



UNIVERZITET SINGIDUNUM

**DEPARTMAN ZA POSTDIPLOMSKE STUDIJE I
MEĐUNARODNU SARADNJU**

MASTER RAD

CYBER KRIMINAL

Mentor:

Doc. dr Gojko Grubor

Kandidat:

Vladimir Ugren 410526/2010

Beograd, 2012.

Apstrakt

U današnje vreme preko dve milijarde ljudi širom planete aktivno koristi usluge internet mreže bilo kada rade, uče u virtuelnim učionicama ,kada koriste usluge telemedicine , međusobno komuniciraju ,zabavljaju se ili obavljaju druge delatnosti,što više ne predstavlja privilegiju pojedinaca već realnost današnje globalizacije i ere informaciono-komunikacionih tehnologija.Ona pruža podjednaku mogućnost i razvijenim i nerazvijenim zemljama da unaprede svoju ekonomiju,obrazovni sistem i mnoge druge aspekte savremenog života.

Ovaj rad je pisan sa željom da pruži celovit uvid u stanje kompjuterskog kriminala – tema koja , s pravom, izaziva sve veću pažnju svetske,a u poslednje vreme i domaće javnosti.Bilo da ste svesni ili ne , kada se od kuće ili sa posla povežete na internet,veoma ste ranjivi.

Abstract

Today more than two billion people worldwide actively use the services of Internet network at any time work, learn in virtual classrooms, when using telemedicine services, communicate with each other, play or other activity, which is no longer the privilege of individuals, but the reality of today's era of globalization and ICT tehnologi.She provides equal opportunity and developed and developing countries to improve their economy, educational system and many other aspects of modern life.

This paper was written with the desire to provide a comprehensive insight into the state computer crime - a topic that, quite rightly, a growing attention of the world, and more recently the domestic public.Any you are aware or not, when you are at home or work to connect internet, you are very vulnerable.

1. Metodologija istraživačkog rada

1.1. Uvodne napomene i obrazloženje rada

Društveni i ekonomski razvoj savremenog čovečanstva u poslednjih nekoliko decenija tesno je vezan ,pa čak i uslovljen , razvojem informacionih tehnologija.Međutim,ta povezanost i oslovljenost nose u sebi značajne rizike i pretnje od zloupotreba,čije posledice mogu dovesti u pitanje najvažnije vrednosti, kako na nacionalnom, tako i na globalnom nivou.Visokotehnološki kriminal zauzima sve značajnije mesto u strukturi savremenog kriminala,a adekvatna i pravovremena socijalna reakcija na tu kategoriju kriminala jeste jedan od bitnih preduslova daljeg razvoja čovečanstva.

Činjenica je da visokotehnološki kriminalitet predstavlja aktuelnu društvenu negativnu pojavu i da se njegovi krivičnopravni oblici i pojavni oblici u praksi Ministarstva unutrašnjih poslova Republike Srbije ispoljavaju kao vidovi savremenog kriminala,uz stalno prisustvo novih oblika.Nema sumnje da živimo u doba tehnologije.Toliko mnogo toga u našoj kulturi zavisno je ne samo od ljudskih aktivnosti i posobnosti ,već i od mašina i mikročipova.Nije ,naravno, potpuno nemoguće živeti bez kola,pokretnih traka (naravno) kompjutera ali , suočimo se s tim – mi to i ne želimo.

Živimo u vremenu ubrzanog razvoja kompjuterske tehnologije kada krivična dela iz oblasti visokotehnološkog kriminala zahvataju sve šire oblasti naših života.Srbija je još na početku sajber kriminala,ali i pored toga u Srbiji se primećuje da se iz godine u godinu poboljšavaju uslovi za sajber kriminal. Napredak ne ide očekivanom brzinom, ali je konstantan, što se posebno može videti po donošenju zakona u toj oblasti, porastu broja web prodavnica, povećanju brzine i internet protoka, porastu broja računara i računarski pismenih ljudi, itd.

1.2 Ciljevi istraživanja

Iz svega do sada rečenog proizlaze sledeći ciljevi istraživanja:

- identifikacija bezbednosnih pretnji u sajber kriminalu;
- analiza direktnih i indirektnih razloga nesigurnosti sajber kriminala;
- identifikovanje glavnih aktuelnih i potencijalnih aktera i načina njihovog delovanja u sajber kriminalu;
- analiza mogućnosti ostvarivanja pretnji ugrožavanja sajber kriminala. Uspostavljanje analitičkog modela za ispitivanje ostvarivosti pretnji u sajber kriminalu;
- identifikovanje materijalnih dobara posebno ugroženih pretnjama u sajber kriminalu;
- analiza potreba za redefinisanjem strategija za odgovor na bezbednosne pretnje u sajber kriminalu.

1.3 Metode istraživanja

Istraživanje je imalo multimetodski karakter i podrazumevalo je kompleksnu analizu dostupnih i novostvorenih izvora podataka. Reč je o dominantno kvalitativnom istraživačkom pristupu i eksploratornoj prirodi uspostavljenih istraživačkih zahteva.Način istraživanja i izbor metoda određeni su definisanim problemom istraživanja, teorijskim i operacionalizovanim

predmetom istraživanja, pretpostavljenom hipotetičkom osnovom i kompleksnošću predmeta istraživanja.

Prethodno definisan predmet istraživanja zahtevao je upotrebu odgovarajućih naučnih metoda kojima su bili obuhvaćeni svi relevantni izvori saznanja. Bezbednosne pretnje sajber kriminalu su složeno polje proučavanja i za njihovu valjanu i obuhvatnu analizu bilo je neophodno koristiti različite metode i teorijska znanja iz više naučnih disciplina.

