UNIVERZA V LJUBLJANI

FAKULTETA ZA DRUŽBENE VEDE

Ula Ušeničnik

Hekerstvo kot grožnja obveščevalni dejavnosti

Magistrsko delo

Ljubljana, 2015

UNIVERZA V LJUBLJANI

FAKULTETA ZA DRUŽBENE VEDE

Ula Ušeničnik

Mentor: izr. prof. dr. Uroš Svete

Hekerstvo kot grožnja obveščevalni dejavnosti

Magistrsko delo

Ljubljana, 2015

Hekerstvo kot grožnja obveščevalni dejavnosti

V današnjem času so podatki najbolj dragocena dobrina, ki jo lahko posedujemo. S prvega mesta so izrinili tako hrano kot naravne vire, postali pa so celo svoj premoženjski razred. Od podatkov ne živijo samo posamezniki in podjetja, pač pa tudi države oziroma njihovi organi nadzora. S porastom pomembnosti podatkov in informacij se je povečala tudi zlonamerna uporaba. Zaradi vrednosti, ki jo ta dobrina predstavlja, se število akterjev, ki bi jo radi izkoristili – in v mnogih primerih jo – povečuje iz dneva v dan. Ne gre samo za željo države po nadzoru nad svojimi državljani, ki etično mejo lahko hitro prestopi; okoristiti se želijo tudi posamezniki, katerih motivi so predvsem finančno pridobivanje s škodovanjem drugim posameznikom, podjetjem in državam. In hekerstvo, kot danes na široko označujemo takšna dejanja, je postalo velika grožnja vsem. Ta magistrska naloga se bo osredotočila na hekerstvo kot grožnjo državam in obveščevalnim dejavnostim, raziskala bo tako grožnjo samo kot možne rešitve problematike.

Ključne besede: hekerstvo, obveščevalna dejavnost, grožnja, HACKINT

Hacking as a threat to Intelligence

These days, data is the most important commodity we can possess. It has surpassed even food and natural resources, and become its own category of wealth. And it’s not only individuals and companies that thrive on data, but also countries and their surveillance authorities. With the increasing importance of the commodity, the number of parties trying to exploit it – and often succeeding – is on the rise as well. And not only do countries trying to police their citizens via surveillance that can easily cross an ethical line; there are also individuals trying to profit by causing damage to other individuals, companies and countries. Hacking, as we broadly refer to such actions today, has become a great threat to all. This MA thesis focuses on hacking as a threat to countries and intelligence services, with research on the threat itself, as well as possible solutions to the problem.

Keywords: hacking, Intelligence, threat, HACKINT

KAZALO

SEZNAM KRATIC

AKOS	Agencija za komunikacijska omrežja in storitve Republike Slovenije
ARPANET	angl. *Advanced Research Projects Agency Network* (Mreža Agencije za projekte naprednejšega raziskovanja)
CEO	angl. *Chief executive officer* (generalni direktor)
CIA	angl. *Central Intelligence Agency* (Centralna obveščevalna agencija Združenih držav Amerike)
DDoS	angl. *Distributed Denial of Service* (napad za zavrnitev storitve)
ENISA	Evropska agencija za varnost omrežij in informacij
EU	Evropska unija
FBI	angl. Federal Bureau of Investigation (Zvezni preiskovalni urad Združenih držav Amerike)
HACKINT	angl. *Hacking Intelligence*
HUMINT	angl. *Human Intelligence*
IKT	Informacijsko-komunikacijska tehnologija
MI5	angl. *Military Intelligence, Section 5* (Vojaška obveščevalna služba, skupina 5)
NATO	angl. *North Atlantic Treaty Organisation* (Organizacija severnoatlantskega sporazuma)
NSA	angl. *National Security Agency* (Agencija za državno varnost Združenih držav Amerike)
OSINT	angl. *Open-source Intelligence*
OVSE	Organizacija za varnost in sodelovanje v Evropi
OZN	Organizacija združenih narodov
RS	Republika Slovenija

SSKJ	Slovar slovenskega knjižnega jezika
SWOT	angl. *Strengths, Weaknesses, Opportunities, Threats* (prednosti, slabosti, priložnosti, grožnje)
ZDA	Združene države Amerike
ZTP	Zakon o tajnih podatkih

1 UVOD

Živimo v moderni informacijski družbi, ki jo poganja globalizacija. Vse skupaj se je začelo s tako imenovano McDonaldizacijo,[1] nadaljuje pa se v svetu tehnologije. Globalizacija je povzročila vse večjo povezanost ljudi po svetu in s tem vse več informacij (Aldrich 2004, 732). Napredek v tehnologiji je v informacijski družbi izjemno hiter. A nobena tehnologija se ne razvija tako hitro kot informacijska in nobena dejavnost družbe se ne spreminja tako hitro, kot ljudje obdelujemo informacije. O tem je pisal že Gordon Moore, soustanovitelj podjetja Intel, ki ima po sebi poimenovan tudi zakon – Moorov zakon. Ta pravi, da se število tranzistorjev na integriranjem vezju podvoji vsako leto, s čimer se povečuje moč procesorjev. Pozneje je pravilo popravil na dvoletno frekvenco, ki so jo strokovnjaki skrajšali na približno 18 mesecev. A mnogi menijo, da zakon ne velja več, predvsem zato, ker je Intel že dvakrat izpustil dvoletno nadgradnjo (Clark 2015). Prav tako se je spremenil način, kako ljudje uporabljamo informacije in z njimi komuniciramo. Obveščevalna dejavnost je imela močan vpliv na razvoj tehnologije in na to, kako ljudje uporabljamo informacije. Obstajajo pa ocene, da je obveščevalna dejavnost začela zaostajati za tehnologijo, saj ne sledi več spremembam, ki se odvijajo v moderni družbi (Berkowitz 1996, 35–36). Prav ta razkorak pa izkoriščajo osebe, ki želijo škodovati obveščevalni dejavnosti (Aldrich 2004, 734).

Preusmeritev družbe s fokusiranja na industrijo se je začela že v 60. in 70. letih prejšnjega stoletja, predvsem v ZDA in na Japonskem, ko je postajalo vse bolj jasno, da se družba spreminja v družbo znanja in informacij (*knowledge society* in *informationalized society*). S tem je pomen pridobila tudi tehnologija, predvsem informacijska tehnologija. Vse skupaj se je začelo zaradi ekonomskih kriz v sedemdesetih, ko je bila uporaba IKT usmerjena v izboljšanje produktivnosti in spodbujanje tekmovalnosti (Taylor in Zhang 2008, 3). Enajsti september 2001 je bil zadnji mejnik, ki je še dodatno podkrepil osredotočanje na računalnike, informacijsko tehnologijo in varnost, še posebej na vprašanja varovanja digitalne infrastrukture, elektronskega nadzora, uporabe hekerstva s strani teroristov in interneta kot sredstva za komunikacijo med državami in proti njim (Latham v Hansen in Nissenbaum 2009, 1155–1156).

[1] '*McDonaldiation*' je proces, s katerim so začela načela restavracij s hitro prehrano prevladovati ne samo v ZDA, ampak tudi drugod po svetu (Keel 2010).

Informacijsko družbo zaznamuje predvsem izločitev informacij iz kulturnega in fizičnega konteksta ter njihovo obravnavanje kot samostojnega objekta. Ločitev je omogočila razvoj mnogih IKT in oblikovala organiziranost moderne družbe (Ramage 2011, 10). Podatki oziroma informacije so danes najbolj zaželena dobrina. S prvih mest so izrinile hrano in naravne vire. Po podatkih Svetovnega gospodarskega foruma so podatki danes svoj premoženjski razred. Facebook je vreden kar 36,5 milijarde dolarjev, Googlova vrednost presega 65 milijard dolarjev in je tik za Microsoftom (skoraj 70 milijard dolarjev), Apple pa na prvem mestu podira vse rekorde z več kot 145 milijardami dolarjev. Prav vsem je skupna ena dobrina – podatki (McCann 2013; Forbes 2015). In od teh živijo tudi obveščevalne agencije. Njihovo delo se namreč vrti okrog zbiranja podatkov, vrednotenja zbranih podatkov, razvrščanja, analiziranja in končno distribucije teh podatkov (Hočevar 2011).

Danes je eden najpomembnejših medijev družbenih konstruktov zagotovo IKT, kibernetska politika pa je po mnenju Rothkopfa (Rothkopf v Svete 2006, 62) prihodnost politike. IKT je v zaznavo varnosti vnesel percepcijo stvarnosti – lahko gre za IKT, ki ogroža sodobne družbe, ali pa za uporabo te tehnologije v modernih konfliktih in nacionalno-varnostnih sistemih držav. Predvsem sta se spremenili zaznavi časa in prostora, zato je njeno zgolj tradicionalno preučevanje nemogoče (Svete 2006, 62).

Kljub mnogim definicijam, kaj hekerstvo je, je še danes dokaj nejasno, kaj zares točno obsega. Definicije se razhajajo do te mere, da so po enih hekerji kriminalci in škodljivci, po drugih pa so tisti pravi hekerji računalniški mojstri, ki obvladajo izdelavo programov, nudijo pomoč itd. Razhajanje v definicijah je opisano v nadaljevanju. Obenem je hekerstvo nekaj, kar je nezaželeno, saj je ne glede na definicije pogosto škodljivo. Gre za težavo, ki se jo mnogi trudijo odpraviti na raznorazne načine.

Medtem ko je internet povzročil revolucijo v načinu komuniciranja in trgovanja, je obenem omogočil izvajanje anonimnega kriminala, ki ga lahko izvaja kdor koli, kjer koli na svetu, s tem pa lahko povzroči hude posledice. Medmrežni kriminal pride v različnih oblikah, kot sta na primer spletna kraja in prevara. Cilj drugih hekerjev je lahko tudi razdiranje kod, tekmovanje med seboj, pravice do samohvale o napadu itd. V vsakem primeru so posledice napada pogosto hude, v najslabšem primeru mora napadena entiteta hitro popraviti 'luknjo', skozi katero je prišel napadalec (Wible 2003, 1577–1578). Med hladno vojno so države vedno vedele, kdo je njihov nasprotnik in kdo je zato kriv za napad nanje. Danes lahko prav vsak kupi poceni računalnik in ga uporabi za izdelavo orožja za masovno uničenje, in to kar iz

domačega naslonjača (Frontline 2014). Hekerji so ena izmed groženj zato, ker so stalna grožnja. So prilagodljivi, se razvijajo, in ne glede na to, koliko denarja je vloženega v preventivo, nikoli ne bo dovolj za popolno zaustavitev grožnje (Barak 2012). Ena izmed njihovih najbolj ogrožajočih sposobnosti je izjemno hitra formulacija ogromne geografsko razširjene skupine za napad (Tobias 2012).

Hekerji predstavljajo asimetrično grožnjo, kar je za moderni svet že običajno, a gre za obratno asimetrijo: manjši in 'šibkejši' akterji, običajno posamezniki ali manjše skupine, napadajo večje (številčnejše) in močnejše akterje, kot so na primer obveščevalne agencije ali države, v katerih so obveščevalne agencije. V asimetričnih konfliktnih naj bi manjše sile skušale uveljaviti lastno voljo in interese ter s tem spremeniti ravnotežje moči. To velja predvsem za čas po hladni vojni, ko je globalizacija postala pojav, ki ima vpliv ne samo na politične, ekonomske in druge sfere, pač pa tudi na varnostno okolje in delovanje vseh akterjev v nacionalno-varnostnem sistemu (Svete in drugi 2010, 247).

Ni vsaka hekerska dejavnost ilegalna; beseda *'hacker'* sama po sebi ni zla in ne pomeni 'kriminalec': poznamo tako imenovane bele hekerje (*white hats*), ki pomagajo odkrivati napake v informacijskih sistemih, da jih organizacije ali podjetja lahko popravijo in s tem preprečijo morebitne napade hekerjev, katerih namen je povzročanje škode (črni hekerji ali *black hats*) (Hoffman 2013; Crovitz 2013).

Pa so hekerski napadi grožnja tudi za nacionalno varnost? Strokovnjaki menijo, da so. Dokaz, kako resna grožnja so lahko, je primer napada na Estonijo leta 2007, ko je napad na vso glavno infrastrukturo (mediji, banke, ministrstva, podjetja in drugi akterji) v državi povzročil zaustavitev celotne družbe za tri tedne. Šlo je za prvi primer napada v t. i. peti dimenziji na državo, kar je sprožilo velik preplah (Traynor 2007; Singel 2009).

Prav iz zgoraj naštetih razlogov raznorazna podjetja in agencije hekerje vse bolj rekrutirajo v svoje vrste. S tem si povrnejo del prednosti, ki jo imajo sicer v rokah napadalci. Osebe, ki pomagajo podjetjem, organizacijam ali agencijam, ki so tarče napada, navadno izhajajo iz zasebnega sektorja. Ponudbe za delo ljudem z izkušnjami v hekerstvu so se med letoma 2012 in 2013 povečale za kar 17 odstotkov (Tobias 2012; Zito Rowe 2013).

2 METODOLOŠKI OKVIR

2.1 OPREDELITEV PREDMETA IN CILJEV PREUČEVANJA

Predmet preučevanja v magistrski nalogi je hekerstvo kot problem obveščevalne dejavnosti. Hekerstvo je široko razširjen fenomen, ki ne ogroža zgolj navadnih uporabnikov vseh vrst tehnologij. S svojo vsesplošno prisotnostjo na spletu, ki ga uporabljajo tako fizični uporabniki kot službe, agencije, združenja idr., je grožnja prav vsem, saj med žrtvami ne dela velikih razlik.

Glavni cilj magistrske naloge je predstaviti hekerstvo kot eno izmed groženj obveščevalni dejavnosti. Moj namen je predstaviti grožnje na splošno, izpostaviti in analizirati hekerstvo ter poleg teoretične podlage dodati tudi pravno podlago in analizo primerov. S tem sem poskusila prikazati, ali je hekerstvo med večjimi ali manjšimi grožnjami tako obveščevalni dejavnosti kot državam na splošno.

Cilj analize primerov je prikazati, s kakšnimi grožnjami so se v preteklosti že srečale obveščevalne službe. Analiza bo pokazala, kdo je bil glavni akter, kdo so bile tarče in kdo je bil v ozadju na strani napadalcev. Cilj analize je prikazati obe strani napada v kar se da jasni luči, da bo primerjava med primeri čim uspešnejša.

Še eden od ciljev magistrske naloge je prikazati HACKINT in njegovo implementacijo v obveščevalno dejavnost. Raziskala sem namreč, ali je bila implementacija uspešna rešitev za zmanjšanje nevarnosti hekerstva. Obenem sem omenila še hektivizem, ki je nova in široko razširjena oblika demonstriranja v moderni družbi.

2.2 RAZISKOVALNO VPRAŠANJE IN HIPOTEZE

Glavno vprašanje, ki me je vodilo pri pisanju magistrske naloge, je: *Ali je hekerstvo grožnja (oziroma izziv) obveščevalni dejavnosti?*

Pri pisanju magistrske naloge sem se opirala tudi na dve hipotezi.

H1: Notranje grožnje hekerjev so za obveščevalno dejavnost nevarnejše kot zunanje.

H2: HACKINT je bila uspešna rešitev za zmanjšanje nevarnosti hekerstva, ki jo ta povzroča obveščevalni dejavnosti.

2.3 METODOLOGIJA

Pri pisanju magistrske naloge sem uporabila več različnih metod zbiranja in analiziranja podatkov. Uporabila sem šest različnih metod: metodo zbiranja primarnih in sekundarnih virov, deskriptivno metodo, analizo in interpretacijo sekundarnih virov, primerjalno metodo, metodo študije primera in SWOT-analizo.

Metoda zbiranja primarnih in sekundarnih virov: zbiranje virov za analizo je predpogoj za uporabo sledečih metod.

Deskriptivna metoda: z metodo opisovanja sem opisala in predstavila temeljna teoretična izhodišča na področju obveščevalne dejavnosti in hekerstva. Pri tem sem uporabila domačo in tujo literaturo v obliki knjig in člankov, ki so dostopni tako v tiskani obliki kot na spletu. S to metodo sem opisala, kaj sta obveščevalna dejavnost in hekerstvo, kaj je HACKINT in kaj je hektivizem. Prav tako mi je ta metoda pomagala raziskati in opisati pravne okvire hekerstva tako na ravni države kot na ravni mednarodne skupnosti.

Analiza in interpretacija sekundarnih virov: pregledala in analizirala sem relevantne monografije, članke in druge spletne vire v povezavi s tematiko magistrske naloge na področju obveščevalne dejavnosti in hekerstva. Ta metoda mi je pomagala prikazati, ali je hekerstvo izziv oziroma grožnja obveščevalni dejavnosti. Obenem sem s to metodo pokazala tudi notranje in zunanje grožnje hekerstva ter morebitno grožnjo, ki jo lahko hekerstvo predstavlja nacionalni varnosti držav, ter hkrati raziskala, kako uspešna je bila implementacija dejavnosti HACKINT.

Primerjalna metoda: primerjala sem različne grožnje, s katerimi se srečuje obveščevalna dejavnost, predvsem pa sem se osredotočila na grožnjo hekerstva. Ker sem razločevala med zunanjimi in notranjimi grožnjami v okviru hekerstva, sem jih med seboj tudi primerjala. Prav tako sem primerjala izbrane primere hekerstva iz zgodovine in analizirala, kakšno stopnjo grožnje so predstavljali obveščevalni dejavnosti in/ali državam.

Metoda študije primera: izbrala sem si več primerov hekerstva oseb in držav v sisteme obveščevalnih dejavnosti, predvsem odmevne primere, ki so prišli v medije, in jih preštudirala.

SWOT-analiza: HACKINT kot dejavnost sem preučila s štirih polov – prednosti, slabosti, priložnosti in groženj ter jih primerjala med seboj. Tako sem dodatno preučila, ali je implementacija dejavnosti v obveščevalno dejavnost primerna.

3 TEMELJNI POJMI

3.1 HEKERSTVO

Hekerstvo je splošno gledano skupek dejanj, ki ga opravljajo hekerji. Znotraj nove sfere kriminala, ki zajema računalniška kazniva dejanja, je hekerstvo pogostvo obravnavano kot svoja kateogija, kamor spadajo vdiranje v sisteme, onemogočanje delovanja spletnih strani ali dejavnosti neke strani oziroma podjetja, namerno nastavljanje virusov in druge škodljive programske opreme, ki poškoduje omrežja in naprave. Hekerji prav tako nastavljajo pasti, v katere se ujamejo nevedni uporabniki in tako hekerjem predajo osebne informacije, številke kreditnih kartic ipd. (*phishing*). Motivacija za izvedbo kibernetskih napadov je lahko velika; napadalci ali skupine lahko segajo od tistih, ki le iščejo informacije, da jih prodajo naprej, do interesnih skupin, ki želijo onemogočiti celotne družbe, in celo do terorističnih skupin, ki si želijo ohromiti vladne službe (Turgeman-Goldschmidt 2005, 8; FindLaw UK 2015).

Hekerstva ne sestavljajo zgolj zlonamerna dejanja, kar je podrobneje opisano v nadaljevanju magistrskega dela. Za potrebe naloge se bom sicer opirala na zgornjo definicijo.

3.2 OBVEŠČEVALNA DEJAVNOST

Obveščevalna dejavnost se lahko definira tako v ožjem kot širšem pomenu. Po Richelsonu (Richelson v Brezovšek in Črnčec 2010, 118) jo širši pomen opredeljuje kot »izdelek, ki nastane z zbiranjem, obdelavo, integracijo, analizo, vrednotenjem in interpretacijo razpoložljivih podatkov v zvezi s tujimi državami ali območji«, ožji pomen pa, da »obveščevalna dejavnost zajema samo zbiranje in analiziranje podatkov in njihovo transformacijo v obveščevalni produkt; vendar so protiobveščevalna dejavnost in tajne operacije prepletene z obveščevalno dejavnostjo« (Brezovšek in Črnčec 2010, 118).

Obveščevalna dejavnost ne obsega samo čistih podatkov, čeprav je to njena osnovna in najobširnejša naloga. Med pomembne naloge obveščevalnih služb spada analiza teh podatkov, saj je dejanska vrednost podatkov vidna šele, ko so analizirani. Med preostale naloge spadajo še prikrite dejavnosti (*covert action)* in protiobveščevalna dejavnost, kjer se uporablja različne metode, med njimi prikrivanje ali namerno zavajanje, da se zaščiti lastne informacije pred nasprotniki (Herman 2001, 4; Shulsky in Schmitt 2002, 2, 8).

Obveščevalna dejavnost ni samo zunanja dejavnost. Vsaka država mora skrbeti tudi za dogajanje znotraj svojih meja, saj grožnje obstoju države lahko izhajajo tudi iz posameznikov ali skupin na domačem ozemlju (Shulsky in Schmitt 2002, 4).

Varnostna dejavnost je po Anžiču (Anžič v Brezovšek in Črnčec 2010, 118) opredeljena »kot dejavnost, ki pretežno temelji na ukrepanjih (tudi preventivnih) na osnovi 'policijskih' pooblastil, vključno tudi s pravico do posebnih operativnih metod in sredstev dela, ki jih tudi uporabljajo obveščevalne službe« (Brezovšek in Črnčec 2010, 119). Varnostno dejavnost definira tudi Purg, in sicer kot »preprečevanje, preiskovanje in odpravljanje določenih oblik ogrožanja varnosti, v tem primeru države«. Purg še piše, da je v primerjavi z obveščevalno dejavnostjo, pri kateri gre bolj za zbiranje in analiziranje podatkov ter njihovo obveščanje, varnostna dejavnost predvsem ukrepanje, ki se po načinu in sredstvih razlikuje od metod in sredstev obveščevalne dejavnosti. Varnostno dejavnost opravljajo temu namenjene varnostne službe in policija (Purg 1995, 34–35).

3.2.1 PROTIOBVEŠČEVALNA DEJAVNOST

V okvir obveščevalne dejavnosti spada tudi protiobveščevalna dejavnost. Ta »obsega pridobivanje vseh podatkov in izvajanje aktivnosti z namenom ocenitve tujih obveščevalnih in varnostnih služb ter onemogočanja delovanja sovražnih služb.« Protiobveščevalna dejavnost se ne sme enačiti s protivohunsko dejavnostjo, ki se ukvarja izključno s preprečevanjem tujim vladam, da bi nezakonito pridobivale državne tajnosti (Richelson v Brezovšek in Črnčec 2010, 119). Po SSKJ (2015) je definicija besede *protiobveščevalen* »ki odkriva in preprečuje delovanje sovražnikovih obveščevalcev«, sorodni izraz pa je tudi *kontraobveščevalen*. Gre za zelo posplošen pojem, saj naloge protiobveščevalne dejavnosti zajemajo tudi varovanje in zaščito prebivalcev, organov, služb in organizacij v državi ter njenih obrambnih sil kot tudi diplomatske misije v tujini pred delovanjem tujih obveščevalnih služb (Hribar 2011, 12; U.S. Department of State 2015).

Anžič se sicer ne strinja, da sta dejavnosti povezani, saj meni, da se protiobveščevalne službe od obveščevalnih ločijo »ne samo po uporabi metod in sredstev dela, temveč tudi po vlogi in funkciji, ki jo imajo v konkretnem varnostnem sistemu« (Anžič v Brezovšek in Črnčec 2010, 119).

3.3 GROŽNJA

Po 135. členu Kazenskega zakonika (KZ-1-UPB2) je grožnja: »Kdor komu, zato da bi ga ustrahoval ali vznemiril, resno zagrozi, da bo napadel njegovo življenje ali telo ali prostost ali

uničil njegovo premoženje velike vrednosti ali da bo ta dejanja storil zoper njegovo bližnjo osebo ...« oziroma »Kdor stori dejanje iz prejšnjega odstavka proti dvema ali več osebam ali z grdim ravnanjem ali z orožjem, nevarnim orodjem, drugim sredstvom ali na tak način, da se lahko telo hudo poškoduje ali zdravje hudo okvari ...« (Kazenski zakonik 2012). SSKJ (2015) navaja, da je grožnja »obljuba, napoved komu česa neprijetnega, hudega«.

4 TEORETIČNI OKVIR

Teorijo varnosti so skozi čas vedno determinirale tri politične paradigme, in sicer **realizem**, **liberalizem** in **radikalna paradigma**. Zadnja se deli na več delov, saj je dokaj netradicionalna v primerjavi z realizmom in liberalizmom. Znotraj tretje tako prepoznamo klasični marksizem, ki je sicer vse manj pomemben vse od konca hladne vojne, in druge netradicionalne pristope, ki se usmerjajo predvsem v razmerje posameznika do okolja v fizičnem in kulturnem smislu. Še en pristop znotraj tretje paradigme je **konstruktivizem**, ki postaja zaradi razširjenosti informacijsko-komunikacijske tehnologije (IKT) vse bolj relevanten. Konstruktivizem se nasprotno od realizma in liberalizma ukvarja s stvarnostjo, ki kot taka ne obstaja, saj je kreacija človeškega uma. Taka stvarnost temelji na podatkih, informacijah in idejah (Svete 2006, 50).

4.1 REALIZEM

Realizem je racionalistično-materialistična in antiutopična teorija, ki temelji na pozitivizmu, v ospredje pa postavlja državo kot najpomembnejšega akterja. Klasični realizem varnost držav povezuje predvsem z njihovo vojaško močjo, saj se v realizmu konflikti rešujejo z uporabo sile. Le država lahko legitimno uporablja silo za doseganje lastnih ciljev tako doma kot v mednarodnih odnosih. V mednarodnih odnosih države med seboj tekmujejo za materialne in nematerialne vire, med katerimi je tudi varnost. Varnost je omejen vir, ki ga nobena država ne more nemoteno uživati v celoti in v enaki meri kot druge države. Zato v realizmu velja prepričanje, da svetovna urejenost deluje po principu hierarhije, znotraj katere so države razporejene glede na svojo vojaško in ekonomsko moč. Večja ekonomska moč tako pomeni tudi večjo vojaško moč, da se država lahko zadostno zavaruje. S tem se dosegata ravnotežje in stabilnost. V tem sistemu države ena drugo stalno potencialno ogrožajo in obenem skušajo preprečevati prednosti svojih nasprotnikov. Zaradi tega nastaja t. i. varnostna dilema (Grizold 1998, 5; Svete 2006, 50–51; Galston 2010, 394).

Varnostna dilema je produkt Johna Hertza iz petdesetih let prejšnjega stoletja, predpostavlja pa, da vsaka akcija ene države v mednarodnem sistemu, kjer država skuša uresničiti svoje interese, nujno pomeni ogrožanje varnosti druge države v tem mednarodnem sistemu, ki je anarhičen (Grizold 1998, 5; Grizold 2001, 138). Osrednji cilj držav je tako preživetje v svetu, ki jim je sovražen, zato je kopičenje moči neizogibno – varnostna dilema spodbuja tehnološki razvoj in oboroževalno tekmo (Evans in Newnham 1998, 465). Vsaka država namreč zaznava lastno varnost kot življenjsko pomembno, enake dejavnosti s strani drugih držav pa kot ogrožajoče dejavnosti. Tako nastane stanje, kjer se nihče ne počuti povsem varnega, kar vodi v tekmovanje in posledično v začaran krog (Grizold 2001, 138–140).

Buzan je opredelil **obrambno dilemo**, kar je nadalje razvit koncept varnostne dileme. Obrambna dilema nastaja iz protislovij med zagotavljanjem vojaške obrambe države in zagotavljanjem celotne nacionalne varnosti. Ta protislovja se najpogosteje kažejo takrat, ko 1) obrambni stroški države onemogočajo doseganje drugih nacionalnovarnostnih ciljev države in 2) ko obrambne priprave v državi postanejo gospodarsko breme, namesto da bi zagotavljale zunanjo obrambo. Najboljši primer tega v sodobnem svetu je Severna Koreja (Grizold 2001, 139).

Druga stran razvoja ideje varnostne dileme, ki prav tako prihaja od Buzana, je **dilema moči in varnosti**. Ta temelji na ideji, da lahko vodi večanje moči in varnosti ene države v zmanjšanje moči in varnosti druge države ali držav. Za razliko od obrambne dileme, ki po mnenju Buzana izhaja iz strahu samega, dilema moči in varnosti izhaja iz strahu pred tem, da bodo morda druge države uporabile svojo vojaško moč (Grizold 2001, 139).

Realizem znotraj samega sebe ni enoten. Prva delitev je na **klasični realizem** in na **neorealizem** oziroma strukturni realizem. Med seboj se razlikujeta glede na to, kako obravnavata načine delovanja držav v mednarodni skupnosti. Klasični realisti so mnenja, da države težijo k prevladi na podlagi delovanja v skladu s človeško naravo, kar vodi v vojne, medtem ko neorealisti zavračajo človekovo naravo kot osnovo za delovanje držav – vedenje držav narekuje struktura mednarodne skupnosti, ki vsakršno deviacijo kaznuje, ko se države ne prilagodijo spremembam. Oboji verjamejo, da je svet urejen anarhično,[2] kar pomeni, da ni neke osrednje avtoritete, ki bi nadzorovala delo držav in jih varovala eno pred drugo. Zato vsaka država skuša preživeti po svoje, kar pahne majhne in šibke države k vzpostavljanju

[2] Realizem ne razume anarhije kot kaosa in nasilja (Svete 2006, 51).

ravnotežja namesto k sodelovanju z velikimi silami. Tekmovanje med državami tako narekuje mednarodna skupnost, a se to tekmovanje ne sme spreobrniti v maksimizacijo moči (Svete 2006, 51–52; Buzan in Hansen 2014, 30).

