UNIVERZA V LJUBLJANI
FAKULTETA ZA DRUŽBENE VEDE

Maja Bolle

Odprtokodna programska oprema in informacijska varnost

Magistrsko delo

Ljubljana, 2014

UNIVERZA V LJUBLJANI
FAKULTETA ZA DRUŽBENE VEDE

Maja Bolle

Mentor: doc. dr. Uroš Svete

Odprtokodna programska oprema in informacijska varnost

Magistrsko delo

Ljubljana, 2014

Zahvala mentorju za potrpežljivost in usmeritve.
T. za lekturo in pomoč ter svetovanje in
družini, ker so verjeli vame.

Odprtokodna programska oprema in informacijska varnost

Informacijska varnost postaja pomembna varnostna tema, zaradi vedno večje odvisnosti od računalniških sistemov. Bojevanje se je z leti preneslo tudi v kibernetski prostor in sedaj tudi že poteka na državni ravni. Vsakodnevne novice o kibernetskih napadih in drugih vdorih v informacijske sisteme za katerimi naj bi stale tudi države z namenom pridobivanja informacij ali potencialnega uničenja sistema (Stuxnet), nas spomnijo na čase hladne vojne. V času hladne vojne je potekal boj med velesilama ZDA in Sovjetsko zvezo, z namenom premoči ene nad drugo na vseh področjih. Boj ni nikdar postal »vroč«, vendar je temeljil na vohunjenju, posredniških vojnah in zbiranju informacij. Ali morda danes zopet poteka nova hladna vojna le, da tokrat v kibernetskem prostoru (»kibernetska hladna vojna«)? Ker niso vse države velesile, ki bi se lahko enakovredno kosale z nasprotnicami v boju v kibernetskem prostoru, se mnoge na defenzivni ravni zatekajo k odprtokodni programski opremi, ki jim poleg varčevanja pri nakupu programskih licenc omogoča tudi večji nadzor nad to opremo.

Ključne besede:

odprtokodna programska oprema, informacijska varnost, kibernetska hladna vojna, hladna vojna, Iskra Delta, kibernetsko bojevanje.

Open source software and information security

Because of our dependence on computer the information security is getting more important thru the years and it is becoming a security issue. Thru the years the conventional warfare transferred to cyber space and is now happening also on national level. Daily news about cyber attacks with the aim to gain information or to destroy the system (Stuxnet), and the cyber attacks that are supposed to be supported by the government reminds us of the cold war era. During cold war there was a struggle between USA and Soviet Union to gain power over each other on all levels. The fight never became "hot", but it was based upon espionage, proxy wars and collecting data. Is there another cold war happening now only this time in cyber space ("cyber cold war")? Not every country is superpower; therefore they can not fight on equal level in cyber warfare. Therefore they use open source software on defensive level. Open source software provides countries with cheaper alternatives and gives them better control of the system itself.

Keywords:
open source software, information security, cyber cold war, cold war, Iskra Delta, cyber warfare.

KAZALO

1 Uvod in metodologija

Smo v dobi, ko življenje in predvsem delo brez računalnika ni več mogoče. Prav zato je to čas, ko je vprašanje informacijske varnosti vedno bolj pereče. Že v devetdesetih letih prejšnjega stoletja so nas presenetile novice o zlorabi sistema Echelon (ki je bil narejen v času hladne vojne z namenom prestrezanja privatne in poslovne komunikacije) v namene industrijskega in političnega vohunjenja proti zaveznikom (Report 2001). Vrhunec razkritij se je zgodil leta 2013, ko je Edward Snowden razkril, kako ameriške varnostne agencije vdirajo v zasebnost posameznikov in tudi držav. Mnogi so se ob tem spomnili na čas hladne vojne. To je bil čas, ko je vladalo nezaupanje med državami. Ene in druge so uporabljale prikrita sredstva za dosego premoči nad drugo, na tehnološkem, strateškem ali diplomatskem področju. Snowden nam je razkril, da velika podjetja, kot so Apple, Microsoft, Skype, Facebook in še mnoga druga, sodelujejo z ameriškimi varnostnimi agencijami pri razvoju programske opreme in vanjo vnašajo stranska vrata ter drugo zlonamerno programsko opremo, preko katere lahko ameriške varnostne agencije nadzorujejo uporabnika. Zaradi vedno večjega števila posegov v integriteto najbolj uporabljanih operacijskih sistemov in drugega programja, so mnoge države začele iskati rešitve v odprtokodni programski opremi, saj so želele biti čim bolj neodvisne od ameriških sistemov (Kimberly 2005). Odprtokodna programska oprema (v nadaljevanju OKPO) je izraz za programsko opremo, katere izvorna koda je prosto dostopna in jo je mogoče prosto uporabljati, raziskovati njeno delovanje, spreminjati in razširjati tako originalne kot dopolnjene in spremenjene kopije te programske opreme; za razliko od zaprtokodne programske opreme, kjer našteto ni omogočeno. Pogoji uporabe OKPO so napisani v različnih licencah, ki vsebujejo smernice uporabe Open Source Initiative. Najpomembnejši kriteriji so prosto razširjanje, dostop do izvorne kode in dovoljenje za spreminjanje ter integracijo te kode (The Open Source Initiative 2013). OKPO je v uporabi in se razvija zlasti v državah v razvoju (Kshetri 2005). Tem državam ponuja cenejšo in varnostno zanesljivejšo alternativo obstoječim zaprtokodnim sistemom.

Z leti je vedno bolj v porastu kibernetski kriminal, kot so vdori v informacijske sisteme ali kraja podatkov. Če smo nekoč mislili, da so najbolj na udaru preprosti uporabniki, smo se močno zmotili. Vedno več je napadov, ki se vršijo na države in državno

infrastrukturo. Še bolj zaskrbljujoče je, ker obstaja vedno več indicev, da za napadi stoji neka država. Taka dejanja, pa lahko že privedejo do tako imenovanega kibernetskega bojevanja. Mediji največ pozornosti posvečajo napadom, ki jih izvaja Kitajska nad ZDA. Z razkritji Edwarda Snowdna, pa se je pokazalo, da dnevno vdira v računalnike po vsem svetu tudi ameriška nacionalno varnostna agencija (National Security Agency v nadaljevanju NSA). Iz takšnega nadzora so bolj ali manj izključene samo ZDA, Kanada, Nova Zelandija, Velika Britanija in Avstralija (tako imenovanih »pet oči«) (Farell 2013). Zato se tudi danes vedno bolj govori o tako imenovani »kibernetski hladni vojni«, ki zopet deli svet in vnaša nezaupanje med države zaradi vdorov v informacijske sisteme. Vedno več je držav, ki se pripravljajo za bojevanje v kibernetskem prostoru z ustanovitvijo vojaških enot ali z razvojem zlonamerne programske opreme, ki jo lahko uporabijo za napade različnih vladnih ali nevladnih akterjev. Ker se mnoge države težje finančno kosajo z velesilami, kot so Kitajska, ZDA in Rusija, si zato na področju kibernetskega bojevanja in kibernetskega kriminala, pomagajo predvsem na defenzivni ravni. Mnoge prehajajo iz zaprtokodnih operacijskih sistemov na odprtokodne operacijske sisteme, ki jih same lažje razvijajo in nadzorujejo, predvsem pa tudi veliko finančno prihranijo na ta račun. Z lastnim razvojem programske opreme, njihovi produkti pridobivajo dodatno vrednost, kar se kaže v večji konkurenčnosti te države na trgu.

Opomba: Prvi del magistrske naloge je bil že objavljen, kot strokovni članek v reviji Sodobni vojaški izzivi 13 (3): 61–79, z naslovom Odprtokodna programska oprema in informacijska varnost (Bolle 2011).

Hipoteza:

H1: V svetu poteka „kibernetska hladna vojna“, ki postaja vedno bolj „vroča“ in katere del je tudi OKPO.

Metodologija:

Analiza vsebine tujih primarnih virov v tiskani in spletni obliki. Prednosti in slabosti uporabe OKPO bom proučila s primerjalno analizo. Področje »kibernetske hladne vojne« in uporabe OKPO bom proučevala s študijami primerov in s pomočjo deduktivnega sklepanja bom skušala predstaviti stanje in analizo trendov v informacijski varnosti. Uporabila bom tudi metodo interpretiranja statistik in analitično sintetično metodo.

2 Zgodovina in filozofija odprte kode

Začetki OKPO segajo v 50-ta leta 20. stoletja. Teza, da so ljudje od nekdaj plačevali za programsko opremo, je napačna. Prvi računalniki so bili izjemno veliki, nezmogljivi glede na današnje standarde, predvsem pa so imeli izjemno slabo programsko opremo. Prvi računalnik, ki je bil na voljo za komercialno uporabo, je bil IBM-ov 701 iz leta 1952, za katerega je moral uporabnik na mesec plačevati 15.000 $ uporabnine. Zaradi visoke cene, si ga je lahko privoščilo le Ministrstvo za obrambo ZDA, kjer je dobil vzdevek „obrambni kalkulator“. Kasnejša različica 701 je bila 705 iz leta 1953, katere cena je bila 1.6 milijona dolarjev. A bolj kot cena takratnih računalnikov, je bila problematična programska oprema. Uporabniški vmesniki so bili uporabniku neprijazni. Tudi sama zmogljivost programske opreme je bila manjša, kot jo je omogočala strojna oprema. Ker je bilo programerjev malo, so se začeli uporabniki združevati, si deliti ideje in programsko opremo, ki bi bolje izkoristila strojne zmogljivosti in zadovoljila potrebe uporabnikov. Sčasoma so se ustanovila prva združenja, ki so povezovala takšne zanesenjake - najbolj znano je združenje SHARE iz leta 1955. Proti koncu 60. let se je sistem spremenil. Podjetja, ki so prodajala strojno opremo, so kupcu priložila tudi pripadajočo programsko opremo, ki je bila takrat brezplačna (Software Becomes a Product 2014). Na drugi strani se je vedno bolj krepil trg programske opreme, ki je ponujal plačljivo programsko opremo. Ker so se kupci začeli pritoževati, da ne želijo imeti prednaložene programske opreme, češ da naj ne bi zadovoljevala njihovih potreb in da ustvarja monopol, je ameriško sodišče 17. januarja 1969 v sodbi ZDA proti IBM razsodilo, da prednaložena programska oprema zavira konkurenco na trgu (Usselman 2009, 249–278). Kot vidimo danes, se mnogi požvižgajo na sklep sodišča, saj dobimo ob nakupu novega računalnika v večini primerov prenaloženo programsko opremo. Takšna politika je z leti Microsoftu omogočila skorajda monopolni položaj na področju operacijskih sistemov.

2.1 Nastanek prve odprtokodne programske opreme

2.1.1 Unix

Šele leta 1970 je podjetje DEC na tržišču ponudilo prvi računalnik PDP-11, ki je imel dovolj nizko ceno (11.000$), da so si ga lahko privoščile univerze in raziskovalni inštituti (Weber 2004, 23). Leta 1969 je Ken Thompson izdelal operacijski sistem na računalniku PDP-7 in ga poimenoval UNICS (ang. Uniplexed information and computing services); sistem so kasneje preimenovali v Unix. Unix se je začel širiti po univerzah in raziskovalnih inštitutih. Do leta 1972 je bilo namestitev le deset. Velikansko prepoznavnost je Unix doživel, ko sta Ken Thompson in Dennis Ritchie na ACM Simpoziju 1973 predstavila znanstveni članek na temo Unix-a. Po objavi članka je število namestitev skokovito naraslo. Podjetje AT&T, pri katerem je bil Thompson zaposlen, je v Unix-u zaslutilo poslovno priložnost in zahtevalo njegovo licenciranje. Prva licenca je bila brezplačna in je uporabnikom dovoljevala še precej svoboščin, vendar AT&T zanjo ni omogočal podpore. V vsaki programski opremi, neizbežno prihaja do pojava t.i. hroščev (angl. bug), ki pomenijo napako v programski kodi, ta pa vodi v nezaželene in nepričakovane izide pri njeni uporabi. Vse to je imelo takojšen vpliv na uporabnike Unix-a, ki so se začeli povezovati v skupine, družno odpravljati hrošče in Unix izboljševati - tega AT&T s svojo licenco ni predvidel. Vseeno, pa je bila koda tako zaprta, da so morale omenjene skupine AT&T za dostop do izvorne kode, plačati nekaj 100$. To je storila tudi raziskovalna skupina BTL, ki je izvorno kodo Unix-a prepisala v C programski jezik, s spremembami v kodi pa omogočila, da je Unix od takrat dalje deloval na vsakršni strojni opremi in vsakem računalniku. Prav tako je omogočal, da so uporabniki sami izdelovali gonilnike (angl. driver) za tiskalnike in podobno opremo, ki so jo potrebovali pri svojem delu. Do leta 1975 je Unix tekel na preko petdesetih inštitucijah po ZDA (Weber 2004, 20–29).

2.1.2 BSD

Pomembno vlogo pri razvoju odprte kode ima kalifornijska univerza Berkeley. Tamkajšnji raziskovalci so leta 1973 pod okriljem profesorja Boba Fabryja ustanovili Oddelek za računalniške znanosti, statistiko in matematiko, na katerem so Unix uporabljali, dopolnjevali in spreminjali. Raziskovalca Bill Joy in Chuck Haley sta razvijala samo jedro Unix-a in ga dopolnjevala. Leta 1978 je Joy izdelal kopico dodatkov za Unix, ki jih je skupaj z jedrom Unix spravil v paket imenovan Berkeley Software Distribution (BSD), ki ni bil samostojni operacijski sistem, temveč distribucija Unix-a. BSD je postal zelo priljubljen med študenti, kot tudi raziskovalci; ti so vedno bolj opuščali Unix in raje uporabljali BSD (Weber 2004, 29–33).

Leta 1968 je začel delovati predhodnik današnjega interneta, ARPANET. Sprva je povezoval agencijo ameriškega obrambnega ministrstva DARPA (Defense Advanced Research Projects Agency) in ostale raziskovalne institucije. DARPA je želela preko ARPANET-a komunicirati z ostalimi inštitucijami, vendar sta bili komunikacija in pošiljanje datotek otežkočena, zaradi nekompatibilnosti med različnimi računalniki in operacijskimi sistemi. Ker bi bilo poenotenje strojne opreme drago, se je DARPA obrnila na razvijalce BSD z namenom, da bi se razvilo programsko opremo, ki bi delovala na vseh strojnih opremah. Fabry je leta 1979 podpisal pogodbo o razvoju BSD, ki bo deloval po željah DARPA. V ta namen je Univerza Berkeley ustanovila nov oddelek imenovan CSRG (Computer System Research Group); leta 1981 so za DARPA razvili 4.1 BSD. Naslednja različica 4.2. BSD iz leta 1983 je vključevala novo razviti TCP/IP protokol za medmrežno komunikacijo, ki ga uporabljamo še danes in je temelj današnjega interneta. Različica 4.2 BSD je bila do takrat najhitreje razširjena distribucija. Bila je naložena na preko 1000 računalnikov. Prav internet in protokol TCP/IP sta ena glavnih krivcev, da se je začela distribucija BSD množično širiti po medmrežju. AT&T je medtem vedno bolj zaostroval licenco za Unix in ji s tem posledično višal ceno. Leta 1989 je bila cena licence 250.000$, česar si univerze niso več mogle privoščiti in zato presedlale na BSD. Da bi lahko celoten operacijski sistem ponudili pod BSD licenco in postali neodvisni od AT&T, so ustvarjalci BSD leta 1981 celotno Unix kodo zamenjali z lastno kodo (Weber 2004, 40–43).

2.1.3 Homebrew Computer Club

Za razvoj odprte kode je ključna tudi skupina Homebrew Computer Club iz leta 1975. Združevala je računalniške zanesenjake, ki so preizkušali meje programske in strojne opreme. Med uporabnikom in programerjem takrat še ni bilo večje ločnice. Načelo kluba je bilo, da so si člani lahko izposodili katero koli programsko opremo (vključno z izvorno kodo), vendar pod pogojem, da so naredili vsaj dve kopiji in ju razdelili drugim, opremo pa vrnili. Bill Gates, ki je istega leta ustanovil podjetje Microsoft, se ni strinjal z načinom delovanja Homebrew, zato je leta 1976 napisal znano protestno pismo z naslovom „Odprto pismo“. Gatesa je jezilo, saj je takrat s soustanoviteljem Microsofta Paulom Allenom napisal programski jezik Basic, ki je bil takrat precej popularen, vendar so ga vsi kopirali, Microsoftu pa zanj nihče ni plačal licence. Gates v pismu opozarja, da večina članov Homebrew krade intelektualno lastnino in s tem onemogoča nadaljnji razvoj, saj razvijalcev finančno ne podprejo (Weber 2004, 35-37).

2.1.4 Free Software Fundation

Richard Stallman, ki ga danes poznamo kot ustanovitelja Free Software Foundation, je začel v 70-ih letih delati na MIT (Massachusetts Institute of Technology). Delal je na oddelku Artificial Intelligence Lab, kjer so raziskovalci razvijali lastno programsko opremo in njeno varnost preizkušali tako, da so drug drugemu vdirali v računalnike. Zelo kmalu je tudi MIT začel omejevati svobodno nameščanje programske opreme. Stallmanu to ni bilo všeč, vrhunec nezadovoljstva pa je dosegel leta 1979, ko je njihov oddelek dobil nove laserske tiskalnike podjetja Xerox. Ker so se v tiskalniku konstantno zatikali papirji, je želel sam popraviti programsko opremo tiskalnika in s tem rešiti problem, vendar mu podjetje Xerox ni želelo dati izvorne kode. Kmalu zatem je na MIT dal odpoved in ustanovil Free Software Foundation. Cilj te neprofitne ustanove je bil, narediti popolnoma brezplačni operacijski sistem, katerega izvorna koda bo na voljo vsem in jo bo mogoče tudi svobodno spreminjati. Operacijski sistem je poimenoval GNU (GNU's Not Unix). Leta 1984 je napisal GNU Manifest, v katerem je razložil pomen besede Free Software; ta ne pomeni nujno brezplačne programske

opreme, temveč svobodno ali prosto programsko opremo. Svoboda se pri tem nanaša na dostopnost do izvorne kode in možnost njenega spreminjanja (beseda „free“ v angleškem jeziku ustvarja semantično zmedo, saj ne razlikuje med brezplačen in svoboden, zato je Stallman rešitev poiskal v španskem izrazu „libre“) (Wynants in Cornelis 2005, 69–85). Stallman torej ne nasprotuje temu, da ima programska oprema ceno, s katero se plača delo programerja, vendar mora biti v svoji osnovi svobodna (špan. libre). V manifestu je napisal štiri temeljna načela Free Software, ki veljajo še danes:

1. Svobodno uporabljati program v katerikoli namen (svoboščina št. 0);
2. Svobodno preučevati program in ga spremeniti po svoji želji. Dostop do izvorne kode je predpogoj za to (svoboščina št. 1);
3. Svobodno posredovanje kopij (svoboščina št. 2);
4. Svoboda izboljšanja programa in objava izboljšav (in prilagojenih verzij) javnosti v korist skupnosti (svoboščina št. 3); dostop do izvorne kode je predpogoj za to.

Ker se je Stallman zavedal možnosti izkoriščanja štirih temeljnih svoboščin proste programske opreme, je naredil še bolj dodelano licenco, ki je nasprotje copyright, imenuje pa se General Public License (GPL). Programska oprema licencirana pod GPL, nikoli ne more postati lastniška, prav tako tudi spremenjena programska oprema, ki izvira iz prosto programske. Tudi nikakršen del kode programske opreme licencirane pod GPL, ne sme postati del lastniške kode programske opreme. Sme se izdati le kombinacija lastniške in proste programske opreme, vendar pod pogojem, da je celotna licencira pod GPL (Weber 2004, 46-49). GPL-licenca je bila sčasoma dopolnjena (zadnja različica je GPL v3) in je služila kot podlaga drugim, bolj specifičnim licencam (Licenses 2014).

2.1.5 Linux

Svetovno najbolj razširjen odprtokodni operacijski sistem na področju super računalnikov je Linux, ki ima 96% tržnega deleža, za njim je Unix s 2.2% in Windows z 0.4% (Statistics 2013). Največji tržni delež ima tudi na področju strežnikov - 68% glede na podatke ankete Security Space 2012 (Web Server Survey 2012). Vendar pa ima Linux še vedno najmanjši delež na področju osebnih računalnikov (2.12%) medtem, ko imata Windows 65% in Mac OS X 8.4% tržnega deleža (December 2013).

Linux je nastal leta 1991 pod okriljem takrat 21-letnega Linusa Torvaldsa. 25. avgusta 1991 je v novičarski skupini comp.os.minix najavil namero o razvoju jedra novega operacijskega sistema (angl. kernel). 17. septembra je na internetu javno objavil prvo različico Linux jedra operacijskega sistema. Ljudi je javno pozval, da njegov sistem preizkusijo in ga izboljšajo. Linux je iz dneva v dan dobival več podpornikov in razvijalcev, zato je bila že leta 1994 izdana prva različica 1.0.0. Leta 1996 je bila izdana različica 2.0.0, istega leta pa je Torvalds tudi patentiral blagovno znamko Linux (Weber 2004, str. 98–128). Linux danes teče na praktično vsaki računalniški arhitekturi (namizni računalniki, super računalniki, strežniki, zapestne ure, igralna konzola Playstation 3 ...) (LinuxGizmos.com 2014).

