UNIVERZA V LJUBLJANI
FAKULTETA ZA DRUŽBENE VEDE

Nenad Kojić

Hektivizem kot grožnja človekovi varnosti

Diplomsko delo

Ljubljana, 2015

UNIVERZA V LJUBLJANI
FAKULTETA ZA DRUŽBENE VEDE

Nenad Kojić
Mentor: izr. prof. dr. Uroš Svete

Hektivizem kot grožnja človekovi varnosti

Diplomsko delo

Ljubljana, 2015

ZAHVALA

Iskrena hvala družini za izkazano brezpogojno ljubezen ter moralno in materialno podporo skozi vsa študijska leta. Posebna zahvalo zaslužita tudi babica Marija in dedek Dmitrije. Bližnjim prijateljem in prijateljicam pa hvala za vso izkazano razumevanje.

Mentorju dr. Urošu Svetetu se zahvaljujem za strokovne nasvete in usmeritve ter za prijaznost in potrpljenje. Hvala dr. Nataši Logar, ki mi je s svojimi nasveti pomagala pri izbiri ustrezne terminologije.

Zahvaljujem se tudi Mojci, najprijaznejši teti na svetu, prijateljici, ki jo vedno iskreno zanima kaj počnem in ki je bila takoj pripravljena lektorirati mojo nalogo.

Hektivizem kot grožnja človekovi varnosti

V času pred razmahom informacijske tehnologije je bilo posameznikovo življenje popolnoma neodvisno od digitalne sfere. Posameznik je vstopal v interakcijo z informacijsko tehnologijo izključno na lastno iniciativo, nenadni tehnološki in družbeni razvoj pa je v zadnjih nekaj letih povzročil nepredvidljivi razmah informacijske tehnologije v vse sfere posameznikovega življenja. Danes živimo v resničnosti sodobne informacijske družbe, ki bi se še pred dvema desetletjema zdela kot delo znanstvene fantastike. Posameznikovi vsakodnevni opravki, služba, prosti čas, zdravje, finance in celo zasebnost so področja življenja, ki so postala neločljivo prepletena z informacijsko tehnologijo in so vsaj deloma prenesena v digitalni svet. Zaradi velike prepletenosti obeh svetov lahko dejanja v digitalnem svetu močno odmevajo v resničnost. Hektivizem je ena izmed oblik digitalne dejavnosti, ki izkorišča opisane lastnosti sodobne družbe, da bi s pomočjo informacijske tehnologije povzročila spremembe v resničnosti. Zaradi vedno hitrejšega razvoja tehnologije in pospešene infiltracije le-te v življenje posameznika fenomen hektivizma nujno potrebuje razlago in oceno potenciala ogrožanja človekove varnosti.

Ključne besede: človekova varnost, digitalno, heker, hektivizem, informacijska družba, informacijska tehnologija.

Hacktivism as a threat to personal security

In times before the proliferatoion of information technology, lives of individuals were completely independent from the digital sphere. The individual has interacted with information technology only by his own initiative. However, a sudden technological and societal progress of the last few years, has caused information technology to become inextricable part of individual's life. Today we live in a modern technological society, that would only a few decades ago, seem as a work of science fiction. Individual's everyday chores, job, free time, health, finances and even his private life are all segments of life unseparabely connected with the information technology and, at least in part, transferred to the digital world. As a consequence of such interconnectedness, the actions performed in digital can have profoundly echoe into reality. Hacktivism is one form of a digital activity, that exploits said properties of modern society to cause real life consequences with the use of information technology. Due to the rapid development and accelerated infilitration of technology in the individual's lifes, the phenomenon of hacktivism is in urgent need of an interpretation and assessment of it's potential to threaten personal security.

Key words: personal security, digital, hacker, hacktivism, information society, information technology.

KAZALO

1 UVOD

Informacijska revolucija je ustvarila pogoje za novo vrsto družbe, ki jo oblikuje informacijska tehnologija. Eden izmed temeljev te družbe, tj. internet, šteje že čez 40 let, svetovni splet pa jih bo čez dve leti dopolnil 25 (The Observer 2013). S pomočjo informacijske tehnologije postajajo vsakdanje, v preteklosti popolnoma »analogne«, aktivnosti, in sicer od potrošnje do socialnih interakcij, stvar digitaliziranega sveta. Vedno večji del svojih življenj preživljamo v tem vzporednem svetu (Li 2013, 302), ki ga s povezovanjem v veliko svetovno medmrežje, ki presega državne meje, omogoča informacijska tehnologija. Ko le-ta pridobiva na pomenu, dejanja z medmrežja vedno močneje odmevajo v vsakdanjem življenju posameznikov in družbe kot celote.

V skladu s temi spremembami se je v spletnem okolju pojavila nova oblika digitalne dejavnosti – hektivizem. Čeprav si zaenkrat nismo enotni, kaj točno omenjeni pojem zaobjema, ga najširše in najpreprosteje lahko razumemo kot uporabo informacijske tehnologije za doseganje politične ali družbene spremembe (Li 2013, 302).

Ker se zavedamo vpliva informacijske tehnologije na naša vsakdanja življenja in ker vemo, da je le-to možno zlonamerno izkoristiti, z njo posameznike oškodovati in celo poškodovati, ter nismo prepričani, kaj hektivizem sploh pomeni, se moramo vprašati, kdo so hektivisti, na kakšen način uporabljajo informacijsko tehnologijo, kakšne spremembe želijo doseči in kako to vpliva na posameznika. Zgornje zavedanje in vprašanja, ki mu sledijo, bodo osrednja tema diplomske naloge. V nalogi bomo namreč ugotavljali, ali hektivistična dejavnost ogroža človekovo varnost.

Opozoriti moramo, da se v nalogi ne bomo posebno ukvarjali z raznolikostjo in s širino konceptov varnosti (od državne oz. nacionalne varnosti, družbene varnosti do globalne varnosti ipd.). Najprej bomo predstavili definicijo hektivizma in potem ugotovili, če je hektivistična dejavnost sploh sposobna ogroziti varnost posameznika oz. njegovega najtesnejšega. Če bo na koncu odgovor na zastavljeno vprašanje pritrdilen, se bodo z različnimi koncepti varnosti lahko ukvarjala prihodnja dela.

Naslednje področje, s katerimi se bodo podrobneje morala ukvarjati prihodnja dela, so pravni vidiki in kršenje zapisanih zakonov. Digitalno pravo in pravne posledice dejanj v digitalnem svetu so preobširna tema, da bi se je lotili v okviru te naloge in zagotovo zahteva samostojno delo. Težave nastopijo že pri osnovah, na primer pri neenotnosti zakonodaje in vprašanju pristojnosti. Digitalni svet je obsežen in presega državne meje. Povsem običajni in vsakdanji

primeri postanejo izredno problematični, ker se lahko zakoni, ki urejajo določena področja, od države do države bistveno razlikujejo. Zaradi tega je izjemno zapleteno že načrtovanje širše svetovne zakonodaje, kaj šele njeno morebitno oblikovanje ali celo uveljavljanje (Slobbe in Verberkt 2012). Namesto podrobne analize zelo raznolikih zapisanih zakonov se bomo v nalogi posvetili opravičljivosti dejanj in poizkusili vzpostaviti zadovoljiv kriterij legitimnosti, ki ga bo možno univerzalno aplicirati na vsak primer.

2 METODOLOŠKI OKVIR

2.1 Predmet in cilj preučevanja

Predmet preučevanja bo hektivizem in uporaba sodobne informacijske tehnologije ter njegov potencialni vpliv na posameznikovo varnost. Kljub velikemu medijskemu senzacionalizmu ob poročanju o hektivizmu in podzavestno zakoreninjenem strahu pred obrobno in z računalniki povezano subkulturo ob predhodnem preučevanju literature nismo zaznali večjih nasprotij med hektivizmom in človekovo varnostjo. V skladu s temi ugotovitvami bo tudi naša hipoteza, postavljena v nadaljevanju.

Za preverjanje hipoteze bomo najprej razjasnili pojem posameznikove varnosti, potem pa bomo ob preučevanju hektivizma predstavili začetke sodobne informacijske družbe in informacijsko revolucijo, s katero je povezan pojav fenomena hektivizma. Če namreč ne razumemo teh začetkov in samega izvora, se ne moremo kompetentno ukvarjati s preučevanjem le-tega. Nadaljevali bomo z njegovim razvojem in v nadaljevanju na podlagi analize prelomnejših dogodkov, označenih za hektivizem, dokončno potrdili ali zavrgli našo hipotezo.

Ciljev preučevanja bo več. Prvi bo natančna definicija hektivizma, ki trenutno manjka in jo nujno potrebujemo za nadaljnje delo. Naslednji cilj bo pregled zgodovine hektivizma, od samih začetkov do danes, in bo služil kot osnova za analizo primerov. Tretji cilj bo analiza treh primerov za preverjanje hipotez. Končni cilj pa je zaključek, v katerem bomo potrdili ali ovrgli hipotezo in dodali komentar.

2.2 Hipoteza

Hipoteza: Hektivizem ne predstavlja grožnje človekovi varnosti.

2.3 Metode preučevanja

Pri pisanju diplomske naloge smo uporabili metodo analize ter interpretacije sekundarnih pisnih in elektronskih virov, monografskih publikacij, člankov, poročil ipd. Uporabili smo metode zgodovinske analize izbranega področja, deskriptivno metodo za razlago in opis različnih konceptov ter nazadnje še študije primerov, s katerimi smo nalogo povezali v celoto in ugotavljali veljavnost hipoteze.

2.4 Pojmi

Informacijska družba: Informacijska družba je nastala skozi informacijsko revolucijo, katere glavna elementa sta mikroelektronika, ki je revolucijo omogočila, in digitalizacija kot

najpomembnejša osnova informacijske družbe. Mikroelektronika je omogočila razvoj tehnologij za prenos podatkov, ki so ključno vplivale na komuniciranje – uporaba interneta je tista, ki narekuje dinamiko sodobne informacijske družbe in ima največje družbene implikacije. Skozi uporabo interneta je informacijska družba povezana v svetovni splet, je interaktivna, kar pomeni, da vsak udeleženec v elektronski mreži ni zgolj potrošnik, temveč tudi potencialni proizvajalec informacij (Svete 2005, 16–20).

Informacijska družba je družba, za katero je značilna visoka stopnja informacijske intenzivnosti v vsakodnevnem življenju večine posameznikov, v večini organizacij in na delovnem mestu, in sicer skozi uporabo splošne in združljive tehnologije za širok niz osebnih, družbenih, izobraževalnih in poslovnih dejavnosti ter s sposobnostjo posredovanja, sprejemanja in izmenjave digitalnih podatkov med prostori, in sicer hitro in neodvisno od razdalje (IBM Community Developement Foundation 1997).

Digitalno: Najpomembnejša osnova informacijske družbe je digitalizacija. Le-ta pomeni razčlenitev informacij na enake dele, imenovane »bite«, pri čemer ni pomembno, ali gre za govor, pisavo, tonski zapis, sliko ali videoposnetek. To omogoča popolno objektivizacijo podatkov in poenoteno shranjevanje vseh vrst informacij, stroškovno ugodno in praktično poljubno posredovanje, enotni medij ter integracijo različnih vrst informacij na enem temelju. Na digitalni tehniki temelječa računalniška omrežja predstavljajo »super« medij, ki je sposoben združiti vse dosedanje informacijske in komunikacijske medije ter jih hkrati dopolniti s funkcionalnimi zmogljivostmi (Svete 2005, 18).

Informacijska tehnologija: Informacijska tehnologija v kontekstu naloge označuje uporabo sodobne mikroelektronske računalniške in digitalne komunikacijske tehnologije za obdelavo, pridobivanje, shranjevanje, spreminjanje, posredovanje in ravnanje z digitaliziranimi podatki (Svete 2005, 16–17).

3 ČLOVEKOVA VARNOST

Človekova varnost ni univerzalen, vsesplošno sprejet izraz. Obstajajo različni, tudi konkurenčni koncepti. Sorodna izraza sta človekova ali individualna varnost (Svete 2005, 93–107). V nalogi se bomo osredotočili na posameznika in zavzeli stališče, da je človekova varnost najvišja vrednota, pomembnejša od preostalih preteklih pojmovanj varnosti.