Moč sicer nima vsesplošno sprejete definicije, a je v najširšem smislu razumljena kot zmožnost vplivanja na delovanje drugih akterjev v mednarodnem sistemu, obenem pa ta moč predstavlja tudi zmožnosti upreti se vplivanju drugih akterjev na naše delovanje z izvajanjem pritiska (Evans in Newnham 1998, 465).

Druga delitev znotraj realizma je na **ofenzivni** in **defenzivni** realizem. Teoretiki defenzivnega trdijo, da države nimajo veliko resničnih interesov za vojaška osvajanja in ekspanzijo, saj stroški presegajo koristi takih dejanj. Tako so soočenja med velikimi silami posledica pretiranih zaznav ogrožanja, obenem pa domače javnosti preveč zaupajo v učinkovitost oboroženih sil kot sredstva za vzpostavljanje varnosti. Nasprotno zagovorniki ofenzivnega realizma zagovarjajo tezo, da anarhija mednarodnega okolja spodbuja države k maksimizaciji njihove relativne moči, saj nobena država ne ve, kdaj se bo pojavila sila, ki bo želela spremeniti trenutno razmerje moči (Svete 2006, 52). Z odpravo grožnje oziroma z zagotovitvijo neke dobrine se ne odpravi oziroma zagotovi tudi možnost, da dobljenega ne bomo spet izgubili oziroma da se grožnja ne bo vrnila. Mnogi realisti namreč poudarjajo, da je kljub današnji navidezni stabilnosti Evrope od konca komunizma minilo šele dobrih 20 let in da nacizem ter fašizem po sedemdesetih letih še nista nujno zgodovina (Galston 2010, 394).

Kljub temu je realizem prek vseh vej enoten, da je glavni akter država in da se na grožnje odgovarja z vojaško močjo, saj sta politični in vojaški sektor tesno povezana. To pomeni, da je konflikt stalno prisoten del mednarodne politike (Buzan in drugi v Buzan 2015, 128; Buzan in Hansen v Buzan 2015, 128).

Realisti ne vidijo potrebe po preoblikovanju svojih teorij, da bi se jih lahko uporabilo za razumevanje varnosti v moderni dobi. Država je še vedno glavni in pogosto edini pomembni, akter, varnost pa je definirana v najožji definiciji, znotraj katere teoretiki ne priznavajo pravice do uporabe moči nedržavnim akterjem. Realisti torej informacijsko revolucijo rešujejo enako kot predhodne velike spremembe, kot je bila na primer globalizacija (Eriksson in Giacomello 2006, 229). Tako je možno sklepati, da bi realisti informacijske grožnje varnosti obravnavali predvsem kot ekonomske probleme, ki niso nujno grožnja državni varnosti, s čimer izgubijo status varnostnih groženj (Buzan v Eriksson in Giacomello 2006, 229; Walt v Eriksson in Giacomello 2006, 229).

Realizem je dokaj toga teorija, ko pride do modernega informacijskega sveta, v katerem živimo, saj zanemarja vpliv globalizacije (Guéhenno v Goetshcel 2000, 264), a je pomembna za nalogo z vidika osredotočanja na države kot na glavne akterje v mednarodnem sistemu. Države so namreč predvsem tarča napadalcev v kibernetskem svetu, a kot bo v nadaljevanju prikazala naloga, so tudi izvrševalci napadov.

Pomen države je pomemben tudi za posameznike, ki so tarče napadov. Država mora zagotoviti, da so njeni prebivalci varni, kar zajema tudi kibernetski svet. Z napadanjem posameznikov (ali podjetij in organizacij kot ločenih akterjev) se ogroža tudi državo in njeno infrastrukturo. Država se mora vpletati v dogajanje znotraj pravnega okvira – zagotavljati tako lastno varnost pred napadi kot postaviti pravno osnovo za reševanje problematike v primeru napada na državljane, skupine, podjetja ali organizacije v državi. Pravo je pomemben vir avoritete, ki jasno izraža pozicijo države o določeni problematiki, sporoča to pozicijo kršiteljem zakonov, obenem pa legitimira uporabo vsakršnih sredstev s strani države. Kljub temu lahko država hitro prestopi zdravo mejo vpeljave sile v obliki zakonov, kar povzroči visoko stopnjo omejevanja in nadzora. S tem napadalci dobijo motivacijo, da najdejo nove načine napadov, ki bodo obšli obstoječe ovire, tako pa se problematika poglablja (Wall 2004, 309; 325; 331).

V globalizaciji realizem sicer ne more uspešno razložiti vloge nedržavnih akterjev pri mednarodni varnosti, a ker naloga raziskuje vpliv hekerstva na obveščevalno dejavnost in na implementacijo HACKINT-a s strani držav, je realizem pomemben del teoretičnega okvira magistrskega dela.

4.2 LIBERALIZEM

Nasprotje realizma je že dolgo časa liberalizem. Anarhična urejenost sveta je namreč gnala mislece do tega, da so iskali načine, kako zagotoviti trajni mir. Ideje o pravičnosti, svobodi in miru so tako osrednje za liberalizem. Gre za prav tako dokaj neenotno teorijo, znotraj katere je več smeri: ekonomske, demokratične, sociološke idr. Nekatere teorije namreč menijo, da je za mir odgovorna ekonomska odvisnost, druge pa, da se razlog skriva v demokratični ureditvi držav. Te naj bi bile bolj miroljubne kot avtoritarno urejene države. Ena izmed novejših liberalnih teorij meni, da mednarodne institucije preprečujejo sebično ravnanje držav, saj naj bi se te odrekle takojšnjim dobičkom v zameno za dolgoročne večje prihodke, ki bi izhajali iz mednarodnega sodelovanja (Svete 2006, 52–53; Dunne 2007, 241). Edward Hallett Carr je liberaliste oklical kar za utopiste, saj so kot idealisti poudarjali pomen mednarodnega prava in

organizacij ter vpliv morale in javnega mnenja na mednarodne zadeve. Liberalizem tako predstavlja mešanico idej o svobodi, pravičnosti, ekonomski učinkovitosti, družbeni pravičnosti in demokratičnem konsenzu (Maffettone 2000, 2; Grizold 2001, 104).

Liberalisti za razliko od realistov nimajo tako slabega mnenja o človeški naravi in so bolj optimistični, saj menijo, da tudi če ljudje niso dobri, so vsaj moralno dovzetni. Zato verjamejo v možnost sodelovanja na vseh stopnjah vladanja, čeprav verjamejo v anarhičnost mednarodnega sistema. Prav tako kot realisti tudi liberalisti verjamejo v egoizem človeka, a menijo, da imajo različne skupine določene interese enake, kar je osnova za povezovanje in sodelovanje tako na državni kot mednarodni ravni (Jackson in Sørensen 1999, 109; Eriksson in Giacomello 2006, 230; Hook 2008, 68).

Liberalizem poudarja medvladne in transnacionalne institucije (v zadnjih letih se je namreč raznolikost akterjev v mednarodnih odnosih močno povečala, med pomembnejšimi nedržavnimi pa najdemo transnacionalne korporacije, družbena gibanja, migrante, teroriste in druge), kooperacijo in skupne dosežke. Zaradi vse večje globalizacije so se začele spreminjati varnostne potrebe, pojavile pa so se težnje po ekonomski, okoljski, družbeni in nazadnje kibernetski varnosti, kar je povzročilo vzpon pomena mednarodne varnosti (Eriksson in Giacomello 2006, 230; Buzan 2015, 128).

Ne glede na raznolikost akterjev v mednarodnih odnosih posamezni akterji le stežka povzročajo večje spremembe v sistemu. Predvsem nedržavni nimajo večjega vpliva na politično, vojaško ali ekonomsko moč države, a vse večja transnacionalna povezanost igralcev na mednarodnem polju lahko močno načne suverenost posameznih držav do te mere, da suverenost postane le še simbol teritorialne skladnosti (Eriksson in Giacomello 2006, 230).

Vse liberalne teorije tako izpostavljajo pomen sodelovanja, a se ne strinjajo glede načinov, kako zagotoviti sodelovanje. Sodelovanje je kljub temu ključno, zato govorimo o **kooperativnem modelu**. Ta model temelji na ideji o varnosti kot skupni dobrini – stanje v mednarodnem sistemu, kjer vlada mir zaradi istega interesa oziroma deljene dobrine. Kooperativni model upošteva dve prvini, in sicer 1) potrebo po krepitvi dvo- in večstranskega sodelovanja med subjekti mednarodnega sistema, da se zagotovi varnost vseh, in 2) holistični koncept sodobne mednarodne varnosti z uravnoteženo uporabo vojaških in nevojaških varnostnih sredstev (Grizold 2001, 140–141; Svete 2006, 53–54).

Neoliberalistični institucionalizem temelji na pomembnosti obstoja mednarodne skupnosti in mednarodnih institucij. Te pomagajo državam, da v anarhičnem sistemu, ki vlada svetu, ne zaznavajo drugih držav kot nevarnih po najslabšem možnem scenariju. Tako med državami omogočajo sodelovanje na več načinov, na primer povečujejo število interakcij med državami, pomagajo uresničevati nacionalne interese, povečujejo transparentnost in informacijsko neprepustnost za povečevanje zaupanja med državami itd., vse z namenom povečevanja skupnih koristi in dosežkov (Svete 2006, 54; Buzan 2015, 129). Nye namreč meni, da je v moderni digitalni skupnosti mehka moč vse pomembnejša, predvsem zaradi mnogih razvijajočih se kanalov, prek katerih poteka globalna interakcija med akterji, ki zlahka presega meje suverenosti posameznih držav (Nye v Eriksson in Giacomello 2006, 231). Kljub temu je treba omeniti, da gre pri mehki moči v prvi vrsti za obliko in ne vsebino. Mehka moč danes ne predstavlja zgolj kooperativnosti, demokratizacije in miru, lahko se pojavi tudi v obliki zavajanja, propagande in terorja (Eriksson in Giacomello 2006, 231).

Liberalistična teorija vsebuje mnogo idej, a med najpomembnejše štejemo teorijo demokratičnega miru, harmonijo interesov, idejo kolektivne varnosti in nazadnje pozitivno vlogo mednarodnega prava ter institucij. Zadnje je pomembno predvsem za spodbujanje sodelovanja, kar je omenjeno že na začetku poglavja (Evans in Newnham 1998, 305).

Kljub povečanju zaupanja med državami je globalizacija povzročila tudi hiter vzpon transnacionalnih mrežnih organizacij in nevladnih organizacij ter hitro širjenje IKT. S tem se vse bolj spodkopava moč držav, pozornost pa se je preusmerila z vojaške moči in varnosti na zagotavljanje ekonomske in socialne blaginje držav. Zaradi tega se spletajo mnoge mednarodne povezave, ki predvsem preprečujejo uporabo sile (Svete 2006, 54). Prav iz tega razloga je vse več povezovanja med zasebno in javno sfero, ki s skupnimi močmi zagotavljata storitve za prebivalce in potrošnike, opaziti pa je bilo tudi trend spojitve civilne in vojaške sfere. Ta gibanja so povzročila, da so se razlike v jurisdikciji, pristojnostih, dolžnostih in tveganjih med različnimi segmenti v družbi zabrisale. Modernizacija je v luči liberalizma videti kot razsvetljenska sila in miroljubna sprememba, kar je spodbudilo idejo kolektivne varnosti, kar je nadalje med drugim vplivalo na ZN in OVSE (Eriksson in Giacomello 2006, 230–231).

Teorija **demokratičnega miru** izhaja iz teze, da lahko večni mir dosežejo samo prave (liberalne) demokracije, ki imajo miroljubne medsebojne odnose. To velja predvsem v primerjavi z avtoritarno urejenimi državami. Prave demokracije so tako miroljubne ena do

druge, za širjenje miru pa uporabljajo tudi mednarodne organizacije. Tako bi v svetu, v katerem obstajajo samo demokracije, večno vladal mir, vojne pa ne bi bilo (Evans in Newnham 1998, 305; Svete 2006, 55).

Harmonija interesov je stara ideja, ki je dokaj povezana s teorijo demokratičnega miru, po njej naj bi se interesi skupin, ki obstajajo v mednarodnem sistemu, ujemali. S tem naj bi se do neke mere zagotovila harmonija, kar bi posledično vodilo v mir, saj se vojna ne bi izplačala (Evans in Newnham 1998, 305).

Ideja sistema kolektivne varnosti je produkt ameriškega predsednika Wilsona ob koncu 1. svetovne vojne. V sistemu kolektivne varnosti bi se voditelji zavezali, da ne bodo uporabljali vojne kot sredstva za doseganje lastnih interesov, pač pa bodo skrbeli en za drugega in se ščitili v primeru agresije drugih držav (Hook 2008, 35). Od konca 1. svetovne vojne se je ideja institucionalizirala dvakrat, prvič v letu 1919 v Društvu narodov in drugič leta 1945 v Organizaciji združenih narodov (Odar 2010, 26).

Kibernetske grožnje in druge ovire, ki so se pojavile z informacijsko revolucijo, so del splošnega trenda globalizacije, ki po mnenju liberalizma šibi suverenost in varnost držav. Moč nedržavnih akterjev se zaradi informacijske revolucije povečuje. Internet je omogočil globalno komunikacijo nevladnim organizacijam, povzročil pa je tudi nastanek organizacij, ki so prisotne izključno na spletu. Ta razvoj ima tako pozitivne kot negativne posledice: na eni strani se lahko integracija, kooperacija in osvoboditev ublažijo, po drugi pa se pojavljajo terorizem, transnacionalni kriminal in destabilizacija držav (Eriksson in Giacomello 2006, 232).

Pomen liberalizma za to nalogo je predvsem pri vlogah, ki jih igrajo premnogi akterji mednarodnega sistema. Liberalizem namreč poudarja raznolikost igralcev mednarodnega polja, predvsem nedržavnih, kar je v tej nalogi ključno. V raziskanih primerih so napadalci mnogokrat nedržavni akterji z veliko močjo, ki je lahko konkurenčna moči držav, ki so pogosto na strani žrtev napadov kibernetskega sveta.

Kljub temu vloga države v okviru liberalizma ni povsem zanemarljiva. Kibernetski kriminal danes presega meje nacionalnih držav in je v veliko primerih mednarodni problem, ki zahteva kooperacijo med državami in njenimi organizacijami. Pomembno je, da se problematika rešuje skupaj, kar povzroča oblikovanje mednarodnh organizacij, sodelovanje organov pregona in obveščevalnih služb med državami, in, ne nazadnje, razvijajoča se intradržavna in

mednarodna zakonodaja. Grožnje globalizacije običajno sicer ne zadevajo skupne varnosti držav ali njihove teritorialne intergritete. Osredotočajo se predvsem na specifične skupine in občasno posameznike, reševanje problemov pa lahko presega meje držav, kar pod vprašaj postavlja tudi koncept nacionalne varnosti (Reinicke v Goetschel 2000, 265).

Globalizacija je povzročila povezavo posameznikov z globalnimi silami, kar poveča zaznavo in občutljivost na globalne dogodke. S tem nastaja globalna družba, ki je postala mediator med lokalno in globalno ravnjo (Shaw v Goetschel 2000, 260). V tem okviru lahko govorimo tudi o mednarodnem javnem mnenju, ki vpliva na vedenje vlad v posameznih državah (Beetham v Goetschel 2000, 260). Razvoj globalne družbe povzroča rast institucij in institucionalne kulture v smeri večjih skladnosti in soglasja. Glavni cilj je doseči globalno odgovornost na različnih področjih in družbo skupnih verdnot in ciljev (Shaw v Goetschel 2000, 262; Kratochwil v Goetschel 2000, 262).

4.3 KONSTRUKTIVIZEM

Konstruktivizem se ukvarja z mednarodnim sistemom kot družbenim prostorom, obenem pa poudarja prav tisti dve prvini, ki ju zanemarjata realizem in institucionalizem: identiteto in interese. Konstruktivizem tako v ospredje postavi kulturno-institucionalno okolje, v katerem se določa vedenje akterjev, hkrati pa zavrača ideje moči in materialnih virov realizma in neorealizma. V to pozitivistično okolje spadajo kultura, prepričanja, norme, ideje in identitete. Konstruktivizem se prav tako ne strinja z nobeno liberalistično teorijo, ki v ospredje postavljajo mednarodni režim, institucije in njihove norme. Glavni interes konstruktivizma je tako preučevanje človeških idej v mednarodnem okolju, in sicer na tri načine. Prvič, konstruktivistična analiza virtualnega sveta poudarja pomen podob in simbolov kot osrednjih elementov družbene realnosti, ki je bila prav s to teorijo uvrščena v znanstveni dialog. Drugič, vedenje akterjev ne izvira le iz materialnih vplivov, ampak tudi iz vpliva identitet. Te vplivajo na interese akterjev, od koder izhaja vpliv na vedenje akterjev. Tretjič, med strukturami, ki nastajajo iz družbene prakse, in identitetami akterjev vlada izmenjujoč se odnos. Družbeno okolje namreč oblikuje akterje, obenem pa odnos akterjev do okolja določajo norme in ideje (Svete 2006, 56–57; Buzan in Hansen 2014, 35). Za razliko od realizma in liberalizma, ki imata oblikovano idejo o tem, kako je videti oziroma naj bi bil videti mednarodni sistem, konstruktivizem običajno tega ne ponuja (Buzan 2015, 128).

Konstruktivizem se ukvarja z družbeno konstrukcijo, saj meni, da tako domača kot tuja politika skupaj s preostalimi vidiki javnega življenja nimata fiksnih lastnosti. Ne obstajajo niti

nacionalni interesi. Obstajajo interesi, ki so konstrukti političnih voditeljev, ti pa so te interese s simboli in podobami pretvorili v uradno politiko svoje države (Hook 2008, 74). Interesi in identitete zato niso statični, ampak se stalno oblikujejo in producirajo (Adler v Eriksson in Giacomello 2006, 233; Wendt v Eriksson in Giacomello 2006, 233).

Teoretiki so mnenja, da obstajata dve realnosti – materialna in družbena. In ker je družbena ustvarjena s strani družbe, je vedno občutljiva na spremembe. Konstruktivizem se tako sprašuje, kako primarni akterji oblikujejo in sprejemajo svoje identiteto in interese. Kljub osredotočanju na ideje in norme ter na njihov regulativen vpliv konstruktivizem poudarja, da imajo norme in ideje tudi konstruktivne učinke. Niso samo odsev materialne strukture in okolja, ampak tudi oblikujejo in definirajo osnovo, na kateri nastaja materialna struktura (Svete 2006, 57; Adler v Eriksson in Giacomello 2006, 233; Wendt v Eriksson in Giacomello 2006, 233). Politične identitete, ki so konstrukt družbe, določajo, katere države so sovražne in katere zaveznice. Na podlagi tega se potem določa sodelovanje in povezovanje z zaveznicami (Hook 2008, 74).

Tudi v konstruktivizmu imajo institucije pomembno vlogo, saj spodbujajo sodelovanje med državami v mednarodnem sistemu, obenem pa omejujejo njihove posamezne interese. Konstruktivizem mednarodni sistem sicer vidi kot umetno tvorbo, sestavljeno iz državnih in nedržavnih institucij. Državni voditelji so ključni akterji mednarodne politike, a je njihovo vedenje oblikovano s strani norm, vrednot in identitet. Konstruktivizem namreč meni, da mednarodni sistem temelji na ideologijah, zgodovini in socializaciji. Družbeno določena je tudi anarhija mednarodnega sistema (Svete 2006, 57).

Tudi konstruktivizem delimo na več vej, in sicer na **modernistični** in **postmodernistični** (ki sicer obstajata še pod drugimi imeni). Ločimo ga tudi na **mehkega** in **trdega**. Prvi dopušča materialne faktorje kot vpliv na vedenje akterjev, drugi pa je to razširil v idejo, da so materialni pogoji, znotraj katerih delujejo akterji, radikalno podrejeni smotru in vrednotam teh akterjev (Svete 2006, 58).

Kopenhagenska šola je še ena teorija znotraj konstruktivizma, razvijala in širila pa se je predvsem pod Buzanom in Wæverjem. Osredotoča se predvsem na idejo **sekuritizacije**, kar pomeni, da s tem, ko nekaj označimo z besedo 'varnost', stvar dobi določen politični pomen, poudarja pa tudi pomembnost regionalne politike. Z oznako 'varnost' predmet postavimo v ospredje in mu povečamo pomembnost (Booth 2007, 108–109; Buzan in Hansen 2014, 36). Gre za besedni akt, z njim pa legitimiramo posebne ukrepe, kot so tajnost, uporaba sile in

invazija v zasebnost. Kljub odličnemu razumevanju varnosti teorija ni predvidela informacijske revolucije (Eriksson in Giacomello 2006, 234). Če to navežem na problem hekerstva, lahko rečemo, da je hekerstvo samo po sebi nekaj, kar doživljajo navadni uporabniki spleta s škodljivimi sporočili in oglasi. Če pa rečemo, da je hekerstvo *varnostna grožnja države*, hekerstvu povečamo pomen, obenem pa ga dojemamo kot veliko večjo nevarnost, kot smo ga v prvem primeru, ko je šlo zgolj za virusna reklamna sporočila na spletu. Povečali smo njegovo pomembnost in pomembnost problema samega, hkrati pa smo ga postavili v ospredje kot eno od resnih groženj, s katerimi se mora država soočiti hitro. Postavili smo ga kot prioriteto v primerjavi s prvim primerom, kjer je bilo hekerstvo zgolj nadloga.

Kibernetska varnost je uspešno sekuritizirana, kar nakazuje institucionalni razvoj v ZDA (Komisija za zaščito kritične infrastrukture,[3] ki jo je vzpostavil predsednik Clinton leta 1996, umestitev kibernetske varnosti v okvir Oddelka za domovinsko varnost in Busheva Nacionalna strategija za zavarovanje kibernetskega prostora[4] iz leta 2003) in v Evropi (kibernetski varnostni center v Estoniji pod okriljem NATA iz leta 2008). Danes je težko ločiti kibernetsko varnost od drugih varnostnih sektorjev. Po besedah Rachel E. Yould je prav informacijska tehnologija tista, ki bo združila varnostne sektorje (Hansen in Nissenbaum 2009, 1157; Yould v Hansen in Nissenbaum 2009, 1157).

V okviru mehkega konstruktivizma obstaja še **teorija ravnotežja groženj**. Teorijo je razvil Stephen M. Walt, pravi pa, da države reagirajo na grožnje, ne na moč. To gre proti realistični teoriji ravnotežja moči, ki pravi, da države skušajo preprečiti nadvlado ene države z uravnoteženjem moči. Po teoriji ravnotežja groženj države uravnotežujejo grožnje, ki jih zaznavajo, in se obnašajo v skladu s tem. Njihova dejanja posledično vplivajo tako na domačo varnost kot na varnost mednarodnega sistema (Bock in Henneberg 2013, 1–2).

Znotraj konstruktivizma lahko obravnavamo tudi **kulturalizem**. Pomen kulture se je v moderni znanosti močno povečal po koncu hladne vojne, ko se je znotraj varnostnih študij oblikoval konsenz o njenem vplivu. Brez konstruktivizma kultura ne bi imela tako velikega pomena. Ta teorija jo namreč vidi kot sistem vrednot in pomenov, ki vpliva na zaznave, komunikacije in delovanje samo ter jih zaznamuje. Kljub temu kultura ni rezultat družbenih

[3] *Commission on Critical Infrastructure Protection*

[4] *The National Strategy to Secure Cyberspace*

konstruktov realnosti, pač pa njihova osnova. Gre za kulturo kot simbolno podlago (Svete 2006, 59).

V konstruktivizmu je tako varnost proizvod priučenih običajev in navad akterjev. Zaznavanje grožnje se razvija in je posledica evolucije, torej se lahko tudi spreminja z razvojem okolja, spreminjanjem navad ipd. Bistvo konstruktivizma je torej konstruktivistična sinteza – temelji na preučevanju interesov in idej, oboje pa jemlje bolj resno, kot jih jemljeta realizem in liberalizem. Konstruktivizem je vmesna pot med skrajnostma, ki sta realizem in liberalizem (Svete 2006, 60–61).

Konstruktivizem pri analizi moči in varnosti v virtualnem svetu poudarja pomen slik in simbolov, ki dopolnjujejo materialni svet računalnikov. Nekateri teoretiki menijo, da bojevanje v kibernetski sferi ljudi loči od vojne do te mere, da je zaznava konflikta povsem drugačna, s tem pa je povezana tudi reakcija na konflikt (Der Derian v Eriksson in Giacomello 2006, 234–235; Everard v Eriksson in Giacomello 2006, 234–235).

Konstruktivizem pokaže moč in vpliv jezika v varnosti modernega časa. Z uporabo imen iz realnega sveta, ko so na primer 'virus', 'črv' ali 'požarni zid', damo kibernetskemu svetu pomen in ga naredimo lažjega za razumevanje. Z uporabo izraza 'vojna' pa damo spletnim napadom in kriminalu poseben pomen, saj je takoj jasno, da gre za resen dogodek, ki ima posledice tudi v fizični realnosti (Eriksson in Giacomello 2006, 235).

Konstruktivizem je od treh omenjenih najbolj aplikativna teorija za to magistrsko nalogo, saj najbolj realno odraža trenutno stanje v mednarodnem sistemu. Kaj je grožnja in kako jo zaznavamo, se spreminja skoraj dnevno, kar je posledica hitrega razvoja tehnologije v modernem času. Zaznavanje grožnje je produkt evolucije okolja in odnosov. Konstruktivizem se osredotoča na posledice globalizacije na vrednote, ki so videne kot potrebne varovanja. Njegova naloga ni ustvariti grožnje, ampak razumeti proces oblikovaja skupnega razumevanja, kaj je grožnja in kako se nanjo kolektivno odzvati (Buzan v Goetschel 2000, 266; Goetschel 2000, 266).

Konstruktivizem je primeren predvsem zato, ker je obravnavana stvarnost produkt človeka in se odvija ločeno od fizične realnosti. Kljub temu je postal internet v zadnjem času eden bolj pomembnih političnih polj, kar se odraža tudi v stopnji kibernetskih napadov in uporabe HACKINT-a. Konstruktivizem je vodilna klasična teorija v nalogi, saj so predmet naloge – hekerstvo – in opisani primeri problem družbene realnosti, znotraj katere se odvijajo. Znotraj

konstruktivizma je za magistrsko nalogo izrednega pomena tudi ideja sekuritizacije, saj je hekerstvo v zadnjih letih pridobilo nov status pomembnosti in nevarnosti za države.

5 OBVEŠČEVALNA DEJAVNOST V SODOBNEM SVETU

Obveščevalna dejavnost se precej razlikuje od drugih nalog in dejavnosti vsake vlade, saj je na prvem mestu to delo, ki je v večini skrito očem javnosti. Čeprav se mnogi avtorji strinjajo, da je to pametno in potrebno, s tem prihaja do pomanjkanja informacij o tem, kaj obveščevalna dejavnost točno je in kako jo najbolje definirati (Lowenthal 2009, 1).

Za obveščevalno dejavnost so pomembni vsi tisti podatki, ki omogočajo formulacijo in implementacijo politik, ki pomagajo državi pri doseganju njenih interesov in v soočenjih z resnimi ali potencialnimi grožnjami. Obenem se obveščevalna dejavnost ukvarja tudi z akcijami, ki pomagajo državnim zunanjim zadevam, obrambi in varnostni politiki. Med pomembne prav tako spadajo informacije o diplomatskih aktivnostih in namerah ter o nasprotnikovih obveščevalnih dejavnostih. Tudi tiste informacije, ki jih nasprotnik ne skuša prikriti, so lahko uporabne – zadeve notranje in zunanje politike, ekonomija države, demografija idr. Od režima vsake države posebej je odvisno, koliko in kakšne informacije so javne. V demokraciji je običajno javnih precej takih podatkov, prav nasprotno pa je pogosto v totalitarnih režimih, kjer se skuša prikriti čim več (Shulsky in Schmitt 2002, 1; Räsänen in Nyce 2013, 657).

Tajnost je lahko velika težava; predvsem v demokratičnih državah, na primer v ZDA, Veliki Britaniji, Nemčiji ipd., ljudje niso preveč navdušeni, da se v političnem sistemu, ki je odprt in naj bi bil transparenten, določene stvari, ki jih delajo tajne službe, skrivajo pred državljani. Mnogi se počutijo zgroženo in nelagodno ob misli, da obstajajo državne skrivnosti, za katere ne vedo in o katerih ne morejo soditi, če so dobre ali slabe. Nekateri namreč načine dela obveščevalnih agencij – prisluškovanje, vohunjenje ipd. – vidijo kot neetična dejanja. Najbolj jih skrbi poseganje v njihovo zasebnost (Lowenthal 2009, 1; Borger 2013; European Parliamentary Research Service 2014).

Informacijska tehnologija je področje, ki se sunkovito spreminja in znotraj katerega je še marsikaj nedorečenega. Razvoj tehnologije se odraža tudi v življenju posameznikov in družb ter v političnih, družbenih in ekonomskih institucijah. Ljudje, družbe in institucije med seboj tekmujejo za prevlado s promoviranjem lastnih idej in politik, s kompetitivno tehnologijo in tehnološkimi standardi (Nissenbaum 2004, 196).