Linux je zgolj jedro operacijskega sistema, zato so razvijalci s celega sveta zanj razvili še grafični vmesnik, namizja, programe, igrice, gonilnike ... in vse to združili v paket imenovan distribucija. Distribucije temeljijo na določenem jedru operacijskega sistema (npr. Linux, BSD ...) in se med seboj razlikujejo po tem, kakšno programsko opremo, namizje in skladišča programske opreme vsebujejo. Svetovno najbolj razširjena in priljubljena Linux distribucija je Ubuntu, ki naj bi jo glede na podatke uporabljalo preko 12 milijonov ljudi na namiznih računalnikih po vsem svetu (Jose 2011).

3 Informacijska varnost odprtokodne programske opreme

Varnost je relativna, saj jo vsak posameznik dojema drugače. Realne grožnje varnosti tudi niso nujno zaznane grožnje varnosti. Poznamo klasično realistično teorijo varnosti, kjer je referenčni objekt varnosti država. Vendar za naše proučevanje informacijske varnosti bolj pridejo v poštev novejše teorije varnosti, ki so nastale po koncu hladne vojne (kot so koncept človekove varnosti, omrežne varnosti, kritična teorija varnosti, konstruktivistična itd.). Skupno novejšim teorijam varnosti je, da se je spremenil referenčni objekt. Spremembe so nastale tako na vertikalni ravni iz države na mednarodno skupnost, družbo in posameznika. Prav tako so nastajale tudi na horizontalni, iz vojaške na gospodarsko, kulturno, identitetno, okoljsko itd. Posledica takšnih širitev je tudi zaznavanje novih tipov groženj (Prezelj 2001). Z razvojem informacijske tehnologije so se pojavile tudi grožnje informacijski tehnologiji. Posledično je nastal koncept informacijske varnosti, ki vključuje varstvo podatkov in informacijskih sistemov, pred nezakonitimi dostopi, razkritjem, uporabo ali uničenjem (CNSS Instruction No. 4009 2010). Na področju informacijske varnosti prevladujeta dva pristopa „top-down“ in „bottom- up“. „Top-down“ pristop izvira iz koncepta nacionalne varnosti in temelji na realistični teoriji. V ospredje postavlja državo in njeno vlogo pri pisanju in sprejemanju zakonodaje, smernic in strategij na področju informacijske varnosti. Za varnost posameznika na področju informacijsko komunikacijske tehnologije (v nadaljevanju IKT) mora poskrbeti država, vendar pa lahko tudi posamezniki posredno ali neposredno ogrožajo državo na področju IKT varnosti (Svete 2005, 206). Slabost takšnega sistema je, da zakonodaja zaostaja za prakso in države v praksi težko ščitijo posameznike na področju varnosti IKT. „Bottom-up“ pristop pa izvira iz koncepta človekove varnosti, liberalistične in konstruktivistične teorije. V ospredje postavlja posameznika z njegovimi normami, vrednotami in interesi. Posameznik na področju varnosti IKT ni zgolj žrtev, ki ga mora država ščititi, ampak je izjemno pomemben dejavnik znotraj informacijske varnosti, saj lahko z svojim delovanjem močno vpliva na informacijsko varnost. Nevešč posameznik na področju IKT lahko zelo ogrozi varnost, po drugi strani pa lahko zelo vešč posameznik veliko prispeva k varnosti (Svete 2005, 202–216).

OKPO na področju informacijske varnosti bolj predstavlja „Bottom-up“, saj daje možnost vsakemu posamezniku možnost nadzora nad lastnim sistemom. Za varnost lastnega sistema je odgovoren vsak posameznik, vendar pa tukaj tudi zelo pride do izraza odprtokodna skupnost, ki javno opozarja na nevarnosti in daje možnost vsakemu, da prispeva k večji varnosti sistema z lastnim razvojem popravkov in predlaganjem rešitev.

Idealen sistem bi bil kombinacija „top-down“ in „bottom-up“. Države potrebujejo strateške usmeritve in zakonodajo na področju informacijske varnosti vendar pa je tudi zelo dobro, da imajo informacijsko bolj vešče posameznike, ki dobro skrbijo za varnost lastnega sistema s čemer preprečujejo širjenje potencialne zlonamerne programske opreme.

Če pobližje pogledamo samo varnost OKPO, se znajdemo pred veliko dilemo. Ali je bolj varen tisti sistem, ki ima manj hroščev ali tisti, ki zelo hitro naredi popravke za ranljivosti ali zopet tretji, katerega ranljivosti prizadenejo manj ljudi? Veliko je raziskav, ki govorijo v prid ene ali druge rešitve. Večina se osredotoča zgolj na enega od zgoraj naštetih aspektov (Laurie 2006, 61). Problematiko varnosti OKPO v nadaljevanju skušam predstaviti v čim širšem kontekstu skozi različne indikatorje (številne distribucije, zlonamerna programska oprema, varnost skozi transparentnost, sistem »veliko oči« in čas za popravek), ki so z informacijsko varnostjo tako ali drugače povezani.

3.1 Številne distribucije

Po podatkih Distro Watch (Distrowatch.com 2013), je na svetu trenutno preko 320 distribucij temelječih na Linux ali Unixu-podobnih operacijskih sistemih. Realno število distribucij je v resnici veliko večje, saj lahko doma vsakdo naredi svojo distribucijo. Prav veliko število distribucij omogoča, da je verjetnost, da bi bila zlonamerna programska oprema pisana za točno določeno distribucijo, veliko manjša kot je to pri zaprtokodni programski opremi. V dveh najbolj razširjenih zaprtokodnih operacijskih sistemih niti ne poznamo pojma distribucija, saj vsak posameznik kupi operacijski sistem, ki ne obstaja v več distribucijah, temveč zgolj različicah (Apple in njegov Mac OS X z različicami Snow Leopard, Mountain Lion, Mavericks ... ter Microsoftov Windows z različicami Windows XP, Vista, 7, 8 ...).

Vsaka različica teh zaprtokodnih operacijskih sistemov temelji na drugačnem jedru, s čimer se zmanjša prenosljivost zlonamerne programske opreme med njimi. Vendar pa ima zlonamerna programska oprema, ki je pisana za zaprtokodne sisteme, zaradi majhnega števila različic in monokulturnosti Microsoftovih operacijskih sistemov, veliko večjo moč razširjanja. Različice se sicer spremenijo redkeje, kot je to na odprtokodnih operacijskih sistemih, prav tako je zaradi razlik v kodi manjša verjetnost, da bi zlonamerna programska oprema okužila več distribucij (Espiner 2006). Z vidika informacijske varnosti je veliko število distribucij, ki je značilno za OKPO, torej prednost.

3.2 Zlonamerna programska oprema

Pod izraz zlonamerna programska oprema razumemo (Malware ang.) programsko opremo, ki se želi infiltrirati ali poškodovati računalniški sistem, ne da bi pri tem uporabnik privolil v to (vključuje računalniške viruse, črve, trojanske konje in vohunsko opremo ipd.) (Malware 2014). Zlonamerna programska oprema je pisana za točno določen operacijski sistem in njegovo različico, saj se izvorna koda med različicami razlikuje. Število zlonamerne programske opreme, ki je pisano za zaprtokodne in odprtokodne sisteme, je zelo različno. Do danes poznamo preko 127 milijona primerov zlonamerne programske opreme, pri čemer zabeležijo dnevno 74.000 novih primerov (PandaLabs Annual Report 2012 2012). Od tega je največ zlonamerne programske opreme pisane za operacijske sisteme Windows 24 milijonov (Virus Definitions & Security Updates 2014), 5393 primerov zlonamerne programske opreme za Linux operacijske sisteme (Linux malware detect 2014) in 130 primerov za Apple Mac OS X (Kaspersky Security Bulletin 2012 2012). Število zlonamerne programske opreme je v zadnjih letih zelo naraslo, tako na odprtokodnih kot zaprtokodnih operacijskih sistemih. Zadnja poročila Kaspersky inštituta ugotavljajo, da se je število povečalo, predvsem zaradi vedno večje priljubljenosti obeh operacijskih sistemov (Linux in Mac OS x) (Kapersky security bulletin 2013 2013). Največ „zaslug“ za novo število zlonamerne programske opreme na področju Linux operacijskih sistemov ima Googlov Android, ki je mobilni odprtokodni operacijski sistem, temelječ na Linux jedru (Kapersky security bulletin 2013 2013). Zaradi vedno večje priljubljenosti Android mobilnih naprav, je posledično tudi vedno več zlonamerne programske opreme (Kapersky security bulletin 2013 2013). Poročilo iz 2007 ugotavlja, da je od Unixu-podobnih operacijskih sistemov najbolj na udaru Linux, ki je tudi najbolj razširjen od vseh odprtokodnih operacijskih sistemov na svetu. Vendar statistike kažejo, da je bil Linux napaden predvsem na področjih strežnikov in ne toliko na področju namiznih računalnikov (Sapronov 2007). Večina strežnikov namreč deluje na Linux-u (Germain 2008).

Kljub temu, da do danes poznamo 5393 primerov zlonamerne programske opreme za OKPO, je življenjska doba te zlonamerne programske opreme zelo kratka in v praksi ne naredi toliko škode, kot jo lahko naredi na Windows operacijskem sistemu. Razlog tiči v administratorskem dostopu (superuser account – bolj znan kot ROOT,

do katerega lahko na Linux in ostalih Unix-podobnih sistemih dostopamo preko ukaza „sudo“- super user do), ki je v Linux, BSD in ostalih Unixu-podobnih operacijskih sistemih avtomatično deaktiviran, iz varnostnih razlogov, da ne bi nevešči uporabniki upravljali s sistemom in ga potencialno pokvarili. (RootSudo 2014). V praksi to pomeni, da si določimo geslo, s katerim nam je omogočeno spreminjanje vseh nastavitev v operacijskem sistemu, vključno z nameščanjem in odstranjevanjem programov. Brez tega gesla v sistemu ne moremo spreminjati skorajda ničesar. Drugače je na operacijskih sistemih Windows. Windows ni poznal prave blokade administratorskega dostopa z geslom, vse do različice Vista in 7, ki pa še vedno ni tako striktna, saj lahko uporabniki v sistemu spremenijo veliko stvari brez administratorskga dostopa (Schneier 2006). Applov operacijski sistem Mac OS X temelji na Unix jedru, kjer je administratorski dostop vnaprej onemogočen in od uporabnika zahteva geslo, podobno, kot Linux, kar je dobra lastnost. (Enabling and using the "root" user in Mac OS X 2014). V primeru okužbe z zlonamerno programsko opremo na Linuxu sistemu škoda ne bo velika, saj zlonamerna programska oprema ne bo imela administratorskega dostopa za celoten sistem; njen efekt bo lokaliziran ali pa ga sploh ne bo (Koetzle 2004; The short life and hard times of a Linux virus 2005). Podobno je bilo ugotovljeno v raziskavi Analysis of the Impact of Open Source Software iz leta 2001 (Peeling in Satchell 2001), kjer so proučevali vpliv virusov na različne operacijske sisteme. Windows je imel takrat preko 60.000 virusov, Mac OS X 40 in Linux 40. Kljub temu da večina virusov, pisanih za Windows, ni naredila velike škode, je več sto virusov povzročilo velikansko škodo. Dve tretjini virusov je naredilo veliko škodo Applovemu Mac OS X sistemu, medtem ko niti eden od Linux virusov ni povzročil večje škode oz. se ni bolj razširil po sistemu (Peeling in Satchell 2001). Varnost Unixu podobnih operacijskih sistemov, lahko kljub temu močno ogrozi tako imenovani korenski komplet (angl. *rootkit*), ki omogoča prikrit dostop do računalniškega sistema in nepooblaščeno uporabo administratorskih pravic (Chuvakin 2003).

Kot vidimo, ni tako pomembno, koliko zlonamerne programske opreme obstaja za nek operacijski sistem, pomembneje je kako široko in na kakšni ravni lahko prizadene sistem. Microsoft je po zgledu odprtokodnih operacijskih sistemov v različicah Vista in 7 onemogočil administratorski dostop in s tem izboljšal varnost sistema.

3.3 Ali »veliko oči« res več vidi?

Sistem „veliko oči“ (angl. many eyes) je sistem pregleda, kjer lahko v teoriji vsak uporabnik pogleda izvorno kodo OKPO – s tem je zmanjšana možnost, da bi OKPO vsebovala zlonamerno kodo, kot so stranska vrata, preko katerih lahko nepooblaščena oseba dobi dostop do našega sistema.

Zagovorniki OKPO velikokrat uporabljajo argument, da sistem „veliko oči“ omogoča hitro detekcijo hroščev v kodi. V praksi ni povsem tako. Večina uporabnikov danes ni veščih programiranja, izvorne kode ne znajo brati ali v njej prepoznati pomanjkljivosti in potencialnih stranskih vrat. Večina uporabnikov uporablja OKPO za vsakodnevna opravila, kot so pisanje besedil, urejanje preglednic, pisanje spletne pošte ... Še vedno pa OKPO omogoča vpogled tistim, ki jih to zanima in so tega sposobni. To je pomembna razlika, saj zaprtokodni sistemi tega ne omogočajo (Laurie 2006, 60). V zgodovini je bilo več primerov, da več let niso odkrili ranljivosti, čeprav je OKPO pregledalo več ljudi. Eden zanimivejših primerov so stranska vrata Kena Thompsona, ki je bil razvijalec sistema Unix, v katerega je stranska vrata vnesel sam. Šele po 14 letih je Thompson to razkril. S tem malim eksperimentom je želel pokazati, da se na druge ljudi ne smemo preveč zanašati. Po njegovem mnenju je varna samo tista koda, ki jo napišemo sami (O’Dowd 2004). Tu se nam poraja vprašanje o človeškem dejavniku. Če je kodo pregledalo veliko ljudi, to še ne pomeni, da je bil pregled tudi dovolj natančen ali da so pregledovalci kompetentni za odkritje vseh ranljivosti.

3.4 Čas za popravek

Čas za popravek je čas med tem, ko zaznamo ranljivost v kodi in časom, ko se naredi popravek. Ta čas je izjemno pomemben in mora biti čim krajši - dlje ko je ranljivost brez popravka, dlje časa je varnost sistema ogrožena. Raziskava primerjave varnosti pri operacijskih sistemih Windows in različnih Linux distribucijah (Debian, Red Hat, Mandark) tekom obdobja enega leta je beležila število zaznanih nevarnosti, časa ki je bil potreben za izdelavo popravka in število popravljenih nevarnosti (Koetzle 2004). Windows je za izdelavo popravkov v povprečju potreboval najmanj časa – 25 dni, sledile so mu Linux distribucije Red Hat in Debian s 57 in Mandark z 82 dnevi.

Zgolj ta podatek pa za primerjavo varnosti operacijskih sistemov ne zadostuje: pri Windowsih so našteli največ nevarnosti najvišje stopnje (67% vseh nevarnosti), sledil je Red Hat s 56% nevarnosti iste stopnje. Raziskava je merila tudi čas, ki je potreben, da popravke vnesejo v distribucijo ponudniki distribucij. Pri OS Windows je bil ta čas identičen izdelavi popravkov, saj distribucije sistemov Windows ne obstajajo. Debian je v povprečju potreboval zgolj 32 dni, kar je veliko manj od časa, ki ga je potreboval za izdelavo popravkov (57 dni), prav tako Red Hat s 47 dnevi. Debian je imel tako dober čas, ker je bil edina proučevana distribucija, ki se posodablja, ne da bi bila potrebna ponovna namestitev celotnega sistema (angl. rolling release); ko jo enkrat namestimo, je ni nikoli več potrebno nameščati, saj se celoten sistem posodablja avtomatično, skupaj z vsemi nameščenimi programi. Zanimivost se je pokazala tudi na področju Microsofta. Za varnost ni pomemben samo čas za izdelavo popravkov, predvsem so pomembni uporabniki, ki si morajo te popravke namestiti. Uporabnike Microsofta je ogrožalo devet ranljivosti najvišje stopnje, vendar večina proučevanih uporabnikov kljub temu več kot 305 dni popravkov ni namestila. To pomeni, da so bili potencialno v povprečju ogroženi 305 dni, kljub temu, da je Microsoft v povprečju izdelal popravke že po 25 dneh (Koetzle 2004). Podatek lahko implicira nižjo računalniško pismenost uporabnikov operacijskega sistema Windows v primerjavi z uporabniki Linuxa.

Če ljudje preko sistema „veliko oči“ v OKPO odkrijejo ranljivost, to nemudoma transparentno objavijo na posebnih spletnih straneh in forumih ipd. (zelo znana taka stran Linux distribucije Ubuntu je Ubuntu Bugs Launchpad (Bugs: Ubuntu 2014). Razvijalci OKPO ranljivost nato v najkrajšem možnem času odpravijo. Seveda obstajajo razlike med razvijalci različnih OKPO. Apache v povprečju izdaja popravke dnevno, tako da ranljivost redko traja dlje od enega dneva. Ubuntu, ki je najbolj razširjena Linux distribucija operacijskega sistema, popravke izdaja glede na prioritete, ki se jih določi preko Ubuntu Bug Launchpad. Ponudniki distribucij odprtokodnih operacijskih sistemov navadno malce zaostajajo za samimi razvijalci. Tako na primer profesionalni odprtokodni program za 3D animacijo Blender (Blender 2014) na svoji spletni strani ponuja različico 2.69, medtem ko uporabniki Ubuntu operacijskega sistema preko Programskega središča Ubuntu lahko namestijo Blender različico 2.66a. Ponudniki svojih baz torej ne osvežujejo skladno z vsakodnevnim razvojem OKPO. To pomanjkljivost odpravlja sistem Skladišče programske opreme (angl. repository), ki uporabnikom omogoča, da najnovejšo različico programa namesti neodvisno od ponudnikov distribucije in v trenutku, ko jo razvijalec objavi. Skladišče programske opreme je bilo narejeno z namenom hitrejšega posredovanja najnovejše različice programske opreme uporabnikom ter hitrejši pridobitvi povratne informacije o kakovosti programske opreme, ki nemudoma pride do razvijalca. Posledično se pospeši razvoj programske opreme (Laurie 2006, 62–64). Leta 2007 je Ubuntu izdal programsko opremo Personal Package Archive (PPA) z namenom, da bi še pospešili in olajšali distribucijo programske opreme preko skladišč programske opreme (Humphrey 2011). Ni nujno, da so vsa skladišča programske opreme varna, saj si dodamo lahko skladišče, ki vsebuje zlonamerno programsko operemo. Zato je priporočeno, da se dodajajo samo skladišča, ki so preverjena in niso „sumljivega porekla“.

Zaprtokodna operacijska sistema Windows in Mac OS nimata sistema "veliko oči", temveč za varnost skrbijo razvijalci obeh sistemov. Vseh ranljivosti ne objavljajo javno, zato tudi ne vemo, kako dolgo smo dovzetni zanje in kakšno je njihovo dejansko število. Kot vidimo, večje število javno objavljenih nevarnosti še ne pomeni bolj ranljivega sistema, temveč bolj transparentnega. OKPO je s tem v prednosti, saj pri zaprtih sistemih za vse varnostne ranljivosti zaradi netransparentnosti sistema ne moremo vedeti.

3.5 Varnost s transparentnostjo?

Velikokrat slišimo, da skrivanje izvorne kode pelje v večjo varnost, vendar to v praksi ne drži. Že eden prvih kriptologov, Auguste Kerckhoffs, je davnega leta 1883 napisal šest načel dobre kriptografije, kar danes imenujemo Kerckhoffsov zakon; ta pravi, da je dober šifrirni sistem varen, tudi če o njem vemo vse razen šifrirnega ključa. Kerckhoffs prav tako zavrača načelo, da je varnost mogoče zagotoviti s skrivanjem; ne zahteva da je šifrirni sistem javen, vendar opozarja, da skrivnost ne zagotavlja večje varnosti, ampak jo celo ogroža (Kovačič 2006, 93–112). Skrit sistem lahko ogroža varnost tako, da lahko vsebuje napake, ki bi jih, če bi bil javen, lahko odkrili in popravili. Eden največjih strokovnjakov za informacijsko varnost in kriptolog Bruce Schneier pravi: „Ne spominjam se nobenega kriptografskega sistema, razvitega na skrivaj, v katerem ne bi, potem ko je bil razkrit javnosti, kriptografska skupnost našla napake“ (Schneier 2002). Podobno se je zgodilo z zelo znanim primerom podatkovne baze Borland InterBase, v kateri so leta 2000 odkrili stranska vrata (angl. backdoor). Ko je podjetje propadlo je objavilo izvorno kodo programske opreme, ki je bila pred tem bila lastniška oz. zaprta koda. Programerji so ugotovili, da so bila podatkovni bazi leta 1994 namerno dodana stranska vrata in so vse do leta 2001 posamezniku omogočala popoln dostop do vseh podatkov in tudi vrinjanje podatkov in vsebin z uporabniškim imenom „politically“ in geslom „correct“. Še bolj zaskrbljujoče je, da so podatkovno bazo uporabljale bostonska borza ter velike korporacije, kot so Motorola, Nokia in Boeing. Na srečo so odprtokodni programerji zelo hitro naredili popravek, ki je stranska vrata zaprl (Poulsen 2001).

V duhu odprte kode tudi Microsoft danes državam omogoča dostop do izvorne kode – a le pod pogoji, ki so napisani v pogodbi Government Security Program. V njej najdemo približno 60 držav, med njimi tudi države Nata, Kitajsko in rusko tajno službo FSB (Espiner 2010). Vendar je Microsoft tisti, ki določi, ali bo državi razkril izvorno kodo ali ne. Med državami, ki jim Microsoft ne omogoča vpogleda, najdemo Venezuelo, Kubo in druge države, ki so prešle na odprto kodo v javni upravi. Nekateri strokovnjaki opozarjajo na slabost takšnega sistema. Richard Clayton z univerze Cambridge opozarja, da države tako lažje najdejo varnostne ranljivosti, ki jih lahko izrabijo za napad na druge države, saj podatka o ranljivosti ne objavijo javno, zanjo vedo le tiste znotraj sistema, ki imajo dostop do izvorne kode. Government Security

Program ima tudi to omejitev, da državam omogoča vpogled v izvorno kodo, ne omogoča pa njenega spreminjanja (Shared Source Initiative 2013).

