UNIVERZA V LJUBLJANI

FAKULTETA ZA DRUŽBENE VEDE

Mitja Topalovič

HEKERJI V OBVEŠČEVALNI DEJAVNOSTI

Diplomsko delo

Ljubljana, 2008

UNIVERZA V LJUBLJANI

FAKULTETA ZA DRUŽBENE VEDE

Mitja Topalovič

Mentor: asist. dr. Uroš Svete

Somentor: asist. dr. Matej Kovačič

HEKERJI V OBVEŠČEVALNI DEJAVNOSTI

Diplomsko delo

Ljubljana, 2008

Zahvala.

Mentorju dr. Urošu Svetetu in somentorju dr. Mateju Kovačiču za nenadomestljivo strokovno pomoč in trud pri nastajanju diplomskega dela,

družini za vso podporo in finančno pomoč pri študiju,

tebi Ines, ki si me spremljala ob vseh vzponih in padcih ter verjela vame in

vsem prijateljem in sorodnikom, ki ste mi vsa ta leta stali ob strani.

HEKERJI V OBVEŠČEVALNI DEJAVNOSTI

Obveščevalne službe so skozi zgodovino predstavljale pomemben člen pri razvoju tehnologije, prav tako so prednosti same tehnologije izrabljale. Obveščevalna dejavnost je danes padla v tokove informacijske revolucije, v obdobju asimetričnih groženj se mora soočiti z novimi izzivi na področju zagotavljanja nacionalne varnosti. Bistven izziv obveščevalne dejavnosti danes, ki sem ga izpostavil tudi v diplomskem delu, je vprašanje smiselnosti uporabe tradicionalnih oblik pridobivanja obveščevalnih podatkov na eni strani in vprašanje pretirane uporabe sodobne tehnologije pri pridobivanju zanesljivih podatkov na drugi strani. Skozi diplomsko delo sem večji del namenil hekerjem, njihovim metodam dela in motivacijskim dejavnikom. Hekerji so s prepričanjem o svobodi informaranja odigrali vidno vlogo pri širjenju računalniških sistemov in interneta. V diplomskem delu izpostavljam vlogo hekerjev v sodobnih konfliktih, v zaključku naloge proučim primere novačenja hekerjev v obveščevalne službe in proučim primere obveščevalno motiviranega hekerstva.

Ključne besede: hekerji, obveščevalna dejavnost, obveščevalno motivirano hekerstvo.

HACKERS IN INTELLIGENCE

Throughout history intelligence services were an important part of the development of technology, while they also exploited the advantages of this same technology. The intelligence was thus confronted with the information revolution and had to face new challenges in the area of assuring national security in the period of asymmetric threats. One of the main challenges of intelligence today, which I present in my thesis, is the question of reasonableness of use of traditional forms of acquiring intelligence information on the one hand and the question of excessive use of modern technology in the acquisition of reliable information on the other hand. In my thesis, I devote the most attention to hackers, their methods and different motivation factors. With their belief in the freedom of information, hackers played a visible role in the spreading of computer systems and the internet. I also present the role of hackers in modern conflicts, study the examples of recruiting hackers into intelligence services and study cases of hack intelligence.

Keywords: hackers, intelligence activities, hack intelligence.

KAZALO

SEZNAM SLIK IN SHEM

1 UVOD

Obveščevalno-varnostne službe so v obdobju hladne vojne posvečale večino pozornosti blokovskim nasprotnikom, njihovo delovanje je bilo usmerjeno predvsem na vojaško in politično področje, danes pa se te službe spopadajo z novimi izzivi, asimetričnimi oblikami ogrožanja tako nacionalne kot mednarodne varnosti, kot sta npr. *terorizem* in *gospodarsko vohunjenje*, kjer ni jasnih nasprotnikov in tudi ne zaveznikov.

Obdobje hladne vojne je tudi obdobje hitrega razvoja znanosti in tehnologije in pri tem je smiselno dodati, da so poleg oborožitvene tekme pomembno vlogo igrale tudi obveščevalne službe. Obveščevalna dejavnost držav znotraj obeh blokov je v obdobju hladne vojne s pomočjo sodobne tehnologije zbirala podatke o nasprotniku, pri tem pa izrazito delovala v strogi tajnosti, informacija je bila zgolj prioriteta oblastvenih organov. Z uvajanjem sodobne tehnologije v obveščevalno sfero so se obveščevalne službe hitro oprijele prednosti tehnologij, pri tem pa je nova tehnologija ponudila možnosti pridobivanja obveščevalnih podatkov s pomočjo novih metod.

Po koncu hladne vojne se je hitro izkazalo, da pretirano naslanjanje na tehnologijo in pridobivanje podatkov s pomočjo tehničnih virov ni prineslo želenih rezultatov. Z velikim izpadom in pomanjkanjem obveščevalnih podatkov so se med prvimi soočili v Združenih državah Amerike po terorističnem napadu 11. septembra 2001, v obdobju zavezniške vojne proti talibanskem režimu v Afganistanu in v iraški vojni. Danes postaja čedalje bolj jasno, da praktično ni mogoče uporabiti sodobne tehnologije v manj razvitih državah oz. v državah, ki te tehnologije ne poznajo. Strokovnjaki s področja nacionalne varnosti in dela obveščevalnih služb so pričeli odpirati debate o vlogi obveščevalno-varnostnih služb v 21. stoletju, stoletju asimetričnih groženj in informacijske eksplozije ter o tem kako se soočiti z nevidnim sovražnikom, ki uporablja vse razpoložljive metode in sredstva.

Obveščevalna dejavnost se bo v obdobju informacijske eksplozije morala nujno preusmeriti iz tajnosti v odprtost in se soočiti s preobremenjenostjo z informacijami, pri tem pa odprtost pomeni tudi medsebojno sodelovanje z ostalimi obveščevalnimi službami. Informacijska eksplozija je torej svet zajela sočasno s procesom globalizacije, pri tem pa družbo predala v objem informacijske tehnologije.

Tako z rojstvom interneta pred nekaj desetletji obenem doživimo rojstvo posebne subkulture računalniških ekspertov, ki jih poznamo kot *hekerje*. Sočasno z razvijanjem nove

tehnologije je rasla subkultura hekerjev, ki je že od vsega začetka poudarjala pomembnost računalniških sistemov in interneta in ga navsezadnje pomagala razširiti. Hekerska dejavnost se je v zadnjih nekaj letih preusmerila iz hekerstva za zabavo v kriminalno in profitno dejavnost. Hekerje danes srečujemo v različnih organizacijah, računalniški industriji, med drugim številna podjetja zaposlujejo hekerje za testiranje varnosti lastnih informacijskih sistemov ali kot svetovalce za računalniško in informacijsko varnost. Seveda pa se obenem moramo zavedati tudi zlonamernih aktivnosti hekerjev, torej poleg nezakonitega vdiranja v računalniške sisteme lahko tukaj govorimo o kraji osebnih podatkov, bančnih računov in o prevarah, vse do politično motiviranih napadov na vladne in nevladne organizacije in hekerski vojni. Ob vseh teh hekerskih aktivnostih pa obveščevalne službe ne ostajajo imune.

Tajnost delovanja obveščevalno-varnostnih služb na eni strani in hekersko prepričanje o svobodi informacij na drugi je bil v preteklosti pogost razlog in predmet upora hekerjev in posledično vdorov v informacijske baze z namenom iskanja zaupnih informacij. Dela obveščevalnih služb brez uporabe informacijsko-komunikacijske tehnologije si ne moremo predstavljati in prave razloge za skrb znotraj obveščevalne sfere je moč iskati v hitrem napredku informacijske tehnologije in nadaljnjem trendu razvoja. Tako računalniški sistemi za uporabnike postajajo čedalje bolj zapleteni, kar lahko razumemo tudi drugače – zaradi kompleksnosti sistemov predstavljajo ti večjo grožnjo za uporabnike s strani hekerjev, pri tem pa so sistemi tudi bolj ranljivi pred izgubo informacij. Motivacijski dejavniki hekerjev so različni, a se večinoma njihova aktivnost prične z radovednostjo in izzivom – in koliko bolj so sistemi nedostopni in zaščiteni, toliko večji je hekerjem izziv za vdiranje v informacijske baze in računalniške sisteme. Zaradi razpršenosti informacij in zahtevnosti sistemov obveščevalne službe tako potrebujejo načrt za vključevanje računalniških strokovnjakov v svoje vrste, kar pa je lahko tudi sporno, saj hekerji svoje znanje pridobijo na nezakonit način, zato se v ozadju vedno znova postavlja vprašanje zaupanja hekerjem.

V diplomskem delu bom sprva skušal čim bolj natančno in jasno definirati hekanje in hekerje, skozi generacijski pregled prikazati različne vloge hekerjev v posamičnem obdobju zgodovine hekerstva. Ključnega pomena za razumevanje vloge hekerjev v sodobnih konfliktih je razumevanje motivacijskih dejavnikov vdiranja hekerjev v računalniške sisteme, pri tem pa ne izostanejo niti metode njihovega dela. Tako bom poskušal skozi celotno nalogo nakazati večplastnost tega pojava in hkrati usmerjati pozornost proti politično motiviranim hekerstvom in

hektivizmom, ki so bistvenega pomena pri razumevanju vloge hekerjev v sodobnih konfliktih. V zadnjem delu naloge bom pozornost usmeril v obveščevalno motivirano hekerstvo in proučil bistvene lastnosti nove metode pridobivanja podatkov s pomočjo kibernetske infiltracije hekerjev v tarčne računalniške in informacijske podatkovne baze z namenom pridobivanja obveščevalnih podatkov ter poskušal s primeri podkrepiti teoretska izhodišča.

2 METODOLOŠKO-HIPOTETIČNI OKVIR

2.1 Predmet proučevanja in struktura naloge

V diplomskem delu bom obravnaval in podrobno proučil hekerstvo in njegovo vlogo v obveščevalni dejavnosti. Z obravnavano tematiko želim bralcu približati problematiko vloge hekerjev v obveščevalni dejavnosti. Naloga je sestavljena iz treh delov. V prvem delu predstavim spremenjeno podobo družbe kot posledico informacijske revolucije, predvsem se v tem delu posvetim globalizaciji in individuaciji, ki sta ključna procesa za razumevanje hekerjev, na kar se dotaknem tudi uporabe informacijsko-komunikacijske tehnologije in pomena le-te pri zagotavljanju varnosti. V drugem delu predstavim glavne značilnosti hekerstva skozi zgodovino, hekerske metode in motivacijo hekerjev za vdiranje v informacijske sisteme, obenem ob motivacijskih dejavnikih med drugim izpostavim koncept politično motivirane hekerske aktivnosti, ki je eden ključnih motivov za razumevanje hekerskega poslanstva v obveščevalno-varnostnih službah.

V tretjem delu obravnavam nove izzive obveščevalno-varnostnih služb v obdobju informacijsko-komukacijske tehnologije (IKT) in asimetričnega bojevanja. Sprva v tem delu proučim vlogo hekerskih metod pri pridobivanju obveščevalnih podatkov skozi primere obveščevalno motiviranega hekerstva, nato prav tako s primeri različnih držav prikažem pomen novačenja hekerjev v obveščevalno-varnostne službe. Obravnavani tematiki sledi sklep in verifikacija hipotez. Večino literature sem pridobil iz samostojnih publikacij in internetnih virov. O omenjeni tematiki so pisali posamezniki, ki so nekoč delovali znotraj obveščevalnih služb in zato iz njihovih poročil ni bilo mogoče pridobiti vseh informacij. Prav tako sem uporabljal odprte vire, na katerih temelji tudi obveščevalna metoda pridobivanja podatkov OSINT.

2.2 Cilji proučevanja

Cilji proučevanja so:

- definirati hekerstvo in hekerje,
- predstaviti motivacijske dejavnike hekerjev,
- opredeliti vlogo hekerstva v obveščevalni dejavnosti,
- opredeliti pomen nove metode pridobivanja obveščevalnih podatkov s pomočjo vdorov v računalniške sisteme.

2.3 Metode proučevanja

Pri izdelavi diplomske naloge sem si pomagal z naslednjimi raziskovalnimi metodami: *metodo analize in interpretacijo sekundarnih pisnih in elektronskih virov* sem uporabil pri proučevanju in raziskovanju monografskih publikacij, člankov, raziskovalnih poročil ipd.; *metodo zgodovinske analize* sem uporabil pri proučevanju zgodovine, *primerjalno-zgodovinsko metodo* sem uporabil pri pregledu in primerjanju generacij hekerjev; opisno (*deskriptivno*) metodo sem uporabil pri razlagi in opisu teoretičnih konceptov.

2.4 Hipoteze

Glavna hipoteza:

H 1: *Vloga in pomen hekerstva se skozi čas in napredek tehnologije spreminjata. V svetu, kjer informacije pridobivajo na moči, bodo hekerji postajali čedalje bolj pomemben člen pri zagotavljanju nacionalne varnosti. Novačenje hekerjev v obveščevalne vrste bo tako v prihodnje postalo stalna praksa obveščevalno-varnostnih služb.*

Delovna hipoteza:

H 2: *Hekerji bodo v prihodnje igrali pomembno vlogo ob načrtovanju in izvajanju hekerskih aktivnosti pred in med samim konfliktom.*

2.5 Opredelitev temeljnih pojmov

Podrobnejša razlaga ključnih pojmov je nujna osnova za nadaljnje proučevanje izbrane tematike. V tem delu bom opredelil pojme, ki se neposredno dotikajo tematike, zato jih v vsebinski del nisem vključil.

2.5.1 Obveščevalna dejavnost

Obveščevalna dejavnost je najširši pojem, ki ga Richelson (Richelson v Purg 1995, 30) definira kot »rezultat zbiranja, analiz, združevanja in interpretacije vseh razpoložljivih podatkov, ki zadevajo enega ali več vidikov tuje države oziroma operativnega področja, ki je neposredno ali potencialno pomembno za načrtovanje« (Purg 1995, 30).

Šaponja (1999, 9) definira obveščevalno dejavnost kot proces, ki zajema zbiranje in analitično obdelavo surovih podatkov in izdela celovit obveščevalni izdelek, ki ga uporabnik potrebuje pri oblikovanju in sprejemanju odločitev na državniškem, političnem, gospodarskem in varnostnem območju. Celoten postopek oziroma proces se imenuje *obveščevalni ciklus*, ki je sestavljen iz petih delov (Richelson v Purg 1995, 31):

- **načrtovanje** (ang. *planning and direction*) zajema management celotnega postopka pridobivanja obveščevalnih podatkov, od identifikacije potrebe po podatkih do izročitve obveščevalnega izdelka naročniku,
- **zbiranje** (ang. *collection*) zajema pridobivanje surovih izdelkov, iz katerih se nato izdela končni obveščevalni podatek. Ta postopek zajema javne vire, tajne agente in tehniko,
- **obdelava** (ang. *processing and exploitation*) se nanaša na spremembo ogromne količine podatkov v obliko, ki je primernejša za izdelavo obveščevalne informacije ter zajema prevajanje, dekodiranje ter sortiranje podatkov tako po vsebini kot količini,
- **analiziranje** (ang. analysis and production) pomeni spremembo osnovne informacije v končni obveščevalni podatek, pri čemer integrira vse razpoložljive podatke,
- **posredovanje** (ang. dissemination) pomeni distribucijo in izročitev končnega obveščevalnega podatka uporabnikom oziroma tistim, ki so sprožili postopek zbiranja informacij.

V ožjem smislu zajema obveščevalna dejavnost le tajno zbiranje in analizo podatkov ter njihovo transformacijo v »obveščevalno informacijo, v širšem pomenu pa k obveščevalni dejavnosti spadajo tudi protiobveščevalne in tajne akcije« (Richelson v Purg 1995, 31).

2.5.2 Obveščevalno-varnostna služba

Obveščevalna dejavnost je organizirana v posebnih organizacijskih oblikah, obveščevalnih organizacijah. Organizirane so lahko kot del državnega aparata in jih imenujemo obveščevalne organizacije v ožjem smislu, ali kar preprosto, službe. Zaradi narave njihovega delovanja, ki je tajno, jih imenujemo tudi tajne službe. Organizirane so lahko tudi kot samostojne nevladne organizacije, najpogosteje znotraj večjih gospodarskih sistemov ali zasebnih organizacij. Imenujemo jih obveščevalne organizacije v širšem smislu /…../. Od državnih služb se ločijo po tem, da lahko izvajajo le obveščevalno dejavnost v širšem smislu, z vsemi njenimi omejitvami. Najbolj pomembni delitvi obveščevalnih organizacij v ožjem smislu sta delitvi na obveščevalno-varnostne službe in varnostne službe (Šaponja 1999, 24).

Obveščevalna služba je posebna organizacijska oblika, v kateri se izvaja obveščevalna dejavnost v tujini oziroma v zvezi s tujino. Obveščevalne službe izvajajo obveščevalno zvrst, protiobveščevalno in varnostno, delujejo pa praktično na vseh področjih. Po svoji naravi so informativne in ne represivne. Njihovi uslužbenci nimajo policijskih pristojnosti (Šaponja 1999, 56). Žunec in Domišljanović sta obveščevalno-varnostne službe opredelila kot »*dejavnosti in organizacije, ki za potrebe države, posebej njenega političnega in vojaškega vodstva, z namenom uresničitve političnih ciljev in zunanjepolitičnih interesev države, zbirajo in analizirajo podatke o možnostih, namenih in dejavnostih tujih sil in drugih obveščevalno in varnostno zanimivih subjektih ter ščitijo pred njihovimi obveščevalnimi in drugimi dejavnostmi, izvzemši odkrito oboroženo agresijo, ki lahko ogrozi nacionalno varnost«* (Žunec in Domišljanović v Brezovšek in Črnčec 2007, 121).

2.5.3 Protiobveščevalna dejavnost

Anžič (1997, 44) protiobveščevalno dejavnost opisuje kot »*dejavnost, ki varuje državo pred delovanjem tujih obveščevalnih služb (lahko tudi posameznikov, skupin, organizacij), ki skušajo*

organizairano, zavestno in z nasilnimi sredstvi rušiti ali omajati ustavno ureditev[1]«.

Prav tako Šaponja (1999, 58), ko govori o obveščevalnih zvrsteh, protiobveščevalno zvrst definira kot »*vrsto obveščevalne dejavnosti, ki je po svoji naravi represivna. Obveščevalna dejavnost se v tem primeru uporablja za odkrivanje, spremljanje, onemogočanje in v nekaterih primerih tudi preiskovanje kaznivih dejanj vohunstva, ki ga izvajajo tuje obveščevalne organizacije. Ne gre pa zgolj za odkrivanje vohunske dejavnosti, marveč tudi za ugotavljanje in spremljanje aktivnosti tujih obveščevalnih organizacij, kadar ne izvajajo vohunske dejavnosti. Protiobveščevalna zvrst ima tudi preventivno varnostno funkcijo.*«

V nadaljevanju razprave o protiobveščevalni dejavnosti Šaponja (ibid., 58) definira protiobveščevalno službo kot službo, »*ki izvaja protiobveščevalno zvrst obveščevalne dejavnosti. Osnovna funkcija je preprečevanje in odkrivanje vsakovrstnega delovanja tujih obveščevalnih služb v državi (obveščevalna služba to izvaja v tujini). Protiobveščevalne službe so organizirane kot samostojne, lahko pa tudi kot del služb za varstvo ustavne ureditve. Štejemo jih med obveščevalno-varnostne službe. Lahko imajo preiskovalna pooblastila, podobna varnostnim službam, če tako določa notranji pravni red.*«

2.5.4 Informacija

Informacijo *Slovar slovenskega knjižnega jezika* opredeljuje kot: 1. *kar se o določeni stvari pove, sporoči; obvestilo, pojasnilo: dati, dobiti informacijo; iskati informacije; imeti dobre, zanesljive informacije; napačna informacija; zahtevali so natančne informacije o bolnikovem zdravstvenem stanju; vir informacij / informacija o dogodku je bila nepotrebna informiranje // mn. celota vednosti o določeni dejavnosti ali področju, namenjena javnosti, podatki: turistične, železniške informacije; izmenjava informacij; oddelek za informacije / radijske, televizijske informacije poročila. 2. elektronska množica vrednosti, ki jo (elektronski) računalnik sprejme ali po obdelavi izda: brati, hraniti informacijo; informacijo sestavlja šestdeset bitov / izhodna, vhodna informacija* (SSKJ 1996, 301).

[1] Anžičevo definicijo izpred več kot deset let je seveda potrebno tudi nekoliko dopolniti, predvsem v smislu trditve o rušenju ustavne ureditve. Protiobveščevalna dejavnost državo danes varuje tudi na področju gospodarskega vohunjenja, kjer pa ni nujno cilj izvajalcev vohunjenja omajati ali rušiti ustavno ureditev. Pravzaprav se danes obveščevalna dejavnost nagiba tudi k zasebnemu sektorju, velike korporacije ustanavljajo lastne obveščevalne komponente znotraj svojih vrst z namenom industrijske ali kompetitivne obveščevalne dejavnosti.

Operativna informacija je osnovni zapis podatkov, ki jih zberemo z obveščevalno dejavnostjo (Šaponja 1999, 57).

Praktično vsak košček informacije s strani današnjih podjetij ali organizacij je shranjen v digitalni obliki. Informacije so potemtakem lahko shranjene na računalniku ali so bile na računalniku ustvarjene. Posebna pozornost se v tem kontekstu posveča varovanju informacij na računalniku in informacijam znotraj elektronskih pošt, ki morebiti predstavljajo eno izmed največjih tveganj za izgubo informacij, saj večina ljudi ne ve kako deluje proces pošiljanja elektronske pošte. Tako so informacije na računalnikih še posebej zanimiva tarča za vohune (Winkler 2005, 23).

Za začetnika informacijske teorije velja Claude E. Shannon[2]. Omenjena mlada disciplina, je nastala pri problemih prenašanja sporočil na daljavo. Za prenos po telekomunikacijah je potrebno sporočilo najprej primerno preurediti. Besedilo, glasbo ali slike /.../ je treba najprej spremeniti v zaporedje takih signalov, ki jih je mogoče pošiljati po pripomočku, ki veže oddajnik in sprejemnik. Pravimo, da je treba sporočilo kodirati. To je pametno napraviti tako, da je prenos kar najbolj ekonomičen, to se pravi zvezan s čim manjšo porabo energije in čim krajši. Zadnja zahteva pomeni, da naj bo količina informacije, ki se prevede v časovni enoti po telekomunikaciji, čim večja. Vprašanje je torej, kako je treba sporočilo kodirati, da bo jakost toka informacije kar največja, in kaj sploh lahko dosežemo s primernim kodiranjem. Razen tega je treba ugotoviti, kaj moramo ukreniti, da bo kodirano sporočilo kar najbolje ustrezalo fizikalnim lastnostim kanala, to se pravi pripomočka, po katerem prenos teče. Dostikrat spremljajo prenos motnje, ki ovirajo pravilno branje sprejetega sporočila. S tem v zvezi se postavlja vprašanje, kakšno jakost ima tedaj lahko tok informacije, da bo verjetnost za pravilno branje sprejetega sporočila še dovolj velika. Ker se v njegovih sestavkih že odgovori na vsa vprašanja, ki smo jih omenili, /.../ štejemo Shanonna za začetnika teorije informacije (Jamnik 1974, 9–10).

Bistveni dosežek njegove teorije je ugotovitev, da lahko informacije izmerimo. Teorija je bila dobro sprejeta v raziskovalnih krogih inženirjev, ki so se ukvarjali s komunikacijami, nekaj njegovih konceptov teorije je našlo svoje mesto celo na področju psihologije in jezikoslovja (Shannon 2008).

[2] Pravi razvoj informacijske teorije se začne z objavo Shannonove knjige *A Mathematical Theory of Communication*.

2.5.5 Obveščevalni podatek in tajni podatek

Obveščevalni podatek je dejstvo, ki ne osvetljuje podatka v času in prostoru (Intelligence – Policy&Process 1985, v Šaponja 1999, 57). Pravimo, da tak podatek ni postavljen v širši kontekst. Podatek je dejansko izolirano dejstvo, temelječe na dogajanjih, aktivnostih, predmetih, ljudeh (Villa 1994, v Šaponja 1999, 57).

Pojem tajen je v prvotnem pomenu v SSKJ opisan kot: »*za katerega javnost, oblast ne ve*« (imeti tajen sestanek, dogodki so ostali tajni, tajna organizacija); v drugem pomenu: »*s katerim se javnost, ljudje ne morejo seznaniti*« (tajno srečanje, tajen sporazum, tajno glasovanje itd.); in v tretjem pomenu: »*ki je tak, da se ne opazi, ne vidi*« (SSKJ 1991, 15–16).

Po zakonu o tajnih podatkih (ZTP) je tajni podatek dejstvo ali sredstvo z delovnega področja organa, ki se nanaša na javno varnost, obrambo, zunanje zadeve ali obveščevalno in varnostno dejavnost države, ki ga je treba zaradi razlogov, določenih v tem zakonu, zavarovati pred nepoklicanimi osebami in ki je v skladu s tem zakonom določeno in označeno za tajno **(**ZTP 2006, 2. člen). Podatki so surovina, iz katere pridobivajo informacije v raznih oblikah, odvisno od načina predstavljanja in uporabljanja. Računalniška datoteka ali zbirka podatkov je organizirana zbirka takih podatkov (Slovenski inštitut za revizijo 1995, 8).

2.5.6 Informacijsko-komunikacijska tehnologija (IKT)

Sunkovit razvoj informacijsko-komunikacijske tehnologije (v angleščini se pogosto uporablja tudi termin *information technology* oz. v prevodu informacijska tehnologija) je sprožil val sprememb, ki so korenito vplivale na vsakodnevno delovanje in obnašanje tako posameznika kot organizacij v več aspektih. Tehnološka prednost zagotavlja nosilcem odločanja celovito, pravočasno in predvsem bolj natančno informacijo, zato je postalo sčasoma za organizacije in organe odločanja potrebno, da sprejmejo novosti informacijske tehnologije (Alberts 1996, 1–2).

Wilson (v Svete 2005, 17) obravnava IKT kot osnovo informacijske revolucije, ki je najbolj očitna v povečevanju zmogljivosti računalnikov, digitalizaciji podatkov in informacij ter v konvergenci nekoč ločenih družbenih podsistemov v novo entiteto produkcijskih, distribucijskih in aplikativnih aktivnosti. Digitalizacija informacijskih procesov je tako omogočila združitev računalnikov, telekomunikacij, televizije in interneta v enotno multimedijsko (komunikacijsko) okolje, prav tako pa povzročila širjenje IKT tehnologije (predvsem njenega informacijskega dela) v skoraj vse družbene sektorje in aktivnosti, od

zdravstva do transporta in izobraževanja.

Zorkoczy je v svojem delu *Informacijska tehnologija* že leta 1987 podal definicijo, ki jo opredeli kot »zbiranje, shranjevanje, obdelavo, razširjenje in uporabo informacije. To ni samo računalniška materialna oprema (ang. *hardware*) ali računalniška programska oprema (ang. *software*), ampak vključuje tudi človeka in njegove cilje za razvoj tehnologije v prihodnosti in vrednote, ki bi jih želel upoštevati. Poleg tega je pomembno, ali jo je človek zmožen obvladati in ali ga bogati« (Zorkoczy 1987, 17).

2.5.7 Asimetrično vojskovanje

Koncept asimetričnega vojskovanje (ang. *asymmetrical warfare*) je star toliko kot samo vojskovanje, vendar je po 11. septembru 2001 postal precej žgoča tema strokovnjakov s področja vojne veščine. Že stoletja in tisočletja šibkejši nasprotniki uporabljajo različne metode, ki bi izničile številčno prednost na bojnem polju s ciljem premagati nasprotnika. Danes obstaja nešteto definicij in razlag asimetričnega bojevanja, vendar vse vsebujejo temeljni element poudarjanja asimetrije med nasprotnikoma.

V U.S. Joint Chiefs of Staff (v Barnett 2003, 15) definirajo asimetrično vojskovanje kot »*poskus oslabljenja nasprotnikove moči, medtem ko se izrablja njegove slabosti z metodami, ki se razlikujejo in odstopajo običajnim oblikam operacij*.« Barnett med drugimi definira asimetrično vojskovanje kot sposobnost, v kateri sovražnik spretno uporabi prednosti in zmogljivosti svojih sil ali šibkosti sovražnikovih sil.