Zbog kompleksnosti proučavanog fenomena u radu su analizirani podaci iz različitih izvora. Postojeći izvori podataka iz kojih se kreirala bazična iskustvena evidencija su:

- naučni i stručni radovi koji se, posredno ili neposredno, bave problemom bezbednosti u sajber kriminalu i načinima ugrožavanja sajber kriminala;
- analiza naučnih i stručnih istraživačkih projekata iz ove oblasti;
- pozitivnopravni propisi (nacionalni, regionalni i međunarodni);
- institucionalni izvori (statistički izveštaji, dokumenta iz arhiva državnih institucija, evidencije kompanija i drugih organizacija, izveštaji ostalih relevantnih institucija);
- evidencije državnih i međunarodnih tela zaduženih za praćenje visoko-tehnološkog kriminaliteta,

međunarodni dokumenti, konvencije, protokoli, međunarodni ugovori i drugi akti, koji su direktno ili indirektno vezani za problem bezbednosti sajber kriminala. U cilju postizanja što većeg stepena pouzdanosti i obuhvatnosti, ovo istraživanje je obuhvatilo kako analizu različitih izvora podataka, tako i komplementarno korišćenje različitih istraživačkih metoda:

1. pregled naučne i stručne literature
2. analiza pravnih dokumenata
3. komparativni metod
4. metod sekundarne analize
5. metod analize sadržaja

1.4 Hipoteze istraživanja

Republika Srbija u novoj informatičkoj eri, zbog svojih skromnih ekonomskih i edukacionih resursa, ima veoma limitiranu moć uvođenja novih tehnologija, što se odražava na efektivnost i efikasnost poslovnih organizacija.

Zbog malih početnih ulaganja i velikog izvoznog potencijala, poslovanje preko Interneta pruža srpskim građanima priliku da se uz jeftine investicije upuste u započinjanje poslovnog poduhvata ili unapređenje već postojećeg.

1.5 Predmet istraživanja

Predmet istraživanja je perspektiva sajber kriminala u Srbiji, u čijem cilju utvrđivanja će se istraživati: najbitniji informatički resursi koji su esencijalni za odvijanje sajber kriminala, modeli sajber kriminala i realno funkcionisanje sajber kriminala dato kroz studije slučaja.

Sadržaj:

1. UVOD	6
2. POJAM CYBER KRIMINALA.....	7
3. VRSTE CYBER KRIMINALA	9
3.1. Cyber špijunaža	11
3.2. Haking	12
3.3. Cyber sabotaza	13
3.4. Cyber terorizam.....	14
3.5. Cyber ratovanje	14
3.6. Cyber prevare	16
3.7. Krađa Internet usluga	16
3.8. Piratstvo softvera.....	17
3.9. Industrijska špijunaža	18
3.10. Internet aukcije.....	19
3.11. Proizvodnja i distribucija nedozvoljenih i štetnih sadržaja	19
3.12. Nadgledanje E-pošte i praćenje e-konferencija	21
3.13. Prisluškivanje	21
3.14. Spam.....	22
3.15. Phishing.....	23
3.16. Analiza kolačića (cookies)	24
4. PROFIL CYBER KRIMINALCA.....	26
5. STUDIJA SLUČAJA:PRAVNA REGULATIVA CYBER KRIMINALA	28
5.1. ORGANIZACIJA I NADLEŽNOST DRŽAVNIH ORGANA U BORBI PROTIV KOMPJUTERSKOG KRIMINALA.....	30
5.1.1.Posebno tužilaštvo.....	30
5.1.2. Služba za borbu protiv visokotehnološkog kriminala.....	31
5.2.3. Nadležnost i organizacija sudova.....	31
5.2.4. Dosadašnja primena ovih zakona.....	31
5.2. PROPISI REPUBLIKE SRBIJE U OBLASTI KOMPJUTERSKOG KRIMINALITETA.....	32
5.2.1. Krivično materijalno pravo.....	32

5.2.2. Konvencija o visokotehnološkom kriminalu.....	34
6. PIRATI NA MREŽI.....	36
6.1. Ratnici u mreži podataka.....	37
6.2. Odbrana od Američkog kriminala.....	41
6.3. Digitalne slobodne ruke.....	46
7. THE KIDS ARE OUT TO PLAY.....	51
7.1. Good times.....	56
8. ZAKLJUČAK.....	65
Literatura.....	66

1. UVOD

Kompjuter je jedno od najznačajnijih otkrića u istoriji čovečanstva. Od pojave prvog kompjutera, sredinom četrdesetih godina prošlog veka, pa do danas, došlo je do rapidnog širenja upotrebe kompjutera u skoro svim oblastima života i rada, tako da danas nema oblasti ljudske delatnosti u kojoj računari nisu našli svoju primenu. Međutim, prilično je poražavajuća činjenica to što je paralelno sa razvojem kompjuterske tehnologije i njenom dostupnošću širokom krugu korisnika rasla i mogućnost njihove zloupotrebe.