4 Prehod javnih uprav na odprto kodo

V zadnjem času beležimo vedno več držav, ki se odločajo za prehod na OKPO. Nekatere države le delno prehajajo na OKPO, in uporabljajo zgolj odprtokodno programje, kot so Libre Office ali Open Office namesto Microsoft Office. Vedno več je držav, ki so se odločile za popoln prehod na OKPO, kar pomeni, da uporabljajo distribucije Linux ali BSD operacijskih sistemov, skupaj s pripadajočo programsko opremo. Večina držav, ki so se odločile za popoln prehod, so ustvarile lastne državne distribucije operacijskih sistemov, ki vsebujejo točno določeno programsko opremo (tisto, ki jo v specifični javni upravi potrebujejo). Te države so zaradi zagotavljanja večje varnosti naredile lastna skladišča programske opreme, ki jih posodabljajo njihove državne institucije in vsebuje programsko opremo, ki je bila razvita posebej za potrebe državnih institucij. S tem države zagotovijo večjo varnost operacijskih sistemov, saj je programska oprema, ki se nahaja v skladiščih, pregledana. Varnost je poleg zmanjšanja stroškov eden glavnih razlogov za prehod državnih javnih uprav na OKPO (Lewis 2006). Nemško mesto München se je odločilo, da bo prihranilo z zamenjavo zaportokodne programske opreme z OKPO. Odločitev, da bodo zamenjali na vseh računalnikih programsko opremo Microsoft Windows Xp z OKPO so sprejeli pred desetimi leti. Na računalnike so namestili lastno distribucijo LiMux temelječo na Ubunti Linux. Decembra 2013 so javnosti uradno naznanili, da je prehod na OKPO končan. Njihove ocene kažejo, da so z prehodom prihranili 11,7 milijona evrov, kolikor bi sicer morali nameniti za licenčnine Microsoft Windows. Vendar se za prehod niso odločili samo iz ekonomskih razlogov. Želeli so biti bolj neodvisni in si prilagajati sistem po lastnih željah in potrebah (Essers 2013).

Ko so leta 1999 prišla v javnost prva poročila, da naj bi ameriška agencija NSA vnesla stranska vrata v vsako kopijo operacijskega sistema Windows 95 (Campbell 1999), so se države zamislile nad varnostjo in nadzorom pri operacijskih sistemih podjetja Microsoft. Zmotile so jih tudi monokulturne monopolistične tendence Microsofta, ki obvladuje več kot 65 odstotkov tržnega deleža na področju namiznih računalnikov. Zaradi tako velikega tržnega deleža ima zlonamerna programska oprema tudi veliko večje možnosti za širitev in uničenje sistema. Microsoft je poleg tega začel kodo dopolnjevati tako, da je omejevala delovanje na drugih sistemih in s tem države „priklenil“ nase (angl. *vendor lock-in*). To je spodbudilo razmišljanje o alternativnih programskih rešitvah, ki bi državam omogočile večji nadzor nad računalniškimi sistemi in večjo transparentnost, večjo neodvisnost od Microsofta in možnost razvoja ter prilagajanja sistema svojim potrebam (Geer in drugi 2003). Mnoge so rešitev našle v OKPO.

V Venezueli so razvili lasten operacijski sistem imenovan Canaima, ki temelji na Debian Linux distribuciji. Državni dekret številka 3.390 (Decreto N° 3.390 2004), veleva uporabo Canaime v javni upravi, prav tako mora biti vsaka posebej razvita programska oprema za potrebe javne uprave licencirana pod licenco GPL (torej mora biti odprtokodna) (Cleto 2004). Hugo Chavez se je za prehod na OKPO (poleg varnosti) odločil tudi zaradi podatka, da gre 75% cene licenčne programske opreme v druge države, 20% gre za podporo tujih agencij in samo 5% ostane venezuelskim programerjem (Proffitt 2002). Podobne razloge kot Venezuela so imele za prehod še Kuba, katere lastna distribucija operacijskega sistema Nova temelji na Linux distribuciji Ubuntu. Kuba se je za prehod na OKPO v prvi vrsti odločila zaradi varnosti, poleg tega pa tudi zaradi ameriškega embarga, ki posledično pomeni, da je bilo na Kubi zelo težko priti do legalnih Windows operacijskih sistemov. Razlog je tudi v ideologiji; dekan Šole za prosto programje na kubanski Univerzi za informacijske znanosti Hector Rodriguez je dejal: „Gibanje prostega programja je bliže ideologiji kubanskega prebivalstva, predvsem zaradi neodvisnost in suverenosti“ (Israel 2009). Tudi Rusija se je odločila za prehod na OKPO, vendar njen prehod še poteka in se bo končal leta 2015. Kot glavni razlog je Putin navedel željo po večji neodvisnosti od drugih držav pri uporabi lastniške programske opreme (Morozov 2011).

Ena bolj zanimivih držav z vidika prehoda na OKPO je Kitajska, ki se je začela za OKPO zelo zanimati že leta 1990, leta 2005 pa je izdelala prvo različico državnega

operacijskega sistema Linux distribucije Red Flag Linux, (kasneje ga nadomesti UbuntuKylin) ki se ga uporablja v javni upravi. Vzporedno so razvili distribucijo Asianux, ki je usmerjen na azijske trge, saj podpira pismenke (Blanchard 2007, 67–102). Kitajska, katere gospodarstvo hitro raste, z njim pa tudi potrebe po čim bolj lokalizirani programski opremi, ki najbolj zadovolji potrebe lokalnih podjetij, z razvojem lastne programske opreme postaja konkurenčna na svetovnih trgih (Saxenian 2003; Holt 2013). Kitajska je imela nekdaj eno najvišjih stopenj piratizacije na svetu, z uporabo OKPO pa se je začela stopnja piratizacije manjšati. Tudi na Kitajskem želijo z uporabo OKPO zagotoviti tudi večjo informacijsko varnost in neodvisnost (Boon-Lock in drugi 2006 197–210).

Evropska unija velja za eno največjih zagovornic uporabe OKPO. Največji odprtokodni projekti in rešitve so nastali na tleh Evropske unije. Linux je naredil Finec Linus Torvalds, Python programski jezik je delo Nizozemskega avtorja Guida van Rassuma, MySQL sistem upravljanja podatkovnih baz je naredil Šved Michael Widenius in še bi lahko naštevali (Gonzalez-Barahona in Robles 2006, 163). Evropska unija zelo podpira razvoj OKPO, zato so ustanovili institucijo The Open Source Observatory and Repository for European public administrations (OSOR), katere namen je razvijati posebne aplikacije in odprtokodno programsko opremo, namenjeno uporabi v javni upravi znotraj EU. S projektom želijo zmanjšati stroške v javni upravi, standardizirati formate in postopke povsod po Evropski uniji, zmanjšati stroške e-vlade (angl. e-government) in pomagati širiti dobro prakso v javni upravi. OSOR je financiran s strani Evropske komisije in podprt s strani vlad na nacionalni, regionalni in lokalni ravni (Open source observatory 2010).

Na kratko še poglejmo, kje pri uporabi OKPO v javni upravi je Slovenija. Leta 2003 je država sprejela dokument Politika Vlade RS pri razvijanju, uvajanju in uporabi programske opreme in rešitev, temelječih na odprti kodi. Znotraj dokumenta lahko preberemo, da bo država podpirala uporabo odprtokodnih rešitev, jih enakopravno obravnavala skupaj z licenčnimi in podpirala izobraževanja o njeni uporabi (Politika Vlade RS pri razvijanju, uvajanju in uporabi programske opreme in rešitev, temelječih na odprti kodi 2003). Dokument se zaenkrat še ni prenesel v prakso. Do 2011 je država na podlagi raziskave Ocena ekonomske upravičenosti MS EA za obdobje 2003-2005 (Ocena ekonomske upravičenosti MS EA za obdobje 2003-2005 2002), ki je ugotavljala, da je licenčna programska oprema finančno bolj smotrna od OKPO zato je preko javnih naročil za potrebe javne uprave kupovala licenčno programsko

opremo MS Office. Pri tem v javni upravi obstajajo svetle izjeme, kot so slovenska sodišča. Če pogledamo primer Vrhovnega sodišča RS, kjer so med leti 2006 - 2007 izvedli prehod in zamenjali pisarniški paket MS Office z Open Office, Microsoftov spletni brskalnik Internet Explorer z Mozilla Firefox in namestili odprtokodno aplikacijo za spletno pošto Thunderbird na 4600 delovnih postaj. Vrhovno sodišče RS ugotavlja, da na leto na ta način prihrani okoli 400.000€ (Sodišča z odprto kodo prihranijo 400 tisoč evrov letno 2011).

Leto 2011 je bilo na tem področju v Sloveniji prelomno, saj je v začetku leta država objavila študijo, s katero izraža namero, da bi do leta 2015 postopoma prešla na uporabo OKPO; sprva zgolj z z menjavo MS Office z Open Office, sčasoma pa bi morda zamenjali celotne operacijske sisteme z odprtokodnimi, kot so Linux distribucije (Študija uvajanja odprtokodne programske opreme (OKPO) na delovnih postajajh v javni upravi 2011). Študija je sprožila velik plaz kritik predvsem s strani ponudnikov licenčnih programskih rešitev; Microsoft je izjavil, da bi mu takšna odločitev vlade letno prinesla vsaj 2.5 milijona evrov izgube (Mihajlovič 2011).

Slovenija je v primerjavi z drugimi državami EU na področju implementacije in uporabe OKPO precej zaostala. Vendar je potrebno na tem mestu izpostaviti tudi potencialno problematiko v primeru prehoda slovenske državne javne uprave na OKPO. Problematične so aplikacije, narejene posebej za uporabo v javni upravi – izdelane so namreč le za Microsoft okolje. Do podobnih težav so prišli tudi v ostalih državah, saj so morali aplikacije, ki so bile posebej izdelane za Microsoft okolje in programe ponovno izdelovati ali pa spremeniti in omogočiti podporo tudi na drugih operacijskih sistemih in kompatibilnost z drugačnimi formati, kar je prineslo povečanje stroškov (Souza 2006, 211–228).

Znani so primeri prehodov z OKPO nazaj na zaprtokodno programsko opremo. Zadnji tak prehod je naredilo nemško zunanje ministrstvo, ki je leta 2005 prešlo na OKPO. Na namizne računalnike so namestili distribucijo Debian Linux. S prehodom so želeli prihraniti denar, ki bi sicer šel za licenčnine. Leta 2007 so v poročilu zapisali, da so s prehodom resnično znižali stroške. Leta 2011 pa so javno najavili, da prehajajo nazaj na MS Windows in MS Office. Kot razlog so navedli pomanjkljivo podporo strojni opremi, kot so tiskalniki in podobno. Stroški se po njihovem mnenju niso zmanjšali, saj so morali veliko denarja vložiti v razvoj lastnih gonilnikov za tiskalnike. Prav tako so se uporabniki pritoževali nad pomanjkanjem funkcij in slabo interoperabilnostjo. Prehod nazaj na MS Windows jih bo po njihovem mnenju stal

manj, ker jim ne bo treba plačevati programerjev za razvoj gonilnikov (No more desktop Linux systems in the German Foreign Office 2011*).*

5 Vojna in kibernetski prostor

Svet je vedno bolj globalno povezan s pomočjo interneta in računalnikov. Prednost interneta je predvsem v hitrejšem pretoku in dostopu do informacij, vendar pa imata splet in svetovna povezanost tudi svojo veliko slabost – kibernetske grožnje (kibernetski kriminal, kibernetski terorizem in kibernetsko bojevanje), ki so v vedno večjem vzponu. Kibernetski kriminal je vsako kriminalno dejanje, kjer je računalnik ali omrežje del kriminalnih dejanj, kot so nepooblaščeno vdiranje v sisteme, razširjanje zlonamerne programske opreme, kraja identitete, zavajanje ipd. (Brvar 1982, 94). Ocenjena vrednost škode, ki jo povzroči kibernetski kriminal iz leta v leto dosega večje številke. Ocenjena vrednost izgube, ki jo prinese kibernetski kriminal naj bi predstavljala približno 1% BDP (bruto domačega proizvoda), kar se na svetovni ravni ocenjuje v rednosti 400 milijard dolarjev (The Economic Impact of Cybercrime and Cyber Espionage 2013).

Tako kot se klasičen kriminal razvija z leti, se tudi kibernetski kriminal danes. Nekoč so ropali banke fizično, danes to storijo preko računalnika, ne da bi sploh prestopili prag banke. Vendar je ena velika razlika med obema oblikama kriminala. S kibernetskim kriminalom veliko lažje pridejo kriminalci do veliko večjih zneskov, kot so to počeli nekoč, ko je bilo potrebno denar fizično nositi ven iz banke (Schneier 2013).

Obstaja več vzrokov za porast spletnega kriminala. Prvi razlog je skokovita rast uporabnikov interneta v zadnjem desetletju. Leta 2000 je bilo na svetu 361 milijonov uporabnikov interneta, leta 2010 pa je ta številka že dosegla 2,4 milijardi uporabnikov. Na svetu je trenutno malo več kot 7 milijard ljudi (Internet World Stats 2014), kar predstavlja skoraj tretjina vsega svetovnega prebivalstva. Drugi vzrok je hiter razvoj in popularizacija novih tehnologij, kot so tablice in pametni telefoni, ki so z uporabo uporabniku bolj prijaznih rešitev in grafičnega vmesnika poenostavile njihovo uporabo in jo s tem naredile bolj priljubljeno. Njihovo priljubljenost izkoriščajo spletni kriminalci z razvojem zlonamerne programske opreme, pisane posebej za

zgoraj naštete produkte (Schneier 2013). Vendar pa so krivci za porast kriminala tudi uporabniki sami. Raziskava NCSA iz leta 2010 je pokazala, da je zgolj 58 odstotkov vprašanih dejalo, da imajo polno zavarovan računalnik s protivirusnimi programi. Po dejanskem pregledu njihovih računalnikov so raziskovalci ugotovili, da je resnično zavarovanih zgolj 37 odstotkov. Leta 2009 je v ZDA 545.000 tisoč gospodinjstev zamenjalo računalnik z novim, po manj kot šestih mesecih, ko so se okužili z zlonamerno programsko opremo (NCSA study 2010). To kaže na dejstvo, da so uporabniki interneta še vedno premalo informirani in poučeni o varnosti njegove uporabe. (McAfee A good decade of Cybercriminal 2010, 8).

Ravno tako je vedno več primerov kibernetskega terorizma, kjer gre za protizakonite napade na računalnike, informacijska omrežja in informacije z namenom prizadetja vlade ali njenega ljudstva. V ozadju napada so lahko politični ali družbeni cilji. Napad mora biti nasilne narave zoper osebo ali lastnino in mora povzročiti dovolj škode, da povzroči strah (Weimann 2004; Theohary in Rollins 2011).

Vendar pa ni samo posameznik tisti, ki je lahko ogrožen preko spleta. Pojavlja se vedno več primerov tako imenovanega, kibernetskega bojevanja, ko države napadajo druga drugo preko interneta. V porastu je tudi spletni »hacktivizem«, kjer gre za politično angažiranje hekerjev z namenom podpore določeni skupini, kot je Wikileaks (Weimann 2004; Pandey 2010). Še bolj zaskrbljujoče je, da vedno več držav trdi, da so bile napadene s strani druge države ali drugih držav, kar poimenujemo kibernetsko bojevanje. Kibernetsko bojevanje je namerno napadanje neke države ali državne infrastrukture s podporo države ali s strani druge z uporabo informacijske tehnologije z namenom uničenja informacij, računalniškega omrežja, kritične infrastruktur ipd. (Cornish in drugi 2010; Krepinevich 2012;).

5.1 Kibernetske vojne

Koncept kibernetskih vojn je bi prvič predstavljen v članku Johna Arquille in Davida Ronfeldta Cyberwar is coming! leta 1993. (Domingo 2012). V članku sta avtorja predstavila kibernetsko vojno, kot neko novo obliko bojevanja, kjer lahko pride do uničenja informacij in komunikacijskih sistemov. Ravno tako sta menila, da bo z razvojem novih tehnologij in rastjo uporabe informacijske tehnologije, ta način bojevanja sčasoma postal dominanten in utegne povzročati vedno več konfliktov (Arquilla in Ronfeldt 1993). Koncept kibernetske vojne pa je našel tudi svoje kritike in podpornike, zato bom v nadaljevanju predstavila ključne ideje zagovornikov teorije kibernetske vojne in njene kritike.

5.1.1 Zagovorniki

Arquilla in Ronfeldt sta menila, da se kibernetska vojna že dogaja in da postaja vedno bolj kompleksna z razvojem informacijske tehnologije, hkrati pa postaja vedno bolj uničujoča. Menita, da bo ta trend viden tudi v prihodnje. Kot prvo potencialno kibernetsko vojno omenjata gruzijsko-ruski konflikt leta 2008 (Arquilla 2012). Njuno tezo potrjuje tudi Dorothy Denning, ki meni da je prihodnost bojevanja ravno v informacijskem bojevanju vključujoč tudi vse svoje oblike: vohunjenje, psihološko bojevanje, elektronsko bojevanje... (Denning 2012). Mnogi analitiki menijo, da ZDA preti kibernetska vojna in zato pozivajo k sprejetju ustreznih pravnih aktov, ki bi omogočili učinkovito obrambo oz. bojevanje, kot na primer »Pogodba o omejitvah kibernetske vojne« (ang. Cyber war limitation treaty) (Rattaray 2001). Rattaray meni, da mora biti uporaba fizično nenasilnih digitalnih napadov za dosego političnih ciljev razumljena, kot nova oblika vojskovanja (Rattaray 2001). Gray pa ugotavlja, da je kibernetsko bojevanje v resnici bojevanje za informacije. Kibernetske boje poimenuje, kot boje brez krvi v kibernetskem prostoru z namenom pridobitve informacij ali onemogočanje dostopa do informacij (Gray 2005).

5.1.2 Kritiki

Na drugi strani pa imamo kritike koncepta kibernetskega bojevanja, ki menijo da je sam koncept velikokrat prenapihnjen. Eden glavnih kritikov je Libicki, ki meni da kibernetski napadi ne morejo narediti toliko škode, kot se prikazuje v medijih. Po njegovo so tudi posledice velikokrat prenapihnjene in senzacionalistične (threat inflation ang.)(Libicki 2007). Ravno tako opozarja na pomanjkljivosti kibernetskega bojevanja. Meni, da koncept premalo definira načrt obrambe ali napada, kot je to omogočeno v konvencionalnih vojnah (Libicki 2012). Rid na drugi strani opozarja, da kibernetski napadi ne zadoščajo Clausewitzevi definiciji vojne (Vojna je nadaljevanje politike z drugimi sredstvi. Vojna je dejanje nasilja, katerega namen je prisiliti nasprotnika, da izvrši naše želje. (Clausewitz 1985)). V kibernetskih vojnah ni uporabljena fizična sila za dosego ciljev, lahko pa je politično motivirana, zato po njegovo kibernetske vojne ne obstajajo in tudi v prihodnje ne bodo (Rid 2012). Schneiner ugotavlja, da je koncept kibernetskih vojn zelo senzacionalistično predstavljen z željo po pridobitvi čim večje pristojnosti vladnih agencij ZDA nad kibernetskim prostorom (Schneiner 2010). Ker se z kibernetskim bojevanjem vedno bolj ukvarja tudi Ministrstvo za obrambo ZDA in NSA, se je tudi sam koncept kibernetskega bojevanja posledično vedno bolj militariziral in je tudi vedno bolj v domeni vojske (Domingo 2012).

Ena glavnih kritik za obstoj kibernetskih vojn je sama definicija. Kot vidimo, ne obstaja niti ena skupna definicija, ki povzema ta pojem. Problematično je tudi, ker ne zadosti klasičnim definicijam vojne. Če na kratko pogledamo lastnosti kibernetskega bojevanja bomo kaj hitro videli, da se zelo razlikuje od konvencionalnega bojevanja. Cornish in Livingstone, ki sta v svojem delu »O kibernetskem bojevanju« (Cornish in drugi 2010) primerjala klasično definicijo Carla Von Clausewitza s kibernetskim bojevanjem sta v svoji analizi ugotovila naslednje:

- kibernetsko bojevanje je ena najbolj resnih groženj kibernetske varnosti v kibernetskem prostoru.
- Ravno tako, kot konvencionalni pri napadih, se lahko tudi tukaj uporablja sredstva za napad na ustroj države, finančne institucije, energetsko infrastrukturo, javni transport, javno mnenje in moralo.