Asimetrično vojskovanje je izraz za vojaški spopad, v katerem imata nasprotnika precej različne bojne zmogljivosti (bojno moč) in sta v tem smislu »asimetrična«. Poznamo veliko primerov, kjer je asimetrija razvidna iz nastopa veliko močnejšega nasprotnika, ki želi s tehnično premočjo pokoriti slabšega, ter veliko primerov, ko poskuša slabši nasprotnik prevzeti pobudo z uporabo različnih strateških in taktičnih potez, ki načelno izstopajo iz okvirov konvencionalnega (oziroma so povsem v nasprotju s sprejetimi konvencijami) bojevanja (Kočevar 2007, 21).

Metz in Johnson (v Svete 2002, 25) predlagata svojo definicijo asimetričnega vojskovanja in sicer »/v/ domeni vojaških zadev in nacionalne varnosti predstavlja asimetrija delovanje, organiziranje in razmišljanje, drugačno od nasprotnikovega, z namenom maksimizirati lastne prednosti ter izkoristititi nasprotnikove šibkosti, pridobiti pobudo ali zagotoviti širše možnosti delovanja. Asimetrija je lahko politično-strateška, vojaško-strateška,

operativna ali njihova komnbinacija. Lahko vsebuje različne metode, tehnologije, vrednote, organizacije, časovno perspektivo ali kombinacije naštetega, prav tako je lahko kratkoročna ali dolgoročna. Razlikujemo tudi namerno oz. načrtno in spontano ter samostojno intisto, ki je povezana s simetričnimi pristopi. Po učinkih se delijo na psihološke in fizične.« Svete pri zgoraj omenjeni definiciji poudarja, da je ena najboljših definicij asimetričnega vojskovanja, pri tem pa hkrati izpostavlja pomanjkljivost definicije, saj meni, da asimetrija oz. asimetrično vojskovanje ni le domena vojaških zadev, prav tako tudi ni domena zgolj obrambnega ali nacionalnovarnostnega sistema, temveč je asimetrija način zagotavljanja interesov, ki zajema tako *posameznika* kot najvišje ravni institucionalne organiziranosti družbe in v dobi globalizacije sega preko državnih mej.

Zgornja definicija asimetričnega vojskovanja je torej dovolj izčrpna in hkrati uporabna tudi pri vključevanju hekerjev v sfero asimetričnega vojskovanja. Vsekakor lahko na ravni posameznikov hekerje štejemo tudi kot izvajalce asimetričnega vojskovanja, saj hekanje sovpada z značilnostmi asimetrije. Hekerji namreč spridoma izkoriščajo nesorazmerja, torej slabosti svojega nasprotnika (t.j. računalniška ekspertiza in poznavanje delovanja informacijskih sistemov), z izvajanjem kognitivnih hekerskih napadov lahko s svojimi napadi vplivajo na čustveno zaznavanje, vedenje in razmišljanje svojih nasprotnikov in s tem povzročijo željeni psihološki učinek. Bistvenega pomena pri povezovanju značilnosti asimetrije in hekerske dejavnosti pa je inovativnost uporabe informacijsko-komunikacijske tehnologije.

2.5.8 Informacijsko bojevanje

Eden prvih avtorjev, ki je podrobno razčlenil koncept informacijskega bojevanja, je Martin C. Libicki v knjigi *What is Information Warfare?* Za informacijsko bojevanje pravi, da kot samostojna, ločena tehnika bojevanja ne more obstajati. Tako informacijsko bojevanje loči med sedmimi različnimi oblikami, ki služijo širšemu konceptu informacijskega bojevanja. Sedem oblik informacijskega bojevanja – konflikti, ki vključujejo zaščito, manipulacijo, tajitev oz. prikrivanje resničnih informacij, razdeli med:

1. bojevanje na področju poveljevanja in nadziranja (ang. command and control warfare),
2. bojevanje na področju obveščevalne dejavnosti (ang. intelligence-based warfare),
3. elektronsko bojevanje (ang. electronic warfare),
4. psihološko bojevanje (ang. psychological warfare),

5. hekersko bojevanje (ang. hacker warfare),
6. ekonomsko informacijsko bojevanje (ang. economic information warfare) in
7. kibernetično bojevanje (ang. cyberwarfare) (Libicki 1995, 4).

Eden prvih teoretikov informacijskega bojevanja Thomas Rona širše definira informacijsko bojevanje kot »*tekmovanje na strateški, operativni in taktični ravni, ki lahko poteka v miru, krizi, konfliktu, med eskalacijo krize, pred/med/ in po vojni med nasprotniki, konkurenti in sovražniki, ki za dosego svojih ciljev uporabljajo informacijska sredstva delovanja*« (Rona v Libicki 1995, 4).

Definicija informacijskega bojevanja Ministrstva za obrambo ZDA pokriva tri temeljne oblike bojevanja na ravni nacionalne varnosti: a. informacijska nadvlada, b. zavarovanje informacij in c. informacijski napad. Informacijsko bojevanje se tako lahko odvija na treh ravneh:

- **nacionalna raven** (usmerjenost proti javnemu sektorju): a. omrežno bojevanje (ang. network warfare), b. ekonomsko bojevanje (ang. economic warfare), c. bojevanje na področju političnega življenja (ang. political warfare) in d. bojevanje na področju poveljevanja in nadziranja (ang. command and control warfare – C2),
- **institucionalna raven** (usmerjenost proti velikim gospodarskim organizacijam, korporacijam, zasebni sektor): a. kiber-vohunstvo, -sabotaže, OSINT (open-source intelligence), b. vohunstvo, ki prihaja znotraj organizacije, c. informacijski sistemi, kot tarča fizičnega napada ipd.,
- **raven posameznika** (napadi, usmerjeni proti posamezniku): a. kraja bančnih in kreditnih kartic, b. kraja osebnih podatkovnih baz ipd.

Informacijsko bojevanje tako zajema akcije, ki pomagajo preprečiti napad na integriteto določenega informacijskega sistema, ga s tem obvarovati pred razkritjem, vdorom, medtem pa z enakimi metodami uničiti nasprotnikov informacijski sistem ter tako ohraniti informacijsko prednost pred nasprotnikom (Waltz 1998, 20).

Kuehl (2002, 12–13) poudarja, da informacijskih operacij ne smemo enačiti z informacijskim bojevanjem. Strokovnjaki s področja vojaške znanosti se pogosto prerekajo, ali informacijsko bojevanje nastopi šele takrat, ko informacijske operacije že odpovejo. Po mnenju avtorja je to le ena izmed številnih razlik med tema dvema izrazoma. Informacijsko bojevanje

namreč zajema šest ključnih elementov z namenom spremljanja informacijskih operacij v obdobju konflikta. Elementi informacijskega bojevanja so:

- *napadi prek računaliških omrežij* (ang. computer network attack),
- *zavajanje* (ang. deception),
- *uničenje* (ang. destruction),
- *elektronsko bojevanje* (ang. electronic warfare),
- *varovanje operacij* (ang. operations security),
- *psihološke operacije* (ang. psychological operations).

Informacijske operacije naj bi bile vodene kot strateška kampanja skozi vse obdobje konflikta. Obenem avtor trdi, da so omenjene operacije veliko bolj obsežne kot samo informacijsko bojevanje. Informacijske operacije so lahko tako zelo uporabno orodje kreiranja okolja pred samim nastopom konflikta, t.j. v predkonfliktni fazi.

Temelj informacijskega bojevanja je torej informacija, ki danes prevladuje v vseh aspektih družbenega življenja. Koncept informacijskega bojevanja postaja neizbežno dejstvo, saj smo danes priča izjemnemu porastu, razvoju in napredku informacijsko-komunikacijske tehnologije.

3 SPREMENJENA PODOBA DRUŽBE KOT POSLEDICA INFORMACIJSKE REVOLUCIJE

3.1 Pomen globalizacije in individualizacije

Skozi zgodovino človeštva vsako obdobje zaznamujejo izumi, odkritja in dosežki, ki so odločilno vplivali na družbeno življenje, prav tako pa so se znanstveno-tehnični dosežki izkazali kot gonilo sprememb skozi zgodovino. V iskanju bistvenih elementov definiranja informacijske revolucije vedno znova končamo v labirintu izrazov, kot so informacijska družba, računalniki, informacijska tehnologija, informacijskih sistemi itd. V naslednjih odstavkih bom posvetil pozornost informacijski revoluciji in kako je informacijska tehnologija spremenila podobo

današnje družbe in s tem tudi družbene varnosti.

Pogosto smo v zadnjem času priča izjemnemu naraščanju zmogljivosti računalnikov, tehnološki napredek združuje sliko, video in zvok in nam tako omogoča vse tesnejšo povezavo televizije in računalnikov v združene digitalne tokove zvoka, slik in besedila. Skoraj nemogoče je v celoti predvideti učinek informacijske revolucije, saj le-ta močno vpliva na naše vsakdanje življenje. Pogosto so spremembe, ki spremljajo nove informacijske tehnologije, tako neopazne, da se jih komaj zavedamo. Pred izumom pisave se je človek moral zanašati na spomin, pred izumom telefonije so ljudje pisali pisma, tehnologija nas po eni strani čedalje bolj izolira od družbenega življenja, človek se od realnega življenja oddaljuje, postajamo čedalje bolj odtujeni od sveta okoli nas, medčloveški stiki strmo upadajo (Triglav 1996, 27).

Ko govorimo o družbenih spremembah, je tukaj smotrno dodati nekaj besed o konceptualizaciji družbenega razvoja, ki nam ga podaja Mlinar (v Trček 2003, 39). Sočasnost osamosvajanja in povezovanja so po avtorjevem mnenju kot logika družbenega razvoja. V tem kontekstu avtor obravnava koncepta dveh dolgoročnih procesov *individualizacije* in *globalizacije*, ki sta bistvenega pomena za razumevanje hekerske subkulture.

Geografska bližina ni več pogoj in zagotovilo za povezanost ali podobnost med prebivalci, posebnosti posameznikov in vse bolj raznovrstnih skupin /med katere spada tudi hekerska subkultura/ lahko v zmeraj manjši meri pojasnimo in predvidimo zgolj na podlagi njihove teritorialne pripadnosti. Z večjo dostopnostjo, ki jo omogoča tudi nova komunikacijska tehnologija, začenjamo razkrivati, da ne le vse bolj odpravljamo prostor kot oviro, temveč tudi izgubljamo predvsem zaščitno vlogo prostora in s tem postajamo vse bolj izpostavljeni (želenim in neželenim) globalnim vplivom in »globalnim vdorom« (Mlinar 1994, 11).

V kontekstu hekerstva predstavlja preseganje teritorialnih mej veliko prednost, saj si lahko hekerji prek spleta izmenjujejo mnenja in izkušnje, predvsem pa postaja povezanost in prepustnost teh mej bistvena za izmenjavanje orodij ter programske opreme za vdiranje v računalniške sisteme. Čeprav hekerska subkultura še zdaleč ni homogena in prostorske omejitve ne predstavljajo bistvenega pomena, si hekerji svoje izkušnje in mnenja izmenjujejo na točno določenem mestu na spletu (npr. IRC[3] kanali, forumi ipd.).

Torej lahko med drugim o procesu globalizacije govorimo kot o procesu časovno-prostorskega zgoščevanja, ki je predvsem posledica razvoja prvotno transportnih in v novejšem

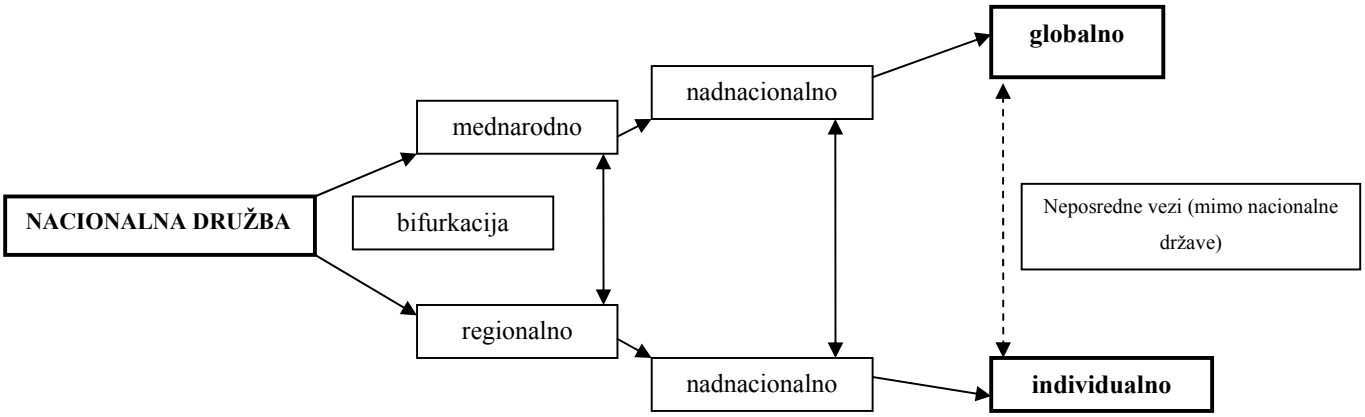
[3] IRC – Internet Relay Chat.

času informacijskih in telekomunikacijskih tehnologij. Ta razvoj omogoča na izkustveni ravni doživljanje sveta kot manjšega, manj razsežnega oz. časovno-prostorsko obvladljivega. Gre torej za možnost preseganja teritorialnih, običajno nacionalnih meja in možnost povezovanja in integriranja akterjev v nove prostorsko-časovne kombinacije. Mlinar izpostavlja pet splošnejših razsežnosti procesa globalizacije:

- globalizacijo kot *povečanje medsebojne odvisnosti v svetovnem merilu*,
- globalizacijo kot *dominantnost in odvisnost* (sočasnost procesov soodvisnosti in svetovne dominacije oziroma pomen globalizacije pri prelivanju kapitala iz periferije v globalne centre),
- globalizacijo kot *svetovno homogenizacijo* (poudarja tendenco razširajanja univerzalnih, svetovnih standardov; tehnološka globalna standardizacija pa je nedvomno predpogoj za nujen obstoj globalizacije),
- globalizacijo kot *prerazporeditev raznovrstnosti sveta* (se kaže kot prisotnost svetovne raznovrstnosti v različnih konkretnih teritorialnih enotah),
- globalizacijo kot preseganje časovne diskontinuitete (omogočajo jo novi načini asinhronega komuniciranja in obstoj določenih dejavnosti v tako imenovanem univerzalnem, globalnem času s tendenco po delovanju »*just in time*«).

Bistvenega pomena za razumevanje hekerstva je tudi proces individua(liza)cije. Mlinar pri definiranju *individua(liza)cije* trdi, da »*odvisnost od skupinskega življenja sicer ni prenehala, vendar združevanje ljudi temelji bolj na izbiri kot pa na tradiciji* /.../« (Trček 2003, 44). Steven Lukes (v Mlinar 1994, 18) pri individuaciji poudari *avtonomijo* (samoopredeljevanje), *zasebnost* (nevmešavanje) in *samouresničevanje* (samorazvoj). Na prvi pogled lahko sicer hekerje označimo kot izrazite individualiste, vendar so se postopoma združili v subkulturo z lastnimi pravili in vrednotami, ki pa so se iz generacije v generacijo bistveno spremenile (*glej* poglavje 4.1).

Shema 3.1: Globalizacija – individualizacija.



Vir: Mlinar (1994, 13).

3.2 Vloga informacijske tehnologije pri zagotavljanju varnosti

Industrijska družba zaradi pospešene avtomatizacije postaja vse bolj infomacijska, narodni dohodek se iz industrijske proizvodnje seli v storitveno dejavnost. Tako Otto in Phillipp Sonntag (v Pivec 2003, 13) o informacijski družbi govorita kot o »*družbi, v kateri večina zaposlenih dela v informacijskih poklicih, torej več z informacijami, signali, simboli, risbami ali slikami kot pa z močjo in materialom.«* Pojem *informacijska družba* se je rodil iz kritične znanstvene obravnave družbenega razvoja, od koder ga je pobrala politika in ga dodobra preoblikovala v pragmatiko. Problem definiranja informacijske družbe se pojavi z dejstvom, da različne znanosti kandidirajo za »skrbnice« pojma informacijske družbe. Tako se pri znanstveni konceptualizaciji informacijske družbe ponuja rešitev v sami interdisciplinarnosti, ki pa je po Sarcevicu ena izmed značilnosti informacijske znanosti. Avtor tako navaja, da ima »*informacijska znanost tri glavne značilnosti, ki so vodilni motivi njenega razvoja in obstoja, deli pa si jih še z mnogimi novimi področji. Prvič: informacijska znanost je po svoji naravi interdisciplinarna, vendar se odnosi z različnimi disciplinami spreminjajo. Drugič: informacijska znanost je usodno povezana z informacijsko tehnologijo. Tehnološki imperativ sili in usmerja razvoj informacijske znanosti tako, kot počne tudi razvoj informacijske družbe. Tretjič: informacijska znanost je, skupaj z mnogimi drugimi področji, aktivna udeleženka pri razvoju informacijske družbe in ima močno družbeno in človeško razsežnost, nad in onkraj tehnologije«* (Sarcevic v Pivec 2003, 22).

Pri vsem tem pa se še vedno postavlja ključno vprašanje, kakšno je nacionalnovarnostnego tveganje oz. kakšne so varnostne implikacije uporabe IKT, ko govorimo

o nacionalni varnosti. Kompleksnost današnjega varnostnega okolja zahteva aktivacijo mehanizmov, ki bodo lahko ustrezno odgovorili na vprašanja tveganj in groženj, ki jih uporaba IKT prinaša v družbo. V mislih imam predvsem izoblikovanje novih varnostnih struktur, ki bodo v navidezno nenevarnem kibernetskem prostoru pomagale preprečevati kibernetska kriminalna dejanja. Svete tako navaja dve vrsti groženj v varnostnem okolju, in sicer tiste, ki jih usmerjajo in določajo njihovi akterji oz. izvajalci, ter strukturne grožnje. Med prvo vrsto groženj spadajo države, formalne ali neformalne skupine ali celo posamezniki, pri tem pa države kot primarni varnostni akterji »uporabljajo« tako tradicionalne grožnje z oboroženim napadom kot netradicionalne, prav tako pa države grožnje izvajajo tudi na področjih trgovine, financ ter energetskega sektorja. Tako avtor za primer navaja kibernetsko bojevanje. V primeru, da nam preneha delovati računalnik, želimo vedeti, ali je to zgolj slučaj ali pa smo bili žrtev napada neke države, mreže oz. zgolj radovednega posameznika (Svete 2005, 74).

Drugo vrsto groženj predstavljajo strukturne grožnje[4], ki so nenamerne in nevojaške narave. Taki dogodki se preprosto zgodijo, ne da bi kdorkoli želel biti vpleten (ibid., 74).

V globalni informacijski družbi sta izvajanje in reševanje konfliktov vse bolj odvisna od t.i. *mehkih virov* in *sredstev moči*, med katerimi pa v ospredje čedalje bolj stopa tudi uporaba IKT. Uporaba IKT se lahko izkaže tudi kot sredstvo zagotavljanja nacionalne/individualne ter mednarodne varnosti. Tako so zmogljivosti IKT dobrodošle pri preprečevanju in odpravi posledic naravnih nesreč, kajti strukturne grožnje prihajajoče iz naravnega okolja, so med najpomembnejšimi izzivi tako za koncept nacionalne kot individualne (človekove) in globalne varnosti[5] (ibid., 113).

Uporaba IKT je na drugi strani prav tako povzročila tudi razpadanje oz. razdelitev gospodarskega, družbenega in političnega prostora ter glavne funkcije države. Sodobnim gospodarskim in družbenim trendom stoji nasproti klasična država in njena navazava na ozemlje. Z informacijsko revolucijo vzpodbujena globalizacija ter nastajanje svetovne (globalne) družbe postavljata pod vprašaj enotnost države, gospodarstva in družbe. Na mednarodnem prizorišču je tako država dobila konkurente v obliki nevladnih organizacij in multinacionalk, na drugi strani

[4] Primeri so grožnje, ki izhajajo iz dogodkov kot so epidemije, naravne in antropogene nesreče ter izguba demokratičnih vrednot in nasilni državljanski nemiri.

[5] Svete navaj primer potresa, ki je 26.12.2004 povzročil uničujoče tsunamije v Indijskem oceanu. Zlasti pri sanaciji škode in zagotavljanju mednarodne pomoči je uporaba IKT odigrala ključno vlogo, saj je spremenila zaznavo dejanske razsežnosti naravne katastrofe s sredstvi, kot so digitaliziran video, digitalni fotoaparati, satelitske komunikacije – internet in pošiljanje multimedijskih vsebin v svet.

pa se tudi državljani ne identificirajo primarno kot državljani države, temveč v različnih okoliščinah kot predstavniki gospodarskih interesov ali transnacionalnih združenj. Na ozemlju temelječa država je izgubila del svoje suverenosti in opravilne sposobnosti ter družbene kompetentnosti zlasti v primerjavi z globaliziranim gospodarstvom in družbo. Hkrati pa tudi njeno zunanjo in varnostno politiko vse bolj določa okolje mednarodnih organizacij in drugih meddržavnih oblik sodelovanja. Svete poudarja, da je praktična in uporabna samo tista definicija globalizacije in njenih učinkov, ki se nanaša na nekaj novega. Prav gotovo je tukaj ogromno doprinesla uporaba IKT, ki ni povzročila zgolj globalizacijskih procesov v posameznih družbenih sektorjih (npr. ekonomskem), temveč je povzročila *civilizacijsko revolucijo s strateškimi učinki*. /Prostorsko neomejena komunikacija/ v realnem času med posamezniki in skupinami je omogočila nastanek popolnoma nove javnosti, prav tako naj bi uporaba IKT omogočila novo obliko političnega dialoga. Konvergenca telekomunikacij, radia, televizije in informacijske tehnologije bo ta učinek le še pospešila, končni rezultat pa bo revolucija, ki bo spremenila civilizacijo v omrežen svet (Svete 2005, 24–25). Toda vse dobre stvari imajo tudi slabe lastnosti in internet pri tem ni izjema. Na to opozarja finski profesor Kari, ki ga v svojem delu *Varnost v informacijski družbi*, navaja Svete (2005, 26).

Zanimiva teza, ki jo pri tem izpostavlja Kari, je dejstvo, da interneta niso razvili z namenom, da bi postal varno omrežje, temveč da bi preživel tudi primer fizičnega uničenja družbe. Pri tem namreč opozarja na zlonamerne uporabnike interneta in pri tem napoveduje konec oz. razpad interneta. Glavni problemi po njegovem mnenju niso zgolj virusi in nezaželena elektronska sporočila, temveč sama struktura interneta, saj naj bi bila povsem neodporna na vse vrste notranjih napadov, pri tem pa izpostavlja največje sovražnike interneta – od hekerjev do profesionalcev, ki se z izsiljevanjem in s kriminalnimi dejanji želijo dokopati do denarja.

Z razvojem in širjenjem interneta je na svoj račun prišla sprva majhna skupina računalniških ekspertov, ki jo danes poznamo kot hekerje. Toda skupina računalniških ekspertov se je postopoma izoblikovala v lastno (sub)kulturo hekerjev. Hekerji danes do skrajnosti izkoriščajo tako prednosti kot slabosti interneta in tako posledično vplivajo na varnost znotraj in zunaj kibernetskega sveta. Douglas (2002, 155) v svojem delu *Hacker Culture* opozarja, da hekerji predstavljajo grožnjo ne samo zaradi dejstva, da jih ostali uporabniki interneta ne razumemo, ampak predvsem zaradi tega, ker razumejo bistvo nečesa, ki nam je zelo pomembno (delovanje računalnikov) na način, ki ga mi ne razumemo. Tako bi lahko v splošnem pomenu

reakcijo na hekanje in hekerje razumeli kot grožnjo tehnologije, vendar tehnologija sama po sebi ni tista, zaradi katere bi jo lahko označili kot *sui generis* grožnjo.

4 HEKERSTVO

4.1 Definicija hekanja in hekerjev

Definiciji hekerja in hekanja sta se skozi čas pogosto spreminjali, saj so se metode vdiranja, tehnologija in namen prav tako spreminjali. Medtem ko se danes pod vprašaj postavlja moralni in družbeni vidik hekanja, se prav tako v ospredje postavlja problematika glede nejasnega in včasih spornega izraza »*hekanja*«. Splošno sprejeta razlaga termina se danes nanaša na neavtoriziran dostop oziroma diskreten vstop v računalniške sisteme ostalih uporabnikov in posledično uporaba teh. Ta definicija je sorazmerno nova v primerjavi z definicijo izpred nekaj desetletij, ko ni vsebovala omenjene negativne konotacije. Pri tem je pomembno poudariti, da so mediji in računalniška industrija veliko pripomogli k širjenju negativnega pomena hekanja (Taylor 1999, XI).

Danes tako hekanje definiramo kot nameren neavtoriziran vstop v področja katerih pravice oziroma lastništvo je že vzpostavljeno. Danes je torej eden izmed ciljev hekerjev[6] zlom varnostnega omrežnega sistema z namenom škodovati celostnosti računalniškega sistema (Wall 2007, 53).

V prvotnem pomenu so izraz »heker« skovali v laboratorijih MIT[7] v začetku 60. let prejšnjega stoletja. Levy v svojem delu *Hackers: The heroes of computer revolution* iz leta 1984 poudarja, da izraz prvotno ni poudarjal izrednih veščin teh posameznikov, temveč je poudarjal igrivost akademskih računalniških programerjev, ki so iskali predvsem najbolj elegantne programske rešitve vsakega problema (Taylor 1999, 25).

Eric Raymond, urednik prenovljene verzije *New Hacker's Dictionary*, definira hekerja[8] kot 1. posameznika, ki uživa v raziskovanju podrobnosti programov ter sistemov in kako razširiti skrajne meje programskih zmožnosti, kar je v nasprotju z večino uporabnikov, ki se z razumevanjem programom in sistemov zadovoljijo na minimalni ravni; 2. kot posameznika, ki

[6] Danes hekerji vdirajo v računalniške sisteme z različnimi motivi, pri tem pa je potrebno poudariti, da je predvsem pri obveščevalno motiviranemu hekerstvu cilj hekanja, tajen vstop v računalniški sistem, prikrito opraviti svojo nalogo (npr. kopiranje podatkov) in nato tudi brez sledi zapustiti sistem.
[7] Massachusetts institute of technology (MIT 2008).
[8] Izvorno heker pomeni posameznika, ki izdeluje pohištvo s pomočjo sekire (Raymond 1996).

uživa (je obseden) v programiranju bolj kot v teoretiziranju o delovanju programov; 3. kot posameznika, ki ceni in spoštuje vrednote hekerskega poslanstva; 4. kot posameznika, ki je hiter programer; 5. kot posameznika, specializiranega za delovanje določenega programa oz. posameznika; 6. kot posameznika, ki uživa v intelektualnem izzivu kreativnosti pri širjenju, preseganju meja delovanja programov; 7. (definicija, ki je prvotni hekerji ne odobravajo) kot škodoželjnega posameznika, ki poskuša z vdiranjem v računalniške sisteme odkriti zaupne in občutljive podatke z brskanjem po računalnikih. Pravilen izraz za posameznika, ki ustreza zadnji definiciji, je izraz *kreker* (Raymond 1996).

Pomembno mesto glede definiranja hekerjev je potrebno nameniti tudi definiciji Bruce-a Schneier-ja, ki o izrazu heker pravi, da je star toliko kot sama radovednost, čeprav je izraz sam precej sodoben. Sodobni stereotip hekerja naj bil po Schneierju sledeč:

- mladoletnik (nekaj nad dvajsetimi leti starosti, v večini pa najstnik moškega spola),
- družbeno izoliran,
- z značilnostmi hekerske kulture: hekerska imena, pravila in žargon (Schneier 2000, 44).

Winn Schwartau hekerje poimenuje za prve informacijske bojevnike v kibernetskem svetu in tako loči med amaterskimi in poklicnimi hekerji. Amaterski hekerji naj bi bili vsi polprofesionalni, ki uporabljajo pripomočke in orodja, ki so jih razvili poklicni hekerji. Schwartau tako podaja profil amaterskih hekerjev, ki naj bi bil:

- običajno predstavnik moškega spola star med dvanajst in osemindvajset let,
- bister, a s slabim uspehom v šoli,
- posebnež in pogosto nedoumljiv,
- izhajajoč iz slabo urejene družine.