3.1 Človekova varnost v teoriji

Čeprav trdimo, da je varnost temeljna prvina obstoja in razvoja človeka od davne preteklosti do danes, so skozi večino pisane zgodovine narod, družba oz. kasneje država igrali vlogo glavnega objekta in subjekta varnosti. Toda po koncu hladne vojne je prišlo do radikalnih strateških, političnih, ekonomskih in kulturnih sprememb, ki jih je še izdatno stopnjevala globalizacija, tako da je omenjen trend skozi prehod v 21. stoletje oblikoval sodobni koncept človekove varnosti, ki ponovno presega okvire posameznih držav ter se osredotoča na posameznika in kompleksno ogrožanje. Zaradi takšnega razvoja posvečamo vedno več pozornosti nekaterim doslej zanemarjenim kulturno-civilizacijskim razsežnostim varnosti, kot so degradacija okolja, podnebne spremembe, neenakomeren razvoj, lakota, revščina, nalezljive bolezni in odvisnosti od sodobnih tehnologij. Ne gre le za zagotavljanje fizičnega obstoja ljudi, ampak tudi njihove blaginje (Bučar in Grizold 2011, 827–829). Varnost v skladu s tem zajema tako ohranitev obstoja posameznika kot fizičnega, duhovnega, duševnega, kulturnega in družbenega bitja, kot tudi zagotovitev kakovosti njegovega bivanja v družbenem in naravnem okolju (Bučar in Grizold 2011, 829).

Pojem človekove varnosti se je začel intenzivno uveljavljati po hladni vojni. Leta 1991 je Program združenih narodov za razvoj v svojem poročilu človekovo varnost opredelil kot »osvobojenost od strahu in potreb«. Poročilo istega programa iz leta 1991 pa že našteva sedem kategorij, ki se kasneje širijo in do danes obsegajo vsaj devet področij človekove varnosti: ekonomsko (revščina, brezdomstvo), finančno (zaposlitev, preživljanje), prehrambno (lakota), zdravstveno (bolezni, zdravstvena oskrba), okoljsko (degradacija, onesnaževanje, naravne katastrofe), osebno (nasilje, kriminal, nesreče), spolno (enakopravnost, ogrožene skupine), skupnostno (diskriminacija, zatiranje, dezintegracija) in politično (represija, kršenje človekovih pravic) varnost. Kategorije so soodvisne in so med seboj povezane v celostni koncept človekove varnosti (Bučar in Grizold 2011, 839–840; Prezelj 2008, 25).

Na zasedanju G-8 1999 v Kölnu so človekovo varnost definirali kot svobodo in varnost posameznika in skupnosti v okolju, v katerem so zagotovljeni preživetje, temeljne človekove pravice in svoboščine ter je zaščiten vsak posameznik (Siedschlag v Svete 2005).

Najožje dojemanje človekove varnosti pomenita osebna varnost pred nasiljem ali škodo in dostop do osnovnih življenjskih potrebščin oz. človekovih dobrin. Širši pristop zagovarja človekovo varnost kot »osvobojenost od nasilja in pomanjkanja« (Vogrin in drugi 2008, 86). Pod to sodi tudi zaščita posameznika pred kriminalom in terorizmom, nalezljivimi boleznimi, politično in drugo korupcijo, zatiranjem in podobno (Bučar in Grizold 2011, 841). Pri širšem pristopu **je pomemben tudi ekonomsko-socialni razvoj** (Vogrin in drugi 2008, 86).

3.2 Človekova varnost v praksi

Pri večini ljudi, predvsem pri državljanih razvitih držav, občutek varnosti izvira iz problemov dnevnega življenja. Glavne skrbi in viri ogrožanja človekove varnosti so namreč zagotovitev delovnega mesta in materialnih zmožnosti, zdravstvena oskrba, degradacija okolja, kriminal in podobno (Svete 2005, 93–107). **Osredotočili se bomo torej na posameznika in njegove interese ter življenjsko okolje, ki mu omogoča izpolnjevanje njegovih želja in potreb**. To pomeni zaščito človeškega dostojanstva, za katero je potrebna »osvobojenost od strahu« (zaščita pred nasiljem) in »osvobojenost od potreb« (zaščita pred pomanjkanjem) (Vogrin in drugi 2008, 85).

Človekova varnost dojema posameznika kot temeljni referenčni objekt varnosti (Prezelj 2008, 17), ki mora biti cilj in končni smisel vseh varnostnih prizadevanj. Druge oblike varnosti niso končni cilj in so lahko le sredstva za dosego končnega cilja (Vogrin v Bučar in Grizold 2011, 841). Naš pristop bo dogmatičen, pri čemer bo posameznikova varnost bistvena in bo imela prednost pred državno varnostjo oz. državno suverenostjo. Sodobni trendi jasno kažejo, da državna varnost, kot jo razumemo tradicionalno, ne zagotavlja tudi posameznikove varnosti. Varnost države v tradicionalnem vojaško-političnem smislu ne zagotavlja nujno tudi posameznikove varnosti (Bučar in Grizold 2011, 843). V znotrajdržavnem konfliktu se lahko državna varnost in človekova varnost celo izključujeta. To bo v skladu tudi s solidarističnim in revolucionarnim, »od spodaj navzgor«, pristopom, katerega središče so posameznik in njegovi interesi (Svete 2005, 93–107).

3.3 Človekova varnost v informacijski družbi

V kontekstu informacijske družbe in informacijske tehnologije velja kot pomembno za človekovo varnostno najprej izpostaviti ogrožanje ekonomskega stanja, političnih in človekovih pravic in pravice do izražanja, predvsem preko zlorabe tehnologije, cenzure in preprečevanja dostopa. Nadalje velja omeniti še zasebno varnost, ki se nanaša na ogrožanje posameznikove identitete in privatnosti pri uporabi informacijske tehnologije (Rosenau in Singh v Svete 2005). V obzir moramo vzeti tudi, da je z močnejšim prepletanjem posameznikovega vsakdana z digitalnim svetom, vedno večji tudi potencial ogrožanja posameznikovih najožjih interesov, torej osebne varnosti (preživetje, nasilje) s pomočjo informacijske tehnologije.

4 TEMELJI IN DEFINICIJA HEKTIVIZMA

Razumevanje »kulture hekanja (hacking)« in »koncepta heka (hack)« je bistveno za razumevanje fenomena hektivizma, ker sta »kultura hekanja« in njen »hek« ena izmed temeljev hektivizma (Jordan in Taylor 2004, 6).

Predvsem zaradi opisanih predsodkov izraz hektivizem danes v pogovoru povzroči mešane reakcije in odpira razprave o problemih legitimnosti, moralnih vprašanjih in celo o varnostnih zadržkih. Ker se zaradi ohlapnih definicij hektivizem pogosto zamenjuje s spletnim aktivizmom ali kiberterorizmom oz. kiberkriminalom, je potrebno objektivno preučiti, kaj hektivizem je in v čem se razlikuje od spletnega aktivizma ter v čem se razlikuje od kiberkriminala oz. kiberterorizma, kar je še pomembneje.

4.1 Hekerski temelji hektivizma

Kultura »hekanja« izvira iz ameriškega Tehnološkega inštituta Massachusettsa (MIT je ang. kratica za Massachusetts Institute of Technology) in sega v obdobje 70-ih let 20. stoletja. Začetki kulture imajo v resnici malo opraviti z računalniki – »hek« so si izmislili študenti iz MIT-a, iz »kluba za modele vlakcev«, ko so svoje modele železnic vzdrževali in uporabljali na nenavadne načine. Čeprav se danes težko znebimo konotacij besede z nedovoljenimi računalniškimi vdori, beseda »hek« izvorno pomeni »poizkus uporabe določene tehnologije na izviren, nenavaden in iznajdljiv način«. Temeljne značilnosti »heka« naj bi bile namreč preprostost, mojstrstvo in nedovoljenost, »hek« pa lahko prenesemo na katerokoli tehnološko področje – kadar tehnologijo uporabimo na način, za katerega ni namenjena; pa naj bodo to modeli železnic ali mreža računalnikov (Jordan in Taylor 2004, 6–7).

»Hek« je nastal kot šaljiva potegavščina, ko so denimo študentje MIT-a čez noč postavili avtomobil Volkswagen na kupolo ene izmed stavb v univerzitetnem kampusu ali ko so na primer izmerili dolžino nekega predmeta, recimo mostu, v večkratniku dolžine telesa enega izmed študentov. Študentje so »shekali« avto na vrh kupole in s »hekanjem« določili, da lokalni most meri 150 Brianov, ker je bilo študentu, čigar telo so uporabili kot merilo, ime Brian. Smešna potegavščina se je potem, ko so jo študentje iz preostalih oddelkov MIT-a (predvsem strojniškega in računalniškega) vzeli za svojo, hitro razširila čez celotno računalniško in informacijsko skupnost. MIT je vedno veljal za eno vodilnih institucij na področju sodobne tehnologije in njihovi študentje so zagotovo služili za vzgled ostalim nadobudnežem, zaradi česar se je koncept »hekanja« zakoreninil v uporabi sodobne

informacijske tehnologije (BBC Four 2013; Jordan in Taylor 2004, 9–10; Levy v Jordan in Taylor 2004, 10).

4.1.1 Heker in hekerska etika

Izraz »heker« se je začel pogosteje uporabljati konec 70-ih letih, in sicer v praksi vedno v povezavi s sodobno informacijsko tehnologijo, ter je pomenil posameznika z izjemnimi sposobnostmi za programiranje. Zaradi določenih razlogov, ki jih bomo razložili v nadaljevanju, se je izraza kmalu zatem oprijel zlovešč sloves izkoriščanja informacijske tehnologije in nedovoljene uporabe izjemnih sposobnosti za programiranje. Posledično se ta slab sloves preslika na vsako dejavnost, povezano s »hekom«. Da bi torej lahko razumeli, zakaj se je izraza oprijelo slabo mnenje, je potrebno podrobneje preučiti razvoj koncepta »hekanja«. V grobem lahko razvoj razčlenimo na sedem generacij, ki pa si ne sledijo popolnoma kronološko in se med seboj prepletajo (Jordan in Taylor 2004, 10–12).

Na začetku lahko identificiramo tri prepletajoče se skupnosti, ki so uporabljale izključno »dober hek« (v tem obdobju se »hekanje« namreč ni uporabljalo v nepoštene namene):

1. zgodnji hekerji, pionirski računalniški ljubitelji, ki so se pojavili v zgodnjih obdobjih računalništva, tj. v 50-ih in 60-ih letih (le-ti so vztrajno eksperimentirali s sposobnostmi velikih osrednjih računalnikov na velikih ameriških univerzah, kot je na primer MIT);
2. hekerji strojne opreme oz. strojni hekerji, inovatorji računalniške opreme (ki so se večinoma ukvarjali s strojno opremo in so v začetku 70-ih igrali ključno vlogo v računalniški revoluciji);
3. hekerji programske opreme oz. programski hekerji, inovativni programerji (ki so bili osredotočeni na ustvarjanje programske opreme, pogosto za spremenjeno strojno opremo, posebej s strani njihovih kolegov, »strojnih hekerjev«) (Levy v Jordan in Taylor 2004, 10).

Na temeljih treh skupin »prve generacije hekerjev« se je rodila značilna hekerska skupnost s temeljnimi vrednotami, ki jih lahko imenujemo »hekerska etika«:

I. popoln in neomejen dostop do računalnikov;
II. vse informacije bi morale biti proste;
III. ne zaupaj avtoriteti in spodbujaj decentralizacijo;
IV. hekerji se sodijo na podlagi hekerskih sposobnosti in ne po pripadnosti uradnim organizacijam ali drugih nepomembnih kriterijih;

V. posameznik lahko z računalnikom ustvari umetnost in lepoto;
VI. računalniki lahko življenje spremenijo na boljše (Levy v Virginia Tech 1997).

Iz zapuščine prve generacije kasneje izhaja »drugi val«, ki pa kljub določenim podskupnostim z novimi pristopi in deviacijami v vrednotah še vedno temelji na »hekerski etiki«. Ponovno so to prepletajoče se skupnosti brez strogih meja in delitev ter skupnosti, ki v osnovi niso zlonamerne:

4. krekerji (od sredine 80-ih izraz »kreker« pomeni osebo, ki nedovoljeno vlomi v posameznikov računalniški sistem, in sicer zlonamerno ali nezlonamerno);
5. strežaji (računalniški programerji, ki izhajajo iz hekerske podkulture in so kljub temu oz. posebej zaradi tega postali del velikih računalniških in informacijskih podjetij, ki po navadi poslujejo v nasprotju s hekersko etiko);
6. odprti viri (skupnosti, ki si v skladu s hekersko etiko prizadevajo, da bi bili »heki« dostopni vsem, ki jih želijo dodatno izpopolnjevati, kar je v močnem kontrastu s komercialnim programiranjem in z interesi velikih podjetij);
7. hektivisti (le-ti se pojavijo sredi 90-ih, ko »hekerske« dejavnosti pod vplivom »hekerske etike« postanejo očitno politično naravnane) (Levy v Jordan in Taylor 2004, 11–12).