Veliko ljudi je verjelo, da bo s prihodom interneta glas dobilo veliko oseb, ki so se do takrat, v času televizije in radia, čutile brez glasu. Razbil se je monopol elit, ki so določale, kaj so novice skozi ostro ločevanje, je bil prepričan radijski voditelj Hugh Hewitt. Menil je še, da sta se možnost in avtoriteta širjenja besedil končno demokratizirali. Lawrence Grossman je trdil, da je internet ljudem dal neko moč, ki je prej niso posedovali. Predsednik družbe CNN Jonathan Klein pa se je bal, da je to preveč moči za človeka, ki zgolj sedi v dnevni sobi v svoji pižami. Spet na drugi strani je stal Brokaw, ki je dejal, da pisci spletnih dnevnikov (*blogov*) predstavljajo demokratizacijo novic. Drugi novinarji so bili ogorčeni, da je njihova konkurenca skupek ljudi, ki pišejo od doma in ki niso delali na novinarskih karierah kot oni sami. Za mnoge je dejstvo, da internet povečuje demokratičnost politike, dobra novica, a so v določenih vidikih v zmoti. Kljub odprtosti in povečani demokratičnosti politike zaradi interneta ter vse večji participaciji ljudi ta odprtost ustvarja nove politične elite (Hindman 2009, 2–4).

Uporaba spleta se stalno povečuje, saj je nanj povezanih vse več ljudi. Ocene za leto 2010 so bile, da bosta na spletu kar 2 milijardi svetovnih uporabnikov. Kljub temu z vse več uporabniki raste tudi nevarnost. Na spletu se pojavljajo razne oblike nevarnosti, ki ogrožajo vse večje število ljudi (Kramer in drugi 2009, xiii).

Komuniciranje je postala ena izmed najpomembnejših aktivnosti sodobne družbe, prav zato je fokusiranje na informacije pomembno za obveščevalno dejavnost. Vse skupaj se je močno olajšalo z napredkom v tehnologiji, a je to bolj postranskega pomena. Dva velika vpliva sta bila še spremembe v vedenju ljudi in institucionalne spremembe. Tako je prišlo do hitrega pretoka informacij, kar omogoča hitrejše delovanje države pri implementaciji politik. Obenem se je povečala 'ponudba' informacij na trgu, česar so se začele zavedati tudi organizacije, ki niso povezane z obveščevalno dejavnostjo. To je tej prineslo veliko konkurenco na trgu pri zbiranju informacij in sporočanju teh informacij najprej političnim odločevalcem (Shulsky in Schmitt 2002, 7).

Cyberpower ('kibernetska moč') je danes temelj globalnega življenja. V politiki, ekonomiji in vojski so informacije in informacijska tehnologija ključne za operativne naloge. Kibernetika je postala del strateškega načrtovanja, prav tako pa postaja del skupnih prizadevanj za nacionalno varnost v državah. Uvedba strateškega okvirja, ki bo vseboval tudi kibernetiko, bo imel tako strukturne kot geopolitične posledice. Strukturne se bodo kazale predvsem v povečanih zmožnostih delovanja uporabnikov na splošno. Opazno bo povečanje varnosti,

razširjen razvoj raziskav in človeškega kapitala, učinkovitejša organizacija idr. Geopolitične aktivnosti se bodo kazale predvsem pri tradicionalni nacionalni varnosti in obrambnih naporih (Kramer 2009, 3).

Dejstvo je, da so kibernetske grožnje nevarne, kibernetska vojna pa resnična. Do danes so vsi napadi imeli resne posledice, a obstaja možnost, da napadalci niso uporabili najmočnejšega orožja, ki ga imajo. Posebej nevarni so zaradi hitrosti, saj je čas med začetkom napada in posledicami skoraj ničen in ga ni lahko izmeriti, kar otežuje delo kriznim odločevalcem. Globalizacija je še ena od nevarnosti, saj kibernetski napadi ogrožajo mnoge države, med katerimi marsikatere neposredno in nevede utrpijo škodo. Prav tako je fizična obramba v primeru kibernetskega napada neuporabna, saj lahko napadalci večino naprav (radarje, alarme, sefe ipd.) napadejo po spletu, ne da bi morali predhodno premagati nacionalne obrambne sile. Pravzaprav se je kibernetska vojna že začela, saj države v 'pripravah' bojnega polja ves čas napadajo omrežja in infrastrukturo ena druge. Vse to se odvija v miru, take vrste bojevanja pa še dodatno omajajo stabilnost mednarodnega sistema, saj brišejo meje med mirom in vojno (Clarke in Knake 2010, 30–31).

Svet, kamor spadajo tudi vojaške zadeve, postaja vse bolj transparenten. Tudi v državah, ki aktivno zatirajo dostop do informacij svojim državljanom, na primer na Kitajskem, to postaja vse težje. Kljub moderni tehnologiji, ki širi novice po svetu, bodo nekatere skrivnosti še vedno ostale skrivnosti, države pa bodo za njihovo prikrivanje in odkrivanje namenjale sredstva. Dve moderni novosti bosta definitivno vplivali na uporabo obveščevalne dejavnosti v vojnem času. Prva so uporniška gibanja, ki brišejo mejo med vojno in kriminalom. Ko države reagirajo na take, pogosto mednarodne, grožnje, prihaja do vpletanja velikega števila ljudi, ki delujejo na različne načine, pod različnimi povelji, kar zapleta koordinacijo reševanja problemov. Druga novost je tehnološka, saj zbiranje podatkov danes omogoča takojšnje posredovanje na terenu v realnem času, moderna tehnologija pa že ustvarja naprave in programe, ki bodo take akcije izvajali tekoče. Prednost je seveda hitrejša identifikacija in eliminacija tarče, a kot so pokazali primeri iz ZDA, obstaja tudi velika slabost: kolateralna škoda (Lever 2012, 239–240).

Kibernetska prihodnost je nepredvidljiva, zato je pomembno, da je njena implementacija v strateške načrte primerno prilagodljiva, da se bodo strukture, procesi in ljudje v prihodnosti lahko prilagodili spremembam. Te so odvisne predvsem od človeškega faktorja in njegovih inovacij. Spreminjanje kibernetike je hitro in postaja vse hitrejše z razvojem nove tehnologije.

Razlog za to so nizke vstopne meje – povezava z internetom danes za večino sveta ni draga in je lahko dostopna (Kramer 2009, 5).

6 HEKERSTVO

Hekerstvo samo po sebi je skupek dejavnosti, ki jih opravljajo hekerji. Teh pojmov namreč ne smemo pomešati med seboj. Heker je oseba, hekerstvo pa so dejanja te osebe – vdori, napadi ipd. Definicij je tako za eno kot drugo besedo veliko, med seboj pa si tudi nasprotujejo. Kot bo možno prebrati v nadaljevanju, si ljudje nasprotujejo, kdo je heker. Eni menijo, da so to tiste zlonamerne osebe, ki namenoma povzročajo škodo v lastno korist, drugi pa, da gre za osebe, ki uživajo v delu z računalnikom, v gradnji programov ipd., niso zlonamerne in ne želijo nikomur škodovati (Amon 2005, 6).

V tej nalogi se bom osredotočila na prve, zlonamerne hekerje, saj so kljub 'napačni' označitvi pod to definicijo bolj znani. Da je tako, so pogosto krivi mediji, ki po navedbah Raymonda (2001) narobe označujejo spletne kriminalce z besedo heker, in tako pravim hekerjem dajejo slab ugled.

Na hekerje se danes gleda predvsem s strahom. V veliki večini so navadni uporabniki spleta neizkušeni oziroma poznajo samo osnove delovanja tehnologije, ki jo uporabljajo, skupaj s kombinacijo poročanja medijev pa gre za 'naučeno' množico brez lastnih izkušenj in vedenj, zato so njihove ideje in mnenja pogosto v razkoraku z resnico (Amon 2005, 6).

Hekerji sami pravijo, da ne vedo, kdo točno so, zato *hekerski manifest* ne more zastopati nečesa, kar zavrača zastopanje. Ponuja pa vsaj nek vpogled v to, kaj je hekerstvo in kdo so hekerji. Hekerji ustvarjajo možnost novim stvarem iz različnih področij (umetnosti, znanosti, kulture itd.), da vstopajo v svet. Vedno so na voljo neke informacije, ki se jih da dobiti in iz njih ustvariti nekaj novega. Kljub temu si hekerji tega ne lastijo; kar naberejo, posredujejo naprej. Hekerji se ne združujejo, in čeprav imajo neke skupne lastnosti, niso svoj razred ali svoja skupnost. Imajo nek skupen interes, da bi dosegli vključevanje razlik, ne pa enotnosti med vsemi (Wark 2008, 13–15).

Eric Steven Raymond na svoji spletni strani piše, da so hekerji med nami že vse od začetka ARPANET-a. Gre za ekspertne programerje in njihovo kulturo, kjer se je ustvarila tudi beseda heker. Raymond piše, da so hekerji ustvarili internet in poskrbeli, da WWW (*World Wide Web*) deluje. Hekerji so bili v samih začetkih predvsem mladi moški, ki so pomagali razviti

strojno in programsko opremo za obstoječe funkcionalnosti, poleg tega pa so, pogosto kot izziv samim sebi, prišli do novih algoritmov in aplikacij, ki so bile vključene v poznejše generacije računalnikov. Te nove funkcije niso le razširile rekreativnih zmogljivosti računalništva in informacijske tehnologije, povečale so tudi praktične sposobnosti, npr. hitrost procesiranja. Raymond prav tako opiše *crackerje*, kar je ime za samooklicane hekerje, ki napadajo računalniške sisteme in telefone. Meni, da to niso pravi hekerji, čeprav jih mediji na široko opisujejo s tem imenom. Hekerji gradijo stvari, *crackerji* pa jih uničujejo. Beseda *cracker* je bila vpeljana okrog leta 1985 kot obramba proti napačni medijski uporabi besede heker (Raymond 2001; Nissenbaum 2004, 197; The Jargon File 2014).

Do razlikovanja v definicijah in do nasprotovanj prihaja iz več razlogov. Eden od njih je zagotovo zgodovinski. Hekerji so kategorija, ki je v zadnjih štirih desetletjih doživela velike spremembe in se močno preoblikovala. Prve definicije, ki so nastale v času začetkov računalništva in spleta, so zagotovo milejše od tistih, ki so se pojavile v nedavnem začetku globalizacije. Razlog se mogoče skriva pri hekerjih samih, ki so se od prvih precej spremenili. Današnji hekerji ne razlikujejo več med svojimi žrtvami, precej ločeni pa so od hekerske etike, ki jih je vodila desetletja nazaj. Spremembe so se zgodile tudi med navadno publiko, ki je spremenila svoje standarde in vrednote, s tem pa začela (in prenehala) tolerirati določena ravnanja. Razlike nastajajo tudi zaradi geografije. Definicije avtorjev iz Severne Amerike so natančnejše, saj sta se tako razvoj kot uporaba interneta najhitreje širila po Severni Ameriki. Profesor Paul A. Taylor s salfordske univerze meni, da negativizem do hekerjev izvira iz časa hladne vojne, ko je bilo treba krivdo za splošno občutenje ranljivosti nekomu pripisati. Uporaba terminologije in simbolike hladne vojne je pripomogla k utrjevanju prepričanj, kako veliko škodo lahko povzročijo hekerji. Na te so se začele opirati predvsem vladne in zasebne avtoritete, ki imajo močan glas v modernih skupnostih, ki hekerje prikazujejo kot nove sovražnike informacijske dobe. Moderna družba, pravo in vlade so z iskanjem novega zla našli način za opravičevanje svojih dejanj (financiranje varnosti, povečanje opreznosti in nove oblike kaznovanja, predvsem pa močno omejevanje prostega pretoka informacij), ki jih je omogočila informacijska revolucija. S povzročitvijo histerije med 'navadnimi' uporabniki spleta obenem vzpostavljajo definicijo, kar je v neki družbi normalno in moralno sprejeto. Razvoj definicije je sam po sebi precej fascinanten, predvsem preoblikovanje definicije, ki hekerje obarva v slabi luči. To namreč ne vpliva le na hekerje same, ampak ima posledice tudi v razvoju nove tehnologije, njenem upravljanju in pomenu. Prodajalcem programske opreme je na primer demonizacija hekerjev (in dejanja hekerjev samih) koristila pri prodaji, saj danes

hekerje pogosto asociiramo z virusi (Nissenbaum 2004, 196–197, 199–200; Halbert v Nissenbaum 2004, 199–200; Ross v Nissenbaum 2004, 200; Amon 2005, 6).

Glavna lastnost hekerstva je bil *'pure hack'*, ki se ni držal teoretičnih korakov in postopkov. Hekerstvo je pomenilo iskanje kakršne koli poti do uspešnega cilja, pa naj bo to reševanje problema ali izum nečesa novega (Nissenbaum 2004, 197). Po opisu Raymonda (2001) hekerji gradijo stvari in rešujejo probleme, prav tako pa verjamejo v svobodo in medsebojno vzajemno pomoč. Heker pa nisi samo zaradi svojih prepričanj, čeprav je pomembno, da v svobodo in pomoč verjameš osebno. Kot heker moraš poznati programske jezike in programiranje, znanje angleščine je zelo pomembno, vaja pa vedno dela mojstra. Hekerji niso bile osebe, ki bi delale na stikih z ljudmi, prav tako pa niso bili preveč naklonjeni mlajšim generacijam, ki so se šele začele ukvarjati s to dejavnostjo. Kljub skoraj obsesivnemu vedenju hekerstvo ni le predanost neki obrti, hekerji so se držali ideologije, imenovane *hekerska etika*, ki je vključevala zavezanost k popolnoma prosto dostopnim računalnikom in informacijam; prepričanje v neizmerno moč tehnologije in njeno sposobnost, da izboljša življenja ljudi; nezaupanje centralizirani avtoriteti; prezir do ovir, ki so onemogočale prost dostop do računalništva; in vztrajanje, da se hekerje ocenjuje izključno glede na njihovo tehnično sposobnost in dosežke (Nissenbaum 2004, 197).

Pravi superhekerji so znani po tem, da programirajo iz zabave in ker jih to veseli. Mnogi programerji delajo svoje delo zato, da plačajo račune, pravi hekerji pa v tem uživajo. Denar ni njihovo glavno vodilo, a vseeno igra vlogo. Najpomembnejše je, da delajo nekaj, kar je zanimivo, zabavno, in da imajo za to delo dobra orodja. Zanimivo delo lahko vključuje marsikaj, a kar hekerje pritegne, so novi tehnološki izzivi. Hekerji radi delajo za ljudi z visokimi standardi, kar jih loči od vseh preostalih. Tako sta Google in Apple dosegla svoj uspeh. Najbolj dolgočasno delo je tako, od katerega se ne naučiš nič, dejanskega dela pa je zelo veliko. Da postaneš dober, moraš svoje delo imeti rad, kar je skupno vsem najboljšim hekerjem (Graham 2004).

Slavna imena, kot so Steve Jobs, Steve Wozniak in Bill Gates, so svoje poti začeli kot hekerji, a v tem primeru je definicija tista, kjer so videti kot škodljivci. Spremenili so uveljavljeno tehnologijo, a brez kakršnih koli političnih ciljev, kot to danes delajo hektivisti. Jobs in Wozniack sta izdelala 'modre škatle' (*'blue boxes'*), ki so omogočale uporabnikom ogoljufati telefonska podjetja. Danes so vse te osebe za mnoge heroji, njihovo poveličevanje in skoraj očiščen status pa je močan kontrast hudo preganjanim hektivizmom (Ludlow 2013).

Danes hekerje vidimo predvsem kot nezaupanja vredne in morda celo nevarne posameznike, ki napadajo sisteme, poškodujejo tuje naprave in integriteto shranjenih informacij, širijo viruse in drugo škodljivo programsko opremo, vdirajo v zasebnost in celo ogrožajo nacionalno varnost (Nissenbaum 2004, 198). V tej nalogi se bom osredotočila na obe vrsti, na 'dobre' in 'slabe' hekerje, kakšna pa je razlika med njimi, piše v nadaljevanju.

Kot že prej omenjeno, so hekerji beli ali črni, oziroma *white hats* ali *black hats*. *Black hats* so 'slabi' hekerji, oziroma *crackerji*, ki želijo s svojim delom vdiranja namenoma škodovati. Vdirajo v računalniške sisteme, ustvarjajo in širijo viruse, iščejo slabosti v povezavah in sistemih ter jih izkoriščajo. Njihovo delo ima samo en namen: veliko škode za lastno korist. *White hats* so 'dobri' hekerji, ki iščejo napake v sistemih, občasno tudi prek pogodbe, ko jih neko podjetje najame prav v te namene, in namesto izkoriščanja teh slabosti v lastne namene pomagajo sisteme popraviti in izboljšati, da so manj ranljivi (PC Tools 2010). *Black hats* lahko povzročijo veliko škode tako na posameznih računalnikih običajnih uporabnikov kot na sistemih velikih organizacij s krajo osebnih in finančnih podatkov, z ogrožanjem varnosti velikih sistemov ali z ugašanjem ali spreminjanjem delovanja spletne strani in omrežja (Techopedia 2014).

Poleg belih in črnih poznamo še dve drugi vrsti hekerjev: *Blue hats* in *Gray hats*. *Blue hats* so posamezniki, ki so specialisti za varnost, ki jih podjetja, kot so Microsoft, Apple, Facebook, Twitter in Google, povabijo, da iščejo slabosti v njihovih produktih, da se te odpravijo v njihovih izdelkih. Nekateri za te programe *bug bounty*[5] ponujajo velike nagrade – avgusta 2013 je za Google prinesel že 2 milijona $ izplačanih nagrad, Facebook pa je za samo eno odpravljeno napako ponudil 33.500 $ – a Appla ni med njimi. Obstajajo tudi hackatoni,[6] dogodki, kjer se srečajo hekerji sveta in tekmujejo za službe (organizirajo jih lahko zaposlovalci v namene rekrutiranja). Potekajo tudi po spletu, kar je za mnoge boljša opcija, saj je stroškovno manj zahtevna, poleg tega pa imajo tako na voljo večji bazen hekerjev z vsega sveta, ko izbirajo najboljše. Tak dogodek je v letu 2015 organiziral spletni portal Quora, kjer se je za najboljšo državo v hekerstvu izkazala Belorusija. *Gray hats* so tisti hekerji, ki stalno hodijo po meji med belimi in črnimi oziroma dobrimi in slabimi. Izvajajo vdore za lastno korist, čeprav je ta običajno manjša kot pri *Black hats*, a obenem tudi pomagajo pri iskanju napak in opozarjajo nanje (PC Tools 2010; Hill 2014; Ravisankar 2015).

[5] *Bug* – angl. hrošč, *bounty* – angl. nagrada

[6] *Hackathon – hacking marathon* (hekerski maraton)

Terminologija izvira iz starih kavbojskih filmov, kjer je dobra stran nosila bele klobuke in slaba črne (Techopedia 2014). Siva je nastala zaradi mešanja lastnosti črnih in belih.

Black hats so lahko tako najstniški amaterji, ki širijo računalniške viruse, kot omrežni kriminalci, ki kradejo številke kreditnih kartic in druge finančne informacije. *Black hat* hekerske dejavnosti vključujejo namestitev programov, ki z enim klikom omogočijo krajo podatkov in začetek napadov oziroma onemogočanja dostopa do spletne strani. Zlonamerni hekerji včasih uporabijo 'neračunalniške' metode za pridobivanje podatkov, na primer klicanje in predstavljanje z drugim imenom in funkcijo, da bi dobili gesla uporabnikov (Techopedia 2014).

Black hats hekerji imajo svoje konference, od katerih sta dve izmed bolj izrazitih DEFCON in Blackhat. Teh konferenc se pogosto udeležujejo varnostni strokovnjaki in akademiki, ki se želijo česa naučiti od *Black hats* hekerjev. Teh konferenc se udeležuje tudi policija, včasih celo z namenom, da ujame *Black hat* hekerje, kot se je to zgodilo leta 2001, ko so aretirali ruskega programerja dan po konferenci DEFCON zaradi pisanja programske opreme, ki dešifrira enkripcijo e-knjig formata Adobe (Techopedia 2014).

6.1 HEKERJI IN DRŽAVA

Pojem varnost se nanaša na vse sfere človekovega obstoja in delovanja – gospodarstvo, sociala, kultura, politika, pravo, ekologija itd. Po Grizoldu je širša definicija varnosti sledeča: »Varnost je stanje, v katerem je uravnotežen fizični, duhovni, duševni ter gmotni obstoj posameznika in družbene skupnosti v razmerju do drugih posameznikov, družbenih skupnosti in narave«. Varnost je v človeku vgrajena kot biološki mehanizem, kjer vsak človek stremi k lastnemu obstoju v okolju, ki je ogrožajoče (Grizold 2001, 126; Brezovšek in Črnčec 2010, 17).

Sodobna varnostna paradigma tako obravnava varnost na treh področjih ali v treh sferah: individualna varnost (vedno relativna), nacionalna varnost in mednarodna varnost (kolektivna dobrina mednarodnega sistema držav). **Nacionalno varnost** Grizold opredeli kot »varnost državnega ozemlja (kopno, vode, zračni prostor), prebivalstva in njihove lastnine, ohranjanje nacionalne suverenosti ter zagotavljanje ustreznih razmer za uresničevanje temeljnih funkcij družbe«. Nacionalna varnost je povezana z individualno, v modernih sistemih pa je sprejeta že kot temeljna človekova pravica, ki jo zagotavlja država (Brezovšek in Črnčec 2010, 17–18).

Država mora skrbeti, da ohranja svojo tajnost. Eno od ključnih orodij za zagotavljanje varnosti je varnostno preverjanje oseb, s čimer država preverja, katere osebe so lojalne, zanesljive in verodostojne ter posledično primerne za delo s skrivnostmi države. Če neka oseba vzbuja dvom o lojalnosti, mora država posredovati, da se zavaruje. Kljub vsemu ima vsak posameznik pravico do zasebnosti, ki mu omogoča osebne skrivnosti. Ta pravica je lahko posamezniku kljub ustavni določbi za določen čas odvzeta, če prekrši pravice drugega posameznika ali ogrozi tajnost države (Brezovšek in Črnčec 2010, 9–10).

Nevarnost pri ohranjanju tajnosti in skrivnosti v državi so žvižgači (*whistleblowers*), ki so pogosto videni kot hekerji, kar v skoraj vseh primerih niso. Žvižgači so na kratko osebe, ki javnosti (policiji, medijem ipd.) razkrijejo neko (običajno kriminalno) dejanje, ki je bilo prikrito. Med bolj znane žvižgače uvrščamo nedavna primera Edwarda Snowdena in Chelsea (prej Bradley) Manning. Slednja sta z ugotovitvijo nepravilnosti izdala državne skrivnosti, kar je za ZDA v obeh primerih povzročilo veliko škode. Žvižgače sicer lahko najdemo po vsem svetu in na vseh področjih, zato jih ne moremo enačiti s hekerji. Mordechai Vanunu je bil izraelski jedrski tehnik, ki je leta 1986 razkril podatke o izraelskem jedrskem programu; Jeffrey Wigand je izdal skrivnosti tobačnega podjetja Brown & Williamson, za katerega je delal štiri leta; Kathryn Bolkovac je bila s policijskimi enotami OZN v Bosni, ko je odkrila, da DynCrop (med drugim) novači dekleta za prostitucijo. To so le nekateri primeri, saj naj bi bilo 'pomembnih' žvižgačev v zgodovini približno 150 (Štamcar 2014; Merriam-Webster 2014). Skupno vsem žvižgačem je, da so imeli dostop do teh podatkov (v ZDA je oseb, ki imajo dostop do tajnih podatkov, več kot 800 tisoč; tretjina je pogodbeno zaposlenih) in ni bilo potrebe po vdorih v podatkovne baze, kar jih loči od hekerjev. Prav tako obstaja razlika v pravicah, saj so žvižgači zaščiteni z Zakonom o zdravstvenem varstvu pri delu, za njihov dobrobit pa obstaja tudi nekaj organizacij, kot so na primer *Whistleblower Protection Program* in *National Whistleblowers Center* v ZDA (National Whistleblowers Center 2012; Shachtman v Šimek 2012; Whistleblower Protection Program 2015; United States Department of Labor 2015).

Kljub nedavnim hekerskim podvigom, opisanim v nadaljevanju, ki so za mnoge povzročili veliko škode, so žvižgači verjetno nevarnejši za podjetja in države, ker 'napad' prihaja od znotraj. Podjetja in organizacije vlagajo precej denarja v zunanjo zaščito, da se zavarujejo pred hekerji, a varnost se začne znotraj, med zaposlenimi, kar so pokazali največji primeri izdanih podatkov v zgodovini (Bara 2015). Škoda, ki jo povzroči žvižgač, je lahko precej

hujša kot napad hekerjev, obenem pa se je pred njimi težje zavarovati in jih skoraj ni mogoče predvideti (Šimek 2012).

Država lahko svoja orodja za zagotavljanje varnosti uporablja tudi za varovanje posameznikov. Te lahko zaščiti pred njimi samimi ali pa pred osebami in institucijami, ki bi jih lahko ogrožale. Problem nastane, ko država ne more več zagotavljati nacionalne varnosti, saj s tem posledično ne more zagotavljati varnosti posameznikov. Problem se lahko odraža tudi na mednarodni ravni (Brezovšek in Črnčec 2010, 10–11).

Ko hekerstvo uporabljajo države (HACKINT), imajo lahko doma precej več ovir kot v tujini. Z nadzorovanjem tujih držav in njihovih uradnikov sicer kršijo zakone tiste države, a imajo več prostora, da podkupujejo tuje uradnike, prisluškujejo pogovorom, namestijo prisluškovalne naprave po diplomacijah ipd. V okviru meja lastne države se lahko stvari hitro zapletejo, saj se je treba ravnati po zakonih, ki v državi veljajo. Tako ima na primer FBI dokaj zvezane roke, saj mora za vsako akcijo, ki jo želi izvesti, zahtevati sodni nalog. Če bi imela agencija bolj proste roke, bi morda prestregla dogodke 11. septembra 2001, a večji manevrski prostor lahko hitro prevesi mnenje državljanov o prednostih in slabostih ter ustvari občutek kršenja svoboščin (Betts 2002, 50).

6.2 HEKERSTVO V KOMERCIALNE NAMENE

Včasih so napadi na korporacije veljali za osamljene primere, danes pa gre za zelo razširjen pojav, ki napadalcem prinese mnoge koristi. Z napadanjem omrežij korporacij napadalci posegajo po zasebnih informacijah in strategijah podjetja, ki ne oškodujejo samo napadenih entitet, v nevarnost spravljajo celotno gospodarstvo, menijo eksperti. Mnogi primeri gospodarskega vohunjenja povzročajo škodo, ki se vrti v stotinah milijonov in lahko povzroči še druge nevšečnosti, kot je na primer izguba delovnih mest. General Hayden, nekdanji direktor NSA in CIA, je dodal, da gre za krajo ameriškega premoženja in ameriške konkurenčne prednosti (Fox 2012).

Mnogim 'pravim' hekerjem se zdi služenje denarja s tako dejavnostjo pod častjo, saj so hekerji zgolj iz akademske radovednosti. Zvrha gledajo na ljudi, ki s takimi dejanji služijo denar, čeprav so pogosto prav oni tisti, ki ustvarjajo orodja za hekerstvo (Custer 2014).

Raj za hekerstvo je po mnenju mnogih Kitajska, kjer se je hekerska kultura začela razvijati v poznih devetdesetih letih prejšnjega stoletja. Mnogi proizvajalci informacijske tehnologije na Kitajskem namreč tekmujejo med seboj, kdo bo dobil več posla s strani države in njenih sil

pregona. Hekerstvo namreč ni le del skritega kriminalnega sveta, ampak odprto cveti na vseh področjih, tako v gospodarstvu kot tudi med uradnimi področji države. Ne glede na namen uporabe je ne le predmet prostega diskurza, pač pa akcija, ki jo spodbujajo tako na sejmih kot na univerzah in spletnih forumih. Kitajsko šolsko ministrstvo in mnoge univerze skupaj z različnimi podjetji organizirajo hekerska tekmovanja, ki se jih udeležujejo iskalci talentov kitajske vojske, čeprav so standardi dokaj povprečni, meni eden od ekspertov, ki se je udeležil tekmovanja v letu 2010. Pogosto se dogaja tudi, da podjetja hekerje najemajo za kibernetsko vohunjenje med konkurenco. Velik razlog za širok razpon te dejavnosti je prav vlada, ki vztraja nad nenehnim nadzorom sumljivih oseb, kar privede policijo, da s podjetji, ki se ukvarjajo z nadzorom, hekerstvom ipd., nadzira državljane. Kitajsko zunanje ministrstvo sicer trdi, da nasprotuje hekerstvu in da je država žrtev tudi sama (Wong 2013).