Dr. Mich Kabay meni, da nekateri hekerji trpijo za klinično motnjo narcisoidnosti. Hekerji se med seboj razlikujejo, zato je težko določiti stereotip hekerja. Običajen značaj hekerja pa naj bi tako bil:

- veličasten občutek svoje lastne pomembnosti,
- prezaposlenost s fantazijo o neskončni uspešnosti,
- potreba po stalni pozornosti in občudovanju,

- izjemno negativen odgovor na ogrožanje samozavesti,
- pomanjkljivost zmožnosti vživljanja v čustva drugega (Schwartau 1994, 339–340).

Bistvo in glavni predmet hekerstva predstavlja torej hekanje. Turklova (v Taylor 1999, 15) poda natančen opis glavnih elementov hekanja, saj spoji širšo in splošno obravnavano definicijo nezakonitega oz. zlonamernega hekanja in smiselnost hekanja z namenom prirejanja poljubno izbrane tehnologije za neobičajne namene. Hekanje tako opredeljuje kot samostojen termin, neodvisen od računalništva, in ga tako najbolje predstavi skozi primer uporabe povsem druge zahtevne tehnologije, ki ima zmožnost hekanja. Tako navaja primer Johna Draperja, bolje poznanega pod vzdevkom *Captain Crunch*, ki je z neverjetnim poznavanjem telefonskih omrežij vdiral v telefonske centrale in tako opravljal brezplačne klice po vsem svetu. Turklova tako navaja glavne značilnosti hekanja, in te so:

- **preprostost**: delo hekerja mora biti kar se da preprosto, a vseeno prepričljivo,
- **spretnost**: delo mora vključevati izjemno sofisticirano znanje in poznavanje delovanja tehnologije,
- **brezmejnost**: delo naj bi bilo protizakonito (Taylor 1999, 15).

Pri navajanju bistvenih značilnosti in značajskih lastnosti hekerjev pa je potrebno biti skrajno pazljiv. Hekerji so se danes preusmerili iz hekanja za zabavo v kriminalno-profitno hekanje. Potemtakem lahko z gotovostjo trdimo, da se je spremenil tudi njihov način dela in s tem tudi njihov značaj. Na tej točki bi rad opozoril, da danes lahko govorimo celo o preseganju stereotipa hekerjev. Bistvene značilnosti hekerjev so se spremenile iz generacije v generacijo, hekerji so si z znanjem in spretnostjo, predvsem pa z razumevanjem zapletene tehnologije izborili svoje mesto ne le v virtualnem, temveč tudi v realnem svetu. Na to kažejo čedalje bolj raznoliki motivacijski dejavniki hekerjev za vdiranje v računalniške sisteme (*glej* poglavje 4.6).

Definicija hekanja, katero potrjujejo in priznavajo tudi etični hekerji sami, je intelektualen *izziv, ki je posledica neškodljivega vstopa z namenom preizkusiti meje varnostnih sistemov; bistvo hekanja naj bi bilo predvsem opozorilo upravljavcem sistemov o morebitnih namerah hekerjev in ne namerno škodovanje sistemom*. Hekanje naj bi torej pomagalo izboljšati varnostno zaščito

informacijskih sistemov[9].

Prvotno hekerji niso predstavljali grožnje, vendar se je sčasoma to spremenilo. Danes obstaja jasna ločnica med t.i. »belimi hekerji« (ang. *white-hat hackers*), ki spoštujejo in zagovarjajo prvotno in tradicionalno, etično poslanstvo hekerjev, in drugo skupino t.i. »črnih hekerjev« (ang. *black-hat hackers*), ki jih vodi neetična miselnost in motivacija, kot sta dobičkonosnost in maščevanje.

Za širše razumevanje je potrebno poznati tudi zlonamerno stran hekerstva, saj lahko vdori v omenjene sisteme povzročijo veliko škodo informacijski infrastrukturi in izgubi občutljivih informacij, ki lahko navsezadnje vodijo celo v finančno ali fizično izgubo. Zanemariti pa ne smemo niti negativnih posledic zlonamernega hekanja, saj napad na sisteme določene organizacije lahko posledično pripomore k izgubi zaupanja v delovanje podjetja ali organizacije ter posledično v izgubo posla (Wall 2007, 55).

Na tej točki je torej potrebno začrtati jasno ločnico med obema skupinama etičnih in neetičnih hekerjev, saj bo le jasna definicija pripomogla k pravilnemu razumevanju hekerskega poslanstva.

4.2 Etični hekerji (legalni hekerji)

Etični hekerji se ponašajo z visoko stopnjo specializiranega znanja, združenega s trdnim prepričanjem o etičnosti svobode dostopa do javnih informacij. Ta skupina hekerjev je s svojimi sposobnostmi, znanjem in domišljijo odigrala ključno vlogo pri razvoju interneta, hkrati testirala skrajne meje programov in sistemov in s tem prisilila programerje, da vzpostavijo višje standarde pri varovanju sistemov in izboljšajo kvaliteto programov. Danes poznamo tri stopnje etičnega hekerstva, to so: a. guruji (ang. »*Gurus*«), ki so eksperti; b. čarovniki (ang. »*Wizards*), ki se od ostalih razlikujejo zaradi visoke stopnje usposobljenosti in znanja. Obe omenjeni skupini zagovarjata hekersko etiko, da je deljenje informacij pozitivnega, dobronamernega pomena za širšo družbo; ter c. samuraji (ang. »*Samurai*«), ki se za razliko od obeh omenjenih stopenj spoprijemajo in ukvarjajo z legalnimi vdori, pravičnim nadzorom, z namenom pomagati pravosodnim organom pri zagotavljanju pravice do zasebnosti ter hkrati priskočiti na pomoč

[9] Ključno vprašanje pri zaščiti informacijskih sistemov je, pred kom naj bi hekerji dejansko izvajali zaščito. V primeru legalne hekerske dejavnosti oz. etičnega hekerstva je zaščita informacijskih sistemov namenjena predvsem krekerjem, ki si poskušajo na nelegalen način zagotoviti podatke. Informacijske sisteme naj bi tako hekerji zaščitili pred zlonamernimi poskusi vdiranja krekerjev. Seveda pa na tej točki obstaja tudi tveganje, da bi heker sam ustvaril luknje v sistemu z namenom, da se dokoplje do željenih podatkov.

strankam, ki imajo legitimne razloge in potrebe po elektronskih ključavničarjih (Wall 2007, 55).

Spletna stran *SearchSecurity.com* definira etičnega hekerja kot strokovnjaka na področju računalništva in omrežij, ki napada varnostne sisteme v imenu podjetij, ki te sisteme posedujejo, z namenom iskanja varnostnih lukenj in pomanjkljivosti, ki bi jih morebiti zlonamerni hekerji lahko uporabili. Z namenom testiranja varnostnih sistemov etični hekerji uporabljajo povsem enake metode kot neetični hekerji, saj kasneje o pomanjkljivosti sistemov poročajo lastnikom in ne izkoriščajo pomanjkljivosti teh v zlonamerne namene. Etično hekerstvo je poznano tudi pod imenom »test prodiranja, vdiranja, ipd« (ang. *penetration test*). Eden izmed prvih primerov etičnega hekerstva sega v 70. leta prejšnjega stoletja, ko je vlada Združenih držav Amerike uporabila skupine strokovnjakov imenovane »*red teams*«, da bi vdrla v svoje računalniške sisteme. Etično hekerstvo je tako sčasoma postalo pomemben člen IT[10] industrije, zaposlovalo pa je tudi posebne skupine etičnih hekerjev (Searchsecurity.com 2008).

C.C. Palmer iz IBM[11]-a definira etično hekerstvo na podoben način. Po njegovem mnenju so različne organizacije zaradi vse pogostejših vdorov v njihove sisteme bile primorane najeti neodvisne skupine računalniških strokovnjakov z namenom preizkusiti varnost lastnih sistemov. Pri tem opozarja, da te skupine uporabljajo povsem enake metode kot neetični hekerji, pri čemer etični hekerji ne zlorabljajo pridobljenih informacij o morebitnih varnostnih luknjah in samemu sistemu in podjetju ne škodujejo. Za razliko od neetičnega hekerstva etični hekerji ocenijo varnost sistema podjetja, sporočijo ugotovitve lastnikom, ki nato poskušajo izboljšati varnost[12] (Palmer 2001, 770).

4.3 Neetični hekerji (krekerji)

Neetično hekerstvo spada nekje med skupino belih in skupino črnih hekerjev, odvisno predvsem od namere škodovanja. Neetične hekerje poimenujemo tudi »krekerji« (ang. crackers). Young (v Wall 2007, 56) razlikuje med dvema skupinama krekerjev: a. utopisti (ang. *utopians*), ki naivno verjamejo, da z odkrivanjem šibkosti in ranljivosti določenega dela družbenega življenja pripomorejo k izboljšavi le-te, in b. skupina t.i. kiber-huliganov (ang. *cyberpunks*), zaznamuje jih veliko bolj agresivna miselna naravnanost kot prvotne etične hekerje, saj namerno povzročajo

[10] IT – informacijska tehnologija.
[11] IBM – International Business Machines Corporation.
[12] Vlada ZDA je tako naredila »varnostno oceno« omrežnih sistemov vojnega letalstva ZDA in sicer nad varnostjo strogo zaupnih podatkov shranjenih v elektronski obliki.

škodo tarčam, ki jim nasprotujejo. Za obe skupini je značilno, da z neavtorizirano prisotnostjo poskušata ustvariti kaos (Wall 2007, 55–56).

Neetični hekerji ali krekerji so hekerji s kriminalnimi[13] težnjami. Njihove metode vdiranja so povsem v nasprotju z etičnim hekerstvom, saj preko neavtoriziranega dostopa poskušajo ogroziti delovanje računalniških sistemov.

Zaradi narave njihovega dela neetične hekerje pogosto štejejo med novodobne vohune 21. stoletja, imenovane kiber-vohuni (ang. *cyber-spies*), vendar ta trditev v celoti ne drži. Hekerji predvsem želijo vstopiti in izstopiti iz sistema, ki ga napadajo, diskretno, brez lastnega izpostavljanja in morebitnega odkritja, z namenom odkriti tajne ali občutljive informacije organizacij oz. podjetij, kot so npr. poslovne skrivnosti, ki bi morebiti bile uporabne v primeru, da si napadeno podjetje želi prisvojiti trg in uničiti konkurenco. Internet danes vsekakor pripomore k širjenju meja kiber-vohunstva na različne načine. *Prvi* način kiber-vohunstva lahko označimo takrat, ko hekerji uporabijo nezadovoljstvo zaposlenih znotraj specifične organizacije, pri čemer jih zaposleni preskrbijo z zaupnimi informacijami organizacije. Hekerji nato te informacije prenesejo izven meja organizacije z namenom maščevati se v imenu zaposlenih v organizaciji. Drugi način je prav tako preko sodelovanja s t.i. »insiderji«, ki hekerjem priskrbijo dostop do občutljivih in zaupnih informacij. Preko insiderjev, ki na računalnike namestijo ustrezno programsko opremo (npr. spyware) ali jim neposredno (zavestno ali ne) posredujejo uporabniška gesla[14], tako hekerjem dovolijo, da pridobijo nadzor nad računalniki in podatkovnimi bazami[15].

Tretji način kiber-vohunstva je lastno, a diskretno preiskovanje določenega sistema s ciljem poiskati uporabniška imena in gesla. Četrti način pa ni nujno ilegalen, saj lahko heker preko zbiranja različnih javno dostopnih podatkov izoblikuje končno sliko. (npr. organizacijska struktura, poslovna naravnanost podjetij, poslovni načrti ipd.) (Wall 2007, 56).

---

[13] Hekerstvo lahko preide v ilegalno delovanje (primer kršenja zakonodaje znotraj ZDA) v primeru ko: a. heker pridobi in si lasti gesla za računalniške sisteme ali omrežja za katere nima pooblastil; b. heker dejansko vstopi v računalniški sistem brez dovoljenja. Četudi za varnost računalniških sistemov ni posebnega nadzora ali posebnih programov, ki ščitijo vstope v sisteme (Schwartau 2000, 41).

[14] Ta pojav se v angleščini imenuje »social engineering«, ki ga natančneje opišem v nadaljevanju.

[15] Do računalnikov lahko posamezniki dostopajo tudi prek t.i. *remote access*-a, ki omogoča oddaljen dostop do računalnikov ali omrežij. V različnih organizacijah ljudje potrebujejo takšne dostope zaradi narave svojega dela (npr. poslovna potovanja) (Searchsecurity.com 2008).

4.4 Generacijski pregled hekerjev skozi zgodovino

Hannemyr prvotne hekerje opredeljuje kot računalniške strokovnjake iz obdobja šestdesetih let prejšnjega stoletja, izraz »hekanje« pa opredeljuje kot sinonim za računalniško delo, posebno če je dodana določena mera strokovnosti. V sedemdesetih letih se je izoblikovala t.i. tehno-hipijevska hekerska (sub)kultura kot protikulturni vzorec. Bistvo druge generacije hekerjev je bila, da bi vsi državljani imeli dostop do računalniških sistemov in da bi računalniki bili skonstruirani tako, da ne bi bili preveč zahtevni za učenje. V osemdesetih letih se izoblikuje današnji pomen izrazov »heker«, »hekanje« in »hekerstvo«, ki bistveno spremenijo odnos do hekerjev (Hannemyr v Taylor 1999, 23).

4.4.1 Prva generacija

Levy, ki hekerje razdeli v tri generacije, prvo generacijo opredeli za računalniške entuziaste v 50. in 60. letih prejšnjega stoletja na Massachuttets Institute of Technology (MIT), kjer so študentje in raziskovalci instituta imeli nalogo programiranja (Taylor 1999, 23).

Mladi, hitro rastoči um inštituta je ustvaril termin hekanja oziroma takrat termin bližnjic programiranja. Hekerstvo je imelo pozitivno vlogo v takratnem obdobju, saj je beseda heker označevala posameznika, ki lahko s pomočjo teh bližnjic izkoristi šibkosti programov in definira meje delovanja programov. Študentje so prav tako bili začetniki razvoja etičnega kodeksa hekanja – verjeli so v svobodo informiranja in tehnologije. V tem obdobju hekerji niso ogrožali varnosti drugih uporabnikov. Hekerji iz te generacije so bili le izdelovalci računalniške programske opreme. Medije in ostalo javnost je pritegnil članek iz leta 1971, ki je govoril o novem fenomenu telefonskih hekerjev, v angleščini imenovanih *phone phreakers*. Članek je poudaril metode teh skupin, celo posameznikov, ki so ukanili telefonski sistem ZDA in brezplačno telefonirali po vsem svetu. *Phreaking* je sestavljanka angleških besed *freak*, *phone* in *free*. Phreakanje se je hitro razširilo po Bellovi zamenjavi človeških operatorjev z računalniškimi.[16] Novi neposredni klicni sistem je temeljil na multifrekvenčnih tonih. Tako je bilo mogoče s pomočjo kombinacije tonov onesposobiti centralo, ki ni utegnila zabeležiti prekinitve klica, poleg tega pa je lahko klicatelj opravil klic, ki ga centrala ni mogla ne zabeležiti in ne zaračunati uporabniku. Vsekakor je v tem obdobju phreakanje pomembno pripomoglo k nadaljnjemu razvoju in razširitvi hekerstva, saj je sčasoma hitro postalo ena izmed najhitrejše

[16] Novembra 1960 začnejo telefonske klice prvič preusmerjati računalniki (Firedragon 888 2008).

rastočih subkultur - virtuozov sodobne komunikacije.

Kot sem že omenil, je hekerstvo do pojava osebnih računalnikov bilo omejeno zgolj na phreakestvo ali zgolj na tiste posameznike, ki so imeli dostop do računalnikov. Vsekakor se zgodovina takšnega hekerstva, kot ga poznamo danes, prične na začetku osemdesetih, ko so osebni računalniki prešli tudi v domove Severne Amerike in Evrope. Za večino nove generacije mladoletnikov so računalniki in hekanje postali nov način življenja (Heaton 2000).

4.4.2 Druga generacija

Druga generacija je bila povsem v znamenju rasti računalnikov in s tem tudi hekerske subkulture. Hekerji so se pogosto sestajali v okviru različnih skupin, kjer so si izmenjavali tehnike hekanja. Vstopnico na takšne sestanke so si posamezniki lahko zagotovili le z dokazovanjem računalniške spretnosti ali z že doseženo slavo. Nekateri hekerji so se v tem obdobju povezali v kohezivne skupnosti in skupine.

Strehovec (2003, 307) opisuje hekersko (sub)kulturo nekje med kreativnostjo in prestopništvom ter pravi, da »hekerji nikakor niso homogena družbena skupina, njihova identiteta je kar se da izmuzljiva in velike razlike so tudi med različnimi generacijami hekerjev. Iz prve, nedvomno romantične generacije konzolnih kavbojev so mutirali v veliko bolj sofisticirano družbeno podskupino, ki jo vedno manj zanima idealizem, solidarnost in uresničevanje *on-line* etike. Tudi reakcije na njihovo dejavnost so kar se da ambivalentne, segajo od odobravanja in simpatij do ostrega zavračanja ter policijskega in sodnega pregona. O hekerjih lahko izvemo zato veliko le, če opazujemo obe strani tega kompleksnega pojava (so medmrežni »underground« in to nikakor niso), namreč tisto, kaj hekerji mislijo o sebi, kako se predstavljajo in, na drugi strani, kakšna je družbena reakcija na ta pojav, kako so, preprosto rečeno, videti v očeh drugih.«

Prav tako Strehovec poudari, da je hekerska (sub)kultura bistveno povezana z računalniškimi aktivnostmi hekerjev, zanjo je zato značilno, da sodi na področje nematerialnih količin in kvalitet, in sicer na podatkovno področje, k svetu informacij. Po avtorjevem mnenju imamo opravka s posebno vrsto subkulture, ki ima izrazito nematerialen značaj, in z nematerialnimi kvalitetami je povezan tudi hekerski slog. Ni jih mogoče prepoznavati po zunanjih materialnih značilnostih, recimo oblačilih, pričeskah, motorjih, razvidnih mestih druženja (kar je bilo značilno za subkulture rokerjev, hipijev in pankerjev), nasprotno, so elita

medmrežja, za katero so geografske, materialne in tudi statusne ter nacionalne opredelitve nebistvene. To pa posebno velja za sodobne generacije hekerjev, medtem ko so bili zgodnji hekerji v 60. in 70. letih 20. stoletja še vezani na fizično skupnost in neposredno komuniciranje, kajti bili so programerji, raziskovalci in študenti v laboratorijih znanih ameriških univerzitetnih središč, pogosto torej kar sodelavci pri projektih, ki so vključevali tudi neposredno komuniciranje v fizičnem prostoru (Strehovec 2003, 308–309).

V sedemdesetih letih prejšnjega stoletja so se tako pojavile skupine, ki so poudarjale moč in razsežnosti nove tehnologije. Tako hekerje iz drugega obdobja Hannemyr označuje tudi kot aktiviste, ki so si globoko prizadevali, da računalnike potrebno preureditijo tako, da bodo lahko dosegljivi vsakemu posamezniku. Hekerji iz drugega obdobja so tako postali tudi začetniki javno dostopnih računalniških točk in izraziti zagovorniki osebnega računalnika (ang. personal computer, krat. PC) (Hannemyr 1997).

4.4.3 Tretja generacija

V 80. letih prejšnjega stoletja je prišlo do prvih zlorab in zlonamernih napadov hekerjev, s tem pa tudi prvih hekerjev, ki so bili obtoženi kraje informacije, neavtoriziranega dostopa do zaupnih informacij, računalniškega sleparstva ipd. Sčasoma hekerjem dostop do informacij in pregled nad vsebino sistemov ni več zadostoval, zato so svoje veščine uporabili tudi v individualno[17] korist. Za hekerje iz te generacije je torej značilna profitna miselnost in ne etični kodeks prvotnih hekerjev. Prve hekerske napade z uporabo virusov beležimo proti koncu 80. let prejšnjega stoletja, ko so virusi postali učinkovito orožje, uperjeno proti različnim posameznikom oz. organizacijam, posebej pa so ti napadi povzročali preglavice računalniškim programerjem protivirusnih programov.

Devetdeseta leta prejšnjega stoletja se niso bistveno razlikovala od prejšnjega obdobja, le da se je obseg napadov bistveno povečal. V General Accounting Office (GAO Report) v ZDA so leta 1995 v svojem poročilu napisali, da so na ministrstvu za obrambo ZDA samo tistega leta zabeležili okoli 250.000 hekerskih napadov. Tarče tovrstnih napadov v tem obdobju so bile tudi spletne strani in informacijske podatkovne baze NASE, FBI, CIA, Vojaškega letalstva ZDA, itd. (Trigaux 2000).

Hekerji so tako še vedno spretno izkoriščali svoje znanje in povzročali finančne in

[17] Mišljeno predvsem v finančnem smislu.

materialne težave svojim tarčam. Tako so v začetku prejšnjega desetletja hekerji npr. povzročili deveturno prekinitev delovanja interneta v vsej ZDA, uspešno »pridobili« podatke o kreditnih in bančnih računih in posledično preusmerili denar na račune po vsem svetu[18] (About.com: PC World Computing Center 2008).

4.5 Metode dela hekerjev

V naslednjem delu bom posvetil nekoliko več pozornosti metodam dela hekerjev. Resnica o sposobnostih hekerjev je večkrat napačno prikazano v filmih in znanstveno-fantastični literaturi. Hekerje pogosto odlikuje kombinacija izpopolnjenih računalniških veščin in znanj o delovanju komunikacijskih sistemov in omrežij, v katera poskušajo vstopiti/vdreti, prav tako pa je izjemnega pomena tudi morebitna informacija, do katere hekerji pridejo s pomočjo notranjih sodelavcev, upravljavcev teh sistemov. Obstajajo tri različne metode, preko katerih si posameznik lahko priskrbi pomembne informacije za nadaljnje vdiranje v sistem: a. preko socialnega inženiringa, b. z uporabo nadzorne programske opreme (ang. *surveillance software*) in s spyware-om, c. z uporabo drugih programov in ukradenih gesel (Wall 2007, 58–59).

4.5.1 Socialni inženiring (ang. *Social Engineering*)

Socialni inženiring je tehnika, s katero z uporabo poznavanja psihologije ljudi, poznavanjem delovanja računalniških sistemov in terminologije ter z uporabo majhnih in »verjetnih« laži pripravimo ciljne osebe, da storijo ali opustijo stvari, katerih običajno ne bi storili ali opustili za tujce ali nepoznane osebe. Gre torej za metodo, ki temelji na psihologiji in sociologiji, s pomočjo katere napadalec »upravlja« z ljudmi napadene organizacije, ki posedujejo ali pa imajo dostop do informacije, ki jih napadalec potrebuje. Napadalec lahko poizkuša pridobiti dostop do njemu zanimivih informacij, lahko samo delčkov, iz katerih sestavlja sliko (ang. *big picture*). Pri tem se poslužuje metod prepričevanja, brskanja po smeteh, direktnega napada, socialnega inženiringa prek telefona ipd. Socialni inženiring pa v podobnih oblikah najdemo v vseh panogah (Cerle 2005, 25).

[18] Ruski krekerji so prestregli 10 milijonov USD, ki so bili v lasti Citibank. Večino denarja so oblasti uspele pridobiti nazaj, okoli 400.000 USD jim ni uspelo najti (About.com: PC World Computing Center 2008).

Cikel dobrega socialnega inženiringa (Radulj v Cerle 2005, 27):

1. Raziskovanje:
    a) izbira cilja, namen, motiv;
    b) proučevanje in uporaba terminologije;
    c) zbiranje koščkov podatkov in informacij;
2. Razvijanje odnosa in pridobivanje zaupanja.
3. Izkoriščanje zaupanja.
4. Uporaba informacije:
    a) razširitev pristopa: 1. pregledovanje; 2. postavljanje programov za analizo in nadzor sistema; 3. uporaba stranskih vrat ali pasti; 4. izkoriščanje napak v programih.
5. Izvršitev napada.
6. Uničevanje dokazov – brisanje sledi (Cerle 2005, 25–28).

Wall socialni inženiring opredeljuje kot tehniko hekanja z namenom pridobiti dostop do notranjih informacij ali gesel, torej preko zaposlenih v tarčni organizaciji. Hekerji, ki uporabljajo to metodo dela, uporabljajo in predstavljajo svoje znanje določenih sistemov tako, da se v očeh sistemskih upravljavcev prikažejo kot posamezniki, ki imajo pravico do vstopa v sistem. Posamezniki se tako naučijo jezika organizacije, uporabe zaupnih terminov in si s tem odprejo pot v sistem; tako si heker priskrbi vse potrebne informacije ter skuša vstopiti v sistem preko osebe, ki mu je podatke zaupala. V primeru, da mu kontaktna oseba ne zaupa vseh potrebnih informacij, si heker poskuša osebne podatke pridobiti iz zavrženih dokumentov, ki jih pogosto v nadaljnjih pogovorih uporabi z namenom ponovnega dokazovanja svoje verodostojnosti. V določenih primerih lahko ti dokumenti vsebujejo vse potrebne informacije za vstop v želen sistem (Wall 2007, 59).

Mitnick tako v svojem delu *The art of deception* na podlagi lastnih izkušenj podrobno opisuje to metodo dela in meni, da je ena izmed bolj sofisticiranih tehnik socialnega inženiringa tudi lažno predstavljanje z uporabo verodostojnih dokumentov, kot so npr. ponarejene službene kartice (ang. *impersonating staff*). Prav tako ta metoda ponuja nasproten pojav socialnega inženiringa (ang. *reverse social engineering*), saj lahko heker poskuša v določenem sistemu ustvariti tehnični problem in ga tako kot pooblaščen izvajalec popraviti in s tem dobiti dostop do

informacij. Takšni napadi, v katerih napadalec pripravi oziroma nastavi določeno situacijo, pomenijo, da v končni fazi žrtev napada pokliče na pomoč napadalca samega (Mitnick in Simon 2002, 60).

Mitnick navaja tudi nekaj splošnih metod socialnega inženiringa, s pomočjo katerih si hekerji pridobijo želene informacije. Mednje spadajo: 1. predstavljanje za sodelavca; 2. predstavljanje za delavca iz partnerskega podjetja, družbe ali pravne službe; 3. predstavljanje za nekoga iz oblastvenih organov; 4. predstavljanje za novega zaposlenega v podjetju, ki potrebuje pomoč; 5. pošiljanje trojanskih konjev v priloženi e-mail pošti; 6. pošiljanje brezplačne programske opreme za namestitev ali posodabljanje, ipd. Prav tako je Mitnick mnenja, da so podjetja z večjim številom zaposlenih bolj ogrožena ko manjša podjetja, saj so informacije lažje dostopne, prav tako naj bi bila velika podjetja bolj ranljiva zaradi preslabo razvitega varnostnega sistema proti vdorom (Mitnick in Simon 2002, 332–333).

Na vojaško-obrambnem področju socialni inženiring bolje poznamo kot konglomerat *psiholoških operacij*, *informacijskih operacij in operacij zavajanja*. Ministrstvo za obrambo ZDA *psihološke operacije* (ang. Psychological Operations, kraj. PsyOps) definira kot načrtovane operacije z namenom prenosa skrbno izbranih informacij do nasprotnikovih sil, s ciljem vplivanja na njihova čustva, ravnanje, mišljenje ter obnašanje in v končni fazi vplivati na odločitve vlad, organizacij, skupin ali posameznikov. Bistvo teh operacij je torej prepričati nasprotnikovo vedenje v korist izvajalca teh operacij (IWS 2007).

Tarča *informacijskih operacij* je v prvi vrsti vodstveni oz. poveljujoč kader. Cilj teh operacij je nasprotnika prepričati ali celo siliti v neko dejanje ali ga od tega odvrniti. Bistveno pri informacijskih operacijah je vplivati na poveljujoči kader s pomočjo različnih metod zavajanja ali prevar, izvajanja psiholoških operacij in elektronskega bojevanja, z namenom izoblikovanja in vplivanja na informacijsko okolje nasprotnika. *Informacijske operacije* (ang. Information operations, kraj. InfoOps) lahko tako definiramo kot akcije z namenom vplivanja na nasprotnikove informacije in informacijske sisteme, medtem ko se obenem izvajajo akcije zaščite lastnih informacij ter informacijskih sistemov. Informacijske operacije naj bi se izvajale v predkonfliktni fazi, torej pred samim konflikom (Kuehl 2002, 11–12).

Operacije vojaškega zavajanja (ang. Military deception, kraj. MILDEC) so akcije namernega zavajanja nasprotnikovega poveljuječega kadra. Cilj teh operacij je nasprotnikove

enote »preusmeriti«, jih zavesti tako, da bodo delovale v korist naših enot. Ključni elementi operacij zavajanja so:

1. *Izbira tarče:* zavajanje mora biti usmerjeno proti nasprotnikovemu vodilnemu, poveljujočemu kadru, saj so poveljniki tisti, ki dajejo povelja.