- Vendar tudi če nekatera dejanja delujejo napadalno in agresivno, še niso nujno tudi vojno dejanje.
- Nujno je potrebno ločiti med kibernetskimi napadi in kibernetskimi napadi, ki bi lahko bili vojno dejanje (npr. neko kibernetsko dejanje teroristične skupine je lahko uničujoče za prizadeto stran vendar to dejanje ni nujno vojno dejanje).
- Kibernetsko bojevanje je tip asimetričnega bojevanja, kjer je lahko ena stran šibka v konvencionalnem načinu bojevanja, vendar je zelo agilna in se lahko hitro prilagaja situacijam. Medtem ko je lahko druga stran močna, vendar okorna. Zato je kibernetsko bojevanje zelo hitro se spreminjajoča oblika bojevanja.
- Kibernetsko bojevanje je lahko del konflikta med državami, lahko pa poteka tudi med nedržavnimi akterji. Težko je določljiv njegov efekt oz. težko identificiramo kdo ali kaj je fokus napada (npr. lahko je napaden celoten strežnik, ki gosti neko spletno stran, ki je dejanska tarča napada. Posledica je, da so s tem napadom prizadeti tudi ostali uporabniki tega strežnika).
- Kibernetsko bojevanje omogoča dosego političnih in strateških ciljev, brez uporabe konvencionalnega orožja.
- Kibernetski prostor daje moč majhnim in sicer nepomembnim akterjem v samem konfliktu (nesorazmernost moči).
- Ravno tako omogoča, da se lahko napadalec skriva za lažnimi IP naslovi, strežniki in na ta način deluje skoraj anonimno.
- Meje so zabrisane v kibernetskem svetu. Napadalec je lahko država, oz. nekdo, ki deluje v imenu države ali celo nekdo, ki je povsem neodvisen. Zato je tudi zabrisana meja med civilnim in vojaškim.
- Kibernetski prostor se mora obravnavati kot »peta dimenzija vojskovanja« (poleg nje poznamo še zrak, morje, kopno in vesolje).
- Kibernetski prostor je »terra nullus« saj ne pripada nikomur. Zato je toliko bolj privlačen za doseganje različnih ciljev. Načelo nevtralnosti interneta je žgoča tema v ZDA, kjer je ameriško sodišče odločilo, da lahko internetni ponudniki omejujejo dostop in pretok informacij (Kravets 2014). Slovenija je na tem področju pred ZDA saj je nevtralnost interneta uzakonila z zakonom Zakona o elektronskih komunikacijah (ZEKom-1), kjer piše: »Operaterji omrežij in izvajalci storitev dostopa do interneta si kar najbolj prizadevajo za ohranitev

odprtega in nevtralnega značaja interneta, s tem da ne smejo omejevati, zadrževati ali upočasnjevati internetnega prometa na ravni posameznih storitev ali aplikacij ali izvajati ukrepov za njihovo razvrednotenje« (Zakona o elektronskih komunikacijah (ZEKom-1) 2012).

- Kibernetski napad, ki je lansiran s strani države je velikokrat samo en delček celotne strategije napada, ki je lahko sestavljena tudi iz konvencionalnih oblik napada.
- Clausewitzevo definicijo vojne: Vojna je dejanje nasilja, katerega namen je prisiliti nasprotnika, da izvrši naše želje. Avtorja to definicijo dopolnjujeta s tem, da se ta definicija lahko uveljavlja tudi za kibernetske vojne, saj po njuno gre za uporabo »sile« oz. »sredstev«, ki niso nujno konvencionalne v svoji obliki, vendar pa pripomorejo k dosegi ciljev.
- Kibernetsko bojevanje mora biti po njuno v domeni države in biti vključeno v nacionalni varnostni strategiji. Zato je po njuno potrebno sprejetji tudi ustrezne pravne akte za efektivno obrambo v primeru napada (Cornish in drugi 2010).

5.1.3 Kriteriji kibernetskega bojevanja

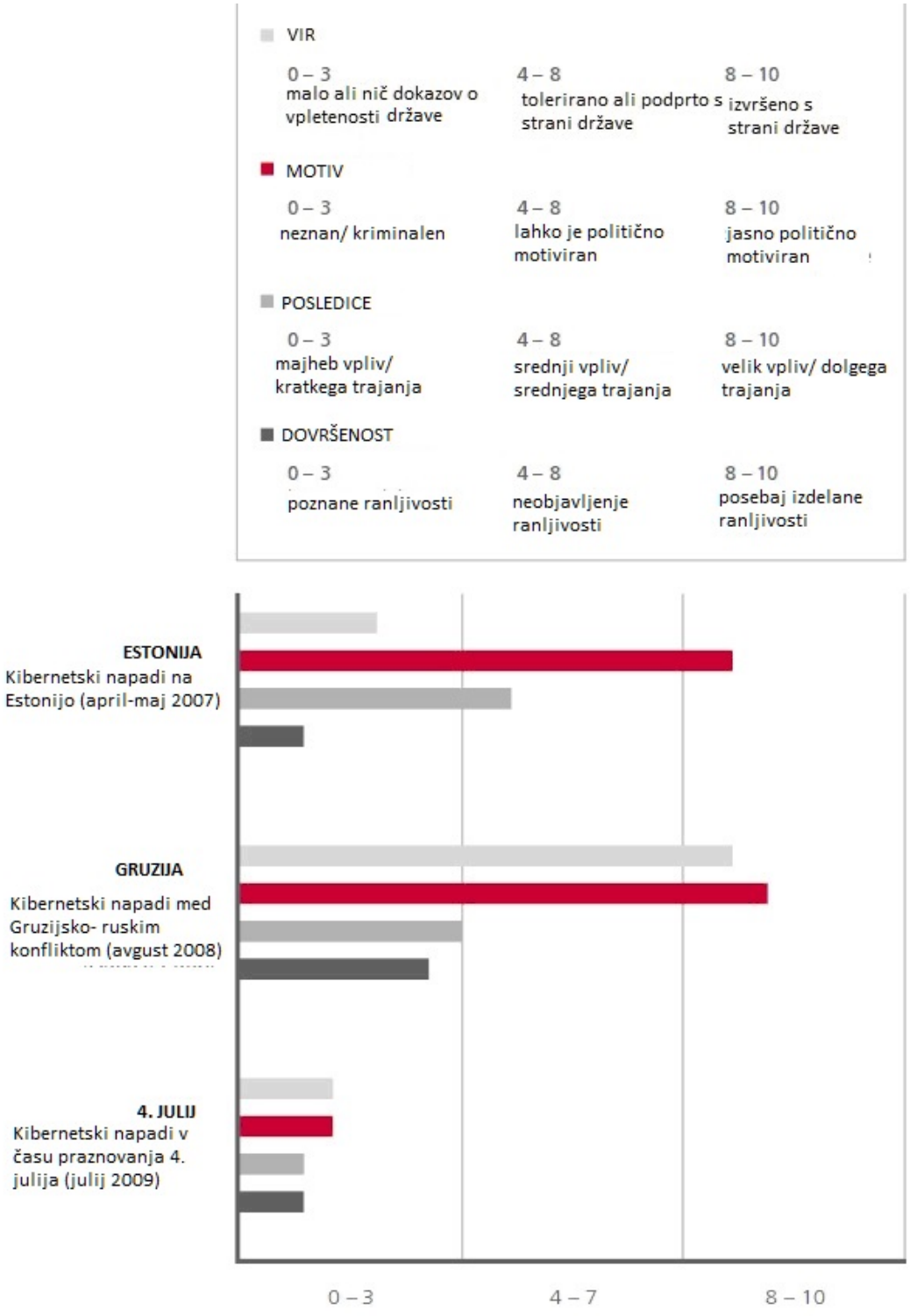
Ker je zelo težko definirati ali gre neko dejanje za kibernetsko bojevanje ali ne, so strokovnjaki v ta namen naredili sistem štirih atributov. Če neko dejanje zadosti vsem štirim atributom, potem gre za kibernetsko bojevanje.

- Vir napada (ali je bil napad izveden ali podprt s strani države)
- Motiv napada (ali je bil napad politično motiviran)
- Posledice (ali je napad naredil škodo)
- Dovršenost (ali je napad vseboval posebne metode, kompleksno načrtovanje) (DeWalt 2009).

Če analiziramo primere napadov na Gruzijo in Estonijo na podlagi zgoraj omenjene metodologije ugotovimo naslednje (glej Graf 5.1). Estonski napad je na področju vira dosegel oceno 2, kar označuje, da niso obstajali dokazi o vpletenosti države. Na področju motiva napada je dobil 8, kar označuje, da je vseboval državne politične cilje. Na področju posledic 4, kar označuje sreden vpliv in srednjega trajanja. In na področju dovršenosti 1 kar označuje majhno dovršenost, ki izrablja že poznane ranljivosti. Glede na ugotovitve težko zaključimo, da je bil napad na Estonijo del kibernetskega bojevanja, saj obstaja premalo indicev o vpletenosti vladnih akterjev in tudi posledice niso bile dolgotrajne in velikega obsega.

Gruzijski napad je na področju vira dosegel 8, kar označuje izvrženost s države. Na področju motiva za napad 9, kar označuje državne politične cilje. Na področju posledic 3, kar označuje majhne posledice in kratkoročni učinek. In na področju dovršenosti 2, kar označuje majhno dovršenost, kjer se je izrabilo že poznane ranljivosti. Glede na analizo napada, lahko zaključimo, da gre v primeru napada na Gruzijo že bolj za kibernetsko bojevanje, kot v primeru Estonije. V primeru Gruzije je bolj jasna vpletenost vladnih akterjev na področju vira napada in motiviranosti za napad. Vendar pa so bile posledice bolj kratkotrajne in tudi dovršenost napada je bila majhna. Napadi, ki so se vršili 4. julija so na vseh področjih dosegli nizko stopnjo, zato za njih ne moremo trditi, da so bili del kibernetskega bojevanja.

Graf 5.1: Analiza napadov na Estonijo, Gruzijo in napadov 4. julija (dan neodvisnosti ZDA)



Vir: DeWalt (2009).

6 Primerjava »kibernetske hladne vojne« z hladno vojno

V zadnjem času velikokrat slišimo termin »kibernetska hladna vojna«, na katero opozarjajo mnogi strokovnjaki, ki nam bi nam pretila z vseh strani. Vendar je to termin, ki ni nastal v znanstveni publikacijah, pač pa preko novinarskih člankov, kjer so novinarji senzacionalistično poimenovali velikanske kraje podatkov nekaterih držav, na drugi strani ustanovitve kibernetskih vojaških oddelkov za morebiten začetek »kibernetske hladne« vojne že v začetki 21. stoletja. Danes je ta termin veliko bolj zastopan tudi v znanstvenih publikacijah, saj obstaja kar nekaj raziskav na temo proučevanja kibernetskih napadov med državami in iskanje podobnosti in razlik z hladno vojno.

Države so prvič postale pozorne na potencialne kibernetske nevarnosti že leta 1988, ko je Morris, ki je bil odprtokodna zlonamerna programska oprema tipa črv, napadla zelo veliko računalnikov. Ocene škode, ki jo je naredil so se gibale med 100.000-10.000.000 dolarjev. Njegov pohod pa je bil tudi povod, da so države prvič v zgodovini začele sprejemati pravne akte, ki bi jih lahko zaščitili pred škodo, ki jo lahko naredi zlonamerna programska oprema. Zato so že naslednje leto ZDA sprejele Zakon o računalniških zlorabah in prevarah (Computer fraud and abouse act) (Dressler 2007). Z leti je število zlonamerne programske opreme samo še naraščalo, z naraščajočim številom uporabnikov računalnikov in interneta. Zlonamerna programska oprema je z leti postajala vedno bolj sofisticirana in je povzročala vedno več škode. Vendar pa so lastnosti kibernetskih groženj (asimetričnost, anarhičnost, težko izsledljivost...), države prvič v zgodovini prestrašile same razsežnosti potencialnih napadov. Zato se je v tistem času pojavil termin kibernetski Pearl Harbor (Sulek in Morgan 2009).

6.1 Kibernetski Pearl Harbor, kibernetska Katrina in kibernetski 9/11

Kibernetski Pearl Harbor je koncept, ki je nastal na osnovi realnega Pearl Harbor napada, ki se je zgodil leta 1941, ko so nenapovedano japonske sile napadle ameriško vojaško oporišče na Havajih. Japonci so uničili 188 ameriških letal, 18 vojaških ladij in ubitih je bilo 2402 ljudi. Kot odgovor na to dejanje so ZDA tudi uradno vstopile v vojno (Barnes 1972). Ta koncept nenadnega, nenapovedanega napada, ki bi imel velikanske posledice, se je dokaj hitro začel implicirati na kibernetske grožnje. Na tako imenovani kibernetski Pearl Harbor, ki bi z enim napadom lahko uničil kritično infrastrukturo. Ne nujno v fizični obliki, vendar bi lahko onesposobil njeno delovanje, kar pa bi imelo velike posledice.

Ravno tako so se po hurikanu Katrina začele pojavljati ideje o kibernetski Katrini in kibernetski 9/11, ki bi ravno tako, kot kibernetski Pearl Harbor napadla nenadoma in nenapovedano. Vendar je ena zelo pomembna razlika med tema dvema konceptoma. Kibernetski Pearl Harbor bi se lahko zgodil, kot napad s strani neke države, medtem ko bi se kibernetska Katrina ali kibernetski 9/11 lahko zgodila kot napad s strani nevladnih akterjev (DeWalt 2009). Ker se trenutno v svetu še ni zgodil ne kibernetski Pearl Harbor niti ne kibernetska Katrina, zato težko predvidevamo kakšna bi bila najboljša strategija v primeru takšnega kibernetskega napada. Ravno zato se vedno več strokovnjakov ozira v preteklost po odgovore, ki bi nas morda bolje pripravili na potencialne kibernetske napade v prihodnosti. Najbolj se ozirajo k hladni vojni (Sulek in Morgan 2009).

6.2 »Kibernetska hladna vojna«

6.2.1 Hladna vojna

Če želimo razumeti termin »kibernetska hladna vojna«, moramo podrobneje pogledati podobnosti in razlike med hladno vojno in »kibernetsko hladno vojno«.
Hladna vojna je obdobje, ki se je začelo takoj po drugi svetovni vojni, kot rivalstvo (tudi na ideološkem področju komunizem proti kapitalizem) v oboroževanju med Sovjetsko zvezo in ZDA ter njunimi zavezniki v želji prevlade ene nad drugo. Državi sta naredili vsaka svoja zavezništva. ZDA so formirale več zavezništev. Vse skupaj pa so tvorile tvorile »Zahodni blok«. Sovjetska zveza je skupaj z članicami »Varšavskega pakta« in tvorila »Vzhodni blok«. Vojna ni nikoli postala vroča oz. nikdar ni prišlo do dejanske uporabe orožja med velesilama, sta pa zato posredovali v več oboroženih konfliktih v drugih državah posredno ali neposredno (kubanska kriza, Vietnam, Koreja, Afganistan, Laos ipd) (Westad 2005). V času hladne vojne sta obe velesili začeli z jedrskim oboroževanjem, ki sta ga kasneje prenesli tudi vesolje. Temeljna doktrina v času hladne vojne je bila vzajemno zagotovljeno uničenje (mutually assured destruction (MAD). Vzajemno zagotovljeno uničenje je temeljilo na predpostavki odvračanja. V primeru izstrelitve jedrskega orožja ene strani na drugo bi druga takoj odgovorila s povračilnim ukrepom izstrelitvijo jedrskega orožja. Pri tem bi bili obe strani deležni velike gmotne škode in žrtev. V primeru uporabe vseh sredstev pa bi lahko prišlo do popolnega uničenja vseh vpletenih. Na srečo nikdar ni prišlo do dejanske uporabe jedrskega orožja med velesilama, vendar sta se v želji po vojaški premoči ene nad drugo uporabili tudi drugih tehnik. Kot so psihološko bojevanje, vohunjenje, kraja podatkov in posredniških vojn (ang. Proxy Wars) Hladna vojna se je prenesla celo v nove sfere bojevanja, kot je npr. vesolje (Leffler 2010). Končala se je leta 1991 z razpadom Sovjetske zveze. Bistvo hladne vojne je bilo ustrahovanje nasprotnika z oboroževanjem in vohunjenje z željo pridobitve podatkov, ki bi omogočili hiter razvoj novih tehnologij in tekmovalnost. Za nas je posebej pomembno zadnje obdobje hladne vojne tako imenovano obdobje Vojne zvezd (ang. Star Wars) To obdobje se je začelo, ko je Ameriški predsednik Ronald Reagan 23. marca 1983 na javni televiziji predstavil projekt SDI (Strategic Defense Initiative) (Leffler 2010).

Namen SDI je bil ,da bi ZDA lahko razvile ščit, ki bi jih branil pred potencialnimi napadi Sovjetske zveze z medcelinskimi balističnimi raketami (ICBM), tudi iz vesolja. SDI je vključeval razvoj veliko novih tehnologij med drugim tudi novih satelitov, ki bi lahko nosili laserje in bi lahko razstrelili ICBM rakete še tekom leta. Vendar niti ena tehnologija, ki so jo razvijali ni delovala. SDI je močno pripomogel k samem tehnološkem razvoju ZDA, kljub temu da same tehnologije in naprave niso nikdar zares delovale, je sam razvoj novih tehnologij močno pomagal ZDA. Največ so se s pomočjo SDI razvili laserji in različni senzorji. SDI je tudi finančno zelo pripomogel različnim raziskovalnim inštitucijam, da so znotraj SDI lahko razvijali nove tehnologije. Močno je tudi povezal samo sodelovanje med različnimi raziskovalnimi inštitucijami. Pripomogle pa je tudi k finančnemu uničenju Sovjetske zveze, ki ni bila več zmožna vlagati velikanskih zneskov za razvoj novih tehnologij in konkuriranje ZDA (Reiss 1992).

Tudi slovensko podjetje Iskra Delta je občutilo moč hladne vojne, ki ga je privedla na kolena. Ker je primer Iskra Delta pomemben za dogajanje na področju IKT na območju Jugoslavije, ga bom v nadaljevanju bolje predstavila.

6.2.2 Primer Iskra Delta

Če se vrnemo v čas hladne vojne in Jugoslavije, kjer je bila družbena lastnina in podjetništvo, kot ga danes poznamo danes, skorajda ni obstajalo. Obstajalo je plansko gospodarstvo, ki je bilo v celoti regulirano s strani države. Navkljub vsemu temu je nastalo podjetje Iskra Delta, ki je postavilo Slovenijo na zemljevid pomembnih proizvajalcev informacijskih tehnologij. Podjetje danes ne obstaja več, vendar je s svojo inovativnostjo in iznajdljivostjo pustilo pečat v zgodovini Slovenije.

V času hladne vojne ni boj samo potekal med velesilama na področju jedrske energije in vojaške moči, ampak tudi na področju inovacij tehnološke premoči. ZDA so kontinuirano ustvarjale dolgoročno strategijo na vojaškem in gospodarskem področju. Del tega je bil tudi strog nadzor nad izvozom visokih tehnologij v druge države, ki niso bile v njenem najtesnejšem zavezništvu. Ameriške obveščevalne službe so nadzirale prodaje lastnih računalniških komponent in računalnikov v tuje države. Računalniške komponente so vsebovale skrito zlonamerno programsko opremo in vohunsko opremo, ki je posredovala podatke v ZDA. Podjetja znotraj ZDA so se lahko prosto ustanavljala na pobude računalniških zanesenjakov, ki so z svojimi idejami in inovacijami postavili Silicijevo dolino. Na drugi strani so bile države, ki so spadale v interesno območje Sovjetske zveze, kateri je pripadala tudi Jugoslavija od leta 1984. Te so bile podvržene planskemu gospodarstvu, ki je onemogočalo prosti trg in prosto ustanavljanje podjetij. Podjetja so se ustanavljala na podlagi državnega planiranja na vsakih pet let. Ravno v naprej predvideno ustanavljanje podjetij in odsotnost prostega trga so onemogočala računalniškim zanesenjakom, da bi podobno, kot Američani lahko z lahkoto ustanovili podjetje in vpeljevali inovacije. Vendar kljub vsem preprekam je v sedemdesetih letih prejšnjega stoletja nastalo podjetje Iskra Delta. Sprva se je podjetje imenovalo Elektrotehna, ki je bilo specializirano za prodajo elektrotehničnih izdelkov v Jugoslaviji. Podjetje je bilo tudi pooblaščeno za uvoz in izvoz le-teh. Leta 1972 so prišli v stik z Ameriškim podjetjem Digital Equipment Corporation (DEC), ki je proizvajalo miniračunalnike. ZDA so omogočale Jugoslaviji nakup njihovih računalnikov, ker je imela Jugoslavija status neuvrščene države. DEC je bilo s svojimi proizvodi konkurenčno takrat največjemu podjetju na področju računalništva IBM, ki je tudi v Jugoslaviji imel zastopništvo preko podjetja Intertrade. IBM-ove računalnike so uporabljale

Jugoslovanke banke in državni aparat. Elektrotehna je podpisala ekskluzivno pogodbo z DEC za prodajo njihovih produktov v Jugoslaviji in poslala inženirje, da so odšli na izobraževanja DEC v ZDA. Zaradi dobrega poznavanja sistemov DEC so bili tudi zelo uspešni pri sami prodaji njihovih produktov. Prodajo so razširili na področje celotne Jugoslavije, posledično so poslali na dodatna izobraževanja vedno več inženirjev. Ker so inženirji želeli prilagoditi programsko okolje uporabnikom, so kmalu ustanovili oddelek Digital, ki je bilo zadolženo za razvoj aplikativne programske opreme. Digital je začel ponujati vedno boljše rešitve, ki so bile prilagojene glede na potrebe jugoslovanskega trga in želje naročnikov. Digitalove rešitve so bile zelo konkurenčne glede na cene drugih ponudnikov, ki so ponujali rešitve tujih podjetij. Digital je imel letno 300% rast na področju zaposlenih in poslovanja. Leta 1977 se je podjetje preimenovalo v Delta. Ker je bilo težko dobiti dovoljenje za uvoz računalnikov so začeli razvijati lasten računalnik po principu OEM (Original Equipment Manufacturer), ki je bil kompatibilen z DEC. Ker so bili sestavni deli relativno dragi, so se odločili, da bodo sestavili računalnik, ki bo vseboval kar se da malo DEC komponent. Vse ostale komponente bodo poskusili naredit sami, oziroma se povezati z Slovenskimi podjetji, ki bi proizvajali za njih te dele. Naredili so tudi lastno programsko opremo, kar je kasneje omogočalo, da je računalnik dobil status »domačega produkta«. Računalnik so želeli predstaviti javnosti na način s čim večjim učinkom, zato so ga podarili Titu za njegov rojstni dan 25. maja 1978. Računalnik je Titu, ko ga je prižgal zaigral jugoslovansko himno in na ekranu izrisal Titov portret. Predstavitev je bila zelo uspešna in vsi jugoslovanski mediji so poročali o Deltinem računalniku. Zvezna vlada se je odločila da bo šla v korak s časom in bo tudi Jugoslavija proizvajala računalnike za vojsko. Vojska je poslala po celotni Jugoslaviji svoje strokovnjake, ki so morali obiskati vsa podjetja, ki so uvažala ali proizvajala računalnike. Vojska je želela imeti v celoti narejen računalnik doma, ki bi vseboval čim manj uvoženih komponent. Po Jugoslaviji je bilo kar nekaj podjetij, kot je bilo Intertrade, ki je prodajalo licenčne tuje računalnike po visokih cenah brez lastne dodane vrednosti in razvoja. Vojska se je glede na videno odločila za Delto. Ker je v Sloveniji proizvajala električne izdelke Iskra se je Delta pripojila Iskri in nastala je Iskra Delta. Proizvodnja je stekla in kmalu so ponujali svoje izdelke tudi v New Yorku, kjer so tudi odprli svoje predstavništvo. Izdelke so predstavljali na največjih sejmih elektronike, zato so postali prepoznavni tudi zunaj meja Jugoslavije. Izvažali so tudi v Sovjetsko zvezo, Indijo, Japonsko, Avstralijo in naredili največji projekt na Kitajskem.