Vsekakor obstaja tudi kriminalna stran hekerstva. Kljub veliki izbiri povsem legalnega dela v svetu hekerstva mnogi še vedno rajši služijo s kriminalnimi dejanji, saj običajno prinesejo veliko več denarja. Pogosto je motivacija denar, saj po besedah enega od hekerjev na Kitajskem vsak gleda zgolj na preživetje – moralne vrednote so prestiž (Wong 2013). Na Kitajskem so med bolj napadenimi spletne igre. To uporabljajo predvsem posamezniki, ki se organizirajo v skupine. Najbolj izkušeni v skupini vdirajo v igralne račune, tisti pod njimi jih olajšajo vsega, kar je vredno (tu gre predvsem za virtualne valute in orožje, ki zunaj igre same nimajo pomena), najnižji sloj v skupini pa vrednosti prodaja drugim uporabnikom, s čimer služijo dejanski denar. Tako lahko naberejo tudi do 16 tisoč dolarjev mesečno (Custer 2014).

Na splošno danes hekerstvo obstaja v podobnih strukturah kot organiziran kriminal, predvsem, ko gre za zapletene sheme, kjer je v igri velik zaslužek. Obstaja cela veriga ljudi, ki so v določenem razmerju med seboj, vsak s svojimi nalogami in znanji. Na vrhu je *CEO* oziroma generalni direktor, ki dejansko ne dela ničesar v nasprotju z zakoni – sam si nikoli ne umaže rok. Pod generalnim direktorjem se nahaja direktor oziroma *underboss*, oseba, h kateri se zatekajo po sredstva napada (trojanski konji in podobni pripomočki *malware*[7]). Pod njim se nahajajo neke vrste območni direktorji oziroma nadzorniki skupin vojakov (*soldiers*), ti pa izvajajo dejanske napade. Čisto na dnu verige so prodajalci (*salespeople* oziroma *associates*), ki ukradene informacije (osebne podatke, bančne informacije, številke kreditnih kartic ipd.) prodajajo naprej (Enterprise Risk Management 2010, 1–2).

[7] Škodljiva programska oprema

Obstajajo tudi drugi načini napada – nekateri hekerji zahtevajo odkupnino za račune, drugi napadajo, da zmanjšajo konkurenco. Ti so lahko najeti s strani konkurenčnih podjetij, predvsem tistih, ki ustvarjajo spletne igre. Četrta vrsta hekerjev zgolj proda nabrane informacije zainteresiranim (znan je primer hekerja, ki je zaslužil čez 800 tisočakov s prodajo celotne baze spletne igre zainteresiranemu kupcu). Kupec lahko s tako bazo manipulira po želji in preusmeri vsa nakazila denarja v igro (pretvorba dejanskega denarja v valuto igre) na svoj račun. Sicer se taka prevara lahko hitro odkrije, a pri bolj priljubljenih igrah se nakup baze lahko povrne že v dnevu ali dveh (Custer 2014).

Prodaja poteka v klepetalnicah, na forumih ali črnih spletnih trgih. Kitajsko spletno podzemlje ima vse, kar si kupec lahko zaželi, napade DDoS, antiviruse, pakete za phishing in podobno, kupec pa lahko storitve plača na enoto, na dan, na teden ali na mesec. Tudi cene niso tako vrtoglave, da si storitev in predhodno pripravljenih paketov za napade ne bi mogli privoščiti tudi navadni uporabniki spleta. Cene za ukradeno blago so širokega ranga in omogočajo nakup vsem – številke s kreditnih kartic, PIN-številke ipd. stanejo od 10 ameriških dolarjev do nekaj tisočakov. Preostali 'produkti', kot so na primer podatki za vohunjenje med konkurenčnimi podjetji, zdravstvene kartoteke podjetij, vsebina poštnih nabiralnikov korporacij ali računi za prenos datotek v podjetjih, stanejo veliko več, ker je tveganje mnogo večje (Enterprise Risk Management 2010, 2; Gu 2013, 2–3, 5).

Danes je hekerstvo za denar že tako razširjeno, da se lahko prijavimo na spletni tečaj in se ga naučimo. Mnogi se tega lotevajo zgolj zaradi zaslužka, ki ga ponuja taka 'kariera'. Eden od intervjuvancev pogovora, ki ga povzema Custer (2014), Little G, je dejal, da ne izpraznijo računov napadenih ljudi. Najprej spremljajo njihove nakupovalne navade, potem pa na podlagi vzorca ustvarijo programe, ki to vedenje posnemajo. Tako na enkrat vzamejo z računov le nekaj juanov, da prevara ni očitna, in tako dlje časa črpajo sredstva. Če je v tej verigi veliko žrtev, to ustvarja velike dobičke.

Na Kitajskem se taka dejanja še posebej izplačajo, saj je zavest o nevarnostih spleta slaba. Tudi podjetja ne vlagajo veliko v varnost svojih iger, ker je to predrago, česar se mnogi ne zavedajo. Poleg tega uporabniki pogosto ne gledajo na varnost, ko izbirajo igro, s katero se bodo kratkočasili. Tudi če stran ponuja orodja, s katerimi bi ljudje lahko bolje zavarovali svoje podatke, jih mnogi ne uporabljajo. Še en dejavnik, ki je prav tako nevaren, je uporaba enakih uporabniških imen in gesel za več različnih strani/iger (Custer 2014).

Da je kljub močni kontroli kibernetskega prostora na Kitajskem, imenovani *The Great Firewall,*[8] še vedno kaos, dokazujejo številni primeri piratske opreme, ki jo uporabljajo tudi vladna podjetja. Microsoft je leta 2012 sprožil več postopkov proti kitajskim podjetjem, ki uporabljajo ilegalno programsko opremo. Ta je v letu 2011 predstavljala kar 9 milijard ameriških dolarjev vreden trg, medtem ko je legalna oprema prinesla približno 3 milijarde dolarjev. Raven piratstva je tako na Kitajskem, ki je ena od hujših prestopnic, kar 77-odstotna (Whitney 2012; Aljazeera America 2015).

Spletne igre se morda zdijo dokaj nepomemben vidik hekerstva, a nevarnost vseeno obstaja. Ker ne gre le za krajo navidezne lastnine – denarja in orožja v igri – lahko vse skupaj označimo za grožnjo državi. S tem ko so napadeni igralci spletnih iger, so napadeni njihovi osebni računi in poleg tega njihovi osebni podatki. Stvari se hitro lahko razvijejo iz kraje virtualnega orožja v igri do praznitve osebnega računa in kraje osebne identitete v realnosti.

Kraja identitete se je pogosto izkazala kot odličen vir za dostop do pomembnih strateških informacij in do denarja, ki lahko financira kriminalna dejanja proti posameznikom, podjetjem ali državi (First Community Bank 2015). Prav iz teh razlogov gre za nacionalno grožnjo. Korak od spletnih iger do ogrožanja nacionalne varnosti se zdi velik, a če vzamemo v zakup, da hekerje spletnih iger najemajo tudi legitimna podjetja, da kontrolirajo svojo konkurenco, lahko hitro opazimo, da je grožnja resna.

Danes je uporabnikov spleta ogromno in velika večina se jih ne zaveda vseh nevarnosti, ki prežijo nanje. Kljub mnogim opozorilom danes še vedno beremo o ljudeh, ki nakazujejo denar 'princem iz Nigerije' in žrtvam raznoraznih katastrof, ki se niso zgodile. Mnogi so krivi sami, a pogosto prihaja do takih stvari zaradi podjetij, ki jim zaupamo svoje podatke v zameno za uporabo njihovih storitev. Temu se v svetu interneta težko izognemo, sploh v času spletnega bančništva, spletnega nakupovanja, e-volitev ipd. Na splošno se pojavlja digitalizacija na vseh področjih, in ko podjetja, organizacije ali države sekajo ovinke pri zagotavljanju svoje varnosti, s tem ogrožajo še mnoge druge. Pogosto se zgodi, da stran, ki je že v uporabi, ne deluje, kot bi morala, a ker je hitrost na tržišču pomembnejša od varnosti, prihaja do napadov. Tako sta v letu 2014 aplikaciji Snapchat in Tinder zaradi napake v računalniški kodi povzročili kup nevšečnosti za uporabnike. Problem nastane tudi pri nadgradnji varnostni pri podjetjih, ki so že dobro uveljavljena. Popolna nadgradnja ali povsem nova namestitev

[8] angl. Veliki požarni zid

varnostnega sistema je velika in draga naloga, ki se mnogim ne zdi vredna naložbe (Gayomali 2014).

Porast spletnega kriminala v zadnjih letih ne kaže, da bi se za mnoge dobičkonosna kriminalna kariera kaj kmalu končala. Hekerski napadi so v zadnji četrtini leta 2013 zrasli za 75 odstotkov, kar 43 odstotkov napadov pa so zakrivili na Kitajskem. Ta sicer v zadnjem času izvaja aktivno čiščenje interneta, ki je v avgustu 2015 po poročanju kitajske policije privedlo do aretacije 15 tisoč kibernetskih kriminalcev, ki so ogrožali varnost interneta. Vse več napadov se pojavlja na korporacije, kjer se izvajajo DDoS-napadi, v zameno za vrnitev baze in vnovično vzpostavitev strani pa hekerji zahtevajo odkupnino. Dva taka večja primera iz leta 2014 sta bila Feedly (ZDA), spletna stran za branje novic, in Domino's pizza (Francija in Belgija). Obe podjetji sta plačilo odkupnine zavrnili in težava se je hitro razrešila, a ugibanja ostajajo, če odkupnina morda vseeno ni bila plačana (McGregor 2014; Aljazeera America 2015).

Tudi najboljšim se zgodi, da so žrtve napadov. Lahko gre za podjetje, ki se ukvarja z varnostjo in je na tem področju med vodilnimi, z najbolj izkušenimi in izobraženimi zaposlenimi, kar jih ponuja trg, a se napadu ne more izogniti. Vedno se najde nekdo, ki je boljši in pametnejši, ki bo izrabil svojo prednost. V takih primerih se zgodi, da je žrtev napada velikan, kot sta na primer Google ali RSA Security.[9] Velika podjetja so sestavljena iz majhnih komponent – ljudi, ki so kljub vsem varnostnim preprekam še vedno najobčutljivejši na napad (Ravenscraft 2014).

Glede na vse večjo količino korporacij, ki utrpijo hekerske napade, se iz vsega skupaj naučimo zelo malo. Čeprav danes na vsakem koraku srečamo opozorila za obnašanje na spletu, da poznamo ljudi, ki so bili žrtve napadov, ali pa smo napad utrpeli sami, smo ljudje še vedno najšibkejši člen v tej verigi. Ni pomembno, kako dobro zavarujemo računalnike in kako odlična je varnostna shema podjetja, ki mu zaupamo svoje podatke, ljudi ne moremo 'nadgraditi', kot to storimo z opremo. Še vedno se bodo našle osebe, ki bodo klikale na nevarne povezave, ki bodo uporabljale prelahka gesla, ki ne bodo posodabljale antivirusnih programov ipd. (Gayomali 2014).

[9] RSA Security je ameriško podjetje, ki se ukvarja z računalniško in s spletno varnostjo.

Nevarnost, ki preži na nas, seveda ni samo 'virtualna'. Gre tudi za fizične nevarnosti, ki se lahko zgodijo v nakupovalnih centrih (naprave za plačilo s kreditno kartico), na bankomatih ipd., čeprav je napad oddaljen. O takih napadih beremo skoraj dnevno, dogajajo pa se tudi v naši okolici – prirejeni bankomati, ki nas olajšajo podatkov, nato pa še denarja, so zelo pogosti. Napad na POS-terminalih za kreditne kartice je konec leta 2013 doletel trgovskega velikana Target v ZDA, kjer so napadalci s t. i. *malware* opremo pobrali osebne in finančne informacije več kot 110 milijonov nakupovalcem. S temi podatki se ustvarijo kloni kartic, s katerimi napadalci lahko zapravljajo na tuj račun (Ravenscraft 2014; Krebs 2014).

Zadnji resnejši fizični napad na kibernetski svet se je zgodil v San Franciscu, kjer je bilo vandaliziranih več kabelskih napeljav. FBI že od leta 2014 raziskuje vsaj 11 napadov na širokopasovno infrastrukturo mesta, razlog za napad pa še ni znan. Ni še jasno, ali so napadi med seboj sploh povezani, a naključje je veliko. Vse pa kaže, da je internetna infrastruktura kljub odlični zaščiti zelo občutljiva (Mills 2015).

6.3 ANALIZA GROŽNJE HEKERSTVA

Danes tehnologija prežema moderni vsakdan vseh do te mere, da se od nje ne moremo ločiti skoraj nikoli. Prav zaradi te nenehne povezanosti je izpostavljenost napadom s strani hekerjev vse večja (Holt 2012, 165). Kibernetski svet ni varen, saj je prav vsaka raven v nevarnosti, ne glede na to, ali je psihična, kot npr. infrastruktura, ali pa gre za programsko opremo, informacije ali ljudi. Vsi so dovzetni za varnostne okvare, ne glede na to, ali gre za napad ali nesrečo (Kramer 2009, 6).

Kot že prej omenjeno, danes hekerstvo lahko primerjamo z organiziranim kriminalom. Večino lastnosti si res delita, a kljub temu obstajajo tudi velike razlike. Glavna razlika med kriminalno organizacijo in hekerstvom, ki povzema predvsem organizacijske principe, je v lokaciji. Medtem ko kriminalne organizacije svoje operacije izvajajo v realnosti, se hekerstvo odvija v varni senci spleta. Napad se lahko zgodi kadar koli in kjer koli, saj splet omogoča globalno povezljivost. Tako je lahko generalni direktor hekerske združbe s Kitajske, *underboss* se nahaja na afriški celini, vodje skupin in vojaki pa po mnogih drugih lokacijah na Zemlji. Kraja podatkov in njihova prodaja se tako lahko odvijajo 24 ur na dan po vsem svetu (Enterprise Risk Management 2010, 2).

Kibernetski napadi, kamor spada hekerstvo, so danes nekaj povsem običajnega. Hekerstva so bile obtožene tako države (med katerimi največkrat Kitajska) kot tudi posamezniki – kriminalci, teroristi itd., ki imajo podobne zmožnosti in sposobnosti kot države. Zaustavljanje

teh napadov je težko, ker je pogosto težko določiti, od kod napad sploh prihaja. Odvračanje napada in povračilo sta lahko diplomatska, ekonomska ali kibernetska. Ker so cilji napadalcev pogosto geopolitični, se jim z enakimi sredstvi lahko učinkovito povrne napad (Kramer 2009, 15).

Na spletu se vsak dan pripeti mnogo različnih napadov, od virusnih okužb do finančnih napadov, ki škodujejo velikim skupinam uporabnikov. Virusni napadi so manjši napadi, ki jih lahko hitro odpravimo, in so predvsem nadloga za uporabnike. Veliki napadi so nevarnejši, saj hkrati oškodujejo veliko število ljudi do te mere, da onemogočijo dostop do spleta celotnim regijam, ali pa okradejo milijone ljudi z zasegom njihovih zasebnih informacij (Skoudis 2009, 172). Škoda, ki nastaja v napadih, je ogromna. Velik del cene (poleg možnih ukradenih informacij, odtujenega denarja ipd.) je odstranjevanje škodljive programske opreme in čiščenje sistema, obenem pa pomeni napad za podjetja tudi upad produktivnosti med zaposlenimi in upad zaupanja pri strankah (Symantec Corporation v Holt 2012, 166; Taylor in drugi v Holt 2012, 166).

Osamljeni majhni (*small-scale*) napadi za pridobivanje denarja so se danes razvili do te mere, da obstajajo skupine ljudi, ki ustvarjajo spletke, prek katerih pridobivajo denar od uporabnikov spleta. Danes svetovni kriminal temelji na kibernetskem kriminalu (Skoudis 2009, 172).

Veliki (*large-scale*) napadi so prešli s tistih, ki so napadali za hobi, in s samostojnih kriminalcev na velike organizirane kriminalne skupine, a se fenomen lahko razvije še naprej, na nedržavne ali državne akterje, ki iščejo načine, kako povzročiti veliko škodo. Primer Estonije iz leta 2007[10] se lahko pogosteje pojavi v bližnji prihodnosti. V teh primerih napadov prihaja do onemogočanja dostopa do storitev, do onemogočanja izvajanja teh storitev, izkoriščanje infrastrukture in njenih pomanjkljivosti oziroma napak in masovne finančne prevare (Skoudis 2009, 177–187). Resna grožnja v zadnjih letih je tudi porast kibernetskega terorizma, proti kateremu se je težko bojevati, zato mnoge države raje posežejo po defenzivi.

[10] Leta 2007 je Estonijo doletel obširen kibernetični napad, ki je onemogočil dostop do mnogih spletnih strani v državi, predvsem do strani organizacij, služb ipd., med drugimi tudi estonskega parlamenta, bank, ministrstev, časopisov idr. Prihajalo je do onemogočanja dostopa, izvajanja storitev in do zasipanja z neželenimi sporočili ('*spam*'). Napadi so trajali tri tedne, nekateri pa so jih označili za WWI – *Web War I* oziroma 1. spletno vojno. Začelo se je s premikom spomenika vojnim žrtvam v času druge svetovne vojne. Rusija je kljub obtožbam Estonije zanikala vpletenost (Traynor 2007; Skoudis 2009, 178; Clarke in Knake 2010, 30).

Teroristi izrabljajo predvsem koristi, ki jih ponuja internet – zelo poceni način komunikacije in organizacije. S to tehniko se široko razširjen problem ekstremizma nekako centralizira brez potrebe po fizični centralizaciji. Obenem internet ponuja veliko polje za širjenje propagande in rekrutiranje, kar zvesto uporabljajo (Kohlmann 2006, 115–116).

Kibernetski vpliv je velik vir moči v mednarodni skupnosti. ZDA imajo v lasti kar 40 odstotkov svetovnih podatkov (odstotek je seveda večji, če upoštevamo vsa družabna omrežja in *cloud*[11] servise: Facebooku svoje informacije zaupa skoraj milijarda in pol ljudi, Amazon pa je vodilni[12] na področju ponujanja *cloud* storitev, s katerimi je začel že leta 2006), a njihov vpliv ni premosorazmeren z zmogljivostjo. To se je zgodilo zaradi raznolikosti in obširnosti sveta, zaradi različnih kultur po svetu in drugačnih občinstev, ki ne reagirajo enako na iste informacije idr. Kljub temu je vpliv spleta močno zaznamoval moderne družbe (Kramer 2009, 16; P. H. 2014; Mims 2014).

7 PRAVNI OKVIR

Hekerstvo nima dobre pravne podlage, kar je eden izmed razlogov, zakaj se ga težko preganja in izkoreninja. Nekaj držav ima urejeno zakonodajo tudi za spletni kriminal, a teh držav je malo. Na mednarodni ravni si med seboj močno razlikujejo, zato je urejanje tam še težje. Ker pa gre pri spletnem kriminalu pogosto za mednarodne razsežnosti, nastajajo težave definiranja in kaznovanja.

7.1 DRŽAVNA RAVEN

7.1.1 SLOVENIJA

Slovenija nima enotne zakonodaje o kibernetski varnosti in boju proti kibernetskemu kriminalu, a nekaj dejavnosti pokriva obstoječa zakonodaja drugih področij. Resolucija o strategiji nacionalne varnosti Republike Slovenije, Resolucija o nacionalnem programu preprečevanja in zatiranja kriminalitete za obdobje 2012–2016, Zakon o elektronskih

[11] *Cloud* (angl. oblak) servisi ponujajo spletno hrambo informacij svojim uporabnikom za lažje dostopanje kjer koli in kadar koli, aplikacije in storitve pa se nahajajo na strežnikih ali v velikih podatkovnih centrih podjetja, ki ponuja storitve računalništva v oblaku (npr. Gmail). S tem se načeloma znižajo stroški posameznega uporabnika, obenem pa uporabniku ni treba skrbeti za nemoteno delovanje (Simčič 2011).

[12] Natančneje, Amazon ponuja kar petkrat več zmogljivosti kot njegovih najbližjih 14 tekmecev skupaj (Asay 2013).

komunikacijah, Kazenski zakonik, Zakon o varstvu osebnih podatkov in Zakon o tajnih podatkih so le nekateri izmed zakonskih predpisov, ki pomagajo pri urejanju kibernetskega sveta (Ministrstvo za izobraževanje, znanost in šport 2015, vii).

V Sloveniji se je v letu 2014 začela razvijati Strategija kibernetske varnosti, katere namen je vzpostaviti sistem, ki bo zagotavljal kibernetsko varnost v državi. Glavni cilj strategije je zagotoviti varen kibernetski prostor, ki bo koristil državi, gospodarstvu in posameznikom. Eden od ciljev strategije je tudi zatiranje kibernetskega kriminala, ki predvideva »nadgradnjo zakonodaje in prilagajanje postopkov boja razvoju informacijskih tehnologij ter … primerno usposobljenost tožilcev in sodnikov«, vzpostavitev nacionalnega organa, ki bo skrbel za kibernetsko varnost, in zanašanje na pomoč mednarodne skupnosti v okviru NATA in preostalih mednarodnih organizacij (Ministrstvo za izobraževanje, znanost in šport 2014, 4–6). Operativne zmogljivosti za realizacijo strategije v Sloveniji imajo SI-CERT, Sektor za informacijsko varnost, MORS-CERT in Urad za informatiko in telekomunikacije na Policiji. Velik problem teh organizacij je pomanjkanje kadra in materialno-tehničnih sredstev, hkrati pa ni koordinacijskega telesa za strateški nivo (Ministrstvo za izobraževanje, znanost in šport 2015, 6).

Zagotavljanje varnosti ni formalno urejeno in poteka predvsem na neformalni ravni, razen kadar za to obstaja pravna podlaga, kot na primer po 81. členu Zakona o elektronskih komunikacijah (ZEKom-1), ki pokriva »obveznost obveščanja in poročanja o kršitvah varnosti ali celovitosti« med AKOS in SI-CERT. Za zagotavljanje varnosti na spletu sicer skrbijo tudi razni projekti, namenjeni širši javnosti, kot so na primer Varni na internetu, SAFE.SI in Spletno oko. Slovenija prav tako sodeluje na mednarodnih kibernetskih usposabljanjih. Tako je že večkrat sodelovala na vaji Cyber Europe pod okriljem ENISA in Cyber Coalition v okviru NATA (Ministrstvo za izobraževanje, znanost in šport 2015, 7–8; Zakon o elektronskih komunikacijah 2012).

V okviru strategije je tudi akcijski načrt odzivanja v primeru kibernetskih incidentov. Za zdaj operativni nivo obsega sodelovanje nacionalnega odzivnega centra z zunanjimi entitetami, kot so ponudniki internetnih storitev, organi pregona, drugi odzivni centri (CERT-i), mediji, AKOS in ENISA itd. Nacionalni odzivni center SI-CERT predstavlja center kibernetskega sveta znotraj Slovenije, skrbi pa za nemoteno in varno delovanje slovenske internetne infrastrukture in izvaja program usposabljanja na področju odzivanja na omrežne incidente za

Slovensko vojsko. Znotraj SI-CERT ima tudi laboratorij za analiziranje škodljive kode (*malware analysis*) (Ministrstvo za izobraževanje, znanost in šport 2015, ii–iii).

7.1.2 TUJINA

Nizozemska ima v členu 138ab Kazenskega zakonika urejeno, da je vdiranje v računalnike s kakršnim koli sredstvom ali namenom obravnavano kot kaznivo dejanje, ki ti lahko prisluži tudi zaporno kazen. Nezakoniti in namerni vdori v računalnike se kaznujejo z do dvema letoma zapora ali z denarno kaznijo. Tako so kaznovani tisti, ki v nek računalnik vdrejo, ko onemogočijo vse varnostne zadržke, s tehnološkimi sredstvi, s ponarejenimi signali ali kriptografskimi ključi ali pa z uporabo uporabniškega imena in gesla, ki ni njihovo. Če se najdeni podatki shranijo, obdelajo in/ali posredujejo naprej ter uporabijo in izkoriščajo za namene storilca ali neke tretje osebe, storilce teh dejanj čaka do štiri leta zapora ali denarna kazen. Prav tako lahko do štiri leta dobijo tisti, ki so vdrli v telekomunikacijski sistem in so pozneje izkoristili dobljene podatke v lastne namene ali za namene neke tretje osebe ali pridobili neavtoriziran dostop do računalnika tretje osebe (Wetboek van Strafrecht 2015).

V **Indiji** so razmere podobne. Hekerstvo je opisano kot namerna izguba, poškodovanje, uničenje ali izbris računalniških virov, zmanjšanje njihove vrednosti in uporabnosti ter vsaka škodljivost, storjena s kakršnimi koli sredstvi. Vsak, ki izvaja hekerska dejanja, se kaznuje z do tremi leti zapora, finančno kaznijo ali kombinacijo obojega. V Zakonu o informacijski tehnologiji iz leta 2000, ki je bil od takrat popravljen v letih 2006 in 2008, je poudarjena namerna škoda oziroma zavedanje, da škoda lahko nastane, ko storitev izvede kaznivo dejanje (Information Technology Act 2000, 14–15, 19). V popravku iz leta 2008 so bili kibernetski prekrški razširjeni, tako da danes vključujejo tudi sporočila, poslana s komunikacijskimi storitvami, ki so po naravi žaljiva, obscena, zavajajoča, škodljiva itd.; zavestno nelegalno pridobljene računalniške kode in informacijske naprave; krajo identitete; vdor v zasebnost in kibernetski terorizem. Vsa dejanja se kaznujejo z do tremi leti zapora, denarno kaznijo od 100 do 200 tisoč rupij ali kombinacijo obeh, razen kibernetskega terorizma, ki lahko prinese dosmrtno zaporno kazen (IT (Amendment) Act 2008, 9–11).

V **Združenih državah Amerike** obstaja več zakonov, ki prepovedujejo vdiranje v računalniške sisteme. Eden izmed njih (18 U.S.C. 1029) se ukvarja z izdelavo in uporabo naprav in programov za pridobitev nepooblaščenega dostopa do varnih računalniških sistemov ter izvajanje poneverb in prevar. Prekrške se kaznuje z denarno kaznijo, zaporno kaznijo do dvajsetih let ali kombinacijo obojega (Cornell University Law School 2012a).

Drugi zakon (18 U.S.C. 1030) prepoveduje dostop do vladnih računalnikov vsem, ki so brez dovoljenja, s tem pa pridobitev občutljivih informacij, ki so lahko uporabljene v škodo države s prenosom, komunikacijo, zlorabo itd. Hekerji, ki so bili obsojeni zaradi kaznivih dejanj, ki kršijo te zakone, so lahko finančno kaznovani, pogojno izpuščeni ali služijo kazen v zaporu, odvisno od resnosti škode. Kazen lahko traja do dvajset let, kazni pa se med seboj lahko kombinirajo. V primeru povzročitve smrti je lahko kazen dosmrtna (Cornell University Law School 2012b). Vlada pod predsednikom Obamo sicer loči hekerstvo na dva dela – legalnega oziroma *fair play* in nelegalnega. Pod prvega spada hekerstvo v namene varovanja nacionalne varnosti, pod drugega pa vsi napadi za pridobivanje poslovnih skrivnosti, da bi pridobili prednost na trgu. Kitajska in druge države ZDA obtožujejo, da najbolj uporabljajo tako legalno kot nelegalno hekerstvo (Wong 2013).

Tudi v **Veliki Britaniji** so uvedli zakone za računalniški kriminal. V skladu z Zakonom o računalniški zlorabi[13] je za kaznivo dejanje štet vdor v računalnik neke druge osebe z možnostjo izvajanja nadaljnjih kaznivih dejanj. Vdor se kaznuje z denarno kaznijo, do pet let zaporne kazni ali oboje. Kot kazniva dejanja se smatrajo tudi namerna poškodovanja računalnikov, onemogočanje dostopa do programov ali podatkov ter vplivanje na delovanje programov ali zanesljivost podatkov. To se kaznuje z do desetimi leti zapora, finančno kaznijo ali kombinacijo obojega. Razlog za uvedbo tega zakona je bil predvsem strah, da bi posamezniki, zlasti zasebni preiskovalci, lahko pridobili informacije o drugih posameznikih brez njihove vednosti ali soglasja. Posameznik mora imeti pravico, da vse zasebne stvari, ki jih ima na svojem računalniku, obdrži zase, uporabo teh podatkov pa dovoli le s svojim soglasjem. Podjetja morajo skrbeti, da so zasebne informacije njihovih uporabnikov varno shranjene. V večini primerov vdor hekerju prinese razmeroma dolgotrajno kazen, ker obstajajo drugi, resnejši elementi kaznivega dejanja kot samo vdor v računalnik. Vdor v sistem se pogosto uporablja kot metoda za druga, večja kazniva dejanja, kot so goljufije ali tatvine. Vdor v računalnik bi bil le obremenilni dejavnik, ki bi lahko dodatno vplival na kazen, ki jo poda sodnik (Legislation.gov.uk 2007; FindLaw UK 2015).