2. *Cilj:* prioritetna naloga zavajanja je nasprotnikove poveljujoče prisiliti v neko dejanje ali jih od teh dejanj odvrniti in ne samo nasprotnikove enote seznaniti z našimi nameni.

3. *Enoten nadzor nad izvajanjem zavajanja:* operacije morajo biti skrbno pripravljene in izvedene tako, da v nasprotnikove vrste ne vnesejo zmede. Pri tem je potrebno paziti, da različni elementi operacije odražajo jasno sliko cilja in da morda operacija zavajanja ne ogroža drugih ciljev.

4. *Zagotovitev varnosti pred izvajanjem operacije:* varnost pred samo izvedbo operacije zavajanja je ključnega pomena, saj je potrebno natančno izvesti tudi zaščito operacije. (npr. komu zaupati informacije o načrtih in poveljih).

5. *Pravočasnost:* operacije zavajanja morajo biti pravočasno načrtovane in izvedene, saj je potrebno upoštevati, da obveščevalne službe nasprotnika morajo informacije pravočasno pridobiti in jih analizirati. Tako je potrebno upoštevati, da traja nekaj časa, preden nasprotnikove enote reagirajo na našo objavo zavajajočih informacij.

6. *Integriranost:* operacije zavajanja morajo biti povsem integrirane v osnovno operacijo, ki jo podpirajo. Načrtovanje operacij zavajanja mora tako teči sočasno s samim načrtovanjem osnovne operacije (Joint Chiefs of Staff, I–3).

4.5.2 Uporaba vohunske in nadzorne programske opreme

Druga najbolj pogosta oblika napadov hekerjev je uporaba prikrite in nadzorne programske opreme, to so t.i. vohunski programi (ang. *spyware software*), namenjeni zbiranju podatkov o uporabnikih (Wall 2007, 60).

Vohunski programi ali »spyware« (ang. *spying software*) je izraz, ki označuje tiste programe, katerih funkcija je vohunjenje in zbiranje podatkov o aktivnostih in navadah uporabnikov interneta, pri čemer le-ti ne vedo natančno, čemu so ti programi namenjeni, jih

sploh ne prepoznajo ali pa ne vedo, da jih imajo na svojem računalniku nameščene. Ta vrsta programov je zelo podobna trojanskim konjem. Spyware[19] je v osnovi marketinško orodje za zbiranje informacij o uporabnikih. Predvsem gre za splošno tržno poizvedovanje o njihovih kupnih navadah na osnovi dejanskih nakupov preko svetovnega spleta ali pa zgolj na osnovi internetnih aktivnosti. Na ta način zbirajo informacije o tem, kaj je uporabniku všeč in kaj ga zanima. Te informacije uporabijo podjetja, ki so vohunske programe zaradi tržnih interesov razvila ali pa te informacije prodajajo naprej za lepo vsoto denarja zainteresiranim tretjim osebam. Do tržnih in posledično finančnih pridobitev se podjetja torej dokopljejo na dokaj moralno vprašljiv in neetičen način. So pa tovrstna programska orodja v nekaterih primerih celo sprejemljiva in opravičljiva (na delovnem mestu[20] ali starševski nadzor nad otroki), a pogosteje se vseeno uporabljajo za neetično zbiranje informacij o uporabnikih (Močnik 2005, 61–62).

Spyware programska oprema deluje podobno kot računalniški virusi. Namesti se samostojno na računalnik in tam skrivno deluje. Prav tako se spyware samostojno namesti v operacijskem sistemu, kar pomeni, da se vedno, ko uporabnik prične uporabljati računalnik, program samostojno zažene. Spyware ni tako nevaren[21] kot računalniški virusi, saj delovanje računalnika samo bremeni, medtem ko ga lahko računalniški virus trajno onesposobi (Winkler 2005, 148).

Spyware pravzaprav izvaja veliko aktivnosti in večina teh je škodljiva. Njegova glavna funkcija je iskanje in posredovanje informacij. Omenjena programska oprema pa lahko išče tudi bolj delikatne informacije, kot je številka kreditne kartice, številka socialnega zavarovanja, telefonske številke, naslovi, uporabniška imena, gesla in internetna zgodovina.

Obstaja vrsta različnih programov, ki predstavljajo različno mero škodljivosti oziroma zahrbtnosti - tako so lahko npr. piškotki (ang. *http cookies* ali samo *cookies*), ki pomagajo uporabnikom preveriti kredibilnost na določenih spletnih straneh, slediti in ohraniti določene informacije o uporabnikih. Kovačič (2003, 106) opredeli piškotke kot »majhne pakete podatkov, ki jih spletni strežnik pošlje spletnemu brskalniku, le-ta pa te podatke shrani na uporabnikov

[19] Pri spywaru gre v bistvu predvsem za nelegalno programsko opremo.
[20] Glede nadzora uporabe določene programske opreme ali elektronske pošte pri zaposlenih je potrebno doreči, da obstajajo bistvene razlike pri izvajanju tega v Evropi in v Združenih državah Amerike. Bistvena razlika je ta, da smo v Evropi zasebnosti komunikacij na delovnem mestu bistveno bolj naklonjeni kot v ZDA, kjer lahko podjetje zaposlenega nadzoruje brez obvestila, če le-ta uporablja opremo podjetja, čeprav se Vrhovno sodišče ZDA o tem še ni povsem razjasnilo (Kovačič 2004).
[21] Spyware programska oprema se ponavadi namesti zraven različnih brezplačnih programov, načeloma ni nevarna, vendar je precej nadležna, saj se pogosto pojavlja kot pojavno okno na ekranu v obliki oglasov.

računalnik in jih vrne strežniku, ko ta to od njega zahteva«.

Hekerji pogosto uporabljajo tudi programsko opremo prestrezanja, to programsko opremo označimo tudi kot *vohljače* (ang. *sniffers*, *sniffing*). Tako lahko hekerji z namestitvijo omenjene programske opreme npr. s prestrezanjem in krajo gesel (ang. *password sniffing*) prestrežejo paketke, ki vsebujejo podatke o uporabniških imenih in geslih. S pomočjo prestrezanja paketkov lahko napadalec spremlja in analizira promet tujih računalnikov. Prestrezanje paketkov (tim. *promisc sniffing*) je bilo včasih posebej priljubljeno na lokalnih Ethernet omrežjih, ki so temeljila na tehnologiji koncentratorjev (ang. *hub*). Takšna omrežja so omogočala, da vsi računalniki v posameznem delu omrežja spremljajo promet vseh računalnikov v istem delu omrežja. Če je posamezen računalnik vključil t.i. »*promisc* način«, je lahko prisluškoval prometu ostalih računalnikov v omrežju. Vendar pa je to tehniko mogoče zaznati. Današnje prestrezanje podatkov poteka predvsem preko spremljanja prometa na usmerjevalnikih (ang. *router*) oziroma podatkovnih povezavah (Kovačič 2003, 107).

4.5.3 Uporaba zlonamerne programske opreme (ang. malicious software, krat. malware)

Tretji način pridobivanja in zbiranja informacij je preko zlonamerne programske opreme, pogosto označene kot tehnika nove generacije hekerjev.

Škodljiva koda ali »malware« je dokument, sporočilo ali program, ki je napisan in namenjen povzročitvi kakršne koli škode in se običajno konča z zlorabo oziroma izgubo podatkov ali z zmanjšanjem produktivnosti delovanja našega informacijskega sistema. Posledice nekaterih škodljivih programov so lahko uničujoče in zelo očitne, medtem ko rezultatov delovanja nekaterih drugih škodljivih programov niti ne zaznamo ali pa so prav tako močno škodljivi pa jih ne opazimo, dokler ni prepozno. Škodljive programe lahko razdelimo v dve skupini, in sicer:

1. V prvo skupino spada tisto, kar se širi na način, kot se širi in reproducira tudi naravni virus prehlada ali gripe (od tod tudi prihaja beseda). Sem štejemo računalniške viruse in črve.
2. V drugo skupino štejemo vse ostale programe, ki se ne širijo po principu virusne okužbe in lahko kakor koli škodujejo našim informacijskim sistemom (trojanski konji, vohunski in reklamni programi, t.i. dialerji, ipd.).

Škodljivo delovanje vsakega od teh programov je različno in tudi ukrepi proti njim oz. za njihovo odstranitev iz našega sistema so specifični za vsakega posebej. Na splošno pa velja, da zlonamerna programska oprema lahko škoduje računalniku samemu ali pa podatkom, ki so na njem shranjeni. Prav tako lahko upočasni internetno povezavo ali pa uporabi računalnik za svojo reprodukcijo in širjenje na ostale informacijske sisteme (Močnik 2005, 55–56).

Malware oz. škodljivo programsko opremo lahko delimo tudi glede na:

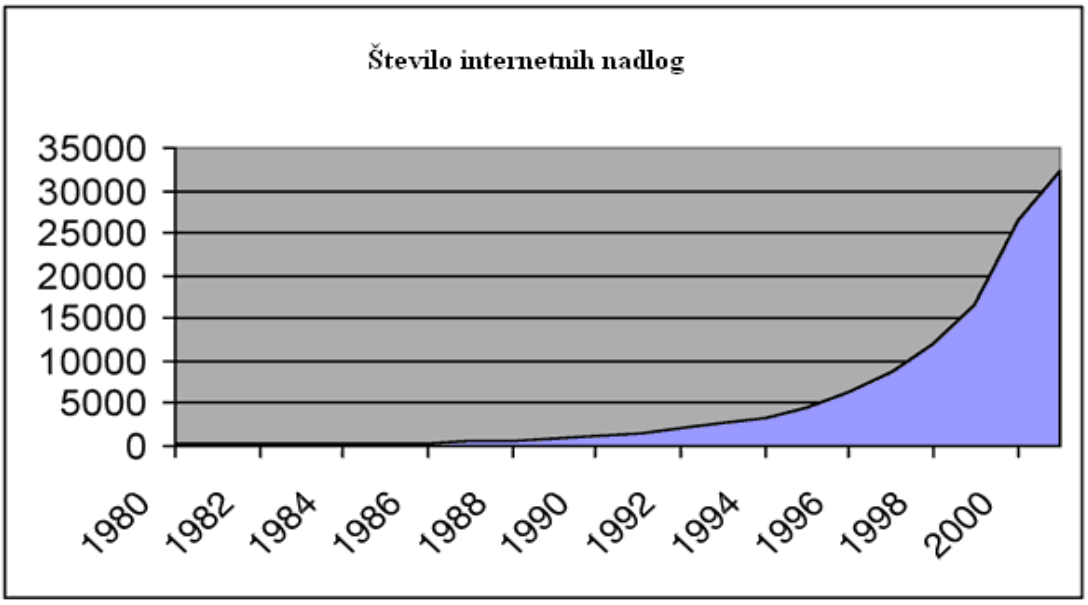
1. *Škodljivost* (posledice oz. stopnja škodljivega delovanja, ki jo tovrstno programje povzroči, je lahko visoka, srednja ali nizka. Prav tako moramo upoštevati posredno in neposredno škodo, ki nastane ob njihovem aktiviranju. Nekateri programi so napisani zelo specifično, zato delujejo zelo neposredno in na točno določen način (npr. brišejo in uničujejo datoteke), medtem ko drugi, kot denimo programi, za masovno pošiljanje sporočil ali DoS (ang. Denial of Service) napadi, povzročajo posredno škodo z znatno upočasnitvijo internetne povezave ter upočasnitvijo internetne povezave ter upočasnitvijo delovanja informacijskega sistema).
2. *Zmožnost reprodukcije in širjenja* (hitrost in zmožnost širjenja je ena izmed bolj specifičnih lastnosti posameznega škodljivega programa. Nekateri se sploh ne razmnožujejo in širijo, medtem ko se drugi, kot, denimo nekateri internetni črvi lahko razširijo precej hitro. Nekateri zlonamerni programi uporabljajo celo več tehnik reprodukcije in širjenja).
3. *Dejanska razširjenost* nekega programa je lahko visoka, srednja ali nizka in se meri glede na geografsko razpršenost ter glede na ocene proizvajalcev in prodajalcev antivirusnih in ostalih aplikacij za zaščito informacijskih sistemov (ibid., 56–57).

V zadnjem desetletju smo priča porastu kriminalnih dejanj in sodelovanju med hekerji in programerji virusov ter nezaželene elektronske pošte (ang. spam.), posledično tudi napredku pri izdelavi hekerskih orodij, kar je vodilo v strukturiranje posebne hekerske industrije. Rezultat tega je, da se je hekerstvo izjemno hitro razvilo v asimetrično dejavnost skozi uporabo sofisticirane programske opreme, npr. trojanskih konjev, računalniških črvov in virusov[22]. S pomočjo posebne

[22] Računalniški virus: širše s tem izrazom označujemo vse programe ali programske kode, namenjene povzročanju škode ali obremenjevanju računalniških sistemov in z zmožnostjo, da se sami širijo. Ločimo destruktivne in instruktivne viruse (Kovačič 2003, 108).

programske opreme (ang. *remote administration trojans*[23], krat. RAT) pa lahko napadalec v končni fazi iz daljave nemoteno upravlja z računalniškimi sistemi (Wall 2007, 60).

Slika 4.1: Prikaz porasta računalniških groženj v zadnjih desetletjih.



Vir: Spyware Killer and Spyware Detector software 2005.

4.5.4 Hekerski vdori

Vdor v računalniški sistem je običajno povezan z veliko znanja in vloženega truda, zato napadalci po uspešnem vdoru naredijo vse, da bi do takega sistema lahko imeli prikrit dostop tudi v prihodnje. Glavni razlog, zaradi katerega napadalci vdirajo v računalniške sisteme, je iskanje informacij, zato se v napadih uporabljajo programi za beleženje pritiskov tipk, programi za spremljanje omrežnega prometa oz. vohljači itd. V nekaterih primerih pa je napadalčev cilj predvsem uničenje sistema, zato vanj namesti logično bombo[24], ki bo po preteku vnaprej določenega časa uničila pomembne podatke. Vsi taki programi morajo v sistemu ostati

[23] So trojanskim konjem podobna orodja, ki napadalcu omogočajo popoln nadzor in upravljanje z našim računalnikom (Močnik 2005, 63).
[24] Logične bombe ne štejemo med viruse, ker se ne razmnožujejo. Prav tako se v nasprotju z virusi aktivirajo takoj in nato prenehajo s svojim delovanjem. Nekateri jih ne bi uvrstili niti med programe, saj so pravzaprav zgolj zamaskirani elementi drugih programov. Njihova naloga je uničiti podatke na računalniku takrat, ko so za to izpolnjeni vsi pogoji (Močnik 2005, 66).

neopaženi tako pred protivirusnimi programi kakor tudi aplikacijami anti-spyware (Bratuša 2006, 87).

Šele ko heker pridobi administratorsko geslo, lahko govorimo o vdoru. Če vdora ne opazimo, lahko pričakujemo naslednji scenarij: napadalec bo nastavil daljinski pristop ukazni vrstici ali celo orodje za daljinsko upravljanje z grafičnim vmesnikom z administratorskimi pooblastili, izključil spremljanje (ang. *auditing*), če je vključeno, izvlekel druge uporabniške račune in gesla ter jih skušal razbiti, namestil program za beleženje pritisnjenih tipk s tipkovnice, namestil trojanske programe, programe za prisluškovanje omrežnemu prometu, iz tega računa napadal tretje sisteme ter prikril ali odstranil sledi svojega vdora (ibid., 79).

Potek dejavnosti hekerja po vdoru (ibid., 79–94):

1. *Oddaljen dostop*. Heker si po vdoru sprva poskuša s pomočjo programske opreme omogočiti oddaljen dostop, saj lahko preko specifične programske opreme iz svojega računalnika upravlja z napadenim računalniškim sistemom. Ko si heker zagotovi dostop lahko tako v tarčni sistem vnaša poljubne ukaze in namešča programsko opremo.
2. *Izvlečenje in razbijanje gesel*. Z nameščanjem posebne programske opreme lahko heker iz tarčnega računalniškega sistema izvleče uporabniška imena in gesla. Potem ko heker izvleče šifrirana gesla (natančneje njihove *hashe*), lahko s programi, kot so LC5, John the Ripper ipd., pridobi gesla v besedilni obliki.
3. *Programi za beleženje pritisnjenih tipk.* S pomočjo omenjenih programov ima napadalec možnost, da iz napadenega računalnika pridobi nadaljnje zaupne podatke, kot so gesla in številke kreditnih kartic. Ti so nameščeni med strojno opremo (tipkovnico) in operacijskim sistemom ter zabeležijo vsako pritisnjeno tipko. Obstaja več takih programov, od katerih nekateri poleg beleženja tipk nudijo še različne druge vrste vohunjenja za uporabniki[25].
4. *Odpiranje sovražnih uporabniških računov.* Hekerji v kompromitiranih oz. vdrtih sistemih običajno izdelujejo svoje uporabniške račune z administratorskimi pooblastili,

[25] Invisible Keylogger je eden najzmogljivejših programov za beleženje pritisnjenih tipk, ki omogoča tudi spremljanje mnogih drugih aplikacij. Program se prodaja legalno, kot orodje za spremljanje dejavnosti otrok, zakonskih partnerjev in zaposlenih v izbranem računalniku. Verjetno pa je jasno, da večina strank uporablja program za nepoštene namene, pred kratkim so na primer v ZDA odkrili učenca, ki je program namestil v učiteljev računalnik, razbral izpitna vprašanja (in jih prodajal sošolcem) (Bratuša 2006, 83).

ker so administratorji običajno pozorni na svoje račune in ker lahko svoja gesla tudi spremenijo.

5. *Oddaljen nadzor.* Tudi če ima napadalec administratorsko geslo, mu to ne pomaga prav veliko, če se ne more prijaviti v sistem, ker v računalniku ne deluje primerna aplikacija (npr. SMB – Server Message Block, telnet). Zato napadalci ob prvi priložnosti v napadeni računalnik namestijo katerega od programov za oddaljeni nadzor. To so tako imenovana stranska vrata (ang. backdoor)[26].
6. *Koreninski kompleti (*ang. *rootkiti).* Termin »rootkit« je med računalniškimi zanesenjaki prisoten že več kot deset let. Rootkit je pravzaprav paket, sestavljen iz majhnih in uporabnih programov, ki napadalcu omogočajo ohranjanje dostopa na ravni uporabnika s sistemskimi ali z administratorskimi pooblastili. Koreninske komplete (rootkit programe) lahko torej definiramo kot skupek programov, ki napadalcu omogoča stalno in prikrito prisotnost v napadenem računalniku. Pri programih rootkit gre torej za tehnike in mehanizme skrivanja zlonamernih programov, kot so virusi, vohunski programi in trojanski programi, predprogrami za blokiranje vohunjenja, protivirusnimi programi in orodji za upravljanje sistema. Programi Rootkit se delijo v več skupin glede na to, ali preživijo ponovni zagon ali ne ter ali se izvajajo v uporabniškem načinu (ang. *user mode*) ali v jedru operacijskega sistema (ang. *kernel mode*). Omenjena programska oprema deluje na podlagi preprostega koncepta, imenovanega modificiranje. Na kratko povedano, programska oprema je ustvarjena zato, da opravlja določene odločitve na podlagi posredovalnih podatkov. Rootkit je dejavnik, ki povzroči spremembo programske opreme tako, da bo ta sprejemala napačne odločitve. V računalniških sistemih je veliko mest, ki so za modifikacije še posebej primerna.
7. *Zakrivanje sledi.* Hekerji običajno takoj po vdoru izključijo varnostno beleženje (ang. *auditing*), odstranijo pa tudi v sistemskem dnevniku že zabeležene dogodke, ki se nanašajo na njihov vdor. S posedovanjem administratorskega gesla to ni težko in ga je mogoče izvesti ročno s pomočjo posebne programske opreme in orodij. Zadnje, kar si napadalec želi, je, da legalni uporabnik v svojem računalniku odkrije njegove datoteke.

[26] Backdoor ali »odpiralec stranskih vrat« je program, ki se brez naše vednosti namesti v naš sistem. Ko se zažene, odpre stranska vrata, skozi katera omogoči napadalcu administrativni dostop do našega sistema. Aktivnosti, ki jih napadalec nato izvaja, so lahko uničujoče. Lahko uničuje datoteke, zbriše vsebino iz trdega diska ali celo pokrade zaupne informacije z našega sistema, ki jih lahko zlorabi ali proda naprej. Primeri takšnih programov so: Orifice2K.sfx, Bionet.318, Antilam in Subseven.213 (Močnik 2005, 63).

Zaradi tega jih skuša narediti čim manj opazne. V ta namen uporablja nevpadljiva imena ter shranjuje na mesta, ki jih uporabnik redko obiskuje. Poleg tega jih lahko naredi nevidne za običajno pregledovanje, z ukazom 'dir' pa tudi za Raziskovalca.

Seveda lahko hekerji napadejo tudi spletne aplikacije in spletne strežnike. Bratuša v delu *Hekerski vdori in zaščita* opisuje metodologijo spletnega napada. Osnovni koraki metodologije napada so (Bratuša 2006, 109–112):

a) *profiliranje infrastrukture* (temeljito razumevanje spletne infrastrukture),
b) *napad na spletni strežnik* (veliko znanih varnostnih pomanjkljivosti spletnih strežnikov je vzrok, zaradi katerega se napadalec pogosto odloči za ta pristop, ki je največkrat tudi uspešen),
c) *pregled spletne aplikacije* (kadar napadalec v spletnem strežniku ne odkrije varnostnih pomanjkljivosti, se ponavadi osredotoči na spletno aplikacijo in tehnologijo v uporabi (ASP, Java, PhP,…),
d) *napad na avtentikacijske mehanizme* (ko napadalec med pregledom spletne aplikacije naleti na avtentikacijo, lahko upravičeno domneva, da se v ozadju skrivajo občutljivi podatki. Najpogosteje se takih mehanizmov loti z orodji za samodejno ugibanje gesel ter s prestrezanjem in ponarejanjem piškotkov.),
e) *napad avtorizacijskih shem* (ko je uporabnik avtoriziran za vstop v sistem, lahko napad nadaljuje tako, da si bo z njim pridobil dostop do informacij, do katerih prej ni imel dostopa),
f) *izvedba funkcionalne analize* (gre za naslednji kritični element pregledovanja spletne aplikacije, v katerem se napadalec posveti posameznim elementom spletne aplikacije, kot so npr. oddaja ter potrditev in spremljanje naročila. Na tej stopnji poizkuša napadalec v aplikacijo vnesti parametre, ki mu bodo omogočili dostop do ključnih delov aplikacije),
g) *izkoriščanje podatkovnih povezav* (nekateri izmed najbolj uničujočih napadov na spletne aplikacije so pravzaprav usmerjeni na zbirke podatkov Back end. To so namreč mesta, kjer se hranijo najzanimivejše informacije o strankah, partnerjih ipd.),
h) *napad na vmesnik za upravljanje spletne aplikacije* (to je oddaljeni nadzor in upravljanje (ang. remote management) spletnih aplikacij. Spletne aplikacije namreč delujejo 24 ur dnevno in vse dni v tednu, zato bi bilo od administratorja neprimerno pričakovati

neprestano sedenje v nadzornem središču. Napadalci se take situacije še kako zavedajo, zato dobro vedo, da ima vsaka spletna aplikacija nekje odprta vrata, ki administratorju omogočajo oddaljeni nadzor in upravljanje aplikacije kakor tudi zbirk podatkov),

i) *napad na odjemalca*[27] (področje, ki ga preizkuševalci spletnih aplikacij pogosto zanemarijo, je varnost spletnih odjemalcev. Uporabniki spletnih aplikacij so tako velikokrat prepuščeni na milost in nemilost napadom, kot so spletni črvi, npr. Nimda),

j) *napad (D)DoS* (kadar napadalcu ne uspe vdreti v spletno aplikacijo na katerega izmed opisanih metodoloških pristopov, se aplikacije loti z napadom (D)DoS (ang. distributed denial of service). Posledica takega napada je nedelovanje spletne aplikacije, kar napadalec najpogosteje doseže s poplavo lažnega prometa, pri čemer mu pomagajo omrežja, imenovana *bot net*. Takšna omrežja sestavljajo računalniki, v katere je napadalec vdrl že pred napadom DoS in vanje namestil orodja za daljinski nadzor.

4.6 Motivacija hekerjev za vdiranje v računalniške sisteme

Številni teoretski pogledi že vrsto let poskušajo razkriti morebitne psihološko usmerjene namere in motivacije hekerjev. Pomembno vlogo v iskanju motivov hekerskega vdiranja je vsekakor imela računalniška varnostna industrija. Tako lahko v osnovi motivacijo hekerjev za vdiranje v računalniške sisteme razdelimo v šest skupin:

1. Občutek zasvojenosti in vdajanja.
2. Nagon radovednosti.
3. Zdolgočasenost z izobraževalnim sistemom.
4. Uživanje ob občutku moči.
5. Uživanje ugleda.
6. Politične namere.

[27] Pri tem je pomembno omeniti tudi t.i. XSS napade (ang. cross-site scripting), ki jih večina uporabnikov še vedno danes jemlje kot nenevarne ali pa jih kar ignorira. Prav tako spletna stran Slo-Tech opozarja na nevarnost spletnih razobličenj v obliki XSS napadov. Spretno formulirana XSS razobličenja so namreč lahko zelo prikrita, s tem pa uporabnike prevarajo, ki lahko prirejene informacije sprejmejo kot legitimne (Slo-Tech 2006). S pomočjo XSS napada tako lahko napadalec doda na zaupanja vredno spletno stran lastno zlonamerno kodo (vstavi program v skriptnem jeziku v tekstovno polje), ki se prikazuje ostalim uporabnikom. Koda je najpogosteje v JavaScript obliki, ki se izvede s pomočjo brskalnika obiskovalca spletne strani (Uranjek 2007).

Kljub poskusu strogega kategoriziranja hekerskih motivov in namer vdiranja je danes še vedno preveč nejasnosti ter fluidnosti med skupinami. Veliko lažje bi bilo namere razdeliti v dve skupini, t.j. med skupino zasvojenosti ter skupino radovednosti (Taylor 1999, 44).

Taylor v svojem delu pogosto navaja in interpretira citate drugih avtorjev in s pluralnostjo argumentov pokriva široko področje nejasnosti hekerskega poslanstva. Tako pri prvi skupini, ki jo navdaja občutek *zasvojenosti in vdajanja,* poudari, da je ena izmed najbolj zanimivih podob hekerstva prav lastnost obsedenosti, katera sicer nosi negativen naboj, vendar poleg obsedenosti posebno vlogo pripisuje tudi praktičnemu znanju. Za to skupino je značilna predvsem ekstremna mera obsedenosti, odvisnosti z iskanjem podrobnih informacij; hekerji so pogosto tako obsedeni s svojim delom, da enostavno ne vedo, kaj počnejo.

Druga skupina, ki jo vodi *nagon po radovednosti*, naj bi se bistveno razlikovala v motivih delovanja hekerjev, vendar je pomembno le to, da obsedenost interpretiramo tudi kot radovednost. Hekerji tako menijo, da njihova visoka mera radovednosti prav najbolj pripomore k izboljševanju tehnologije.

V tretjo skupino motivov, za katero je značilno *dolgočasje*, sodijo hekerji, ki svoja dejanja opravičujejo kot pomanjkanje izzivov v okviru izobraževalnih ustanov, v pomanjkanju dostopa do občutljivejših področij dela z računalnikom.

Četrta skupina se ponaša z *občutkom in željo po moči*. Nedvomno je smotrno poudariti, da se motiv in želja po moči dopolnjujeta z nagnjenostjo k radovednosti. Vdiranje v zahtevnejše in večje računalniške sisteme hekerjem daje poseben občutek moči in se tako napadalec sam sebi dokaže kot sposobnejši od sistemskih administratorjev.

V peto skupino sodijo motivi, povezani z *željo po uživanju ugleda* med hekerskimi vrstniki. Čeprav stereotipna podoba hekerja označuje družbeno nezrelega posameznika, ki se izogiba stikov z ljudmi in kot nadomestilo z njimi postavlja v ospredje računalnike, se hekerji vsekakor ne izključujejo iz družbenega vsakdana. Pogosto si medsebojno delijo izkušnje, zgodbe, mnenja in informacije, učijo mlajše generacije hekerstva in se nemalokrat družijo in izmenjujejo mnenja na konferencah. Tako Taylor v svoji knjigi objavi pogovor s hekerjem, ki pravi, da je ugled med sovrstniki izjemno pomemben, saj bolj kot si prepoznaven, več svobode in dostopov imaš.

