijet.

Nadalje, takozvani „Zippies“ su u studenom 1994. koristili DDoS napade kao odmazdu za Zakon o kaznenom pravosuđu. Njihov napad je preopteretio poslužitelje vladinih web stranica, uzrokujući njihovo gašenje tjednima.

„Hongkonške plavuše“ su ciljale na kineske računalne sustave kako bi stanovništvu omogućile besplatan pristup internetu. To je primjer akcije koja je bila izravnije usmjerena na Internet i kontrolu nad njim.

Electronic Disturbance Theatre (EDT) je dalje doprinosio razvoju haktivizma. EDT je imao cilj razbijanja pregrade između online i offline aktivizma te je stvorila „Floodnet“. Ovaj program je omogućio „normalnim“ osobama, onima koji nemaju hakerskog iskustva da provedu zajednički DDoS napad. EDT je bio podrška Zapatistima. („Pojam "Zapatisti" se općenito odnosi na skupinu ljudi koji sudjeluju u anti globalističkoj borbi za demokraciju i zemljišnu reformu u Chiapasu, Meksiko, organizirani oko EZLN-a (Zapatistička nacionalna oslobodilačka fronta“).[26] Kao podrška zapatističkim pobunjenicima grupa je organizirala velike DDoS napade na američke i meksičke poslužitelje. [27]

2003. godine, 15- godišnji V. Pool je kreirao web stranicu „4.chan.org“ te je tom stranicom privukao puno prometa. Platforma je bila namijenjena razmjeni različitih ideja i stavova. Na

[26] Brief Historical Background to the Zapatista Movement. Hemispheric Institute. https://hemisphericinstitute.org/en/su10-tourism/item/879-su10-brief-historical-background-zapatista-movement.html (pristupljeno: 12.04.2024.)
[27] Brief Historical Background to the Zapatista Movement. Hemispheric Institute. https://hemisphericinstitute.org/en/su10-tourism/item/879-su10-brief-historical-background-zapatista-movement.html (pristupljeno: 12.04.2024.)

forumima stranice su hakeri razmjenjivali savjete o hakiranju i kodiranju te se to razvilo u slobodnu grupu za pridruživanje i napuštanje. Članovi bez računa su djelovali s korisničkim imenom „anonymous“ te su usvojili ovo ime za svoju grupu.

Do 2008. haktivisti su izveli nekoliko DDoS napada na Scientologiju („Ovo je samonaziv prilično kontroverzne doktrine koju je stvorio američki drugorazredni pisac znanstvene fantastike Ron Hubbard ranih 1950-ih…u mnogim zemljama zabranjena je djelatnost scijentoloških centara, jer se njezini sljedbenici služe metodama karakterističnim za totalitarne sekte, potiskujući volju osnovnih članova zajednice i prisiljavajući ih da svoju imovinu daju na raspolaganje vođama.“[28]). Izveli su napad nakon što je organizacija pokušala ukloniti video koji je procurio na YouTube. Tijekom ove kampanje, „Anonymousi“ su organizirali i online i offline prosvjede čime je moguće uvidjeti kako je haktivistički pokret još više prešao online granice.

[28] Scijentologija - što je to? Podarilove. https://podarilove.ru/hr/saentologiya-chto-eto-cerkov-saentologii-saentologiya-sekta-saentologiya-v-rossii-izvestnye-lyud/ (pristupljeno: 12.04.2024.)

5. Primjeri skupina haktivizma

5.1. Anonymous

Podrijetlo Anonymousa leži u neugodnom, ponekad duhovitom ali i zastrašujućem svijetu internetskog „trolanja“ (engl. trolling) namjerno učestalo širenje sarkastičnih komentara na društvenim mrežama ili forumima upućenih slučajno odabranoj osobi s ciljem izazivanja sukoba.) [29]. Do 2007. godine Anonymousi su bili toliko poznati po trolanju da su ih Fox News prozvali „stroj mržnje na internetu“. Anonymous je uživajući prigrlio ovaj naziv čime se pojačala pažnja medija. Šest mjeseci nakon što je Anonymous zaradio naziv „stroj mržnje na internetu“, drugi su pojedinci, uglavnom sa stranice „4chan“, koristili ime Anonymous te su povezali s njim klasičan prikaz ljudi bez glave u crnim odijelima. Prvo su koristili ime Anonymousa da trolaju a zatim da organiziraju ozbiljne ulične demonstracije. Trolanje protiv Scijentologije je započelo u siječnju 2008., započeto zloglasnim internetskim videom regrutacije Toma Cruisea hvaleći napore crkve da stvori nove i bolje stvarnosti. Video je procurio na Internet zbog kritičara crkve te je odmah postao viralan.

Scijentološka crkva je zaprijetila web izdavačima pravnim postupkom ako oni ne uklone video. To je Anonymous-u dalo dozu samopouzdanja te se napad na Scijentologiju i sa njihove strane smatra jednim od najlegendarnijih napada. Anonymous je pokrenuo DDoS napada na scijentološke web stranice, naručivao je neplaćene pizze na adrese crkve, lažirao slike golih dijelova tijela, nemilosrdno telefonski šalili crkvu, posebice telefonsku liniju gdje pozivatelji mogu dobiti savjete o „pravoj tehnologiji uma“. U roku od nekoliko tjedana je trolanje dalo rezultate, te je nastao projekt Chanology, politička kampanja protiv Scijentološke crkve, koja traje do danas.

Jedan od virusnih videa koji poziva na sustavno razbijanje scijentološke crkve je uzrokovao da dovoljan broj pojedinaca prosvjeduje u 127 gradova 10. veljače 2008. godine. Protestiralo je više od 7000 pojedinaca a mnogi od njih su nosili plastičnu masku Guy-a Fawkes-a kako bi sakrili svoj identitet. Od tog dana nadalje, ta maska je postala ikona potpisa Anonymousa. [30]

[29] Značenje trolanje. Riječnik.com. https://www.xn--rjenik-k2a.com/Trolanje (pristupljeno:03.04.2024.)
[30] Goode, L. (2015) Anonymous and the Political Ethos of Hacktivism, Popular Communication, 13 (1), 79.

U veljači 2010. godine pojedinci su koordinirali „Operaciju Titstorm“, DDoS napad na Australijsku vladu kao znak prosvjeda protiv zakona koji je sumjeren na suzbijanje pornografije. Anonymous je poslao e- poruku medijima u kojoj navode na nijedna vlada nema pravo uskratiti svojim građanima pristup informacijama samo zato što to smatraju neželjenim.