S pojavom drugega vala so bili hekerji opredeljeni kot nova podkultura in so takoj postali deležni tudi medijske pozornosti. Izstopali so kot nenavadno domači z novimi tehnologijami informacijske revolucije, ki je naznanjala (kot se je zdelo) zelo nepredvidljive spremembe – ljudem je bila ta nova računalniška podkultura vsaj sumljiva, če jih ni celo naravnost strašila. Izdelki in prizadevanja »hekerjev« so se z razvojem sodobne informacijske tehnologije začeli prvič tudi neposredno dotikati vsakodnevnih življenj, kar je prinašalo dodatno nelagodje. Seme, iz katerega se kasneje rodi strah pred zloveščim mojstrom informacijske tehnologije, je tako začelo kliti (Jordan in Taylor 2004, 12–15; McLaughlin 2012, 24–29).

Prva generacija sama je že imela neke vrste radikalno politično motivacijo, ker si je prizadevala moč računalnika vnesti med ljudi. V hekerski etiki je globoko zakoreninjeno prizadevanje za neomejen dostop do računalniških zmogljivosti in informacij. Na nek način sta želja po »hekanju« in želja po bolj demokratični uporabi informacijske tehnologije postali nerazdružljivi z vidika »hekerske agende«. To je kot dvorezni meč sicer služilo razvoju novih inovativnih pogledov na družbo, medtem ko je po drugi strani fascinacija nad novimi

tehnologijami družbo odvračala od socialnih skrbi. Predvsem slednje je ponovno vznemirjalo navadnega državljana (Jordan in Taylor 2004, 12–15; McLaughlin 2012, 24–29).

Hekerji drugega vala še vedno izhajajo iz vrednot prve generacije, toda sčasoma je pritisk naredil svoje, ko so se določene skupine začele odločneje oddaljevati od »hekerske etike« in zasledovati drugačne cilje. Izvirne »hekerske vrednote« so se po odprtem dostopu do računalniških in informacijskih tehnologij ter informacij kot dobrin za izboljšanje stanja zaznanega demokratičnega deficita v družbi sčasoma uklonile bolj sebičnim prizadevanjem. Določene podskupnosti so namreč več pozornosti namenile uporabi informacijske tehnologije za lastno korist, priložnostim za komercialno in celo zlonamerno kriminalno izkoriščanje ter zastraševanje nastajajoče mlade informacijske družbe. Čeprav ti posamezniki in skupine po navadi izhajajo iz katere od skupnosti »drugega vala«, je zanje značilno močno oddaljevanje od hekerske etike, predvsem na področju zlonamernosti (Jordan in Taylor 2004, 12–15; McLaughlin 2012, 24–29).

Čeprav zlonamerno in izključno za lastno korist deluje le izjemno majhen odstotek hekerjev, so njihove aktivnosti prižgale sod smodnika, ki je bil nelagodje pred nepredvidljivim in povsod prisotnim računalnikom, ki lahko na nenavadne načine vpliva na vsakdanje življenje ljudi, predvsem tistih, ki nove tehnologije ne razumejo dobro. Svojo mero so prispevale še skupine, ki so si s pomočjo različnih vzvodov, tj. kapitala in vpliva ter množičnih medijev, prizadevale kopičiti in monopolizirati moč računalnika in informacije za svojo korist ter jim je bilo zato blatenje »hekerske podkulture« v interesu. Tako je bil sloves besede »heker« za vedno omadeževan (Jordan in Taylor 2004, 12–15; McLaughlin 2012, 24–29, 37–39).

Dodatni problem predstavljata še pogosto prizadevanje določenih hekerskih skupin za popolno informacijsko svobodo, ki je vsaj v nekaterih okoliščinah radikalna in problematična, in nedovoljenost, ki je ena od temeljnih značilnosti »heka«. Na tak način je hekerska aktivnost, čeprav ni niti slučajno zlonamerna, hitro postala nezakonita in moralno sporna. Toda »**hekanje« je miselnost – je radovednost in odkrivanje načinov za učinkovitejše delovanje (**Bickford v McLaughlin 2012, 23**). Razumeti moramo, da »hekanje« v osnovi ni destruktivna aktivnost, ampak je v povezavi s »hekersko etiko« ravno nasprotna dejavnost, saj je konstruktivna družbena sila, ki si prizadeva za svobodno uporabo in decentralizacijo informacijske tehnologije.** Za objektivno preučevanje je zelo pomembno, da se znebimo predsodkov, povezanih s konceptom »heka« (McLaughlin 2012, 37–39).

4.1.2 Sodobni heker

V nadaljevanju moramo v obzir vzeti še to, da je v tem trenutku sodobna informacijska družba že v polnem zamahu ter da je računalniška tehnologija skozi napredek že postala dostopna večini državljanov razvitega sveta in da ima dve bistveni značilnosti: Prva lastnost je preprostost, saj računalniška tehnologija od uporabnikov več ne zahteva kompleksnega znanja ali izjemnih sposobnosti za programiranje. Druga pomembna značilnost pa je interaktivnost, ki omogoča vsakemu udeležencu, da ni zgolj potrošnik, temveč tudi potencialni proizvajalec (Svete 2005, 20). Na nek način je »heker« vsaka oseba, ki ima dostop do informacijske tehnologije in ki jo veseli odkrivanje načinov, kako zaobiti njene omejitve ali jo uporabiti na inovativen način. Vsak posameznik z dostopom do informacijske tehnologije ima potencialni vpliv na informacijsko družbo. Posameznike brez posebnih programerskih sposobnosti, ki uporabljajo že uveljavljeno programsko opremo in orodja, ki so jih za množično uporabo priredili sposobnejši hekerji, imenujemo z malenkost slabšalnim izrazom »script-kiddies« oz. po slovensko »skriptarji« (Andress in Winterfeld 2014, 208–211; Kovačič 2008; Jordan in Taylor 2004, 12–15; McLaughlin 2012, 23–29).

4.2 Definicija hektivizma

Dokaj uveljavljena definicija v grobem hektivizem definira kot »kombinacijo množičnega političnega protesta z računalniškim »hekanjem« skozi »nenasilno uporabo nezakonitih ali zakonito spornih digitalnih orodij za dosego političnih ciljev« (Samuel 2004, 36). Orodja in metode hektivistov so razobličenje spletne strani, parodija spletne strani, virtualni protesti v obliki množičnega pošiljanja e-pošte in virtualne blokade, kot na primer napad s poplavljanjem (DoS), porazdeljeni napad s poplavljanjem (DDoS), ugrabitev domene oz. preusmerjanje, nedovoljen dostop do informacij in podobno (Andress in Winterfeld 2014, 208–211; Janssen 2014).

Prof. Dorothy Dunning iz Georgetownske Univerze definira hektivizem kot »konvergenco hekanja z aktivizmom, pri kateri »hekanje« pomeni operacije, ki izkoriščajo informacijsko tehnologijo na nenavaden in pogosto nezakonit način, tipično s pomočjo posebne hekerske programske opreme. S tem prinaša metode državljanske nepokorščine v digitalni prostor, zato hektivizem vključuje elektronsko državljansko nepokorščino (Denning 2001, 263).«

S takšno definicijo se strinjajo tudi znani samooklicani hektivisti, člani Teatra elektronskih motenj (ang. Electronic Disturbance Theater), ki v svoji izjavi navajajo, da »bodo pri dejavnostih v elektronskih in digitalnih oblikah vedno pogosteje uporabljena načela

tradicionalne državljanske nepokorščine, kot sta denimo motenje posesti in blokada (Wray 1998).« Na nek način hektivisti zase trdijo, da samo sledijo tradicijam Gandhija ali Martina Luthra Kinga mlajšega, ko poizkušajo privesti do družbenih in političnih sprememb skozi nenasilne in nezlonamerne dejavnosti (Thomas 2001).

Technopedia hektivizem definira kot »hekersko uporabo spletne strani ali računalniške mreže, z namenom posredovanja družbenega ali političnega sporočila.« Nato nadaljuje, da hektivisti informacijske tehnologije ne izrabljajo zlonamerno, ampak da so njihove aktivnosti lahko disruptivne in tudi nezakonite, z namenom zadostne osvetlitve družbenega ali političnega problema, na katerega poskušajo opozoriti. Motivira jih namreč aktivna želja po boju proti vladnemu nadzoru in cenzuri ter omejevanju uporabe informacijske tehnologije. Hektivizem je od informacijske tehnologije odvisna strategija za izvajanje spletne državljanske nepokorščine (Janssen 2014).

Hektivisti so torej vedno hekerski oz. inovativni uporabniki informacijske tehnologije. So bolj ali manj sposobni hekerji, politično ali ideološko motivirani in osredotočeni na vplivanje na mnenja o določeni zadevi. Čeprav je raznolikost ciljev, za katere si potencialno prizadevajo, praktično neskončna, gre običajno za vprašanja, ki imajo na kakršenkoli način opraviti s hekersko etiko – protikorporativne vrednote, svoboda govora in izražanja, državljanske svoboščine, prost pretok informacij, človekove pravice in podobno (Andress in Winterfeld 2014, 23–29).

Na podlagi tega je naša definicija hektivizma sledeča: **Hektivisti so politično ali ideološko motivirani hekerji, ki nezlonamerno in v skladu s hekersko etiko informacijsko tehnologijo uporabljajo za protest, opozarjanje na problem in posredovanje sporočil z namenom vplivanja na družbene in politične spremembe.**

4.2.1 Kiberterorizem in kiberkriminal.

Kiberkriminal je vsaka oblika kaznivega dejanja, pri kateri je uporabljena računalniška oz. v širšem smislu informacijska tehnologija, ki je lahko tarča kaznivega dejanja ali pa je kaznivo dejanje izvedeno s pomočjo informacijske tehnologije (Kovačič 2008).

Kiberkriminalci s pomočjo informacijske tehnologije nedovoljeno dostopajo do informacij in jih uporabljajo izkoriščevalsko ali zlonamerno. Po navadi gre za spletno goljufijo, spletno krajo in trgovanje s podatki, spletno krajo, uničenje ali trgovanje z intelektualno lastnino, krajo identitete in nepooblaščeni dostop do računalnika (Kovačič 2008).

Običajno so to kazniva dejanja iz koristoljubja, in sicer za pridobitev protipravne premoženjske koristi; motivacija za tovrstna dejanja je lahko tudi osebna, ko gre na primer za kaznivo dejanje iz maščevanja. Čeprav je motivacija za izvajanje kiberkriminalnih dejanj videti različna, gre praktično v vseh primerih predvsem za zadovoljitev lastnih sebičnih ciljev na račun dobrobiti drugih (Kovačič 2008, Janssen 2014, Dennis 2014).

Za namene naloge bomo uporabili naslednjo definicijo kiberkriminalcev: **Kiberkriminalce motivira lastna korist, saj informacijsko tehnologijo zlonamerno in brezobzirno uporabljajo za uresničitev svojih sebičnih ciljev.**

Za kiberterorizem trenutno nimamo enotne definicije. NATO v svoji definiciji iz leta 2008 navaja, da je kiberterorizem »kibernetski napad, ki uporablja ali izkorišča informacijsko mrežo za povzročitev zadostne mere uničenja, ki bo ustvarila dovolj strahu, da bo v ustrahovani družbi vplivala na želene spremembe (NATO v Kostadinov 2012).«

Z definicijo postreže tudi ameriški Državni center za zaščito infrastrukture, po katerem je kiberterorizem »kaznivo dejanje, povzročeno skozi informacijsko tehnologijo, s posledicami nasilja, smrti in/ali uničenja in povzročanja strahu ter z namenom izsiljevanja sprememb v vladni politiki (Wilson 2005, 6).

Pri kiberterorizmu gre za konvergenco terorizma z digitalnim svetom. Informacijska tehnologija je uporabljena za napad, katerega glavni namen je prisiliti vlado ali državljane, da se uklonijo zahtevam. Dejanje mora povzročiti nasilje ali strah (Stohl v Kostadinov 2012).

Na podlagi tega lahko zapišemo tudi delovno definicijo kiberterorizma: **Kiberteroristi so ideološko in politično motivirani, saj informacijsko tehnologijo zlonamerno uporabljajo za povzročanje strahu in nasilja, ki bo ustrahovalo žrtve, da se uklonijo njihovim zahtevam.**

4.2.2 Kriteriji za določanje hektivizma.

Pri postavljanju meje med hektivizmom in kiberterorizmom je ključna zlonamernost uporabljenih metod. Ko aktivnosti katerekoli skupine, na primer krekerjev ali hektivistov, postanejo zlonamerne, moramo le-te na novo opredeliti kot teroristične ali kriminalne hekerje.