V šesto in zadnjo skupijo štejemo hekerje s *politično motivacijo*. Hekerji pogosto trdijo, da so temeljna sila znotraj družbe vpoklicani nasprotovanju ponovni vzpostavitvi tradicionalnih

vrednot v novi informacijski družbi. Predvsem želijo dokazati, da so tradicionalne vrednote osnovane na pravici do fizične lastnine, ki so čedalje bolj anahronistične, zastarele (Taylor 1999, 43–65).

Wall (2007, 62–65) odpre povsem novo serijo motivacijskih dejavnikov, saj meni, da hekerji vdirajo v računalniške sisteme zaradi:

- zadovoljstva,
- ugleda med sovrstniki,
- morebitnih delodajalcev,
- kriminalnih namenov,
- maščevanja,
- distanciranja od žrtev napadov in
- političnega protesta.

Medtem ko so tri skupine precej podobne Taylorjevi razlagi, bom pozornost osredotočil na preostale, nove skupine. Wall meni, da hekerji pogosto vdirajo v računalniške sistema zaradi morebitnih delodajalcev, saj je praksa v preteklosti pokazala, da organizacije pogosto zaposlujejo hekerje kot varnostne svetovalce. Prav tako čedalje bolj v ospredje prihajajo hekerji s profitno miselnostjo, ki pogosto sovpada s kaznivimi dejanji. Tako hekerje pogosto vodi sla po denarju, izsiljevanju, sleparstvu ipd.. Zlonamerni hekerji tako izsiljujejo denar, številke bančnih kartic ali zahtevano informacijo.

Motivi hekerjev so pogosto tudi maščevalni, še posebej do konkurentov izven ali znotraj organizacije. Maščevalna taktika napadov zelo variira, saj posamezniki, ki se počutijo prikrajšane s strani določene organizacije, z napadi pogosto skušajo popraviti krivico. Tako so sredstva teh napadov predvsem črvi. Napadi so najpogostejši v času, ko posameznike iz podjetja odpustijo ali ko so primorani odstopiti.

Povsem nov motivacijski dejavnik hekerjev je distanciranost od žrtve. Wall navaja primer, ko heker zaradi občutka oddaljenosti od žrtve in posledično neranljivosti ter anonimnosti dosega svoje cilje. Hekerji napadajo tudi v znak političnih protestov z namenom rušiti obstoječe stanje miru ali poskušati pospešiti favorizirane politične procese. Protest lahko zajame obliko

hekerskega aktivizem ali hektivizma, informacijskega bojevanja ali kiberterorizma. Tarča teh napadov je pogosto kritična informacijska infrastruktura (Wall 2007, 64–65).

4.7 Hekerski aktivizem ali hektivizem

Hektivizem je izraz, ki povezuje tradicionalne metode političnega protesta na eni strani in tehnološki napredek računalništva in hekerstva na drugi. Hektivisti uporabljajo povsem enake metode kot hekerji, zato je težko začrtati jasno ločnico med hekerstvom in hektivizmom. Politične motive hekerjev smo lahko zaznali že na samem začetku hekerske dejavnosti, vendar so ti bili nekoliko v ozadju. Začetke politično aktivnega hekerstva lahko izvlečemo že iz prve generacije in Levyjevega hekerskega manifesta, ko si hekerji predvsem prizadevajo omogočiti državljanom javen dostop do računalnikov in svobodo informiranosti. Za prvo in drugo generacijo hekerjev je torej značilna želja po razširjenosti tehnologije in hekerskega znanja.

Naslednji korak hektivisti naredijo v obdobju vietnamske vojne, potem ko je ameriška vlada povečala obrambne izdatke zaradi vojne tako, da je odvzela določen delež denarja od plačanih telefonskih računov. Posledica tega dejanja je bila objava phone-phreakinga v reviji Technological American Party (TAP) in drugih nasvetov, kako telefonirati zastonj. V osemdesetih letih se je ustanovila nemška hekerska skupina Chaos Computer Club (CCC), katera se je v političnem kontekstu borila predvsem za svobodo informiranja. Omenjena skupina je po jedrski katastrofi v Černobilu razširila informacije o resnosti incidenta in sodelovala z nemško stranko Zelenih v skupnem ocenjevanju vključitve novih računalniških sistemov v zvezni parlament (Wall 2001, 59–72).

Brian Still podrobno razgradi koncept hektivizma in ga opredeli kot hekanje v politične ali družbene namene na medmrežju. Tako se politično motivirani hekerji večkrat individualno ali v skupinah povežejo z nevladnimi organizaciji, drugimi političnimi aktivisti in združenji. Tarče njihovih opozoril ali napadov so vlade, ki so odgovorne za politično, ekonomsko ali družbeno neenakost ali zatiranje (Still 2005).

Strehovec (2003, 311–312) opisuje hektivizem kot uspešno zvezo med hekerstvom in aktivizmom na ravni nove družbene kritičnosti in subverzivnosti, ki sta usmerjeni k elektronski civilni neposlušnosti, k intervencionizmu taktičnih medijev in k drugim oblikam protestov, ki so lahko v kiberprostoru pogosto uspešnejši kot v tradicionalnih oblikah. Hektivisti imajo pozitiven odnos do tehnologije, odraščali so z njenimi novostmi in pridobitvami in pogosto tudi sami

oblikujejo programe, namenjene temu, kako motiti ali onesposobiti svoje on-line nasprotnike. Ko gre za protiglobalizacijska gibanja, nam veliki mediji sicer praviloma dobavljajo podobe spopadov protestnikov z lokalnimi policijami, vendar pa imajo pogosto močnejše učinke od uličnih protestov prav hekersko-aktivistični napadi na spletne strani in komunikacijske sisteme organizatorjev in udeležencev konferenc mednarodnih forumov, se pravi akcije nestrinjanja, ki jih vodijo on-line protestniki, dejavni v različnih skupinah. Za njihove protestne akcije so značilna onesposabljanja strežnikov, blokiranje komunikacijske sposobnosti svojih nasprotnikov, virtualne zasedbe (angl. *sit-ins*).

4.7.1 Virtualne zasede ali blokade

Hekerske zasede in blokade lahko v virtualnem svetu enačimo s fizičnimi zasedami in blokadami. Predvsem je cilj v obeh primerih priklicati pozornost in vzpodbuditi željo protestnikov po motenju in oviranju normalnega poteka operacij in blokirati dostop do njih. Z virtualnimi zasedami lahko tisoče hektivistov istočasno obišče določeno spletno stran, jo s tem okupira in posledično onemogoči dostop drugim uporabnikom. Pri tem pa v ospredje prihaja nerešeno vprašanje legalnosti virtualnih zasedb, namreč napadi lahko kršijo zakonodajo na področju distribucije ilegalne programske opreme ali orodij, ki pomaga hektivistom oškodovati lastnike spletnih strani. Orodja, s katerimi lahko hektivisti ustvarijo virtualno zasedo, je mogoče namestiti prek interneta in pri tem ni nujna hkratna prisotnost vseh na določeni strani, temveč se lahko s pomočjo programske opreme nastavi čas, ko protestnik vstopi v spletno stran (Denning 2001, 264–266).

4.7.2 E-poštne bombe

Hektivisti svoje cilje uresničujejo tudi tako, da preko elektronske pošte zasujejo svoje tarče s t.i. *e-poštnimi* bombami (ang. e-mail bomb). Takšen napad omogoča posebna programska oprema, ki avtomatsko pošilja elektronsko pošto in tako povzroči preobremenitev elektronskega poštnega predala. Tako lahko takšen napad imenujemo tudi virtualna blokada, saj lahko v celoti povzroči zastoj normalnega dela. Takšen napad lahko traja tudi do dveh tednov, s povprečjem okoli 800 elektronskih pošt dnevno[28]. Čeprav se ta način napada pogosteje uporablja v primerih

[28] Primer pošiljanja e-poštnih bomb s strani tamilskih tigrov (Šrilanka) iz leta 1998.

maščevanja ali trpinčenja, ga hektivisti pogosto uporabijo v namen političnega protestiranja. V obdobju konflikta na Kosovu so protestniki na obeh straneh zasuli spletne strani vlad. Po poročanju Natovega predstavnika Jamie-a Shea je spletni strežnik NATA samo od enega hekerja prejel okoli 2000 sporočil vsakodnevno in tako povzročil preobremenitev. Kot povračilen ukrep je prebivalec Kalifornije kot maščevanje za napad na Natov strežnik vrnil napad s 500.000 sporočil v nekaj dneh in tako onesposobil delovanje vladne spletne strani v takratni Jugoslaviji (Denning 2001, 269–270).

4.7.3 Ogrožanje spletnih aplikacij

Mediji pogosto poročajo o vdorih hekerjev v spletne strani, kjer zamenjajo določeno sporočilo strani ali ga sami dodajo. Tako čedalje bolj sporočila hektivistov nakazujejo nestrinjanje s politično držo določene države, kot v primeru skupine portugalskih hekerjev, ki so okoli 40 indonezijskim stranem septembra 1998 dodali slogan »*Svobodni vzhodni Timor*«. Hekerji so poleg tega na spletne strani naložili spletne povezave do strani, ki opisujejo zlorabe človekovih pravic v Indoneziji. Naslednji način hektivizma, preko katerega hekerji spremenijo, kar drugi obiskovalci želijo poizvedeti, ko obiščejo željo spletno stran, je zamenjati obstoječi DNS (ang. Domain Name Service), tako da se domena spletne strani spremeni v IP naslov (ang. *Internet protocol adress*) neke druge strani. Ko uporabnik želi obiskati želeno spletno stran, tako pristane na strani, na katero ga heker preusmeri[29] (Denning 2001, 272–274).

Hekerski vdori tako že vrsto let predstavljajo grožnjo varnosti informacijskih sistemov. Raziskave na tej strani in onstran Atlantika vsako leto prikazujejo večanje števila vdorov v omenjene sisteme. Raziskava *Information Security Breaches 2002* je odkrila, da je 44 % odstotkov podjetij v Veliki Britaniji leta 2001 utrpelo vsaj en zlonameren, neavtoriziran vdor, kar je dvakrat več kot v podobni raziskavi iz leta 2000 (Wall 2007, 53).

Napadi »pharming« (gre za skovanko med angleškima besedama *farming* in *pharmacy*) so verjetno bolj nevarni za uporabnika, saj jih je nekoliko težje prepoznati. Praviloma gre pri omenjenih napadih za neposreden napad na DNS strežnike ali za napad na določeno datoteko, ki se nahaja na računalniku uporabnika (gre za t.i. datoteko o gostiteljih oz. *host file,* kjer se

[29] Vsekakor omembe vredna tehnika je tudi t.i. *pharming* tehnika, ki vključuje spreminjanje naslovov sistema DNS, tako da uporabnik ne obišče originalnih spletnih strani, ampak druge, narejene posebej za zbiranje zaupnih podatkov, predvsem informacije za uporabo e-bank (IP-RS 2008).

nahajajo podatki o URL-jih in domenah). Uporabnik je potemtakem prepričan, da se nahaja na pravi strain, saj je vtipkal pravi URL naslov strani, v bistvu pa ga je eden od omenjenih načinov napada preusmeril na lažne strani. Pogosto se zgodi, da v teh primerih uporabnik nasede lažnem zaupanju in je dovolj prepričan, da vnaša svoje osebne podatke v obrazce, ki se nahajajo na takšnih straneh (IP-RS 2008).

Če računalniške sisteme, ki vsebujejo občutljive informacije, fizično ločimo od ostalega omrežja, torej jih povsem odmaknemo od zunanjega sveta, je praktično nemogoče vdreti. Omrežje, ki služi samo za potrebe zaposlenih znotraj določene organizacije, imenujemo *intranet*. Tveganje se sunkovito poveča, če računalniškim sistemom dovolimo, da operirajo tudi izven omrežja. Eden izmed načinov, ki lahko prepreči vdore v računalniške sisteme, je striktno analiziranje in nadzorovanje vseh datotek, ki prihajajo v sistem[30]. Pri tem načinu je problem nadzora vseh datotek, saj je proces nadzorovanja precej zamuden. V postopku varnostni pregled prenesenih datotek se ugotovi, ali obstaja možnost za tveganje oz. ali lahko prenesene datoteke posredno ali neposredno oškodujejo računalniški sistem (Libicki 1995, 53–54).

Organizacije, ki skrbno varujejo zaupne in občutljive podatke, so čedalje bolj tarča napadov. Winkler je mnenja, da šele z razumevanjem podrobnosti tveganj lahko začnemo z učinkovito in primerno strategijo zaščite organizacije in s tem tudi lažje upravljamo z morebitnimi tveganji. Z zaznavanjem ranljivosti določenega sistema je potrebno poiskati optimalno rešitev. Cilj varnostne programske opreme torej ni izničiti tveganja, temveč jih optimizirati (Winkler 2005, 35).

4.8 Hekersko vojskovanje

Nekatere skrajne oblike hektivističnega političnega protestiranja lahko vodijo celo v spopad med hekerji, ki ga označimo kot hekersko vojskovanje (ang. *hacker warfare*). Koncept hekerskega vojskovanja je prvi predstavil in definiral Libicki v knjigi *What is information warfare?* iz leta 1995, potem ko ga je uvrstil med sedem oblik informacijskega bojevanja. Številni avtorji, med njimi je tudi Winn Schwartau, povezujejo informacijsko bojevanje izključno z napadi prek računalniških omrežij. V nasprotju s fizično obliko spopada, so ti napadi svojstveni do specifičnih lastnosti tarčnih sistemov, ker izkoriščajo luknje v varnostni strukturi sistema. V tem kontekstu napadeni sistem nosi odgovornost za lastno propadanje (Libicki 1995, 49).

[30] Sistemski administratorji danes raje uporabljajo možnost nadzorovanja izhodnih povezav.

Hekersko vojskovanje se lahko razvija v številnih oblikah. Napadi lahko segajo od uničenja datotek in podatkovnih baz, kraje informacij, idej ali posla, nezakonitega nadzorovanja ali prisluškovanja (zbiranja obveščevalnih podatkov), vstavljanja napačnih, zavajajočih informacij, dostopa do podatkov z namero nadaljnjega izsiljevanja, pa tudi do paraliziranja celotnega računalniškega omrežja. Svoje cilje pogosto uresničujejo z računalniškimi virusi, logičnimi bombami, trojanskimi konji ali programsko opremo prestrezanja. Čeprav se hekersko vojskovanje v osnovi ne razlikuje, ko gre za civilni hekerski boj ali vojaški, so ponavadi vojaški računalniški sistemi veliko bolj zaščiteni kot civilni, saj niso namenjeni javnosti. Kritični informacijski sistemi so povečini povsem izključeni iz javnih omrežij, torej so fizično ločeni od ostalih omrežij. Računalniški napadi so lahko *fizične*, *sintaktične* in *semantične*[31] narave, vendar se večino pozornosti usmerja na sintaktične napade. Razlog za skrb pred fizičnimi napadi je danes zanemarljiva, čeprav lahko npr. večje računalnike, ki poganjajo ostale računalniške sisteme, napadalci uničijo, če izključijo hlajenje prek ostalih računalnikov[32]. Semantični napadi so usmerjeni proti pomenu sporočila, ki ga računalniki prejmejo od drugod.

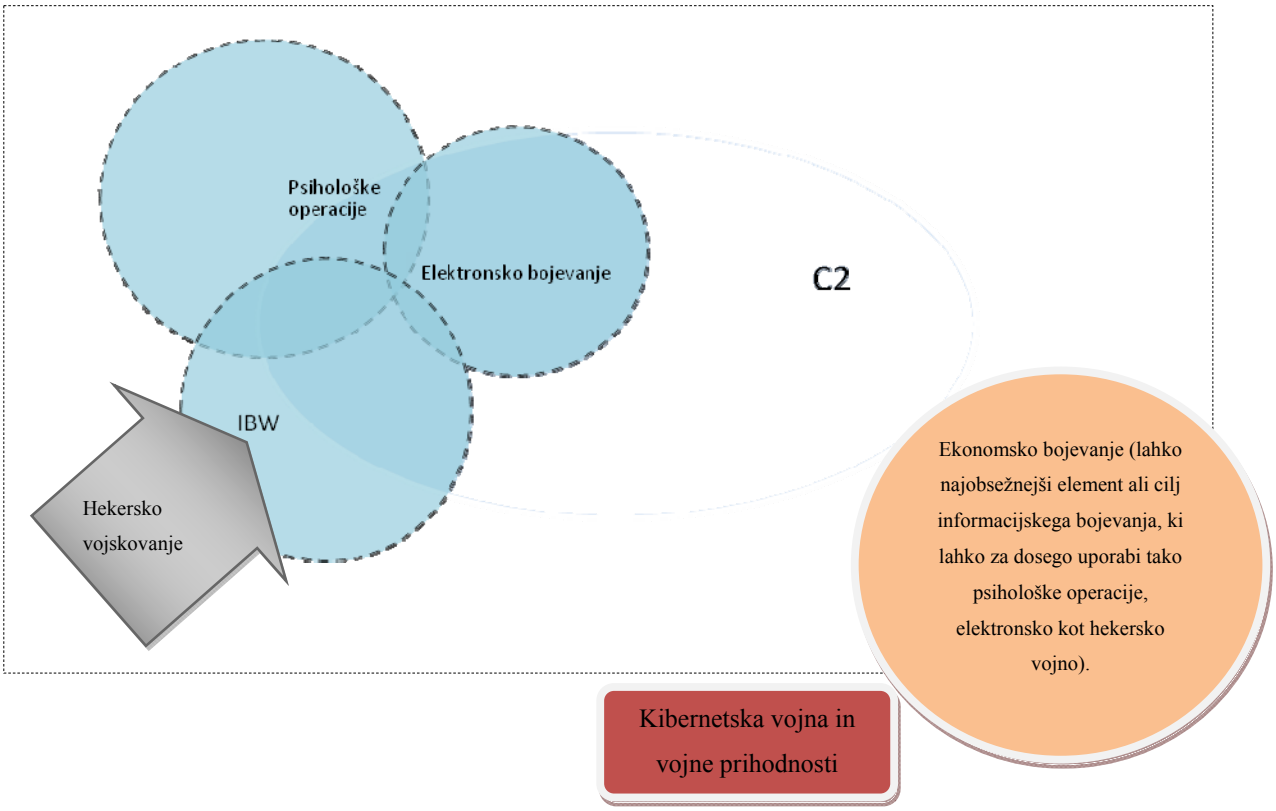
Tako lahko hekersko vojskovanje, kot vsako drugo obliko vojskovanja, delimo na obrambno in napadalno. Bistvo obrambnih operacij je zavarovanje lastnih računalniških sistemov in zaščita pred morebitnimi napadi, medtem ko je naloga napadalnih operacij v hekerski vojni določiti področje napadov. Čedalje bolj prihajajo v ospredje vprašanja o smotrnosti uporabe instrumentov hekerskega vojskovanja na ravni politike, če omenjeno vojskovanje lahko resnično definiramo kot vojno in ali je v prihodnosti resnično možna. Tako so ti incidenti, ki jih dnevno beležimo, v porastu in rastejo še hitreje, kot raste svetovno število uporabnikov interneta. Zdi se torej pretirano in nenavadno, če bi bili mnenja, da hekerski napadi ne ogrožajo in ne morejo ogroziti nacionalne varnosti, torej bi jih izključili (Libicki 1995, 49–53).

Spodnja shema prikazuje štiri ustaljene oblike informacijske bojevanja: a. bojevanje na področju poveljevanja in nadziranja – C2, b. elektronsko bojevanje, c. psihološke operacije in d. bojevanje na področju obveščevalne dejavnosti. Koncept hekerskega bojevanja je ena izmed

[31] *Fizični* napadi so usmerjeni predvsem v fizično uničenje računalniških sistemov, pri *sintaktičnih* napadih se nasprotnikove sisteme onesposablja s programskimi sredstvi, kot so npr. virusi, trojanski konji ter druga podobna orodja, ali pa se poskuša z vdori od zunaj ali od znotraj onemogočiti delovanje informacijskih sistemov, glavni namen *semantičnih* napadov pa je vplivanje na zaznave nasprotnika ali na oblikovanje njegovih mnenj in stališč.
[32] Na tej točki je potrebno poudariti, da so tovrstni napadi danes samo teoretično možni.

novih oblik informacijskega bojevanja in bo tako sčasoma postala peta ustaljena oblika (Hawkins 1997).

Shema 4.2: Shematski prikaz oblik informacijskega bojevanja.



Vir: A hero report (Hawkins 1997).

Danes se pojavljajo skupine računalniških hekerjev, ki so čedalje bolj vpletene v regionalne, verske in etnične konflikte, kar je razvidno še posebej iz kašmirskega primera, kjer si na obeh sprtih straneh prizadevajo motiti informacijske sisteme in širiti lastno propagando. V nemirnem Kašmirju se je po decembru 2001 napetost še zaostrila, k temu so pripomogle hekerske skupine, ki zagovarjajo interese islama in Pakistana. Izjemno politično naravnani napadi so usmerjeni proti Indiji, saj jim hekerji povzročajo precej težav s črvi, popačenji spletnih strani in z DDOS napadi. Število poskusov vdiranja narašča, še posebej pa si hekerji prizadevajo pridobiti občutljive in tajne podatke iz številnih centrov za atomske in jedrske raziskave. Takšna oblika hekerskega asimetričnega bojevanja danes več ne predstavlja prvovrstnih fenomenov, saj je na številnih spletnih straneh možno pridobiti hekerska orodja za vdiranje. Vprašanje, ki se ob

tem postavlja je, ali lahko ti napadi predstavljajo resno grožnjo ali samo motenje.

Da lahko napadi eskalirajo celo v resno grožnjo ali povzročijo poglobitev krize, lahko razberemo iz naslednjega primera palestinsko-izraelskega konflikta, v katerega so se vključili tudi hekerji. Izraelski hekerji so s pomočjo DDOS napadov blokirali spletne strani Hezbolaha in Hamasa v Libanonu, tarča so med drugimi bile tudi spletne strani Združenih držav Amerike in palestinskih oblasti. Navidezno nepomemben napad na spletne strani je povzročil pravo kibernetsko vojno, ki je hitro prerasla v mednarodni incident. Palestinci in ostale podporne islamske organizacije so hitro pozvale h kibernetski sveti vojni (poimenovali so jo tudi kiber-džihad ali e-džihad). Kmalu po pozivu so palestinski hekerji udarili po spletnih straneh izraelskega parlamenta, ministrstva za zunanje zadeve, izraelskih obrambnih sil, izraelske banke in borzne hiše v Tel Aviv-u. Čeprav omenjeni primer resnejših in dolgoročnih posledic za palestinsko-izraelski konflikt ni imel, primer jasno kaže na specifike tovrstnih obračunov ter v končni fazi predstavlja model, kako lahko v prihodnje takšni incidenti izgledajo. Palestinsko-izraelski hekerski spopad se je sicer začel leta 1999 in je najvišjo stopnjo dosegel jesni leta 2000. Do konca januarja 2001 so hekerji povzročili škodo več kot 160 izraelskim spletnim stranem in okoli 35 palestinskim, vključno z ameriško spletno stranjo. V obdobju med julijem 1999 in sredino aprila 2002 je bilo razobličenih 548 izraelskih domen (.il) skupno od 1.295 razobličenih strani na Bližnjem Vzhodu, poleg tega so številne spletne strani tarča DDOS napadov. Ekstremistične islamske skupine, tesno povezane z Hezbolahom, so konec leta 2001 objavile nov val napadov. Napade so razporedili v štiri faze, med katerimi je bila prva faza usmerjena v povzročitev sesutja vladnih spletnih strani Izraela, tarča drugih napadov sta bili izraelska banka (Bank of Israel) in borzna hiša v Tel Avivu. Tretja faza naj bi bila usmerjena proti dobaviteljem internetnih storitev, zadnja faza pa naj bi povsem uničila spletne trgovine in s tem ogrozila milijone dolarje vredne transakcije (Allen in Demchak 2003).

Informacijsko bojevanje naj bi v osnovi bilo namenjeno zgolj motenju nasprotnika v vojnem obdobju kot del vojne strategije. V primeru kašmirske hekerske vojne indijske strani trdijo, da je pakistanska obveščevalna služba ISI (ang. *Inter-Services Intelligence*) rekrutirala v svoje vrste hekerje. Tako naj bi indijske oblasti prepoznale metode in tehnike vdiranja nekega hekerja, ki ga je ISI že odkrila v preteklosti (Anhal 2001, 52–53).

Estonija je v prejšnjem stoletju bila precej na udaru Sovjetov in kasneje Rusov. Posledice druge svetovne vojne, sovjetske okupacije, hladna vojna in proces transformiranja države so v

Estoncih pustile posebno stanje nasprotovanja ruskim državljanom. V obdobju, ko je Estonija bila povsem pod taktirko Moskve, so v Talinu postavili bronasti spomenik neznanemu sovjetskemu vojaku kot spomin na obdobje druge svetovne vojne. In prav ta spomenik, ki je Estoncem predstavljal zgolj afirmacijo sovjetske prevlade na domačih tleh, je bil predmet spora med rusko manjšino v Estoniji in Estonci, saj so slednji po osamosvojitvi sklenili, da ga umaknejo na vojaško pokopališče na obrobje prestolnice. Politična in etnična nesoglasja med njimi so odprla tudi možnost spopada v kibernetskem svetu. Rusi naj bi izvedli kibernetski napad na Estonijo in s tem ogrozili nacionalno varnost Estonije – tako je iz navidez nepomembnega hekerskega napada nastala verjetnost rušenja regionalne stabilnosti. 26. aprila lani so nesoglasja povzročila virtualne napade na estonsko omrežno infrastrukturo, pri tem pa so tarče napadov bile vladne službe, medijske agencije, bančne institucije itd. Napad je bil torej izrazito politično usmerjen, tako izrazite posledice pa je pustil predvsem zaradi tega, ker so Estonci vajeni uporabe bančnih storitev preko interneta[33]. Nekaj dni pred samim napadom so ruske forume preplavile debate o napadu na informacijsko infrastrukturo, nekateri so navajali celo tarče napadov. Kibernetski napad oz. protest proti estonskim oblastem se je odvil konec aprila 2007 z natančnim programom izvedbe napadov. Napad je povzročil še večje neodobravanje Estoncev, ki so tako preplavili ulice Talina. V naslednjih dneh so Estonci utrpeli posledice hekerskega napada na bančne strežnike, spletne strani, izobraževalne ustanove, medije, medtem ko je omrežje estonske vlade preplavila zlonamerna programska oprema. Estonske oblasti niso uspele poiskati napadalca, še vedno ostaja nepojasnjeno, ali so morda za napadi stale ruske oblasti, skoraj povsem očitno pa je, da so napad izvršili ruski državljani. V primeru hekerskega napada na estonsko informacijsko infrastrukturo naj bi šlo za izjemno dobro organizirano dejanje, saj so se napadi pričeli sočasno, ruski forumi pa so sprotno objavljali nove tarče (Evron 2008, 121–126).

Primera kašmirske hekerske vojne in hekerskega napada na estonsko informacijsko infrastrukturo sta nakazala morebitne posledice teh dejanj, ki niso omejene le na področje medmrežja. Globalna trenda, kot sta industrializacija in urbanizacija, sta povzročila razpršenost tehnologije, pri tem pa ustvarila svet odvisen in ranljiv. Čeprav estonski primer ni povzročil škode kritični informacijski infrastrukturi, je nakazal nekaj varnostnih lukenj, ki jih napadalec lahko izkoristi v primeru ogrožanja varnosti posameznika, gospodarstva in države. Uspešen

[33] Estonija izrablja možnosti uporabe internetnih storitev, njihova družba postaja čedalje bolj e-družba. Na zadnjih volitvah v Estonski parlament je preko 30.000 državljanov oddalo glasove prek interneta.

napad, ki bi bil usmerjen v energetsko dejavnost države, bi lahko povzročil motenje energetske dobave ali jo celo onesposobil. Če bi do tega prišlo, lahko celotno področje napada ostane brez elektrike, kar lahko vodi v neposredno motenje letalskega, avtomobilskega, železniškega prometa, pri tem pa je dejansko nemogoče oceniti posredno škodo takšnega napada (Evron 2008, 124–126).