Na **Kitajskem** je zakonov, ki urejajo kibernetski kriminal, več, ločijo pa se v dve skupini – napadi, ki neposredno ciljajo na računalniške sisteme in informacijske mreže, in druga kriminalna dejanja, storjena z uporabo računalnika in z njim povezanih omrežij. Obstaja sicer

[13] *Computer Misuse Act*

devet širokih kategorij, ki urejajo prepovedana dejanja, materiale in informacije, povezane z internetom. Devet kategorij zajema informacije, ki 1) so v nasprotju z ustavo, zakoni in administrativno ureditvijo; 2) se upirajo režimu države in socializmu; 3) spodkopavajo režim ali sabotirajo enotnost države; 4) spodbujajo etnično nasilje, rasno diskriminacijo ali motijo rasno enotnost; 5) širijo govorice ali motijo družbeni red; 6) širijo fevdalna praznoverja, obscenosti, pornografijo in igre na srečo, spodbujajo nasilje ali teror in nagovarjajo druge k izvajanju prekrškov; 7) javno sramotijo ali očrnijo; 8) škodujejo slovesu ali interesom države in 9) vključujejo vsebino, prepovedano z zakoni (Liang in Lu 2010, 106, 111–112). Prvi poskus urejanja problematike je iz leta 1994, imenuje pa se Odlok za varnostno zaščito računalniških informacijskih sistemov,[14] ki poslancem omogoča nadzor, pregled in vodenje varnostne zaščite računalniških informacijskih sistemov, obenem pa jim dovoljuje preiskavo kriminalnih aktivnosti, ki ogrožajo računalniške mreže (Tai v Liang in Lu 2010, 112). V letu 1997 je posodobljeno kazensko pravo upoštevalo še nepooblaščen dostop do informacij, ki zadevajo državo, obrambo države in njen znanstveni in tehnološki razvoj; dostopanje, brisanje, spreminjanje ali kakršno koli vmešavanje v računalniški sistem, ki ima hujše posledice. Naslovilo je izdelavo in širjenje virusov in druga kriminalna dejanja, kot so finančna prevara, poneverba, kraja državnih skrivnosti ipd. Vnovična posodobitev je prišla v letu 2000, imenovana Odločitev v zvezi z vzdrževanjem internetne varnosti,[15] ki je preuredila kategorije kriminalnih dejanj v šest kategorij, ki so okvirno vsebovale prej omenjene prekrške (Keith in Lin v Liang in Lu 2010, 112–113). Poleg obširne zakonodaje iz let 1997 in 2000 obstaja še nekaj dodatnih specifičnih ureditev za kibernetski kriminal (Liang in Lu 2010, 113). Prva ureditev uporabe interneta je bila sicer predstavljena že leta 1996 pod imenom Začasni pravilnik o ravnanju z mednarodnim mreženjem računalniških informacij[16] (Gomez v Liang in Lu 2010, 113).

7.2 RAVEN MEDNARODNE SKUPNOSTI

Po napadu na Estonijo v letu 2007 je problematika hekerstva postala predmet, s katerim so se morali soočiti mnogi politiki in vodje držav. Kljub obilici literature na to temo v zadnjem desetletju jasno in nedvoumno mednarodno soglasje o pravnem statusu kibernetskega bojevanja doslej ni obstajalo, obenem pa so stališča znanstvenikov mednarodnega prava

[14] *Ordinance for Security Protection of Computer Information System*

[15] *Decision Regarding the Maintenance of Internet Security*

[16] *Interim Regulations on the Management of International Networking of Computer Information*

presenetljivo dosegla visoko stopnjo heterogenosti. So kibernetski napadi prepovedani po doktrini neuporabe sile ali dovoljenih v okviru koncepta samoobrambe? So tudi predmet vojnega prava? Jih obravnavamo kot oborožen napad? Lahko države v primeru priznanega napada uveljavljajo pravico do samoobrambe (Kelsey 2008, 1428–1429; Anastasiou Papanastasiou 2014)?

Poleg teh vprašanj je treba upoštevati tudi vse konvencije, ki so trenutno v veljavi v okviru mednarodnega humanitarnega prava. In čeprav obstaja splošno sprejet dogovor, da morajo pravne omejitve veljati tudi za uporabo kibernetskega orožja v vojni, v okviru mednarodnega prava ni določila, ki bi naslovilo vsakršno uporabo ali eksplicitno prepovedovalo uporabo kibernetskega orožja (Kelsey 2008, 1430). Usklajevanje nacionalnih in mednarodnih kodeksov, pravil in zakonov je prav tako velik izziv zaradi količine vpletenih organizacij in agencij, ki so odgovorne za različna področja (npr. policija, FBI, CIA, MI5) znotraj in zunaj meja držav (Hughes 2009, 21).

Mnogi menijo, da kibernetskega bojevanja ne moremo uspešno uravnavati z obstoječim mednarodnim pravom, in pozivajo k vpeljavi nove konvencije, ki bi regulirala njegovo uporabo. Ideja ima tudi nasprotnike, med katerimi je vlada ZDA, ki so proti vzpostavitvi nove zakonodaje. Izpostavili so, da je razvoj na področju tehnologije, s katerim se razvija tudi kibernetski kriminal, prehiter za vzpostavljanje nove zakonodaje, saj bi bila ta v hipu zastarela (Kelsey 2008, 1430). Poleg tega je velik del mednarodnega prava sestavljen iz priznanih običajnih zakonov narodov, torej orodje za regulacijo že obstaja in ga lahko apliciramo tudi na kibernetsko bojevanje (Hughes 2009, 21).

Konvencija o kibernetski kriminaliteti[17] ali Budimpeštanska konvencija Sveta Evrope izhaja iz leta 2001, stremi pa k zagotavljanju varnosti pred kibernetskim kriminalom s spodbujanjem kooperacije in sprejetja primerne zakonodaje. Po konvenciji, ki služi kot referenčni okvir, se članice zavežejo, da bodo sprejele potrebno notranjo zakonodajo, ki se dotika nepooblaščenih vstopov v računalniške sisteme; prestrezanja prenosov podatkov; naklepnih dejanj poškodovanja, uničenja, izbrisa, spreminjanja ipd. podatkov; uporabe naprav ali programov za storitev kaznivih dejanj; ponaredb in goljufij; in vsebinskih kršitev (npr. otroška pornografija). V konvenciji so določena tudi načela mednarodnega sodelovanja, kar vključuje medsebojno pomoč, izročevanje itd. Leta 2003 je bil konvenciji dodan Dodatni protokol h Konvenciji o

[17] Convention on Cybercrime

kibernetski kriminaliteti,[18] ki ureja rasistična in ksenofobična dejanja znotraj informacijskih sistemov (Council of Europe 2001; MKKKDP[19] 2004).

Razvoj nacionalnih strategij in zakonodaje na področju kibernetike je odvisen od dogodkov, ki se zgodijo znotraj te sfere. Po raziskavah organizacije RAND obstaja pet razlogov, da so države začele z razvojem strategij kibernetske varnosti: napad na Estonijo leta 2007, naraščajoča skrb o kitajskih sposobnostih digitalnega vohunjenja, resni in organizirani kriminalni napadi, visok porast spletnih prevar nižje stopnje in nenehno intenzivno napadanje finančnih sistemov in varovanih vladnih informacij (Robinson in drugi 2013, ix).

Kibernetski kriminal se tiče tudi NATA, ki ima težave v tej neteritorialni domeni. Vsakršna akcija proti kibernetskim grožnjam je lahko hitro zunaj jurisdikcijskega področja. Prav zato je bilo treba previdno oblikovanje novih operacijskih zmožnosti, da bi bila lahko organizacija kos novim izzivom. NATO je tako po napadu na Estonijo leta 2007 izjavil, da je varovanje informacijskih sistemov ključni del transformacije sil organizacije. Najpomembnejši sta komunikacija in koordinacija, predvsem z nevojaškimi organizacijami, ki nadzirajo več kot 90 odstotkov globalne kibernetske infrastrukture. Za tako vrste sodelovanje je potrebna 24-urna pripravljenost, kar je mnoge potisnilo v preoblikovanje struktur, da vključujejo tudi civilno delovanje, in sodelovanje z državami, ki niso članice NATA. Organ za vodenje kibernetske varnosti[20] v Bruslju je tako poskus centraliziranja koordinacije odzivanja na vse kibernetske grožnje. V Talinu so ustanovili Kooperativni center odličnosti za kibernetsko obrambo[21], ki je prvi center, ki bo odgovoren za dolgoročno razvijanje doktrine in strategije kibernetske obrambe. Njegova naloga je raziskati, kako lahko zveza okrepi svojo obrambo. Kljub temu je politično-pravni vidik še vedno šibak, saj mednarodno pravo nima – in mogoče niti ne bo imelo – določene vloge znotraj ofenzivnih in defenzivnih kibernetskih akcij. Zakonov, ki bi urejali to področje, skoraj ni, za kar so morda krive velesile, kot so ZDA, Rusija in Kitajska, ki si želijo več strateške nejasnosti, ko oblikujejo nacionalne kibernetske vojaške sposobnosti. Še en razlog tiči v nizki tehnični izobraženosti diplomatov in zakonodajalcev o problemih

---

[18] *Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems*

[19] Zakon o ratifikaciji Konvencije o kibernetski kriminaliteti in Dodatnega protokola h Konvenciji o kibernetski kriminaliteti, ki obravnava inkriminacijo rasističnih in ksenofobičnih dejanj, storjenih v informacijskih sistemih.

[20] *Cyber Defence Management Authority*

[21] *Cooperative Cyber Defence Centre of Excellence*

kibernetske obrambe. To se sicer lahko kmalu spremeni, ki bodo nove vodilne položaje začele zasedati mlajše, tehnološko bolj podkovane generacije. In čeprav je vloga NATA kot globalne avtoritete v kibernetskem prostoru omejena, organizacija zaradi statusa vodilnega mednarodnega vojaškega zavezništva lahko legitimno začne z razvojem globalne vizije za kibernetski red (Hughes 2009, 19–21; New York Times v Hansen in Nissenbaum 2009, 1156; North Atlantic Council v Hansen in Nissenbaum 2009, 1156).

8 HEKTIVIZEM IN HACKINT

8.1 HEKTIVIZEM

Hektivizem je pogosto definiran kot »zveza med političnim aktivizmom in hekerstvom«. Dejansko gre za običajno državljansko neposlušnost s tehnologijo hekerjev. Tako je prišlo do eksplozivnega širjenja digitalnih kaznivih dejanj za širok spekter političnih vzrokov. Hektivizem lahko definiramo še kot »nenasilen napad z nelegalnimi ali pravno nejasnimi digitalnimi orodji s ciljem doseganja političnih ciljev«. Gre predvsem za spletne napade na tuje računalnike ali omrežja, z namenom motenja delovanja, a brez namena povzročanja resne škode. Definicij je sicer mnogo, a vse se strinjajo, da je hektivizem nenasilen, kar ga z lahkoto ločuje od kibernetskega terorizma (*cyber terrorism*) (Samuel 2004, 1–3; Denning v Samuel 2004, 2). Hektivisti uporabljajo enaka orodja in tehnike kot hekerji, a iz političnih razlogov (Illia v Tanczer 2015, 2).

Hektivizem je direkten, saj tisti, ki ga izvajajo, verjamejo, da je neposredno soočenje učinkovitejše od drugih oblik spletnega aktivizma, kar jih že takoj ločuje od drugih aktivistov, ki uporabljajo splet oziroma digitalna orodja. Kibernetskega terorizma ne uporabljajo, ker se zavedajo človeške blaginje in ji ne želijo škodovati, samega hekerstva pa se izogibajo, ker menijo, da je treba njihove sposobnosti na tem področju izkoristiti za pomembne socialne cilje. Prisotni so zgolj na spletu, kar vidijo kot svojo domeno, predvsem pa zato, ker je globalni splet vse pomembnejše politično prizorišče (Samuel 2004, 3).

Na spletni strani Hacktivismo (2014), ki je stran mednarodne skupine hekerjev, delavcev za človekove pravice, pravnikov in umetnikov, ti navajajo, da verjamejo v zasebnost in dostop do informacij kot človekove osnovne pravice. Prav tako se zavzemajo za prosto dostopnost programske opreme. Kot etična izhodišča za svoje delo navajajo Splošno deklaracijo

človekovih pravic[22] in Mednarodni pakt o državljanskih in političnih pravicah.[23] Njihova misija so vodenje in objava znanstvenih raziskav na področju informacijske tehnologije, komunikacij in elektronskih medijev ter pomoč (če je mogoče) nevladnim organizacijam, skupinam za socialno pravičnost in organizacijam za človekove pravice ob uporabi sodobnih informacijskih tehnologij. Posebej poudarijo, da niso »internetna obveščevalna skupina«[24] in da niso *black hats*, ki bi škodovali drugim za doseganje lastnega ugleda. Prav tako ne stremijo k dobičkom in pravijo, da nikoli ne bodo.

Na spletni strani so objavili tudi deklaracijo, kjer piše, da so resno vznemirjeni nad hitrim širjenjem cenzure interneta, ki ga sponzorirajo države, širi pa se ob pomoči mednarodnih korporacij. Glede prej omenjene cenzure opozarjajo, da je po Splošni deklaraciji človekovih pravic pravica vsakega posameznika do svobode mišljenja in izražanja, ta pravica pa prav tako vključuje svobodo mnenja brez vmešavanja ter iskanje, sprejem in širjenje informacij in idej s kakršnimi koli sredstvi in ne glede na meje. Opominjajo, da so nekatere države Združenih narodov podpisale Mednarodni pakt o državljanskih in političnih pravicah ali pa ga tako ratificirale, da bi državljanom preprečile njegovo uporabo na sodiščih; kljub temu pa slednje države še vedno zatirajo dostop do določenih informacij na spletu. Opozarjajo, da internet hitro postaja način represije, namesto instrument osvoboditve. Priznavajo pravico vlade, da prepove objavo ustrezno kategoriziranih državnih skrivnosti, otroške pornografije in zadev, povezanih s posameznikovo zasebnostjo in privilegiji, ter druge sprejete omejitve, vendar nasprotujejo uporabi državne oblasti za nadzor dostopa do del kritikov, intelektualcev, umetnikov ali verskih osebnosti. Poudarjajo, da sponzorirana cenzura interneta razjeda miren in civiliziran soobstoj, ki vpliva na uresničevanje demokracije, ter ogroža socialno-ekonomski razvoj narodov. Menijo, da je podprta cenzura spleta huda oblika organiziranega in sistematičnega nasilja nad državljani, ki je namenjena ustvarjanju zmede in ksenofobije ter je obenem kršitev zaupanja. Zato izjavljajo, da bodo preučili načine in sredstva za izogibanje državno-sponzorirani cenzuri interneta in bodo uvedli tehnologije za izpodbijanje kršitev pravice do informacij (Cult of the Dead Cow 2001; Hacktivismo 2001).

Po zgornjih navedbah je očitno, da ne gre za zlonamerne napade, kar lahko pripisujemo kibernetskim teroristom ali *black hats* hekerjem, ki škodujejo za pridobitev lastne koristi in za

[22] *Universal Declaration of Human Rights*

[23] *International Covenant on Civil and Political Rights*

[24] *Internet Intelligence group*

povzročitev čim večje škode nič hudega sluteči populaciji. Hektivisti so tako novodobni Robin Hoodi spleta.

Med najbolj znanimi skupinami hektivistov je skupina *Anonymous*, ki je razširjena po vsem svetu, prepoznavna pa je predvsem po maskah, ki zakrivajo obraze članov. Skupina je povezana z velikimi imeni, kot je WikiLeaks, kar jim je prislužilo hudo preganjanje. Njihovo udejanjanje naj bi segalo v leto 2008, ko so protestirali verski manjšini scientologov z DDoS-napadi in izdajo dokumentov, a so od takrat močno razširili svojo prisotnost po vsem svetu. V ospredje so prišli predvsem med svetovnimi protesti proti bankam, bankirjem, vladam ipd. pred nekaj leti, zadnja leta pa so močni podporniki Gaze v njenih konfliktih z Izraelom (Waites 2011; Peck 2013; Schwartz 2012).

Njihovo delo je bilo sprva namenjeno le šalam na spletu, a so se zaradi scientologije začeli vse bolj politično udejanjati. Točne definicije zanje dejansko sploh ni, saj imajo velik spekter dejanj, ki jih izvajajo, od norčevanja in zbadanja do resnih političnih sodelovanj. Ker nimajo centraliziranega vodstva oziroma sploh nimajo neke hierarhije v organizaciji, določenih vodij in geografskega epicentra, je težko o njih povedati kar koli odločilnega. *Anonymous* so prej blagovna znamka (*brand*) kot struktura, njihova dejanja so podprta z liberalnimi vrednotami in anarhističnimi težnjami. Komentatorji političnih dejanj si zaman prizadevajo opisati etiko, sociologijo in zgodovino skupine znotraj že ustaljenih parametrov. Vsak se lahko po svoje politično udejanja na spletu pod krinko anonimne skupine, kar mnogi izkoriščajo za ilegalna in kriminalna dejanja, mnogi pa pozabljajo oziroma niti ne vedo, da člani skupine, ki so podpirali WikiLeaks, niso iste osebe, ki so leta 2008 protestirale proti scientologiji (Coleman 2011; Krupnick 2011; Šimek 2012).

Njihov najnovejši projekt je ISIS oziroma Islamska država, ki so ji člani organizacije napovedali vojno. Z več mesecev dolgo akcijo so se lotili nadzorovanja spleta, kjer so iskali spletne strani in račune na družabnih omrežjih, ki so bili v podporo Islamski državi. S ciljem razkrinkanja so napadli strani in račune, ki so se izkazali v podporo ekstremistom, ki so širili propagando, uporabljali račune za potrebe obveščevalne dejavnosti, rekrutirali nove člane ipd., *Anonymous* pa niso ušla niti podjetja, ki ponujajo gostovanje takim spletnim stranem. Mnogokrat se namreč zgodi, da podjetja vedo, v kakšne namene se uporabljajo njihove storitve, a zaradi dobrega zaslužka to spregledajo. Med podjetji na seznamu skupine so se znašla velika imena iz Evrope, Velike Britanije in ZDA, na primer Yahoo! Europe. V okviru spletne kampanje #OpISIS je bilo po poročanju skupine napadenih 233 strani, od tega so jih

uničili 85. Prijavili in odstranili naj bi tudi 25 tisoč Twitter računov, a ta tehnika je dokaj neučinkovita, saj so bili izgubljeni računi hitro nadomeščeni (Cuthbertson 2015). Poleg spletnega napada naj bi skupina razkrila tudi domnevne tehnične strokovnjake ISIS in jih prijavila primernim organom. Razlog za napad je poskus pritiska na Twitter, da se začne aktivno ukvarjati z nadziranjem ekstremističnih računov. Čeprav se Twitter s tem delno že ukvarja, mnogi računi vseeno uidejo moderatorjem podjetja. In čeprav skupina kaže manjše uspehe na področju umikanja škodljive vsebine, ZDA morda te pomoči ne potrebujejo. Zaposleni v obveščevalnih uradih namreč želijo, da vsebina ostaja na spletu, saj s tem lažje nemoteno nadzirajo dogajanje na vzhodu in zbirajo informacije, saj so družabni mediji eden od virov, ki prikazuje tekoče stanje organizacije (Daileda in Franceschi-Bicchierai 2014; McKay 2015).

Člani *Anonymous* prihajajo iz različnih okolij in ozadij. Nekaj jih je dejanskih hekerjev, ki skrbijo za napade, kjer skupina onemogoča dostop do strani, izvajanje nalog spletnih portalov, onemogočanje dostopanja do informacij in podobno. Večina drugih je sicer tehnološko precej izobraženih, a skrbijo bolj za grafično podobo, videoposnetke in tako naprej. Predvsem gre za vključitev zaradi osebnih prepričanj in želje po enakosti, pravičnosti in miru (Coleman 2011).

Čustva do skupine so različna, a so povsem bipolarna – mnogi jih podpirajo, mnogim so vandali in nadloga. Ljudje so se v razmerju do njih opredelili za eno ali drugo stran. Napadeni jih vidijo predvsem kot težavo in spletni vandalizem, medtem ko so mnogi prepričani, da gre za zaveznike. Visoko priljubljenost v zadnjih letih vse bolj pridobivajo med mladimi, predvsem s protesti proti kapitalizmu, modernim sistemom držav, spletni cenzuri in podobnemu (Krupnick 2011; Coleman 2011).

Čeprav napadi v večini primerov ne povzročijo velike škode, so člani zadnja leta že večkrat preplačali svojo vpletenost. Mnogi so namreč soočeni z zapornimi kaznimi od nekaj mesecev do več let in s hudimi denarnimi kaznimi za povračilo škode, ki je bila storjena med napadom. Mnogim so določene tudi ure družbeno koristnega dela. Predvsem so pomembne stopnja vpletenosti v napad, vrsta napada in starost napadalca (Parker 2014).

Čeprav se mnogokrat zdi napad precej neškodljiv, državni organi vse bolj poudarjajo grožnjo hektivistov v zameno za financiranje delovanja. Profesor Peter Ludlow z Northwestern University je dejal, da organizacije, kot sta NSA in FBI, denarja za delovanje ne dobijo, če ne

prepričajo vlade in zasebnih podjetij, da so v nevarnosti.[25] A mnogi se ne strinjajo z močnim kaznovanjem, ki ga izvajajo predvsem v ZDA. Gabriella Coleman, profesorica z McGill University v ZDA in glavna znanstvenica s področja *Anonymous*, je dejala, da je sicer razumno pričakovati kazen, če se izvaja nezakonita dejanja, a da so kazni v primeru hektivistov, ki povzročajo zanemarljivo škodo, prehude. Meni, da je to zgolj norčevanje iz demokratičnega procesa in iz pravice ljudi do protesta[26] (Parker 2014).

8.2 HACKINT

Paul McFedries na svoji spletni strani HACKINT oziroma *Hackint* opiše kot »skrivne informacije, predvsem vojaške narave, ki so bile pridobljene z vdorom v računalniški sistem«.[27] Citat je vzet iz časnika *The Daily Telegraph,* kjer se je beseda pojavila v članku 'Web speak' 25. oktobra 2001. McFedries sicer navaja, da je bil prvi znani zapis te besede 4. oktobra 2001 v *The Times of London* (McFedries 2001).

Beseda je sestavljena iz dveh besed – *hacking* (hekerstvo) in *intelligence* (obveščevalna dejavnost), kar bi po slovensko torej pomenilo **hekerska obveščevalna dejavnost** (McFedries 2001). Gre za način pridobivanja podatkov s hekerstvom (in tako spada med druge, bolj znane načine pridobivanja informacij s strani obveščevalne dejavnosti, npr. OSINT, HUMINT ipd., omenjene že na začetku te naloge).

8.2.1 IMPLEMENTACIJA

Zbiranje podatkov s strani države je stara tehnika, ki je starejša od HACKINT-a. Vsaka vlada že desetletja izvaja tako imenovani *data mining,* s katerim zbira podatke o državljanih in nevarnostih, ki jih ti povzročajo. Vse od sredine devetdesetih let prejšnjega stoletja lahko zaznamo visoko povečanje zbiranja takšnih informacij – vsako leto se količina skoraj podvoji. Da je stvar še lažja, se zmogljivost računalnikov močno povečuje, cene pa se zmanjšujejo. Vsekakor bi bilo nespametno, da bi države zavrgle takšno možnost, kar so mnoge pokazale z vpeljavo taktike brez slehernega obotavljanja (Slobogin 2008, 317).

---

[25] »The only way they can get money is if they can convince the government and private business that we are under threat. Otherwise, it all goes away.« (Parker 2014)

[26] »But to really hammer the individuals for political action when the damage to these companies is nonexistent? It's just a mockery of the democratic process and the right of people to protest.« (Parker 2014)

[27] »Hacking Intelligence — information that has been obtained by hacking into a computer system and used for military purposes.« (McFedries 2001)

Pred napadom leta 2001 so v ZDA nadzorovali predvsem prevarante, ki bi želeli škodovati državi, *data mining* pa so uporabljali tudi za nadzor uspešnosti različnih programov. V zadnjih letih, predvsem pa po 11. septembru, so začeli z uporabo sistema za odkrivanje kriminala in terorizma (Slobogin 2008, 317). S povečevanjem nevarnosti se povečujeta tako želja kot morda tudi potreba po večjem nadzoru spleta.

Ministrstvo za pravosodje v ZDA je v letu 2014 dvignilo prah z namenom širjenja svojih moči v digitalne vode. Hočejo namreč dovoljenje za zbiranje, prebiranje in zaseganje digitalnih informacij zunaj območja svoje jurisdikcije, čemur Google ostro nasprotuje. Po mnenju spletnega giganta to namreč pomeni, da bi se s tem odprla vrata vladnemu hekerstvu v katerem koli objektu na svetu. Obrnili so se na predložitveni odbor v Washingtonu, ki resno razmišlja o predlaganih spremembah. Dejali so, da bi imelo sprejetje teh sprememb močne ustavne, pravne in geopolitične posledice, zato je bolje, da o vsem skupaj odloča kongres. Google je mnenja, da bi FBI tako dobil dovoljenje, da izvaja prikrite napade na strežnike po vsem svetu, kar bi jim omogočilo dostop do ogromne količine zasebnih informacij. Ne glede na namen, da se išče le po ZDA, Google meni, da je to nemogoče zagotoviti (Pilkington 2015; Bennett 2015a).

Google predvsem skrbi želja, da bi FBI izvajal nadzor na daljavo, predvsem na računalnikih, ki imajo prikrito geografsko lokacijo. To bi pomenilo, da se nadzor izvaja tudi zunaj meja ZDA. Google pa ni edini, ki je podal svoje mnenje na to temo. Njihova nasprotovanja in še 37 drugih mnenj bo pregledal precej neznan Svetovalni odbor o kazenskem pravilniku,[28] ki ga sestavljajo večinoma sodniki in ki je odgovoren za zvezna pravila in zakone, tudi tiste, ki se tičejo FBI (Pilkington 2015; Bennett 2015a).

Za zdaj še velja, da vsi agenti, ki želijo nalog za preiskavo, zanj zaprosijo pri sodniku, ki je odgovoren za določeno okrožje, kjer naj bi preiskava potekala. Sodniki so omejeni z izdajo nalogov le znotraj svoje pristojnosti. A ministrstvo za pravosodje meni, da v času računalnikov to ni več optimalna rešitev, zato iskanje zunaj okrožja – se pravi na spletu – zahteva spremembe v zakonodaji, kar bi obenem olajšalo tudi trenutne logistične težave. Računalniki lahko pokrivajo več jurisdikcij in pridobivanje več kot enega naloga zaplete reševanje problema. Še enkrat so poudarili, da bodo preiskovali predvsem tiste naprave, ki skrivajo svoj geografski izvor, in da ne bodo izvajali pregledov brez sodnega naloga. Menijo,

[28] *Advisory Committee on Criminal Rules*

da je prav tam največja težava – vse več ljudi izkorišča spletno anonimnost in se s skrivanjem IP-naslovov izmika oblastem. Zato je veliko težje določiti, v katero okrožje mora FBI po nalog za preiskavo, kar otežuje delo agencije. Dodali so, da bi nove pristojnosti izvajali le, če bi obstajal »verjeten vzrok za iskanje ali zaseg dokazov ali za izvršitev kaznivega dejanja«[29] (Bennett 2014; Pilkington 2015; Bennett 2015a).

Kljub temu pravne skupine ostajajo neprepričane, saj menijo, da je oblika zapisa prošnje po spremembah preveč ohlapna in nejasno določa nove pristojnosti FBI, kar bi lahko imelo katastrofalne globalne posledice. Ameriška zveza za državljanske svoboščine[30] je dodala, da bi bile posledice tudi nacionalne, saj bi nove spremembe lahko kršile 4. amandma ameriške ustave, ki prepoveduje nerazumne preiskave in zasege. Eden od tehnologov ACLU, Christopher Soghoian, dodaja, da gre za nevarno željo po ekspanziji moči, saj si FBI želi prikrito dostopati do informacij, med drugim tudi z uporabo škodljive programske opreme (*malware*) (Bennett 2014; Pilkington 2015).

FBI že 15 let razvija svoje tehnike za računalniški nadzor in zadnje čase vse pogosteje uporablja »tehniko mrežne preiskave«, [31] ki na preiskovane naprave vgradi škodljivo programsko opremo, kar omogoča agentom obvladovanje te naprave. S to tehniko lahko vklapljajo ali izklapljajo kamere in zvočne snemalnike, prenašajo celotno bazo podatkov in dostopajo do vseh preostalih naprav, ki so povezane v isto omrežje. Google je do teh dejanj kritičen, saj meni, da bi s tem lahko oškodovali tretje osebe, katerih zasebne informacije bi bile zasežene v masovnih zasegih agencije (Pilkington 2015).

Prihaja predvsem do obtožb hipokrizije, predvsem v času, ko so ZDA stalno pod napadom tujih držav. Med zadnjimi v nizu napadov, ki so se zgodili, je bil napad na produkcijsko hišo Sony, zakrivila pa naj bi ga Severna Koreja, čeprav za to ni dokazov, kar je potrdil tudi FBI. Razlog za povezavo s Severno Korejo morda izhaja zgolj iz uporabljenega programskega orodja, ki spominja na programsko opremo prejšnjih napadov, ki jih je zakrivila azijska država. Prav zaradi teh napadov je kibernetska varnost postala del politike, ki je vse pomembnejši, predvsem za ameriško vlado. Prav zato jim očitajo predlagane spremembe, saj se z njihovo uresničitvijo dejanja FBI ne bodo razlikovala od dejanj napadalcev. Google je

[29] »Probable cause to search for or seize evidence, fruits, or instrumentalities of crime« (Pilkington 2015).