U ime Internet slobode, Anonymous se usredotočio na prosvjed protiv ACTA-e. (Trgovinski sporazum protiv krivotvorenja), ali legalnim putem (e-mail, telefonski pozivi, dostava neplaćene pizze). Grupa je na kraju uspjela privući znatan broj uličnih članova i simpatizera. Nadalje, uspostavljen je poslužitelj AnonOps u studenom 2010. godine.

Do 2011. godine, Anonymous je prepoznat kao nepokolebljiv i kontraverzan zagovarač za slobodu govora. Anonymous, potaknut blokadom tuniske vlade WikiLeaks, objavio je AnonOps video da pokreću OpTunisia. Tehnički tim hakera napalo je web stranice tuniske vlade i uništio softver koji je vlada koristila kao dio svog diktatorskog režima, kojim su špijunirali građane. [31]

Anonymous je ciljao na vladine web stranice zemalja Sjeverne Afrike i Arapskog poluotoka kao i Male Azije koje su se 2011. našle zahvaćene građanskim pobunama. Anonymous je upotrijebio svoja računala i znanje za podršku prosvjednicima na terenu, čije su vlade u mnogim slučajevima odlučile uskratiti im pristup društvenim mrežama ili internetu u cjelini.

Tijekom godina Anonymous je izvršio još napada te su do 2018., skoro pa u potpunosti smanjili svoj utjecaj no skupina se ponovno pojavila 2020. godine kako bi podržala prosvjede protiv policijske brutalnosti na George-a Floyd-a u Americi.

5.2. The Jester

Na dan 5. ožujka 2012. godine se dogodio jedan od neobičnijih napada u povijesti. Dogodio se na Twitteru ali neki ljudi tvrde da se nikada nije dogodilo. Haker koji je sebe prozvao The Jester je zamijenio svoju uobičajenu sliku na Twitteru sa QR kodom. Svatko tko je odlučio skenirati kod je upao u zamku. Naime, The Jester je objavio da je povukao sve podatke na mobilnim uređajima

[31] Goode L (2015) Anonymous and the Political Ethos of Hacktivism, Popular Communication, 13 (1), 82.

koji su skenirali njegov QR kod. Ako je informacija pripadala jednom od „loših momaka“ vjerojatno je poslana FBI-u. Problem je što se zapravo ne zna jeli se ovaj napad zapravo dogodio.[32]

The Jester je najpoznatiji primjer domoljubnog, proameričkog haktivizma. 2009. godine trupe američke vojske su se borile u Afganistanu. U prosincu 2009. godine talibani su napali prednju operativnu bazu Chapman te je to rezultiralo smrću 6 službenika CIA. Talibanska web stranica alemarah.info je oborena te odgovornost za to preuzima The Jester.

Njegov prvotni cilj bio je razvijanje alata koji bi pomogli u testiranju i očvršćivanju poslužitelja. Kada je postao svjestan da džihadisti koriste javne web stranice za skrivanje informacija, počeo ih je obarati. Srušio je nekoliko stranica za skupinu Westboro Baptist Church. Članovi crkve su prosvjedovali na vojničkim sprovodima držeći natpise poput „Bog mrzi pe****“.

Navodno su mnogi njegovi napadi bile samo učinkovite umne igre. Otkriveno je da je dugačak popis džihadističkih web stranica za koje je The Jester tvrdio da će ih srušiti zapravo samo stare web stranice čija je registracija domene istekla. [33]

5.3. LuLzSec

U svibnju 2011. godine Fox.com je bio na meti novonastale hakerske grupe pod imenom LulzSec. Grupa je otkrila slabost na stranici te je otkrila imena 73 000. američkih natjecatelja X Factora. Nadalje, napali su američki televizijski program gdje su podmetnuli lažnu priču da su pokojni reperi Tupac Shakur i Biggie Smalls zapravo živi i da žive na New Zelandu. Kasnije su napali Nintendo i Sonyjev PlayStation Network, ukrali su privatne podatke. Smatrali su sebe „piratima novijih dana“ te su sebe nazivali bogovima kada su napadali stranice. [34]

[32] Freed, A. M. & Levi, R. (2021). Malicious Life Podcast: The Jester - Hacktivist for Good. cyberreason. https://www.cybereason.com/blog/malicious-life-podcast-the-jester-hacktivist-for-good (preuzeto 15.04.2024.)
[33]Simmons, D. (2011). Jester: a powerful, prolific and patriotic hacker with balls. Mobility Digest. http://mobilitydigest.com/jester-a-powerful-prolific-and-patriotic-hacker-with-balls/ (preuzeto 25.04.2024.)
[34] Arthur, C. (2013). LulzSec: what they did, who they were and how they were caught. The Guardian. https://www.theguardian.com/technology/2013/may/16/lulzsec-hacking-fbi-jail (preuzeto 15.04.2024.)

Članovi grupe se nikada nisu sreli u pravom životu. Neki su bili u SAD-u a neki u Velikoj Britaniji, što ukazuje na to da je hakiranje postalo globalizirano.

Pad grupe je povezan s napadom na stranicu povezanu s FBI-em. Upadom na vladinu a ne komercijalnu stranicu, LulzSec dovodi na sebe pozornost federalnih vlasti u SAD-u. Zatim je Monsegur (jedan od članova) zaboravio prikriti svoju lokaciju korištenjem sustava Tor. FBI ga je uočio te su mu se agenti pojavili na vratima u domu na Manhattan-u. Ponuđen mu je izbor: da bude uhićen ili da surađuje. Monsegur je imao dvije nećakinje za koje je preuzeo roditeljsku skrb te nije htio da žive u domovima. Zbog toga je izabrao suradnju s FBI-em čime je sudbina njegovih nećakinja odlučila o sudbini LulzSec-a.

Eventualno su svi članovi LulzSeca bili uhićeni. [35]

5.4. WikiLeaks

WikiLeaks je medijska organizacija i web stranica koja je funkcionirala kao središte za razmjenu povjerljivih i povlaštenih informacija. Osnovao ju je prethodno spomenuti australijski računalni programer i aktivist Julian Assange.