Verjetno najbolj aktualen primer prihaja prav iz avgustovskega konflikta med Rusijo in Gruzijo, med katerima naj bi pred dejanskim spopadom potekala celo kibernetska vojna. Dobro koordinirani DDOS napadi, naj bi se začeli že okoli 20. julija povzročili preobremenitev in nedelovanje gruzijskih strežnikov, pri tem pa naj bi bil tarča napadov tudi strežnik predsednika Gruzije Mihaila Šakašvilija. Čeprav se zaenkrat še ne ve, kdo naj bi bil za napadi, gruzijske oblasti obtožujejo Ruse, vendar ruska vlada vpletenost zanika. Tarča napadov po vojaškem spopadu so bile tudi komunikacije gruzijskih medijev in transportnih podjetij. Po ameriški analizi in na podlagi jasnih dokazov, naj bi za napadi stala ruska hekersko-kriminalna skupina, imenovana *Russian Bussiness Network*. Bill Woodcock, raziskovalni direktor v *Packet Clearing House*, je prepričan, da bodo tovrstni napadi stalnica v prihodnjih konfliktih, saj so stroški minimalni – cena tovrstnega napada znaša okoli 4 ameriške cente/računalniški sistem, pri tem pa omeni, da bi sprožitev kibernetskega napada znašala približno toliko kot menjava tankovskih gosenic (Markoff 2008).

Konflikti v kibernetskem prostoru danes tako predstavljajo prostor političnega in propagandnega boja. Svete (2005, 258–259) ugotavlja, da /p/rva ugotovitev glede uporabe IKT v sodobnih konfliktih tako pojasnuje njeno vplivanje na sam izid konfliktov, kjer ima lahko dvojen učinek: lahko je sredstvo, ki prinaša informacijsko razvitemu akterju dodatno prednost, na drugi strani pa je ravno to njegovo odvisnost mogoče zlorabiti z uporabo sredstev asimetričnega vojskovanja. Tehnološka razvitost tudi v obdobju globalizacije ter informacijskih družb sama ne zagotavlja odločilne prednosti, ki še vedno temelji predvsem na razvoju uporabe organiziranega nasilja ob človeškem dejavniku. Avtor v svojem delu navaja ugotovitev Cronina in Crawforda, da je lahko uporaba IKT med različnimi akterji sodobnih konfliktov lahko trojna:

- *fizična* (nanaša se na fizično uničenje nasprotnikovih informacijskih in komunikacijskih sredstev /.../),

- *»mehka«* (druga raven je programska (sintaktična), pri čemer se nasprotnikove sisteme onesposablja s programskimi sredstvi, kot so npr. virusi, trojanski konji ter druga podobna orodja, ali pa se poskuša z vdori od zunaj ali od znotraj onemogočiti delovanje informacijskih sistemov),

- *psihična* (lahko jo imenujemo tudi omrežno bojevanje oz. semantična raven). Če je bil glavni cilj prvih dveh onemogočanje delovanja sistemov, pa psihična poudarja tihe vdore, katerih glavni namen je vplivanje na zaznave nasprotnika, oblikovanje njegovih mnenj in stališč, zagotavljanje in utrjevanje prevar ter delovanje v »epistemološkem« bojevanju.

Podobno vlogo, kot jo ima IKT v sodobnih konfliktih, ima tudi hekanje. Libicki je eden izmed prvih avtorjev, ki je določil napade na računalniške sisteme v kontekstu informacijskega bojevanja in jih uvrstil med *fizične*, *sintaktične* in *semantične* (Thompson 2008).

Splošno velja, da je skoraj praktično nemogoče *fizično* uničiti računalniške sisteme prek hekerskih napadov, čeprav lahko računalniške sisteme, ki poganjajo ostale manjše računalniške sisteme, napadalci uničijo, če izklopijo hlajenje, vendar je skrb pred tovrstnimi napadi danes zanemarljiva[34]. Podobno kot Libicki, Svete (2005, 120) kot naslednjo raven v izvajanju kibernetskega bojevanja omenja tudi *sintaktične* napade, ki so izrazito hekerska usmeritev, saj se s kodo premaguje drugo kodo. Za razliko od prejšnjih dveh oblik napadov, kjer je potrebno določeno elitno znanje, razvito v času informacijske dobe, so *semantični* bistveno starejši in bi jih danes lahkko poimenovali *informacijski* oz. *dezinformacijski napadi*.

Cybenko med drugimi definira kognitivno hekanje (ang. *Cognitive hacking*) kot napad na računalniški sistem, usmerjen v mišljenje uporabnika, pri katerem je za dosego ciljev napada heker primoran vplivati na uporabnikovo mišljenje in vedenje. Kognitivni napadi spadajo pod semantične napade, delimo jih na prikrite ali tajne in odkrite ali javne. Prikriti kognitivni hekerski napadi so napadi, ki za svoj cilj uporabljajo elemente manipuliranja, zavajujočih netočnih ali neresničnih informacij. Odprti ali javni kognitivni hekerski napadi pa so uporabniku

[34] Dober primer, kako je mogoče fizično uničiti računalniški sistem, je virus imenovan Chernobyl (kraj. CIH). Virus okuži .exe datoteke in se hitro širi preko omenjenih datotek. Virus poleg datotek napada tudi BIOS in določene čipe v okuženih računalnikih. Virus po okužbi začne uničevati trdi disk in preuredi nastavitve v BIOS-u. CIH lahko okuži računalniške sisteme tistih uporabnikov, ki uporabljajo operacijska sistema Okna 95 ali 98 (ang. Windows 95/98) (CERT.org 1999). Z namenom motenja dobave s plinom, so Američani leta 1982 potaknili računalniški virus, ki je spremenil delovanje plinskih turbin in prekomerno povečal pritisk v plinovodih. Rezultat tega je bila največja nejedrska eksplozija v zgodovini človeštva videna celo z vesolja (Hoffman 2004).

vidni in npr. vsebujejo elemente razobličenja. Na tej točki je pomembno poudariti, da imajo prikriti napadi manj predvidljive posledice in so zato veliko bolj učinkoviti kot javni napadi (Cybenko 2002).

Kot primer kognitivnih hekerskih napadov v sodobnem konfliktu lahko ponudimo primer *operacije Iraška svoboda*, kjer so bile uporabljene metode spreminjanja vsebin spletnih strani ter poskusi pretiranega obremenjevanja nasprotnih strežnikov. Tako so hekerji v februarju 2003 spremenili povezave na spletni strani iraškega časopisa Iraq Daily, ki je vodila do iraškega televizijskega programa, na svojo stran, kjer so iraškemu ljudstvu sporočali svojo resnico o dogajanju v Iraku (Svete 2005, 228).

V sodobnih konfliktih lahko tako kibernetski prostor obravnavamo kot nadgradnjo konfliktov ali kot »soprizorišče« konflikta. Sicer delovanje hekerjev v navideznem svetu morda ni odločilno za potek vojaških operacij, vendar lahko hekerji z agresivnimi akcijami povzročijo škodo nasprotujoči strani in pri tem pomagajo obrniti tehtnico v prid izvajalcev informacijskih akcij že pred samim konfliktom.

5 OBVEŠČEVALNA DEJAVNOST V INFORMACIJSKI DOBI

Informacijska revolucija, ki je sedaj v polnem teku, je poskrbela, da je dobilo razmerje med informacijo in močjo popolnoma novo dimenzijo. Novo je dejstvo, da je informacija postala cilj in sredstvo vojskovanja in je enako pomembna kot informacija v vojskovanju samem. Informacija torej ni več zgolj sredstvo, ki povečuje učinkovitost ubojnih tehnologij, kot je bilo znano v preteklosti, ampak odpira nove možnosti za neubojne napade, ki lahko onesposobijo, porazijo, odvrnejo ali prisilijo nasprotnika (Bishop in Goldman v Črnčec 2005, 28). Čedalje bolj je potreba po pridobitvi informacije v kratkem času, ki omogoča ustrezno, pravočasno reakcijo, postala imperativ sodobnega »vojskovanja« oziroma delovanja na vseh področjih v zasebnem in v javnem življenju posameznika, v javnem in zasebnem sektorju države, skupin držav ali naddržavnih subjektov (Črnčec 2005, 28).

Uporaba sodobnih tehnologij, s katerimi razpolagajo razvite države, je v spopadu s staro-novo grožnjo terorizma imperativ. Asimetrično vojskovanje poteka na različne načine in po vseh celinah. Razvoj informacijske tehnologije postavlja tiste, ki s to tehnologije razpolagajo, v veliko prednost pred ostalimi, ki te tehnologije nimajo, ter so, če želijo biti konkurenčni, prisiljeni v

nabavo in razvoj te tehnologije (Brezovšek in Črnčec 2007, 199).

Dogodki, povezani z 11. septembrom 2001, so dodobra zmajali stebre obveščevalno-varnostnim službam, jih tako postavili pred nove izzive, predvsem pa so v ospredje postavili ključna vprašanja v zvezi z metodami pridobivanja podatkov v obveščevalne dejavnosti. Tako se danes obveščevalna sfera giba v okolju, kjer so tradicionalne oblike ogrožanja nacionalne varnosti povsem na dnu seznama groženj, saj prevladujejo asimetrične oblike, kot sta terorizem, kriminal, ipd. Nove izzive morajo obveščevalno-varnostne službe tako iskati predvsem v povezavi z odkrivanjem teh groženj, kjer pa se tradicionalne metode lahko izkažejo za povsem neuporabne.

Svete meni (2005, 192), da se bo tretje tisočletje od drugega bistveno ločilo, saj bo večina sodobnih družb prešla v informacijske. Globalno prevlado si bodo zagotovile tiste države, ki bodo posedovale moč na temelju delovanja obveščevalnih in informacijskih služb. Tako danes v ZDA, Nemčiji, Kitajski, pa tudi Švici in Švedski vse večjo pozornost posvečajo informacijam, ki so se medtem razvile v odločilni dejavnik modernega sveta. Med vsemi deli nacionalnovarnostnih sistemov sodobnih držav je obveščevalno-varnostni podsistem gotovo med prvimi zaznal pomen uporabe IKT za pridobivanje podatkov oz. način obveščevalne dejavnosti, v zadnjem času pa uporabo IKT obravnavajo predvsem kot sredstvo za zagotavljanje koordinirane dejavnosti znotraj obveščevalne skupnosti. Predvsem zahodne države so se na podlagi izkušenj, pridobljenih v terorističnih napadih na ZDA, Španijo in Veliko Britanijo, začele zavedati, da disperzirana obveščevalna dejavnost ne bo kos sodobnim varnostnim izzivom, povezanim s terorizmom. Kako pomembna je uporaba IKT v tej dejavnosti, pa priča tudi obstoj posebnih obveščevalnih služb, katerih področje delovanja je skorajda izključno vezano na IKT in internet oz. sodobne komunikacijske tehnologije.

Bistvo razprave, ki poteka že nekaj desetletij, je predvsem narava vojskovanja v prihodnje in s tem vzporedno sovpada tudi koncept revolucije v vojaških zadevah, bolje poznana kot RMA (ang. *Revolutions in Military Affairs*). Številni teoretiki predvsem v okviru te debate zagovarjajo zmogljivost /…/ tehnologije, še posebej sposobnost natančnega vodenja in hitrega prenosa podatkov, ki bo v končni fazi odigrala ključno vlogo na bojišču. Na drugi strani nasprotniki revolucije v vojaških zadevah nasprotujejo temu konceptu, saj menijo, da je RMA prej evolucionarna kot revolucionarna, ter opozarjajo, da nova tehnologija ne bo prinesla novega koncepta vojskovanja. Vsekakor pa se obe strani povsem strinjata, da bo obveščevalna dejavnost

z ustreznimi odgovori na izzive, s pravočasnim ukrepanjem in izrazito natančnostjo veliko pripomogla pri odvračanju nasprotnikov (Dupont 2003, 15).

Vedeti, kaj v zadostnem času in to uspešno uporabiti, je zlata definicija »*real time*« (obveščevalne) informacije (Keegan 2004 v Obramba 2005, 28). Svetovni splet, internet, omogoča velikemu številu ljudi po svetu hiter dostop do ogromne količin informacij, medtem ko je v preteklosti, pred komaj nekaj desetletji, bila informacija privilegij ozkega kroga ljudi, ki so svojo moč največkrat črpali prav iz tega vira. Ne glede na to, ali pa ravno zaradi tega ostajajo klasične obveščevalno-varnostne službe pomemben vir zagotavljanja informacij, ki niso na voljo širši javnosti. Pojav sodobne tehnologije in med drugim interneta je veliko pripomogel, da se je najstarejši način pridobivanja podatkov v sodobni, bogati, postmoderni državi zanemaril in umaknil pred bolj tehnološko in tehnično podprtimi načini (Črnčec 2005, 28–29).

Presenetljivo malo pozornosti se posveča spremembam, ki jih prinaša nova tehnologija, upravljanju in integraciji obveščevalnih sistemov. Jasno opredeljena ločnica, ki je potekala med strateškimi in operativnimi nalogami obveščevalno-varnostnih služb, med operacijami in obveščevalno dejavnostjo, bo postala nejasna, naloge povsem zamegljene. Definicij, kaj obveščevalna dejavnost je, danes mrgoli, vendar te podobo delovanja obveščevalno-varnostnih služb vse prej kot pa pojasnijo. Tako bi bilo smotrno začeti pri vprašanju, kaj obveščevalna dejavnosti *ni.* Obveščevalna dejavnost ni le informacija ali podatek. Obveščevalna dejavnost je oboje hkrati, obravnavano kot proces, ovrednoteno z jasnim namenom, torej dopolniti ali razjasniti delo politikom in podpreti vojaške operacije (Dupont 2003, 15–16).

5.1 Metode pridobivanja obveščevalnih podatkov

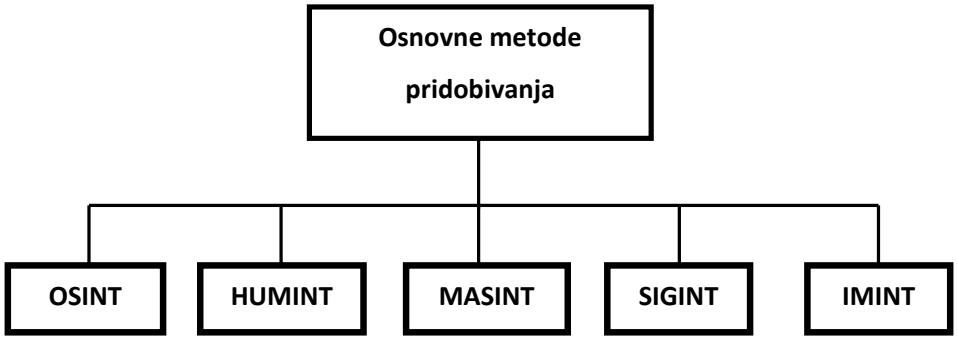
V literaturi so različne klasifikacije načinov in metod za zbiranje podatkov, ki jih uporabljajo obveščevalno-varnostne službe. V svetu je najpogostejša ameriška klasifikacija na obveščevalne discipline (Šaponja 1999, 80–81).

Clark v Intelligence Analysis predstavlja klasifikacijo načinov in metod zbiranja obveščevalnih podatkov na primeru obveščevalne skupnosti ZDA. Omenjena obveščevalna skupnost je uvedla končnico INT, ki je krajšava za *intelligence* zgolj zaradi preprostosti uporabe. Tako metode zbiranja delimo na:

1. zbiranja podatkov prek brskanja po javno dostopnih podatkih (ang. *Open Source*, kraj. *OSINT – Open Source intelligence*);

2. zbiranja podatkov z uporabo človeških virov (ang. *Human intelligence*, kraj. *HUMINT*);
3. zbiranja podatkov z uporabo tehničnih metod pridobivanja, in sicer so to kvantitativne in kvalitativne analize podatkov (merskih, prostorskih, valovne dolžine, časovnih, ipd), ki jih pridobimo s pomočjo posebnih naprav (ang. *Measurements and Signatures intelligence*, kraj. *MASINT*);
4. zbiranja podatkov z uporabo tehničnih sredstev, zbira podatke v obliki prestrezanja različnih signalov ali elektromagnetskih valovanj (ang. *Signals intelligence*, kraj. *SIGINT*);
5. zbiranja podatkov z uporabo slikovnega materiala (ang. *Imagery intelligence*, kraj. *IMINT*) (Clark 2007, 84-85).

Shema 5.1: Prikaz metod pridobivanja obveščevalnih podatkov obveščevalne skupnosti ZDA.



Vir: Clark (2007, 85).

Informacijska revolucija je v obveščevalno sfero ponesla tudi možnost uporabe metod za pridobivanje obveščevalnih podatkov, ki v preteklosti niso prišle v poštev. Pridobivanje obveščevalnih podatkov je čedalje bolj usmerjeno k tehničnim metodam in sistemom, ki jih nameščajo na različne oborožitveni sisteme ladij, letal, podmornic ipd. Obveščevalno-varnostne službe ZDA in koalicijskih sil so si tako v Afganistanu z namenom uloviti Osamo bin Ladna pomagale s številnimi novimi tehnologijami, kot so sateliti, brezpilotna vohunska letala ipd. Čedalje več je govora o nadomestljivosti metode HUMINT s tehničnimi metodami, kar pa se je v primeru terorističnih napadov na ZDA 11. septembra izkazalo za povsem napačno mišljenje. Teroristični napadi na ZDA so bili jasno opozorilo strokovnjakom s področja obveščevalne

dejavnosti, da HUMINT metode ni mogoče nadomestiti s tehničnimi metodami, temveč ravno nasprotno, pridobljeni podatki, ki jih vohuni pridobijo s pomočjo medsebojne interakcije, so še vedno najbolj kvalitetni, a jih pridobijo še vedno zelo malo. Tako bo v prihodnje tajnost dela obveščevalnih služb usmerjena predvsem v podporo vojaškim operacijam in ne več k oblikovanju posebnih poročil politične in gospodarske narave. Obveščevalno delo in pridobivanje podatkov bo v 21. stoletju torej zaznamovano s pridihom nove tehnologije, pri čemer pa se ne sme pozabiti na pridobivanje podatkov prek človeških virov.

Znotraj obveščevalno-varnostnih služb bodo načrtovalci prisiljeni razširiti področje pridobivanja podatkov zaradi novih virov ogrožanja nacionalne varnosti, kot so terorizem, transnacionalen organizirani kriminal, ilegalne migracije ipd. Majhne države in teroristične skupine iščejo prednosti v asimetriji, ko se soočajo, bojujejo ali želijo motiti tehnično dovršene sisteme obveščevalno-varnostnih služb. Omenjene netradicionalne oblike ogrožanja varnosti so se povsem ustalile in postale povsem nekaj običajnega na mednarodnem prizorišču, poleg tega so obveščevalno-varnostne službe prisilile v širjenje področja svojega delovanja, nekateri celo govorijo o rekonstruiranju. Bolj kot se države opremijo in naslanjajo na pridobivanje obveščevalnih podatkov s pomočjo sodobne tehnologije, bolj se sovražnik nauči branjenja in v končni fazi tudi soočenja s slabostmi tehnike (Dupont 2003, 25–26).

5.1.1 Obveščevalna dejavnost in informacijsko bojevanje

Obveščevalno-varnostne službe čedalje bolj postajajo aktivni igralec v kontekstu informacijskega bojevanja, predvsem zaradi neposredne vpletenosti v načrtovanje in izvrševanje strategije informacijskega bojevanja. Sektorji znotraj obveščevalno-varnostnih služb, odgovorni za pridobivanje obveščevalnih podatkov, morajo tesno sodelovati z načrtovalci potreb z namenom razviti ali dopolniti doktrino informacijskega bojevanja in sovpadajočih informacijskih operacij. Ostali sektorji pa bodo imeli nalogo poročati o šibkih točkah znotraj obveščevalnih služb in odkrivati morebitne sovražnike ter hkrati identificirati tarče informacijskega bojevanja (Dupont 2003, 32–33).

Po mnenju Davies-a (1999, 115) predstavlja informacijsko bojevanje zgolj en vidik revolucije v vojaških zadevah. Omenjeni avtor meni, da ni nikakršnega dvoma o tem, da je informacijska tehnologija, vključno od računalniških sistemov do satelitov, izoblikovala prizorišče novih groženj in možnosti, na katere je potrebno biti dobro pripravljen in v tem

kontekstu obveščevalno-varnostne službe smatramo za *conditio sine qua non* obdobja informacijske eksplozije.

V literaturi lahko opazimo dva nasprotna pogleda o obveščevalni dejavnosti, ko govorimo o metodah pridobivanja obveščevalnih podatkov; prvi zagovarja zmožnost uporabe visoko dovršene tehnologije, mednje uvrščamo kibernetske vdore in motenje (s tem pa se sama od sebe ponujata besedni zvezi »*digitalno vohunjenje*« ali »*digitalna sabotaža*«), medtem ko se drugi pogled ukvarja s prenovo metode pridobivanja podatkov prek človeških virov. Od konca hladne vojne je primaren vir zbiranja obveščevalnih podatkov potekal prek tehničnih metod, imenovanih TECHINT (ang. *technical intelligence*), v katere spadata SIGINT in IMINT. Številni navdušenci nad informacijskim bojevanjem pa odpirajo možnost uporabe kibernetskih vdorov kot metodo pridobivanja obveščevalnih podatkov imenovano HACKINT (ang. *hacking intelligence*) (Davies 1999, 117).

5.1.2 HACKINT (ang. hack intelligence)

Napad na informacijske podatkovne baze prek omrežja je vsekakor nov, povsem drugačen in edinstven fenomen v leksikonu obveščevalne dejavnosti. Pridobivanje podatkov z novo metodo tajnega pridobivanja podatkov je velik potencial za obveščevalne službe, saj ta metoda ponuja visoko mero produktivnosti dela z malo stroški v primerjavi z izobraževanjem in organiziranjem operacij tajnih agentov, s prestrezanjem signalov in satelitskimi slikami. Vsekakor pa je strani potrebna tudi previdnost glede pretiravanja uporabe te metode, saj poročila kažejo, da skrbno varovanih podatkov obveščevalne službe ne pridobivajo preko te metode, vendar so hkrati opozorili na povečanje tovrstnih napadov.

Kljub temu se v zadnjem času pogosto dogaja, da se prav hekerji z vdiranjem v računalniške sisteme poskušajo dokopati do zaupnih podatkov, na kar opozarja tudi direktor britanske obveščevalne službe MI5 (ang. Military Intelligence, Section 5). Direktor MI5 Jonathan Evans, v zaupnem dokumentu namreč opozarja okoli 300 britanskih podjetij, da so tarče kitajskih obveščevalnih kibernetskih napadov. Direktor namreč opozarja, da so napadi usmerjeni iz vrst kitajskih državnih organizacij. Tarče tovrstnih napadov naj bi bile največje evropske naftne in gradbene korporacije, hkrati pa se napadov ne morejo izogniti niti manjša

podjetja vpletena v kakršnokoli posle s Ljudsko republiko Kitajsko[35]. Kitajski hekerji naj bi uporabili programsko opremo trojanskih konjev, jih namestili v računalniške sisteme ter prekopirali zaupne podatke (Schneier 2007).

Računalniške sisteme znotraj obrambnega sistema in obveščevalne skupnosti, ki vsebujejo občutljive podatke, lahko zaščitimo s posebno računalniško programsko in strojno opremo, poleg tega lahko računalnike povsem izločimo iz zunanjega sveta s fizično izolacijo (ang. *'stand-alone' systems*) (Davies 2002, 322–323).

5.1.2.1 Primeri obveščevalno motiviranega hekerstva

Leta 1990 je izšla knjiga Clifforda Stolla z naslovom *The Cuckoo's Egg* in tako svetu predstavila sposobnosti glavnega akterja Marcus-a Hess-a in njegovih sovrstnikov v primeru incidenta imenovanega hannovrski hekerski incident (ang. *Hannover Hacker*). Splošno lahko povzamemo, da je začetek HACKINT-a odmeven »*Hannover Hacker*« incident, čeprav obstaja še veliko dokumentiranih napadov te vrste. V navedenem primeru je skupina zahodnonemških hekerjev imenovana »*The Chaos Computer Club*, ki jo je vodil Markus Hess, sistematično vdirala in preiskovala omrežja računalnikov Ministrstva za obrambo Združenih držav Amerike v začetku 80-tih. Njihove akcije je podprla takratna ruska KGB (rus. *Komitet Gosudarstevennoye Besopasnostiye*, ang. *Committee for State Security*) (Davies 2002, 312).

Cliff Stoll, ki je potek lova na nemškega hekerja opisal skozi lastne izkušnje, je bil sistemski administrator v laboratoriju Lawrence Berkeley z nalogo nadzorovanja računov. Ko je na računu opazil razliko, je odkril, da je nekdo vdrl v sistem, poleg tega si je s pomočjo posebne programske opreme pridobil veljavna uporabniška imena in gesla. Takoj ko je Stoll preklical uporabniško ime in geslo, je Hess uporabil drugo kombinacijo gesel. Stoll je nadrejene obvestil o dejavnosti hekerja, vendar jih je vseeno uspel prepričati, da hekerju nastavijo vabo, namesto da računalnike odstranijo iz omrežja. Naslednja naloga Stoll-a je bil poziv lokalnih oblasti, da prestrežejo klice, in naposled so ugotovili, da klic prihaja od Tymnet[36] operaterja iz Oakland-a. Po številnih neuspešnih akcijah so kmalu zatem hekerja le izsledili v Hannovru, takratni Zahodni Nemčiji. V tistih časih je delo Markus-a Hess-a predstavljalo povsem nov način hekerstva, zato

[35] V Združenih državah Amerike so kitajske hekerje označili kot edino resno grožnjo varnosti ameriške tehnologije.
[36] Tymnet je bila ena izmed številnih služb, ki je imela na voljo lokalne številke, neposredni dostop do računalnikov pa so nadzorni računalniki zaznali kot klic na daljavo (medkrajevni klic).

so za pomoč poklical FBI in nemške organe oblasti, ki so Hess-a izsledili in ga aretirali. Po ocenah strokovnjakov naj bi bil Hess nevaren heker. Svoje aktivnosti je opravljal preko univerze v Bremnu ali prek nemškega omrežja DATEX-P preko satelitske povezave ali transatlantskega komunikacijskega kabla v Tymnet. Preko Tymnet-a si je heker z vdiranjem zagotovil dostop do laboratorija Lawrence Berkeley, ki ga je uporabil kot odskočno desko za nadaljevanje svojega poslanstva v celotnem omrežju ARPANET-ain MILNET-a[37]. Znotraj vojaškega omrežja MILNET je Hess lahko napadal okoli 400 računalnikov vojske ZDA po svetu, med njimi so bili SRI International (neodvisen in neprofiten inštitut za raziskave), Darcom vojske ZDA v Seckenheimu, Zahodna Nemčija, vojaška baza Fort Bruckner na Japonskem, vojaško letalsko bazo Ramstein, Zahodna Nemčija, nadzorne sisteme vojnega letalstva ZDA, podatkovno bazo Pentagona, imenovano OPTIMUS, itd. Po odkritju so ugotovili, da je Hess bil heker in hkrati vohun, saj ga je rekrutirala sovjetska KGB. Svoja odkritja in informacije je predal dalje Sovjetom, med njimi so bili predvsem logistični in kadrovski podatki o premikanju vojaške opreme in osebja (Kremen 1998).

Najvišji predstavniki Pentagona so bili osupli, ko so hekerji nakazali možnosti in posledice vdorov v vojaško in civilno informacijsko infrastrukturo. Z uporabo programske opreme, ki je bila na voljo na internetu, je skupina hekerjev iz vrst NSA (ang. *National Security Agency*) nakazala možnost izklopa električne dobave v celotnih Združenih državah Amerike v samo nekaj dneh, pri tem pa prikazala slabosti sistemov za poveljevanje in nadzor znotraj pacifiškega poveljstva vojske ZDA. Operacijo so poimenovali *Eligible Receiver 97.* Skupino 35 hekerjev je najela ena izmed najbolj tajnih obveščevalno-varnostnih agencij na svetu z namenom vdora v informacijsko infrastrukturo vojske ZDA. Hekerji so v nekaj dneh vdrli v 36 od 40.000 omrežij ministrstva za obrambo. Poleg omenjenega napada na vire električne energije so iz uporabe izključili telefonsko številko za nujno pomoč 911 v predelu Washingtona in drugih mestih, poleg tega pa so imeli dostop do uporabe sistemov na križarki, ki je v tistem času izvajala naloge na morju (Christensen 1999).