Čeprav obe dejanji, tako hektivistično kot kiberteroristično, lahko izhajata iz podobne ideološke ali politične motivacije in se izvajata za doseganje podobne ideološke ali politične agende, je hektivizem po naravi nenasilen akt. Za razliko od kiberterorizma hektivizem za

dosego ideoloških ali političnih ciljev ne uporablja metod za vnašanje strahu in terorja med splošno populacijo; namesto tega jih poizkuša uresničiti z opozarjanjem in s spodbujanjem smiselne razprave. Konceptualno sta torej hektivizem in kiberterorizem dva popolnoma različna pojma, čeprav lahko razlikovanje med obema v praksi povzroči kar nekaj težav, ker je debata o ideoloških in političnih ciljih precej subjektivna zadeva, poleg tega pa lahko tudi dejanje, za katerega se vsi strinjamo, da je skrajno plemenito, povzroči kolateralno škodo. Kljub temu med hektivizmom in kiberterorizmom teče debela in razločna meja (Thomas 2001).

Tudi med hektivizmom in kiberkriminalom sicer res lahko potegnemo mejo na podlagi zlonamernosti, vsaj kar se tiče najbolj značilnega kiberkriminala in v osnovi nenasilnih in hvalevrednih hektivističnih prizadevanj. Dokler so dejanja motivirana izključno s prizadevanjem za lastno korist oz. izključno za korist skupine in je tehnologija uporabljena na izkoriščevalski način, je dejanje zlonamerno in ga ne moremo opredeliti drugače kot kiberkriminal. Težje je razlikovati pri nezakonitih dejanjih, ki se na prvi pogled mogoče ne zdijo izkoriščevalska ali zlonamerna, še posebej kadar gre za manjše kršitve neuniverzalnih zapisanih zakonov, ki jih v drugih državah ne poznajo. Četudi se namreč strinjamo, da hektivistične metode niso zlonamerne, to še ne pomeni, da včasih niso v nasprotju z zapisanimi zakoni in da ne morejo povzročiti kolateralne škode – zato je za razlikovanje med hektivizmom in kiberkriminalom zelo pomembno, da natančno ugotovimo, kdaj kršenje nekega veljavnega, čeprav manj pomembnega ali neuniverzalnega, zakona ali kolateralna škoda nista več opravičljiva in dejanja moramo označiti kot kiberkriminal. Bolj kot ukvarjanje z bolj ali manj hujšimi kršitvami pisanih zakonov posameznih držav je tukaj odločilna moralna upravičenost. **Bistveni dejavniki za upravičenost so:**

- **1. škoda, povzročena tretjim osebam;**
- **2. prevzemanje odgovornosti in javna podpora ter**
- **3. smiselna utemeljitev dejanja.**

- Prizadevanja z veliko podpore, za katere posamezniki brez oporekanja prevzamejo odgovornost in sprejemajo posledice, so kljub kršenju pisanih zakonov zagotovo manj moralno sporna, kot recimo prikrito kršenje zakona na škodo širše družbe, za uresničitev obrobnega prizadevanja majhne skupine. Trdimo lahko, da je dejanje kljub temu, da ni legalno, vseeno legitimno. Dejanje, četudi ni v skladu z zakoni določene

države, se lahko šteje za hektivistično, dokler je moralno opravičljivo oz. ga večina smatra kot legitimno.

Povzročena škoda je pogosto odvisna predvsem od tega, ali je tarča »heka« javna, zasebna, komercialna ali nekomercialna entiteta. Napad na javno, nekomercialno informativno spletno stran, še posebej če so informacije na strani nebistvene, povzroči le nekaj neugodnosti za vse, ki želijo dostopati do informacij na strani – v primeru, da stran postreže z varljivimi ali s spornimi informacijami, napada res ni težko opravičiti. Nekaj popolnoma drugega, po mojem mnenju skoraj nemogočega, je opravičiti napad na pomembno javno entiteto, ki povzroči veliko škode, na primer esencialno infrastrukturo ali recimo javni bolnišnični strežnik; tako torej dejanja, katerih posledica je lahko celo smrt, niso samo neopravičljiva, ampak so naravnost zlonamerna, zato v tem primeru ni govora o hektivizmu. Napad na zasebno komercialno stran načeloma ne more neposredno ogrožati fizičnih življenj, čeprav lahko povzroči precej finančne škode – tak napad lahko opravičimo v primeru velike javne podpore, recimo napada na podjetje, ki krši človekove pravice. Omeniti velja še moralne posledice, ki jih lahko ima napad na zasebne posameznike in jih moramo vzeti v obzir (kršitev posameznikove pravice do svobode govora, kršenje pravice do zasebnosti in lastnine). Še posebno dobre razloge za opravičilo pa potrebujemo, ko pride do uničevanja zasebne lastnine.

Povzročena škoda ni odvisna samo od vrste žrtve, ampak tudi od vrste dejanja. Nekatere aktivnosti povzročijo manj škode kot druge. Razobličenje spletne strani ima načeloma manj resne posledice od napada s poplavljanjem, čeprav je tudi to odvisno od vsebine objavljenega na tej strani; recimo objava zasebnih ali občutljivih informacij na javni strani ima lahko resne posledice, medtem ko parodija veliko manj. Napade, ki v osnovi povzročijo več škode, je težje opravičiti (Thomas 2001).

Na nek način mora biti škoda povzročena proporcionalno, da je moralno opravičena. Proporcionalno dejanje je tisto, ki ga podpira dovolj posameznikov in ki se ne zanaša na ranljivosti v sistemu oz. ga ne izkorišča. Majhna skupina hekerjev tako ne bi smela sama onesposobiti veliko večje korporacije (Slobbe in Verberkt 2012, 19).

Sprejemanje odgovornosti: Še eden od faktorjev, ko poskušamo opravičiti kršenje zakona, je sprejemanje odgovornosti za storjeno dejanje. Poleg tega, da morajo biti hekerji motivirani z moralno sprejemljivimi zadevami in delovati nenasilno, morajo tudi vsaj delno sprejeti odgovornost, da bi bila njihova dejanja moralno opravičljiva.

Sprejemanje odgovornosti signalizira moralnost motivacije. Kljub temu obstaja pomembna razlika med samim sprejemanjem odgovornosti za dejanje in sprejemanjem posledic dejanja. Načeloma hekerji in hekerske skupine sprejemajo odgovornost za dejanja pod psevdonimi ali kot skupina pod skupnim imenom, medtem ko z različnimi sredstvi poskušajo zakriti pravo identiteto in lokacije posameznikov, z namenom izogibanja kazenskemu pregonu in pravnim posledicam. Takšno prikrito dejanje je težje opravičiti kot denimo napol prikrito, med katerim odgovornost prevzame skupina in posamezniki svoje identitete in lokacije sicer ne razkrivajo, ampak je tudi ne poskušajo aktivno zakriti. Navsezadnje tudi teroristi prevzemajo odgovornost za napade, dokler sta njihova identiteta in lokacija prikriti. Protest, ulični ali digitalni, se lahko, kljub temu da so posamezni protestniki anonimni, opraviči, dokler ti svoje anonimnosti ne izkoriščajo – če se anonimnost izkorišča, mora protest omogočati, da se takšen posameznik sankcionira (Slobbe in Verberkt 2012, 19). Čisto dejanje elektronske državljanske nepokorščine, pri katerem posamezniki svoje identitete in lokacije ne poskušajo zakriti in so celo pripravljeni sprejeti pravne posledice, saj to še močneje osvetli problem, na katerega opozarjajo, pa je na nek način že v osnovi upravičeno. Cilj državljanske nepokorščine po navadi že v osnovi uživa večjo količino javne podpore (Thomas 2001).

Smiselna utemeljitev: Če heker ali skupina hekerjev poizkuša svoja dejanja opravičiti brez razkritja prave identitete in lokacije, mora imeti odločno kognitivno posest nad smiselno utemeljitvijo moralnosti svojih dejanj. Navsezadnje odgovornost kot skupina za svoja dejanja prevzemajo tudi teroristične organizacije. Prizadevanje mora biti že na splošno hvalevredno in uživati dobro mero javne podpore. Še bolje je, če je sodelovanje v dejavnosti omogočeno širšim množicam, ki lahko na tak način aktivno izražajo podporo. Žrtev napada, pa tudi javnost, katere mir je bil moten, ima pravico do natančne razlage o motivaciji za takšno dejanje in zakaj naj bi bilo le-to upravičeno. Pripravljenost povzročanja resnih posledic za uresničevanje nekih obrobnih stališč, ki niso niti dobro artikulirana, kaj šele podprta s smiselno utemeljitvijo, ni samo neupravičeno, ampak skoraj zagotovo zlonamerno (Thomas 2001).

Čeprav trije kriteriji ne zagotavljajo nekega popolnoma objektivnega merila, so kljub temu boljše in univerzalnejše orodje za določanje legitimnosti posameznih primerov kot neenotni zapisani zakoni. Za vsako dejanje posebej pretehtamo med povzročeno škodo, prevzeto odgovornostjo in javno podporo oz. smiselnostjo utemeljitve, da določimo, če je dejanje akt hektivizma ali gre za kiberkriminal oz. kiberterorizem. Koordiniran in dolgotrajen napad na veliko komercialno stran ali napad na esencialno infrastrukturo, ki povzroči veliko finančno

škodo oz. ima trajne posledice, lahko izvede majhna skupina elitnih hekerjev. To je napad zaradi uresničitve interesov posameznikov na račun škode večjega števila ljudi – tudi če posamezniki trdijo, da so motivirani z višjimi cilji, je tak napad praktično neupravičen. Nekaj popolnoma drugega je, veliki finančni škodi navkljub, če veliko komercialno stran napade in onesposobi ogromna množica uporabnikov računalniške tehnologije ob minimalni podpori skupine sposobnih hekerjev, in sicer z dobro utemeljenimi cilji (Thomas 2001).

Hektivizem je moteč in pogosto nezakonit, ampak nikoli zlonameren. **Nezakonito dejanje se šteje za hektivistično, če je moralno upravičeno, sicer velja za neupravičeno in ga opredelimo kot kiberkriminal oz. kiberterorizem.** Kot smo ugotovili v zgornjih odstavkih, je kiberkriminal vedno nelegalen in zlonameren, včasih disruptiven, kiberterorizem pa je zmeraj disruptiven in zlonameren ter nelegalen (Thomas 2001). Vsaka hekerska dejavnost z elementi kiberkriminala ali kiberterorizma ne more biti hektivistična. Hektivizma tudi ne smemo zamenjevati s spletnim aktivizmom, ki je navadna legalna aktivistična dejavnost na spletu, brez hekerske uporabe računalniške tehnologije.

Če navedemo praktičen primer: Spletni aktivisti so enostavno posamezniki ali skupine, ki izvajajo nesporne aktivistične dejavnosti na spletu. Lahko vzpodbujajo različne kampanje, komunikacijo z vladnimi uradniki, delijo poročila o stanju, pomembne naslove, datume in podatke, zbirajo podpise in podobno. Če pa ti posamezniki ali skupine začnejo na primer organizirati in izvajati množično pošiljanje več protestnih e-sporočil nekaterim vladnim uradnikom, z namenom prenasičenosti in onemogočanja njihovih spletnih poštnih predalov, jih moramo soditi na podlagi treh omenjenih kriterijev, saj so njihove dejavnosti postale disruptivne in v nekaterih državah najbrž tudi nelegalne. Spletni strežnik žrtvinega poštnega predala se lahko zlomi pod pritiskom in ne more sprejemati niti poštnih sporočil z drugačnim, nasprotnim mnenjem. Če napad ni zlonameren, torej če je moralno upravičen, na primer, da javni uradnik zavzema rasistična stališča ali pa je uradnik vlade, ki krši človekove pravice, ter v napadih sodeluje veliko število ljudi ob podpori širše javnosti, govorimo o hektivizmu. V primeru, da je posameznik razmeroma zgleden vladni uradnik in ga skupina napade iz osebnih razlogov ali zaradi obrobnega prepričanja, na primer zaradi zamere oz maščevanja ali iz zabave, so hekerji, ki napad izvedejo, kiberkriminalci. Za kiberterorizem bi šlo v primeru, da bi napad na uradnika služil kot grožnja drugim; na primer ponovitev napada na predale vseh, ki se ne bodo uklonili določenim zahtevam – še bolj, če bi skupina napad izvedla na spletnem strežniku nujne službe, ki sprejema nujna sporočila o nesrečah – takšen napad lahko namreč povzroči celo izgubo življenja.

5 ANALIZA ZGODOVINE IN PRIMEROV HEKTIVIZMA

Skozi prejšnja poglavja smo predstavili temelje hektivizma, globoko motivacijo in vrednote, na podlagi katerih le-ta deluje, ter, kar je najpomembneje, smo definirali, kaj je in kaj ni hektivizem. V tem poglavju bomo na kratko povzeli zgodovino hektivistične dejavnosti, ki bo uvod za analizo primerov v naslednjem poglavju – študije najodmevnejših primerov iz sodobne zgodovine, ki so jih oklicali za hektivizem.