WikiLeaks je prvi put privukao svjetsku pozornost 2007. godine kada je objavio priručnik za američke zatvorske čuvare u zaljevu Guantanamo. Svoj napredak je postigao 2010. godine kada je surađivao s The New York Timesom, The Guardianom, Der Spiegelom, Le Mondeom i El Paisom pri objavljivanju milijuna povjerljivih diplomatskih brzojava. Objavio je više od 10 milijuna procurjelih dokumenata i povezanih analiza, na užas političara, vlada i korporacija.

WikiLeaks je objavio stotine tisuća američkih vojnih dokumenata i videa iz afganistanskog i iračkog rata, uključujući takozvane snimke kolateralnog ubojstva.

2016. godine su objavili e-mailove američkih dužnosnika koji pokazuju da isti favoriziraju Hillary Clinton u odnosu na ljevičara Bernija Sandersa na predsjedničkim primarnim izvorima. WikiLeaks

[35] Pendergras, S. (2012). Hackers gone wild: the 2011 spring break of lulzsec. Issues In Information Systems, 13(1), 141.

je također optužen za otkrivanje identiteta homoseksualca u konzervativnoj zemlji Saudijskoj Arabiji, no grupa je odbacila te optužbe. [36]

Najgori skandal koji je pogodio WikiLeaks ima veze sa samim osnivačem Julianom Assanage-om. 2012. godine je zatvoren u ekvadorskom veleposlanstvu u Londonu kada je bio optužen sa silovanje u Švedskoj. Švedski tužitelji su odustali od istrage 2017. godine, ali J. Assanage je ostao u veleposlanstvu zbog straha da će ga SAD izručiti zbog otkrivanja državnih tajni.

5.5. Telecomix

Telecomix, slično kao i Anonymous, sami sebe opisuju kao decentralizirane „pojave“. Jedan od poznatijih projekata u koje je bio uključen Telecomix je ugradnja dial-up modema kako bi egipatskim građanima omogućili zaobilaženje interneta lokalne vlade. Slične aktivnosti provodili su i u Siriji. Pomogli su objaviti datoteke koje se odnose na sustave nadzora Američke tvrtke Blue Coat. Ovaj čin je prisilio Blue Coat da prizna da je njihove proizvode koristila sirijska vlada u svojoj represiji.

Telecomix je haktivistička skupina koja se više fokusira na obranu i obrazovanje nego ofenzivne strategije. Slijede potpuno decentraliziranu strukturu i zalažu se uglavnom za slobodu izražavanja i to nazivaju „datalove“. [37]

[36] Ludlow, P. (2010). WikiLeaks and Hacktivist Culture. The Nation. https://www.thenation.com/article/archive/wikileaks-and-hacktivist-culture/ (preuzeto 12.04.2024.)
[37] Chopitea, T.(2012). Threat Modelling of Hacktivist Groups Organization, Chain of Command, and Attack Methods, Chalmers University of Technology.

6. Upitnost etičnosti i moralnosti hakiranja

Izraz informacijska etika je uveden 1980-ih. Uveli su ga Koening i Hauptman, koji su potom krenuli u uspostavljanje „Časopisa za informacijsku etiku“ 1922. godine. Časopis je korišten kao opća oznaka za raspravu o pitanjima u vezi s povjerljivošću informacija. Uključene discipline na početku su bile knjižničarske i informacijske znanosti te studije poslovanja i upravljanja. Tek kasnije su im se pridružili studiji informacijskih tehnologija. [38]

Ovo poglavlje prikazuje debatu i pitanje u kojem kontekstu je etično i moralno hakirati, te postavlja pitanje je li cilj opravdava sredstva? U poglavlju se uspoređuju vlasnička prava u „realnom“ i digitalnom svijetu. Nadalje, daje argumente koji pokušavaju opravdati hakiranje kao način sprečavanja otpada, kao društvenu korist i slično. Na posljetku, hakiranje se pokušava opravdati kao vrsta građanskog neposluha.

6.1. Vlasnička prava u digitalnom okruženju

Na prvi pogled se može činiti očitim da je hakiranje pogrešno. Djelo hakiranja je zlonamjerno i pogrešno jer predstavljaju digitalni prijelaz na vlasništvo druge osobe. Smatra se da neovlašteni ulazak u tuđe računalo nije drugačiji od provale u nečiju kuću. Čin provale je moralno pogrešan, bez obzira na to jeli dovodi do štete, jer krši pravo vlasnika na kontroliranje vlastitog zemljišta i vlastite imovine. Slično tome, digitalni prijestup je pogrešan, bez obzira na to rezultira li štetom jer krši vlasničko pravo osobe da isključi druge osobe iz korištenja računala koje je kao i zemljište fizičko vlasništvo.

Postoje dva problema s ovim argumentom. Prvo, pod pretpostavkom da je hakiranje vrsta provale tj. neovlaštenog pristupa, svako hakiranje nije pogrešno jer nije svaki neovlašteni pristup pogrešan. Dopušteno je neovlašteno ući na tuđi posjed ako je to jedini način zarobljavanja zločinca koji bježi s mjesta zločina. Čin manje provale je moralno opravdan kao jedini način da se osigura veliko

[38] Himma, K. E. (2008). The Handbook of Information and Computer Ethics. 1st ed. New Jersey: WILEY, 102.

dobro zaustavljanja zločinca. Ako je hakiranje provala, onda je ono potrebno da se osigura neko dobro koje značajno nadmašuje uključeno zlo neovlaštenog pristupa.

Drugo, i možda još važnije, nije jasno jeli koncept neovlaštenog pristupa ispravan te odnosi li se na digitalne provale. Izraz „neovlašten pristup“ uglavnom je rezerviran za radnje u kojima jedna osoba ulazi u fizički prostor u vlasništvu druge. Hakiranje nije u doslovnom smislu ulazak u fizički prostor čiji je vlasnik druga osoba.

Unatoč tome, čini se jasnim da digitalne provale zadiru u interese korisnika računala. Čini se jasnim da neovlašteni upad u računalo zadire u imovinska prava žrtve. Netko tko dobije pristup nečijem računalu bez dopuštenja te osobe, prisvaja fizički objekt u kojem osoba ima legitimni imovinski interes.