Rezultati napada, ki je potekal med 9. in 13. junijem 1997 so bili zastrašujoči. Skupina hekerjev je prikazala simulacijo napada na pacifiško poveljstvo vojske ZDA, pri tem pa naj bi hekerji nadzorovali celotno poveljstvo. S strani Pentagona je bil Eligible Receiver označen za

[37] ARPANET (predhodnik današnjega interneta) je bilo omrežje, namenjeno civilni uporabi, ki ga je razvilo Ministrstvo za obrambo ZDA, medtem ko je MILNET bilo omrežje namenjeno, zgolj vojaški uporabi.

zelo pomembno vajo, ki je nakazala šibkosti sistemov in potrebo po boljši organizaciji v primeru napadov na računalniške sisteme in informacijsko infrastrukturo. Vaja naj bi se začela brez opozoril, po dolgih pripravah računalniških strokovnjakov znotraj NSA, cilji napada pa so bili računalniki ameriške vojske v sektorju pacifiškega poveljstva in znotraj ZDA. Naloge hekerjev so bile preproste – izvesti informacijski napad na pacifiško poveljstvo in ZDA prisiliti, da omilijo sovražno politiko do severnokorejskega režima v Pyongyangu. Hekerji naj bi bili plačani najemniki s strani Severne Koreje. NSA je torej s pomočjo hekerjev imenovanih »*Red Team*« (rdeča ekipa), nakazala kako enostavno lahko tuje države onesposobijo delovanje računalnikov. Hekerji, ki so bili nameščeni na Havajih in po drugih predelih Združenih držav Amerike, so vdrli v računalniške sisteme in pridobili dostop do nadzora električne energije za celotno državo. Glavna tarča, torej pacifiško poveljstvo, ki razpolaga z okoli 100.000 ljudi, bi lahko pričela vojno s Severno Korejo in Kitajsko. Po napadu so hekerji uspešno prikrili sled, tako da ni bilo mogoče izslediti, od kod napad poteka, le ena izmed številnih ekip, ki je delovala na območju celinskega dela ZDA, je bila odkrita (Gertz 1998).

Operacija, ki je bila uperjena proti lastnim računalniškim sistemom in informacijskim bazam, je torej prvotno prikazala pomanjkanje zavedanja, da kibernetski vdori lahko vodijo do spopada. John Hamre, ki je bil namestnik ministra za obrambo med 1997 in 1999, je v intervjuju predstavil pomembnost omenjene operacije. Prve dni se oblasti dejansko sploh niso zavedale, da jim preti napad. Rdeča ekipa hekerjev je izvrstno izvedla napad, predvsem pa je pomagala pri dvigu zavesti na področju obrambe o razsežnosti morebitnega kibernetskega napada (Cyberwar! Frontline 2003).

Operacija *Moonlight Maz*e se nanaša na izjemno tajen incident, pri katerem so v ZDA odkrili sledi vdiranja v računalniške sisteme Pentagona, NASE, ministrstva za energijo, zasebnih univerz in raziskovalnih laboratorijev. Napadi so se začeli marca 1998 in so potekali skoraj dve leti. Spletna stran *Frontline* omenja izjemno zanesljive vire, ki poročajo o sistematskem kopiranju na tisoče podatkov – mednje sodijo mape z namestitvijo in položajem vojakov ter vojaško opremo. Strokovnjaki znotraj ministrstva za obrambo ZDA so izsledili sled v bivšo Sovjetsko zvezo, vendar pokrovitelj teh napadov še ni odkrit, medtem ko Ruska federacija zavrača kakršnokoli vpletenost. Operacijo Moonlight Maze še vedno aktivno preiskujejo obveščevalno-varnostne službe ZDA (Cyberwar! Frontline 2003). Mediji so ta incident označili za vrh kibernetskega spopada, uperjen proti Združenim državam Amerike, pri tem pa opozarjajo

na tajnost delovanja hekerjev, ki delajo za Rusko federacijo[38]. Pri tem poudarjajo sistematičnost vdorov v računalniške sisteme ministrstva za obrambo, s pomočjo katerih so si pridobili ogromno število občutljivih informacij.

Kljub temu, da so v FBI našli sled, ki jih je vodila v Rusko federacijo[39], preiskovalci menijo, da ni mogoče povsem dokazati, da je motiv hekerjev vohunjenje, čeprav ključni dokazi nakazujejo vpletenost bivše Sovjetske zveze in njihovih obveščevalnih služb in operacij pridobivanja obveščevalnih podatkov. Michael Vatis, ki je leta 2000 pred kongresom nastopil kot direktor FBI-jevega centra za zaščito državne infrastrukture (ang. *National Infrastructure Protection Center*), je razjasnil nekaj dejstev okoli omenjene operacije, in sicer, da strogo tajnih podatkov napadalec ni uspel pridobiti, vendar so prestregli zelo občutljive informacijo o raziskavah za obrambne namene. Predstavnik ministrstva za energijo je poudaril, da napadi niso bili naključni, temveč skrajno organizirani, kar dodatno meče luč na obveščevalno hekerstvo (Drogin 1999).

Poročilo James-a Adams-a o operaciji navaja, da hekerje dandanes zaposlujejo vladne organizacije, velike korporacije in skupine, ki izvajajo organiziran kriminal. Adams poudarja, da bodo hekerji v prihodnje čedalje bolj prisotni v tej podobi, pri tem jih v prihodnje primerja z dejanji teroristov. Po njegovih podatkih so si ruski hekerji v obdobju izvajanja operacije uspeli pridobiti za nekaj 10 do 100 milijonov dolarjev vredne informacije (Adams 2000).

Podoben primer so ZDA zabeležile leta 2003. Tarči sistematskega vdiranja, domnevno hekerjev kitajske vojske, naj bi bili vlada in industrija ZDA. Napade so izsledili v kitajski provinci Guangdong, pri tem pa odkrili posebne tehnike, ki nakazujejo vpletenost kitajske vojske. Alan Paller, takratni direktor inštituta SANS, izobraževalne in raziskovalne organizacije, namenjene kibernetski varnosti, meni, da je nemogoče izvesti tovrstne napade izven vojaškega sektorja, saj so napadi vsebovali posebne tehnike, poleg tega so hekerji v časovnem obdobju 30 minut brez kakršnih napak zapustili tarčne sisteme. Shawn Carpenter, ki je bil zaposlen kot svetovalec za omrežno varnost v Sandia National Laboratories, kjer se izdela večina jedrskega arzenala za potrebo vojske ZDA, je imel nalogo sledenja kitajskih hekerjev oz. kibervohunov, obenem pa mu je vojaška obveščevalna služba zagotovila prikrito identiteto za sledenje.

[38] Ruska federacija kakšnokoli vpletenost zanika.
[39] Napadalca so odkrili 20 milj (32 km) izven Moskve, deloval je pretežno ob delavnikih med osmo uro zjutraj in peto popoldne, poleg tega napadi na omenjeno informacijsko infrastrukturo se niso vršili med ruskimi prazniki (Adams 2000).

Operaciji, v kateri so hekerji vdirali v sisteme ZDA in pri tem izvajali kibernetsko vohunstvo, so uradniki nadeli ime *Titan Rain.* Carpenter je hekerjem sledil vse od septembra 2003, ko je analiziral vdor v računalniške sisteme podjetja Lockheed Martin. Carpenter je ugotovil, da so hekerji izvedli nekaj mesecev kasneje skoraj identičen napad na sisteme v omenjenih laboratorijih. Njihovi napadi so bili usmerjeni proti kraji izjemno občutljivih podatkov vojaške narave. Carpenter je počasi, a vztrajno sledil napadom, ki so jih izvajali hekerji, in posledično ugotovil, da izhajajo iz 3 usmerjevalnikov (ang. *router*) iz kitajske province Guangdong, ki so povezani v lokalno omrežje in internet (Thornburgh 2005).

Veliko pozornosti se je v tem obdobju namenilo tudi dvema britanskima hekerjema, ki sta podobno kot omenjeni Hess vdirala v računalniške sisteme oblasti ZDA. Britanska hekerja, 16-letni Richard Pryce in 21-letni Mathew Bevan, sta vdrla v več vojaških računalniških informacijskih baz. Prvega so leta 1995 obtožili, ker naj bi si pridobil neavtoriziran dostop do datotek, povezanih z razvojem balističnega orožja in poročil ameriških vohunov v Severni Koreji iz leta 1994 glede razvijanja jedrskega orožja omenjene države.

Bevan, strokovnjak za informacijsko tehnologijo, je bil obsojen leta 1996 zaradi omogočanja neavtoriziranih dostopov. Pryce je uporabljal vzdevek »*Datastream Cowboy*«, medtem ko se je Bevan ponašal z vzdevkom »*Kuji*«. Slednji je bil pravzaprav mentor prvemu, saj ga je naučil vdorov v sisteme. Po poročilih različnih medijev naj bi Kuji bil tuj agent.

Pryce and Bevan sta med drugimi vdrla v Rome Air Development Center, letalsko bazo Griffiss, in preden so oblasti ugotovile njihovo prisotnost (po petih dneh), sta vdrla še v sedem ostalih sistemov, prekopirala različne datoteke, vključno z izredno varovanim bojnim simulatorjem, in namestila programsko opremo, ki je prebrala uporabniške račune z gesli vsakogar, ki se je prijavil v sistem. Rome Air Development Center je služil kot lansirna ploščad za nadaljnje napade na kritično informacijsko infrastrukturo ZDA. Pri tem sta s povsem legalnimi gesli prekopirala nešteto datotek[40] iz baz NASE, Wright-Patterson letalske baze ter različnih obrambnih sistemov itd. Pryce je preko Rome Air Development Center vdrl v korejske računalniške sisteme. Mediji so kasneje poročali, da oblasti ZDA več ur niso vedele, ali je napad uperjen proti Severni ali proti Južni Koreji. Predvsem je oblasti v ZDA skrbelo, da bi Severne Korejce sled peljala v ZDA in bi vdor vzeli kot agresivno dejanje proti njim. Naposled so

[40] Eden izmed prenosov datoteke iz vesoljskega centra Goddard preko dobavitelja v Latviji. Ekipa, ki je vse to skrbno nadzorovala je prenos datoteke pravočasno prekinila.

Američani ugotovili, da gre za južnokorejski Inštitut za atomske raziskave. Pryca in Bevana so kmalu zatem aretirali, vendar sta v obdobju sedmih mesecev vdrla v številne računalniške sisteme in kritični informacijski infrastrukturi ZDA naredila nepopravljivo škodo.

Veliko medijske pozornosti so pritegnili tudi nizozemski hekerji, ki so vdrli v 34 sistemov ZDA v obdobju 1990 in 1991. Pridobili so si podatke o delu zaposlenih v različnih sektorjih obrambnega sistema, o razvoju orožja in opise o premikih vojaške opreme in osebja. Tarča napadov so bili sistemi Naval Sea Systems Command, sistem vojaške pripravljenosti ameriške vojske v Ft. Belvoiru v Virginii in laboratorij za raziskovanje raketnih projektilov v Aberdeenu v Marylandu. Vsaj eden izmed sistemov, ki je bil tarča napada in posledično vdora, je neposredno podpiral ameriške vojaške operacije v operaciji Puščavski vihar neposredno pred zalivsko vojno. Hekerji so vdrli v sisteme, prekopirali originale, spremenili datoteke in namestili programsko opremo, ki bi v bodoče dovolila dostop do sistema, prav tako pa so hekerji iskali zaupne informacije o jedrskem orožju. Preden so jih oblasti odkrile, so hekerji neavtorizirano vdrli v sistem in spremljali podrobnosti o namerah ZDA v operaciji. Hekerji so si nagrabili toliko občutljivih datotek o raketah vrste *patriot*, da je bilo potrebno vdreti v nove računalnike, ker ni bilo več prostora za namestitev. Prav tako so nizozemski hekerji izklopili računalnike, ki so kasneje služili programu mobilizacije vojakov za operacijo Puščavski vihar. Ključne besede, ki so jih uporabljali pri iskanju podatkov, so bile »*vojska*«, »*jedrsko*«, »*Desert Storm*« in »*Desert Shield*«. Preiskovalci so ugotovili, da so hekerji sicer neodvisni, vendar so sumili, da so želeli podatke prodati ruskemu KGB[41] ali iraški obveščevalni službi, vendar naposled ni bilo mogoče pridobiti dovolj trdnih dokazov, da bi to teorijo potrdili (US Department of Energy, Training Center 2008).

Vsekakor je preveč površno meniti, da občutljivi (ne spadajo med strogo zaupne) podatki nimajo posebne obveščevalne vrednosti. Večina pridobljenih podatkov ali informacij, ki so jih hekerji s pomočjo neavtoriziranega dostopa do informacijskih baz pridobili, so bili logistične narave, ki pa lahko odkrije načrte, kapaciteto in sposobnost sil. Kibernetski vdori, navedeni v zgornjih primerih, so nakazali povsem neraziskano področje, med pridobivanjem podatkov prek brskanja po javno dostopnih bazah in tajnim delovanjem. Elektronska pošta lahko potencialno vsebuje dragocene informacije, lahko jo celo enačimo s telefonskimi pogovori ali prestrezanjem pošiljk. Tako lahko nenevarna elektronska pošta, ki vsebuje povsem nezaupne podatke,

[41] KGB so razpustili 6. novembra 1991.

imenovane tudi informacije nizkega razreda (ang. low-grade intelligence), služi navsezadnje kot ozadje za analizo in se kasneje dopolni tudi z bolj občutljivi zaupnimi podatki pri izdelavi celotne slike oz. izoblikovanje dokončnih informacij (Davies 1999, 118–119).

5.2 Novačenje hekerjev v obveščevalno-varnostne službe

Dejstvo, da so hekerji zaželeni v vrstah obveščevalno-varnostnih služb, že nekaj časa ni presenetljivo, saj lahko ti posamezniki zagotovijo tajen dostop do podatkov in tako vohunijo z majhno verjetnostjo, da jih izsledijo. Narava kompleksnosti uporabe nove tehnologije, združevanje tradicionalnega telefonskega sistema in informacijske tehnologije v enotno platformo, soočanja z novodobnimi viri ogrožanja varnosti posameznika, družbe/države in mednarodne skupnosti v kibernetskem prostoru, so povzročile spremembe v delovanju obveščevalno-varnostnih služb, pri tem pa so se morale nujno usmeriti k iskanjem rešitev in zaščiti omenjenih akterjev v varnostnem okolju. Zaradi vseh omenjenih sprememb obveščevalne službe zahtevajo polno vključenost ali sodelovanje vrhunskih računalniških strokovnjakov. Novačenje hekerjev v obveščevalno sfero tako danes ni nič presenetljivega. Globalnost informacijsko-komunikacijske tehnologije je povečalo število nasprotnikov za uporabnike tako v domačem kot mednarodnem okolju.

Schwartau (2000, 316–317) meni, da je vprašanje novačenja hekerjev v organizacije z namenom obrambe informacijske infrastrukture nekega podjetja ali celo kritične infrastrukture države precej občutljivo. In kaj je na tem tako občutljivega?

Ko določena organizacija zaposli v svoje vrste etičnega hekerja na mesto sistemskega administratorja ali morda celo programerja, postane za delodajalca ključno vprašanje zaupanja hekerjem. Največji izziv ali dilema, s katero se delodajalci soočajo, je dejstvo, kako je mogoče celoten uspeh nekega podjetja ali celo odgovornost preložiti v roke tehnično podkovanih posameznikov ali skupin, katerih pravila so predvsem nedoumljiva. Podjetniki si želijo denarja, ljudje na oblasti si želijo moči, medtem ko hekerje vodi le napredek tehnologije. In tukaj se soočimo z vprašanjem, ali je mogoče to združiti (Schwartau 2000, 316–317).

Winkler (2005, 258–259) navaja nekaj dejstev, zakaj določena organizacija v svojih vrstah ne sme zaposliti ali najeti hekerje kot svetovalce za zaščito informacijske infrastrukture.

Winkler meni, da v primeru zaposlitve hekerja[42] delodajalec tvega, saj enostavno sama logika zaposlitve nekoga, ki je svoje znanje pridobil na nezakonit način, ni smiselna. Zaposlovanje hekerja za zaščito slikovito primerja z morilcem, ki svojo žrtev zabode, nato postane kirurg z namenom preprečiti, da njegova žrtev umre. Prav tako je mnenja, da ne moremo enačiti dejanja vdiranja v sistem s testiranjem sistemov proti vdorom in da večina hekerjev ne zna varnostno testirati sisteme.

Kot sem že omenil, Schwartau definira hekerje kot prve informacijske bojevnike. Winkler v svoji knjigi *Spies Among Us* prav tako uvaja izraz informacijskih bojevnikov. Za razliko od Schwartau-a, Winkler govori o informacijskih bojevnikih[43] kot o grožnji, ki preti posameznikom in organizacijam, vendar kljub vsemu dodaja, da lahko imajo nalogo pomagati pri uresničevanju ciljev države, med drugim tudi iskanju informacij v vseh možnih oblikah. Ti posamezniki se od ostalih ločijo predvsem v ekstremnih sposobnostih, znanju, ki se ne more enačiti z ostalimi. Njihovi cilji so lahko tudi izrazito strateškega pomena, njihove naloge so jasno začrtane, izvajajo jih z namenom uresničitve in zagotavljanja dolgoročne strateške prednosti. Dolgoročno gledano, se ti posamezniki lahko pripravljajo celo na vojno stanje. Tako se lahko prebijejo v tujo infrastrukturo in načrtujejo prevzeti ali celo onesposobiti delovanje določenih sistemov. Prav tako avtor omenja, da je hekerstvo postalo osnovna metoda številnim državam za vdiranje v infrastrukturo. Dovoljuje celo majhnim državam, da povzročijo stanje asimetričnega vojskovanja, pri tem pa je cilj izvajanja asimetrije poraziti nasprotnika brez uporabe vojaške sile. Do leta 2000 je več kot 100 držav poskušalo vzpostaviti in zagotoviti kapacitete za izvajanje informacijskega vojskovanja. Oktobra 2004 so južnokorejski uradniki poročali, da je Severna Koreja začela uriti 500 ljudi z namenom izvajanja vojne prek računalnikov.

Za razliko od navadnih informacijskih bojevnikov Winkler obravnava tudi t.i. »zbiratelje obveščevalnih podatkov« kot posameznike, ki delajo znotraj obveščevalne dejavnosti, pri tem pa jih odlikuje povsem drugačna motivacija, predvsem zaradi tega, ker so del obveščevalno-varnostnih služb in vojaške organizacije. Medtem ko strokovnjaki s področja informacijskega bojevanja končajo delo takrat, ko onesposobijo delovanje informacijske infrastrukture, informacijski bojevniki takrat šele pričnejo z zbiranjem informacij. Naloga teh je torej

[42] Winkler (2005, 258) ima v mislih tiste hekerje, ki so bili v preteklosti že obsojeni zaradi kriminalnih dejanj ali so dejansko sami priznali, da so izvajali kriminalna dejanja.
[43] Po Winklerju informacijski bojevniki niso le računalniški bojevniki temveč tudi ostali, ki si prizadevajo pridobiti in zbirati podatke v vseh možnih oblikah. Avtor vseeno uvršča informacijske bojevnike v tradicionalno hekersko skupnost (ibid., 258).

pridobivanje obveščevalnih podatkov. Kot je bilo že omenjeno, je okoli 100 držav do nedavnega poskušalo vzpostaviti omenjene kapacitete za normalno delovanje. Čeprav večina ljudi v ZDA verjame, da so tarče teh posameznikov usmerjene proti informacijam organov zagotavljanja nacionalne varnosti, so cilji uperjeni predvsem v korporacije in posameznike. Torej obveščevalna dejavnost danes ni več domena samo oblastvenih organov, temveč so korporacije in druge organizacije razvile lastne kapacitete obveščevalne dejavnosti. Predvsem je cilj in poslanstvo teh služb, da si zagotovijo informacije o konkurenčnih podjetjih (Winkler 2005, 66–68).

5.2.1 Primeri novačenja hekerjev v obveščevalne vrste

Ruski GRU (rus. *Glavnoje Razvedyvatel'noje Upravlenije*, ang. *Main intelligence Directorate*), ki ga v slovenski jezik lahko prevedemo kot osrednji direktorat za obveščevalno dejavnost, po navedbah Winklerja razpolaga z najbolj naprednim hekerskim znanjem na svetu, saj meni, da se lahko z njim primerjajo samo nekateri informacijski centri v Združenih državah Amerike. Že samo dejstvo, da ima GRU pristojnost izvajanja strateških priprav na morebiten vojaški spopad, nakazuje strah vzbujajočo spoštovanje. Čeprav Ruska federacija posveča največ pozornosti čečenskim teroristom, so ZDA še vedno največja vojaška nasprotnica in v primeru priprav na morebitno vojno stanje proti ZDA, bi GRU vsekakor poskušal onesposobiti delovanje sistemov kritične infrastrukture ZDA. Tako so po vsej verjetnosti že pripravili načrt, kako onesposobiti sisteme, ki bi jim zadal nepopravljivo škodo. Winkler celo navaja, da sicer ne verjame v »*elektronski Pearl Harbour*«, toda če je katera skupina sposobna izvesti računalniški napad po japonskem vzorcu napada na pristanišče na Havajih, je to prav ruski GRU (Winkler 2005, 85).

Leta 1999 so v Ruski federaciji izvedli operacijo, imenovano *Moonlight Maze*, njena tarča pa je bila računalniška infrastruktura v Pentagonu in podatki, povezani s tehničnimi raziskavami na področju obrambe. Čeprav ukradeni podatki niso bili strogo zaupni, so imeli neprecenljivo vrednost za tuje vlade, teroristične skupine, privatna podjetja itd., saj so uspeli pridobiti informacije, povezane z vojaško logistiko, načrtovanjem, plačili in naročili, o osebju in, morda najpomembnejše, uspeli so ugotoviti potek pošiljanja elektronskih pošt znotraj oddelkov v Pentagonu. Oleg Gordievsky, bivši KGB-jevec v Londonu, je podprl številna hipotetična vprašanja o ruskih hekerjih znotraj obveščevalnih vrst. Tako naj bi organizirane skupine in hekerji delovali z naslednico KGB-ja FSB. Navaja tudi primer nekega hekerja, ki so mu ponudili

možnost sodelovanja z obveščevalno službo ali iti v zapor (Alvey 2001, 53).

Prav tako številni drugi avtorji in strokovnjaki navajajo, da ruske obveščevalno-varnostne službe novačijo hekerje v svoje vrste z namenom vohunjenja na domačih in tujih tleh. V Ruski federaciji je znan primer izpred nekaj let, ko naj bi veleposlaništvo Združenih držav Amerike tajno rekrutiralo ruskega hekerja v svoje vrste z namenom tajnega sodelovanja z obveščevalno-varnostnimi službami proti Ruski federaciji. Kiberkriminal v Rusiji se zadnja leta ekstremno povečuje: leta 2000 je bilo registriranih 1.375 dejanj kibernetskega kriminala, kar je pomenilo 18 % rast v primerjavi s prejšnjim letom. Odstotek seveda v primerjavi z Zahodom ne pomeni pretirane skrbi, če ne upoštevamo, da ima samo 4.5 % prebivalstva Ruske federacije dostop do interneta v primerjavi z ZDA, kjer podatki kažejo, da je teh okoli 49.1 %. Po nekaterih ocenah strokovnjaki ocenjujejo, da je v Ruski federaciji med 250 in 500 hekerjev, okoli 40 izmed njih lahko najemajo različne organizacije. Prav tako so raziskave pokazale, da je ruski heker star med 16 in 34 let, ponavadi moškega spola ter seveda izjemnega tehničnega znanja (Alvey 2001, 52–53).

Spletna stran Globalsecurity.com navaja številne primere ruskih hekerjev, med njimi tudi primere novačenja hekerjev v vrste FSB[44]-ja z namemon iskanja informacij. Spletna stran prav tako omenja primere šolanja hekerjev v »edini« hekerski šoli Ilye Vasilyeva v prestolnici Ruske federacije imenovani »*shkola hackerov*«. Ruski hekerji veljajo za precej bolj inovativne v svoji dejavnosti, saj jim primankuje sredstev (GlobalSecurity.org 2000).

Čeprav se na Kitajskem soočajo s problemom pomanjkanja uporabe novih tehnologij po celotni državi, si ena izmed najmočnejših gospodarskih sil na svetu prizadeva zagotoviti enakovreden položaj z ostalimi svetovnimi gospodarskimi velesilami 21. stoletja. Gospodarsko vohunjenje postaja čedalje večja prioritetna naloga znotraj obveščevalne dejavnosti LR Kitajske, saj so med drugimi vojaške obveščevalne zmogljivosti preusmerili v gospodarsko vohunstvo (Winkler 2005, 85-86). Ljudska informacijska vojna je kitajski pogled na izvajanje informacijskega bojevanja, medtem ko jo ameriški dokumenti imenujejo nacionalistični heking oz. uporaba hekerskega znanja za potrebe (kitajskih) nacionalnih interesov (Svete 2005, 147).

Prav tako lahko v vsakoletnih analizah ocene vojaške moči Ljudske republike Kitajske, ki jih za ameriški kongres izvaja ministrstvo za obrambo, razberemo, da so enote Ljudske osvobodilne armade (kraj. LOA) izurjene tudi v informacijskem bojevanju, saj nasprotnikove

[44] Ang. Federal Security Service of the Russian Federation (rus. *Federalnaya Sluzhba Bezopasnosti).*

računalniške in informacijske sisteme napadajo s pomočjo virusov. Ljudska osvobodilna armada je prav tako povečala vlogo omenjenih enot na vojaških vajah (Office of the Secretary of Defence 2005).

Tako LOA v svoje vrste privablja čedalje več računalniških ekspertov[45]. Svete (2005, 149) navaja, da je v enotah vedno več računalnikarjev-vojakov (kit. Jisuanjibing) ter omrežnih bojevnikov (kit. Wangluozhansh) rekrutiranih v oborožene sile. Vsi med njimi obvladajo tuje jezike (angleščino), njihov glavni cilj pa je uposabljanje za digitalno uničenje nasprotnika oz. njegove infrastrukture.

LR Kitajska je posebej zanimiva tudi v luči novačenja hekerjev v obveščevalno sfero. Kitajski vojaški hekerji naj bi pripravili podroben načrt kibernetskega napada z namenom nevtraliziranja celotne flote letalonosilk ameriške vojske. Razlog za takšen napad naj bila želja po dominiranju v elektronskem svetu do leta 2050. Tarča kitajskih napadov naj bi bila sovražnikova komunikacijska, vojaška in finančna infrastruktura že pred samim konfliktom, analizirajo uradniki znotraj obveščevalne skupnosti ZDA. Kitajski vojaški hekerji so že opozorili na svoje sposobnosti v operaciji Titan Rain, poleg tega svoj interes za prisotnost kažejo tudi drugje po svetu. Napadi, ki jih izvajajo kitajske oblasti, so tako pogosto in čedalje bolj agresivni, leta 2005 so jih v Pentagonu prešteli prek 79.000, med katerimi je bilo okoli 1.300 uspešnih. Po mnenju Jim Melnick-a, upokojenega računalniškega strokovnjaka v Pentagonu, kitajski vojaški hekerji vdirajo v sisteme z namenom iskanja in novačenja talentiranih posameznikov v kiber-vojsko (Reid 2007).

Kitajski hekerji torej prestavljajo velik razlog za skrb, saj svojo dejavnost čedalje bolj usmerjajo iz tradicionalnih metod pridobivanja obveščevalnih podatkov proti pridobivanju podatkov s pomočjo sodobne tehnologije in še posebej hekanja. LR Kitajska naj bi po določenih virih uporabljala agresivne metode v obveščevalni dejavnosti, s hekerskimi vdori pa naj bi poskušala pridobiti tajne podatke (Evans 2007).

Posebno pozornost je potrebno nameniti Severni Koreji, saj po nekaterih podatkih predstavlja eno izmed vodilnih proizvajalk hekerjev, ki jih posledično privabijo tudi v obveščevalne vrste. Po ocenah ministrstva za obrambo Južne Koreje, naj bi Severnokorejci

[45] Kitajski hekerji naj bi vztrajno napadali točno določene tarče večkrat dnevno (direktor inštituta SANS Allen Paller omenja okoli 100 napadov dnevno). Pri tem so tarče napadov državni organi in velike korporacije. Zanimiv podatek je tudi ta, da naj bi okoli 40.000 hekerjev zbiralo obveščevalne podatke iz ameriških informacijskih sistemov in sistemov njihovih zaveznikov (Rogers 2008).

izurili okoli 600 hekerjev z namenom obveščevalnega bojevanja in izvajanja kibernetski napadov uperjenih proti Združenim državam Amerike in Južni Koreji. Severnokorejski računalniški strokovnjaki so vključeni v petletni univerzitetni program, med njimi posebne ekipe izberejo hekerje, katerih naloga je zbirati vojaške podatke od ZDA, Južne Koreje in Japonske in izvajati kibernetske napade (Soo-jeong Lee 2004).

