Kiberkriminal

Nekateri kiberkriminal definirajo kot vsako obliko kriminala, pri kateri je uporabljena računalniška oziroma v širšem smislu celo informacijska tehnologija. Vendar pa sta Douglas Thomas in Brian D. Loader mnenja, da kiberkriminal ni zgolj samo uporaba informacijsko-komunikacijske tehnologije v kriminalne namene, pač pa je bistveni element kiberkriminala v tem, da ta kriminal ne bi bil mogoč brez uporabe tehnologije, vsaj ne v takem obsegu (Thomas in Loader, 2000: 6). Poleg tega se kiberkriminal po Reitingerju od navadnega kriminala razlikuje še po treh pomembnih značilnostih: lahko je izveden na daljavo; identiteto osebe, ki kaznivo dejanje izvede je mogoče razmeroma enostavno zakriti ali ponarediti (to je tudi razlog za številne internetne prevare, tim. *phishing*); poleg tega pa sledenje izvornemu komunikacijskemu sredstvu, preko katerega se je nekdo povezal v kiberprostor, ni vedno mogoče, saj izurjeni napadalci pogosto uporabljajo tehniko povezovanja preko različnih sistemov (ang. *looping* ali *weaving*, gre za tehniko, ko se napadalec na ciljni sistem ne poveže neposredno, pač pa preko številnih drugih sistemov, po možnosti lociranih v različnih državah, kar onemogoči ali vsaj oteži sledenje) (Reitinger, 2000: 137). Thomas pravi: "*[Hekerji] razumejo, da če 'kriminal' ne more biti povezan s telesom, le-ta ne more biti kaznovan*" (Thomas, 2000: 24). To je tudi razlog, zakaj ljudje kiberkriminalce pogosto dojemajo kot napol čudežna bitja in zakaj se o hekerjih in njihovih sposobnostih pogosto spletajo napol mi(s)tične predstave.

Kiberkriminalci

Izraz "heker" (ang. *hacker*) je prvi uporabil Joseph Weizenbaum leta 1976 (Voiskounsky, Babveva in Smyslova, 2000: 57), popularno pa izraz danes opisuje posameznika, ki ima veliko računalniško-tehničnega znanja, to znanje pa izkorišča za napad na računalniške sisteme, kar hekerje uvršča v polje računalniške kriminalitete. Izraz *hekanje* se večinoma uporablja za "*kompleksno mešanico legalnih in nelegalnih aktivnosti, od legitimnega kreativnega programiranja, do prepovedanega vdiranja in manipulacije svetovnih telefonskih ali računalniških sistemov*" (Taylor, 2000: 36); najbolj pogosto pa se ga dojema kot sofisticirano ilegalno dejavnost. Čeprav z izrazom heker danes poljudno označujejo kateregakoli kiberkriminalca, pa Thomas in Loader kiberkriminalce delita v tri kategorije: hekerje in phreakerje (ang. *phreaker*; gre za "telefonske hekerje", ki se ukvarjajo z zlorabo telefonskih sistemov; phreakerji so bili predhodniki hekerjev, formirati pa so se začeli v ZDA konec 70-tih let, v današnjem času jih skorajda ni več), ki vdirajo v sisteme večinoma iz radovednosti in ne povzročajo škode; trgovce z informacijami, katerih glavni motiv je profit; ter teroriste, ekstremiste in deviantneže, ki informacijske sisteme uporabljajo za nezakonite politične

ali družbene dejavnosti (npr. razširjanje sovražnega govora, otroške pornografije, napade na strežnike sovražnih držav itd.) (Thomas, 2000: 6-8).

Obstaja pa še druga delitev, ki kaže, kako se je pojem (in odnos do njega) razvijal skozi čas. Levy pravi, da obstajajo štiri generacije hekerjev, s katerimi se je pojem hekerja spreminjal skozi čas. Prva generacija, ki izvira iz MIT, je v 50-tih in 60-tih letih prejšnjega stoletja razvila prve programske tehnike. Drugo generacijo predstavljajo tisti posamezniki, ki so razvili prve osebne računalnike in s tem omogočili dostop računalniške tehnologije širšim množicam. Tretjo generacijo označujejo vodilni razvijalci računalniških iger. Četrto pa osebe, ki na nedovoljene načine vstopajo v tuje računalnike (Taylor, 2000: 36). Iz te delitve tudi izhaja, da so bili prvotni hekerji predvsem ustvarjalni, zadnja generacija hekerjev pa naj bi bila že v večji ali manjši meri destruktivna. Podobnega mnenja je bil tudi sogovornik Arctus:[1] "*Saj se to ve, kdo so, oz. kdo so bili - pionirji na področju računalništva, in to je to!*" (Arctus, 2006a).