Međutim, moralna prava nisu apsolutna. Ako je dopušten neovlašten ulaz na nečije zemljište s ciljem uhićenja zločinca u bijegu, tada pravo osobe na vlasništvo može biti nadjačano važnijim pravima. Vlasnička prava su slabija kada je nečiji život ugrožen. Unatoč tome na hakeru leži teret da ukaže da je određena provala moralno dopuštena. To će uključivati dokazivanje da će prava vlasništva ili privatnosti biti nadmašena interesima i ciljevima koje je moguće postići samo provalom. U mjeri u kojoj upad u računalo uključuje nanošenje štete na datoteke korisnika, upad može biti opravdan samo u mjeri u kojoj služi većim interesima. [39]

6.2. Društvene koristi računalnih provala

Hakeri ističu na računalne provale imaju niz društvenih prednosti. Dobivanjem uvida u rad postojećih mreža, hakeri razvijaju znanje koje se može koristiti za poboljšanje tih mreža. Same provale privlače pozornost na sigurnosne nedostatke koje mogu iskoristiti zlonamjerni hakeri ili, još gore, teroristi. To su dobrobiti koje doprinose javnom dobru i time su opravdane.

No ovaj argument „pada u vodu“. Sama činjenica da bi netko mogao učiniti puno društvenog dobra krađom, recimo, milijarde dolara od Billa Gatesa ne može opravdati krađu te svote ako Gates ima

[39] Delmas, C. (2018). Is Hacktivism the New Civil Disobedience? Raisons Politiques, 69(1), 63.

pravo vlasništva na sav taj novac. Smatra se da se postizanje neke društvene koristi može postići bez kršenja prava privatnosti.

6.3. Računalne provale kao način sprječavanja otpada

Hakeri opravdavaju računalne provale argumentom da koriste računalne resurse koji bi inače pošli u nepovrat, točnije u „otpad“. S tog gledišta, moralno je dopušteno učiniti sve što je potrebno kako bi se spriječilo da vrijedni resursi odu u nepovrat.

Ovaj argument pokušava identificirati moralno načelo koje bi moglo ograničiti druga prava, poput prava na vlasništvo. Ključno je napomenuti da su prava često ograničena određenim moralnim načelima. Na primjer, pravo na život je ograničeno moralnim načelom koje dopušta osobama da ubiju ako je to potrebno da iste osobe spase svoj život od određene prijetnje.

Ipak, ovaj argument također ne uspijeva opravdati hakiranje. Ako jedna osoba ima pravo vlasništva nad nekim objektom, nije u redu da taj objekt prisvoje druge osobe bez dopuštenja kako bi spriječile propast tog objekta. [40]

6.4. Računalne provale kao način ostvarivanja prava na slobodan protok sadržaja

Argument da računalne provale služe kao način ostvarivanja prava na slobodan protok sadržaja se temelji na ideji da moralno pravo na slobodno izražavanje podrazumijeva da ne bi trebalo biti ograničenja slobodnog protoka sadržaja. Naime, smatra se da informacije ili sadržaj općenito moraju biti besplatne.

[40] Delmas, C. (2018). Is Hacktivism the New Civil Disobedience? Raisons Politiques, 69(1), 66.

Ovaj argument također pokušava identificirati moralno načelo koje bi moglo ograničiti neka prava, štoviše, argument je utemeljen na navodno jačem pravu od privatnosti i vlasništva, a to je pravo na slobodno izražavanje.

Međutim, ovaj argument nije uspješniji od ostalih u opravdavanju hakiranja. Argument isključuje postojanje bilo kakvog drugog prava na privatnost informacija koje osobe imaju i razumno tu privatnost očekuju. Primjer prava na privatnost je medicinska dokumentacija. [41]

6.5. Opravdanost haktivizma kao građanskog neposluha

Odnedavno dolazi do novog opravdavanja hakiranja kao slobodnog izražavanja. Prema ovom argumentu, napadi na vladine stranice se mogu opravdati kao oblik građanskog neposluha. Budući da je građanski neposluh moralno opravdan kao protest protiv nepravde, dopušteno je počiniti računalnu provalu u znak protesta. U mjeri u kojoj je dopušteno organizirati protest protiv na primjer zakona koji krše ljudska prava, u istoj toj mjeri je dopušteno upadati u vladine mreže kako bi se bunilo protiv tog istog zakona. Dakle, računalne provale koje bi inače bile moralno neprihvatljive jesu moralno dopuštene ako su politički motivirane.

Ne računa se svaki digitalni aktivizam kao haktivizam ili građanski neposluh. Objavljivanje web stranice u Sjedinjenim Američkim Državama s peticijom za prekid rata u Iraku bi bio oblik digitalnog aktivizma, ali ne i haktivizma jer ne uključuje neovlašteni digitalni upad.

Pitanje jeli aktivizam opravdan oblik građanskog neposluha se rješava ovisno o slučaju. Neki haktivisti ne pokušavaju sakriti svoj identitet i prihvaćaju odgovornost, dok drugi identitet skrivaju kako bi izbjegli otkrivanje. Neka djela digitalnog upada ne uključuju značajnu štetu nedužnim trećim stranama (na primjer, rušenje vladine web stranice u znak prosvjeda protiv njene politike), dok druga djela to čine (na primjer, gašenje komercijalne web stranice DDoS napadima). Akti haktivizma koji ne utječu na nedužne treće strane imaju drugačiju „moralnu kvalitetu“ nego radnje koje štete nevinim trećim stranama.

[41] Levesque, M. (2006). Hacktivism: The How and Why of Activism for the Digital Age. The International Handbook of Virtual Learning Environments, 1206.

Kolika je šteta uzrokovana ovisi o tome jeli meta javna, privatna, jeli komercijalni ili nekomercijalni subjekt. Napadi na javne, čisto informativne stranice, obično uzrokuju manje štete nego napadi na privatne web stranice. Razlog tomu je taj da napadi na privatne web stranice mogu rezultirati značajnim poslovnim gubicima koji se mogu prenijeti na potrošače u obliku viših cijena ili na zaposlenike u oblik otkaza. [42]

Koliko štete je učinjeno također ovisi i o prirodi napada. Oštećenje web stranica čini se daleko manje vjerojatno da će prouzročiti značajnu štetu od napada koji uskraćuju pristup web stranici. Promjena „Ministarstvo pravosuđa“ u „Ministarstvo nepravde“ vjerojatno neće rezultirati značajnom štetom za interese trećih strana. U najgorem slučaju, samo će izazvati neugodnost i sramotu vladinoj agenciji koja vodi web stranicu.