Uporedo sa razvojem i umrežavanjem poverljivih računarskih mreža (RM) u sistem globalne mreže – Internet, rastu i potencijalne pretnje od različitih napada sa interneta, uključujući brojne maliciozne programe, socijalni inženjering i druge napade hakera, krakera, vandala i kompjuterskih terorista. Pojedincu, ili grupi pojedinaca, čija su obeležja: posebnost, sofisticiranost, prodornost, tehnička potkovanost i sl., teško je se suprotstaviti, a još teže ih je zaustaviti. Takvog pojedinca je izuzetno teško otkriti u trenutku kad vrši svoje delovanje, a baš taj trenutak predstavlja najbolji trenutak za njegovo identifikovanje i hvatanje. S druge pak strane, internet koji je toliko ranjiv i nesiguran zbog ogromnog broja korisnika, (na dan 31.12.2000. godine broj korisnika Interneta bio je 360.985.492 ukupne svetske populacije, dok je 31. 03. 2011. godine bilo 2.095.006.005 korisnika Interneta, ili 480,40% više nego 2000. godine),¹ otvorenosti i nereguliranosti predstavlja idealno skrovište različitih tipova kriminalaca. Iako su ranije napadi na RM internet tipa bili pretežno eksterni, novije analize pokazuju da mnogo veće finansijske gubitke i drugu štetu nanose interni napadi. Razlozi su u samoj prirodi mreža internet tipa u sistemu e-poslovanja u kojima interni učesnici nisu samo zaposleni u organizaciji (za koje postoji određen stepen poverenja), već i poslovni partneri, zaposleni u firmama podružnicama, kooperanti, dostavljači, itd., koji iz razloga jednostavnosti korišćenja i povećanja efikasnosti i produktivnosti rada imaju vrlo sličan ako ne i isti pristup RM organizacije kao i interno zaposleni.

Sa syber krimonom problem imaju, kako nerazvijene zemlje i zemlje u tranziciji, tako i zemlje sa razvijenim ekonomijama. Tako je (prema podacima kompanije za računarsku bezbednost Symantec, proizvođač antivirusnog softvera Norton) sajber krimonom u svetu u 2011. godini bio pogođen 431 milion ljudi, uz finansijsku štetu od 114 milijardi dolara, a samo u SAD bilo je više od 74 miliona žrtava sajber kriminala, uz direktne finansijske gubitke od 32 milijarde dolara. Prema navodima u izveštaju Symanteca, više od dve trećine odraslih u svetu koji koriste Internet, ili preciznije 69 odsto njih, bilo je nekad u svom životu žrtva sajber kriminala, što znači da je milion ljudi dnevno pogođeno tim nezakonitim radnjama.²

2. POJAM CYBER KRIMINALA

Od pojave prvih oblika kompjuterskog kriminala do njegovog kakvog-takvog definisanja prošlo je mnogo godina, a odmah zatim pojavio se novi fenomen kriminala - cyber kriminal. Sve učestaliji vidovi i načini zloupotrebe kompjutera podstakli su naučnu i stručnu javnost da se pozabavi ovim oblikom kriminalnog ponašanja. Ipak, ne postoji opšteprihvaćena definicija cyber kriminala. Naime, teškoće u definisanju cyber kriminala proizilaze zbog toga što se radi o relativno novom obliku kriminalnog ponašanja, ali i zbog toga što postoji velika fenomenološka raznovrsnost ove pojave, koja se teško može obuhvatiti jednom definicijom.

Treba razlikovati kompjuterski od cyber kriminala. Kompjuterski kriminal obuhvata zločine počinjene nad računarom, materijalima sadržanim u njemu (softver i podaci) i računar se koristi kao sredstvo ili cilj izvršenja krivičnih dela. On obuhvata kriminalni upad u drugi kompjuterski sistem, krađu kompjuterskih podataka, ili korišćenja on-line sistema za vršenje ili pomoć u izvršenju prevara. Tu spadaju hakerisanje, napad ometanja servisa, neovlašćeno korišćenje podataka i cyber vandalizam. Cyber kriminal opisuje kriminalne aktivnosti koje su počinjene korišćenjem elektronskih komunikacionih medija. U najširem smislu, Cyber kriminal je svaka kriminalna delatnost koja se vrši uz upotrebu računara i računarskih sistema i mreža.³

Razmerama cyber kriminala i opasnostima koje prete od njega bavio se i Deseti kongres Ujedinjenih Nacija koji je bio posvećen Prevenciji od kriminala i tretmanu počinioca aprila 2000. godine, a rezultat toga je dokument koji se naziva "Kriminal vezan za kompjuterske mreže" (*Crime related to computer networks*).⁴

Radna grupa eksperata pod ovim kriminalom podrazumeva "kriminal koji se odnosi na bilo koji oblik kriminala koji se može izvršavati sa kompjuterskim sistemima i mrežama, u kompjuterskim sistemima i mrežama ili protiv kompjuterskih sistema i mreža". To je, u suštini, kriminal koji se odvija u elektronskom okruženju. Ako se pod kompjuterskim sistemom podrazumeva svaki uređaj ili grupa uređaja međusobno povezanih i kojima se vrši automatska obrada podataka (ili bilo kojih drugih funkcija), onda je jasno da bez njih i kompjuterskih mreža nema ovog kriminala. Cyber kriminal je kompleksan, jer on pokriva raznovrsne kriminalne aktivnosti vezane za napade na kompjuterske podatke i sisteme, napade vezane za računare, sadržaje, intelektualnu svojinu i sl.

Evo još nekoliko definicija cyber kriminala koje idu u prilog kompleksnosti ovog pojma:⁵

1. Cyber kriminal ili e-kriminal ili visokotehnološki kriminal obuhvata aktivnosti u kojima su kompjuteri i slični informatički uređaji i kompjuterska mreža *predmet, sredstvo, cilj ili mesto* krivičnog dela.
2. Cyber kriminal predstavlja kriminalne aktivnosti koje uključuju korišćenje informatičke tehnologije za nedozvoljen pristup, oštećenja podataka, oštećenje ili upad u kompjuterske sisteme, elektronsku prevaru, elektronsku krađu...
3. Cyber kriminal je kriminal počinjen na internetu uz korišćenje kompjutera ili sličnog uređaja kao sredstvo ili cilj krivičnog dela.
4. Cyber kriminal je kriminalna aktivnost počinjena uz upotrebu *kompjutera ili* počinjena uz upotrebu *kompjutera ili sličnog sredstva i interneta*. Od ilegalnog preuzimanja muzičkih fajlova do krađe onlajn banaka, identiteta, širenja virusa, itd.