[30] *American Civil Liberties Union* (ACLU)

[31] *network investigative techniques* (NITs)

prepričan, da ameriška vlada tvega diplomatske odnose s tujino, ki jih je pridobivala več let in ki dovoljujejo čezmejne preiskave, a le če se z njimi strinjajo vse udeležene strani (Biddle 2014; Pilkington 2015).

Že oktobra prejšnjega leta je direktor FBI James Comey dejal, da je problem v enkripciji, ki nas vse vodi v temne kraje. Vprašal se je, če smo postali tako nezaupljivi do vlade in izvajalcev kazenskega pregona, da smo pripravljeni pustiti zlonamernim akterjem, da prosto odidejo, in s tem pustiti žrtvam, da same skušajo najti pravico zase[32] (Pilkington 2015; Cook 2015).

Sicer pa to ni prvič, da bi država posegla po tej obliki nadzora. Danes že daljnega leta 2001 sta dva italijanska programerja pod spletnimi imeni ALoR in NaGA napisala program Ettercap, ki je hitro postal zelo priljubljen. Šlo je za odprtokodni brezplačni program, ki je omogočal prisluškovanje, dostop do gesel in oddaljeni dostop in manipulacijo računalnikov, zato so ga hitro uporabljali ne le tisti, ki so imeli zle namene, ampak tudi analitiki, ki so z njim testirali lastna omrežja (Jeffries 2013).

Program je bil tako dober, da sta avtorja, s pravimi imeni Alberto Ornaghi in Marco Valleri, dobila klic s strani milanske policije, ki je želela program zase. Prosili so namreč za različico programa, ki bo na napravah z operacijskim sistemom Windows omogočala prisluškovanje pogovorom po Skypu. Tako je majhna agencija za varnostno svetovanje postala prvi distributer hekerske opreme za policijo. Podjetje Hacking Team, ki je bazirano v Milanu, a ima pisarne tudi v tujini, je imelo leta 2013 že 40 zaposlenih, svoje izdelke pa naj bi prodajalo več ducat državam na šestih kontinentih (Jeffries 2013; The Enemies of Internet 2015).

Oprema podjetja Hacking Team naj bi bila celo boljša kot kontroverzna oprema PRISM[33] ameriške NSA, saj lahko z njo policija zbere ogromne količine podatkov – sledijo lahko telefonom, Skype, Yahoo Messenger, Google Talk in MSN Messenger pogovorom, elektronski pošti, iskalni zgodovini v brskalnikih, uporabijo pa lahko tudi mikrofone in kamere prenosnikov tarč. Oprema je narejena tako, da obide vse varnostne ovire, kot je

[32] »Have we become so mistrustful of government and law enforcement in particular that we are willing to let bad guys walk away, willing to leave victims in search of justice?« (Pilkington 2015)

[33] *Planning Tool for Resource Integration, Synchronization, and Management* je orodje za shranjevanje in obdelavo informacij, ki se pretakajo preko ameriških strežnikov. Obstoj orodja je javnosti izdal Edward Snowden, kasneje pa ga je potrdila tudi ameriška vlada (Dreyfuss in Dreyfuss 2013).

antivirusna oprema, in na napravi tarče deluje povsem nevidno. Poleg tega podjetje za svoje programe nudi tudi funkcije po meri uporabnika, redne posodobitve in tehnično podporo, kar je redka novost v panogi. Hacking Team pa ni več edino podjetje, ki ponuja takšne storitve. Danes imajo konkurenco, med večjimi imeni pa najdemo še Gamma International in VUPEN (Jeffries 2013; Zetter 2013; The Enemies of Internet 2015).

A vse ima svoje meje, tudi komercialna hekerska oprema. Podjetje Hacking Team svojih izdelkov ne prodaja državam, ki so na NATO, EU ali ZDA črni list (*blacklist*). Njihove storitve so na voljo le organom pregona in obveščevalnim službam. Te trditve podjetja vsekakor niso pomirile kritikov, ki menijo, da oprema ni primerna, saj je večkrat prišla v napačne roke in povzročila marsikatero nadlogo. Najbolj odmevni so trije primeri:

1. Napad na ameriško državljanko, ki naj bi dobila elektronsko pošto prijatelja, zaposlenega na Harvardu, v kateri se je skrivala povezava za *phishing*[34] napad na turški spletni strani. Na strani je bila datoteka, ki se je namestila na računalnik, povezana pa naj bi bila prav z opremo podjetja Hacking Team. Naslovnica se je sama zavedla pasti in pustila podjetju Arsenal Consulting, ki se ukvarja z digitalno forenziko, da ustvari vabo, ki je sprožila napad. Datoteke niso dobili, kljub temu pa je sum na opremo podjetja Hacking Team močan. Vse to seveda sproža še debato o tem, ali je šlo za napad, sponzoriran s strani turške vlade (ki je tudi del NATA), ki je na ozemlju ZDA vohunila za ameriško državljanko.
2. Oprema podjetja naj bi se po poročanju uporabila v Maroku, kjer se je pojavila na računalnikih prodemokratične novičarske strani Mamfakinch, kar je časnik privedlo v težave.
3. Tretji primer navaja aktivista Ahmeda Mansoora v Združenih arabskih emiratih, ki naj bi na svoj računalnik prejel trojanskega konja, ki naj bi izhajal iz podjetja Hacking Team (Jeffries 2013; Zetter 2013; The Enemies of Internet 2015).

Podjetje Hacking Team vse očitke zavrača. Kritik je sicer relativno malo in le redke se dotikajo moralnega vidika programske opreme – nekateri kritiki so mnenja, da je sama oprema nevarna že zato, ker bi lahko države oziroma organizacije (policija, obveščevalne

[34] *Phishing*, slov. spletno ribarjenje, je kraja podatkov preko spleta. Običajno gre za vabo, ki uporabnika popelje na lažno spletno stran, ki odtuji pomembne podatke (npr. lažne bančne strani, ki zahtevajo bančne podatke, tat pa s tem lahko dostopa do tujih bančnih računov) (SI-CERT 2015).

službe), ki sicer ustrezajo merilom prodaje in opremo kupijo legalno, izkoristile novo pridobljeno moč. Podjetje trdi, da se zaveda moči svoje opreme, zato je zelo selektivno pri njeni prodaji, a vsekakor ne more zagotoviti, da se zlorabe ne bi pojavljale. V primeru teh namreč ne more storiti veliko (Jeffries 2013; Zetter 2013; The Enemies of Internet 2015).

8.2.2 SWOT-ANALIZA HACKINTA

SWOT-analiza temelji na štirih različnih polih, ki jih lahko raziščemo med analizo predmeta – prednosti, slabosti, priložnosti in grožnje. Poli se ločijo na notranje in na zunanje, kjer lahko na notranje (prednosti in slabosti) vplivamo sami, na zunanje (priložnosti in grožnje) pa ne moremo. Priložnosti se nam ponujajo same in jih lahko zgolj izkoristimo, ko pa se pojavijo grožnje, se jim lahko zgolj izognemo. S SWOT-analizo obdelamo vse možne vidike predmeta, kamor na primer spadajo dejavnost kot celota, njena zakonodaja, razvoj predmeta, vodstvo in zaposleni, finance itd. (Doren 2012).

S SWOT-analizo HACKINT-a bom skušala prikazati, ali je HACKINT dejavnost, ki jo država potrebuje. Analizirala bom prednosti in slabosti dejavnosti same in raziskala, kakšne so v primerjavi s prednostmi in slabosti, če dejavnost vpeljemo v državni sistem. Raziskala bom tudi priložnosti, ki se ponujajo za vpeljavo in izboljšanje panoge, ter grožnje, ki se pojavljajo tako ob HACKINT-u kot zaradi njega.

8.2.2.1 Strengths – prednosti

HACKINT omogoča dodaten nadzor nad lastno državo, obenem pa prispeva dodatno stopnjo varnosti. V današnjem času vsakdanjik mnogih ljudi poteka večinoma po spletu, v to množico ljudi je vštetih tudi mnogo kriminalcev. Teroristični napadi se danes pogosto načrtujejo kar po računalniku; ljudi se novači na družbenih omrežjih, orožje se kupuje na spletnih črnih trgih ipd., na spletu pa lahko najdemo tudi prosto dostopne načrte za izdelavo bomb. Obveščevalna dejavnost bi tako z notranjim nadzorom lažje spremljala take dejavnosti in s tem dvignila uspešnost preprečevanja takšnih katastrof.

Na drugi strani bi lahko s HACKINT zbiranjem podatkov vsaka država nadzorovala tudi druge države in njihove dejavnosti. Po eni strani bi nadzirala njihove politične in vojaške aktivnosti, preverjala njihovo spoštovanje dogovorov in sporazumov ter z dostopom do gospodarskih informacij vplivala na mednarodni trg. Prav tako bi lahko pomagala njihovim silam pri notranjem nadzoru, skupaj pa bi se lahko uspešneje borili proti mednarodnemu kriminalu.

Kljub temu bi z vsesplošno uvedbo HACKINT-a v obveščevalne sisteme vse države spet vzpostavile neke vrste *status quo*. Tako kot je bilo z oboroževalno tekmo, kjer so se ves čas med seboj ogrožale s tem, da so lovile ena drugo po količini orožja, bi z vpeljavo HACKINT-a vse države sicer imele odlično orožje, ki bi kaj kmalu pomenilo izgubo prednostnega položaja, ko bi imeli tak sistem vsi. Po eni strani bi bile vse države izpostavljene napadu, s tem pa vse njihove strateške, vojaške in politične ambicije, a obenem bi s takim sistemom vse države imele sposobnost napade zavrniti. Tako bi mednarodno vohunjenje kmalu postalo brezpredmetno.

8.2.2.2 Weaknesses – slabosti

Glede na zgornje načine uporabe HACKINT-a se ob prednostih seveda takoj pojavijo tudi slabosti. Te so bile omenjene že prej, ko so ZDA z namigi o HACKINT-u dvignile veliko prahu. Če država vpelje HACKINT, lahko hitro pride do zlorab in čezmernega nadzora, kar lahko vodi v totalitarno državo in sistem, ki temelji na stalnem nadzoru *Big Brother*.

Dejstvo je, da pri zbiranju informacij po spletu ne moremo zagotoviti, da bomo zbirali samo tiste informacije, ki nam jih je dovoljeno zbirati. V zbranih paketih se hitro najdejo osebne informacije, do katerih država nima pravice dostopati. Mogoče jih ne bi uporabila takoj, jih je pa vredno shraniti.

To se danes že dogaja; velika podjetja, kot je Facebook, so bile že mnogokrat na udaru zaradi podatkov, ki ostanejo v njihovih bazah tudi po tem, ko uporabniki že izbrišejo svoje račune (BBC 2009). Problem nastane, ko ne gre zgolj za imena in priimke, v tej bazi so pogosto tudi bančni računi, naslovi in telefonske številke, ki jih podjetja vestno shranjujejo na svojih strežnikih. Kljub obljubam, da tega ne počnejo in da je marsikje kup zakonov, ki ščitijo ljudi pred tako zlorabo, ni nikjer zagotovila, da osebe, ki imajo dostop do teh podatkov, zbranega ne zlorabijo in da tega ne bi počela tudi vsaka država, če bi imela to možnost.

Če bi vsaka država imela opcijo napasti drugo državo in z državnim hekerstvom dostopati do vseh mogočih pomembnih informacij, bi se države lahko zavarovale z zavajanjem. V primeru napada bi lahko strateško nastavljene lažne informacije zavedle napadalce v mišljenje, da so dobili kup pomembnih podatkov v napadu, dejansko pa bi šlo za neškodljiv napad.

8.2.2.3 Opportunities – priložnosti

Z uvedbo HACKINT-a se ponujajo mnoge priložnosti v smislu izravnavanja mednarodnega političnega polja. Države, ki bi prve uvedle HACKINT, bi imele določen čas veliko prednost.

Nadzorovale bi lahko politične, vojaške in gospodarske vidike držav, za katere se še posebej zanimajo, ne glede na to, ali gre za sovražne ali zavezniške sile.

Po najboljšem scenariju bi zgolj izvajale nadzor in skrbele za korektno delovanje, preprečevale bi kršenje zakonov, sporazumov in pravic. Posledično bi iz strahu nad stalnim nadzorom vse države delovale pregledneje in z manj kršitvami.

Po drugi strani tak sistem omogoča plodna tla za nov val skrivnosti in zavajanja. Vsaka država bi poskusila poiskati nove načine, kako prikriti svoje delovanje in ohraniti državne skrivnosti tajne. Prav vsak akter v mednarodnih odnosih ima namreč nekaj interesov, ki niso javno dostopni, ki jih ne deli z drugimi akterji in katerih obstoj vestno prikriva. Prav te informacije so najbolj želene in HACKINT je zanje ena večjih groženj. Prav zato je zelo verjetno, da bi vsaka država našla nove načine prikrivanja, ki bi lahko vsebovali že prej omenjeno zavajanje in nastavljanje vab z lažnimi podatki.

8.2.2.4 Threats – grožnje

Z uvedbo HACKINT-a kot veje obveščevalne dejavnosti vsaka država izpostavi samo sebe drugim državam. Če ima vsaka od njih svojo enoto, so vse približno enako šibke – razlikujejo se le po finančni podpori enote in po izkušenosti zaposlenih v enoti. Prednost take enote se kaj kmalu izniči, vsaj v mednarodnem merilu vohunjenja.

Grožnjo bi predstavljal predvsem napredek v opremi in znanju zaposlenih, s tem pa bi se lahko porajala možna kraja opreme. Nevarnost lahko povzročijo tudi zaposleni, ki so najšibkejši člen v taki verigi. Izdajanje skrivnosti, prodaja programske opreme ipd. so stvari, ki lahko zaradi sebičnih interesov dosežejo vrtoglave cene in imajo katastrofalne posledice.

Vpliv na trg prav tako ni zanemarljiv. Po dobri plati bi se lahko povečala konkurenčnost, znižale bi se cene produktov, monopolizem bi opešal ipd., a seveda je pri takih stvareh tudi slaba stran. S krajo poslovnih idej bi lahko kaj hitro prišlo do monopola na trgu, če bi država, ki ukrade načrte oziroma poslovne ideje, te načrte izpeljala, preden jih je nameravala na trg poslati druga država. Te načrte se lahko tudi posodobi, nadgradi ipd. in izdelek države, ki si je vse skupaj zamislila, kaj kmalu postane brezpredmeten. Še ena stran takih kraj je izsiljevanje z odkupnino ipd., kar lahko resno poškoduje države, mednarodni trg in mednarodne odnose.

8.2.2.5 Primerjava

Iz SWOT-analize lahko razberemo, da gredo nekatere prednosti in priložnosti z roko v roki; enako velja tudi za slabosti in grožnje. Predvsem je razvidno, da vpeljava HACKINT-a v

državni sistem zagotavljanja varnosti v državi ne prinaša dovolj prednosti, slabosti pa precej. Čeprav se lahko poveča varnost držav in mednarodne skupnosti in obstaja možnost za boljši nadzor trga, predstavljajo velik problem sebični interesi posameznih držav. Tem se v zameno za večjo varnost, enakost in mir veliko držav ne bi želelo odreči, nedvomno pa bi sledilo izkoriščanje moči.

9 ŠTUDIJA PRIMEROV

9.1 PRISLUŠKOVALNE AFERE ZDA

Amerika je bila v zadnjih letih večkrat tarča afer prisluškovanja, še najbolj odmevno zaradi prisluškovanja nemški kanclerki Angeli Merkel. Obama naj bi prisluškovanje odredil že leta 2010, poročajo nemški časopisi, a zadeva naj bi segala še dlje, v leto 2002, ko je Angela Merkel vodila opozicijo, leta pred kandidaturo za kanclerko. Vse skupaj naj bi se končalo poleti 2013, tedne pred obiskom Obame v Berlinu. Obama je takrat zagotovil, da telefon Angele Merkel *trenutno* ni nadzorovan in v prihodnosti tudi ne bo, a dogodkov iz preteklosti ni želel komentirati (Sherwell 2013; Moulson in Dahlburg 2013; Appelbaum in drugi 2013).

Podobne pritožbe so prišle tudi iz Francije in Brazilije ter še nekaj drugih držav. Ameriški zavezniki so sicer vedeli, da jih ZDA nadzorujejo, a niso vedeli, do kakšne mere. Francoska predstavnica vlade je dejala, da so taka dejanja nesprejemljiva, ker se dogajajo med zavezniki, obenem pa so primer poseganja v zasebnost. Brazilska predsednica Dilma Rousseff je v luči teh dogodkov odpovedala obisk Washingtona. Na prisluškovanje se je odzval tudi italijanski premier Enrico Letta, ki je o vsem skupaj govoril z Johnom Kerryjem. Ta je zagotovil, da se ZDA trudijo najti pravo razmerje med zagotavljanjem varnosti glede na potrebe in ohranjanjem zasebnosti glede na pričakovanja (Moulson in Dahlburg 2013).

Bernard Kouchner, nekdanji zunanji minister Francije, je v radijskem intervjuju dejal, da je treba sicer priznati, da tudi Francija prisluškuje, saj vsi prisluškujejo vsem, a da je problem v tem, da nimajo enakih pogojev kot ZDA, zaradi česar so druge države ljubosumne (Sherwell 2013; Moulson in Dahlburg 2013).

ZDA se zavedajo, da bi razkritje teh afer pomenilo hud udarec za odnose z Evropo, a zagovorniki prisluškovalne prakse menijo, da bi morali biti Evropejci hvaležni, da se je to zgodilo, saj Amerika s tem nadzira možne teroristične grožnje. Mike Rogers, predsednik odbora za obveščevalno dejavnost (*intelligence committee*) predstavniškega doma (in prav

tako republikanec), je dejal, da če bi francoski državljani vedeli, za kaj zares gre, bi iz hvaležnosti že ploskali in odpirali šampanjec. Peter King, republikanski kongresnik, je stopil na stran Rogersa in dejal, da bi se Obama moral nehati opravičevati za dejanja NSA. »Realnost je, da je NSA rešila na tisoče življenj, ne samo v ZDA, ampak tudi v Franciji, Nemčiji in po vsej Evropi. Odkrito povedano je NSA storila veliko za našo državo in za predsednika, on je vrhovni poveljnik. On bi moral stati za NSA.«[35] (Sherwell 2013).

John Schindler, nekdanji uslužbenec NSA, je poudaril, da je bil napad na dvojčka v New Yorku leta 2001 načrtovan v Nemčiji. Na omrežju Twitter je opozoril, da bi Nemčija izvajala strog nadzor na ZDA, če bi bil napad v Nemčiji in načrtovan v Ameriki. Tudi nekaj nemških obveščevalcev je stopilo na stran ZDA, med katerimi je eden od njih dejal, da bi brez informacij iz Amerike Nemčija utrpela več terorističnih napadov v preteklosti (Sherwell 2013).

Kljub vsem obljubam Obame so se nove obtožbe vohunjenja v Nemčiji spet pojavile julija 2014. V začetku meseca je bilo odkrito, da ZDA vohunijo po obrambnem ministrstvu Nemčije. To je prišlo na dan le teden po odkritju delavca nemške tuje obveščevalne agencije. Ta je bil aretiran na podlagi suma, da je obveščevalec CIA. Priznal je, da je pošiljal informacije svojemu kontaktu v ZDA. Temu je sledil ukaz Nemčije, da se direktor CIA oddelka iz Nemčije takoj vrne v Ameriko. Javno ogorčenje nad razodetji je močan pritisk na Angelo Merkel, od katere zahtevajo resne ukrepe proti ZDA (Breidthardt in Siebold 2014).

9.2 KITAJSKI NAPADI NA ZDA

Napadi, ki naj bi jih zakrivila Kitajska, segajo že nekaj let v preteklost, predvsem pa gre za kibernetsko vohunjenje, ki se je začelo v vladnih agencijah in se je razširilo tudi v zasebni sektor za pridobivanje prednosti pred zahodno tržno konkurenco. Med letoma 2007 in 2009 je bila država obsojena kraje načrtov bojnega letala F-35 z računalnikov podjetja, ki ga je Pentagon najel za izdelavo zračnega plovila. Kitajsko bojno letalo F-31 je po mnenju mnogih podobno ameriški različici, ugibanja o tehničnih zmožnostih pa še ostajajo. Amerika je prepričana, da je Kitajska odtujila več terabajtov podatkov, skupaj z načrti za motor in radar. Kitajska je obtožbe zanikala z izjavo, da zanje ZDA nimajo nobene podlage. Ko se je o kraji

[35] »The reality is the NSA has saved thousands of lives not just in the United States but in France, Germany and throughout Europe. Quite frankly, the NSA has done so much for our country and so much for the president, he's the commander in chief. He should stand with the NSA.« (Sherwell 2013)

poročalo prvič, je podjetje Lockheed Martin zagotovilo, da jim ni znano, da bi bile v napadu ukradene tajne informacije. V letu 2015 se je debata o letalih spet odprla zaradi dokumentov Edwarda Snowdna, tokrat pa podjetje na namige o podobnosti med plovili ni želelo komentirati (Gross 2011; Boykoff 2015; Pagliery 2015a).

Julija 2014 so mediji poročali o novem kitajskem napadu na ZDA. Napad naj bi se sicer zgodil že marca istega leta, v napadu pa so kitajski hekerji vdrli v računalniško omrežje ameriške vladne agencije, ki hrani osebne podatke o vseh zveznih uslužbencih. Hekerji so pridobili dostop do nekaj zbirk podatkov agencije, preden so jih odkrili in jim blokirali nadaljnji dostop. Še vedno ni znano, kako globoko v bazo je hekerjem uspelo priti. V bazi se namreč nahajajo podatki o prosilcih za dostop do tajnih podatkov,[36] podatki o njihovih stikih v tujini, prejšnjih delovnih mestih in osebni podatki, kot je pretekla uporaba drog (Schmidt in drugi 2014; BBC 2014).

Po navedbah Oddelka za domovinsko varnost[37] ni še nihče v oddelku identificiral, ali so bili osebni podatki morda odtujeni, napad sam pa je bil s strani oddelka potrjen. Določena je bila tudi ekipa za oceno in ublažitev vsakršnih ugotovljenih tveganj. Napad naj bi izviral iz Kitajske, a se še ne ve, če so napadalci povezani s tamkajšnjo vlado. Sicer pa se je na Kitajskem v istem času nahajal John Kerry. Na Kitajsko je odšel skupaj z drugimi visokimi uradniki na letni strateški in ekonomski dialog med državama glede poslovnih odnosov ter gospodarskih in obrambnih vprašanj. Pozneje je povedal, da je za napad izvedel šele, ko se je srečanje že zaključilo (Schmidt in drugi 2014; BBC 2014).

Vdori v računalnike in računalniške sisteme imajo sicer dolgo zgodovino med državama in so že dolgo vir nesoglasij. Kitajska ima dokaze, da je Agencija za državno varnost[38] vdrla v sisteme podjetja Huawei, velikega izdelovalca opreme za računalniška omrežja na Kitajskem, in zagnala več programov, ki so prestregli pogovore med kitajskimi voditelji in vojsko. Zadnje je razkril Edward Snowden (Schmidt in drugi 2014; BBC 2014).

Uradne osebe, zadolžene za primer, pravijo, da je bil napad opazen zato, ker kljub napadom, ki se odvijajo skoraj vsak dan, napadalci redko uspejo predreti varnostne prepreke. Eden

[36] *applicants for security clearances*

[37] *Department of Homeland Security*

[38] *National Security Agency*

podobnih napadov se je zgodil leta 2013 v Oddelku za energijo,[39] kjer so napadalci uspešno odnesli osebne podatke zaposlenih in izvajalcev. Agencija je napada morala razkriti zaradi zakonov, ki to določajo, za primer, če pride do grožnje osebnim podatkom. Agencije napade lahko zamolčijo, le če gre za krajo državnih skrivnosti, ne pa tudi za krajo osebnih podatkov (Schmidt in drugi 2014).

Še ena afera se je zgodila nekaj tednov prej v maju 2014, ko so ZDA obtožile pet častnikov kitajske vojske, da so vdrli v več podjetij zasebnega sektorja v Ameriki v boju za konkurenčno prednost v sektorjih kovin, sončne in jedrske energije. Ta napad velja za prvi primer kibernetskega vohunjenja v svojih vrstah. Kljub majhni verjetnosti, da bodo častniki kdaj odslužili svojo kazen, so ZDA objavile slike vseh petih častnikov, za katere menijo, da so odgovorni (Schmidt in drugi 2014; BBC 2014; Wee 2014).

ZDA sicer priznavajo, da vohunijo za Kitajsko, a za razliko od vzhodnjakov ne vohunijo za tujimi podjetji in zbranih informacij pozneje ne posredujejo svojim podjetjem, je povedala BBC-urednica za Kitajsko Carrie Gracie. Peking navadno take napade odpravi s skomigom, saj meni, da gre za obtožbe ljudi, ki težko prenašajo hitro tehnološko rast vzhoda, je dodala (BBC 2014).

Kitajska je na obtožbe odgovorila z izjavo, da »odločno nasprotuje«[40] internetnemu hekerstvu. Tiskovni predstavnik kitajskega zunanjega ministrstva Hong Lei je dodal, da si »nekateri ameriški mediji in podjetja za kibernetsko varnost stalno prizadevajo omadeževati Kitajsko in ustvariti t. i. kitajsko kibernetsko grožnjo«.[41] Obenem je še dejal, da ZDA nikoli niso imele zadostnih dokazov in da je Kitajska prepričana, da takih poročil ni vredno spodbijati (BBC 2014).

Kljub temu so bili v letu 2015 na Kitajskem spet obtoženi še enega napada na ZDA. V začetku poletja je bilo razkrito, da naj bi kitajski hekerji vdrli v bazo s podatki federalnih javnih uslužbencev in odtujili osebne podatke 4 milijonov ljudi. Pozneje so se pojavila nova ugibanja, da se številka giblje med 9 in 14 milijoni, med zaseženimi informacijami pa naj bi bila večina v povezavi z nekdanjimi, sedaj že upokojenimi javnimi uslužbenci. Mnogi

[39] *Department of Energy*

[40] »resolutely opposed« (BBC 2014)

[41] »Some of the American media and cyber-security firms are making constant efforts to smear China and create the so-called China cyber threat.« (BBC 2014)

ameriški strokovnjaki so mnenja, da gre za načrtovanje podrobnejših napadov v prihodnje. Jason Polancich meni, da bo Kitajska s temi podatki poskusila izsiljevati ali podkupovati ljudi, da vohunijo zanjo, ali pa bo zgolj izkoristila novo znanje o delovnih projektih zaposlenih in njihovih dovolilnicah (Pagliery 2015a; The Guardian 2015).

Da gre za državno vohunstvo, naj bi nakazovalo dejstvo, kakšne vrste podatki so bili ukradeni. Ne gre za številke kreditnih kartic, s čimer lahko hekerji dobro zaslužijo na črnem trgu, niti za osebne podatke osebnega zavarovanja (*social security number*), ki bi omogočili krajo osebne identitete. Mnoga varnostna podjetja teh podatkov na črnem trgu niso zasledila, kar se sicer običajno zgodi hitro po kraji (Pagliery 2015a).

O kredibilnosti izjav, da je napad povzročila Kitajska, dvomijo tudi Američani. Razlogi naj bi bili predvsem politični; napad nekaj tednov pred strateškim in ekonomskim dialogom med državama ni smiseln, meni Elizabeth Wishnick z univerze Columbia, ki je obenem izpostavila tudi dejstvo, da ameriška vlada ni podala nobenih konkretnih dokazov. Armond Caglar, strokovnjak za hekerstvo pri TSC Advantage,[42] pa je dodal, da nihče ne more zagotovo vedeti, kakšen razlog se je skrival za napadom te vrste, čeprav je podjetje ThreatConnect, ki skrbi za kibernetsko varnost, našlo povezave med tem napadom in napadom na zavarovalniškega giganta Anthem. Za napadom na Anthem naj bi bila Kitajska, zavarovalnica pa naj bi se okužila z zlonamerno e-pošto, katere izvor je bil prirejen, da je predstavljal ameriško organizacijo OPM[43] (Pagliery 2015a).

9.3 NAPAD NA PODJETJE HACKING TEAM JULIJA 2015

Sredi leta 2015 se je zgodil hekerski napad na prej omenjeno podjetje Hacking Team, ki državam omogoča spletni nadzor nad prebivalci. Podjetje je bilo v preteklosti povezano s kar nekaj primeri dostopanja do osebnih podatkov, ki niso povsem legalni, čeprav samo delovanje podjetja ni ilegalno, vsekakor pa za mnoge moralno vprašljivo. Prav zaradi slednjega so se znašli na seznamu *Enemies of the Internet* (sovražniki spleta), kamor so jih uvrstili *Reporters Without Borders*. Napadalci so na spletu objavili 400 GB težko datoteko, v kateri so dokumenti podjetja, izvorna koda njihove programske opreme in notranje komunikacije

[42] *Tailored Solutions & Consulting, Inc.* (TSC Advantage) je podjetje, ki se ukvarja s kibernetsko varnostjo v ZDA.

[43] *Office of Personnel Management* ali Urad za upravljanje kadrov.

podjetja. Napaden je bil tudi Twitter račun podjetja, kjer so napadalci spremenili biografijo, sliko računa, obenem pa objavili dokaze o napadu (Ragan 2015a).