5.1 Rojstvo hektivizma.

Kot smo zapisali v četrtem poglavju, hekerska kultura izvira iz massachusettskega inštituta za tehnologijo, kjer je nastala večina praktičnih potegavščin študentov, pri katerih so tehnologijo uporabljali na inovativne načine. Takšen hekerski način razmišljanja je v tem času postal značilen za študente MIT-a, ki so se ukvarjali s sodobno tehnologijo. Na ta način je hekerska kultura neločljivo povezana z računalniško tehnologijo; odkar namreč obstajajo računalniki, poznamo tudi hekerje. V resnici se za večino napredkov računalniške in informacijske tehnologije lahko zahvalimo ravno ljudem, ki so želeli stvari razstaviti, videti, kako delujejo, in jih uporabiti na načine, za katere te stvari prvotno sploh niso namenjene. Google, Apple, Microsoft in Facebook so rojeni ravno iz hekerskega načina razmišljanja.

Z vedno večjim vplivom informacijske tehnologije na vsakdanja življenja posameznikov so popularna socialna in aktivistična gibanja v osemdesetih in devetdesetih letih prejšnjega stoletja začela spoznavati pomen novih tehnologij za krepitev svojih prizadevanj. Družbeni aktivizem je svoje dejavnosti, predvsem protestne, okrepil z uporabo nove informacijske tehnologije. Tako so bili računalniki NASE in Urada ZDA za energijo okuženi s protijedrskim protestnim črvom, imenovanim WANK, aktivistična skupina Zippies pa je s pomočjo napadov s poplavljanjem na vladne strani v Veliki Britaniji protestirala proti prepovedi rabe zabav na prostem. Skupaj s širjenjem novih tehnologij je v tem času začela odraščati tudi novonastala hekerska kultura – hekerska etika in vrednote so postajale vedno bolj politične,

hekerska prizadevanja pa so postajala stvar resničnosti. V takšnem okolju sredi devetdesetih je nastal hektivizem, kombinacija hekerske kulture in družbenega aktivizma – z uporabo digitalne tehnologije za zasledovanje političnih in ideoloških ciljev. Poleg splošnih aktivističnih prizadevanj, človekovih pravic, svoboščin in okoljevarstva so enako pomembne postale tudi hekerske vrednote in hekerska etika, prost dostop do tehnologije in svoboda informacij. Od takrat se izraz hektivizem uporablja precej široko, po moje mnenju večinoma prenagljeno in brez zadostnega razumevanja posamezne situacije, v zvezi z večino digitalnih protestov in udejstvovanj proti raznim akterjem, od multinacionalnih korporacij, vlad, celo podeželskih organov pregona, do moralno spornih skupin in posameznikov. Za hektiviste so označeni posamezniki, večje in manjše, odprte in skrivne skupine. Takšna uporaba izraza je napačna zaradi velike nediskriminatornosti.

V določenih primerih niti sodelujoči sami niso bili prepričani, če so njihove metode primerne, če gre ali ne gre za hektivizem. V prejšnjem poglavju smo zato podali primerno definicijo hektivizma in merila, s pomočjo katerih lahko za vsako situacijo posebej določimo, če je dejanje akt hektivizma ali pa je primerneje govoriti o dejanju kiberkriminala oz. kiberterorizma. Samo če je resnično govora o hektivizmu, lahko ocenimo še učinke (Casserly 2012, McCormick 2013).

Za namen preverjanja resničnosti naših hipotez bomo analizirali pomembnejše primere, ki so jih za hektivizem označili predvsem množični mediji in širša javnost. Šlo bo za aktivnosti bolj ali manj šibko povezanega kolektiva uporabnikov informacijske tehnologije, imenovanega Anonymous. Z dejavnostmi kolektiva Anonymous je namreč hektivizem prvič v zgodovini začel resno zanimati tudi povprečnega uporabnika množičnih medijev in ne zgolj obrobne skupine strokovnjakov za informacijsko varnost. Hektivizem je postal »mainstream«, zato imenovalnik Anonymous danes mnogi že dojemajo kot sinonim za hektivizem, čeprav je takšna trditev prenagljena. Za boljše razumevanje in kvalitetnejšo analizo bomo v naslednjih odstavkih predstavili začetke kolektiva Anonymous. Potem bom analizirali primera Operacije Payback in Operacije Arabska pomlad.

5.2 Anonymous.

Na kratko je Anonymous ohlapno povezana mreža predvsem politično in ideološko motiviranih uporabnikov interneta, ki s pomočjo informacijske tehnologije izražajo svoja prepričanja in v skladu z njimi poskušajo vplivati na resnične spremembe. Njihovi motivacija in cilji, predvsem pa metode so izjemno raznovrstni; motivacija in cilji so bili v preteklosti

hvalevredni in splošno sprejeti kot moralno opravičljivi, po drugi strani pa tudi naravnost zlonamerni. Njihove metode zakonite, nezakonite, uporabljene upravičeno ali neupravičeno. Zaenkrat tega sicer ne bomo ocenjevali, moramo pa razumeti, da vseh aktivnosti Anonymous po definiciji iz prejšnjega poglavja ne moremo označiti za hektivizem (BBC Four 2014).

Anonymous je nastal leta 2003 na spletnem forumu 4chan in je predstavljal nekakšen skupni glas te decentralizirane spletne skupnosti. Spletni forum ni zahteval registracije uporabnikov, zato je lahko vsak uporabnik svoje mnenje izrazil kot anonimnež, pod uporabniškim imenom Anonymous. V skupnosti 4chan je krožila notranja šala, da vso vsebino na spletni strani 4chan objavlja ena oseba, ki ji je ime Anonymous (slo. anonimen) – da je Anonymous en sam človek, čeprav so pod tem imenom kolektivno objavljali milijoni t. i. Anonov, anonimnih uporabnikov 4chan. Preko objav na 4chan se je kolektiv organiziral in izvajal različne spletne aktivnosti. Delovanje kolektiva je vedno motivirala ideja ali cilj, privlačen dovolj velikemu številu članov – po navadi je šlo samo za zabavo, pogosto precej žaljivo, vmes celo naravnost groteskno, večinoma pa daleč od resnih političnih in ideoloških tem. V tem obdobju so bile aktivnosti članov, ki so jih koordinirali preko 4chan pod uporabniškim imenom Anonymous, včasih vsaj nezakonite, če že ne naravnost zlonamerne. Posamezen član, ki anonimno sodeluje v dejavnosti kolektiva, je imenovan Anon (BBC Four 2014).

Ker se lahko pridruži prav vsak uporabnik interneta, ne obstaja en Anonymous ali ena stalna skupina Anonymous. Anonymous je resnično lahko prav vsak: srednješolec, pisarniški delavec, aktivist, borec za svobodo, mašnik ali kiberterorist; vsak, ki ima idejo ali stališče in ju je pripravljen izraziti. Anonymous nima vodstva in nima hierarhične strukture. Vsaka dejavnost ima mogoče nekaj vplivnih članov, ki so ob določenih trenutkih nekakšni de facto vodje, ki imajo največ vpliva na smer, v katero se kolektiv premika. Ena od Anonov, pod psevdonimom Homocranula, je potek dejavnosti opisala kot »jato ptic, ki skupaj leti zelo potihoma, potem pa ena ptica naenkrat zavije v svojo smer in sledi ji celotna masa jate« (BBC Four 2013). Če je določena ideja privlačna in navdihne dovolj veliko število uporabnikov interneta, se lahko takšna večja ali manjša skupina poveže in deluje kot Anonymous, ko si s pomočjo informacijske tehnologije prizadeva za njeno uresničitev. Vsak posamezni Anon lahko za tarčo predlaga karkoli in kogarkoli, in sicer od izkoriščevalske multinacionalke do razvajene srednješolke – če pritegne dovolj motiviranih Anonov, bodo začeli delovati za uresničitev ideje. Anonymous je torej neke vrste »internetni zbor«, ki se zbere okrog dovolj privlačne ideje in si s pomočjo uporabe interneta in informacijske tehnologije prizadeva za njeno uresničitev. Eden izmed Anonov je zbor opisal kot »multinacionalni, multikulturni,

multidimenzionalni zbor. Le-ta vključuje jude, ateiste, mormone, kristjane, hindujce, budiste, wiccane in unitariance, skratka kogarkoli, ki se je pripravljen zbrati in je pripravljen biti del kolektivne množice – del kolektivne množice interneta, skupine vseh, a nobenega posebej. Boj ene osebe za svobodo je boj vseh nas (Landers 2008, BBC Four 2014).«

V začetku leta 2008 pa se je skupnost zapletla v konflikt s Cerkvijo scientologije. Cerkev si je prizadevala cenzurirati zabaven posnetek njihovega člana, sicer vplivnega filmskega igralca, ki je pricurljal v javnost in močno zabaval širšo spletno skupnost, še posebej uporabnike 4chan. Anonymous tega »napada na zabavo kot njihovo najvišjo vrednoto« niso sprejeli mirno. Edini logičen odziv je bil, da se zberejo in v obrambo svojih vrednot udarijo po scientologiji, tako kot so to že storili v preteklosti, za realizacijo precej manj pomembnih potegavščin. Na nek način to ni bil samo napad na zabavo, ampak napad na hekersko etiko, ki je vsaj podzavestno temelj praktično vsake računalniške in internetne podkulture. Če bi preučevali nastanek in razvoj spletne skupnosti 4chan, bi videli, da ta v svojem bistvu močno spoštuje, celo temelji na hekerskih vrednotah. Na nek način izhaja iz teh vrednot tudi značilna »obsedenost z zabavo«. S serijo protestov, potegavščin in »hekov«, usmerjenih na Scientološko cerkev, šaljivo imenovanih Projekt Chanology, so samo za zabavo in obrambo le-te in hekerske etike, v duhu boja proti cenzuri in za svobodo informacij njihove aktivnosti postale izrazito ideološko in politično motivirane. Dejavnosti uporabnikov 4chan so postajale izrazito hektivistične. Projekt Chanology se je na koncu manifestiral celo v obliki resničnih protestov in zborovanj pred zgradbami scientološke cerkve, na katerih so udeleženci svojo anonimnost ohranjali z maskami Guya Fawkesa, ki se je tedaj že uveljavila kot uradni obraz Anonymous (BBC Four 2014).

Dejavnosti so pritegnile pozornost širše javnosti, predvsem aktivistično naravnanih uporabnikov interneta, politično motiviranih hekerjev in oklicanih hektivističnih skupin. Dejanja Anonymous so odmevala, ker so običajni uporabniki interneta z dejanji na spletu vplivali na oprijemljive spremembe v resničnosti. Gibanje se je napajalo iz teh uspehov in raslo. Anonymous je začel na nek način dozorevati, ko so sodelujoči začutili, da njihov glas nekaj velja, in razumeli, da moč prinaša odgovornost. Anonymous je hitro prerasel 4chan in Projekt Chanology. Posamezniki, že zdavnaj ne samo uporabniki 4chan, ampak celotnega spleta, so se v vedno večjem številu začeli zbirati pod imenom Anonymous, z namenom vplivanja na različna družbena vprašanja in protest proti kršenju človekovih pravic ter boj za svobodo informacij in proti protipiratski kampanji (BBC Four 2014).

5.3 Operacija Payback

5.3.1 Ozadje Operacije Payback.

Operacija se je pričela 17. septembra 2010, ko je indijsko podjetje AiPlex Software po naročilu Bollywoodskih studijev z DDoS napadom onesposobilo priljubljeno spletno stran za izmenjavo vsebine Pirate Bay. Podjetje je imelo s skupino Motion Pictures Association of America (MPAA), ki se ukvarja z zaščito avtorskih pravic, sklenjeno pogodbo, po kateri so spletne strani, ki so kršile avtorske pravice, obvestili, zatem pa izvajali DDoS napad s poplavljanjem, če se stran na obvestilo ni ustrezno odzvala. Protipiratski aktivisti so se začeli povezovati kot kolektiv Anonymous in so 17. septembra prvotno načrtovali direktni DDoS napad na spletno stran AiPlex Software, ampak jih je pri tem prehitel neznani heker, ki je v lastni režiji onesposobil omenjeno spletno stran. Kolektiv je hitro spremenil načrt in se odločil napasti MPAA in Mednarodno federacijo fonografske industrije (IFPI). Napad je povzročil skupno 30 ur nedostopnosti spletnih strani obeh organizacij. Čez dva dni je bil izveden še napad na spletni strani dveh drugih organizacij za avtorske pravice, tj. Ameriškega združenja snemalne industrije (RIAA) in Britanske fonografske industrije (BPI) (McLaughlin 2012, 62–66).