Leta 1985 so na Kitajskem pod imenom Projekt Milijarda zgradili policijsko omrežje za celotno Kitajsko. Sistem je omogoča prenos datotek in elektronsko pošto. Vrednost projekta je bila takrat 10 milijonov dolarjev. To je bil največji nakup Kitajske v Jugoslaviji. Kasneje so želeli Kitajci nadgraditev sistema in so ponudili za nadgradnjo 100 milijonov dolarjev. Vendar se je Jugoslovanska oblast ustrašila velikanskih zneskov, zato niso dovolili obiska Kitajske delegacije v Delti. Podobna podtikanja in onemogočanja so se začela tudi pri kasnejših projektih z Indijo in ostalimi državami.

Ker je hladna vojna z leti samo še eskalirala, se je to poznalo tudi na delovanju Iskra Delte, ki je z leti postala že zelo pomemben igralec na področju informacijske tehnologije. Za Vzhod je Iskra Delta predstavljala okno do najnovejše informacijske tehnologije. Na drugi strani pa je za Zahod začela predstavljati vedno večjo nevarnost, da nebi njena tehnologija prišla v posest Vzhoda. Zahodne varnostne službe naj bi začele uničevati Iskra Delto, ker so se bali, da bi njena tehnologija prišla v roke Vzhoda. Pritiskali so na vodilne, da se ukine razvojni oddelek. To so utemeljevali s trditvami, da se bolj finančno izplača proizvodno sodelovanje z ameriškimi podjetji. V medijih so se začele pojavljati novice, da Iskra Delta vedno bolj brede v rdeče številke zaradi vztrajanja na lastnem razvoju, ki je po njihovo neekonomičen. Vzhod je na drugi strani začel pritiskati na Iskra Delto, da je zadrževal plačila za izdelke, s čemer ni imela več denarja za razvoj in inovacije. Leta 1989 je občutila resnično moč hladne vojne, ko se je znašla v primežu dveh velesil, ki sta jo vsaka na svoj način začele onemogočati. Pomoč in podporo ji je odklonilo tudi vodstvo lastne države. Ker je vodstvo Iskra Delte ugotovilo, da takšnih pritiskov podjetje ne bo zdržalo, se je na pobudo direktorja odločilo odstopiti s svojih položajev, saj niso hoteli popustiti ne na eni ne na drugi strani. Iskra Delta je po šestih mesecih pristala v likvidaciji. Iz nje je kasneje nastalo več podjetij (Škrubej 2008).

6.2.3 Definicija

"Kibernetska hladna vojna" je kibernetsko bojevanje ki poteka trenutno med državami, za dosego tehnološke prednosti pred drugo oz. onesposobljenje nasprotnika. Vsebuje kibernetsko vohunjenje, napad, uporabo zlonamerne programske opreme ter druge metode za dosego ciljev (Definition 2013). Strokovnjaki jo poimenujejo, da je to »hladna vojna«, ker za enkrat še nima fizičnih posledic. Čeprav so jo napadi, kot je Stuxnet naredili že bolj »vročo«.

Za začetek kibernetskega bojevanja oz. potencialne "kibernetske hladne vojne" bi težko označili določen dogodek. V zgodovini se je zgodilo že veliko napadov. Če naštejemo samo najbolj glavne. Leta 1994 se zgodijo napadi znotraj rusko-čečenskega konflikta, 1999 napadi na Nato v sklopu konflikta na Kosovu, 2000 napadi na Bližnjem vzhodu, 2001 Titan Rain (napadi kitajskih hekerjev na ZDA) (Geers 2007). Vendar obstaja neko soglasje v stroki, da se je prvi resnejši kibernetski napad (ki naj bi bil politično motiviran) zgodil leta 2007, ko je bila napadena kritična infrastruktura Estonije. Do tedaj noben napad ni bil tako razsežen in ni imel takšnih posledic za neko državo, kot napad na Estonijo. Napadene so bile vladne spletne strani, strani medijev in estonske banke. Šlo je za DDOS napad (porazdeljenja zavrnitev storitve ang. Distributed Denial of Service) , kjer je nekdo z veliko količino zahtev spravil estonske strežnike na kolena, spletne strani pa niso bile dostopne štiri dni. Estonski minister za zunanje zadeve je za napad obsodil Rusijo oz. Kremelj. Povod za napad naj bi bil načrt Estonije, da premakne spomenik ruskega bronastega vojaka na drugo lokacijo. Odgovornost za napad je prevzelo več organizacij in posameznikov, vendar nikakor niso mogli direktno naprtiti odgovornosti Rusiji, kljub več raziskavam. Po tem dejanju so ZDA in mnoge druge države spremenile nacionalne varnostne strategije oz. sprejele nove pravne akte. Začelo se je tudi veliko investirati na področju kibernetske obrambe na nacionalni ravni. Busheva administracija je sprejela Celovito nacionalno kibernetsko varnostno pobudo (ang. Comprehensive National Cybersecurity Initiative (CNCI)), ki je dobila finančno podporo 30 milijard dolarjev. Vendar naj bi celoten program stal veliko več (Greenberg 2009). Ali danes zopet poteka podoben boj med velesilami le da tokrat v kibernetskem prostoru? Na to vprašanje bom poskušala odgovoriti v nadaljevanju preko primerjalne analize.

6.3 Podobnosti in razlike med hladno in "kibernetsko hladno vojno"

6.3.1 Strategije in taktike

Prva podobnost, ki jo zasledimo je v odgovorih na zaznane grožnje. V obeh primerih težko ocenimo uspešnost zastavljenih strategij in taktik. V primeru SDI se ni vedelo ali bodo sistemi delovali, ker nikdar ni prišlo do dejanske izstrelitve ICBM raket s strani Sovjetske zveze, ki bi postavile SDI na preizkus. Ravno tako, kot pri kibernetskih napadih ne moremo vedeti ali bi bilo mogoče izvesti kibernetski napad na primer na ZDA v velikanskem obsegu oz. v kolikšni meri bi deloval. Vendar si v obeh primerih države niso mogle privoščiti, da bi bile napadene, zato so preventivno začele graditi obrambo proti potencialnim napadom (Sulek in Morgan 2009). Podobnost najdemo tudi na načinu spopadanja s samo grožnjo. V času hladne vojne je bila dominantna strategija odvračanje od napada z zagotovim uničenjem obeh strani. V primeru kibernetskih napadov je tudi v uporabi vedno bolj strategija odvračanja z izgradnjo novih kibernetskih varnostnih centrov, vzpostavitvijo kibernetskih vojaški oddelkov in sprejetjem pravnih aktov, ki sankcionirajo takšna dejanja (McConnell 2010). Po drugi strani pa ravno takšne novice o novih kapacitetah mnogim hekerjem predstavljajo izziv. Tretjo podrobnost najdemo v uporabljeni strategiji. V času hladne vojne je bilo v uporabi psihološko bojevanje z namenom demotivacije nasprotnika in tudi vohunjenje z namenom pridobitve informacij. Tudi to najdemo v »kibernetski hladni vojni«. Če pogledamo primer lažnega Facebook računa Admirala Jamesa Stavridisa, ki so ga ustvarili kitajski hekerji z namenom pridobitve informacij s strani ostalih vojakov in vojaškega osebja (Reed 2012). Podobnost najdemo tudi na področju posredniških vojn. V času hladne vojne sta velesili posredovali v veliko konfliktih posredno ali neposredno, (Afganistan, Vietnam ipd.) z željo pridobitve večjega vpliva nad določeno državo ali celo regijo. Podobno se dogaja v »kibernetski hladni vojni«. Države direktno ne napadejo ena druge, saj bi to izzvalo mednarodne sankcije. Zato veliko raje napadajo preko posrednikov, kot so hekerji iz lastne ali tuje države z namenom prikritja vpletenosti (Mumford 2013).

6.3.2 Cena

Drugi element primerjave je sama cena izdelave obrambnih sistemov. V primeru hladne vojne je bila izdelava ICBM raket relativno nizka, v primerjavi z izdelavo obrambnega sistema SDI, pred potencialnim napadom. Podobno je tudi pri kibernetskih napadih. Relativno zelo poceni je izdelava zlonamerne programske opreme oz. neke druge ofenzivne programske opreme. V raziskavi iz leta 2002 so ugotovili, da bi potrebovali samo 5 let in 200 milijonov dolarjev, da bi lahko izvedli velik kibernetski napad (Kane 2002). Za razliko od razvoja jedrskega orožja, je kibernetska orožje zelo lahko duplicirati medtem, ko države vlagajo velikanske zneske v razvoj obrambnih sistemov pred kibernetskimi napadi (Sulek in Morgan 2009).

6.3.3 »Hladnost bojevanja«

Tretja podobnost je v grožnji sami. V času hladne vojne se je sicer vedelo kdo je »sovražnik«, vendar na srečo nikdar ni sama vojna prešla v vročo vojno. Glavni nasprotnici ZDA in Sovjetska zveza sta vseskozi vohunili ena za drugo, v želji po prevladi nad drugo predvsem v tehnološkem, ekonomske, diplomatskem in oborožitvenem smislu (Sulek in Morgan 2009). Kibernetsko bojevanje je »hladno« bojevanje, saj za enkrat še ni prešlo v stanje »vročega« oz. uporabo konvencionalnega orožja. Ravno tako države, kot so Kitajska uporabljajo kibernetske napade za pridobivanje podatkov in vohunjenje (Operacija Titan Rain), z namenom pridobitve hitrejšega tehnološkega razvoja. Samo leta 2007 so zabeležili preko 37.000 vdorov (ni podatka koliko je bilo uspešnih) v vladne sisteme ZDA in sisteme javnega sektorja ZDA. Bilo je tudi preko 80.000 želenih vdorov v računalniške sisteme Ministrstva za obrambo ZDA. Za velikim številom vdorov so stale Rusija in Kitajska (Sulek in Morgan 2009). Tudi vedno več je indicev, da za določenimi napadi stojijo države (podobno, kot v hladni vojni vedno bolj vemo kdo je »sovražnik«). Vendar pa je meja tukaj še vedno precej zabrisana, saj lahko za dejanji nekega »heckerja« stoji država, kar je težko dokazljivo (Cornish in drugi 2010).

6.3.4 Akterji

Počasi se začenja v svetu oblikovati podoba med kom sploh poteka kibernetsko bojevanje oz. tekmovanje. Največ napadov je v medijih predstavljenih s strani Kitajske do ZDA. Oblikovati so se začela nekakšna zavezništva med državami. Tako zasledimo članice Nata na eni strani in Rusijo in Kitajsko skupaj na drugi strani. Sama porazdelitev držav je nekako podobna, kot je bila v času hladne vojne (DeWalt 2009). Vendar ni strogo bipolarna, kot je bila v času hladne vojne. Prej bi lahko rekli multipolarna, ker so v kibernetsko bojevanje vključeni ne samo državni akterji ampak tudi nedržavni (predvsem teroristične skupine) (Sulek in Morgan 2009).

Slika 6.1: Države, ki razvijajo napredna ofenzivna kibernetska sredstva

Vir: DeWalt (2009).

6.3.5 Pravni akti

V času hladne vojne sta se sprejela dva ključna mednarodna dokumenta SALT I (1969) in SALT II (1979) (sporazuma o omejevanju jedrskega orožja – ang. Strategic Arms Limitation Talks), ki sta omejevala oboroževanje obeh akterjev. Obe pogodbi pa sta sčasoma privedli do podpisa START (1991) (Pogodba o zmanjševanju strateškega orožja - ang. Strategic Arms Reduction Treaty), ki pa je zmanjševala količino jedrskega orožja (Leffler 2010). Ker postaja boj vedno večji med državami v kibernetskem prostoru in se napadi vršijo dnevno, so mnoge države že sprejele ustrezne pravne akte na nacionalni ravni. Leta 2001 je Svet Evrope sprejel Konvencijo o kibernetski kriminaliteti (ang. Convention on Cybercrime), ki jo je podpisalo preko 40 držav. Konvencija zavezuje države podpisnice, da si bodo med seboj pomagale v boju proti kibernetskemu kriminalu in tudi lažje skupaj identificirale kriminalce (Cybercrime 2013). ZDA se zavzemajo za podpis pogodbe med njimi in Rusijo o omejevanju kibernetskih napadov (Gorman 2010). Leta 2011 so Kitajska, Rusija, Tadžikistan in Uzbekistan Združenim narodom predlagale sprejetje mednarodnega kodeksa ravnanja na področju informacijske varnosti (ang. International code of conduct for information security) (Political Contacts 2011). Predlog ni bil podprt s strani zahodnih držav, saj naj bi po njihovo preveč omejeval svoboščine. Leta 2013 sta v duhu hladne vojne ZDA in Rusija vzpostavili med seboj “rdeči telefon” kibernetskih napadov. Ta omogoča varno glasovno komunikacijo med kibernetskimkoordinatorjem ZDA na eni strani in ruskim namestnikom sekretarja varnostnega sveta (Gallagher 2013).

Večina strokovnjakov opozarja, da bi morala mednarodna skupnost sprejeti nekakšen skupni pravni akt, ki bi točno definiral strategije v primeru napadov in tudi sankcije, zato predlagajo Pogodbo o kibernetskem bojevanju (Treaty on Cyberwarfare) (Denning 2000).

6.3.6 Vzpostavitev vojaških kibernetskih oddelkov

V času hladne vojne sta državi vzpostavljali nove vojaške enote in namenjale vedno več denarja v vojaške namene. Podobno delajo države tudi sedaj. Kot odgovor na estonski napad leta 2007 je Nato v Estonskem glavnemu mestu Tallinu, postavil svoj Center odličnosti za kibernetsko obrambo. Ravno tako so ZDA leta 2009 javnosti predstavile ustanovitev Kibernetskega poveljstva (U.S. Cyber Command), ki je del Strateškega poveljstva (U.S. Strategic Command). Kibernetsko poveljstvo vodi general s štirimi zvezdicami. Njegov namen pa je zaščita vitalnega vojaška omrežja. Podobno enoto ustanavlja tudi Velika Britanija (ang. Office of Cyber Security (OCS)). Namen OCS je spopadanje z vedno večjim številom napadov in tudi v primeru velikega napada pripraviti ofenziven protinapad. Podobne enote ustanavljajo tudi druge države po svetu (DeWalt 2009). Kitajska je glede uradne predstavitve vojaških enot za kibernetsko bojevanje veliko bolj skrivnostna. Vendar je poročilo ameriške nacionalne varnostne agencije (NSA) razkrilo, da naj bi obstajala enota 61398, ki deluje znotraj kitajske ljudske armade in naj bi bila odgovorna za veliko napadov (Obel 2013). Rusija ravno tako uradno ustanavlja posebno vojaško enoto za kibernetsko bojevanje znotraj ruskih oboroženih enot (Defense Russian Military Creating Cyber Warfare Branch 2013). Podobne enote najdemo še v Indiji, Iranu, Južni Koreji, Veliki Britaniji in Nemčiji (Clarke 2010). Richarda A. Clarke ugotavlja, da imajo ZDA dober ofenziven sistem za kibernetsko napadanje, vendar pa po njegovo pešajo ravno na področju obrambe. Tukaj predvsem izpostavlja pomanjkanje obrambnih kapacitet, za zaščito kritične infrastruktur in ostale infrastrukture, ki ni direktno povezana z vojsko. Po njegovo smo v primeru kibernetskega napada kljub dragi zaščiti vojaške infrastrukture, posamezniki prepuščeni samemu sebi (Clarke 2010). V primeru hladne vojne se je dogajalo podobno. Države so se oboroževale na ofenzivni ravni, teh hkrati vzpostavljale drage obrambne sisteme na defenzivni ravni, vendar so malo pozabljale na civilno prebivalstvo, ki se je moralo znajti samo (primer Vietnam). Podobno se dogaja v času »kibernetske hladne vojne«. Kot vidimo se države z vzpostavitvijo novih enot za kibernetsko bojevanje pripravljajo na morebitne napade. Pri tem pa pozabljajo na civilno prebivalstvo in kakšne posledice bi imeli potencialni napadi na njih. Kot pravi Clarke, bi morale države bolje zaščititi vse uporabnike informacijske tehnologije in ne samo vojsko. Ravno zaradi zgoraj naštetih

razlogov, strokovnjaki opozarjajo, da je potrebno reševati in se pripravljati na potencialen kibernetski napad na podoben način, kot se je to dogajalo v času hladne vojne. Pri tem predvsem izpostavljajo, da je potrebno vzpostaviti sistem za alarmiranje, ki bi nadzoroval kibernetski prostor in identificiral napad in sam izvor napada, podobo kot je to bil SDI z namenom hitrega reagiranja ob morebitnem napadu s strani Sovjetske zveze (McConnell 2010).

6.3.7 Primeri napadov na države v sklopu »kibernetske hladne vojne«

Število napadov z leti skokovito narašča, zato bom v tej točki predstavila predvsem napade, ki se vršijo med ZDA, Kitajsko in Rusijo, ter napade, ki so začeli »kibernetsko hladno vojno« delati vedno bolj vročo. Sam tip napadov bom razdelila v dva tipa napadov na vohunjenje in sabotaže.

6.3.7.1 Vohunjenje in vdor v sisteme z namenom pridobitve podatkov:

- **Titan Rain.** Leta 2004 so hekerji vdrli v računalniške sisteme velikih ameriških podjetij, ki so močno povezana z ministrstvom za obrambo ZDA, kot so Lockheed, Nasa in Redstone Arsenal. Ukradli velikanske količine podatkov teh podjetji, za napadom pa naj bi stala Kitajska (Lewis 2005). Ocenjuje se, da Kitajska in Rusija izvajata podobne akcije predvsem z namenom pridobitve hitrejšega tehnološkega napredka oz. tehnološke prednosti pred ZDA (Gorman 2009).
- **Operacija Aurora.** Kitajska skupina hekerjev imenovana Elderwood, ki ima močne povezave s Kitajsko ljudsko armado je junija 2009 napadla več ameriških podjetij z namenom pridobitve informacij in podatkov. Napadeno je bilo preko 34 podjetij med njimi so bila tudi Google, Adobe Systems, Yahoo, Symantec, Morgan Stanley, Dow Chemicals in še mnoge druge. Analiza napada je pokazala, da se je napad vršil skozi varnostno luknjo v Microsoft Internet Explorerju, zato so mnoge države pozvale svoje državljane, (Nemčija, Francija in Avstralija) naj uporabljajo alternativne spletne brskalnike (Zetter 2010). Microsoft je v roku enega tedna zakrpal varnostno luknjo, vendar je tudi priznal, da je vedel za luknjo že od septembra prejšnjega leta (Naraine 2010).