5. Cyber kriminal obuhvata krivična dela u sajber prostoru protiv ličnosti, protiv imovine i protiv države. Sajber kriminal obuhvata: dela u sajber prostoru protiv telekomunikacionih službi, komunikaciju u cilju zločinačkog udruživanja telekomunikacionu pirateriju zločinačkog udruživanja, telekomunikacionu pirateriju, rasturanje materijala neprikladnog sadržaja, pranje novca, elektronski vandalizam, terorizam i telekomunikacije, prevare vezane za elektronsko poslovanje.

U literaturi se mogu uočiti shvatanja po kojima cyber kriminal podrazumeva kriminalne prekršaje koji su stvoreni ili omogućeni razvojem informaciono komunikacione tehnologije (IKT) ili tradicionalni kriminal koji je transformisan upotrebom računara tako da je licima koja vrše istragu neophodno poznavanje računara. Pored dela protiv bezbednosti računarskih podataka obuhvata i tradicionalni kriminal koji je transformisan razvojem IKT (npr. krađa identiteta).⁶ Takvo određenje cyber kriminala ne zadovoljava metodološka pravila definisanja, ne ukazuju na ulogu računarske mreže i druge bitne elemente cyber kriminala.

Kod cyber kriminala kompjuterske mreže pojavljuju se u nekoliko osnovnih uloga,⁷ i to kao:

- 1) Cilj napada – napadaju se servisi, funkcije i sadržaji koji se nalaze na mreži. Krađu se usluge, podaci ili identitet, oštećuju se ili uništavaju delovi ili cela mreža i kompjuterski sistemi, ili se ometaju funkcije njihovog rada. Svakako cilj počinilaca (hakera) je mreža u koju se ubacuju virusi ili crvi, te se vrše kriminalne radnje nanoseći tako velike štete.
- 2) Alat –kriminalci su od pamtiveka koristili razna oružja i oruđa u činjenju kriminalnih dela i tako “prljali” ruke, dok današnji moderni kriminalci ne “prljaju” ruke koristeći kompjutersku mrežu u činjenju svojih kriminalnih dela. Nekada ova upotreba mreže predstavlja potpuno novi alat, dok se u drugim prilikama već postojeći toliko usavršava da ga je teško i prepoznati. Korišćenje ovog novog alata naročito je popularno kod dečije pornografije, zloupotreba intelektualne svojine ili online prodaje nedozvoljene robe (droge, ljudskih organa, dece, oružja i sl.).
- 3) Okruženje - Najčešće okruženje u kome se realizuju napadi služi za prikrivanje kriminalnih radnji, kao što je slučaj sa pedofilima, ali ni drugi sajber kriminalci nisu ništa manje uspešni u korišćenju okruženja.
- 4) Dokaz - kao što se u klasičnom kriminalu pojavljuje nož, otrov, pištolj ili neko drugo sredstvo izvršenja dela, tako se i kompjuterska mreža i IKT koriste u dokaznom postupku za cyber kriminal.

Cyber kriminalu je nesporno priznato “svojstvo” kriminala kao obliku ponašanja koji je protivzakonit, mada su se pored ovog pojavili i drugi termini: Internet kriminal, eKriminal, kriminal visokih tehnologija, mrežni kriminal, i sl.). Ovaj kriminal se svrstava u najizrazitiji oblik transnacionalnog kriminala protiv koga ni borba ne može biti konvencionalna.

Imajući u vidu prethodna sagledavanja pojma cyber kriminala, posebno različitost u pristupima pojedinih autora, zaključujemo da je neophodno imati veoma širok pristup prilikom definisanja ove vrste kriminalnog ponašanja. Naime, jedna sveobuhvatna definicija mora inkorporisati u svojoj strukturi tri bitna elementa: način izvršenja, sredstvo izvršenja i posledicu kriminalnog delovanja. Pod načinom izvršenja se podrazumeva svojevrsna upotreba

kompjuterske tehnologije i informacionih sistema, a kompjuter služi kao osnovno sredstvo za izvršenje krivičnih dela, pri čemu je potrebno da nastupi i određena kažnjiva posledica. U tom smislu, najpotpunija definicija bi bila: ***Cyber kriminal predstavlja oblik kriminalnog ponašanja, kod koga se korišćenje kompjuterske tehnologije i informacionih sistema ispoljava kao način izvršenja krivičnog dela, ili se kompjuter upotrebljava kao sredstvo ili cilj izvršenja, čime se ostvaruje neka u krivično-pravnom smislu relevantna posledica.***⁸

Dakle, bez obzira na postojanje brojnih teškoća u definisanju ovog kriminala, kao i postojanje izraženih tendencija da mu se ne priznaju specifičnosti koje prate kriminal uopšte, ipak je jasno da takvi stavovi ne mogu biti prihvatljivi jer se ne mogu zanemariti ni zastrašujući načini realizacije ovog kriminala, kao ni posledice ovakvog delovanja. Problemi nastaju i zbog novih elemenata za diferenciranje ovog od drugih oblika kriminala, te je otuda posebno važno pitanje koje su to vrste cyber kriminala.

3. VRSTE CYBER KRIMINALA

Još 2000. godine Ujedinjene nacije su na svom Desetom kongresu za suzbijanje kriminala i postupanju prema prestupnicima podelile cyber-kriminal na dve sub-kategorije:

1. Cyber-kriminal u užem smislu – svako nezakonito ponašanje usmereno na elektronske operacije sigurnosti kompjuterskih sistema i podataka koji se u njima obrađuju
2. Cyber-kriminal u širem smislu – svako nezakonito ponašanje vezano za ili u odnosu na kompjuterski sistem i mrežu, uključujući i takav kriminal kakvo je nezakonito posedovanje, nuđenje i distribuiranje informacija preko kompjuterskih sistema i mreža

Istim dokumentom su definisani i konkretni oblici ovog kriminaliteta u skladu sa Preporukom Saveta Evrope i listom OECD-a te u dela cyber kriminala u užem smislu spadaju:

- 1) neautorizovani pristup kompjuterskom sistemu ili mreži kršenjem mera sigurnosti;
- 2) oštećenje kompjuterskih podataka ili programa;
- 3) kompjuterske sabotaze;
- 4) neovlašćeno presretanje komunikacija od i u kompjuterskim sistemima i mrežama;
- 5) kompjuterska špijunaža.