Dva dni po pričetku napadov je Anonymous svoja dejanja pojasnil z izjavo in jasno predstavil motivacijo za svoja dejanja in svoje cilje. Kolektiv je organizacijo obsodil poizkusa nadzora nad medmrežjem in izkoriščanja interneta za zaslužek. Pojasnili so, da ne morejo »stati križem rok in opazovati«, medtem ko pohlepne organizacije onemogočajo širjenje idej in napadajo posameznike, ki želijo v skladu s svojimi, po hekerski etiki, osnovnimi pravicami, samo deliti ideje z drugimi. Kolektiv je zagrozil, da bodo napadi trajali, dokler ne bodo informacije in podatki zares svobodni. Morda se zdi anarhično, celo naivno, ampak vodilni Anoni so se zavedali, kako pomembno je dobro artikulirati motivacijo za svoja dejanja, zato so svoja stališča sčasoma »rafinirali«. Anonymous so se odločili boriti za spremembo patentnih in avtorskih zakonov in ne za njihovo popolno prenehanje, kot je pojasnil eden izmed Anonov: »Poizkušamo razdelati naše ideale, da bi bili slišani in sprejeti. Nihče nas ne bo poslušal, če bo naš cilj legalizacija piratstva, ampak če poprosimo za spremembo avtorskih zakonov, skrajšanje njihovega trajanja na razumno dobo, bo vse precej bolj smiselno.« Operacija Payback ni temeljila na naivnih zahtevah o ukinitvi vseh protipiratskih zakonov, kot so mnogi napačno prepričani, ampak si je prizadevala za popolnoma realistične cilje (McLaughlin 2012, 62–66).

5.3.2 Nadaljevanje Operacije Payback.

DDoS napadi so prejeli precej medijske pozornosti, kar je navdihnilo sodelujoče, da napadejo še dve protipiratski odvetniški pisarni in znano britansko protipiratsko odvetniško pisarno ACS: Law. Anonymous so z DDoS napadom onesposobili uradno spletno stran ACS: Law in »d0xali (hekerski žargon za pridobiti zaupne podatke)« sistem podjetja, pri čemer je bilo razkritih precej občutljivih finančnih informacij in celo nepravilnosti v poslovanju (Enigmax 2010, McLaughlin 2012, 62–66).

Operacija se je začela kot protinapad na skupine, ki so napadle znano piratsko spletno stran Pirate Bay, ampak je sčasoma prerasla v boj proti »vsemu protipiratskemu«. Oktobra je skupina napadla portugalsko ministrstvo za kulturo, ki je septembra vložilo tožbo zoper Pirate Bay. Spletna stran ministrstva je bila najprej razobličena s sporočilom v podporo Pirate Bay, nekaj sekund kasneje pa tudi preusmerjena na naslov *thepiratebay.org*. Poleg tega je bil »d0xan« tudi elektronski poštni predal ministrstva, čeprav o morebitni pomembnosti vsebine elektronske pošte ni podatkov (Ernesto 2008). Isti mesec je Anonymous udaril tudi po znanem glasbeniku Genu Simmonsu, članu skupine KISS, ki je na spletu precej zbadajoče in provokativno obsodil kršenje avtorskih pravic in dejavnosti Anonymous. Kolektiv tega ni spregledal in je Simmonsovi spletni strani (simmonsrecords.com in genesimmons.com) z DDoS napadom onesposobil za skupno več kot 24 ur. Takoj po prenehanju napadov je Simmons ponovno podražil Anonymous, zato lahko predvidevamo, da ga le-ti niso pretirano prizadeli. Napadi na različne strani, ki so se borile proti kršenju avtorski pravic, so potekali do novembra, ko je bila napadena tudi spletna stran Ameriške pisarne za avtorske pravice, kar je označilo prvi napad na katerokoli vladno spletno stran. Napad na ameriško vladno stran je kasneje sprožil preiskavo FBI o aktivnostih Anonymous (Ernesto 2010b). Novembra so DDoS napadi na spletne strani različnih organizacij počasi potihnili. Marca 2011 je bilo izvedenih nekaj DDoS napadov za poizkus oživitve Operacije Payback, ki pa niso pritegnili dovolj pozornosti, zato so aktivnosti začele počasi izzvenevati (Anderson 2011). Operacija Payback je podobno kot Projekt Chanology navdihnil precej dejanskih uličnih aktivističnih aktivnosti, katerih podrobnosti pa za nalogo niso pomembne (McLaughlin 2012, 62–66).

5.3.3 Operacija Avenge Assange.

Z decembrom 2010 je Operacija Payback ponovno oživela. Vrhunec je bil dosežen z dogodki, povezanimi z WikiLeaks in poimenovanimi Operacija Avenge Assange oz. Operacija maščevanje Assangea, po ustanovitelju omenjene organizacije. Novembra 2010 so vplivne novinarske agencije The New York Times, The Guardian, Der Spiegel, Le Monde in El Pais

začele z objavo več kot četrt milijona ukradenih depeš, ki sta si jih izmenjevala Državni sekretariat ZDA in njihove diplomatske izpostave. Depeše je pod vodstvom Avstralca Juliana Assangea razkrivala neprofitna organizacija WikiLeaks, s ciljem preprečevanja državnih skrivnosti in svobode informacij (Daly 2011; McLaughlin 2012, 66–69).

Kmalu po objavi so mnoga večja podjetja prenehala poslovati z WikiLeaks, vključno z MasterCard, Visa, PayPal, Amazon.com, Apple, Bank of America, EveryDNS in WikiLeaksov ameriški ponudnik gostovanja Tableau Software. Spletni bančniki Mastercard, Visa in Paypal so celo zadržali del nakazanih sredstev. Na odločitve omenjenih podjetij je najbrž vplival politični pritisk, predvsem iz Washingtona. Da je šlo za nadzor nad informacijami pod pretvezo nacionalne varnosti in kopičenje informacij za povečanje lastnega dobička, je lahko eden izmed logičnih zaključkov (Daly 2011). Večja podjetja so sicer pojasnila, da so prenehala poslovati zaradi nezakonitosti WikiLeaks dejavnosti, kar pa je bil zelo slab argument. V zvezi z nezakonitostjo gre samo za špekulacije. Glede na to, da so vsa omenjena podjetja brez zadržkov poslovala in še vedno poslujejo s kriminalnimi posamezniki in skupinami, na primer z rasističnimi in neonacističnimi organizacijami, pa je takšna izjava očitno nekonsistentna. Upoštevajoč omenjeno, se je kolektiv Anonymous angažiral v svoji izjavi, »da na internetu velja samo sodba množice in da so dejanja korporacij nesprejemljiva, saj se uklanjajo vladnemu pritisku, po krivem obsojajo WikiLeaks, zatirajo svobodo govora ter so nekonsistentne in dvolične, saj kljub poslovanju z rasističnimi in s kriminalnimi organizacijami blokirajo WikiLeaks, ki pa ni kriminalna organizacija, ampak služi ljudem svobodnega sveta in uporabnikom interneta. Kaznovati WikiLeaks zaradi distribucije informacij, ki so osramotile vplivne, je sramota internetu, ki je ne nameravajo sprejeti« (Anonymous 2010; McLaughlin 2012, 66–69).

7. decembra 2010 je bilo izvedenih število DDoS napadov na spletne strani PayPal, MasterCard in Vise, ki so bile onesposobljene nekaj ur. Šlo je za precej velik uspeh, glede na to, da so njihove spletne strani ustvarjene za sprejemanje velike količine prometa. Kolektiv je poizkušal tudi z napadom na Amazon.com, ampak množica ni dosegla kritične mase, zato je spletna stran ostala dosegljiva. Po napadih je PayPal sprostil zadržana sredstva, namenjena WikiLeaks, vendar ni obnovil njihovega računa (McLaughlin 2012, 66–69).

Operacija Payback se je začela preprosto kot operacija za obrambo priljubljene spletne strani za deljenje vsebine The Pirate Bay, potem pa se je hitro spremenila v širšo protipiratsko kampanjo in postala simbol Anonymousove zavezanosti svobodi govora.

5.3.4 Metode in organizacija Operacije Payback.

Operacija je bila v klasičnem stilu Anonymous organizirana preko programa za spletno komuniciranje IRC. Na kanalu #command je bila skupina organizatorjev, medtem ko so na #operationpayback skupine posameznikov izvajale napade na cilje spletne strani – oba kanala sta bila odprta vsakomur, ki se je želel pridružiti. Dejavnosti so večinoma zaobjemale DDoS napade s poplavljanjem. Za večino le-teh je bila uporabljena prirejena različica programske opreme Low Orbit Ion Cannon (LOIC). Prirejena različica je imela dodan t. i. »hive-mind« način, ki je omogočil učinkovitejše povezovanje več računalnikov v »botnet« mrežo in lažji nadzor preko IRC, kar je močno olajšalo koordinacijo napadov in omogočilo hitro onesposabljanje ciljne spletne strani. Izdana so bila tudi podrobna navodila, kar je skupaj s prirejeno programsko opremo pomenilo, da je bilo sodelovati resnično preprosto in omogočeno prav vsakemu posamezniku z dostopom do računalnika in spleta. Sodelovalo ogromno število »skriptarjev« ob omejeni podpori sposobnih hekerjev (Constantin 2010; McLaughlin 2012, 62–69).

5.4 Arabska pomlad

5.4.1 Operacija Tunizija.

Z začetkom Arabske pomladi se je v podporo protivladnih protestov aktiviral tudi kolektiv Anonymous. 2. januarja 2010 so pričeli z Operacijo Tunizija, ko je bilo z DDoS napadenih veliko število tunizijskih vladnih spletnih strani: spletna stran predsednika, premierja, ministrstva za industrijo, ministrstva za zunanje zadeve, borze in stran vladne agencije, ki je cenzurirala spletne disidente, poljudno imenovane Ammar 404 (BBC Four 2014; McLaughlin 2012, 69–72).

Operacija Tunizija ima na nek način korenine v Operaciji Avenge Assange. Vsesplošna vladna cenzura interneta, še posebej pa cenzura tunizijskega dela WikiLeaks, je pritegnila pozornost Anonymous. Internetna svoboda v Tuniziji je bila zelo omejena. Vladne agencije so izvajale precej sofisticirane operacije, nadzirale državljane in celo uničevale njihovo spletno vsebino, če je ta izražala nezadovoljstvo z oblastjo. Tunizija ni imela prostega dostopa do spleta (BBC Four 2014; McLaughlin 2012, 69–72).

Anonymous je z izjavo na YouTube ponovno pojasnil, da so tunizijsko vlado obsojali nadzora nad informacijami, prikrivanja resnice, širjenja dezinformacij in omejevanja svoboščin svojih državljanov za lastno korist. Anonymous se je z videoizjavo zavezal pomoči zatiranim in boju proti nadzoru peščice nad večino. Napovedali so napad na vsako organizacijo, ki bo

poizkušala s cenzuro. Zanimivo je, da je sporočilo vsebovalo tudi širše opozorilo vladam celega sveta in Operacijo Tunizijo označilo za sporočilo celemu svetu in priporočilo vsem, ki bi želeli omejevati svobodo t. i. državljanov sveta (BBC Four 2014, McLaughlin 2012, 69–72).

Poleg tradicionalnih DDoS napadov, predvsem proti tunizijskim vladnim spletnim stranem, se je Anonymous angažiral kot še nikoli prej. Protestnikom so posredovali navodila za izogibanje vladnemu nadzoru ter so sestavili in s pomočjo tunizijskih članov med protestnike razdelili t. i. »paket za oskrbo«, ki je vseboval programsko opremo za preboj vladne blokade in dostop do spleta. Poleg tega so pomagali pri širjenju informacij o protestih iz države in o mednarodnem dogajanju v državo (BBC Four 2014; McLaughlin 2012, 69–72).

5.4.2 Operacija Egipt.

Tako kot Operacija Tunizija, je bila tudi Operacija Egipt primarno reakcija na vladno cenzuro. 26. januarja so bili izvedeni DDoS napadi na spletne strani egiptovskega kabineta, ministrstva za notranje zadeve ter ministrstva za komunikacije in informacijsko tehnologijo (BBC Four 2014; McLaughlin 2012, 70–72).

Kot navadno je Anonymousov računalniški glas v izjavi, objavljeni na spletni strani YouTube, artikuliral kolektivno motivacijo in cilje. Egiptovsko vlado je obsodil cenzuriranja lastnega ljudstva, kršenja temeljnih človekovih pravic s kršenjem pravice do svobode govora, svobode združevanja in prostega dostopa do informacij. Ponovno je napovedal napad na vsako organizacijo, ki bo podpirala takšno zatiranje (BBC Four 2014; McLaughlin 2012, 70–72).

DDoS napadi na vladne spletne strani so potekali nekaj dni, podobno kot v primeru Operacije Tunizija. Tako kot tunizijski protestniki so tudi Egipčani dobili navodila in svoj »paket za oskrbo« (BBC Four 2014, McLaughlin 2012, 70–72).