6.3.7.2 Sabotaže

- **Stuxnet.** Stuxnet je zlonamerna programska oprema tipa črv, ki je junija 2010 napadla iransko jedrsko infrastrukturo. Izdelala naj bi jo ZDA v sodelovanju z Izraelom. Stuxnet se je razširil preko operacijskega sistema Microsoft Windows in je napadal Siemensove industrijske kontrolne sisteme. Okužil je predvsem Iranske industrijske sisteme, predvsem jedrski program. Gre za prvo zlonamerno programsko opremo, ki ni samo vohunila ampak je tudi spremenila delovanje industrijske opreme (CBSNEWS 2010). Stuxnet je spremenil hitrost delovanja nekateri centrifug, zaradi česar so prenehale delovati in so jih morali zamenjati z novimi. Okužil je tudi jedrsko elektrarno v regiji Bushehr, ki je ustavila svoje delovanje za nekaj časa in so jo šele po večkratnih poizkusih ponovno zagnali. Napadena je bila tudi iranska naftna industrija. Vpletenost ZDA in Izraela v razvoj Stuxnet je razkril žvižgač Edward Snowden (Kahlili 2013). Stuxnet je tudi prvi napad, ki je naredil »kibernetsko hladno vojno« potencialno »vročo«, saj bi lahko fizično uničil infrastrukturo. Odkrili so tudi še drugo različico Stuxneta, ki bi zaprl ventile, posledično bi narasel pritisk in prišlo bi do jedrske eksplozije (Robertson 2013).
- **Napad na električno omrežje ZDA**. Aprila 2009 naj bi bilo napadeno električno omrežje ZDA s strani Kitajske in Rusije. Državi naj bi vdrli v sistem in za seboj pustili zlonamerno programsko opremo, ki bi lahko prekinila delovanje sistema. Na srečo so zlonamerno programsko opremo hitro odkrili in ni naredila nobene škode. Uničenje električnega omrežja v ZDA bi pomenilo katastrofalne posledice za ameriško gospodarstvo, podzemne javne prevoze...(Gorman 2009). Ranljivost električnega omrežja ZDA je potrdila tudi študija MIT, ki ugotavlja, da z vzpostavitvijo vedno novejše tehnologije, ki omogoča bolj učinkovito rabo elektrike in njeno distribucijo povečujemo ranljivost (Kassakian 2011).

7 Odprtokodna programska oprema v vlogi bojevanja

Sprva bi mislili, da na področju kibernetskega bojevanja OKPO nima kaj veliko možnosti, vendar se motimo. OKPO ima, kot temeljno vrednoto svobodo in različne svoboščine. Že zaradi temeljnega pristopa je postala vedno bolj priljubljena v državah, kjer se krši človekove pravice in svoboda govora. Tudi v državah, kot je Kitajska za katero vemo, da krši človekove pravice in omejuje svoboden dostop do informacij z »velikim požarnim zidom Kitajske«, je OKPO dala možnost, da zaobidejo vladen nadzor spletne komunikacije. Ljudem je dala možnost neodvisno od države, komunicirati med seboj, državam samim pa možnost razvijati lastno programsko opremo neodvisno od velikih multikoorporacij. V nadaljevanju bom predstavila javnosti bolj znano OKPO, ki je nastala kot potreba po večji anonimnosti, varnosti ali neodvisnosti najsi bo to od države ali multikoorporacij.

TOR: je odprtokodno anonimizacijsko omrežje, ki internetni promet preusmeri nase in ga šifrira. Uporabniku naj bi omogočal popolno anonimnost na spletu. Ravno tako naj bi onemogočal tudi vladnim agencijam poizvedovanje za uporabnikom. Dnevno naj bi ga uporabljajo preko 500.000 uporabnikov. Medtem, ko naj bi imel po svetu preko 4 milijone uporabnikov. Prvotno naj bi bil Tor razvit s strani ameriške mornarice in 60% celotnega razvojnega proračuna je dobil s strani Ministrstva za obrambo ZDA. Uporabnike TOR-a lahko razdelimo v tri skupine. Prva skupina so običajni uporabniki, ki enostavno ne želijo, da se njihovo delo na računalniku nekje beleži. Druga skupina so tisti, ki se bojijo kibernetskega vohunjenja in tretja skupina so tisti, ki ne želijo biti deležni državne cenzure interneta in želijo dostopati do vseh informacij neodvisno. Tor je zelo priljubljen med političnimi aktivisti v Rusiji, Siriji in na Kitajskem, saj jih zaradi Tor-a vlada težje izsledi in cenzurira njihove objave. Ko so leta 2013 s pomočjo Edwarda Snowdena na plan prišla razkritja o vohunjenju za uporabniki Googla s strani ameriške nacionalne varnostne agencije (NSA), se je število uporabnikov Tor-a v enem samem tednu podvojilo (Dredge 2013). Vendar ima Tor tudi slabost. Zaradi omogočanja anonimnosti njegovih uporabnikov je postal zlata jama za pedofile, prekupčevalce z drogo in druge kriminalce (Schneier 2007).

DuckDuckGo: je odprtokodni spletni brskalnik, ki za razliko od Google spletnega brskalnika dopušča uporabniku popolno anonimnosti pri iskanih izrazih. Ravno tako, naj nebi beležil uporabnikovih iskanih gesel, kot to počne Google in na podlagi tega kreira preferenčni vrstni red rezultatov iskanja in s tem zaobide cenzuro na internetu (Hamilton 2013). Onemogočal naj bi tudi vladnim agencijam poizvedovanje za uporabnikom (About DuckDuckGo 2013).

OccupyOS: je posebna varnostno izpopolnjena različica odprtokodnega operacijskega sistema, ki temelji na Linux jedru, namenjena pa je aktivistom in političnim nasprotnikom. Uporabnikom omogoča varno delo na računalniku, varno brskanje po spletu in varno komunikacijo z ostalimi uporabniki znotraj, saj vsa komunikacija poteka preko Tor-a. Vse datoteke, email in ostale korespondence so avtomatično kriptirane (Rafati 2011).

Vendar niso samo posamezniki tisti, ki želijo večjo neodvisnost in anonimnost. Tudi države so se odločile za razvoj lastnih operacijskih sistemov, ki temeljijo na OKPO, zaradi želje po večji varnosti, nadzorom nad sistemom in neodvisnosti od drugih.

Rusija: Ruski premier Vladimir Putin je leta 2010 oznanil načrt migracije na odprtokodni operacijski sistem, razvit s strani države. Celotna migracija naj bi bila zaključena do konca leta 2015. Kot razlog za migracijo so navedli željo po večji neodvisnosti od informacijske tehnologije, razvite s strani ZDA in želje po večjem nadzorom nad sistemom samim (AFP 2010).

Kitajska: Kitajska je začela uporabljati OKPO na nacionalni ravni že zelo zgodaj. Država se je že v začetku leta 2000 odločila, da bodo investirali v razvoj lasnega operacijskega sistema, ki bi bil nameščen na vseh vladnih računalnikih. Leta 2000 je izšla prva različica Red Flag Linux. Država se ni strinjala s politiko Microsofta in je tudi menila, da nima dovolj nadzora nad varnostjo operacijskega sistema (Smith 2000). Zato so leta 2000 izdali ukaz, da morajo iz vseh računalnikov odstraniti Microsof Windows in ga zamenjati z Red Flag Linux (Microsoft in China: Clash of titans 2000). Kitajska je leta 2009 izvedla prebrisan manever, ko je v javnost lansirala novico o razvoju najbolj varnega odprtokodnega operacijskega sistema imenovanega Kylin, v katerega naj nebi mogel nihče vdreti. Kylin naj bi bil glede na novice nov

nacionalni operacijski sistem, ki bi zamenjal Red Flag Linux. Novica o Kylin je bila bolj zastraševalni manever drugih držav (Danchev 2009). Leta 2013 je Kitajska dejansko dala v javnost nov odprtokodni operacijski sistem, ki temelji na odprtokodnem operacijskem sistemu Ubuntu Linux imenovan UbuntuKylin. Z UbuntuKylin želijo opremiti vse vladne računalnike, saj je posebej prirejen za potrebe Kitajske in je tudi varnostno malce izpopolnjen (Finley 2013).

Kuba: Kuba je leta 2009 izdala lastno različico odprtokodnega operacijskega sistema imenovanega Nova. Z Novo želijo zamenjati vse Microsoft Windows operacijske sisteme, ker želijo biti neodvisni od ZDA tudi na informacijskem področju. Za Microsoftove izdelke menijo, da niso zaupanja vredni, saj naj bi bili narejeni v sodelovanju z Ameriško nacionalno varnostno agencijo, ki naj bi lahko tudi dostopala do podatkov na računalniku preko Windows operacijskega sistema. Nova je v uporabi v vladi in tudi v civilni sferi (Israel 2009).

Kot vidimo, OKPO je v uporabi tudi na področju kibernetskega bojevanja, vendar bolj v defenzivne namene. Ker si ne morejo vse države privoščiti drage kibernetske obrambne infrastrukture in kibernetskih vojaških enot, se mnoge odločajo za cenejšo različico obrambe, ki jim jo omogoča OKPO. OKPO omogoča razvoj lastnih nacionalnih distribuciji operacijskih sistemov. Preko OKPO so države veliko bolj neodvisne od multikoorporacij in potencialnih vdorov skozi stranska vrata Ameriške nacionalne varnostne agencije, saj je izvorna koda transparentna. OKPO je vedno bolj tudi v uporabi pri političnih aktivistih, ki so preganjani s strani držav. Uporabljajo OKPO, kot je Tor, OcupyyOs in druge načine ki jim omogočajo, da zaobidejo vladne cenzure in nemoteno ter šifrirano komunicirajo s svojimi podporniki. Opazimo lahko tudi še en trend, ki je bil podoben tudi v času hladne vojne. Države, ki se odločajo za prehod na OKPO iz varnostnih razlogov so predvsem države, ki so bile tudi »zaveznice« v času hladne vojne. Za razvoj in uporabo lasnih operacijskih sistemov so se odločile Kitajska, Venezuela, Severna Koreja in Kuba. Te države so si tudi ideološko precej blizu in so tradicionalno sumničave do zahoda predvsem do ZDA.

8 Razkritja Edwarda Snowdna

Edward Snowden je bivši pogodbeni sodelavec NSA, ki je v javnost dal strogo zaupne podatke o prisluškovanjih in zbiranju podatkov NSA. Za enkrat je objavil za približno 1.5 milijona dokumentov preko različnih svetovnih časopisov, kot so The Guardian, The Washington Post, Le Monde, Der Spiegel, L'espresso in še mnogo drugih. 6 junija 2013 je časopis The Guardian istočasno s časopisom The Washington Post, objavil članek v katerem Edward Snowden razkriva skrivne podatke, kako NSA na skrivaj pridobiva telefonske podatke preko operaterja Verizon. Takšno pridobivanje podatkov omogoča NSA Zakon o domovinski varnosti (ang. The Patriot Act). Dokumenti tudi razkrivajo, da se podatki pridobivajo tudi preko ostalih operaterjev, kot so AT&T in BellSouth. Vendar pa se razkritja Edwarda Snowdna niso končala tukaj. Do konca leta 2013 je preko različnih časopisov objavil še veliko več podatkov, katerih razkritja bom na kratko povzela v nadaljevanju.

- **Britanski the Guardian** je bil prvi, ki je objavil novice in tudi dokumente Edwarda. Največ preko novinarja Glenna Greewald, ki je razkril podatke programa Boundless Informant, ki ga uporablja NSA za sledenje količine podatkov, ki so v analizi skozi določeno časovno obdobje. Iz teh podatkov je razvidno, da so samo Avstralija, Kanada, Nova Zelandija in Združeno Kraljestvo izključeni iz napadov NSA (imenovanih »pet oči«). Glede na podatke so najbolj na udaru z napadi Irak, Kitajska, Saudska Arabija in znotraj EU Nemčija. V obdobju trideset dni je bilo preko sistema Boundless Informant zbranih 97 milijard podatkov (kot so IP naslovi, elektronska pošta, čas in kraj telefonskih klicev ...). Od tega je bilo 3 milijarde podatkov zbranih iz računalniških omrežij znotraj ZDA in približno 500 milijonov iz omrežij znotraj Nemčije (Greenwald 2013a). Iz The Guardian tudi izvemo da, je leta 2009 v času srečanja G-20 v Londonu Služba za vladne komunikacije, (Government Communications Headquarters GCHQ) prestregla komunikacijo tujih diplomatov (MacAskill 2013a). Ravno tako je preko programa Tempora prestregla velike količine podatkov preko optičnega omrežja in jih posredovala NSA. Podatki pridobljeni preko programa Tempora, so shranjeni tri dni, medtem, ko so metapodatki shranjeni trideset dni (MacAskill 2013b). Razkrije tudi obstoj programa XKeyscore, ki vladnim analitikom omogoča iskanje

pomembnih informacij znotraj velikih podatkovnih baz, kot so spletna pošta, zgodovina spletnega iskanja in podobno. Vse to lahko počno brez predhodne odobritve (Greenwald 2013b). Izvemo tudi, da Microsoft sodeluje z NSA. Razvil je sistem, ki mu omogoča prestrezanje kriptiranih sporočil v spletni pošti Outlook.com, še preden so ta kriptirana in jih posreduje sistemu NSA imenovanemu Prism (Greenwald 2013c); Prism je sistem, ki pobira uporabnikove podatke od različnih ponudnikov, kot so Microsoft, Yahoo, Google, Facebook, Paltalk, AOL, Skype, YouTube in Apple (Greenwald 2013a). Guardian razkrije tudi, da NSA sodeluje z velikimi tehnološkimi podjetji, z namenom uporabe slabšega kriptiranja v programski opremi in vnosom varnostnih lukenj (Greenwald 2013č); da je NSA večkrat želela vdreti v Tor anonimizacijsko omrežje z namenom pridobitve informacij o uporabnikih. Po večkratnih poskusih jim je uspelo z namestitvijo zlonamerne programske opreme. V nekaterih primerih je NSA celo uspelo preusmeriti uporabnika Tor iz anonimne mreže na nevarovane mreže, preko katerih so tudi lažje ugotovili identiteto posameznika (Greenwald 2013e).

Če nekako povzamemo ugotovitve The Guardian na hitro vidimo, da je časopis objavljal novice, ki so zadevale mednarodno skupnost Veliko Britanijo in ZDA in ne toliko lokalne novice, ki bi zadevale samo Veliko Britanijo. Razkril je obstoj programov Xkeyscore in Prism, kjer gre za zbiranje podatkov iz celega sveta.

Na drugi strani imamo nemški Der Spiegel, ki je kot bomo videli v nadaljevanju, objavljal bolj lokalne novice, ki so zadevale prisluškovanje v Nemčiji in Evropski Uniji.

- **Nemški Der Spiegel,** je objavil novico o vohunjenju NSA za diplomatskimi misijami Evropske Unije in njenimi delegati, vključno z delegacijo v Združenih narodih (Poitras in drugi 2013). Prisluškovali so tudi v stavbi Združenih Narodov v New Yorku (Neue NSA-Dokumente: US-Geheimdienst hörte Zentrale der Vereinten Nationen ab 2013). Prisluškovanja se niso končala tukaj saj so tudi celo nemški kanclerki Angeli Merkel prisluškovali in še ostalim 35 svetovnim voditeljem (Appelbaum 2013b); celo na strehi ameriške ambasade v Berlinu naj bi delovala »prisluškovalna postaja« (Embassy Espionage: The NSA's Secret Spy Hub in Berlin 2013). Iz Der Spiegel izvemo, da so tudi Nemške obveščevalne agencije imele dostop do programa

XKeyscore. Nemške obveščevalne agencije so tudi oskrbovale NSA z lastnimi podatki, v zameno za dostop do programov kot so XKeyscore ('Prolific Partner': German Intelligence Used NSA Spy Program 2013); Interno poročilo NSA razkrije ustanovitev delovne skupine za vdore v pametne telefone Iphone, Android in operacijski sistem Apple iOS. Podobno skupino ustanovi tudi Centralna britanska obveščevalna služba, z namenov vdora v telefone BlackBerry. Isto poročilo tudi razkrije obstoj majhnih programčkov imenovanih »skripti«, ki omogočajo nadzor 38 funkcij znotraj operacijskega sistema iOS 3 in iOS4, kot so določanje lokacije, glasovna sporočila, fotografije, Facebook, Yahoo! Messenger in Google Earth (Rosenbach 2013). Der Spiegel razkrije katalog NSA naprav in programske opreme, za vdiranje v računalniške sisteme in prisluškovanje. Naprave so zmožne zajeti sliko zaslona računalnika in uporablja se tudi USB ključek, ki istočasno oddaja podatke preko zračnih valov in še mnoge druge (Appelbaum 2013c); NSA je skupaj z FBI (Federal Bureau of Investigation) tudi prestrezal pošiljke strojne opreme in računalnikov z namenom, da je v njih namestil vohunsko opremo za nadzor in prisluškovanje (Appelbaum 2013a).

Novic nista objavljala samo sledeča medija, ampak tudi bolj lokalni mediji, ki so objavljali specifične članke nanašajoč se na državo iz katere prihaja medij.

- **Južnokitajski časopis South China Morning** objavi**,** da je NSA vdrla v več Kitajskih mobilnih operaterjev in pridobila podatke njihovih uporabnikov (EXCLUSIVE: US spies on Chinese mobile phone companies, steals SMS data: Edward Snowden 2013); Vdrli so tudi v Kitajsko Univerzo v Hong Kongu in Univerzo Tsinghua v Pekingu (Lam 2013a) in leta 2009 so vdrli so v Pacnet (Azijski ponudnik optičnega omrežja) (Lam 2013b).
- **Avstralski Sunday Morning Herrald** razkrije, da sta tudi Avstralija in Nova Zelandija oskrbovali NSA z podatki, ki sta jih sami zasegli (Dorling 2013).
- **Ameriški the Washington Post** objavi, da NSA v ZDA razvija zelo zmogljiv »kvantni« računalnik, ki naj bi imel zmožnost vdreti v vsak tip šifriranih podatkov. Celoten projekt naj bi stal 79,7 milijona ameriških dolarjev. Ko bo enkrat računalnik dokončno zgrajen, bo omogočal NSA, dostop do vseh

šifriranih podatkov (kreditne kartice, banke, zdravstveni podatki in še mnoge druge) (Rich 2013).

- **Nemški Süddeutsche Zeitung** razkrije kako so telekomunikacijska podjetja Verizon Business, British Telecomunications, Vodafone Cable, Global Crossing, Level 3, Viatel in Interoute pomagala Centrali britanske obveščevalne službe, da se je priklopila na optična omrežja in prestrezala promet (spletna pošta, podatki, klici, obiske spletnih strani in sporočila). Zaradi same razvejanosti omrežja, lahko prestrezajo promet po skorajda celotni EU (Goetz 2013).

Vsa ta razkritja so močno zamajala odnose med ZDA in ostalimi državami. Vse prizadete države so v javnih sporočilih obsodila dejanja NSA in sprenevedanje ZDA (West 2013). Morda se je še najbolj ostro odzvala na razkritja Nemčija in njena kanclerka Angela Merkel, ki je primerjala dejanja NSA s Stasi (Staatssicherheit - državnovarnostna služba v Nemški demokratični republiki) in je bila ogorčena ker je do tedaj veljalo načelo, da se med zavezniki ne prisluškuje (Traynor 2013). Kanclerka Merkel je obljubila državljanom sprejetje pogodbe, ki bi prepovedovala vohunjenje za nemškimi državljani, vendar ni dovolj posluha za podpis takšne pogodbe s strani ZDA (Veit in Meiritz 2014). Razkritje, da naj bi Apple sodeloval z NSA, je privedlo tudi do tega, da sta dve največji nemški stranki Krščanski demokrati in Socialni demokrati sprejeli smernice, ki zapovedujejo uporabo šifrirnih telefonov za vse pomembnejše politike v državi. To pomeni, da s tem prepovedujejo uporabo Iphone telefonov, ker ne zadoščajo varnostnim kriterijem, ki sta jih sprejeli stranki (Apple repealed: German politicians to use encrypted phones to block NSA spying 2013). Tudi posamezniki so izgubili zaupanje v velika podjetja, kot so Microsoft in Apple, ko so zvedeli, da le-ta sodelujejo z NSA pri razvoju programske opreme z namenom nadzora uporabnika (West 2013).

8.1 Posledice razkritij Edward Snowdna za OKPO

Vsa razkritja so privedla, da je vedno več ljudi začelo razmišljati o uporabi odprtokodne programske opreme ravno iz varnostnih razlogov. Težko sicer trdimo ali je bolj varna odprtokodna ali zaprtokodna programska oprema, vendar pa nam OKPO omogoča vpogled in njeno spreminjanje po naših željah. Ravno argument večjega nadzora nad lastnimi sistemi in neodvisen razvoj lastnih sistemov, je prepričal Nemčijo po razkritjih, da je ob vnovični zmagi Angele Merkel na volitvah 2013 napisala v koalicijsko pogodbo sledeče:

- Cilj nove vlade je, da obdrži ključno tehnologijo proizvajano v Nemčiji oziroma v Evropi.
- Vlada se bo zavzemala za večjo uporabo OKPO v Nemčiji in Evropski Uniji.
- Vedno, ko se bo kupovalo novo programsko ali strojno opremo bodo morali proučiti tudi odprtokodne rešitve. Prednost pri izboru bodo imele rešitve, ki bodo cenovno učinkovite in bodo imele inovativni potencial.
- Večjo globalno konkurenčnost želijo doseči z razvojem lastne programske opreme »programska oprema narejena v Nemčiji«. Cilj je izboljšati varnost lastne programske opreme, izboljšati varovanje podatkov in jo narediti uporabniku bolj prijazno in jo prilagoditi njegovim potrebam.
- OKPO bo imel prioriteto pri uporabi v analiziranju varnosti informacijske tehnologije, ker omogoča izmenjavanje ugotovitev in ponovno uporabo rezultatov in rešitev.
- Vsi vladni dokumenti bodo objavljeni tudi v odprtokodnih formatih (Deutschlands Zukunft gestalten 2013).