Seul[46] celo opozarja, da je njihova severna soseda izurila vsako leto okoli 100 t.i. »*kibervojakov*« (ang. *cybersoldiers*) zadnjih dvajset let. Diplomiranci elitnega hekerskega programa na univerzi Mirim naj bi bili sposobni izvesti vse od programiranja virusov do vdiranja v še tako zahtevna omrežja in računalniške sisteme. Od leta 1994 naj bi vojaško osebje in obveščevalni agentje Južne Koreje opozarjali na rastočo grožnjo informacijskega bojevanja s strani Severne Koreje, čeprav niso uspeli pridobiti trdnih dokazov o obstoju omenjene univerze. Kljub temu pa Južna Koreja skrbno uri svoje »informacijske strokovnjake« v primeru kibernetskega napada s strani severne sosede. Južnokorejsko obrambno poročilo iz leta 2000 je razkrilo zanimive podatke, saj naj bi bilo kar 5 % proračuna Južne Koreje namenjenih tehnološkemu razvoju in informacijskemu bojevanju. V poročilu pa izstopa podatek, da naj bi južnokorejska vojska razpolagala s 177 vojaškimi računalniškimi bazami, namenjenimi za urjenje, in izurila tako več kot 200.000 »informacijskih tehnikov« (McWilliams 2003).

Prav tako se nekatere navidez »manj« aktivne države na področju informacijskega bojevanja prebijajo v sam svetovni vrh obveščevalnega hekerstva. In med njimi sta obveščevalni dejavnosti republike Francije in Zvezne republike Nemčije, ki počasi, a vztrajno razvijata sektorje hekerjev znotraj obveščevalno-varnostnih služb. Francozi in njihova obveščevalno-varnostna služba za zunanjo varnost *Direction Générale de la Sécurité Extérieure*[47] (v nadaljevanju kraj. *DGSE*) sicer že precej časa namenja posebno pozornost hekerski skupnosti in poudarja pomembnost hekerjev pri pridobivanju informacij, med drugim so usposobili eno izmed najboljših skupin hekerjev na svetu.

Francozi podpirajo tudi hekersko podzemlje, večinoma z namenom prekrivanja lastne aktivnosti in pridobivanja podatkov. Dr. Spafford z univerze Purdue je izjavil, da je Francija odkrila nove ranljivosti računalniških sistemov in jih delila s hekersko skupnostjo, kar pomeni,

[46] Ocene so lahko tudi pretirane.

[47] Francoska obveščevalna-varnostna služba za zunanjo varnost deluje v okviru ministrstva za obrambo, področje delovanja pa je usmerjeno predvsem v vojaško obveščevalno dejavnost, pridobivanje obveščevalnih podatkov strateške narave, prav tako pa svoje delo opravlja tudi na področju protiobveščevalne dejavnosti zunaj meje republike Francije (FAS 2008).

da so omogočili hekerjem uporabljati povsem nove metode napadov na računalniške sisteme, poleg tega pa so s to potezo uspešno prikrili svojo ilegalno aktivnost, ki jo izvaja DGSE. Torej, če povprečen heker lahko vdre v računalniški sistem z dovršenim napadom, potem bodo podjetja, ki so bila tarča francoskih hekerjev, zagotovo sklepala, da je napad izvedel mladoleten heker, ne pa izjemno izurjen operativec znotraj DGSE (Winkler 2005, 90–92).

Podobno kot francoska DGSE ima tudi nemška *Bundesnachrichtendienst* (ang. *Federal Intelligence Service*, kraj. BND) oz. Zvezna obveščevalno-varnostna služba izjemno močno hekersko komponento. Projekt, imenovan *Rahab,* naj bi se začel leta 1990 in poteka še danes, namen projekta naj bi bil s pomočjo hekerskih metod vdreti v računalniška omrežja in sisteme Komisije za globalno informacijsko infrastrukturo (ang. *Global Information Infrastructure Commission*), saj bi si z vdori v številne vladne in nevladne računalniške sisteme tako lahko zagotovili preživetje. Eden izmed največjih uspehov omenjenega projekta je bil vdor v sistem SWIFT, ki predstavlja enega izmed največjih finančnih omrežij na svetu. Sistem SWIFT dnevno nadzoruje milijarde dolarjev vredne transakcije med finančnimi institucijami po svetu in če je verjeti nekaterim poročilom, lahko Nemčija prav s pomočjo vdiranja v informacijsko infrastrukturo spremlja večino vseh svetovnih transakcij. Vrednost takšnih obveščevalnih podatkov je neprecenljiva, po vsej verjetnosti pa Nemčija zagotovo uporablja te informacije. Pri tem pa ima tudi BND možnost, da ukrade številne podatke zasebnim podjetjem (Winkler 2005, 94–95).

Pomembno vlogo pri obveščevalnem hekerstvu igra tukaj tudi država Izrael, ki naj bi imela tretjo najbolj razvito obveščevalno skupnost na svetu, takoj za Združenimi državami Amerike in Rusko federacijo. Izraelski Mosad (ang. Mossad) in LAKAM[48] (obveščevalna služba ministrstva za obrambo) naj bi v preteklosti že novačili hekerje v svoje vrste. Obe omenjeni obveščevalno-varnostni službi podpirata hekersko dejavnost podobno kot francoska DGSE, pri tem pa poskušata novačiti nove in še bolj talentirane hekerje (Winkler 2005, 93–94).

[48] LAKAM (ang. Lekem) je bil ustanovljen leta 1960 z namenom zbiranja in pridobivanja znanstvenih podatkov »na vse možne načine« (Internetna enciklopedija Wikipedia 2008).

6 ZAKLJUČEK IN VERIFIKACIJA HIPOTEZ

Hekerstvo je danes odraz domišljije, kreativnosti uporabe tehnologije, ki pa ni omejeno zgolj na področje računalništva. Tako z vsakim novim tehnološkim napredkom znanost dobiva strokovnjake, hekerje spremljevalce, ki z nadobudnim očesom opazujejo vsak nov korak tehnoloških dosežkov. Internet, najodmevnejši krik informacijske revolucije, je bil sprva namenjen zgolj peščici posameznikov znotraj državne uprave. Med drugim smo tudi s pomočjo hekerskega prizadevanja po svobodi informiranja in dostopa do računalniških sistemov danes praktično že omrežili celoten planet. Informacijsko-komunikacijska tehnologija danes v svetu igra izjemno pomembno vlogo, tako v zasebni kot javni sferi. S sabo je omenjena tehnologija prinesla val sprememb v družbi, pri tem jo je iz (post)industrijske dobe pahnila v informacijsko, tako družbo preplavila z novimi možnostmi e-storitev, posameznika obenem oddaljila od družbe in ga hkrati povezala z ostalim svetom. Vendar ima informatizacija družbe tudi svojo negativno plat. Tako se je hekerska kreativnost uporabe tehnologije, napredno znanje in uporaba tehnologije v tako obsežnem okolju, kot je kibernetski prostor, hitro prelevila v izkoriščanje potenciala, ki ga ponuja internet. Hekerje so po začetnih vdorih, krajah podatkov in zlorabah bančnih storitev kmalu začeli označevati kot kiberkriminalce, prvotna filozofija hekerjev je kmalu bila pozabljena, mediji in računalniška industrija pa sta k napačni predstavi hekerskega poslanstva postavila temeljni kamen za izgradnjo zgrešene podobe hekanja.

Skozi diplomsko nalogo sem proučil večplasten pojav hekerstva in njegovo vlogo v različnih obdobjih, predstavil motivacijo hekerjev za vdiranje v računalniške sisteme in njihove metode dela ter označil vlogo hekerjev v sodobnih konfliktih. Kot sem opisal v poglavju o hekerskem vojskovanju, hekerji čedalje bolj igrajo vlogo aktivnega igralca tudi pri sodobnih konfliktih. S tem lahko ***potrdim*** drugo hipotezo, *Hekerji bodo v prihodnje igrali pomembno vlogo ob načrtovanju in izvajanju hekerskih aktivnosti pred in med samim konfliktom.* Številni navedeni primeri (Gruzija, Estonija, Pakistan in Indija, itd.) hekerske vpletenosti v politično dogajanje po svetu so dokaz, da so hekerji čedalje bolj prisotni v političnih konfliktih. Kljub povdarjanju individualnosti pri delu hekerjev, se ti združijo v organizirano in navzven nepovezano skupino s točno določenimi (političnimi) cilji. Tako lahko preko spleta objavljajo propagandni material ali z dezinformacijami širijo neresnice o nasprotniku. Hekerji so nase opozorili tudi v številnih simulacijah, ko so jasno nakazali možnosti in posledice uporabe

hekerskih vdorov pri izvedbi tovrstnih operacij.

V zadnjem delu sem v celoti posvetil pozornost obveščevalno motiviranemu hekerstvu, ki se v zadnjih časih vse bolj pogosto omenja tako v strokovni literaturi kot v medijih. Seveda je pri tem potrebno poudariti, da obveščevalno-varnostne službe držav, ki sem jih v zaključnem poglavju obravnaval, podatkov o novačenju hekerjev v svoje vrste ne objavljajo, čeprav je v številnih člankih novačenje hekerjev precej polemizirana tema. Eno izmed ključnih vprašanj, na katerega sem poskušal odgovoriti, je, zakaj obveščevalno-varnostne službe danes v svoje vrste privabljajo hekerje in kaj je pri tem tako spornega. Napredek tehnologije, povečanje zmogljivosti delovanja računalniških sistemov in s tem tudi hitrosti prenosa podatkov, možnost objave in izmenjave (prestrezanja) podatkov prek svetovnega spleta, obseg podatkov na svetovnem spletu, izdelovanje vse bolj kompleksne in zahtevne programske opreme, združevanje različnih medijev v enotno platformo, dostopnost podatkov na vsakem koraku, so med drugimi številni razlogi za novačenje hekerjev v obveščevalne vrste. Pri tem pa moram poudariti, da imam vseskozi v mislih tudi dejstvo, da obveščevalna dejavnost danes ni več domena samo nacionalne države, velike korporacije že same v svoje enote dodajajo hekerje z namenom pridobivanja podatkov konkurenčnih korporacij.

Cilj naloge je bil tako potrditi ali ovreči zastavljeno hipotezo, *Vloga in pomen hekerstva se skozi čas in napredek tehnologije spreminjata. V svetu, kjer informacije pridobivajo na moči, bodo hekerji postajali čedalje bolj pomemben člen pri zagotavljanju nacionalne varnosti. Novačenje hekerjev v obveščevalne vrste bo tako v prihodnje postalo stalna praksa obveščevalno-varnostnih služb.* V prejšnjem odstavku in skozi diplomsko delo sem že nekoliko nakazal, da lahko prvo hipotezo ***delno potrdim***, kar pomeni, da ni mogoče popolnoma trditi, da so novačenja hekerjev v svoje vrste stalna praksa obveščevalno-varnostnih služb. Predvsem bi rad bil nekoliko pazljiv glede potrditve prve hipoteze, saj trdnih dokazov o načrtnem novačenju hekerjev ni ali niso dostopni javnosti. Zgodovina obveščevalno motiviranega hekerstva je sicer bogata, a se vseeno večina objavljenih člankov nanaša na objavo poročil določenih preiskovalnih agencij ali služb, ki so bila tarča napadov in že pred samo preiskavo s prstom kažejo na najbolj predvidljivega storilca. V nekaterih primerih obveščevalno motiviranega hekerstva (npr. primer Severne Koreje in Južne Koreje) se pogosto celo pretirava, zato ni mogoče pridobiti jasne, objektivne slike.

Ob zaključku diplomske naloge bi rad vseeno pustil nekoliko odprtega manevrskega

prostora glede dokončne potrditve hipoteze, saj bomo v prihodnje po vsej verjetnosti še velikokrat deležni poskusov pridobivanja obveščevalnih podatkov s hekerskimi metodami. Obveščevalna dejavnost je v vsej svoji zgodovini predstavljala pomemben člen pri razvoju tehnologije. Kibernetski prostor in možnost kibernetske infiltracije hekerjev v tuje računalniške in informacijske sisteme z namenom pridobivanja obveščevalnih podatkov so vsekakor novo poglavje v leksikonu delovanja obveščevalnih služb.

7 LITERATURA

1. About.com: PC World Computing Center. 2008. *Hacking's History*. Dostopno prek: http://pcworld.about.com/news/Apr102001id45764.htm (23. marec 2008).

2. Adams, James. 2000. *Testimony of James Adams, Chief Executive Officer, Infrastructure Defense, INC*. Dostopno prek: http://www.senate.gov/~gov_affairs/030200_adams.htm (10. junij 2008).

3. Albert S., David. 1996. *The Unintended Consequences of Information Age Technologies: Avoiding the Pitfalls, Seizing the Initiative*. Washington DC: National Defense University.

4. Alvey, Ruth. 2001. Russian hackers for hire: the rise of the e-mercenary. *Jane's Intelligence Review* 13 (7): 52–53.

5. Allen D., Patrick in Chris C. Demchak. 2003. *The Palestinian-Israel: Cyberwar*. Dostopno prek: http://findarticles.com/p/articles/mi_m0PBZ/is_2_83/ai_106732244/pg_1?tag=artBody;col1 (7. avgust 2008).

6. Anhal, Aarti. 2002. Hackers take Kashmir dispute to cyberspace. *Jane's Intelligence Review* 14 (10): 52–53.

7. Office of the Secretary of Defence. 2005. Annual Report to Congress: *The Military Power of the People's Republic of China*. Dostopno prek: http://www.defenselink.mil/news/Jul2005/d20050719china.pdf (16. avgust 2008).

8. Barnett W., Roger. 2003. *Asymmetrical Warfare*. Washington DC: Brassey's Inc.

9. Bratuša, Tomaž. 2006. *Hekerski vdori in zaščita*. Ljubljana: Založba Pasadena d.o.o..

10. Palmer, C.C.. 2001. *Ethnical Hacking*. Dostopno prek: http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci921117,00.html (27. april. 2008).

11. Cerle, Gaber. 2005. Upravljanje informacijske varnosti – socialni inženiring. *Varstvoslovje* 7 (1): 23-30.

12. CERT.org. 1999. *CIH – Chernobyl virus*. Dostopno prek: http://www.cert.org/incident_notes/IN-99-03.html (5. september 2008).

13. Christensen, John. 1999. *Bracing for guerilla warfare in cyberspace: There are lots of opportunities; that's very scary.* Dostopno prek: http://edition.cnn.com/TECH/specials/hackers/cyberterror/ (9. junij 2008).

14. Clark, M. Robert. 2007. *Intelligence Analysis: A Target-Centric Approach*. Second Edition. Washington D.C.: CQ Press.

15. Cybenko, George, Annarita Giani in Paul Thompson. 2002. *Cognitive Hacking: A Battle for the Mind*. Dostopno prek: http://www.ists.dartmouth.edu/library/chb0802.pdf (7. avgust 2008).

16. Cyberwar! Frontline. 2003. *Interview John Hamre*. Dostopno prek: http://www.pbs.org/wgbh/pages/frontline/shows/cyberwar/interviews/hamre.html (10. Junij 2008).

17. Cyberwar! Frontline. 2003. *Moonlight Maze*. Dostopno prek: http://www.pbs.org/wgbh/pages/frontline/shows/cyberwar/warnings/ (10. junij 2008).

18. Črnčec, Damir. 2005. Obveščevalno-varnostna dejavnost v 21. stoletju: potreba po *deliti* z ostalimi. *Revija Obramba* 37 (2): 28–30.

19. Davies, P.H.J.. 1999. The information warfare and the future of the spy. *Information, Communication & Society* 2(2): 115–133.

20. Davies, P.H.J.. 2002. Intelligence, Information Technology, and Information Warfare. V *Annual Review of Information Science and Technology*, ur. Blaise Cronin, 312–352. Medford, NJ: Information Today, Inc.

21. Denning, E. Dorothy. 2001. *Activism, Hacktivism, and Cyberterrorism: The Internet as a tool for influencing foreign policy*. Dostopno prek:

http://www.rand.org/pubs/monograph_reports/MR1382/MR1382.ch8.pdf (10. april 2008).

22. Douglas, Thomas. 2002. *Hacker Culture*. USA: University of Minnesota Press.

23. Drogin, Bob. 1999. *Russians Seem to be Hacking into Pentagon: Sensitive information taken, but nothing top secret.* Dostopno prek: http://www.sfgate.com/cgi-bin/article.cgi?file=/chronicle/archive/1999/10/07/MN58558.DTL (10. junij 2008).

24. Dupont, Alan. 2003. Intelligence for the Twenty-First Century. *Intelligence and National Security* 18 (4): 15–39.

25. Evans, Michael. 2007. *China 'tops list' of cyber-hackers seeking UK government secrets*. Dostopno prek: http://www.timesonline.co.uk/tol/news/world/asia/article2393979.ece (11. junij 2008).

26. Evron, Gadi. 2008. *Battling Botnets and Online Mobs: Estonia's Defence Efforts during Internet War.* Dostopna prek: http://www.ciaonet.org/journals/gjia/v9i1/0000699.pdf (8. junij 2008).

27. FAS 2008. *DGSE – General Directorate for External Security*. Dostopno prek: http://www.fas.org/irp/world/france/defense/dgse/index.html (6. september 2008).

28. Fire Dragon 888. 2008. *The History of Hacking*. Dostopno prek: http://pirates888.blogs.friendster.com/my_blog/2005/12/the_history_of_.html (20. junij 2008).

29. Gertz, Bill. 1998. *NSA's Operation Eligible Receiver*. Dostopno prek: http://www.infosecnews.org/hypermail/9804/0217.html (10. junij 2008).

30. GlobalSecurity.org. 2000. *Russia / Hackers*. Dostopno prek: http://www.globalsecurity.org/intell/library/news/2000/05/000526-cyber1.htm 8. avgust 2008).

31. Hannemyr, Gisle. 1997. *Technology and Pleasure: Hacking considered constructive*. Dostopno prek: http://hannemyr.com/essay/oks97.html#HDR2 (11. april 2008).

32. Hawkins, F. Charles. 1997. *Coming to grips with information warfare: Western perspective.* Dostopno prek: http://www.herolibrary.org/iwa4web.htm (20. marec 2008).

33. Heaton, Jordana. 2000. *Hacker History*. Dostopno prek: http://www.slais.ubc.ca/PEOPLE/students/student-projects/J_Heaton/prehistory.htm (23. marec 2008).

34. Hoffman E., David. 2004. *CIA splipped bugs to Soviets*. Dostopno prek: http://www.msnbc.msn.com/id/4394002 (7. september 2008).

35. IP-RS. 2008. *"Pharming"* napadi. Dostopno prek: http://www.ip-rs.si/varstvo-osebnih-podatkov/informacijske-tehnologije-in-osebni-podatki/varstvo-osebnih-podatkov-na-internetu/#c411 (5. september 2008).

36. IWS: Information Warfare Site. 2007. *Definition of Psychological Operations.* Dostopno prek: http://www.iwar.org.uk/psyops/ (16. avgust 2008).

37. Jamnik, Rajko. 1974. *Elementi teorije informacije*. Ljubljana: Državna založba.

38. Joint Chiefs of Staff. 1996. *Joint Pub. 3–58. Joint Doctrine for Military Deception*. Dostopno prek: http://www.dtic.mil/doctrine/jel/new_pubs/jp3_58.pdf (16. avgust 2008).

39. Kočevar, Iztok. 2007. Nelinearno in asimetrično bojevanje: kaj ostane šibkim? *Revija Obramba* 39 (1): 21–23.

40. Kovačič, Matej. 2006. *Nadzor in zasebnost v informacijski družbi: filozofski, sociološki, pravni in tehnični vidiki nadzora in zasebnost na internetu*. Ljubljana: Znanstvena knjižnica, Fakulteta za družbene vede.

41. Kovačič, Matej. 2004. *Zasebnost na delovnem mestu*. Dostopno prek: http://matej.owca.info/workplace.html (4. september 2008).

42. Kovačič, Matej. 2003. *Zasebnost na internetu*. Ljubljana: Mirovni inštitut, Inštitut za sodobne družbene in politične študije.

43. Kremen H. Stanley. 1998. *Apprehending the Computer Hacker: The Collection and use of Evidence.* Dostopno prek: http://www.shk-dplc.com/cfo/articles/hack.htm (25. maj 2008).

44. Kuehl, Dan. 2002. *Information Operations: The Hard Reality of Soft Power. Joint Command, Control and Information Warfare School Joint Forces Staff College*, NDU. Dostopno prek: http://www.iwar.org.uk/iwar/resources/jiopc/io-textbook.pdf (7. avgust 2008).

45. Libicki C., Martin. 1995. *What is Information Warfare?* Wahington DC: National Defense University.

46. Markoff, John. 2008. *Before the Gunfire, Cyberattaacks*. Dostopno prek: http://www.nytimes.com/2008/08/13/technology/13cyber.html?_r=1&scp=2&sq=cyberwar%20georgia&st=cse&oref=slogin (5. september 2008).

47. *Massachusetts Institute of Technology – MIT*. Dostopno prek: http://web.mit.edu/ (17. junij 2008).

48. McWilliams, Brian. 2003. *North Korea's School for Hackers.* Dostopno prek: http://www.wired.com/politics/law/news/2003/06/59043 (13. junij 2008).

49. Mitnick D. Kevin in William L. Simon. 2002. *The art of deception*. Indianapolis, Indiana: Wiley Publishing Inc..

50. Mlinar, Zdravko. 1994. *Individuacija in globalizacija v prostoru*. Ljubljana: Slovenska akademija znanosti in umetnosti.

51. Močnik, Peter. 2005. Škodljivi računalniški programi. *Varstvoslovje* 7 (1): 55–68.

52. Pivec, Franci. 2003. *Informacijska družba*. Maribor: Subkulturni azil.

53. Purg, Adam. 1995. *Obveščevalne službe*. Ljubljana: Enotnost.

54. Raymond S. Eric. 1996. *Jargon File Resources: The New Hacker's Dictionary*. Dostopno prek: http://www.ccil.org/jargon/jargon_23.html#SEC30 (3. april 2008).

55. Reid, Tim. 2007. *China's cyber army is preparing to march on America, says Pentagon*. Times Online. Dostopno prek: http://technology.timesonline.co.uk/tol/news/tech_and_web/the_web/article2409865.ece (11. junij 2008).

56. Rogers, Jack. 2008. *China has penetrated key U.S. databases: SANS director*. Dostopno prek: http://www.ssr-i.net/pdf/40.000%20Chinese%20hackers%20collect%20US%20information.pdf (7. september 2008).

57. SearchSecurity.com. 2008. *Definitions. Ethnical Hacker.* Dostopno prek: http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci921117,00.html (27. april. 2008).

58. SearchSecurity.com. 2008. *Definitions. Remote Access.* Dostopno prek: http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci212887,00.html (17. junij 2008).

59. Schneier, Bruce. 2007. *MI5 Sounds Alarm on Internet Spying from China*. Dostopno prek: http://www.schneier.com/blog/archives/2007/12/mi5_sounds_alar.html (5. september 2008).

60. Schneier, Bruce. 2000. *Secrets and Lies: digital security in a networked world*. USA: Wiley Computer Publishing.

61. Schwartau, Winn. 1994. *Information warfare. Cyberterrorism: protecting your personal security in the electronic age.* New York: Thunder's Mouth Press.

62. Schwartau, Winn. 2000. *Cybershock: surviving hackers, phreakers, identity thieves, internet terrorists and weapons of mass disruption.* New York: Thunder's Mouth Press.

63. *Shannon, Claude*. Dostopno prek: http://www.nyu.edu/pages/linguistics/courses/v610003/shan.html (16. avgust 2008).

64. *Slovar slovenskega knjižnega jezika*. 1996. Ljubljana: Založba DZS.

65. Slovenski inštitut za revizijo. 1995. *Obvladovanje informacij in ravnanje z njimi*. Ljubljana: Zveza računovodij, finančnikov in revizorjev Slovenije.

66. Slo-Tech. 2006. *XSS – nova (stara) oblika spletnih razobličen*. Dostopno prek: http://slo-tech.com/forum/t233542 (3. september 2008).

67. Soo-jeong Lee. 2004. *North Korea has 600 computer hackers, South Korea claims*. Dostopno prek: http://www.securityfocus.com/news/9649 (12. junij 2008).

68. Spyware Killer and Spyware Detector software. Pestpatrol. 2005. Dostopno prek: http://www.acesoft.net/spyware_killer_detector/spyware_killer_detector.htm (17. junij 2008).

69. Steele D. Robert. 2002. *New Craft of Intelligence: Achieving asymmetric advantage in the face of non-traditional threats.* Dostopno prek: http://www.intelligenceisthefuture.com/New%20Craft%20of%20Intelligence.pdf (24. april 2008).

70. Still, Brian. 2005. *Hacking for a cause.* Dostopno prek: http://firstmonday.org/issues/issue10_9/still/ (27. februar 2008).

71. Strehovec, Janez. 2003. *Umetnost interneta: umetnostno delo in besedilo v času medmrežja*. Ljubljana: Študentska založba.

72. Svete, Uroš. 2005. *Varnost v informacijski družbi*. Ljubljana: Fakulteta za družbene vede.

73. Svete, Uroš. 2002. *Vloga in pomen informacijske tehnologije v sodobnem asimetričnem vojskovanju*. Magistrsko delo. Ljubljana: Fakulteta za družbene vede.

74. Šaponja, Vladimir. 1999. *Taktika dela obveščevalnovarnostnih služb*. Ljubljana: Visoka policijsko-varnostna šola.

75. Taylor, A. Paul. 1999. *Hackers: crime in the digital sublime*. London: Routledge, Taylor & Francis Group.

76. Thompson, Paul. 2008. *Utility-Theoretic Information Retrieval, Cognitive Hacking, and Intelligence and Security Informatics.* Dostopno prek: http://www.ists.dartmouth.edu/library/uti0903.pdf (7. avgust 2008).

77. Thornburgh, Nathan. 2005. *The Invasion of Chinese Cyberspies (And the Man Who Tried to Stop Them).* Dostopno prek: http://www.time.com/time/magazine/article/0,9171,1098961-1,00.html (10. junij 2008).

78. Trček, Franc. 2003. *Problem informacijske (ne)dostopnosti*. Ljubljana: Center za prostorsko sociologijo, Fakulteta za družbene vede.

79. Triglav, Joc. 1996. Informacijska revolucija. *Življenje in tehnika* 47 (1): 27.

80. Trigaux, Robert. 2000. *A history of hacking. St. Petersburg Times Online*. Dostopno prek: http://www.sptimes.com/Hackers/history.hacking.html (4. april 2008).

81. Uranjek, Toni. 2007. *Tehnike vdorov II.: Napadi na spletne strani*. Dostopno prek: http://slowug.org/files/folders/2748/download.aspx (3. september 2008).

82. US Department of Energy, Training Center. 2008. *Hacking from U.S. Government Computers from Overseas: Foreign Hackers working from overseas via the Internet penetrated sensitive U.S. Government computer systems*. Dostopno prek: http://www.ntc.doe.gov/cita/ci_awareness_guide/spystory/Hacking.htm (10. junij 2008).

83. Wall S., David. 2001. *Crime and the Internet*. London and New York: Routledge. Taylor and Francis Group.

84. Wall S., David. 2007. *Cybercrime: the transformation of crime in the information age*. Cambridge, UK: Polity Press.

85. Waltz, Edward. 1998. *Information warfare: principles and operations*. Boston, London: Artech House.

86. Internetna enciklopedija Wikipedia. 2008. *LAKAM*. Dostopno prek: http://sl.wikipedia.org/wiki/LAKAM (25. maj 2008).

87. Winkler, Era. 2005. *Spies among us: how to stop the spies, terrorists, hackers and criminals you don't even know you encounter every day.* Indianapolis, Indiana: Wiley Publishing Inc.

88. *Zakon o tajnih podatkih* (ZTP). Ur. l. RS 87/2001. Dostopno prek: http://zakonodaja.gov.si/rpsi/r03/predpis_ZAKO2133.html (16. junij 2008).

89. Zorkoczy, Peter. 1987. *Informacijska tehnologija*. Ljubljana: Cankarjeva Založba.