Od dela cyber kriminala u širem smislu najčešće se pojavljuju:

- 1) kompjuterski falsifikati;
- 2) kompjuterske krađe;
- 3) tehničke manipulacije uređajima ili elektronskim komponentama uređaja;
- 4) zloupotrebe sistema plaćanja kao što su manipulacije i krađe elektronskih kreditnih kartica ili korišćenje lažnih šifri u nezakonitim finansijskim aktivnostima.

Evropska konvencija o cyber kriminalu predviđa 4 grupe dela:

- dela protiv poverljivosti, integriteta i dostupnosti kompjuterskih podataka i sistema – njih čine nezakoniti pristup, presretanje, uplitanje u podatke ili sisteme, korišćenje uređaja (proizvodnja, prodaja, uvoz, distribucija), programa, pasvorda;
- dela vezana za kompjutere – kod kojih su falsifikovanje i krađe najtipičniji oblici napada;
- dela vezana za sadržaje – dečija pornografija je najčešći sadržaj koji se pojavljuje u ovoj grupi obuhvatajući posedovanje, distribuciju, transmisiju, čuvanje ili činjenje dostupnim i raspoloživim ovih materijala, njihova proizvodnja radi distribucije i obrada u kompjuterskom sistemu ili na nosiocu podataka;
- dela vezana za kršenje autorskih i srodnih prava obuhvataju reprodukovanje i distribuciju neautorizovanih primeraka dela kompjuterskim sistemima.

U Enciklopediji cyber kriminala⁹ navodi se da FBI i Nacionalni centar za kriminal belih kragnj SAD (*National White Collar Crime Center*) otkrivaju i prate sledeće oblike:

- upade u kompjuterske mreže;
- industrijsku špijunažu;
- softversku pirateriju;
- dečiju pornografiju;
- bombardovanje elektronskom poštom;
- “njuškanje” pasvorda;
- “prerušavanje” jednog računara da elektronski “liči” na drugi kako bi se moglo pristupiti sistemu koji je pod restrikcijama; i
- krađu kreditnih kartica.

Zavisno od tipa počinjenih dela cyber kriminal može biti:

a) Politički, koga čine:

- cyber špijunaža;
- haking;
- cyber sabotaza;
- cyber terorizam;
- cyber ratovanje.

b) Ekonomski:

- cyber prevare;
- haking;
- krađa Internet usluga i vremena;
- piratstvo softvera, mikročipova i baza podataka;
- cyber industrijska špijunaža;
- prevare Internet aukcije (neisporučivanje proizvoda, lažna prezentacija proizvoda, lažna procena, nadgrađivanje cene proizvoda, udruživanje radi postizanja veće cene, trgovina robom sa crnog tržišta, višestruke ličnosti).

c) Proizvodnja i distribucija nedozvoljenih i štetnih sadržaja:

- dečija pornografija;
- pedofilija;
- verske sekte;
- širenje rasističkih, nacističkih i sličnih ideja i stavova;
- zloupotreba žena i dece.
- Manipulacija zabranjenim proizvodima, supstancama i robama:
 - ✓ drogom;
 - ✓ ljudskim organima;
 - ✓ oružjem.

e) Povrede cyber privatnosti:

- nadgledanje e-pošte;
- spam
- phishing
- prisluškivanje
- praćenje e-konferencija
- prikacinjavanje i analiza "cookies".

Jasno je da veliki broj različitih klasifikacija sam po sebi pokazuje raznovrsnost ovih dela i kompleksnost njihovih pojava oblika, ali i različitost kriterijuma koji se koriste.

3.1. Cyber špijunaža

Osnovno obeležje špijunaže je odavanje tajne, a osnovni oblik je saopštavanje, predaja ili činjenje dostupnim poverljivih podataka. Pri tome špijunaža može biti motivisana vojnim, političkim ili ekonomskim razlozima, zbog čega se mnoge zemlje preko svojih tajnih službi angažuju u otkrivanju političkih, vojnih, ekonomskih i službenih tajni drugih zemalja.

Cyber špijunaža je akt ili praksa dobijanja tajne bez odobrenja nosioca informacija (ličnih, osetljivih, vlasničkih ili tajnog karaktera), od pojedinaca, konkurenata, rivala, grupa, vlade i neprijatelja za ličnu ekonomsku, političku ili vojnu prednost koristeći nelegalne metode na internetnu, mrežama ili pojedinačnim računarima.

Cyber špijunaža je metod koji se koristi preko interneta. Za izvođenje cyber špijunaže uglavnom se koriste špijunski programi (RAT, Keylogger,...), trojanski konji (specijalni trojanci napravljeni da špijuniraju korisnika), virusi...

Tokom godina bilo je mnogo slučajeva cyber špijunaže, ali svakako jedan od najvećih je "Shady RAT". Ovu operaciju je otkrila kompanija McAfee u Avgustu 2011. godine. Operacija "Shady RAT" trajala je pet godina i došlo je do krađe intelektualnog vlasništva više od 70 državnih agencija, multinacionalnih korporacija i drugih organizacija iz 14 zemalja.