Kot vidimo iz koalicijske pogodbe Nemčije, bo le-ta usmerjala svoj tehnološki razvoj in konkurenčnost ravno z razvojem lastne programske opreme in proizvodnjo ključne tehnologije v Nemčiji, ali vsaj znotraj Evrope tudi iz varnostnih razlogov. Podobne tendence najdemo tudi v drugih državah, kot so Kitajska, ki razvija lastne procesorje in ima tendence zgraditi super računalnik, ki bo v celoti iz delov narejenih na Kitajskem (Thibodeau 2013). Trend je v razvoju lastne tehnologije, ki ji z razvojem tudi lastne programske opreme dodamo večjo dodano vrednost. In kje je na tem področju Slovenija. Trenutno smo bolj daleč od takšnih velikih razvojnih projektov v

informacijski tehnologiji. Vendar pa ni bilo vedno tako, imeli smo podjetje Iskra Delta, ki je veliko vlagalo v razvoj lastne programske opreme in rešitve. Lasten razvoj jim je tudi omogočal konkurenčno postavljanje cen in prodor na svetovne trge, kot so Kitajska, Indija ipd.

9 Sklep

Hladna vojna se je uradno končala s padcem berlinskega zidu 9. novembra 1989. Vendar ali se je res takrat končala. Posledice oboroževanja in vohunjenja so pustile na ljudeh globok pečat. Jasen upor zoper nadzorovanje njihove zasebnosti so 15. januarja 1990 ljudje pokazali z vdorom v nemški Stasi, ker je ta želel uničiti vso dokumentacijo, ki jo je na prikrit način dobil. Jeza do tajnih služb se je razplamtela tudi po ostalih državah bivšega Vzhodnega bloka. Po razpadu Sovjetske zveze so mnoge države postale samostojne in demokratične. Ustanovile so posebne Komisije za nadzor nad tajnimi službami in spisale zakone za nadzor tajnih služb z namenom, da se kaj takega, kot se je dogajalo med hladno vojno nikdar več ne zgodi. Tajni dokumenti so s časoma postali javni. Ljudje so videli nov začetek in svetlejšo prihodnost po koncu hladne vojne. Po koncu hladne vojne se je začel skokovit razvoj informacijske tehnologije. Svet je postal med seboj bolje povezan. Razdalje med ljudmi so se zmanjšale na en »klik« na računalniški miški. Kar naenkrat nam je vse postalo na dosegu roke. Vendar smo z razkritji Edwarda Snowdna spoznali, da ima tudi to svojo temno plat. Mnogi ljudje so se ob razkritjih spomnili nepooblaščenih vdorov v njihovo zasebnost iz časa hladne vojne. Vendar pa so se opozarjanja, da v svetu poteka »kibernetska hladna vojna« s strani strokovnjakov pojavljala že mnogo prej. Saj so prihajala na dan mnoga poročila o vdorih v računalniške sisteme in kraje podatkov neke države. Z analiziranjem napadov so strokovnjaki velikokrat ugotovili, da za napadi stoji neka druga država. Največ poročanja so bili deležni vdori s strani ZDA in Kitajske, ki sta največ vdirali ena drugi. V nadaljevanju bom potrdila hipotezo **H1: V svetu poteka »kibernetska hladna vojna«, ki postaja vedno bolj „vroča“ in katere del je tudi OKPO**. Če najprej primerjamo hladno vojno s »kibernetsko hladno vojno« ugotovimo naslednje. Razlike v obeh tipih vojn najdemo predvsem v »orožju«. Če je nekoč za glavno orožje hladne vojne s katerim so države ustrahovale druga drugo bilo jedrsko orožje, je to danes informacijska tehnologija. Podobnost najdemo na področju pravnih aktov. V času hladne vojne so države omejevale oboroževanje s pogodbami, kot so SALT in START. Tudi danes države sprejemajo vedno več pogodb, ki omejujejo in sankcionirajo kibernetsko oboroževanje in bojevanje v kibernetskem svetu. Ključna razlika je v samem strošku proizvodnje takšnega orožja. Vrednosti jedrskega orožja so se štele v milijonih in milijardah,

medtem, ko lahko s preprosto zlonamerno programsko opremo naredimo gromozansko škodo. Razlika je tudi v samem dupliciranju orožja. Jedrskega orožja ne moremo preprosto duplicirati z enim »klikom«, kot to lahko naredimo z zlonamerno programsko opremo, s čemer tudi veliko finančno prihranimo. Podobnost najdemo tudi v načinu bojevanja, ki je »hladen«. Vključuje krajo informacij in vohunjenje z namenom pridobitve tehnološke ali kakšne druge prednosti ter uporaba »posrednikov«. V času hladne vojne sta velesili bili boj preko posredniških vojn na tujih ozemljih (Vietnam, Koreja ...). Danes se dogaja podobno saj države uporabljajo »posrednike« za kibernetske napade, kot so hekerji s čimer se lažje izognejo mednarodnim sankcijam. Podobnost najdemo tudi na področju zaščite civilistov, ki so podobno, kot v času hladne vojne tudi v času »kibernetske hladne vojne« bolj prepuščeni samemu sebi na področju zaščite pred napadi. V času hladne vojne je bila dominantna strategija odvračanje od napada z zagotovim uničenjem obeh strani. V primeru kibernetskih napadov je tudi v uporabi vedno bolj strategija odvračanja z izgradnjo novih kibernetskih varnostnih centrov, vzpostavitvijo kibernetskih vojaški oddelkov in sprejetjem pravnih aktov, ki sankcionirajo takšna dejanja. Razliko najdemo na področju akterjev. V času hladne vojne sta bila nekako samo dva akterja. V obdobju »kibernetske hladne vojne« pa je akterjev več, saj poleg državnih akterjev sodelujejo tudi nedržavni akterji, ki lahko na skrivaj delajo v resnici s podporo neke države.

Hipotezo tudi potrjujem v točki, da »kibernetska hladna vojna« postaja vedno bolj »vroča«. Primer Stuxnet napada je marsikomu pognal strah v kosti, saj nam je pokazal česa vse je dejansko zmožna zlonamerna programska oprema. V primeru Stuxneta bi lahko dejansko prišlo do jedrske eksplozije, če bi uporabili v napadu drugo različico zlonamerne programske opreme, ki bi zaprla ventile jedrske elektrarne. Efekt uničenja bi bil podoben atomski bombi le s to razliko, da vojski ki bi sicer morala odvreči atomsko bombo sploh ne bi bilo potrebno prestopiti meje države, ki jo napada.

Hipotezo potrjujem tudi na področju uporabe OKPO znotraj »kibernetske hladne vojne«. OKPO nastopa v ofenzivni in defenzivni vlogi. OKPO je lahko ofenzivna. Prva zlonamerna programska oprema Morris črv je bila odprtokodne narave. Države lahko in tudi razvijajo odprtokodne programske rešitve zlonamerne programske opreme. Vendar je v primeru »kibernetske hladne vojne« veliko bolj defenzivne narave, saj se zanjo odločajo države, ki si želijo same zaščititi informacijsko infrastrukturo in kritično

infrastrukturo na nacionalni ravni. OKPO jim omogoča večjo transparentnost in neodvisnost od drugih držav pri samem razvoju programske opreme in predvsem prihranek stroškov. Pred razkritji Edward Snowdna se je večina držav odločala za prehod na OKPO predvsem iz finančnega stališča, kot je to storilo mesto München. Razkritja so prinesla informacije, da velika podjetja, kot so Microsoft, Google, Facebook, Skype in Apple sodelujejo z NSA pri razvoju programske opreme. S svojo programsko opremo omogočajo NSA pridobivanje uporabnikovih podatkov in vohunjenje za njimi. Po razkritjih so nekatere države, kot je Nemčija zelo spremenile politiko do zaprtokodne programske opreme in začele močno podpirati OKPO tudi zaradi želje po večji neodvisnosti od zaprtokodnih sistemov in Amerike. Nemčija je celo v koalicijsko pogodbo napisala, da se bo država zavzemala za večjo uporabo OKPO.

OKPO pa ne omogoča neodvisnosti samo državam od velikih podjetij in drugih držav. Omogoča tudi neodvisnost posameznika od države, zato je vedno bolj tudi v uporabi pri političnih aktivistih, ki so preganjani s strani držav. Uporaba Tor, OcupyyOs in drugih načinov, ki jim omogočajo, da zaobidejo vladno vohunjenje in nemoteno ter šifrirano komunicirajo s svojimi podporniki.

Želja po večji neodvisnosti se ne konča tukaj. Če pogledamo primer Iskra Delta iz časa hladne vojne. To je bilo podjetje, ki je v času najostrejše hladne vojne začelo prodajati cenejše računalnike, temelječe na ameriških komponentah podjetja DEC. Kmalu so začeli razvijati lasten računalnik, ki bi imel čim manj tujih komponent. Razvijali so lastno programsko opremo in rešitve. Vsakemu računalniku, ki so ga sestavili in mu dodali lastno programsko opremo, so dodali izjemno dodano vrednost. Njihove rešitve so opazile največje države, kot so Amerika, Kitajska, Indija, Japonska in Avstralija. Bili so mnogo cenejši v svoji ponudbi od največjih ponudnikov, kot je IBM. Z razvojem lastne programske opreme, so reševali probleme in našli rešitve, ki so se za tiste čase zdele fikcija. Dobivali so milijonska naročila in če bi še danes obstajali bi verjetno tudi Slovenija imela danes svojo Silicijevo dolino. A zataknilo se je, ker so se znašli v primežu hladne vojne. ZDA so imele zelo strogo politiko glede izvoza in prodaje visoko tehnoloških izdelkov na Vzhod. Na drugi strani pa je Vzhod želel njihove rešitve, ki so bile veliko cenejše in so omogočale Vzhodu preko njih priti do visoko tehnoloških izdelkov. Zahod je pritiskal na njih, da morajo ukiniti razvojni oddelek, ki je razvijal lastno programsko opremo in raje preiti na ameriške licenčne

rešitve. Vzhod je, kot sredstvo moči uporabil denar in začel zadrževati z izplačili za dobavljeno blago.

Zakaj je ta zgodba za nas tako pomembna. Lasten razvoj, ki da dodano vrednost. Tega se zelo zaveda Nemčija, ki je to vpisala v koalicijsko pogodbo, da bo vsa ključna tehnologija proizvedena v Nemčiji ali vsaj v Evropi. Že v času hladne vojne so države vgrajevale zlonamerno programsko opremo v strojno opremo z namenom vohunjenja in nadzorovanje sistema. Danes ni nič drugače. Edward Snowden je to tudi razkril v svojih poročilih. Po razkritjih so se mnoge države, kot je Nemčija odločile, da bodo prednost dale lastnemu razvoju strojne in programske opreme. Le na ta način si lahko zagotovijo neoporečnost sistemov. Nemčija vidi prednost na tem področju ravno v OKPO, ker ji omogoča neodvisno razvijanje programske opreme, direktni vpogled v izvorno kodo, cenejša je in javno se objavljajo vse ranljivosti in pomanjkljivosti. Globalno konkurenčnost svojih produktov, kot to zapiše v koalicijski pogodbi, Nemčija lahko doseže samo z naprednimi in cenovno konkurenčnimi izdelki.

Slovenija se je trenutno znašla v gospodarski krizi. Izhod iz krize je inovacija in proizvodnja izdelkov z dodano vrednostjo. Morda bi bilo smiselno, da tudi Slovenija prouči OKPO in kakšen bi imela vpliv na gospodarstvo. Nekoč smo že imeli visoko tehnološko podjetje Iskra Delta, ki je konkuriralo na svetovnem tržišču. Tudi danes imamo nekaj podjetij, ki so ravno zaradi svojih inovacij v samem svetovnem vrhu. Naj nas zgodovina nauči, da ne ponovimo podobnih napak. Prihodnost je v lastnem razvoju.

10 Literatura

- *About DuckDuckGo*. 2013. Dostopno prek: https://duckduckgo.com/about (12. december 2013).
- *AFP*. 2010. *Russia to create 'Windows rival'*. Dostopno prek: http://www.google.com/hostednews/afp/article/ALeqM5ghjg_tT6QzNQjXXT5HCKrIvCUMKQ?docId=CNG.649f81a02bcbfc0e7603d630f2ab1828.511 (11. december 2013).
- Appelbaum, Jacob. 2013a. *Berlin Complains: Did US Tap Chancellor Merkel's Mobile Phone?* Dostopno prek: http://www.spiegel.de/international/world/merkel-calls-obama-over-suspicions-us-tapped-her-mobile-phone-a-929642.html (20. januar 2014).
- --- 2013b. *Berlin Complains: Did US Tap Chancellor Merkel's Mobile Phone?* Dostopno prek: http://www.spiegel.de/international/world/merkel-calls-obama-over-suspicions-us-tapped-her-mobile-phone-a-929642.html (20. januar 2014).
- --- 2013c. *Shopping for Spy Gear: Catalog Advertises NSA Toolbox.* Dostopno prek: http://www.spiegel.de/international/world/catalog-reveals-nsa-has-back-doors-for-numerous-devices-a-940994.html (20. januar 2014).
- *Apple repealed: German politicians to use encrypted phones to block NSA spying*. 2013. Dostopno prek: http://rt.com/news/german-politicians-encrypted-phones-132/ (20. januar 2014).
- Arquilla, John in David Ronfeldt. 1993. 'Cyber war is Coming!' *Comparative Strategy* 12 (2): 31–32.
- --- 2012. *'Cyberwarfare Is Already Upon Us' Foreign PolicyMarch/April*. Dostopno prek: http://www.foreignpolicy.com/articles/2012/02/27/cyberwar_is_already_upon_us (12. december 2013).
- Barnes, Elmer Harry. 1972. *Pearl Harbor after a Quarter of a Century*. New York: Arno Press.
- Blanchard, F. Jean-Marc. 2007. China, multinational corporations, and globalization: beijing and Microsoft battle over the opening of China's gates. V

Asian perspective, ur. Jean-Marc F. Blanchard, 67–102 Seoul: Institute for Far Eastern Studies.

- *Blender.* 2014. Dostopno prek: http://www.blender.org/ (12. januar 2014).
- Bolle, Maja. 2011. Odprtokodna programska oprema in informacijska varnost. *Sodobni vojaški izzivi* 13 (3): 61–79.
- Boon-Lock, Yeo, Loisa Liu in Sunil Saxena. 2006. When China Dances with OSS. V *Open Sources 2.0: The Continuing Evolution*, ur. Chris DiBona, Mark Stone in Danese Cooper, 197–210. Kalifornija: O'Reilly Media.
- Brvar, Bogo. 1982. Pojavne oblike zlorabe računalnika. *Revija za kriminalistiko in kriminologijo* 33 (2): 92–104.
- *Bugs: Ubuntu .*2014. Dostopno prek: https://bugs.launchpad.net/ubuntu (1. januar 2014).
- Campbell, Duncan. 1999. *NSA Backdoor Into Windows*. Dostopno prek: http://www.theforbiddenknowledge.com/hardtruth/nsa_backdoor_windows.htm (12. marec 2011).
- --- 2013. *Revealed: Britain's 'secret listening post in the heart of Berlin'*. Dostopno prek: http://www.independent.co.uk/news/uk/home-news/revealed-britains-secret-listening-post-in-the-heart-of-berlin-8921548.html (20. januar 2014).
- CBSNEWS. 2010. *Iran Confirms Stuxnet Worm Halted Centrifuges*. Dostopno prek: http://www.cbsnews.com/stories/2010/11/29/world/main7100197.shtml (20. februar 2012).
- Chuvakin, Anton. 2003. *An Overview of Unix Rootkits.* Dostopno prek: http://www.rootsecure.net/content/downloads/pdf/unix_rootkits_overview.pdf (12. januar 2014).
- Clarke, A. Richard. 2010. *The Next Threat to National Security and What to Do About It*. New York: HarperCollins Publishers.
- Clausewitz, Carl von. 1985. *O vojni*. Časopis za kritiko znanosti 75/76. Ljubljana: Tiskarna Kresija.
- Cleto, A. Sojo. 2004. *Venezuela Embraces Linux and Open Source Software, but Faces Challenges*. Dostopno prek: http://venezuelanalysis.com/news/827 (3. maj 2011).

- *CNSS Instruction No. 4009*. 2010. Dostopno prek: http://www.ncix.gov/publications/policy/docs/CNSSI_4009.pdf (12. januar 2014).
- Cornish, Paul, David Livingstone, Dave Clemente in Claire Yorke. 2010. *On cyber warfare*. London: The Royal Institute of International Affairs.
- *Cybercrime*. 2013. Dostopno prek: http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/default_en.asp (20. januar 2014).
- Danchev, Dancho. 2009. *China's 'secure' OS Kylin - a threat to U.S offensive cyber capabilities?* Dostopno prek: http://www.zdnet.com/blog/security/chinas-secure-os-kylin-a-threat-to-u-s-offensive-cyber-capabilities/3385 (20. januar 2012).
- *December.* 2013. Dostopno prek: http://www.w3counter.com/globalstats.php (1. januar 2014).
- *Decreto N° 3.390.* 2004. Dostopno prek: http://asl.mct.gob.ve/images/Marco_legal/decreto3390.pdf (20. maj 2011).
- *Defense Russian Military Creating Cyber Warfare Branch.* 2013. Dostopno prek: http://en.ria.ru/military_news/20130820/182856856.html (1. januar 2014).
- *Definition*. 2013. Dostopno prek: http://searchsecurity.techtarget.com/definition/cyberwarfare (2. januar 2014).
- Denning, Dorothy. 2000. Reflections on Cyberweapons Controls. *Computer Security Journal* 16 (4): 43–53.
- --- 2012. Stuxnet: What Has Changed? *Future Internet* 4 (3): 672–687.
- *Deutschlands Zukunft gestalten*. 2013. Dostopno prek: http://www.bundesregierung.de/Content/DE/_Anlagen/2013/2013-12-17-koalitionsvertrag.pdf?__blob=publicationFile&v=2 (20. januar 2014).
- DeWalt, Dave. 2009. *McAfee Virtual Criminology Report 2009*. Dostopno prek: http://www.csg.ethz.ch/education/lectures/ManSec/HS2013/VCR (2. februar 2012).
- *Distrowatch.com.* 2013. Dostopno prek: http://distrowatch.com/ (12. januar 2013).

- Domingo, Francis Rico. 2012. *Chinese Cyber Warfare and its Implications on Selected Southeast Asian States*. Dostopno prek: http://icaps.nsysu.edu.tw/ezfiles/122/1122/img/1421/40.pdf (12. januar 2014).
- Dorling, Philip. 2013. *Snowden reveals Australia's links to US spy web*. Dostopno prek: http://www.smh.com.au/world/snowden-reveals-australias-links-to-us-spy-web-20130708-2plyg.html#ixzz2pYVvgZhP (20. januar 2014).
- Dredge, Stuart. 2013. *What is Tor? A beginner's guide to the privacy tool*. Dostopno prek: http://www.theguardian.com/technology/2013/nov/05/tor-beginners-guide-nsa-browser (20. januar 2014).
- Dressler, Joshua. 2007. *"United States v. Morris". Cases and Materials on Criminal Law*. St. Paul, MN: Thomson/West.
- *Embassy Espionage: The NSA's Secret Spy Hub in Berlin*. 2013. Dostopno prek: http://www.spiegel.de/international/germany/cover-story-how-nsa-spied-on-merkel-cell-phone-from-berlin-embassy-a-930205.html (17. januar 2014).
- *Enabling and using the "root" user in Mac OS X*. 2014. Dostopno prek: http://support.apple.com/kb/ht1528 (21. januar 2014).
- Espiner, Tom. 2006. *Trend Micro: Open source is more secure*. Dostopno prek: http://news.cnet.com/2100-7355_3-6083490.html (20. januar 2013).
- --- *2010. Microsoft opens source code to Russian secret service.* Dostopno prek: http://tinyurl.com/2w8moaq *(3. januar 2013).*
- Essers, Loek. 2013. *Munich open source switch 'completed successfully'*. Dostopno prek: http://www.cio.co.uk/news/change-management/munich-open-source-completed-successfully/ (20. januar 2014).
- *EXCLUSIVE: US spies on Chinese mobile phone companies, steals SMS data: Edward Snowden.* 2013. Dostopno prek: http://www.scmp.com/news/china/article/1266821/us-hacks-chinese-mobile-phone-companies-steals-sms-data-edward-snowden (20. januar 2014).
- Farell Paul. 2013. *History of 5-Eyes – explainer.* Dostopno prek: http://www.theguardian.com/world/2013/dec/02/history-of-5-eyes-explainer (20. januar 2014).
- Finley, Klint. 2013. *People's Republic of Open Source: China Preps National Linux Distro.* Dostopno prek:

http://www.wired.com/wiredenterprise/2013/03/ubuntu-china/ (20. december 2013)

- Gallagher, Sean. 2013. *US, Russia to install "cyber-hotline" to prevent accidental cyberwar*. Dostopno prek: http://arstechnica.com/information-technology/2013/06/us-russia-to-install-cyber-hotline-to-prevent-accidental-cyberwar/ (12. december 2013).
- Geer, Daniel, Rebecca Bace, Peter Gutmann, Perry Metzger, Charles P. Pfleeger, John S. Quarterman in Bruce Schneier. 2003. *CyberInsecurity: The Cost of Monopoly How the Dominance of Microsoft's Products Poses a Risk to Security.* Dostopno prek: http://www.ccianet.org/papers/cyberinsecurity.pdf (18. november 2012).
- Geers, Keneth. 2007. *Cyberspace Changing Nature of Warfare - Black Hat*. Dostopno prek: http://www.blackhat.com/presentations/bh-jp-08/bh-jp-08-Geers/BlackHat-Japan-08-Geers-Cyber-Warfare-Whitepaper.pdf (2. januar 2014).
- Germain, M. Jack. 2008. *Linux: A Tempting Target for Malware?* Dostopno prek: http://www.linuxinsider.com/story/62275.html (1. junij 2013).
- Goetz, John. 2013. *British Officials Have Far-Reaching Access To Internet And Telephone Communications.* Dostopno prek: http://international.sueddeutsche.de/post/59603415442/british-officials-have-far-reaching-access-to-internet (20. januar 2014).
- Gonzalez-Barahona, M. Jesus in Gregorio Robles. 2006. Libre Software in Europe. V *Open Sources 2.0: The Continuing Evolution*, ur. Chris DiBona, Mark Stone in Danese Cooper, 161–189. Kalifornija: O'Reilly Media.
- Gorman, Siobhan. 2009. *Electricity Grid in U.S. Penetrated By Spies*. Dostopno prek: http://online.wsj.com/news/articles/SB123914805204099085 (11. maj 2012).
- --- 2010. *U.S. Backs Talks on Cyber Warfare*. Dostopno prek: http://online.wsj.com/news/articles/SB10001424052748703340904575284964215965730 (11. december 2013).
- Gray, Collin. 2005. *Another Blood Century Future Warfare*. London: Orion Book Ltd.