Po samodefiniciji pa se hekerji v hekerskem slovarju (*Jargonfile*) opisujejo kot "*osebe, ki uživajo v raziskovanju računalniških sistemov in iskanju novih načinov njihove uporabe; osebe, ki navdušeno (celo obsedeno) programirajo ... osebe, ki uživajo v intelektualnih izzivih v aktivnem premagovanju in zaobhajanju omejitev*" (MIT, 2003). Eden izmed slovenskih hekerjev, Exceed, je v pogovoru povedal: "*ne razumem zakaj ljudje izraz hekanje vedno povezujejo z vdiranjem in asocialnimi tipi. ta termin ne pomeni nič drugega kot da si zelo dober v neki stvari, pa naj si bo to računalništvo ali kaj drugega. sem menja da je to bolj način razmišljanja, želja po znanju, izziv...*" (Kovačič, 2004a). V enem izmed svojih člankov, v katerem opisuje hekersko tehniko prekoračitve medpomnilnika (ang. *buffer overflow*), je tako zapisal: "*Dokument je posvečen vsem, ki vedo, da sta hekanje in učenje način življenja in ne vsakdanje delo, modna muha ali skupek navodil prebranih v strokovni literaturi*" (Exceed, 2004). Na vprašanje zakaj se ukvarja s hekanjem pa je odgovoril: "*zaradi želje po znanju in izziva*" (Kovačič, 2004a).

Podobnega mnenja, da namreč hekanje ni nujno povezano zgolj z računalništvom, ter da gre za način življenja, je bil tudi sogovornik freejack:

> "*Hacker je oseba, ki rad preučuje vse stvari in to do največje možne mere. Med drugim tudi oz. še posebej na videz nepomembne podrobnosti, v upanju po odkritju 'skritih' posebnosti le te, uporabnost in slabe lastnosti/šibki člen. Npr. možno je 'hackat' knjigo, s tem da se jo uporabi za*

1 Intervjuji z nekaterimi slovenskimi hekerji so bili opravljeni v okviru ciljnega raziskovalnega projekta "*Računalniška/kibernetična kriminaliteta v Sloveniji*"; vodja projekta je bila dr. Nina Peršak, sodelavci P. Gorkič, M. Kovačič in A. Završnik, nosilec pa Inštitut za kriminologijo pri Pravni fakulteti v Ljubljani. Rezultati so bili objavljeni v poročilu z naslovom "*Računalniška/kibernetična kriminaliteta v Sloveniji*", 2006, ki je dostopno na Inštitutu za kriminologijo pri Pravni fakulteti v Ljubljani. Sogovorniki so v pogovorih uporabljali svoja "hekerska imena", oz. svoje vzdevke.

izravnavo mize ali uporabit list oz. njegovo ostrino za rezanje stvari. Smisel tega je, da je bila knjiga uporabljena v nek drug način in ne za branje, ki je njena primarna oz. osnovna uporabnost. Podobno lahko govorimo v zvezi z računalniki, ko je nek del, programske ali strojne opreme, uporabljen v namen, za katerega ni bil primarno zasnovan. Poleg računalnikov in ostalih stvari, se v vsakdanjem življenju pojavlja še izraz 'social hacking'. Z znanjem psihologije, lahko nekdo prepriča človeka, da naredi nekaj, kar mu reče (v mejah normale seveda). Čeprav se sam izraz sicer uporablja redko, se z njim srečamo vsak dan; žene, možje, fantje, punce, učiteljice, ipd. (npr. ti reče sestra; naredi to zame, pa te ne bom zatožila, kot si takrat naredil to in to). Izven konteksta računalniškega sveta, je uporabljen še izraz 'vadding', ki govori o raziskovanju stvari, do katerih povprečen človek sicer nima dostopa; do kleti, podstrešja javnih zgradb, vzdrževalnih tunelov, jaškov dvigala, itd. Včasih se takšne oz. določene dejavnosti v človeku razvijejo in se od definicije 'hacker' odcepijo, ter postanejo nove/druge, npr. 'phreaking'; termin, uporabljen v navezi z 'heckanjem' telefonov oz. telefonskih sistemov ali 'carding', ki v bistvu predstavlja goljufijo s kreditnimi karticami in je nezakonita. Skratka; gre na nagnjenje, ki se izraža tudi zunaj sveta računalništva, vendar ob uporabi istih metod; da odkrije nekaj, kar je navadnemu človeku 'skrito'. ... Oseba, ki jo opišemo z besedo/pojmom 'hacker' je v bistvu željna znanja. Veliko bere, zbira informacije, ne samo določene, ampak vsakršne. Zaradi tega ima znanje, ki je potrebno za npr. vdor v računalniško omrežje, vendar pri tem, za razliko od crackerjev, tudi ostane. Biti hacker ni nekaj kar delaš, ampak je način življenja." (Freejack, 2003).

Podobno razmišlja tudi Arctus: "*Človek, ki je nekoč bil hacker, bo vedno ostal hacker, če ne po svojih dejanjih pa po miselnosti. Ne pozabimo, da se ne dajo 'hackat' samo računalniki. Tudi ljudje, živali in ostali mehanizmi/organizmi imajo svoje ranljivosti (exploits), ki jih lahko človek izkorišča sebi v prid. Je mogoče hacking naravna selekcija, boj za obstanek, boj za prevlado in moč?*" (Arctus, 2004a).