Ukradeni podaci navodno uključuju i one sa oznakom državne tajne, arhive email prepiski, pregovaračke planove i podatke o novim naftnim i gasnim nalazištima, ugovore i mnogo drugih dokumenata. Tokom petogodišnje kampanje napada, grupa koja stoji iza ovih aktivnosti, prema tvrdnjama McAfee-ja, koristila je malware koji je u nekim slučajevima ostao neprimećen u nekim mrežama dugi niz godina.



Slika 1. Zemlje koje su bile mete napada špijunaže¹⁰

McAfee je podatke izvukao iz upravljačkog servera botnet mreže koji je prikupljao logove sa podacima, koji sežu još u 2006. godinu. Ovakva vrsta pretnje nazivana je APT (Advanced Persistent Threat) zbog svoje sofisticiranosti i prikrivene prirode. Joe Stewart iz kompanije Dell SecureWorks, otkrio je da su napadači za prikrivanje svojih lokacija koristili deset godina star kineski alat "HTran".

3.2. *Haking*

Haking kao pojava postao je stvarni problem tek u poslednjoj deceniji 20 - og veka, naročito usled njegovog naglog razvoja. Haking je takav pristup kompjuterskom ili komunikacionom sistemu za koje ne postoji dozvola njegovog korišćenja. Osnovno obeležje hakinga je narušavanje sistema zaštite i neovlašćeni upadi u tuđe informacione sisteme, što je u klasičnom smislu ekvivalentno upadu u tuđe objekte.

Osnovne karakteristike hakinga su:

- Neautorizovan i brižljivo planiran pristup;
- Nasilan pristup, jer je u pitanju probijanje zaštite sistema;
- Pristup se realizuje kroz upad u sistem, pri čemu se termin "upad" koristi za označavanje raznih metoda i tehnika provaljivanja u sistem;
- Upadi u sistem baziraju se na visokom profesionalnom znanju;
- Mesto upada je po pravilu udaljeno od mesta gde se nalazi napadač;
- Činjenjem hakinga napadač, po pravilu, istovremeno čini i druga dela: špijunažu, prevaru, proneveru, krađu usluga, sabotažu, distribuciju virusa i razne druge manipulacije;
- Haking mogu da čine pojedinci ili grupe.

Haking kao nuspojava omasovljenja računarskih tehnologija i elektronskih sredstava može se podeliti na amaterski (hakovanje vrše amateri) i profesionalni (hakovanje vrše profesionalni kriminalci). Osim ove podele postoji i podela na druge vrste hakinga. Tako da haking može biti i u sledecim slučajevima :

- po nameri : dobronamerni i / ili maliciozni (štetni);
- po cilju: čitanje, uništenje, menjanje, distribuiranje, fabrikovanje podataka, ostavljanje poruka, startovanje programa bez dozvole, brisanje ili ispravljanje programa i podataka;
- po počiniocima: pojedinačni i / ili grupe;
- po mestu odakle je napad krenuo: eksterni i interni;
- po realizovanju od strane grupe: organizovani i / ili stihijski.

U skorije vreme brojni su hakerski napadi grupe Anonimni (Anonymous). Ovu grupu čine hakeri širom sveta i smatra se najbrojnijom hakerskom grupom. Serija njihovih najpoznatijih napada započela je napadom na Sagentološku crkvu, a zatim su se na listi našle vlade Egipta i Irana, potom kompanije u vlasništvu konzervativnih aktivista i milijardera Čarlsa i Dejvida Koha. U znak odmazde zbog saradnje sa FBI na identifikaciji članova grupe, Anonimni su napali i kompaniju HBGary Federal. U jeku kampanje koju su američke vlasti vodile protiv WikiLeaks-a, Anonimni su pokrenuli operaciju odmazde usmerenu protiv kompanija PayPal, Visa i MasterCard koje su pritiskute zahtevima američkih vlasti prekinule saradnju sa WikiLeaks-om i obustavile transfer finansijskih donacija na račun WikiLeaks-a. Grupa je preuzela odgovornost za napad na nekoliko sajtova kompanije Sony u aprilu koji su usledili kao odgovor za izvođenje pred sud nekolicine PlayStation 3 hakera. Anonimni su osporili optužbe kompanije Sony za kasniji napad na PlayStation Networks i Sony Online Entertainment i upad u bazu podataka za koji je kompanija optužila ovu grupu, priznavši samo učešće u početnim DDoS napadima. Hakerska grupa Anonimni je u Julu 2011. godine hakovala kompjutersku mrežu vojne alijanse NATO i domogla se oko gigajbta poverljivih podataka, zatim u oktobru 2011. godine članovi hakerske zajednice Anonimni preuzeli su odgovornost za napad na više od 40 tajnih veb sajtova sa dečijom pornografijom i objavljivanje imena više od 1500 članova jednog od hakovanih pornografskih sajtova.

3.3. *Cyber sabotaža*

Sabotaža je prikriveno i podmuklo delovanje, čime se nanosi šteta drugima, a cyber sabotaža podrazumeva uništenje ili oštećenje kompjutera i drugih uređaja za obradu podataka u okviru kompjuterskih sistema, ili brisanje, menjanje, odnosno sprečavanje korišćenja informacija sadržanih u memoriji informatičkih uređaja. Najčešći vidovi cyber sabotaže su oni koji deluju destruktivno na operativno-informativne mehanizme i korisničke programe, pre svega, one koji imaju funkciju čuvanja podataka. To se najčešće realizuje korišćenjem standardnih uslužnih programa, sopstvenih programa ili korišćenjem tehnika kao što su logička bomba, trojanci, sporedna vrata ili virusi. Saboteri mogu imati različite motive, koji mogu biti političkog, ekonomskog, vojnog službenog ili privatnog karaktera.