To se, međutim, ne bi trebalo shvatiti kao sugeriranje da narušavanje web stranica ne uzrokuje značajnu štetu nevinim trećim stranama. Objavljivanje osjetljivih i privatnih informacija, poput broja socijalnog osiguranja, moglo bi dovesti do značajne štete za te pojedince.

Razumno je smatrati da će DoS i DDoS napadi vjerojatno prouzročiti puno veću štetu. Ove napade je puno teže opravdati kao moralnima. Doista, koordiniran i trajan DDoS napad na najveće komercijalne web stranice može rezultirati ekonomskim padom koji utječe na milijune ljudi.

Jedan važan čimbenik u procjeni djela građanskog neposluha je da su osobe koje su ga počinile spremne prihvatiti odgovornost za ta djela. Spremnost sudionika da prihvate osobnu odgovornost za ishod radnji nužan je uvjet za opravdanje čina građanskog neposluha. Da bi se hakiranje kvalificiralo kao čin građanskog neposluha, hakeri moraju biti jasno motivirani etičkim razlozima, moraju biti nenasilni i biti spremni prihvatiti posljedice svojih djela. [43]

Postoji razlika između preuzimanja odgovornosti za djelo i spremnosti na prihvaćanje pravnih posljedica toga čina. Odgovornost se može preuzeti i bez prihvaćanja posljedica. Način na koji se to može napraviti je korištenjem neke vrste pseudonima umjesto pravog imena ili pripisivanjem djela skupini koja štiti imena svojih članova. Haktivisti obično pokušavaju sakriti svoj identitet kako bi izbjegli kazneni progon- čak i kada preuzimaju odgovornost.

[42] Himma, K. E. (2008). The Handbook of Information and Computer Ethics. 1st ed. New Jersey: WILEY, 192.

Mnogi haktiviste poistovjećuju s teroristima. Teroristi obično preuzimaju odgovornost kao skupine, ali pokušavaju izbjeći posljedice svojih postupaka prikrivanjem svoga identiteta i lokacije. Naravno, ova sličnost s haktivistima je neusporediva: teroristi namjerno pokušavaju nanijeti tešku i nepovratnu štetu nevinim ljudima dok haktivisti ne. Poanta je ilustrirati da postoji moralno značajna razlika između traženja i prihvaćanja odgovornosti. [44]

Sljedeći čimbenik koji je potrebno uzeti u obzir je motivacijski program iza elektroničkog oblika građanskog neposluha nije toliko transparentan kao motivacijski program iza klasičnog oblika građanskog neposluha. Dok su prosvjednici koji su zatvorili državnu autocestu Washington nosili natpise i upozorili tisak da su prosvjedovali zbog nezadovoljstva određenom mjerom, poanta nekih navodnih djela haktivista nije jasna. DDoS napad usmjeren protiv Amazon.com-a može značiti mnogo stvari, a neke nemaju veze sa izražavanjem političkog stajališta. Izostanak jasne poruke je problematičan s moralnog stajališta.

Djela haktivizma često su motivirana prosvjedom protiv kršenja ljudskih prava od strane opresivnih nedemokratskih režima i usmjereni su na vladine poslužitelje u vlasništvu vladinih tijela u tim režimima. Bitno je napomenuti da se mnoga takva djela neće računati kao oblik građanskog neposluha. Razlog tome je da mnogi od ovih napada dolaze od strane osoba koje žive izvan represivnog režima i ne podliježu pravnim posljedicama unutar režima. Naravno u ovakvim slučajevima, prihvaćanje odgovornosti nije potrebo da bi čin hakiranja bio moralno opravdan. Sukladno tome, takvi napadi, koji potječu izvan granica tih država, mogu biti opravdani kao haktivizam ali ne i kao oblik građanskog neposluha.

Primarni učinak napada na takve stranice i na takve režime je skretanje pozornosti na kršenje ljudskih prava u tim državama. Narušavanje vladine web stranice koja ne pruža osnovne usluge ili informacije vjerojatno neće imati značajnijeg utjecaja na nevine građane. Nadalje, ti ciljani režimi ne poštuju pravo na slobodu izražavanja. Puno je teže „obaviti čin“ građanskog neposluha i iskazati nezadovoljstvo i neslaganje bez straha od odmazde. Zbog toga su djela haktivizma često uspješna u skretanju pozornosti na nepravdu i u poticanju rasprave.

Kenneth Einar Himma i Herman T. Tavani navode „Općenito gledajući, haktivisti nisu učinili ono što bi trebali kako bi bili sigurni da njihova djela nisu problematična s moralnog stajališta. U svojoj

[44] Levesque, M. (2006). Hacktivism: The How and Why of Activism for the Digital Age. The International Handbook of Virtual Learning Environments, 1210.

revnosti da unaprijede svoje moralne ciljeve, počinili su djela koja se čine problematičnijima s moralnog gledišta. Ako su glavni mediji i teoretičari pogrešno shvatili haktiviste, oni mogu kriviti samo sebe.“[45]

[45] Himma, K. E. (2008). The Handbook of Information and Computer Ethics. 1st ed. New Jersey: WILEY, 216.

7. Prijedlozi zakona koji utječu na haktiviste

Prijetnja koju predstavljaju hakeri nije ostala nezapažena među zakonodavcima. Naime, razne nacije su primijetile bitnost ovog problema te su donijele zakone koji zabranjuju hakiranje i sve ostale oblike kibernetičkog kriminala. Na primjer, Vijeće iz 2001. godine, Europska konvencija o kibernetičkom kriminalu je uspostavila okvir za domaće pravne režime. Propisani režimi su opći i moguće ih je primijeniti na oblike haktivizma koji nalikuju tradicionalnim oblicima prosvjeda. Pravni sustavi u Sjedinjenim Američkim državama i Ujedinjenom Kraljevstvu imaju dugo utvrđena načela koja štite slobodu izražavanja. U kontekstu haktivizma kao oblika prosvjeda, ta se načela mogu koristiti za zaštitu uske podskupine haktivizma od opće zabrane hakiranja.

Cilj zakonodavaca je doći do ravnoteže između zaštite ljudskih prava kao što je sloboda izražavanja i suzbijanja kibernetičkog kriminala.