Odgovornost za napad je prevzel heker pod imenom PhineasFisher, ki je leto prej napadel podjetje Gamma International, enega od glavnih tekmecev Hacking Teama, ki je bil dolgo na udaru zaradi poslovanja z avtoritarnimi državami. V napadu na podjetje, ki prodaja nadzorno opremo FinFisher, je objavil 40 GB podatkov (Franceschi-Bicchierai 2015b).

V napadu je bilo obelodanjeno, da podjetje med drugim trguje z Južno Korejo, Kazahstanom, Savdsko Arabijo, Omanom, Libanonom in Mongolijo, kljub trditvam, da med kupci njihove opreme ni avtoritativnih držav in držav, ki zatirajo svoje državljane. Med državami, s katerimi naj bi podjetje sklenilo posle, je tudi Sudan, ki je po poročanju Human Rights Watch odgovoren za več kot 170 smrti v letu 2013, ko so varnostne sile nasilno zatirale proteste proti vladi. Sudan je še ena od držav, za katere je podjetje trdilo, da z njimi ne posluje. V razgaljenih dokumentih je Sudan, skupaj z Rusijo, označen z »*Not officially suported*«[44] (Ragan 2015a).

V zbirki dokumentov so tudi osebni podatki zaposlenih in strank. Gre predvsem za objavljena gesla, ki so po vseh standardih neprimerna in zelo lahka. Na voljo so tudi IP-naslovi in gesla storitev VPN,[45] ki so jih uporabljale stranke podjetja (Ragan 2015a). VPN-računi so sicer vsi že zapadli in niso več v uporabi (Ragan 2015b).

Razkritje napada se je zgodilo na nedeljo zvečer, podjetje, ki ima sedež v Italiji, pa se je s problemom soočilo šele zjutraj naslednjega dne. Prvi odzivi s strani podjetja so bili širjenje strahu z namigi, da datoteka ne vsebuje le lažnih podatkov, ampak tudi virus, in s pozivi, naj se širjenje zato preneha. Christian Pozzi, ki je taka sporočila, skupaj z grožnjami z zaporom vsem varnostnim raziskovalcem, širil na Twitterju, je sicer svoj račun deaktiviral oziroma zaprl (Ragan 2015b).

Hacking Team je po napadu takoj obvestil svoje kupce, naj prenehajo z uporabo vseh storitev, ki jih je podjetje ponujalo – vsem so poslali elektronsko pošto, v kateri so pozvali svoje

---

[44] »Uradno nepodprte«

[45] *Virtual Private Network* ali navidezno zasebno omrežje. NZO je omrežje, zgrajeno na javni omrežni infrastrukturi (internet), ki izkorišča cenovno ugodnejši medij za prenos podatkov in poslovnih komunikacij na varen način (Telemach 2015).

uporabnike, naj prenehajo z uporabo sistema Remote Control,[46] znanega tudi pod imenom Galileo. Po prvih poročanjih, ki jih je objavila spletna stran Motherboard, podjetje še ni moglo dostopati do nabiralnikov elektronske pošte (Ragan 2015b; Franceschi-Bicchierai 2015a).

Nekaj dni po napadu je spletni medij Gizmodo povprašal Hacking Team o prodaji spletnega orožja državam na črnih listah organizacij, kot so Združeni narodi (v tem primeru je največ komentarjev na sodelovanje podjetja s Sudanom). Ameriški predstavnik podjetja Eric Rabe je dejal, da gre za dokaj relativno zadevo, saj ljudje ne vidijo vseh držav enako (na primer, na čigavi strani so, saj so ljudje v preteklosti negativno označili mnoge zaveznike Zahoda), in glede na to, da se vlade spreminjajo in v različnih obdobjih prejemajo različno kritiko, gre za zelo zahtevno zadevo. Na koncu je dodal, da tudi take države, ki imajo visoko stopnjo aktivizma, morda potrebujejo tako opremo, kot jo ponuja Hacking Team, saj so lahko idealen prostor za razvoj terorizma. To vseeno ne opraviči sodelovanja z nekaterimi državami, kot je na primer Etiopija, ki je programsko opremo uporabljala za vohunjenje za novinarji, ki jih je vlada označila za teroriste. Tako razmišljanje je podobno razmišljanju direktorja podjetja Davida Vincenzettija, ki je v enem od objavljenih elektronskih sporočil kolegu vprašal, ali dejansko obstaja demokratična država, ki ne krši nobenih pravic in ima popolnoma čisto zgodovino človekovih pravic. Sporočilo se je nanašalo na mnogo negativnih kritik podjetja in slabo podobo v medijih (Knibbs 2015).

Gre za velik problem za podjetje, a glede na vse izpostavljene podatke so na udaru tudi države, ki so ali še vedno sodelujejo s podjetjem. Napad se je sicer zgodil na akterja na mednarodnem trgu, a s tem je bilo izpostavljenih in ogroženih kar nekaj držav in njihovih sistemov, kar seveda ogroža varnost teh držav in izpostavlja njihove interese.

9.4 IZKORIŠČANJE NAPADA NA SPLETNO STRAN ASHLEY MADISON 2015

Poleti 2015 je skupina hekerjev, samooklicana The Impact Team, napadla spletno stran Ashley Madison, ki je svojim uporabnikom ponujala lahko pot do nezvestobe, podatke pa objavila na spletu. Napad, ki je izpostavil uporabnike, finančne zapise, podatke o zaposlenih in druge občutljive informacije, se je po besedah napadalcev zgodil zaradi lastnikov strani, ki so z lažnimi obljubami dokončnega izbrisa podatkov uporabnikov za samo 19 ameriških dolarjev zavajali uporabnike in kršili njihovo zasebnost ter odlično zaslužili – v letu 2014 naj bi samo z možnostjo izbrisa zaslužili več kot milijon in pol dolarjev, obenem pa obdržali

[46] Oddaljeni sistem za nadzor

finančne podatke, imena in naslove uporabnikov. V napadu je bilo zajetih in potencialno ogroženih več kot 30 milijonov ljudi. Da se je objava zajetih podatkov sploh zgodila, naj bi bilo krivo podjetje Avid Life Media, ki si lasti Ashley Madison, saj ni sprejelo zahtev hekerske skupine, da dokončno odstrani spletni strani Ashley Madison in Established Men (še ena od strani v lasti podjetja, ki ponuja posebne osebne storitve) (Krebs 2015a).

Dejanje je problematično že samo po sebi, saj objava takšnih informacij škoduje vsem uporabnikom strani, ne le podjetju. A težava sega mnogo globlje, in sicer do uporabnikov samih in njihovih povezav. Veliko se jih je namreč prijavilo na spletno stran z uporabo službenih elektronskih naslovov, med takimi je precej oseb, ki so zaposlene v vladnih službah in organih po vsem svetu – po poročanjih je takih računov med 10 in 15 tisoč, a je treba omeniti, da gre lahko za lažne prijave tretjih oseb s tujimi poštnimi naslovi, kjer računi niso bili nikoli uporabljeni (Stern 2015; Bennett 2015b; Krebs 2015b). Uporaba vladnih elektronskih naslovov, ki so postali dostopni vsem z nekaj znanja za pregled izdanih informacij, omogoča hitro in lahko identifikacijo uporabnikov. Hiter pregled na CCN-u je odkril ne samo vladne delavce, ampak tudi skupno čez 12 tisoč vojakov iz vseh vej ameriške vojske. Mnogi uporabniki so se sicer registrirali z lažnim imenom, a so plačali z osebnimi kreditnimi karticami, kar poleg njihovih finančnih podatkov izda še pravo ime in naslov (Pagliery 2015b). S tem je bilo izpostavljenih mnogo obveščevalnih in vojaških podatkov mnogih držav, kar je velika varnostna grožnja (Waddell 2015).

Tehnika pridobivanja takih podatkov je pravzaprav zelo lahka – s potrditvijo identitete, za kar se od uporabnika zahteva mnoge osebne podatke, je omogočen dostop do omejenih delov spletne strani, ki ponujajo boljše ugodnosti. Kombinacija podatkov iz podobnih napadov, ki jih pogosto lahko kupimo na črnem trgu na spletu, hekerjem omogoča sestavo natančne identitete določene osebe, kar lahko izrabljajo za dostop do drugih spletnih strani ali celo računalnika (Waddell 2015).

Da je stanje resno, dokazujejo tudi poročanja o ruskih in kitajskih obveščevalnih službah, ki objavljene podatke prečesavajo za iskanje informacij o ameriških obveščevalnih uslužbencih, ki omogočajo osebno prepoznavanje. Tuje obveščevalne službe tako kombinirajo in preverjajo podatke iz več hekerskih napadov, da bi identificirale in potencialno ogrozile operativce. Obe državi sta sicer skušali prikriti svoje sledi, predvsem z uporabo nevladnih entitet, kot so hekerske skupine in zasebna podjetja. Sicer obe državi uporabljata tudi vladna

sredstva za izvajanje kibernetskih napadov. Napadi so sicer stalnica že približno desetletje, da pa se grožnja razvija, je razvidno prav iz primerov, kot je Ashley Madison (Sciutto 2015).

9.5 PRIMERJAVA IN UGOTOVITVE

HACKINT kot tehnika pridobivanja informacij na državni ravni v namene njene zaščite in varovanja ni novost. Čeprav se je močneje razširila šele v zadnjih letih, je uporaba tehnologije in spleta že dolga leta nepogrešljiva taktika. Danes je dobra tehnologija poceni in lahko dostopna, do uporabe pripomočkov za vohunjenje pa lahko dostopa že vsak navaden uporabnik.[47] Zato niti ni presenetljivo, da države v vse večji meri posegajo po takšnih in drugačnih prikritih tehnikah pridobivanja informacij. Nadzor nad takšnimi dejanji je dokaj ničen, saj je ne glede na sprejete sporazume, ki temeljijo predvsem na etičnosti, HACKINT v interesu velike večine akterjev.

Kot je očitno iz primera podjetja Hacking Team, je držav, ki uporabljajo kibernetične načine zbiranja podatkov z uporabo hekerske opreme več kot dovolj za uspešen posel. Podjetje je bilo ustanovljeno povsem legitimno, njihove storitve pa je uporabljalo mnogo držav in državnih agencij. Čeprav so si kritike prislužili z več primeri vprašljivega zbiranja informacij za svoje stranke, je napad na podjetje, ki je razkril še mnoge vprašljive kupce, samo še dodatno podžgal nasprotnike tako podjetja kot storitev, ki jih ta ponuja.

Kot sem ugotovila že v SWOT-analizi HACKINT-a, je negativnih posledic več kot pozitivnih, kar dokazuje tudi primer prisluškovanja v ZDA. Prišlo je do zlorabe položaja, kjer so imele ZDA prednost v tehnologiji, kar so izrabile sebi v prid za izpolnjevanje lastnih interesov. Opravičila, da s tem pomagajo preprečiti nevarnosti, ki grozijo Evropi, se mnogim zdijo prazne in zavajajoče trditve. Ne glede na to, koliko držav izvaja take akcije (in po izjavah Francije je mogoče sklepati, da je to dokaj razširjen pojav), je razlog za negativne reakcije na razkritja predvsem na strani etičnosti, moralnosti in (ne)spoštovanja mednarodnih sporazumov, seveda zgolj v uradnem smislu. Pomembno je namreč ločiti, kaj države počnejo javno – sem spadajo izjave, sporazumi, sodelovanja ipd. – in kaj počnejo zasebno oziroma

[47] Ena izmed pogostejših uporab je '*nanny cam*', kamera, običajno skrita v igračah, knjigah ipd., ki nadzoruje delo varuške. Uporaba takšnih pripomočkov se je danes že močno razširila, nadzoruje pa veliko več kot le varstvo otrok. Danes se kamere skrivajo lahko že kjer koli, na primer v stenskih urah ali osveževalcih zraka, v svinčnikih in kravatah. Poleg kamer so med drugim na voljo tudi naprave, ki blokirajo signale, naprave, ki spremljajo našo uporabo računalnikov, GPS-sledilniki in podobno (Ionescu 2010).

tajno. Prav zato lahko države podpišejo mnoge sporazume, sodelovalne in prijateljske pogodbe, in si zagotavljajo odprto pomoč, a vsaka od njih bo še vedno izvajala prikrite akcije za pridobitev prednosti pred drugimi. Enako velja za podjetje Hacking Team, ki je imelo uraden seznam kupcev, in interni seznam, na katerem so se pojavile države, katerih status strank podjetje ni želelo priznati.

V primeru Ashley Madison pa lahko potrdim dva problema, ki sta bila že omenjena v tej nalogi, in sicer 1) slaba skrb podjetij za varnost in zasebnost tako podjetja kot uporabnikov storitev predstavlja velik problem, ki samo spodbuja kibernetski kriminal, in 2) človek je najšibkejši člen digitalnega sveta, in če sami ne poskrbimo za lastno varnost, je zelo verjetno, da bomo slej ali prej žrtev napada. Predvsem zadnje je pomemben dejavnik napada na Ashley Madison, saj poleg vseh osebnih težav, ki jih je za člane strani povzročila že registracija sama (poroča se celo o samomorih zaradi razkritja podatkov), napad predstavlja veliko varnostno grožnjo zaradi vojaških in vladnih podatkov, ki so bili z njim razkriti. Problem ene osebe tako hitro postane problem organizacije in države.

Čeprav mnogi menijo, da take vrste nadzor ni etičen in lahko vodi v le še večje težave, je očitno, da je HACKINT pomemben del politike vsake države, zato lahko pričakujemo, da se bo v prihodnosti njegova uporaba le še razširila.

10 UGOTOVITVE IN SKLEP

Glede na pomembnost podatkov v moderni dobi je brez težav sklepati, da gre za eno od bolj iskanih dobrin na svetu, ne glede na to, kdo smo in kaj počnemo z njo. In ker danes podatki in informacije prepletajo naš vsakdanjik do te mere, da so od njega neločljivi, so tudi del varnostnega vprašanja vsakega posameznika, podjetja in države.

Danes v mednarodnih odnosih akterji ves čas iščejo ravnotežje, s katerim se uravnavajo mir in pozitivni odnosi v družbi. A ker ima vsaka država svoje interese, ki so velikokrat v nasprotju z interesi drugih, se s poskusi uresničevanja ves čas medsebojno ogrožajo. Vsaka bi namreč rada pridobila prednost pred drugimi, za tako tekmovanje pa so podatki in informacije ključne. Prav zato se mnogokrat zgodi, da za pridobivanje informacij, ki bi jim pomagale pridobiti prednost pred drugimi, niso pridobljene povsem etično ali legalno. Prav tak primer so prisluškovalne afere ZDA, ki so nedavno prišle v javnost, in kitajski napadi na ZDA.

Pričakovati je, da ima vsak akter, pa naj bo to posameznik, podjetje ali država, nekaj skrivnosti. Lahko gre za osebne, ki so sicer majhne v primerjavi z drugimi, a za vsakega posameznika kljub temu zelo pomembne. Veliko večji pomen imajo gospodarske skrivnosti, ki omogočajo podjetjem, da v svetu visoke konkurence dobro poslujejo, od česar imajo koristi tudi posamezniki in države. Verjetno najpomembnejše v širšem smislu so državne skrivnosti, ki niso skrite zgolj pred očmi drugih držav, ampak so mnogokrat nedostopne tudi prebivalcem te države. To je seveda razumljivo, a kljub temu obstajajo tako pravne kot fizične osebe, ki bi te skrivnosti rade poznale iz takih in drugačnih razlogov.

Prav zato je pomembno, da zna vsaka država primerno poskrbeti, da skrivnosti ostanejo skrite nepovabljenim očem. V svetu digitalizacije je to vse večji izziv, ne le zaradi velike količine podatkov, ki se globalno pretakajo vsak dan, pač pa tudi zaradi lahkega dostopanja, ki ga omogoča digitalizacija. Kljub vsem pozitivnim posledicam, ki sta jih globalizacija in digitalizacija povzročili, ne moremo zanemariti dejstva, da se je vzporedno povečala tudi priložnost za kriminal. Tako danes mnogi dobro služijo – mnogi pa veliko izgubijo – na račun kibernetskega kriminala, pa naj gre za finančne goljufije, krajo identitete ali trgovanje s skrivnostmi.

V večini primerov so vpleteni hekerji. Kot je naloga že raziskala, je izraz za današnje dogajanje uporabljen neprimerno, a se je v zavesti vseh zasidral tako močno, da je za potrebe prikaza problematike uporabljen tudi v tem magistrskem delu. Dejstvo namreč je, da je hekerstvo problem moderne družbe. Je oblika kriminala, ki napada vse, ne glede na to, kdo smo, kaj smo in kaj počnemo – grožnjo predstavlja vsem, a na različnih ravneh. Prav zato lahko pritrdilno odgovorim na raziskovalno vprašanje, ki me je vodilo pri pisanju te magistrske naloge: *Ali je hekerstvo grožnja (oziroma izziv) obveščevalni dejavnosti?*

Glede na izbrane primere analize v nalogi pa zavračam obe hipotezi.

Prvo, ki se glasi: *Notranje grožnje hekerjev so za obveščevalno dejavnost nevarnejše kot zunanje* zavračam zato, ker je iz analiziranih primerov razvidno, da v veliki večini primerov, ki imajo visoko stopnjo škode, napad prihaja od zunaj. V primeru nemške afere je bil napad s strani ZDA; v primeru napada na ZDA lahko sklepamo, da je bil napad s strani Kitajske (kljub njihovemu zanikanju); v primerih Hacking Teama in Ashley Madison je napadalec sicer neznan, a lahko rečemo, da gre za mednarodni napad zaradi podatkov, ki so prišli v javnost, in strank, ki so bile s tem napadene.

Drugo hipotezo, ki se glasi: *HACKINT je bila uspešna rešitev za zmanjšanje nevarnosti hekerstva, ki jo ta povzroča obveščevalni dejavnosti*, prav tako zavračam, saj je iz primerov razvidno, da to obliko zbiranja informacij države primarno uporabljajo z namenom napada namesto obrambe, v primeru Hacking Team podjetja pa nedemokratične države za zatiranje civilistov v državah s totalitarnim režimom. Dejansko se z uporabo HACKINTA kot sredstva napada za pridobivanje prednosti problem hekerstva ne le povečuje, pač pa tudi poslabšuje. V primerih napadov na podjetja, predvsem v okviru napada na Ashley Madison, je ogroženost države celo posredna, na kar obveščevalne dejavnosti niso mogle vplivati in bodo s težavo zajezile storjeno škodo. Če bodo ljudje še vedno tako lahkotno obravnavali zasebno varnost, se države hekerstva ne bodo zlahka obranile.

V globalizaciji, ko je svet tesno povezan, grožnje pa vse bolj transnacionalne, je pomembno, da obstajajo mehanizmi, ki bodo uspešno reševali globalne probleme. Kibernetski svet omogoča, da se grožnje posameznikom, organizacijam in državam širijo z neverjetno hitrostjo v okolju, ki nima fizičnega prostora, ima pa fizične posledice. HACKINT, ne glede na svoje slabosti, začenja gibanje, ki je še v povojih in zahteva nenehno koordinacijo in prilagajanje realnim razmeram.

Problemi se pojavijo znotraj posameznih držav, med katerimi zakonodaja zelo variira. Medtem ko nekateri narodi kibernetske grožnje postavljajo na sam vrh pomembnosti pri varovanju države in prebivalcev, je v drugih državah razvoj kibernetske zakonodaje ne le pomanjkljiv, pogosto tudi ne obstaja. To predstavlja težavo pri kooperaciji, ki jo zahteva transnacionalnost problema kibernetskih groženj. Dokler vsaka država posamezno tega področja ne bo uredila, da se lahko začne gradnja na mednarodni ravni, in dokler bodo države izkoriščale svoje tehnološke prednosti za dominanco v mednarodnem prostoru, bo bojevanje s kibernetskim kriminalom težko.

11 LITERATURA

1. Aldrich, Richard J. 2004. Transatlantic Intelligence and Security Cooperation. V *International Affairs (Royal Institute of International Affairs 1944-)* 80 (4): 731–753. Dostopno prek: http://www.jstor.org/stable/3569532 (10. december 2013).
2. *Aljazeera America*. 2015. Chinese arrest 15,000 in cybercrime sweep. Dostopno prek: http://america.aljazeera.com/articles/2015/8/18/chinese-arrest-15000-in-cybercrime-sweep.html (9. september 2015).
3. Amon, Bojan. 2005. *Rekonstrukcija podobe hekerstva*. Diplomsko delo. Dostopno prek: http://dk.fdv.uni-lj.si/dela/Amon-Bojan.PDF (17. junij 2014).
4. Anastasiou Papanastasiou, Afroditi. 2014. Cyber War Law. Dostopno prek: http://cyberwarlaw.eu/ (19. junij 2014).
5. Appelbaum, Jacob, Holger Stark, Marcel Rosenbach in Jörg Schindler. 2013. Berlin Complains: Did US Tap Chancellor Merkel's Mobile Phone? *Spiegel Online International*, 23. oktober. Dostopno prek: http://www.spiegel.de/international/world/merkel-calls-obama-over-suspicions-us-tapped-her-mobile-phone-a-929642.html (22. julij 2014).
6. Asay, Matt. 2013. Gartner: AWS Now Five Times The Size Of Other Cloud Vendors Combined. *Readwrite*, 21. avgust. Dostopno prek: http://readwrite.com/2013/08/21/gartner-aws-now-5-times-the-size-of-other-cloud-vendors-combined (8. september 2015).
7. Bara, George. 2015. Whistleblowers vs. hackers. The final showdown. *LinkedIn*, 10. februar. Dostopno prek: https://www.linkedin.com/pulse/whistleblowers-vs-hackers-final-showdown-george-bara (11. september 2015).
8. Barak, Sylvie. 2012. National security threat: hacking the smart grid. *EE Times*, 5. april. Dostopno prek: http://www.eetimes.com/document.asp?doc_id=1261499 (21. februar 2014).
9. *BBC*. 2009. Websites 'keeping deleted photos', 21. maj. Dostopno prek: http://news.bbc.co.uk/2/hi/8060407.stm (10. september 2015).
10. --- 2014. Chinese hackers 'broke into US personnel network', 10. julij. Dostopno prek: http://www.bbc.com/news/world-us-canada-28251610 (15. februar 2015).
11. Bennett, Cory. 2014. Privacy advocates seek DC's help to restrain FBI. *The Hill*, 5. november. Dostopno prek: http://thehill.com/policy/cybersecurity/223084-privacy-advocates-call-for-dcs-help-to-restrain-fbi (11. september 2015).

12. --- 2015a. Google warns against expanding FBI hacking power. *The Hill*, 17. februar. Dostopno prek: http://thehill.com/policy/cybersecurity/233028-google-warns-against-expanding-fbi-hacking-power (11. september 2015).
13. --- 2015b. 15,000 government emails revealed in Ashley Madison leak. *The Hill*, 19. avgust. Dostopno prek: http://thehill.com/policy/cybersecurity/251431-ashley-madison-leak-appears-real-includes-thousands-of-government-emails (8. oktober 2015).
14. Berkowitz, Bruce D. 1996. Information Age Intelligence. V *Foreign Policy* 103: 35–50. Dostopno prek: http://www.jstor.org/stable/1149201 (5. februar 2014).
15. Betts, Richard K. 2002. Fixing Intelligence. V *Foreign Affairs*, 81 (1): 43–59. Dostopno prek: http://www.jstor.org/stable/20033002?origin=JSTOR-pdf (10. december 2013).
16. Biddle, Sam. 2014. Everything You Need to Know About Sony's Unprecedented Hacking Disaster. *Gawker*, 15. december. Dostopno prek: http://sonyhack.gawker.com/everything-you-need-to-know-about-sonys-unprecedented-h-1671217518 (9. september 2015).
17. Bock, Andreas M. in Ingo Henneberg. 2013. *Why Balancing Fails – Theoretical reflections on Stephan M. Walt's »Balance of Threat« Theory.* Dostopno prek: http://www.jaeger.uni-koeln.de/fileadmin/templates/publikationen/aipa/AIPA_2_2013.pdf (4. september 2014).
18. Booth, Ken. 2007. *Theory of World Security*. Cambridge: Cambridge University Press.
19. Borger, Julian. 2013. GCHQ and European spy agencies worked together on mass surveillance. *The Guardian*, 1. november. Dostopno prek: http://www.theguardian.com/uk-news/2013/nov/01/gchq-europe-spy-agencies-mass-surveillance-snowden (8. oktober 2015).
20. Boykoff, Pamela. 2015. China denies suggestions it stole designs for new U.S. fighter. *CNN*, 20. januar. Dostopno prek: http://edition.cnn.com/2015/01/19/world/china-us-f35-fighter-denial/?iid=EL (19. junij 2015).
21. Breidthardt, Annika in Sabine Siebold. 2014. U.S. top spy to leave Berlin by end of week: newspaper. *Reuters,* 15. julij. Dostopno prek: http://www.reuters.com/article/2014/07/15/us-germany-usa-spying-leave-idUSKBN0FK1WL20140715 (22. julij 2014).
22. Brezovšek, Marjan in Damir Črnčec. 2010. *Demokratična uprava in tajnost podatkov*. Ljubljana: Fakulteta za družbene vede.

23. Buzan, Barry in Lene Hansen. 2014. *The evolution of international security studies*. Cambridge: Cambridge University Press.
24. Buzan, Barry. 2015. The English School: A neglected approach to International Security Studies. V *Security Dialogue*, 46 (2): 126–143. Dostopno prek: http://sdi.sagepub.com.nukweb.nuk.uni-lj.si/content/46/2/126.full.pdf+html (11. september 2015).
25. Clark, Don. 2015. Moore's Law Is Showing Its Age. *Wall Street Journal*, 16. julij. Dostopno prek: http://www.wsj.com/articles/moores-law-is-showing-its-age-1437076232 (7. oktober 2015).
26. Clarke, Richard A. in Robert K. Knake. 2010. *Cyber war: the next threat to national security and what to do about it.* New York: Ecco.
27. Coleman, E. Gabirella. 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 (1. september 2014).
28. Cook, James. 2015. Google is worried that the US government is going to start hacking into computers all over the world. *Business Insider*, 19. februar. Dostopno prek: http://www.businessinsider.com/google-comments-new-us-government-hacking-law-2015-2 (22. februar 2015).
29. *Cornell University Law School*. 2012a. 18 U.S. Code § 1029 - Fraud and related activity in connection with access devices. Dostopno prek: https://www.law.cornell.edu/uscode/text/18/1029 (11. september 2015).
30. --- 2012b. 18 U.S. Code § 1030 - Fraud and related activity in connection with computers. Dostopno prek: https://www.law.cornell.edu/uscode/text/18/1030 (11. september 2015).
31. *Council of Europe.* 2001. Convention on Cybercrime. Dostopno prek: http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm (11. september 2015).
32. Crovitz, Gordon L. 2013. White Hats vs. Black Hats. *The Wall Street Journal*, 4. avgust. Dostopno prek: http://online.wsj.com/news/articles/SB10001424127887324635904578643943968885044 (6. februar 2014).
33. *Cult of the Dead Cow*. 2001. The Hacktivismo Declaration. Dostopno prek: http://www.cultdeadcow.com/cDc_files/declaration.html (25. avgust 2015).
34. Custer, C. 2014. Hacking China's online games for profit: an interview with a Chinese hacker. *Tech in Asia*, 2. maj. Dostopno prek: https://www.techinasia.com/hacking-chinas-online-games-for-profit-an-interview-with-a-chinese-hacker/ (30. maj 2015).

35. Cuthbertson, Anthony. 2015. Anonymous exposes US and UK companies hosting pro-Isis websites. *International Business Times*, 8. april. Dostopno prek: http://www.ibtimes.co.uk/anonymous-exposes-us-uk-companies-hosting-pro-isis-websites-1495426 (9. september 2015).
36. Daileda, Colin in Lorenzo Franceschi-Bicchierai. 2014. U.S. Intelligence Officials Want ISIL Fighters to Keep Tweeting. *Mashable*, 11. julij. Dostopno prek: http://mashable.com/2014/07/11/us-wants-iraq-radicals-to-tweet/ (9. september 2015).
37. Doren, Daisy. 2012. SWOT analiza in ozka grla. *E-podjetnik*, 31. januar. Dostopno prek: http://www.e-podjetnik.org/podjetnistvo/10-organizacija/28-swot (5. julij 2015).
38. Dreyfuss, Benjamin in Emily Dreyfuss. 2013. What is the NSA's PRISM program? (FAQ). *CNET*, 7. junij. Dostopno prek: http://www.cnet.com/news/what-is-the-nsas-prism-program-faq/ (25. avgust 2015).
39. Dunne, Tim. 2007. Liberalizem. V *Globalizacija svetovne politike. Uvod v mednarodne odnose*, ur. John Baylis in Steve Smith, 327–261. Ljubljana: Fakulteta za družbene vede.
40. *Enterprise Risk Management.* 2010. Commercial Hacking: The Mafia Returns. Dostopno prek: http://www.emrisk.com/sites/default/files/newsletters/ERMNewsletter_June_20101.pdf (14. junij 2015).
41. Eriksson, Johan in Giampiero Giacomello. 2006. The Information Revolution, Security, and International Relations: (IR) Relevant Theory? V *International Political Science Review / Revue internationale de science politique*, 27 (3): 221–244. Dostopno prek: http://www.jstor.org/stable/20445053 (10. december 2013).
42. *European Parliamentary Research Service*. 2014. NSA surveillance of EU citizens. Dostopno prek: http://epthinktank.eu/2014/03/12/nsa-surveillance-of-eu-citizens/ (8. oktober 2015).
43. Evans, Graham in Jefferey Newnham. 1998. *The Penguin Dictionary of International Relations*. London: Penguin Books.
44. *FindLaw UK*. 2015. What do I need to know about computer hacking? Dostopno prek: http://findlaw.co.uk/law/criminal/crimes_a_z/500428.html (11. september 2015).
45. *First Community Bank*. 2015. What can identity thieves do with stolen personal information? Dostopno prek: https://www.fcbresource.com/SecurityCenter/What-can-identity-thieves-do-with-stolen-personal-.aspx (9. september 2015).
46. *Forbes*. 2015. The World's Most Valuable Brands. Dostopno prek: http://www.forbes.com/powerful-brands/list/ (7. oktober 2015).