Tudi znani ameriški varnostni strokovnjak in kriptolog Bruce Schneier hekanje razume kot stanje duha, pri čemer pa ta način razmišljanja povsem ločuje od namena uporabe le-tega: "*Heker je nekdo, ki razmišlja izven okvirov. Je nekdo, ki opusti običajno modrost in namesto tega naredi nekaj drugega. Je nekdo, ki gleda na rob in se sprašuje kaj je na oni strani. Je nekdo, ki vidi niz pravil in se sprašuje, kaj se zgodi, če jim ne slediš. Heker je nekdo, ki eksperimentira z omejitvami sistema zaradi intelektualne radovednosti. ... Računalniki so odlično igrišče za hekerje. Računalniki in računalniška omrežja so ogromni zakladi skrivnega znanja. Internet je brezmejna pokrajina neodkritih informacij. Več kot veš, več lahko storiš. ... To je varnostno hekanje: vdiranje v sisteme s pomočjo razmišljanja na drug način. 'Heker' je stanje duha in nabor veščin; kako to uporabiš, pa je drugo vprašanje.*" (Schneier, 2006a).

Vsekakor izraz “hack” ni nujno vezan samo na računalništvo, pač pa se uporablja kot označitev kreativne uporabe nečesa. Eden bolj znanih neračunalniških “hackov” je odprtokodna licenca GNU GPL, ki jo je leta 1989 pripravil Richard Stallman. GPL licenca uporabniku računalniškega programa daje pravico reprodukcije programa pod nekaterimi pogoji, glavni je, da uporabnik skupaj s programom (oziroma na zahtevo) distribuira tudi njegovo programsko kodo, vključno z vsemi lastnimi spremembami in izboljšavami programa. Ta zahteva je znana pod imenom “copyleft” (v nasprotju s “copyright”), avtorskopravno zakonodajo izkorišča za širjenje pravic uporabnikov in ne za njihovo ožanje. Zato se v zvezi s tim. copyleftom govori o tem, da gre v tem primeru za “hack” avtorsko pravne zakonodaje (Wikipedia, 2005), skratka za povsem zakonito, a drugačno rabo od prvotno mišljene.

S samodefinicijo hekerjev se vzpostavlja tudi delitev na tim. “črne” (ang. *black hat*) in “bele” (ang. *white hat*) hekerje. Tim. “beli hekerji” poudarjajo, da spoštujejo določena etična načela, predvsem se izogibajo namernemu povzročanju škode. Eden takšnih, ki se za hobi ukvarja s preganjanjem tistih, katerih namen je predvsem povzročanje škode je v pogovoru povedal: “*Ja pri tem kar počnem jaz se včasih poslužim tudi stvari, ki niso ravno legalne.. ... Če se gre za ddos, potem pač moram nekako priti do vzorca... glede na to, da se gre za veliko okuženih računalnikov, to avtomatsko pomeni da imam na izbiro dooosti slabo zaščitenih mačin. V eno moram vdreti, da si izborim vzorec... to je "nelegalni " del. Vedno pustim sporočilo, da je računalnik okužen, in seveda brišem vzorec..*” (Kovačič, 2006b).
Res pa je, da razlika med tem kaj je zlonamerno povzročanje škode in kaj ne, zunanjemu opazovalcu pogosto ni povsem jasna. Eden glavnih hekerskih idealov je svoboda: svoboda govora, svoboda raziskovanja (kar vključuje tudi reverzni inženiring), svoboda deljenja informacij (“*informacije želijo biti svobodne*”) ter svoboda od oblasti. Exceed je v pogovoru zapisal: “*popolnoma se strinjam s tem sloganom* (s sloganom 'information wants to be free / informacije želijo biti svobodne', m. op.), *kajti če so informacije svobodne potem je tudi družba svobodna*” (Kovačič, 2004a). Podobnega mnenja pa je bil tudi član skupine “Reci NE NATO!”: “*Ja, recimo information must be free. Dokler so na voljo le redkim, so možne zlorabe s strani te manjšine. Zavoljo preprečitve zlorab s strani manjšine bi bilo dobro, da so bolj free*” (Kovačič, 2004b). Seveda pa je govora izključno o informacijah države in korporacij, ne pa tudi o informacijah posameznikov: “*Tukaj bi izpostavil predvsem učinke spama in hackanja. V kolikor so posledice za kogarkoli bistveno škodljive, potem je potrebno zadeve omejiti. V kolikor pa gre za neškodljive zadeve, pa jih je potrebno tolerirati. Problem spama je v drezanju v zasebnost (teženju z motečimi vsebinami, reklamami) in zbiranja podatkov o posameznikih. Zbiranje podatkov o posameznikih je*