A. Europska konvencija o kibernetičkom kriminalu

Sastavljači konvencije su smatrali ključnim međunarodnu suradnju da bi regulacija kibernetičkog kriminala bila učinkovita. Zbog toga potpisuje zajedničku kaznenu politiku u vezi s kibernetičkim kriminalom a stranke potpisnice su obvezujuće uspostaviti domaće kaznene zakone.

Članak 2. Konvencije zahtijeva reguliranje nezakonitog pristupa računalnim sustavima. Stranke imaju obvezu donijeti kaznene zakone koji zabranjuju pristup računalnog sustava bez prava. Članak nadalje precizira da se takav pristup može dobiti ili zaobilaženjem sigurnosnih mjera ili iskorištavanjem ovlaštenog pristupa te zahtijeva da uspostave kaznene zakone zabrane namjernog, neovlaštenog presretanja računalnih podataka.

B. SOPA- Stop Online Piracy Act

Značajan broj osoba je čuo a i koristio web stranice na kojima je moguće besplatno gledati televizijske emisije, preuzeti filmove i skinuti albume. Iako su takve aktivnosti očito kršenje zakona o autorskim pravima, prolaze bez kontrole zbog njihove enormne količine. SOPA je prijedlog zakona koji ima za cilj suzbijanje kršenja autorskih prava i ograničenje krađe intelektualnog vlasništva ograničavanjem pristupa stranicama koje omogućuju trgovinu piratskim sadržajem. Cilj SOPA-e je prekinuti dotok piratskim stranicama zahtijevajući od američkih tražilica i drugih

pružatelja da uskrate svoje usluge. To znači da određene stranice, poput Googlea, ne bi mogle prikazivati određene stranice a procesori plaćanja, poput Ebay-a i PayPal-a ne bi mogle omogućiti prijenos sredstava.

SOPA je opsežan i detaljan zakon s preko sedamdeset stranica odredbi koje ciljaju na različita pitanja koja utječu na neovlašteno korištenje materijala zaštićenog autorskim pravom. SOPA navodi da je njezin cilj „promicati prosperitet, kreativnost, poduzetništvo i inovacije borbom protiv krađe američke imovine."

Iako su zakonodavci imali dobre namjere u predlaganju ovog zakona, smatra se da SOPA ima štetne posljedice. Protivnici navode da je način na koji je SOPA napisan promiče cenzuru i prepun je potencijala za neželjene posljedice. Pristaše zakona odbacuju optužbe o cenzuri, govoreći da je svrha zakona obnoviti pokvareni sustav koji ne sprječava adekvatno kriminalno ponašanje.

Enorman broj web stranica se udružio u znak protesta protiv prijedloga zakona. Uveli su potpuno zatamnjenje svojih web stranica na dvadeset i četiri sata kako bi pokazali potencijalni negativni učinak zakona. Neke od stranica koje su zauzele stav protiv zakona su Facebook, Google i E-Bay, no čak je i Wikipedia, jedna od najneutralnijih stranica, zauzela isti stav te se priključila zatamnjenju web stranice. Wikipedia je navela za donošenje zakona da „bi bilo razarajuće za slobodni i otvoreni web". [46]

C. ACTA- The Anti- Counterfeiting Trade Agreement

Acta je trgovinski sporazum protiv krivotvorenja. Ima za cilj stvoriti međunarodne standarde za provedbu prava intelektualnog vlasništva. Mnogi Europljani kao i Amerikanci, ali u manjoj mjeri, se protive tom sporazumu jer se izravno ne bavi niti zaustavlja piratstvo na smislen način. Osim toga, većina vladinih dužnosnika je potpisala sporazum u tajnosti, bez javnog inputa.

Glavni pružatelji internetskih usluga posebno su bili zabrinuti zbog svoje potencijalne odgovornosti prema zakonu. Određeni pružatelji usluga bili su toliko zabrinuti da je 18. siječnja 2012. bio dan koordinirane akcije tisuća web stranica, uključujući Wikipediju i Reddit, koje su postale nedostupne, prikazujući samo crnu pozadinu i tekst koji opisuje potencijalni učinak zakona. Google je također cenzurirao svoj logo u znak protesta

[46] Pratyusha, C, (2013). An Analysis of the Stop Online Piracy Act. Law School Student Scholarship, 16.

Online aktivisti koordinirali su izvan mrežnu akciju, okupivši 15 000 prosvjednika u Krakowu i 5 000 u Wroclawu, te su povećali medijsku pozornost u ostatku Europe.[47]

Anonymous je napao nekoliko službenih web stranica američke vlade u znak protesta protiv ACTA-e. Anonymous navodi da ako ACTA-u potpišu sve zemlje sudionice, da će doći do rata koji će pljusnuti paklenu vatru na sve neprijatelje slobode govora, privatnosti i internetske slobode. Također navode da će izbaciti sve zle korporacije i vlade s „njihovog interneta". [48]

D. CISPA- Cyber Intelligence Sharing and Protection Act

„Tim se zakonskim prijedlogom ispunjava zahtjev privatnog sektora za dobivanje informacija kojima raspolažu državne obavještajne službe. Određuje se da će direktor obavještajne službe donijeti procedure u skladu s kojima će informacije o cyber prijetnjama kojima raspolaže obavještajna zajednica biti podijeljene s ovlaštenim osobama u privatnim kompanijama, a u skladu s potrebama nacionalne sigurnosti. Isto tako striktno se određuju uvjeti pod kojima informacije koje entiteti privatnog sektora razmijene s državnim agencijama mogu biti proslijeđene drugim vladinim službama, što znači da informacije mogu biti podijeljene s drugima samo uz ograničenja koja je odredila privatna kompanija koja ih je dala. Informacije ne smiju biti iskorištene za stjecanje nepoštene prednosti na tržištu. Izričito je navedeno da tako podijeljene informacije vlada ne može upotrijebiti za regulativne svrhe niti one mogu biti proslijeđene drugim državnim tijelima ako se privatni entitet od kojega je informacija potekla s tim ne složi. Vlada se obvezuje da te informacije neće koristiti za druge svrhe osim za svrhe cyber sigurnosti i nacionalne sigurnosti SAD-a."[49]

CISPA bi omogućila dobrovoljnu razmjenu informacija između privatnih tvrtki i vlade u slučaju kibernetičkog napada. Podržavatelji tvrde da je CISPA neophodna za zaštitu SAD-a od cyber napada iz zemalja poput Kine i Irana. Protivnici smatraju da to omogućuje tvrtkama da jednostavno predaju privatne podatke korisnika vladi zahvaljujući klauzuli o odgovornosti. Prijedlog zakona je potaknuo ogromnu količinu masovnog aktivizma jer zakon stvara rupu u svim već poznatim zakonima o privatnosti te daje imunitet tvrtkama da dijele privatne podatke.