Pokušaj da se aktivno preduhitre sve veći upadi kompjuterskih provalnika - hakera u važne kompjuterske sisteme, administrativne, korporacijske i vojne jeste i nova cyber-strategija SAD, koja, između ostalog, hakerski napad na kompjuterske sisteme u SAD smatra činom rata, zbog čega će Pentagon biti spreman da po potrebi uzvrat i tradicionalnom vojnom silom.

Ovo je svakako u funkciji upozorenja, jer se polazi od osnovanog uverenja da veliki hakerski napadi na ključne kompjuterske sisteme nisu mogući bez neke vrste institucionalne podrške država iz kojih ti upadi dolaze. Čak i u slučaju da hakeri nisu deo ratne mašinerije neke države, ona će, ako napad dolazi sa njene teritorije, biti proglašena odgovornom na sličan način kao što bi bila odgovorna ako bi sa njenog tla bio organizovan neki teroristički napad. Paralela je utočište koje je talibanski režim u Avganistanu pružao "Al-Kaidi", što je bio razlog za američku intervenciju i okupaciju ove zemlje poslije terorističke diverzije od 11. septembra 2001.

3.4. Cyber terorizam

Sajber terorizam obično podrazumeva napade na kompjuterske sisteme ili mreže iz kojih stoje neki politički ciljevi. Često su namenjeni za zastrašivanje vlade ili građana neke države ili izazivanje ekonomskog gubitka. Pod sajber terorizmom podrazumevaju se i fizički napadi i uništavanje važnih kompjuterskih sistema i infrastruktura.

Postoje tri osnovna načina na koja teroristi mogu da koriste računare za koordinisanje, planiranje i izvršavanje svojih aktivnosti u ostvarivanju svojih ciljeva:

1. Korišćenje računara kao alata. Terorističke grupe koriste internet za propagiranje svojih ideja preko web sajtova i prikupljanje finansijskih sredstava, obično u vidu dobrotvornih priloga, kao i prikupljanje i razmenu obaveštajnih podataka,
2. Teroristi mogu da koriste računare u planiranju i organizovanju svojih programa rada. Oni u računarima drže svoje finansijske knjige, terorističke planove, potencijalne ciljeve, dnevnike prismothe, planove napada...
3. Cyber-teroristi mogu da koriste računare za neovlašćen pristup vladinim i privatnim informacionim sistemima u cilju izazivanja ozbiljnih, čak i katastrofalnih posledica.

Razvojem računarske tehnologije, terorističke organizacije su dobile novo oružje za ostvarivanje svojih ciljeva. Terorističke grupe koriste računare i Internet za širenje svojih ideja. Oni koriste veb sajtove za regrutovanje novih članova kao i za prikupljanje sredstava. Kriminalci čak pomoću svojih tehničkih veština kradu informacije sa kreditnih kartica, kako bi finansirali terorističke aktivnosti. Vrlo je teško boriti se protiv sajber terorizma, jer novi, napredni alati za sajber kriminal onemogućavaju identifikaciju terorista tokom njihovih napada.

3.5. Cyber ratovanje

Cyber ratovanje je podvrsta informacionog ratovanja, koja se odvija u cyber prostoru.¹¹ Na cyber prostor može uticati bilo koja grupa koja poseduje računare koji se mogu povezati u postojeće računarske mreže. Internet napadi neke grupe mogu biti usmereni na namerno ubacivanje dezinformacija na neke internet forume, enciklopedije, blogove i web stranice sličnog karaktera ili mogu biti strogo usmereni prema mrežnoj sabotaži tj. internet terorizmu.

Objekat cyber napada mogu da budu informacioni resursi, odnosno njihov potencijalni cilj može da bude sve što povezuju, pokreću i opslužuju kompjuteri: vojni kompjuterski sistemi, sistemi državne uprave, sistemi za kontrolu vazdušnog i železničkog saobraćaja, sistemi za snabdevanje gasom, vodom i električnom energijom i slično. S obzirom na to koliko takvih sistema ima, posebno u informaciono razvijenim zemljama, za koje i kakve funkcije se koriste i kolika je njihova osetljivost na poremećaje i destrukciju činjenica je da informacioni ambijent nudi teroristima pravo bogatstvo izbora veoma atraktivnih i visoko vrednih ciljeva.

Nekada je cyber ratovanje podrazumevalo samo međusobno bockanje „zaraćenih” država: testirali su se kapacitet, procenjivala se infrastruktura, tražile su se sigurnosne rupe. Sa većom integracijom ključnih sistema za upravljanje (ekonomskih, vojnih, komunikacionih) stvorili su se uslovi i za pravi cyber rat.

¹¹ Cyber prostor prvi spominje William Gibson 1984. godine u svojoj naučno fantastičnoj noveli. Postoji više definicija cyber prostora. Jones Telecommunication & Multimedia Encyclopedia - "Cyber prostor je vrsta "zajednice" sačinjene od mreže kompjutera u kojoj se elementi tradicionalnog društva nalaze u obliku bajtova i bitova."

Iako razmere ovog nevidljivog sukoba nisu poznate, jasno je da su najistaknutiji akteri Amerika i Kina. To nije samo digitalni rat dve države, već su u sukob uvučene i najveće svetske internet kompanije kao što su Facebook, Google,...

Dublji sloj ovih sukoba daleko je od očiju javnosti. Ciljevi su poznati, ali sofisticirane tehnike koje se razvijaju drže se u tajnosti. Američki Pentagon ulaže ogromna finansijska sredstva ne samo u cilju razvijanja defanzivnog štita protiv hakerskih napada već i za razvoj ofanzivnih tehnika.