potrebno regulirati. Drezanje v zasebnost pa omejiti." (Kovačič, 2004b). Seveda pa je problem v tem, da lahko do škode lahko pride tudi z objavo "državnih" in "korporativnih" informacij:

avtor	*sporočilo*
Matej:	Kaj pa če vdreš v bazo ministrstva za obrambo?
recinenato:	Ja, tukaj je problem pač v tem kateri podatki morajo biti skriti, kateri pa ne. Vendar vseeno. Kako boš te podatke uporabil? Če z njimi ne narediš nič, v redu... ni problema... Če pa jih predaš Al Kajdi, ki nato napade šibke točke Bežigrada, to ni v redu. Mogoče bi bilo najbolje, da so vsi podatki dostopni in bi se raje osredotočili na njihovo (zlo)rabo. Samo to nekako ni pravi način...
recinenato:	Ja kje je meja? Ne vem... če vdreš v banko in sesuješ informacijski sistem, potem to zihr ni dobro. Če pa vdreš v banko in svoji punci, ki dela v banki pošlješ simpatičen pop-up, to ni škodljivo. Seveda, finančni direktor bo mogoče rekel, da je škodljivo, ker uporabljam njihovo infrastrukturo v zasebne namene. Ampak kratek telefonski klic iz službenega telefona se tudi praviloma torelira...

Pogovor s predstavnikom skupine "Reci NE NATO!" (Kovačič, 2004b).

Pri razmišljanju o zlonamernih in dobronamernih hekerjih pa je zanimiv pristop nepodpisanega avtorja razmišljanja v pravni reviji *Harvard Law Review*. Revija je namreč objavila anonimno razmišljanje o varnostnih incidentih na internetu, v katerem avtor ubira povsem nov pristop. Trdi namreč, da bi na računalniška omrežja morali gledati kot na nekakšne organizme z imunskimi sistemi - za katere je značilno, da jih napadi bolezni krepijo. Po mnenju avtorja imajo odkrite in izrabljene varnostne ranljivosti za posledico reakcijo - odpravo teh ranljivosti s strani proizvajalcev ter povišano varnostno kulturo uporabnikov. To po mnenju avtorja krepi "imunski sistem" interneta in zmanjšuje verjetnost, da bi nekoč prišlo do katastrofalnega napada, ki bi lahko ogrozil nacionalno ali celo globalno varnost (Harward Law Review, 2006: 2442). Zaradi tega po njegovem mnenju nekatere oblike kiberkriminala - pa čeprav so zlonamerne - prinašajo več koristi kot stroškov, to pa bi bilo po njegovem mnenju potrebno upoštevati tudi pri obravnavi kiberkriminalnih dejanj (Harward Law Review, 2006: 2442).

Haktivizem

Ni naključje, da so bili hekerji eni prvih razvijalcev prosto dostopnih šifrirnih programov, prostega programja, odprte kode in nasprotniki kakršnekoli oblike cenzure in državne regulacije interneta. Glavni motiv hekerstva sta tako predvsem svoboda in radovednost, ki pa sta v začetku 1990-tih pogosto prerasla v aktivizem. Znano besedilo iz *Hekerskega Manifesta* (gre za besedilo *The Conscience of a Hacker*, ki ga je januarja 1986 v magazinu Phrack objavil heker Loyd Blankenship pod psevdonimom The Mentor) s katerim se sodobni hekerji pogosto identificirajo in ga citirajo, to dobro opisuje: "*Da, sem kriminalec. Moj zločin je radovednost. Moj zločin je, da sodim ljudi po*

tem, kar rečejo in mislijo, ne po tem, kako izgledajo. Moj zločin je, da sem bolj bistroumen kot vi, nekaj, česar mi nikoli ne boste oprostili. / Yes, I am a criminal. My crime is that of curiosity. My crime is that of judging people by what they say and think, not what they look like. My crime is that of outsmarting you, something that you will never forgive me for.".

Ti hekerji (po lastni samodefiniciji naj bi bili to tudi edini pravi hekerji) so zaslužni za razvoj številnih orodij za zaščito zasebnosti, orodij za povečevanje informacijske varnosti, pa tudi za širjenje zavedanja o in obrambe človekovih pravic v kiberprostoru. Nekateri od njih se povezujejo tudi s klasičnimi političnimi aktivisti (npr. s tim. antiglobalisti) in jim brezplačno nudijo tehnično podporo pri vzdrževanju informacijskih servisov ter nelegalnim političnem oz. aktivističnem delovanju na spletu, za kar se uporablja tudi izraz haktivizem (ang. *hacktivism*).