[47] Farrad, B. (2015). Lobbying and Lawmaking in the European Union: The Development of Copyright Law and the Rejection of the Anti–Counterfeiting Trade Agreement. Oxford Journal of Legal Studies 35(3), 496.
[48] Cheredar, T. (2012). Anonymous says ACTA must be killed with fire, hacks U.S. government websites. VentureBeat. https://venturebeat.com/media/anonymous-acta-gov-websites-hack/ (pristupljeno: 19.04.2024.)
[49] Kovačević, B. (2014). Američko Javno-privatno Partnerstvo I Cyber Sigurnost. Politička Misao, 50(3), 6.

Hakerska skupina Anonymous zatražila je od web stranica da zacrne svoje naslovnice u znak protesta protiv zakona u SAD-u koji bi omogućio internetskim tvrtkama i vladinim agencijama da lakše dijele osobne podatke.

Zaključak

Haktivizam je složena pojava koja je dokazala da se kibernetički prostor počinje spajati s onim iz pravog života i da prosvjedi prelaze klasične državne granice. Kroz povijest nam je pokazano kako haktivisti djeluju i koliko zapravo mogu pomoći pri ukazivanju na neki cilj ili ideju. Iako mnogi haktiviste utrpavaju u isti koš kao i klasične hakere, nemoguće je ignorirati borbe koje su oni dobili a tiču se sigurnosti i privatnosti svih nas, korisnika interneta. Zakoni pokušajem cenzure slobode govora i privatnosti ugnjetavaju sav narod koji ima pravo na njih a haktivisti su oni koji čine nešto povodom toga. Zato se mnoge nacije pokušavaju riješiti haktivista, jer osim što traže sigurnost i privatnost, također otkrivaju državne tajne. Ipak, postoji podjela u percepciji haktivista. Iako haktivisti najčešće imaju dobar cilj, stvara se debata oko toga jeli njihov način etičan i moralan. Smatra da se s moralnog gledišta, haktivisti u više slučajeva rade pogrešku te da se njihova djela ne mogu opravdati. Mišljena su podijeljena: mnogi teoretičari smatraju da su haktivisti neshvaćeni heroji koji se bore za prava i slobode, dok ostali smatraju da su haktivisti zločinci koji imaju dobru ideju. No, kriminalno djelo je još uvijek kriminalno djelo. Iako mnogi haktivisti imaju ciljeve koji su dobre naravni, na primjer sloboda govora ili ljudska prava, postupci kojima se oni služe mogu biti neopravdani i mogu imati negativne posljedice.

Konačno, haktivizam će se nastaviti mijenjati i razvijati te je potrebno još više razmotriti i proučavati moralne, etičke i pravne aspekte ove pojave. Haktivisti se suočavaju sa izazovom koji postavlja pitanje kako postići ravnotežu između borbe protiv nepravde i poštivanja zakona i etičkih normi.

Istraživačka pitanja ovog završnog rada su dokazana.

1. Kako se haktivizam razlikuje od tradicionalnih oblika aktivizma?

Haktivizam koristi tehnološke i kompjuterske alate za provođenje svojih akcija dok se kod tradicionalnog aktivizma koriste drukčije metode. Haktivizam uglavnom djeluje u online okruženju i to anonimno dok tradicinalni aktivisti koriste javne prostore za širenje svojih poruka. Nadalje, haktivizam je problematičniji oblik aktivizma jer mnoge haktivističke akcije uključuju ilegalne radnje. Etika tradicionalng aktivizma je prihvaćenija kao legitimna forma izražavanja.

2. Koje su etičke dileme i moralni izazovi s kojima se suočavaju haktivisti?

Prva dilema s kojom se haktivisti suočavaju je legitimnost ciljeva prema nezakonitosti korištenih metoda. Iako mnogi imaju plemenite ciljeve, metode kojima se koriste su najčešće nezakonite. Sljedeća dilema postavlja pitanje jeli cilj opravdava sredstva? Dolazi do izazova gdje je potrebno procijeniti jesu li određene štetne metode opravdane ako će se njima doći do pozitivnog ishoda.

3. Kako se vlasti i korporacije odnose prema haktivizmu?

Vlasti i korporacije najčešće haktiviste tretiraju kao kriminalce te njihove akcije kao kriminalna djela. Zbog toga se pokušavaju uvesti mnogi zakoni i prijedlozi zakona kojima bi se rad haktivista ograničio. Problem dolazi kada se tim zakonima i ostalim osobama uklanjaju prava na govor i slobodan protok informacija.

4. Kako se haktivisti bore protiv cenzure i ograničavanja slobode govora na internetu?

Haktivisti se koriste raznim metodama kako bi se izborili protiv cenzure i za svoja prava. Haktivisti često objavljuju informacije u javnost čime potiču javnu svijest i stvaraju pritisak na institucije. Provode razne cyber napade kao što su na primjer DDoS napadi. Neki haktivisti koriste i kreativnije strategije kao što su stvaranje parodija i memova. Kombiniranjem ovih strategija, haktivisti se bore za slobodu govora i izražavanja na internetu te se suprotstavljaju vladama i korporacijama koje pokušavaju kontrolirati i cenzurirati digitalni prostor.

Bibliografija

1. Anderson, P. D. (2020). Privacy for the weak, transparency for the powerful: the cypherpunk ethics of Julian Assange. Ethics and Information Technology.

2. Arnell, P., & Reid, A. (2009). Hackers beware: the cautionary story of Gary McKinnon. Information & Communications Technology Law, 18(1), 1–12.

3. Arthur, C. (2013). LulzSec: what they did, who they were and how they were caught. The Guardian. https://www.theguardian.com/technology/2013/may/16/lulzsec-hacking-fbi-jail (preuzeto 15.04.2024.)

4. Black hat, White hat, and Gray hat hackers – Definition and Explanation. Kaspersky, https://www.kaspersky.com/resource-center/definitions/hacker-hat-types (preuzeto 02.04.2024.)