5.4.3 Metode in organizacija Operacij Tunizija in Egipt.

DDoS napadi so se ponovno izvajali s pomočjo prirejene programske opreme in s pomočjo IRC kanalov, na katerih sta bili operaciji organizirani. V obeh operacijah je sodelovalo ogromno število ljudi iz celega sveta, večinoma kot »skriptarji«, ki so svoje računalnike prostovoljno dodali v »botnet«. Zelo pomembno vlogo so odigrali sposobni tuji hekerji, ki so sestavili navodila in oba »paketa za oskrbo«, in lokalni tunizijski hekerji, ki so poleg sodelovanja v DDoS napadih imeli pomembno vlogo pri distribuciji »paketa za oskrbo«. Hekerji izven omenjenih držav so po spletu dostavili programsko opremo tunizijskim in

egiptovskim kolegom, ki so jo potem na različne načine delili naprej, predvsem preko fizičnih medijev in po spletu znotraj državne blokade. »Paket za oskrbo« za Tunizijo je vseboval Tor programsko opremo in »skripto« Greasemonkey, s katerim so državljani enostavno zaobšli vladno blokado, medtem ko je bil egiptovski paket bolj zapleten in je vseboval navodila za »dial-up« oz. osnovno vzpostavitev povezave preko telefonske linije, ker so oblasti državo praktično popolnoma odklopile od svetovnega spleta. Egiptovski »paket za oskrbo« je vseboval tudi praktična navodila za pomoč protestnikom v arabskem jeziku, na primer za preprečevanje posledic stika s solzivcem in osnove prve pomoči, navodila za bežanje pred organi pregona, obrambo pred policijskimi prsi, osnove taktike, maskiranje obraza in podobno (Claiborne 2011, Ryan 2011).

6 SKLEP

6.1 Vpliv in posledice Operacije Payback

DDoS napadi Operacije Payback so bili res številni in obširni, vendar večjih posledic vseeno niso imeli. Zaradi poplavljanja so bile strani nedostopne le za določen čas, njihova vsebina pa ni bila poškodovana. Določene organizacije so napade kritizirale z vidika omejevanja dostopa do informacij, saj uporabniki v času napadov niso mogli dostopati do vsebin. Prav tako je bilo omenjeno kršenje Gene Simmonsove svobode govora, medtem ko je bila njegova stran nedostopna. Kljub temu njegov odziv priča, da Simmonsa napadi niso pretirano prizadeli (CMU Editorial 2010). Sami napadi gotovo niso povzročili večje škode, čeprav je razumljivo, da jih določeni akterji, predvsem organizacije za zaščito avtorskih pravic in večja podjetja želijo prikazati kot takšne (McLaughlin 2012, 62–69).

Bolj kontroverzni se zdijo ukradeni podatki, zlasti »d0xana« vsebina podjetja ACS: Law, ki bi jo lahko označili vsaj za občutljivo, ker je razkrila določene podrobnosti in nepravilnosti v poslovanju. Če je bila to samo predstava za javnost, ni jasno, vendar je lastnik podjetja ACS:Law takoj po napadih izjavil, da ga »bolj skrbi, ko njegov vlak zamuja 10 minut ali ko mora v vrsti čakati na kavo, kot pa takšne neumnosti (McLaughlin 2012, 68).« Razkrita vsebina je ne glede na izjavo močno vplivala na poslovanje podjetja – kljub temu se to zdi bolj usluga javnosti kot kakršnakoli škoda, saj so bile navsezadnje razkrite nepravilnosti v poslovanju. Razkriti podatki iz poštnega predala ACAPOR niso vsebovali ključnih informacij (McLaughlin 2012, 62–69).

Operacija Payback sama ni prinesla direktnih in specifičnih zakonodajnih sprememb, kljub temu pa je bila njena velika baza podpornikov zagotovo ena izmed ključnih pri lobiranju proti Aktu za ustavitev piratstva (SOPA) in Aktu za zaščito IP (PIA) (Weisman 2012). Operacija je tudi močno osvetlila debato o avtorskih pravicah in svobodi govora, saj je pritegnila želeno pozornost in s tem gotovo vplivala na mnenje javnosti – kampanja ni bila neuspešna, čeprav ni neposredno povzročila oprijemljivih sprememb (McLaughlin 2012, 62–69).

Najbolj zanimivi s stališča ogrožanja varnosti oz. povzročanja materialne škode so DDoS napadi na spletne strani podjetij, ki so se decembra 2010 odločila, da bodo prenehala poslovati z WikiLeaks. Gre tudi za podjetja, katerih zaslužek je vsaj do neke mere odvisen od spletnih transakcij, zato je nedostopnost spletne strani verjetno pomenila zmanjšano sposobnost poslovanja, kar pomeni finančno izgubo in bi potencialno lahko vplivalo na vse zaposlene v podjetju, sploh če bi prišlo do omembe vredne škode. Podatkov o natančnih številkah ni zaslediti. Naše mnenje je, da napadov ne moremo opredeliti kot kiberkriminal. Konec koncev so podjetja tista, ki so neupravičeno zadrževala nakazana sredstva in s tem povzročala direktno finančno škodo, medtem ko so napadi mogoče povzročili nekaj posredne škode, o kateri pa sploh nismo prepričani. PayPal je sicer hitro spremenil stališče in sprostil sredstva, medtem ko sta MasterCard in Visa zadržala sredstva, dokler ju WikiLeaks s tožbo leta 2013 ni prisilil v sprostitev. Glede na to, da se velika podjetja večinoma niso dala motiti, napadi najbrž niso povzročili bistvene škode. Kljub temu, da so vse strani zdaj že sprostile sredstva WikiLeaksu, ki so mu bila namenjena že pred letom 2010, blokada poslovanja še vedno traja (WikiLeaks 2013). Tako kot Operacija Payback, tudi njen podaljšek, Operacija Avenge Assange, ni imela omembe vrednega direktnega vpliva. Ponovno pa so napadi pritegnili ogromno medijske pozornosti in osvetlili problematiko (McLaughlin 2012, 62–69).

Aktivnosti Anonymous so bile izrazito »hektivistične«, praktično že od samega začetka. Z Operacijo Payback je kolektiv dosegel novo stopnjo v artikulaciji svoje motivacije in ciljev – sčasoma so opustili svoja začetna nerealistična in pretirano idealistična prizadevanja ter so se odločili zasledovati resne in realistične cilje – vse to govori v prid premišljenosti in načrtovanemu delovanju, kar zagotovo ugodno vpliva na lagodje povprečnega posameznika, ki bi mu dejavnosti t. i. »uporniških hekerjev« utegnile povzročiti skrbi. Aktivnosti so bile že od samega začetka tudi izrazito politično motivirane, nenasilne in nezlonamerne, cilji jasno artikulirani in podprti s strani širše javnosti, metode pa hekerske. Čeprav je bila ob napadih na spletne strani večjih korporacij z Operacijo Avenge Assange povzročena vsaj posredna materialna škoda, niti slučajno ni šlo za delovanje za lastno korist, z namenom povzročanja

nevarnosti, vnašanja strahu ali uničevanja kakršnekoli, kaj šele ključne infrastrukture. Dejanja Operacije Payback in Operacije Avenge Assange niti slučajno niso dejanja kiberterorizma ali kiberkriminala, čeprav so bile določene aktivnosti v nasprotju z zapisanimi zakoni nekaterih držav in so bile zato deležne pozornosti organov pregona (McLaughlin 2012, 62–69). V dejavnostih obeh operacij je sodelovalo ogromno število ljudi, pritegnili pa so tudi veliko količino pozornosti, zaradi katere je debata o piratstvu in avtorskih pravicah postala resna tema. Morda edino v primeru PayPala operaciji res nista vplivali na neposredne spremembe, sta pa zagotovo vplivali posredno, tj. skozi širjenje ozaveščenosti in širjenje sporočila. Obe operaciji sta prikazali, da takšne vrste hektivizem ne ogroža varnosti posameznikov in je lahko v nasprotnem primeru celo metoda za izražanje posameznikovih vrednot in prizadevanja za njegove interese. V tem primeru lahko govorimo o obogatitvi prizadevanj za posameznikove interese in človekove pravice (McLaughlin 2012, 62–69).

6.2 Vpliv in posledice Operacij Tunizija in Egipt.

Z Operacijo Tunizija je bilo izvedenih osem uspešnih DDoS napadov na tunizijske vladne spletne strani. Vlada je bila prisiljena napadene strani odstraniti s svetovnega spleta, tako da so bile po napadih dostopne samo spletnemu prometu znotraj državne blokade. Napadi so očitno prizadeli tunizijske oblasti, ki so 5. januarja poizkušale odgovoriti s svojim DDoS napadom na Anonymousovo spletno stran. Oblasti so se tudi posebej aktivno angažirale proti hekerjem znotraj države, ko so v zvezi z DDoS napadi aretirale nekaj spletnih aktivistov in blogerjev (Ryan 2011).

Še posebej uspešni so bili napadi med egiptovsko revolucijo leta 2011, ko je kolektivu uspelo spletne strani sneti in obdržati nedosegljive do trenutka, ko je oblast priznala poraz (Somaiya 2011).

Največji prispevek pa sta imela oba »paketa za oskrbo« z navodili in programsko opremo za preboj spletnih blokad, ki sta pomagala mnogim Tunizijcem in Egipčanom ter revoluciji sami. V času, ko je vlada poizkušala uveljaviti svojo prevlado nad državljani ter ko jim je odrekala svobodo izražanja in dostop do interneta, so ljudje v obeh državah s pomočjo Anonymous zaobšli vladno cenzuro in se imeli možnost na spletu prikrito organizirati. S pomočjo paketa programske opreme se je zavedanje o dogajanju v obeh državah lahko razširilo po celem svetu (BBC Four 2014, McLaughlin 2012, 69–72).

Operaciji Tunizija in Egipt sta bili izrazito hektivistični. Ljudje po celem svetu so se zbrali v podporo zatiranim državljanom obeh držav. Motivacija za le-to je bila politična in ideološka,

hekerske in nezlonamerne dejavnosti pa sta poganjala empatija do zatiranih in prizadevanje za splošno dobro. V primeru obeh operacij lahko trdimo, da sta meli vsaj do neke mere celo neposredni vpliv na potek revolucije, predvsem s »paketom za oskrbo«. Protestniki v obeh državah so se z videoposnetki zahvalili Anonymous in prikazali veliko mero hvaležnosti, kar priča o prispevku kolektiva Anonymous (BBC Four 2013). Arabska pomlad je v naslednjem razvoju zavila v svojo smer, sledili pa so protesti v drugih državah bližnjega vzhoda, med katerimi pa je vloga Anonymous manj vidna in precej nejasna. V dogodkih, ki so sledili, težko govorimo o pravem »hektivizmu«. Takšen primer sta Libija in kasneje Sirija, kjer so se hekerji na obeh straneh, vladni in protivladni, oklicali za Anonymous ter zasledovali različne lastne bolj ali manj jasne cilje. Na podlagi tega menimo, da se hektivizem arabske pomladi začne ter konča z operacijama Tunizija in Egipt. Na podlagi analize lahko trdimo, da je hektivistična dejavnost v obeh primerih pozitivno vplivala na življenja posameznikov. Prav tako zopet ni govora o ogrožanju človekove varnosti. Tako kot pri prejšnjem primeru bi z lahkoto predstavili zelo dober argument ravno za nasprotno (BBC Four 2014, McLaughlin 2012, 69–72).

6.3 Hipoteza: Hektivizem ne predstavlja grožnje človekovi varnosti.

V prvem delu naloge smo prikazali, kako zelo pomembno je, da pravilno definiramo hektivizem in natančno ugotovimo, če v določenem primeru resnično lahko govorimo o hektivizmu, preden se lotimo poglobljene analize in učinka dejavnosti na človekovo varnost. S popotnico zmožnosti učinkovite identifikacije hektivizma smo zatem skozi oba primera najodmevnejše hektivistične dejavnosti ugotavljali, če je res šlo za hektivizem, kot smo ga denifirali, in ali je bila v primeru hektivistične dejavnosti na kakršenkoli način ogrožena človekova varnost.

Analiza prvega primera jasno prikaže, da človekova varnost v nobenem trenutku ni bila resno ogrožena. Ne le, da v primeru hektivizma ne moremo govoriti o omembe vrednem ogrožanju človekove varnosti, temveč je lahko hektivistična dejavnost celo metoda za izražanje vrednot in prizadevanja za uresničitev interesov z veliko podporo javnosti. Ko se skozi premišljeno, načrtovano dejavnost hektivizem razvija in dobiva smisel, to na nek način celo obratno sorazmerno vpliva na človekovo varnost. Omenjeno še nekoliko izraziteje potrjuje analiza drugega primera.