Denningova haktivizem definira kot povezavo med aktivizmom (pri katerem gre za uporabo interneta v namene širjenja informacij, debatiranje, načrtovanje in koordinacijo političnih in družbeno angažiranih aktivnosti, itd., skratka legitimno uporabo, ki ni dekstruktivna) in hekanjem. Po njeni definiciji je haktivizem sicer v osnovi dejavnost povzročanja motenj, ne pa tudi resni škodi. Kot primere navaja virtualno zasedništvo (razobličenja spletnih strani), virtualne blokade (politično ali aktivistično motivirani DOS napadi), pošiljanje poštnih bomb, vdore ter širjenje računalniških virusov in črvov (Denning, 2001: 241). Uporabo hekerskih tehnik v aktivistične a destruktivne namene (npr. povzročanje ekonomske škode ali ogrožanje življenja ljudi) pa Denningova uporablja izraz kiberterorizem (Denning, 2001: 241). Izraz kiberterorizem je sicer sporen, saj so nekateri mnenja, da kiberterorizem kot ena izmed zvrsti terorizma sploh ne obstaja oz. gre za bolj teroretični pojem (npr. Schneier v Beyond Fear (Schneier, 2003: 233-237). Kljub temu sta na internetu znana vsaj dva primera varnostnih incidentov, ki bi ju glede na definicijo Dorothy E. Dennig lahko šteli za kiberterorizem.[2]

Definicija haktivizma, kot ga podaja Denningova, ne vključuje tistih oblik internetnega aktivizma, pri katerih gre za nudenje informacijske podpore političnim aktivistom, oziroma za legalno onemogočanje nadzornih in cenzorskih mehanizmov. Enega izmed takih primerov predstavlja gibanje *Cypherpunk* (izraz izvira iz izraza *cyberpunk* - kiberpank in besede *cipher* - šifra), ki je bilo ustanovljeno leta 1992 na Berkleyski univerzi, njegovi izvori pa sicer segajo že v pozna 80-ta leta 20. stoletja. Cypherpunkerji so zagovarjali individualne svoboščine posameznika nasproti državi v

2 Gre za tim. 911 worm, računalniški virus, ki se je pojavil aprila 2000 in je po uspešni okužbi skušal z modemom klicati na številko za klic v sili (v ZDA je to številka 911) (CERT, 2000). Podoben primer se je zgodil tudi julija 2002, ko je nekdo napisal virus, ki je zamenjal klicne številke uporabnikov storitve WebTV s številko 911 (U.S. Department of Justice, 2004). Lažni klici na številko 911 so motili delovanje reševalnih služb in policije.

virtualnem svetu, ustanovljeni pa so bili z namenom razvijanja programov in sistemov za anonimizacijo na internetu, šifriranje podatkov in sporočil, elektronsko podpisovanje ter anonimni digitalni denar (Hughes, 1993, May, 1988 ter May, 1995). Podobna projekta sta še Hacktivismo[3] in Peekabooty.[4] Na nek način tim. beli hekerji tvorijo jedro civilne družbe na internetu, ki je v veliki meri zaslužna za varovanje digitalnih človekovih pravic. Član skupine "Reci NE NATO!" je zapisal: "*Tehnologija daje moč tistemu, ki ima znanje. Ponavadi je to manjšina. Ta manjšina pa ima lahko dobre ali slabe namene. Ne pozabimo, vladarji so manjšina. Problem sam ni v tehnologiji. Problem je v uporabi tehnologije. Neka manjšina, ki se je po "krivici" ne sliši dovolj s pomočjo tehnologije postane glasnejša. S pomočjo tehnologij je boj med vladajočimi in vladanimi lahko enakovrednejši. Vladani lahko s pomočjo premetenosti izbrskajo marsikatero informacijo, ki je vladajoči neupravičeno ne pustijo v javnost. V takih primerih je hackersko napadanje upravičeno. Določene informacije po krivem niso javne.*" (Kovačič, 2004b).

"Dobronamerni" in "zlonamerni" hekerji

Tim. beli hekerji sami vzpostavljajo distinkcijo do tim. črnih hekerjev, ki jih označujejo z izrazom kreker (ang. *cracker*). To so osebe, ki hekersko znanje zlorabljajo za slabe namene, predvsem nezakonito vdiranje v računalnike s pridobitnimi nameni ter povzročanje škode. Izraz kreker se sicer uporablja tudi za posameznike, ki se ukvarjajo z im. reverznim inženiringom programske opreme, predvsem z namenom razbijanja zaščite programov prek kopiranjem. Ena izmed krekerskih skupin z imenom Wsi.Crk je okrog leto dni delovala tudi v Sloveniji. Skupina se je ukvarjala z razbijanjem zaščit predvsem slovenske programske opreme, za nadaljno distribucijo pa je poskrbela skupina Warez.Si (Arctus, 2006b).