- Greenberg, Andy. 2009. *Sketching Obama's Cyberplans*. Dostopno prek: http://www.forbes.com/2009/02/20/paul-kurtz-security-technology-security_kurtz.html (12. februar 2013).
- Greenwald, Glenn. 2013a. *Boundless Informant: the NSA's secret tool to track global surveillance data*. Dostopno prek: http://www.theguardian.com/world/2013/jun/08/nsa-boundless-informant-global-datamining (2. januar 2014).
- --- 2013b. *XKeyscore: NSA tool collects 'nearly everything a user does on the internet'*. Dostopno prek: http://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data (2. december 2013).
- --- 2013c. *Microsoft handed the NSA access to encrypted messages.* Dostopno prek: http://www.theguardian.com/world/2013/jul/11/microsoft-nsa-collaboration-user-data (20. januar 2014).
- --- 2013č. *Revealed: how US and UK spy agencies defeat internet privacy and security*. Dostopno prek: http://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security (20. januar 2014).
- --- 2013d. *NSA and GCHQ target Tor network that protects anonymity of web users.* Dostopno prek: http://www.theguardian.com/world/2013/oct/04/nsa-gchq-attack-tor-network-encryption (1. januar 2014).
- --- 2013e. *NSA Prism program taps in to user data of Apple, Google and others.* Dostopno prek: http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data (2. januar 2014).
- Hamilton, Stuart. 2013. *The Struggle To Scale: Keeping Up with the Internet.* Dostopno prek: http://www.ifla.org/files/assets/faife/publications/spotlights/5.%20CASE03-Google.pdf (20. januar 2014).
- Holt, Richard. 2013. *China develops national open-source operating system.* Dostopno prek: http://www.telegraph.co.uk/technology/news/9948817/China-develops-national-open-source-operating-system.html (11. januar 2014).
- Humphrey, Benjami. 2011. *The Evolution of the Personal Package Archive system.* Dostopno prek: http://www.omgubuntu.co.uk/2011/05/the-evolution-of-the-personal-package-archive-system (12. januar 2014).
- *Internet World Stats. 2014.* Dostopno prek:

http://www.internetworldstats.com/stats.htm (20. januar 2014).

- Israel, Esteban. 2009. *Cuba launches own Linux variant to counter U.S.* Dostopno prek: http://www.reuters.com/article/2009/02/11/us-cuba-software-idUSTRE51A77S20090211 (11. december 2013).
- Jose, Manuel. 2011. *The Goal is 200 Million Ubuntu Users in 4 Years - Mark Shuttleworth*: Dostopno prek http://www.techdrivein.com/2011/05/goal-is-200-million-ubuntu-users-in-4.html (23. 1. 2014).
- Kahlili, Reza. 2013. *Iran to sue U.S. over 'Stuxnet' Sabotage*. Dostopno prek: http://www.wnd.com/2013/07/iran-u-s-sabotaged-our-nuke-program/ (20. januar 2014).
- Kane, Margaret. 2002. *US Vulnerable to Data Sneak Attack*. Dostopno prek: http://news.cnet.com/2100-1017-949605.html (20. junij 2012).
- *Kaspersky Security Bulletin 2012*. 2012. Dostopno prek: http://www.securelist.com/en/analysis/204792255/Kaspersky_Security_Bulletin_2012_The_overall_statistics_for_2012#2 (12. januar 2014).
- *Kaspersky security bulletin 2013.* 2013. Dostopno prek: http://media.kaspersky.com/pdf/KSB_2013_EN.pdf (12. januar 2014).
- Kassakian, G. John. 2011. *MIT STUDY ONTHE FUTURE OF THE ECTRIC GRID*. Dostopno prek: http://mitei.mit.edu/system/files/Electric_Grid_Full_Report.pdf (20. januar 2014).
- Kimberly, Simon. 2005. The value of open standards and open-source software in government environments. *IBM SYSTEMS JOURNAL* 44 (2): 227–238.
- Koetzle, Laura. 2004. *Is Linux More Secure Than Windows?* Dostopno prek: http://carlosversati.googlecode.com/svn-history/r4/trunk/tcc/papers/LinuxWindowsSecurity.pdf (20. julij 2013).
- Kovačič, Matej. 2006. Kriptografija, anonimizacija in odprta koda kot boji za svobodo na internetu. *Javnost - the public* 13: 93–110.
- Kravets, David. 2014. *Federal Court Guts Net Neutrality Rules*. Dostopno prek: http://www.wired.com/threatlevel/2014/01/court-kills-net-neutrality/ (24. januar 2014).

- Krepinevich, Andrew. 2012. *Cyber warfare: a »nucler option«?* Dostopno prek: http://tinyurl.com/kh2pabn (12. januar 2014).
- Kshetri, Nir. 2005. Economics of Linux Adoption and Developing Countries. *IEEE Software* 21 (1): 74–81.
- Lam, Lana. 2013a. *EXCLUSIVE: NSA targeted China's Tsinghua University in extensive hacking attacks, says Snowden.* Dostopno prek: http://www.scmp.com/news/china/article/1266892/exclusive-nsa-targeted-chinas-tsinghua-university-extensive-hacking (20. januar 2014).
- --- 2013b. *EXCLUSIVE: US hacked Pacnet, Asia Pacific fibre-optic network operator, in 2009*. Dostopno prek: http://www.scmp.com/news/hong-kong/article/1266875/exclusive-us-hacked-pacnet-asia-pacific-fibre-optic-network-operator (20. januar 2014).
- Laurie, Ben. 2006. Open Sources and Security. V *Open Sources 2.0: The Continuing Evolution*, ur. Chris DiBona, Mark Stone in Danese Cooper, 57–71. Kalifornija: O Reilly Media.
- Leffler, Melvyn. 2010. *THE CAMBRIDGE HISTORY OF THE COLD WAR*. Volume I, II in III. New York: Cambridge University Press.
- Lewis, A. James. 2005. *Computer Espionage, Titan Rain and China*. Dostopno prek: http://csis.org/files/media/csis/pubs/051214_china_titan_rain.pdf (12. julij 2013).
- --- 2006. *Government Open Source Policies - Avgust 2007*. Dostopno prek: http://csis.org/files/media/csis/pubs/070820_open_source_policies.pdf (12. julij 2011).
- Libicki, Martin. 2007. *Conquest in Cyberspace National Security and Information Warfare*. Cambridge: Cambridge University Press.
- --- 2012. 'Cyberspace Is Not a Warfighting Domain'. *I/S: A Journal of Law and Policy for the Information Society* 8 (2): 321–336.
- *Licenses*. 2014. Dostopno prek: http://www.gnu.org/licenses/licenses.html (18. januar 2014).
- *Linux malware detect.* 2014. Dostopno prek: https://www.rfxn.com/projects/linux-malware-detect/ (12. januar 2014).

- *LinuxGizmos.com*. 2014. Dostopno prek http://linuxgizmos.com (1. januar 2014)
- MacAskill, Ewen. 2013a. GCHQ *intercepted foreign politicians' communications at G20 summits*. Dostopno prek: http://www.theguardian.com/uk/2013/jun/16/gchq-intercepted-communications-g20-summits (3. januar 2014).
- --- 2013b. *GCHQ taps fibre-optic cables for secret access to world's communications*. Dostopno prek: http://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa (2. januarja 2014).
- *Malware.* 2014. Dostopno prek: http://www.techterms.com/definition/malware (17. januar 2014).
- *McAfee A good decade of Cybercriminal.* 2010. Dostopno prek: http://www.mcafee.com/uk/resources/reports/rp-good-decade-for-cybercrime.pdf (15. maj 2013).
- McConnell, Mike. 2010. *To win the cyber-war, look to the Cold War*. Dostopno prek: http://www.washingtonpost.com/wp-dyn/content/article/2010/02/25/AR2010022502493.html (11. december 2011).
- *Microsoft in China: Clash of titans*. 2000. Dostopno prek: http://edition.cnn.com/2000/TECH/computing/02/23/microsoft.china.idg/ (20. december 2013).
- Mihajlovič, Novica. 2011. *Microsoft gre nad Pahorja, zdaj hoče pošteno konkurenco.* Dostopno prek: http://www.finance.si/305433/Microsoft-gre-nad-Pahorja-zdaj-ho%E8e-po%B9teno-konkurenco (24. december 2011).
- Morozov, Evgeny. 2011. *A Walled Wide Web for Nervous Autocrats*. Dostopno prek: http://online.wsj.com/article/SB10001424052748704415104576065641376054226.html (29. julij 2012).
- Mumford, Andrew. 2013. Proxy Warfare and the Future of Conflict. *The RUSI Journal* 158 (2): 40–46.
- Naraine, Ryan. 2010. *Microsoft knew of IE zero-day flaw since last September*. Dostopno prek: http://www.zdnet.com/blog/security/microsoft-knew-of-ie-zero-day-flaw-since-last-september/5324 (12. december 2013).

- *NCSA study.* 2010. Dostopno prek: http://tinyurl.com/nyo5lnb (12. december 2012).
- *Neue NSA-Dokumente: US-Geheimdienst hörte Zentrale der Vereinten Nationen ab.* 2013. Dostopno prek: http://www.spiegel.de/politik/ausland/nsa-hoerte-zentrale-der-vereinte-nationen-in-new-york-ab-a-918421.html (20. januar 2014).
- *No more desktop Linux systems in the German Foreign Office.* 2011. Dostopno prek: http://www.linuxtoday.com/it_management/2011021700735NWDPMS (15. december 2012).
- O'Dowd, Dan. 2004. *White Paper: Linux in Defense.* Dostopno prek: http://www.ghs.com/linux/security.html (18. december 2013).
- Obel, Mike. 2013. *Chinese Army Cyber Warfare Unit Identified As Source Of Hacking Attacks Against US Targets - Report*. Dostopno prek: http://www.ibtimes.com/chinese-army-cyber-warfare-unit-identified-source-hacking-attacks-against-us-targets-report-1092614 (11. december 2013).
- *Ocena ekonomske upravičenosti MS EA za obdobje 2003-2005*. 2002. Dostopno prek: http://e-uprava.gov.si/eud/e-uprava/Studija%20upravicenosti%20MS%20EA.pdf / (23. julij 2012).
- *Open source observatory.* 2010. Dostopno prek: https://joinup.ec.europa.eu/community/osor/description (12. marec 2013).
- *PandaLabs Annual Report 2012.* 2012. Dostopno prek: http://press.pandasecurity.com/wp-content/uploads/2013/02/PandaLabs-Annual-Report-2012.pdf (11. januar 2014).
- Pandey, Nandan Sheo. 2010. *Hacktivism of Chinese Characteristics and the Google Inc. Cyber Attack Episode*. Berlin: ISPSW Publications. Institut für Strategie- Politik- Sicherheits- und Wirtschaftsberatung (ISPSW).
- Peeling, Nic in Julian Satchell. 2001. *Analysis of the Impact of Open Source Software*. Dostopno prek: http://www.math.unipd.it/~bellio/Analysis%2520of%2520the%2520Impact%2520of%2520Open%2520Source%2520Software.pdf (19. marec 2013).

- Poitras, Laura, Marcel Rosenbach, Fidelius Schmid in Holger Stark. 2013. *NSA horcht EU-Vertretungen mit Wanzen aus.* http://www.spiegel.de/netzwelt/netzpolitik/nsa-hat-wanzen-in-eu-gebaeuden-installiert-a-908515.html (20. 1. 2014).
- Political Contacts. 2011. Dostopno prek: http://www.rusemb.org.uk/policycontact/49 (2. december 2012).
- *Politika Vlade RS pri razvijanju, uvajanju in uporabi programske opreme in rešitev, temelječih na odprti kodi.* 2003. Dostopno prek: http://www.epractice.eu/files/media/media_312.pdf (20. junij 2011).
- Poulsen, Kevin. 2001. *Borland Interbase backdoor exposed. Open source reveals foolishly hardcoded password*. Dostopno prek: http://www.theregister.co.uk/2001/01/12/borland_interbase_backdoor_exposed/ (12. maj 2013).
- Prezelj, Iztok. 2001. Grožnje varnosti, varnostna tveganja in izzivi v sodobni družbi. *Teorija in praksa* 38 (1): 127–141.
- Proffitt, Brian. 2002. *Venezuela's Government Shifts to Open Source Software*. Dostopno prek: http://www.Linuxtoday.com/developer/2002083001126NWLLPB (15. marec 2011).
- *'Prolific Partner': German Intelligence Used NSA Spy Program*. 2013. Dostopno prek: http://www.spiegel.de/international/germany/german-intelligence-agencies-used-nsa-spying-program-a-912173.html (20. januar 2014).
- Rafati, Reza. 2011. *Anonymous Operating System: OccupyOS*. Dostopno prek: http://www.cyberwarzone.com/cyberwarfare/anonymous-operating-system-occupyos (17. december 2013).
- Rattaray, J. Gregory. 2001. *Strategic Warfare in Cyberspace* Massachusetts: MIT Press.
- Reed, John. 2012. *Chinese Spies Use Fake Facebook Pages to Gain Intel*. Dostopno prek: http://defensetech.org/2012/03/12/chinese-spies-use-fake-facebook-pages-to-gain-intel/ (20. januar 2014).
- Reiss, Edward. 1992. *The Strategic Defense Initiative*. New York: Cambridge University Press.

- Report. 2001. Dostopno prek: http://www.fas.org/irp/program/process/rapport_echelon_en.pdf (20. januar 2014).
- Rich, Steven. 2013. *NSA seeks to build quantum computer that could crack most types of encryption*. Dostopno prek: http://www.washingtonpost.com/world/national-security/nsa-seeks-to-build-quantum-computer-that-could-crack-most-types-of-encryption/2014/01/02/8fff297e-7195-11e3-8def-a33011492df2_story.html (20. januar 2014).
- Rid, Thomas. 2012. 'Cyber War Will Not Take Place'. *Journal of Strategic Studies* 35 (1): 5–32.
- Robertson, Jordan. 2013. *Stuxnet Had Earlier, Potentially Explosive Version, Symantec Says*. Dostopno prek: http://go.bloomberg.com/tech-blog/2013-02-26-stuxnet-had-earlier-potentially-explosive-version-symantec-says/ (1. januar 2014).
- *RootSudo*. 2014. Dostopno prek: https://help.ubuntu.com/community/RootSudo (12. januar 2014).
- Rosenbach, Marcel. 2013. *iSpy: How the NSA Accesses Smartphone Data.* Dostopno prek: http://www.spiegel.de/international/world/how-the-nsa-spies-on-smartphones-including-the-blackberry-a-921161.html (12. januar 2014).
- Sapronov, Konstantin. 2007. *Kaspersky Security Bulletin 2006: Malware for Unix-type systems.* Dostopno prek: http://www.securelist.com/en/analysis/204791925/Kaspersky_Security_Bulletin_2006_Malware_for_Unix_type_systems (23. december 2013).
- Saxenian, AnnaLee. 2003. Government and Guanxi: The Chinese Software Industry in Transiton. *The Software Industry in Emerging Markets.* Cheltenham: Edward Elgar.
- Schneier, Bruce. 2002. *Secrecy, Security, and Obscurity. Crypto-Gram*. Dostopno prek: http://www.schneier.com/crypto-gram-0205.html (17. marec 2013).
- --- 2006. *Microsoft Vista's Endless Security Warnings*. http://www.schneier.com/blog/archives/2006/04/microsoft_vista.html (23. julij 2031).

- --- 2007. *Lesson From Tor Hack: Anonymity and Privacy Aren't the Same*. Dostopno prek: http://www.wired.com/politics/security/commentary/securitymatters/2007/09/security_matters_0920?currentPage=all (12. december 2013).
- --- 2013. *The Battle for Power on the Internet.* Dostopno prek: http://www.isn.ethz.ch/Digital-Library/Articles/Detail/?id=174223&lng=en (1. januar 2014).
- *Shared Source Initiative.* 2013. Dostopno prek: http://www.microsoft.com/resources/sharedsource/gsp.mspx (12. december 2013).
- Smith, S. Craig. 2000. *Fearing Control by Microsoft , China Backs the Linux System*. Dostopno prek: http://www.nytimes.com/learning/students/pop/articles/08soft.html (18. december 2010).
- *Sodišča z odprto kodo prihranijo 400 tisoč evrov letno*. 2011. Dostopno prek: http://www.finance.si/305469/Sodi%B9%E8a-z-odprto-kodo-prihranijo-400-tiso%E8-evrov-letno/rss1 (12. julij 2012).
- *Software Becomes a Product*. 2014. Dostopno prek: http://www.computerhistory.org/revolution/mainframe-computers/7/172 (20. januar 2014).
- Souza, Bruno. 2006. How Much Freedom Do You Want. V *Open Sources 2.0: The Continuing Evolution*, ur. Chris DiBona, Mark Stone in Danese Cooper, 211–229. Kalifornija: O Reilly Media.
- *Statistics.* 2013. Dostopno prek: http://www.top500.org/statistics/ (22. december 2013).
- Sulek, David in Ned Morgan. 2009. What analogies can tell us about the future of cyber security. V *The Virtual Battlefield: Perspectives on Cyber Warfare*, ur. Christian Czosseck, 118–131. Cambridge: Cambridge University Press.
- Svete, Uroš. 2005. *Varnost v informacijski družbi*. Ljubljana: Fakulteta za družbene vede.
- Škrubej, Janez. 2008. *Hladna vojna in bitka za informacijsko tehnologijo*. Ljubljana: Založba Pasadena.

- *Študija uvajanja odprtokodne programske opreme (OKPO) na delovnih postajajh v javni upravi*. 2011. Dostopno prek: mju.gov.si/.../Studija_uvajanja_OKPO_na_DP_v_JU_koncna_razlicica_17.2.2011.pdf (19. julij 2011).
- *The Economic Impact of Cybercrime and Cyber Espionage.* 2013. Dostopno prek: http://www.mcafee.com/sg/resources/reports/rp-economic-impact-cybercrime.pdf (12. januar 2014).
- *The Open Source Initiative.* 2013. Dostopno prek: http://opensource.org/ (20. januar 2014).
- *The short life and hard times of a Linux virus.* 2005. Dostopno prek: http://librenix.com/?inode=21 (23. december 2011).
- Theohary, A. Catherine in John Rollins. 2011. *Terrorist Use of the Internet*. Washington: Congressional Research Service (CRS).
- Thibodeau, Patrick. 2013. *What China's supercomputing push means for the U.S.* Dostopno prek: http://www.computerworld.com/s/article/9239912/What_China_s_supercomputing_push_means_for_the_U.S. (22. januar 2014).
- Traynor, Ian. 2013. *Merkel compared NSA to Stasi in heated encounter with Obama.* Dostopno prek: http://www.theguardian.com/world/2013/dec/17/merkel-compares-nsa-stasi-obama (20. januar 2014).
- Usselman W. Steven. 2009. Unbundling IBM Antitrust and the Incentives to Innovation. V *The Challenge of Remaining Innovative: Insights from Twentieth-Century American Business,* ur. Sally H. Clarke, Naomi R. Lamoreaux in Steven W. Usselman, 249–278. Kalifornija: Stanford University Press.
- Veit, Medick in Annette Meiritz. 2014. Dostopno prek: http://www.spiegel.de/international/germany/us-german-no-spy-deal-in-danger-of-failure-a-943614.html (19. januar 2014).
- *Virus Definitions & Security Updates.* 2014. Dostopno prek: http://www.symantec.com/security_response/definitions.jsp (12. januar 2014).

- *Web Server Survey*. 2012. Dostopno prek: https://secure1.securityspace.com/s_survey/data/201211/index.html (20. julij 2013).
- Weber, Steven. 2004. *The success of open source*. Cambridge: Harward University Press.
- Weimann, Gabriel. 2004. *Cyberterrorism: How Real Is the Threat?* USIP Special Reports 119. Washington: *United States Institute of Peace (USIP)*.
- West, Angus. 2013. *14 disturbing things Snowden has taught us (so far).* Dostopno prek: http://www.globalpost.com/dispatch/news/politics/130703/edward-snowden-leaks (20. januar 2014).
- Westad, Odd Arne. 2005. *The global cold war – Third world interventions and the making of our times*. Cambridge: Cambridge University Press
- Wynants, Marleen in Jan Cornelis. 2005. *How Open is the Future? Economic, Social & Cultural Scenarios inspired by Free & Open-Source Software*. Bruselj: Brussels University Press.
- *Zakona o elektronskih komunikacijah* (ZEKom-1). Ur. L. RS 109/2012 (31. december 2012)
- Zetter, Kim. 2010. *Google Hack Attack Was Ultra Sophisticated*. Dostopno prek: http://www.wired.com/threatlevel/2010/01/operation-aurora/ (12. februar 2012).