Zaradi tega lahko hipotezo brez dvoma potrdimo. Hektivizem, kot je definiran, namreč ne predstavlja grožnje človekovi varnosti. V drugem primeru lahko namignemo na pojav zrelega

hektivizma – kot političnega akterja, ki si prizadeva za višji cilj. Potencialno je lahko hektivizem celo orodje, ki lahko prispeva k človekovi varnosti, kot je ta opredeljena v širšem smislu, tj. z družbenim razvojem. Iz teh razlogov bi bilo v prihodnjih delih zagotovo potrebno preučiti, če in kako lahko hektivizem kot politični subjekt potencialno pozitivno vpliva na človekovo varnost.

7 LITERATURA

1. Anderson, Nate. 2011a. Anonymous revives Operation Payback, wages war on »copywrong«. *Ars Technica,* 9. marec. Dostopno prek: http://arstechnica.com/tech-policy/2011/03/anonymous-revives-operation-payback-targets-copywrong (18. september 2014).
2. --- 2011b. How one man tracked down Anonymous – and paid a heavy price. *Ars Technica,* 10. februar. Dostopno prek: http://arstechnica.com/tech-policy/2011/02/how-one-security-firm-tracked-anonymousand-paid-a-heavy-price/ (22. september 2014).
3. Andress, Jason in Steve Winterfeld. 2014. *Cyber Warfare: Second Edition.* Waltham: Elsevier.
4. Anonymous. 2010. *MasterCard Manifesto*. Dostopno prek: http://anonymousartwork.deviantart.com/art/Mastercard-Manifesto-189259509 (18. september 2014).
5. Aycock, John. 2006. Computer Viruses and Malware. *Advances in Information Security* 22:11–25.
6. Barwise, Mike. 2010. *What is an internet worm?* Dostopno prek: http://www.bbc.co.uk/webwise/guides/internet-worms (17. september 2014).
7. BBC Four. 2013. *How Hackers Changed the World: We are Legion*. London, 20. februar.

8. Bickford, Robert. 1989. *Are you a hacker?* Dostopno prek: http://www.textfiles.com/hacking/hacker.txt (16. september 2014).
9. Casserly, Martyn. 2012. What is Hacktivism? A short history of Anonymous, Lulzsec and the Arab Spring. *PC Advisor,* 3. december. Dostopno prek: http://www.pcadvisor.co.uk/features/internet/3414409/what-is-hacktivism-short-history-anonymous-lulzsec-arab-spring (17. september 2014).
10. Claiborne, Clay. 2011. Tunisian Anonymous activists take on Egyptian cause. *Daily Kos, 5.* februar. Dostopno prek: http://www.dailykos.com/story/2011/02/05/941329/-Tunisian-Anonymous-activists-take-on-Egyptian-cause (22. september 2014).
11. CMU Editorial. 2010. RIAA site goes down following LimeWire win. *CMU Daily,* 1. november. Dostopno prek: http://www.thecmuwebsite.com/article/riaa-site-goes-down-following-limewire-win (18. september 2014).
12. Coleman, Gabriella. 2011. Anonymous: From the Lulz to Collective Action. *The New Everyday,* 6. april. Dostopno prek: http://mediacommons.futureofthebook.org/tne/pieces/anonymous-lulz-collective-action (18. september 2014).
13. Constantin, Lucian. 2010. Anonymous DDoS Tool Gets Botnet Capabilities. *Softpedia,* 27. september. Dostopno prek: http://news.softpedia.com/news/Anonymous-DDoS-Tool-Gets-Botnet-Capabilities-158163.shtml (18. september 2014).
14. Daly, Angela. 2011. Private Power and New Media: The Case of the Corporate Suppression of WikiLeaks and its Implications for the Exercise of Fundamental Rights on the Internet. V *Human Rights and Risks in the Digital Era: Globalization and the Effects of Information Technologies,* ur. Christina M. Akrivopolou in Nicolaos Garipidis, 81–96. Hershey: IGI Global.
15. Denning, Dorothy E. 2001. Activism, Hacktivism and Cyberterrorism: An Internet as a Tool for Influencing Foreign Policy. *V Networks and Netwars: The Future of Terror, Crime and Militancy,* ur. Arquilla John in David Ronfeldt, 239–288. Santa Monica: RAND Corporation.
16. Dennis, Michael Aaron. 2014. Cybercrime. *Encyclopaedia Britannica.* Dostopno prek: http://www.britannica.com/EBchecked/topic/130595/cybercrime (17. september 2014).
17. Dibbell, Julian. 2009. *The Assclown Offensive: How to Enrage the Church of Scientology.* Dostopno prek: http://archive.wired.com/culture/culturereviews/magazine/17-10/mf_chanology?currentPage=all (18. september 2014).

18. Enigmax. 2010. ACS:LAW Anti-Piracy Law Firm Torn Appart by Leaked Emails. *TorrentFreak,* 25. september. Dostopno prek: https://torrentfreak.com/acslaw-anti-piracy-law-firm-torn-apart-by-leaked-emails-100925 (18. september 2014).
19. Ernesto. 2010a. Movie Rental Outfit Hacked, Emails Leaked, Redirected to The Pirate Bay. *TorrentFreak,* 18. oktober. Dostopno prek: https://torrentfreak.com/movie-rental-outfit-hacked-emails-leaked-redirected-to-the-pirate-bay-101018 (18. september 2014).
20. --- 2010b. Behind the Scenes At Anonymous' Operation Payback. *TorrentFreak,* 15. november. Dostopno prek: https://torrentfreak.com/behind-the-scenes-at-anonymous-operation-payback-111015 (18. september 2014).
21. Hampson, Noah C.N. 2012. Hacktivism: A New Breed of Protest in a Networked World. *Boston College International and Comperative Law Review* 35 (2): 511–542.
22. Himma, Kenneth Einar. 2005. Hacking as Politically Motivated Digital Civil Disobedience: Is Hacktivism Morally Justified? Seattle: Pacific University.
23. IBM Community Developement Foundation. 1997. *The Net Result – Report of the National Working Party for Social Inclusion.* London: IBM United Kingdom Limited, Corporate Affairs, Community Developemenent Foundation.
24. Janssen, Cory. 2014. *Technopedia explains Hacktivism*. Dostopno prek: http://www.techopedia.com/definition/2410/hacktivism (17. september 2014).
25. Jordan, Tim in Paul Taylor. 2004. *Hacktivism and Cyberwars*. London: Routledge.
26. Kaplan, Dan. 2008. DDoS hack attack targets Church of Scientology. *SC Magazine,* 25. januar. Dostopno prek: http://www.scmagazine.com/ddos-hack-attack-targets-church-of-scientology/article/104588 (18. september 2014).
27. Kovačič, Matej. 2008. *Seminar preiskovalnih sodnikov o Kiberkriminalu*. Podčetrtek, 16. maj.
28. Kostadinov, Dimitar. 2012. *Cyberterrorism defined (as distinct from cybercrime)*. Dostopno prek: http://resources.infosecinstitute.com/cyberterrorism-distinct-from-cybercrime (17. september 2014).
29. Landers, Chris. 2008. *Anonymous Takes On Scientology*. Dostopno prek: http://www2.citypaper.com/arts/story.asp?id=15543 (17. september 2014).
30. Levy, Stephen. 1984. *Hackers: Computer Heroes of the Computer Revolution*. New York: Delta Trade Paperbacks.
31. Li, Xiang. 2013. Hacktivism and the First Amendment: Drawing the Line Between Cyber Protests and Crime. *Harvard Journal of Law & Technology* 27: 302–323.

32. Majoras, Deborah Platt, Orson Swindle, Thomas B. Leary, Pamela Jones Harbour in Jon Leibowitz. 2005. Monitoring Software on Your PC: Spyware, Adware and Other Software. Washington: Federal Trade Comission.
33. Mansfield-Devine, Steve. 2011. Hacktivism: assessing the damage. Network Security (8): 5–13.
34. McCormick, TY. 2013. Hacktivism: A Short History. *Foreign Policy,* 29. april. Dostopno prek: http://www.foreignpolicy.com/articles/2013/04/29/hacktivism (17. september 2014).
35. McLaughlin, Victoria. 2012. *Anonymous: What do we have to fear from hacktivism, the lulz and the hive mind?* Charlottesville: University of Virginia.
36. NATO. 2008. *Cyber defence concept MC0571*.
37. Prezelj, Iztok. 2008. Človekova varnost v teoriji in praksi. *Delo in varnost* LIII (6): 17–26.
38. Republic of Turkey Ministry of Justice. 2014. *Cybercrime Essay.* Dostopno prek: http://www.justice.gov.tr/e-journal/pdf/cybercrime_essay.pdf (16. september 2014).
39. Rosenau, J.N. in J.P Singh. 2002. *Information Technologies and Global Politics: The Changing Scope of Power and Governance.* Albany: State University of New York Press.
40. Ryan, Yasmine. 2011. *Tunisia's bitter cyberwar*. Dostopno prek: http://www.aljazeera.com/indepth/features/2011/01/20111614145839362.html (22. september 2014).
41. Samuel, Alexandra Whitney. 2004. *»Hacktivism and the Future of Political Participation«*. Cambridge: Harvard University.
42. Siedschlag, A. 2002. Krieg im 21. Jahrhundert – »Zuruck in die Zukunft«? *WeltTrends* 35: 11–16.
43. Singel, Ryan. 2008a. *Anonymous Hacker Shoot For Scientologists, Hit Dutch School Kids.* Dostopno prek: http://www.wired.com/2008/01/anonymous-hacke (18. september 2014).
44. --- 2008b. *Anonymous Hackers Track Saboteur, Find and Punish the Wrong Guy – UPDATED*. Dostopno prek: http://www.wired.com/2008/01/anonymous-hac-1 (18. september 2014).
45. Slobbe, J. in S.L.C Verberkt. 2012. *Hacktivists: Cyberterrorists or Online Activists*. Nijmegen: Radboud University.

46. Somaiya, Ravi. 2011. Hackers Shut Down Government Sites. *The New York Times,* 2. februar. Dostopno prek: http://www.nytimes.com/2011/02/03/world/middleeast/03hackers.html?_r=4& (22. september 2014).
47. Stohl, Michael. 2007. Cyber terrorism: a clear and present danger, the sum of all fears, breaking point or patriot games? *Crime, Law and Social Change* 46 (4): 223–238.
48. Svete, Uroš. 2005. *Varnost v informacijski družbi.* Ljubljana: Fakulteta za družbene vede.
49. *The Observer*. 2013. *Digital revolution: time to question our love affair with new tech,* 10.marec. Dostopno prek: http://www.theguardian.com/commentisfree/2013/mar/10/new-technology-bleak-or-brave (16. september 2014).
50. Thomas, Julie L.C. 2001. *Ethics of Hacktivism.* London: SANS Institute.
51. UCSB. 2014. *What is the difference between a computer virus and a computer worm?* Dostopno prek: http://scienceline.ucsb.edu/getkey.php?key=52 (17. september 2014).
52. Virginia Tech Department of Computer Science. 1997. *The Hacker's Code of Ethics.* Dostopno prek: http://courses.cs.vt.edu/professionalism/WorldCodes/Hackers.Code.html (14. februar 2015).
53. Vogrin, Andreja, Iztok Prezelj in Bojko Bučar, 2008. *Človekova varnost v mednarodnih odnosih.* Ljubljana: FDV.
54. *Why We Protest*. Dostopno prek: http://whyweprotest.net (18. september 2014).
55. Weisenthal, Joe. 2011. Notorious Hacker Group LulzSec Just Announced That It's Finished. *Business Insider,* 25. junij. Dostopno prek: http://www.businessinsider.com/lulzsec-finished-2011-6?op=1(22. september 2014).
56. Weisman, Jonathan. 2012. After an Online Firestorm, Congress Shelves Antipiracy Bills. *The New York Times,* 20. januar. Dostopno prek: http://www.nytimes.com/2012/01/21/technology/senate-postpones-piracy-vote.html?_r=2& (18. september 2014).
57. WikiLeaks. 2013. *MasterCard breaks ranks in WikiLeaks blockade*. Dostopno prek: https://wikileaks.org/MasterCard-breaks-ranks-in.html (18. september 2014).
58. Wilson, Clay. 2005. *Computer Attack and Cyberterrorism: Vulnerabilities and Policy Issues for Congress. CRS Report for Congress*. Dostopno prek: http://www.iwar.org.uk/cyberterror/resources/crs/45184.pdf (1. junij 2015).
59. Wray, Stefan. 1998. *The Electronic Disturbance Theater and Electronic Civil Disobediance.* Dostopno prek: http://www.thing.net/~rdom/ecd/EDTECD.html (17. september 2014).