Medijske prezentacije hekerje pogosto predstavljajo kot zlonamerne posameznike in praviloma ne ločujejo med belimi in črnimi hekerji, s čimer pomagajo pri opravičevanju povečanja nadzora in oglaševanju izdelkov za področje informacijske varnosti. Poleg tega se vzpostavlja še distinkcija do skriptarjev (ang. *script kiddie*). To so osebe, ki nimajo pretiranega računalniškega znanja, pač pa za vdore uporabljajo javno dostopna vdiralska orodja, ki so jih razvili drugi. Če so krekerji praviloma visoko motivirani in vdirajo v točno določene sisteme, pa skriptarji navadno ne iščejo točno določenih žrtev, pač pa po internetu povsem naključno iščejo slabo zaščitene računalnike, v katere potem poskušajo vdreti, njihovi motivi pa so večinoma samodokazovanje, zabava ali vandalizem.

3 Hacktivismo je oddelek hekerske skupine *Cult of the Dead Cow* (cDc), katerega namen je boj za prost dostop do informacij in proti cenzuri na internetu. Hacktivismo je bil ustanovljen leta 1999 (Cultdeadcow.com, 2001).

4 Cilj projekta Peekabooty je izdelava orodij za onemogočanje cenzure na internetu. Več o projektu na: <http://www.peek-a-booty.org/>.

Sogovornik *VolkD*[5] je bil mnenja, da je večina tim. skriptarjev prične svojimi aktivnostmi proti koncu osnovne šole, najbolj destruktivni so okrog starosti 16 let, nekje do 18-tega ali 19-tega leta starosti pa s svojimi aktivnostmi prenehajo, oziroma jih prerastejo (Kovačič, 2006b). Kot jih je opisal eden izmed sogovornikov: "*srečujem jih skoraj vsakodnevno na raznih forumih. Mulci, ki mislijo, da bodo oboroženi z Sub7* (gre za znano hekersko orodje oz. trojanskega konja, m. op.) *in XP-ji osvojili svet. Nimajo želje po znanju in si želijo vse instantno. Njihov edini motiv je bahanje*" (Kovačič, 2004a). Tipičen primer za to je tudi naslednji zapis pogovora na IRC-u avtorja "Bl4cky": "*PLISS KDO VE: jaz bi rabo nek virus :D za učitelco da bi ji poslal neki po mailu, pa bi ona to odprla in bi se ji naloil virus in bi jaz lahko pol dostopil do njenih podatkov ? ... rabim test. in ga ima na pcju*" (Božič, 2006). V kontrast takemu razmišljanju lahko postavimo izjavo 16-letnega britanskega študenta Richarda Prycea, znanega tudi kot Datastream Cowboy, ki je leta 1994 vdrl v več visoko zaupnih ameriških vojaških sistemov: "*Nekateri so gledali televizijo po šest ur na dan, jaz pa sem hekal računalnike.*" (Ungoed-Thomas, 1998).

Že njihovi motivi (zabava, vandalizem) ter pomanjkanje znanja ter celo želje po znanju, dajejo slutiti, da je glavni problem skriptarjev predvsem neustrezna oz. napačna motiviranost. Sogovornik *VolkD* temu razmišljanju pritrjuje: "*Najbolj mi je bil pa zanimiv en ddosnet* [prikrito omrežje namenjeno DDOS napadom, m. op.] *od enega 17-let starega fanta z okolice Novega mesta. Ta je imel stvari narejene tako, da je za okužbo uporabil RX-e* [gre za orodje rxBot, m. op.] *, potem jih je pa nadomestil z svojim programom napisanim v delphiju. ddosnet je bil majhen, kake 70 računalnikov. Šel sem tako daleč, da sem prišel do imena in priimka. Poklical, dobil na telefon mamo in izvedel še ostale podatke. Fanta sem zanimiral za povsem druge stvari. Danes piše komercialne programe. Z enim res dobrim programom v delphiju, je zaslužil malo manj kot 1000 EUR.*" (Kovačič, 2006b).

Informacijsko-obveščevalni napadi

Poleg "klasičnega", hekerskega kibekriminala, strokovnjaki v zadnjih letih čedalje pogosteje opozarjajo tudi na problem informacijskih groženj s strani obveščevalnih služb, organiziranih (kiber)kriminalnih skupin ter celo na pojav kiberterorizma.

Nekatere analize kažejo, da se tehnike informacijskega bojevanja pojavljajo že vsaj od konca 80-ih

5 *VolkD*, gre za starejšega gospoda, je bil sredi leta 2004 žrtev DDOS napada (Volkd, 2004). Med reševanjem incidenta se je seznanil s prikritimi omrežji - botneti. Od tedaj naprej se za hobi ukvarja z analizo in uničevanjem prikritih omrežij. Pri tem se včasih posluži tudi nezakonitih metod. Če namreč želi pridobiti tim. "virusni vzorec" prikritega omrežja, mora vdreti v nek okužen računalnik. Kljub temu, da je njegov namen uničevanje nezakonitih prikritih omrežij, pa omenjeno pridobivanje virusnih vzorcev predstavlja kršitev zakonodaje.

let prejšnjega stoletja, ko je skupina nemških hekerjev izvedla več napadov na ameriške vojaške informacijsko komunikacijske sisteme, kasneje pa se je izkazalo, da so pridobljene informacije in znanje posredovali sovjetski tajni službi KGB v Vzhodnem Berlinu. Celoten incident, predvsem pa informacijsko odkrivanje in preiskava hekerskega napada sta podrobno opisana v knjigi *The Cuckoo's Egg* avtorja Cliffa Stolla, ki je izšla leta 1990.