47. Fox, Michelle. 2012. 10 Ways Companies Get Hacked. *CNBC*, 6. julij. Dostopno prek: http://www.cnbc.com/id/48087514 (9. junij 2015).
48. Franceschi-Bicchierai, Lorenzo. 2015a. Hacking Team Asks Customers to Stop Using Its Software After Hack. *Motherboard*, 6. julij 2015. Dostopno prek: http://motherboard.vice.com/read/hacking-team-asks-customers-to-stop-using-its-software-after-hack (9. julij 2015).
49. --- 2015b. Hacker Claims Responsibility for the Hit on Hacking Team. *Motherboard*, 6. julij 2015. Dostopno prek: http://motherboard.vice.com/read/hacker-claims-responsibility-for-the-hit-on-hacking-team (9. julij 2015).
50. *Frontline*. 2014. Interview: James Christy. Dostopno prek: http://www.pbs.org/wgbh/pages/frontline/shows/hackers/interviews/christy.html (21. februar 2014).
51. Galston, William A. 2010. Realism in political theory. V *European Journal of Political Theory*, 9 (4): 385–411. Dostopno prek: http://ept.sagepub.com.nukweb.nuk.uni-lj.si/content/9/4/385.full.pdf+html (27. avgust 2015).
52. Gayomali, Chris. 2014. Why Do Companies Keep Getting Hacked? *Fast Company*, 24. februar. Dostopno prek: http://www.fastcompany.com/3026672/the-code-war/why-do-companies-keep-getting-hacked (31. maj 2015).
53. Goetschel, Laurent. 2000. Globalisation and Security: The Challenge of Collective Action in a Politically Fragmented World. V *Global Society*, 14 (2): 259–277. Dostopno prek: http://www-tandfonline-com.nukweb.nuk.uni-lj.si/doi/abs/10.1080/13600820050008476 (11. oktober 2015).
54. Graham, Paul. 2004. *Great hackers*. Dostopno prek: http://www.paulgraham.com/gh.html (28. maj 2014).
55. Grizold, Anton. 1998. Institucionalizacija zagotavljanja mednarodne varnosti. V *Perspektive sodobne varnosti*, ur. Anton Grizold, 1–15. Ljubljana: Fakulteta za družbene vede.
56. --- 2001. Varnostna paradigma v mednarodnih odnosih. V *Človek, država in vojna*, ur. Evan Luard, 83–161. Ljubljana: Fakulteta za družbene vede.
57. Gross, Michael Joseph. 2011. Enter the Cyber-dragon. *Vanity Fair*, september. Dostopno prek: http://www.vanityfair.com/news/2011/09/chinese-hacking-201109 (7. september 2015).
58. Gu, Lion. 2013. *Beyond Online Gaming Cybercrime: Revisiting the Chinese Underground Market*. Dostopno prek: http://www.trendmicro.com/cloud-

content/us/pdfs/security-intelligence/white-papers/wp-beyond-online-gaming-cybercrime.pdf (9. september 2015).

59. *Hacktivismo.* 2001. The Hacktivismo declaration. Dostopno prek: http://www.hacktivismo.com/public/declarations/en.php (11. september 2015).
60. ---. Dostopno prek: http://www.hacktivismo.com/about/index.php (12. junij 2014).
61. Hansen, Lene in Helen Nissenbaum. 2009. Digital Disaster, Cyber Security, and the Copenhagen School. V *International Studies Quarterly*, 53 (4): 1155–1175. Dostopno prek: http://www.jstor.org/stable/27735139 (8. september 2015).
62. Herman, Michael. 2001. *Intelligence Services in the Information Age: Theory and Practice.* London: Frank Cass Publishers.
63. Hill, Kashmir. 2014. When It's A Good Idea To Invite An Army Of Hackers To Attack You. *Forbes*, 10. september. Dostopno prek: http://www.forbes.com/sites/kashmirhill/2014/09/10/bug-bounty-programs/ (5. september 2015).
64. Hindman, Matthew. 2009. *The Myth of Digital Democracy*. Princeton: Princeton University Press.
65. Hočevar, Barbara. 2011. Kaj je obveščevalno-varnostna dejavnost? *Delo*, 3. februar. Dostopno prek: http://www.delo.si/clanek/138997 (21. februar 2014).
66. Hoffman, Chris. 2013. Hacker Hat Colors Explained: Black Hats, White Hats, and Gray Hats. *How to Geek*, 20. april. Dostopno prek: http://www.howtogeek.com/157460/hacker-hat-colors-explained-black-hats-white-hats-and-gray-hats/ (6. februar 2014).
67. Holt, Thomas J. 2012. Examining the Forces Shaping Cybercrime Markets Online. V *Social Science Computer Review*, 31 (2): 165–177. Dostopno prek: http://ssc.sagepub.com/content/31/2/165.full.pdf+html (27. avgust 2015).
68. Hook, Steven W. 2008. *U.S. Foreign Policy: The Paradox of World Power*. Washington, D. C.: CQ Press.
69. Hribar, Gašper. 2012. *Protiobveščevalna dejavnost v Republiki Sloveniji*. Diplomsko delo. Dostopno prek: http://dkum.ukm.si/IzpisGradiva.php?id=20455 (5. september 2015).
70. Hughes, Rex. 2009. NATO IN CYBERSPACE: Digital Defences. V *The World Today*, 65 (4): 19–21. Dostopno prek: http://www.jstor.org/stable/41548884 (7. september 2015).
71. *Information Technology Act, 2000.* Dostopno prek: http://www.dot.gov.in/sites/default/files/itbill2000_0.pdf (25. avgust 2015).

72. Ionescu, Daniel. 12 Top Spy Gadgets. *PC World*, 22. julij. Dostopno prek: http://www.pcworld.com/article/201703/Spy_Gear_for_Your_Inner_Evelyn_Salt_and_James_Bond.html (26. avgust 2015).
73. *IT (Amendment) Act, 2008*. Dostopno prek: http://deity.gov.in/sites/upload_files/dit/files/downloads/itact2000/it_amendment_act2008.pdf (8. september 2015).
74. Jackson, Robert in Georg Sørensen. 1999. *Introduction to international relations*. Oxford: Oxford University Press.
75. Jeffries, Adrianne. 2013. Meet Hacking Team, the company that helps the police hack you. *The Verge*, 13. september. Dostopno prek: http://www.theverge.com/2013/9/13/4723610/meet-hacking-team-the-company-that-helps-police-hack-into-computers (12. april 2015).
76. *Kazenski zakonik* (KZ-1-UPB2). Ur. l. RS 50/2012. Dostopno prek: http://www.uradni-list.si/1/content?id=109161 (10. julij 2014).
77. Keel, Robert O. 2010. *The McDonaldization of Society*. Dostopno prek: http://www.umsl.edu/~keelr/010/mcdonsoc.html (15. februar 2014).
78. Kelsey, Jeffrey T. G. 2008. Hacking into International Humanitarian Law: The Principles of Distinction and Neutrality in the Age of Cyber Warfare. V *Michigan Law Review*, 106 (7): 1427–1451. Dostopno prek: http://www.jstor.org/stable/40041623?origin=JSTOR-pdf (10. december 2013).
79. Knibbs, Kate. 2015. Hacking Team's Lame Excuse for Selling Digital Weapons to Sudan. *Gizmodo*, 8. julij 2015. Dostopno prek: http://gizmodo.com/hacking-teams-lame-excuse-for-selling-digital-weapons-t-1716375503 (9. julij 2015).
80. Kohlmann, Evan F. 2006. The Real Online Terrorist Threat. V *Foreign Affairs*, 85 (5): 115–124. Dostopno prek: http://www.jstor.org/stable/20032074 (9. september 2015).
81. Kramer, Franklin D. 2009. Cyberpower and National Security: Policy Recommendations for a Strategic Framework. V *Cyberpower and National Security*, ur. Franklin D. Kramer, Stuart H. Starr in Larry K. Wentz, 3–23. Washington, D. C.: National Defense University Press in Potomac Books.
82. Kramer, Franklin D., Stuart H. Starr in Larry K. Wentz, ur. 2009. *Cyberpower and National Security*. Washington, D. C.: National Defense University Press in Potomac Books.

83. Krebs, Brian. 2014. A First Look at the Target Intrusion, Malware. *Krebs on Security*, 15. januar. Dostopno prek: http://krebsonsecurity.com/2014/01/a-first-look-at-the-target-intrusion-malware/ (9. junij 2015).
84. --- 2015a. Online Cheating Site AshleyMadison Hacked. *Krebs on Security*, 19. julij. Dostopno prek: http://krebsonsecurity.com/2015/07/online-cheating-site-ashleymadison-hacked/ (10. september 2015).
85. --- 2015b. Was the Ashley Madison Database Leaked? *Krebs on Security*, 18. avgust. Dostopno prek: http://krebsonsecurity.com/2015/08/was-the-ashley-madison-database-leaked/ (8. oktober 2015).
86. Krupnick, Matt. 2011. Freedom fighters or vandals? No consensus on Anonymous. *San Jose Mercury News*, 16. avgust. Dostopno prek: http://www.mercurynews.com /top-stories/ci_18686764 (1. september 2014).
87. *Legislation.gov.uk.* 2007. Computer Misuse Act 1990. Dostopno prek: http://www.legislation.gov.uk/ukpga/1990/18/contents (11. september 2015).
88. Lever, Paul. 2012. Inteligence and War. V *The Oxford Handbook of War*, ur. Julian Lindley-French in Yves Boyer, 228–241. New York: Oxford University Press.
89. Liang, Bin in Hong Lu. 2010. Internet Development, Censorship, and Cyber Crimes in China. V *Journal of Contemporary Criminal Justice*, 26 (1): 103–120. Dostopno prek: http://ccj.sagepub.com.nukweb.nuk.uni-lj.si/content/26/1/103.full.pdf+html (7. september 2015).
90. Lowenthal, Mark M. 2009. *Intelligence: From Secrets to Policy*. Washington, D. C.: CQ Press.
91. Ludlow, Peter. 2013. Hacktivists as Gadflies. *The New York Times*, 13. april. Dostopno prek: http://opinionator.blogs.nytimes.com/2013/04/13/hacktivists-as-gadflies/?_php=true&_type=blogs&_php=true&_type=blogs&_r=1 (12. junij 2014).
92. Maffettone, Sebastiano. 2000. Liberalism and its critique: Is the therapy worse than the disease? V *Philosophy and Social Criticism*, 26 (3): 1–37. Dosopno prek: http://psc.sagepub.com.nukweb.nuk.uni-lj.si/content/26/3/1.full.pdf+html (27. avgust 2015).
93. McCann, Joe. 2013. Data Is The Most Valuable Commodity On Earth. *Subprint*, 3. september. Dostopno prek: http://subprint.com/blog/data-is-the-most-valuable-commodity-on-earth (18. februar 2014).
94. McFedries, Paul. 2001. *Hackint*. Dostopno prek: http://wordspy.com/words/ hackint.asp (26. maj 2014).

95. McGregor, Jay. 2014. The Top 5 Most Brutal Cyber Attacks Of 2014 So Far. *Forbes*, 28. julij. Dostopno prek: http://www.forbes.com/sites/jaymcgregor/2014/07/28/the-top-5-most-brutal-cyber-attacks-of-2014-so-far/ (31. maj 2015).
96. McKay, Tom. 2015. Anonymous Just Declared War on ISIS with a Massive Hack. *Mic*, 17. marec. Dostopno prek: http://mic.com/articles/112944/anonymous-went-after-the-islamic-state-with-a-massive-hack-but-was-it-a-good-idea (9. september 2015).
97. *Merriam-Webster*. 2014. Dostopno prek: http://www.merriam-webster.com/ (1. julij 2014).
98. Mills, Chris. 2015. FBI Investigating Attacks On Physical Internet Infrastructure In SF. *Gizmodo*, 30. junij. Dostopno prek: http://gizmodo.com/fbi-investigating-attacks-on-physical-internet-infrastr-1715087202 (5. julij 2015).
99. Mims, Christopher. 2014. Amazon and Google are in an epic battle to dominate the cloud—and Amazon may already have won. *Quartz*, 16. april. Dostopno prek: http://qz.com/196819/how-amazon-beat-google-attempt-to-dominate-the-cloud-before-it-even-got-started/ (8. september 2015).
100. *Ministrstvo za izobraževanje, znanost in šport*. 2014. Strategija kibernetske varnosti. Dostopno prek: http://www.mizs.gov.si/fileadmin/mizs.gov.si/pageuploads/Informacijska_druzba/pdf/Digitalna_Slovenija_2020_29_8_14_Strategija_kib_varnost1.pdf (7. september 2015).
101. --- 2015. Nacionalna strategija kibernetske varnosti. Dostopno prek: http://www.mizs.gov.si/fileadmin/mizs.gov.si/pageuploads/Informacijska_druzba/pdf/DSi_NSKV_v2.5_20150306.pdf (7. september 2015).
102. Moulson, Geir in John-Thor Dahlburg. 2013. Angela Merkel's Cell Phone Tapped By NSA? U.S. Accused Of Spying On German Chancellor. *The Huffington Post*, 23. december. Dostopno prek: http://www.huffingtonpost.com/2013/10/23/merkel-phone-tapped_n_4150812.html (22. julij 2014).
103. *National Whistleblowers Center*. 2012. Dostopno prek: http://www.whistleblowers.org/index.php (11. september 2015).
104. Nissenbaum, Helen. 2004. Hackers and the contested ontology of cyberspace. V *New Media & Society*, 6 (2): 195–217. Dostopno prek: http://nms.sagepub.com/content/6/2/195 (10. december 2013).

105. Odar, Vlado. 2010. *Mednarodna varnost in sodobno pomorsko piratstvo*. Magistrsko delo. Dostopno prek: http://dk.fdv.uni-lj.si/magistrska/pdfs/mag_odar-vlado.pdf (4. september 2014).

106. P. H. 2014. The incorporated woman. *The Economist*, 27. junij. Dostopno prek: http://www.economist.com/blogs/schumpeter/2014/06/who-owns-your-personal-data (8. september 2015).

107. Pagliery, Jose. 2015a. Why would China hack the U.S. government? *CNN Money*, 5. junij. Dostopno prek: http://money.cnn.com/2015/06/05/technology/why-china-hacks-us/ (19. junij 2015).

108. --- 2015b. Now you can search the Ashley Madison cheaters list. *CNN Money*, 19. avgust. Dostopno prek: http://money.cnn.com/2015/08/19/technology/ashley-madison-search/ (10. september).

109. Parker, Chris. 2014. Anonymous Unmasked. *Huffington Post*, 6. januar. Dostopno prek: http://www.huffingtonpost.com/high-times/anonymous-unmasked_b0_5065038.html (9. avgust 2015).

110. *PC Tools.* 2010. What's a Blackhat Hacker? Dostopno prek: http://www.pctools.com/security-news/blackhat-hacker/ (16. junij 2014).

111. Peck, Michael. 2013. Why Did Anonymous Have to Attack Israel on Holocaust Memorial Day? *Forbes*, 8. april. Dostopno prek: http://www.forbes.com/sites/michaelpeck/2013/04/08/why-did-anonymous-have-to-attack-israel-on-holocaust-memorial-day/ (1. september 2014).

112. Pilkington, Ed. 2015. Google warns of US government 'hacking any facility' in the world. *The Guardian*, 18. februar. Dostopno prek: http://www.theguardian.com/technology/2015/feb/18/google-warns-government-hacking-committee-hearing (21. februar 2015).

113. Purg, Adam. 1995. *Obveščevalne službe: povezave med obveščevalnimi službami, političnimi sistemi in državno suverenostjo v luči iskanja modela sodobnega obveščevalnega sistema Republike Slovenije*. Ljubljana: Enotnost.

114. Ragan, Steve. 2015a. Hacking Team hacked, attackers claim 400GB in dumped data. *CSO Online*, 5. julij 2015. Dostopno prek: http://www.csoonline.com/article/2943968/data-breach/hacking-team-hacked-attackers-claim-400gb-in-dumped-data.html (9. julij 2015).

115. --- 2015b. Hacking Team responds to data breach, issues public threats and denials. *CSO Online*, 6. julij 2015. Dostopno prek: http://www.csoonline.com/

article/2944333/data-breach/hacking-team-responds-to-data-breach-issues-public-threats-and-denials.html (9. julij 2015).

116. Ramage, Magnus. 2011. Competing Models of Information in the History of Cybernetics. V *Perspectives on Information*, ur. Magnus Ramage in David Chapman, 8–20. New York: Routledge.

117. Räsänen, Minna in James M. Nyce. 2013. The Raw is Cooked: Data in Intelligence Practice. V *Science, Technology, & Human Values*, 38 (5): 655–677. Dostopno prek: http://sth.sagepub.com.nukweb.nuk.uni-lj.si/content/38/5/655.full.pdf+html (10. september 2015).

118. Ravenscraft, Eric. 2014. What We Can Learn from the Biggest Corporate Hacks. *Lifehacker*, 16. december. Dostopno prek: http://lifehacker.com/what-we-can-learn-from-the-biggest-corporate-hacks-1671682353 (9. junij 2015).

119. Ravisankar, Vivek. 2015. Hacking Hackathons: How 4,000 Events Taught Me the Four Keys for Any Organization to be a Successful Host. *Forbes*, 4. marec. Dostopno prek: http://www.forbes.com/sites/vivekravisankar/2015/03/04/hacking-hackathons-how-4000-events-taught-me-the-four-keys-for-any-organization-to-be-a-successful-host/ (5. september 2015).

120. Raymond, Eric Steven. 2001. *How To Become A Hacker*. Dostopno prek: http://catb.org/~esr/faqs/hacker-howto.html (28. maj 2014).

121. Robinson, Neil, Luke Gribbon, Veronika Horvath in Kate Robertson. 2013. *Cyber-security threat characterisation: A rapid comparative analysis*. Dostopno prek: http://www.rand.org/content/dam/rand/pubs/research_reports/RR200/RR235/RAND_RR235.pdf (11. september 2015).

122. Samuel, Alexandra. 2004. *Hacktivism and the Future of Political Participation*. Doktorska disertacija. Dostopno prek: http://alexandrasamuel.com/dissertation/pdfs/Samuel-Hacktivism-entire.pdf (10. junij 2014).

123. Schmidt, Michael S., David E. Sanger in Nicole Perlroth. 2014. Chinese Hackers Pursue Key Data on U.S. Workers. *The New York Times*, 9. julij. Dostopno prek: http://www.nytimes.com/2014/07/10/world/asia/chinese-hackers-pursue-key-data-on-us-workers.html (15. februar 2015).

124. Schwartz, Matthew J. 2012. Who Is Anonymous: 10 Key Facts. *Dark reading*, 6. februar. Dostopno prek: http://www.darkreading.com/attacks-and-breaches/who-is-anonymous-10-key-facts/d/d-id/1102672?page_number=1 (7. maj 2015).

125. Sciutto, Jim. 2015. China, Russia amassing personal info seized in hacks for counter-intelligence. *CNN Politics*, 2. september. Dostopno prek: http://edition.cnn.com/2015/09/01/politics/china-russia-cyberattacks-military/index.html?sr=tw090215chinarussiamadison1120aVodTopPhoto (10. september 2015).

126. Sherwell, Philip. 2013. Barack Obama 'approved tapping Angela Merkel's phone 3 years ago'. *The Telegraph*, 27. oktober. Dostopno prek: http://www.telegraph.co.uk/news/worldnews/europe/germany/10407282/Barack-Obama-approved-tapping-Angela-Merkels-phone-3-years-ago.html (22. julij 2014).

127. Shulsky, Abram N. in Gary J. Schmitt. 2002. *Silent warfare: understanding the world of intelligence*. Washington D. C.: Potomac Books Inc.

128. *SI-CERT*. 2015. Phishing. Dostopno prek: https://www.cert.si/si/varnostne-groznje/phishing/ (12. april 2015).

129. Simčič, Milan. 2011. Kaj je sploh računalništvo v oblaku? *Moj mikro*, 18. julij. Dostopno prek: http://www.mojmikro.si/center/povem_naglas/kaj_je_sploh_racunalnistvo_v_oblaku (8. september 2015).

130. Singel, Ryan. 2009. Is the Hacking Threat to National Security Overblown? *Wired*, 3. junij. Dostopno prek: http://www.wired.com/threatlevel/2009/06/cyberthreat/ (21. februar 2014).

131. Skoudis, Edward. 2009. Information Security Issues in Cyberspace. V *Cyberpower and National Security*, ur. Franklin D. Kramer, Stuart H. Starr in Larry K. Wentz, 171–205. Washington, D. C.: National Defense University Press in Potomac Books.

132. Slobogin, Christopher. 2008. Government Data Mining and the Fourth Amendment. V *The University of Chicago Law Review*, 75 (1): 317–341. Dostopno prek: http://www.jstor.org/stable/20141910?origin=JSTOR-pdf (10. december 2013).

133. *Slovar slovenskega knjižnega jezika*. Dostopno prek: http://bos.zrc-sazu.si/sskj.html (5. september 2015).

134. Stern, Marlow. 2015. Ashley Madison Hack: 10,000 Gov't Officials' Email Addresses on Leaked Ashley Madison List. *The Daily Beast*, 19. avgust. Dostopno prek: http://www.thedailybeast.com/articles/2015/08/19/ashley-madison-hack-identities-of-33-million-aspiring-adulterers-released-online.html (8. oktober 2015).

135. Svete, Uroš, Damijan Guštin in Vladimir Prebilič. 2010. Asimetrija in vojaška organiziranost: slovenske izkušnje. V *Mednarodne razsežnosti varnosti Slovenije*, ur. Marjan Malešič, 247–280. Ljubljana: Fakulteta za družbene vede.

136. Svete, Uroš. 2006. Informacijsko-komunikacijska tehnologija in sodobne varnostne teorije. V *Varnost v postmoderni družbi*, ur. Marjan Malešič, 47–67. Ljubljana: Fakulteta za družbene vede.

137. Šimek, Jakub. 2012. Hacktivists and Whistleblowers – an Emerging Hybrid Threat? V *Panorama of global security environment*, ur. Marian Majer, Róbert Ondrejcsák in Vladimír Tarasovič, 663–679. Bratislava, CENNA. Dostopno prek: http://cenaa.org/analysis/hacktivists-and-whistleblowers-an-emerging-hybrid-threat/ (11. september 2015).

138. Štamcar, Miha. 2014. Deset najpomembnejših žvižgačev. *Dnevnikova priloga Objektiv*, 19 (21. junij).

139. Tanczer, Leonie Maria. 2015. Hacktivism and the male-only stereotype. V *New Media & Society*, 14. januar. Dostopno prek: http://nms.sagepub.com.nukweb.nuk.uni-lj.si/content/early/2015/01/12/1461444814567983.full.pdf+html (11. september 2015).

140. Taylor, Richard in Bin Zhang. 2008. *Measuring the Impact of ICT: Theories of Information and Development.* Dostopno prek: https://www.academia.edu/2068941/Measuring_the_Impact_of_ICT_Theories_of_Information_and_Developoment (6. september 2014).

141. *Techopedia*. 2014. Black Hat Hacker. Dostopno prek: http://www.techopedia.com/definition/26342/black-hat-hacker (16. junij 2014).

142. *Telemach*. VPN povezava. Dostopno prek: http://www.telemach.si/sl/poslovni-uporabniki/varnostne-resitve/vpn-povezava (9. julij 2015).

143. *The Enemies of Internet*. 2015. Hacking Team. Dostopno prek: http://surveillance.rsf.org/en/hacking-team/ (12. april 2015).

144. *The Guardian.* 2015. Second hack of federal records hit intelligence and military personnel, 12. junij. Dostopno prek: http://www.theguardian.com/technology/2015/jun/12/hacking-personnel-data-4-million-federal-workers (19. junij 2015).

145. *The Jargon File.* 2014. Cracker. Dostopno prek: http://catb.org/jargon/html/C/cracker.html (13. junij 2014).

146. Tobias, Mark Weber. 2012. Hacking The Hackers: A Counter-Intelligence Operation Against Digital Gangs. *Forbes*, 26. april. Dostopno prek: http://www.forbes.com/sites/marcwebertobias/2012/04/26/hacking-the-hackers-a-counter-intelligence-operation-against-digital-gangs/ (21. februar 2014).

147. Traynor, Ian. 2007. Russia accused of unleashing cyberwar to disable Estonia. *The Guardian*, 17. maj. Dostopno prek: http://www.theguardian.com/world/2007/may/17/topstories3.russia (13. junij 2014).

148. Turgeman-Goldschmidt, Orly. 2005. Hackers' Accounts: Hacking as a Social Entertainment. V *Social Science Computer Review*, 23 (1): 8–23.

149. *U.S. Department of State.* 2015. Counterintelligence Investigations. Dostopno prek: http://www.state.gov/m/ds/terrorism/c8653.htm (5. september 2015).

150. *United States Department of Labor*. 2015. Whistleblower Protections. Dostopno prek: http://www.dol.gov/compliance/laws/comp-whistleblower.htm (11. september 2015).

151. Waddell, Kaveh. 2015. The Release of Ashley Madison Users' Info Is More Than Just Embarrassing—It's a Security Threat. *National Journal*, 19. avgust. Dostopno prek: http://www.nationaljournal.com/tech/2015/08/19/release-ashley-madison-users-info-is-more-than-just-embarrassing-its-security-threat (10. september 2015).

152. Waites, Rosie. 2011. V for Vendetta masks: Who's behind them? *BBC News Magazine*, 20. oktober. Dostopno prek: http://www.bbc.co.uk/news/magazine-15359735 (1. september 2014).

153. Wall, David S. 2004. Digital Realism and the Governance of Spam as Cybercrime. V *European Journal on Criminal Policy and Research*, 10 (4), 309–335. dostopno prek: http://link.springer.com.nukweb.nuk.uni-lj.si/article/10.1007/s10610-005-0554-8 (10. oktober 2015).

154. Wark, McKenzie. 2008. *Hekerski manifest*. Ljubljana: Maska.

155. Wee, Sui-Lee. 2014. China confronts U.S. envoy over cyber-spying accusations. *Reuters*, 20. maj. Dostopno prek: http://www.reuters.com/article/2014/05/20/us-china-usa-espionage-idUSBREA4J03D20140520 (15. februar 2015).

156. *Wetboek van Strafrecht*. Dostopno prek: http://wetten.overheid.nl/BWBR0001854/TweedeBoek/TitelV/Artikel138ab/geldigheidsdatum_16-07-2015 (24. avgust 2015).

157. *Whistleblower Protection Program*. 2015. Dostopno prek: http://www.whistleblowers.gov/index.html (11. september 2015).

158. Whitney, Lance. 2012. Microsoft reportedly asks China to stop state-run software pirates. *CNET*, 20. september. Dostopno prek: http://www.cnet.com/news/

microsoft-reportedly-asks-china-to-stop-state-run-software-pirates/ (9. september 2015).

159. Wible, Brent. 2003. A Site Where Hackers Are Welcome: Using Hack-In Contests to Shape Preferences and Deter Computer Crime. V *The Yale Law Journal*, 112 (6): 1577–1623. Dostopno prek: http://www.jstor.org/stable/3657453 (10. december 2013).

160. Wong, Edward. 2013. Hackers Find China Is Land of Opportunity. *The New York Times*, 22. maj. Dostopno prek: http://www.nytimes.com/2013/05/23/world/asia/in-china-hacking-has-widespread-acceptance.html?pagewanted=all&_r=3& (6. september 2015).

161. *Zakon o elektronskih komunikacijah* (ZEKom-1). Uradni list RS 109/2012. Dostopno prek: https://www.uradni-list.si/1/content?id=111442 (7. september 2015).

162. *Zakon o ratifikaciji Konvencije o kibernetski kriminaliteti in Dodatnega protokola h Konvenciji o kibernetski kriminaliteti, ki obravnava inkriminacijo rasističnih in ksenofobičnih dejanj, storjenih v informacijskih sistemih* (MKKKDP). Uradni list RS 62/2004. Dostopno prek: http://www.uradni-list.si/1/objava.jsp?urlmpid=200468 (11. september 2015).

163. Zetter, Kim. 2013. American gets targeted by digital spy toolsold to foreign governments. *Wired*, 4. junij. Dostopno prek: http://www.wired.com/2013/06/spy-tool-sold-to-governments/ (12. april 2015).

164. Zito Rowe, Ashley. 2013. Hiring for Hackers Continues to Rise. *Wanted Analytics*, 26. oktober. Dostopno prek: http://www.wantedanalytics.com/insight/2013/10/26/hiring-for-hackers-continues-to-rise/ (21. februar 2014).