5. Bradbury, D. (2011). The World's Dumbest Hackers. Infosecurity, 8(2), 16–19.

6. Brief Historical Background to the Zapatista Movement. Hemispheric Institute. https://hemisphericinstitute.org/en/su10-tourism/item/879-su10-brief-historical-background-zapatista-movement.html (preuzeto 12.04.2024.)

7. Brooks, E. (2023). What Is Activism: Definition, Types, Role, Examples, Importance, LIBERTIES, Creative Commons, https://www.liberties.eu/en/stories/activism/44871 (preuzeto 3.4.2024.)

8. Cheredar, T. (2012). Anonymous says ACTA must be killed with fire, hacks U.S. government websites. VentureBeat. https://venturebeat.com/media/anonymous-acta-gov-websites-hack/ (preuzeto 19.04.2024.)

9. Chopitea, T. (2012). Threat Modelling of Hacktivist Groups: Organization, Chain of Command, and Attack Methods. Master of Science Thesis in Secure and Dependable Computer Systems. Chalmers University of Technology. Göteborg, Sweden.

10. Deshmukh, R. V., & Devadkar, K. K. (2015). Understanding DDoS Attack & its Effect in Cloud Environment. Procedia Computer Science, 49, 202–210

11. Delmas, C. (2018). Is Hacktivism the New Civil Disobedience? Raisons Politiques, 69(1), 63-81

12. Devitt, M. (2001). A brief history of computer hacking. // Dynamic Chiropractic 19, 13. https://www.dynamicchiropractic.com/mpacms/dc/article.php?id=18078 (preuzeto 04.03.2024.)

13. Farrad, B. (2015). Lobbying and Lawmaking in the European Union: The Development of Copyright Law and the Rejection of the Anti–Counterfeiting Trade Agreement. Oxford Journal of Legal Studies 35(3) 487-514.

14. Fox, J. (2021). Top 10 famous hackers, https://www.cobalt.io/blog/top-ten-famous-hackers (preuzeto 30.05.2024.)

15. Freed, A. M., & Levi, R. (2021). Malicious Life Podcast: The Jester - Hacktivist for Good. cyberreason. https://www.cybereason.com/blog/malicious-life-podcast-the-jester-hacktivist-for-good (preuzeto 15.04.2024.)

16. Goode, L (2015) Anonymous and the Political Ethos of Hacktivism, Popular Communication, 13 (1), 74-86.

17. Griffiths, C. (2022). The Latest 2022 Cyber Crime Statistics (updated November 2022). AAG. https://aag-it.com/the-latest-2022-cyber-crime-statistics/ (preuzeto 29.03.2024.)

18. Hampson, N.C.N. (2012). Hacktivism: A New Breed of Protest in a Networked World, Boston College International and Comparative Law Review, 35(2), 511-542.

19. Himma, K. E. (2008). The Handbook of Information and Computer Ethics. 1st ed. New Jersey: WILEY.

20. Jordan, T. (2016). A genealogy of hacking. Convergence: The International Journal of Research into New Media Technologies, 23(5), 528–544.

21. Kovačević, B. (2014). Američko Javno-privatno Partnerstvo I Cyber Sigurnost. Politička Misao 50(3).

22. Levesque, M. (2006). Hacktivism: The How and Why of Activism for the Digital Age. The International Handbook of Virtual Learning Environments, 1203-1214

23. Lu, Y., Luo, X., Polgar, M., & Cao, Y. (2010). Social Network Analysis of a Criminal Hacker Community. Journal of Computer Information Systems, 51(2), 31–41.

24. Ludlow, P. (2010). WikiLeaks and Hacktivist Culture. The Nation. https://www.thenation.com/article/archive/wikileaks-and-hacktivist-culture/ (preuzeto 12.04.2024.)

25. Martini, M. (2017). Mourning for a hacktivist: grieving the death of Aaron Swartz on a digital memorial. Media, Culture & Society, 40(2), 228–245.

26. Pendergras, S. (2012). Hackers gone wild: the 2011 spring break of lulzsec. Issues In Information Systems, 13(1), 133-143.

27. Phillips, P. J. & Pohl, G, (2022). The Economics of Information and Human Factors in Cybersecurity. SSRN Electronic Journal.

28. Pogrebna, G., & Skilton, M. (2019). A Sneak Peek into the Motivation of a Cybercriminal. Navigating New Cyber Risks, 31–54.

29. Prasad Tulasi, S. (2014.). Ethical Hacking and Types of Hackers, International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE), 11(2), 24-27.

30. Pratyusha, C. (2013). An Analysis of the Stop Online Piracy Act. Law School Student Scholarship.

31. Richterich, A. & Wenz, K. (2017). Introduction. Making and Hacking. Digital Culture & Society, 3(1), 5–22.

32. Scijentologija – što je to? Podarilove. https://podarilove.ru/hr/saentologiya-chto-eto-cerkov-saentologii-saentologiya-sekta-saentologiya-v-rossii-izvestnye-lyud/ (preuzeto 12.04.2024.)

33. Simmons, D. (2011). Jester: a powerful, prolific and patriotic hacker with balls. Mobility Digest. http://mobilitydigest.com/jester-a-powerful-prolific-and-patriotic-hacker-with-balls/ (preuzeto 25.04.2024.)

34. Sukhai, N. (2004). Hacking and cybercrime. In Proceedings of the 1st annual conference on Information security curriculum development (InfoSecCD '04). Association for Computing Machinery, New York, NY, USA, 128–132.

35. U.S. Department of Justice. US.GOV. https://www.usa.gov/federal-agencies/u-s-department-of-justice (preuzeto 29.03.2024.)

36. Virtual Sit-In. techopedia. https://www.techopedia.com/definition/29626/virtual-sit-in (preuzeto 03.04.2024.)

37. White Hat Hackers: The Good, the Bad, or the Ugly? Kaspersky, https://www.kaspersky.com/resource-center/definitions/white-hat-hackers (preuzeto 02.04.2024.)

38. What is a Black-Hat hacker? Kaspersky, https://www.kaspersky.com/resource-center/threats/black-hat-hacker (preuzeto 02.04.2024)

39. What is a denial of service attack (DoS) ? Paloalto Networks. https://www.paloaltonetworks.com/cyberpedia/what-is-a-denial-of-service-attack-dos (preuzeto 15.04.2024.)

40. Značenje trolanje. Riječnik.com. https://www.xn--rjenik-k2a.com/Trolanje (preuzeto 03.04.2024.)