Prav tako omrežno kibernetsko bojevanje postaja del sodobnih nevojaških operacij nekaterih držav. Na to nakazujeta tako primera Severne Koreje, kot tudi Kitajske. Že od leta 1994 vojaški strokovnjaki opozarjajo na Automated Warfare Institute (Mirrim College) v Severni Koreji, kjer naj bi načrtno šolali računalniške strokovnjake z namenom informacijskega bojevanja. Oktobra 2004 je bilo predstavljeno poročilo obrambnega ministra Južne Koreje parlamentarnemu odboru za obrambo, v katerem je navedeno, da naj bi po njihovih obveščevalnih podatkih Severna Koreja v tem času izšolala okrog 600 računalniških strokovnjakov usposobljenih za izvajanje obveščevalnih dejavnosti proti Južni Koreji, Japonski in ZDA. V Južni Koreji so sredi leta 2004 zaznali tudi 211 uspešnih vdorov v računalnike desetih državnih ustanov, med drugim južnokorejskega parlamenta, inštituta za obrambne študije, univerz in zasebnih podjetij, za katere je domnevno odgovorna Severna Koreja (Kovačič, 2006a: 193-194).

Podobni podatki prihajajo tudi iz Kitajske, ki uporablja koncept integriranega omrežno-elektronskega bojevanja (Svete, 2005), v okviru katerega so pričeli vzpostavljati sile kibernetske varnosti, katerih naloga je tudi izvajanje kibernetskih napadov in vzpostavitev vohunskih mrež za delovanje v informacijsko komunikacijskih omrežjih. Posledica novega koncepta je tudi operacija Titan Rain, kjer je šlo za serijo omrežnih napadov na ameriške vladne in poslovne strežnike med leti 2003 in 2005 ter kasneje, in za katerimi je verjetno stala kitajska vojska. Leta 2005 so nekateri varnostni strokovnjaki v ZDA opazili povečano hekersko aktivnost, varnostni strokovnjaki SANS inštituta pa so hekerje uspeli izslediti do računalnikov v kitajski provinci Guandong. Novembra 2005 so neznani napadalci uspešno vdrli v pomembne vojaške računalnike (najprej v U.S. Army Information Systems Engineering Command v Fort Huachuca, nato v Defense Information Systems Agency v Arlingtonu, sledil je napad na Naval Ocean Systems Center v San Diegu ter v sistem U.S. Army Space and Strategic Defense v Huntsvillu). Napadalci naj bi med drugim ukradli programsko opremo za načrtovanje vojaških poletov, uspešno pa so vdrli tudi v različne računalnike nekaterih podjetij, ki pogodbeno sodelujejo z vojsko (Espiner, 2005).

Leta 2006 so neznani hekerji preko (oziroma iz) kitajskih strežnikov vdrli v računalnike ameriškega *Bureau of Industry and Security*, ki je del ameriškega trgovinskega ministrstva in je zadolžen za

izdajo izvoznih dovoljenj za tehnologije dvojne rabe. Proizvajalci tehnologij dvojne rabe, mednje se v ZDA štejejo tudi specializirane kriptografske naprave, morajo namreč temu uradu v postopku prošnje za pridobitev licence predložiti detajlno dokumentacijo o svojem proizvodu. Posledica tega je, da omenjeni urad v svojih sistemih hrani obsežno zbirko občutljivih podatkov o kriptografskih in drugih tehnologijah dvojne rabe, ter zato predstavlja željen cilj napadalcev (Schneier, 2006b)

Tudi novejše analize (Rogin, 2007 in Elegant, 2007) kažejo, da kitajska vojska zelo verjetno načrtno šola računalniške hekerje in načrtno izvaja informacijske napade. V letu 2007 so bili nekoliko bolj medijsko odmevni napadi na računalniške sisteme nemške vlade v maju in napadi na računalniške sisteme ameriškega obrambnega ministrstva v juniju, za katere so se kasneje pojavile špekulacije, da jih je naročila Kitajska vlada, izvedla pa ena izmed hekerskih skupin, ki jih štejejo med tim. kitajsko civilno kiber milico (Hruska, 2008). V decembru je direktor britanske obveščevalne službe MI5 direktorjem 300 večjih britanskih podjetij poslal pismo, v katerem jih je opozoril, da so tarče kitajskih obveščevalnih kibernapadov (Schneier, 2007). Tarče napadov naj bi bila velika gradbena in naftna podjetja, pa tudi odvetniške pisarne in ostala podjetja, ki poslujejo s Kitajsko ali upravljajo s strateško pomembnimi informacijami, v zadnjem času pa tudi aktivisti, ki se zavzemajo za človekove pravice.

V začetku leta 2008 so namreč številni aktivisti za podporo Tibetu in novinarske agencije, ki so poročale o nasilju v Tibetu od neznancev prejela elektronska sporočila v katerih naj bi bile fotografije pobitih tibetanskih protestnikov oziroma druga gradiva, ki naj bi pričala o nasilju kitajske države v Tibetu, v resnici pa so bile datoteke okužene z virusom, ki je na računalnik naložil in zagnal program za prestrezanje tipkanja (tim. *keylogger*), program pa je bil dodatno modificiran, da bi ga protivirusni programi ne zaznali (tim. metamorfni virus) (F-Secure, 2008).

Da so napadi na informacijsko komunikacijske sisteme z razmeroma nizko stopnjo tveganja lahko precej uspešni je v ZDA pokazala tudi vojaška simulacija Operation Eligible Receiver leta 1997, ko je 35 računalniških strokovnjakov National Security Agency uspešno vdrlo v številne vojaške in civilne računalnike, ki so nadzorovali ključne infrastrukturne sisteme.[6] Zato ne preseneča opozorilo nekdanjega direktorja CIE Jamesa R. Woolseya, ki je že leta 2000 opozoril na možen pojav tim. instruktivnih virusov katerih namen bi bila kraja podatkov, spreminjanje vsebine datotek ali elektronsko prisluškovanje (Poulsen, 2000). Da je bilo njegovo opozorilo pred sedmimi leti še kako na mestu pa dokazuje razvoj kasnejših dogodkov na tem področju; v svojem opozorilu decembra

6 Informacija o tej operaciji je dostopna tudi v poročilu, pripravljenem za *Cyber Security Research and Development Act*, ki ga je 4. februarja 2002 v *House of Representatives* podal Boehlert iz odbora za znanost, str. 3–4 (Boehlert, 2002).

2007 je namreč direktor britanske MI5 zatrdil, da kitajski vladni hekerji za vohunjenje uporabljajo posebej napisane trojanske konje ter je predstavnikom podjetij poslal digitalne prstne odtise (kontrolne vsote) teh programov ter IP naslove strežnikov iz katerih se izvajajo napadi.

Haktivizem in kiberterorizem

Nekoliko drugačni, a nič manj nevarni niso niti napadi, ki temeljijo na tim. ljudski informacijski vojni (Svete, 2005: 147) oziroma tim. haktivizmu. Znani so napadi kitajskih in srbskih uporabnikov interneta na strežnike zveze NATO leta 1999, v letu 2007 pa tudi obsežni informacijski napadi, predvsem napadi onemogočanja storitve (DDoS) na estonske vladne in zasebne strežnike, ki so močno ohromili delovanje estonskih vladnih strežnikov, bank, medijskih portalov, itd. in povzročili veliko gospodarsko škodo.

Da so takšni napadi z razmeroma resnimi posledicami mogoči tudi v Sloveniji kaže primer napada z onemogočanjem storitve na DNS strežnike slovenskega ponudnika dostopa do interneta Siol leta 2004. Napadalec je z napadom uspel za več dni resno motiti delovanje največjega slovenskega ponudnika dostopa do interneta. Slovenske spletne strani – predvsem spletne strani medijskih hiš - so sicer že doživele nekaj manjših napadov z onemogočanjem storitve, kar jim je povzročilo večjo gospodarsko škodo.[7]

Nekatera izmed teh ravnanj bi lahko šteli celo za tim. kiberterorizem. Nekateri avtorji, npr. Schneier, so sicer mnenja, da je kiberterorizem bolj teoretični pojem, a nekateri primeri kažejo, da bi bilo mogoče kibernetsko bojevanje nekoč v prihodnosti uporabiti tudi za teroristične namene. Znana sta dva primera varnostnih incidentov v ZDA, kjer je računalniški virus na okuženih sistemih sprožil klice na številko za klic v sili in s tem povzročil preobremenjenost operaterjev in posledično motnje pri delovanju reševalnih služb in policije, ter primer, ko je napad z onemogočanjem (tim. DDoS napad) leta 2003 povzročil motnje v delovanju sistema za vodenje ladij v pristanišču v Hustonu (BBC News, 2003). Istega leta se je zgodil še nekoliko resnejši incident, ko je računalniški črv Slammer za pet ur ohromil nadzorno varnostni sistem jedrske elektrarne v Ohiu (v času incidenta je bila jedrska elektrarna v mirovanju, podvojeni del varnostnega sistema elektrarne pa ni bil ogrožen) (Poulsen, 2003). To kaže na to, da bodo imeli kibernetski napadi v prihodnosti lahko resne posledice tudi v svetu fizične varnosti in ne samo v sferi ekonomije in obrambe.

7 Več o tem v poročilu z naslovom "*Računalniška/kibernetična kriminaliteta v Sloveniji*", 2006, ki je dostopno na Inštitutu za kriminologijo pri Pravni fakulteti v Ljubljani.