Predsednik Amerika Barak Obama dao je smernice za cyber ratovanje. Te smernice daju dozvolu vojsci Sjedinjenih Američkih Država da šalje neku vrstu koda kroz protivničku državnu mrežu kako bi se verifikovalo da konekcija sa ključnom infrastrukturom, koja bi bila napadnuta prema potrebi, funkcioniše. Kôd bi mogao da ima i pasivnu funkciju koja bi se aktivirala u slučaju (*cyber*) rata. Pentagon je solidan deo budžeta za cyber ratovanje potrošio na razvoj kompleksne simulacije Interneta koja ispunjava sve neophodne infrastrukturne (civilne i vojne) uslove da bi bila realna. Tu se testira novo oružje, ali i sva moguća scenarija, od moćnog hakerskog napada na Ameriku do prekida pristupa svetskoj mreži.

U toku prve polovine 2011. Godine uhakovani su Međunarodni monetarni fond, Gmail nalozi Obaminih saradnika, infrastruktura Bele kuće (koja nije bila kritična), kao i veliki broj najjačih američkih korporacija. Kineska vojska hakera smeštena je u gradu Jinan (400 km od Pekinga). Poznato je da su u maju 2011. godine uhakovani i sistemi sedišta EU u Briselu, serveri vlade Južne Koreje, kao i francusko ministarstvo finansija. Naravno, ne može se svaki napad sa sigurnošću pripisati Kinezima, ali se ocenjuje da postoji nivo sofisticiranosti koji je moguć samo pod režijom država, a nikako pojedinaca ili hakerskih grupa.

Potaknut eskalacijom državnog cyber ratovanja i stvaranja cyber vojnih jedinica na svim stranama svijeta, NATO je na seriji konferencija ili summita tokom 2010. godine objavio da menja svoj obrambeni fokus sa klasičnog ratovanja prema cyber ratovanju jer opasnost više ne preti od tradicionalnih neprijatelja u meri u kojoj preti od novih napada koristeći internet tehnologije. Ovim se stvorio potencijal da se ravnoteža sa cyber kriminala prebaci na cyber ratovanje i da metode koje su u prošlosti korištene od strane kriminalnih organizacija postanu okosnica nove vojne doktrine u kojoj će svi napadati sve bez vidljivih žrtava takvog tipa ratovanja

Rast broja i značaja pretnji u sajber prostoru naterao je veliki broj država da oformi posebne jedinice i tela za njihovo predupređivanje, a neke su formirale i komande za sajber ratovanje. Tako se i Francuska, nakon nekoliko zapadnih država, ali i vojne alijanse NATO, odlučila da pri Generalštabu Francuske vojske formira komandu za sajber ratovanje.

Sredinom 2010. godine je javno objavljeno postojanje računarskog „crva“ nazvanog Stuxnet koji napada određene softverske sisteme u industrijskim postrojenjima. Ovaj veoma sofisticirani virus napao je najmanje 5 postrojenja u Iranu, sa najverovatnijim ciljem da praktično uništi proces obogaćivanja uranijuma. Eksperti su procenili da je razvoj Stuxneta verovatno najkompleksniji i najskuplji napor u istoriji razvoja malware softvera. Zbog toga su odmah mnogi posumnjali da iza svega stoji neka od država protivnika. Naravno, zabeleženi su i brojni odgovori Irana u vidu različitih napada i pokušaja obaranja sistema u mnogim državama Zapada.

3.6. Cyber prevare

Cyber prevara se odnosi na bilo koju prevaru pri čijem izvršenju se lice koje u nameri pribavljanja protivpravne imovinske koristi za sebe ili drugoga iskoristi jednu ili više komponenti Interneta kao što su chat rooms (sobe za caskanje) , veb stranice (Web sites) , elektronska pošta (e-mail) da bi se stvorili uslovi za lažno prikazivanje ili prikrivanje činjenica kojim bi se neko lice dovelo u zabludu ili u njoj održavalo, da bi to lice učinilo nešto na štetu svoje ili tuđe imovine tako što bi na primer sprovelo neko finansijsku transakciju ili prenelo neke podatke nekoj finansijskoj instituciji koja je meta napada.¹²

Broj oblika prevara, kao i način njihove realizacije je praktično neograničen i u praksi se susreću kako one vrlo primitivne i grube, tako i one prevare kod kojih učinioci ispoljavaju veliki stepen veštine i rafiniranost. Ono što karakterise cyber prevare ja da one daleko dopiru zbog veličine Interneta kao tržišta, da se brzo šire jer sa Internetom kao medijem sve se dešava mnogo brže, i niski troškovi izvođenja ovakvih vrsta prevara .

Cyber prevaranti zloupotrebljavaju upravo one karakteristike Cyber-prostora koje doprinose rastu elektronske trgovine: anonimnost, distanca između prodavca i kupca i trenutna priroda transakcija. Uz to, oni koriste prednost činjenice da prevara preko Interneta ne zahteva pristup do nekog sistema za isplatu, kao što to zahteva svaka druga vrsta prevara i sto je digitalno tržište jos uvek nedovoljno uredjeno i kao takvo konfuzno za potrošače, sto za njih predstavlja skoro idealne uslove za prevaru.

Najpoznatija prevara je naravno Nigerijska prevara. Po istraživanju holandske agencije Ultrascan koja se već gotovo dvije decenije bavi istragama i analizom internet prevara, nigerijska email prevara je u toku 2009. godine u Hrvatskoj odnela gotovo milion dolara, a preko milion dolara u Srbiji i Crnoj Gori za isti period, dok su širom sveta prevaranti napravili zapanjujući profit od 9.3 milijarde dolara samo u prošloj godini.¹³

Sredinom 2011. Godine u Rumuniji je uhapšeno oko 90 ljudi zbog internet prevare. Oni su od 2009. Godine do 2011. godine varali ljude koji su hteli da kupe automobile preko sajtova eBay i Craigslist, tako što su davali lažne oglase na tim sajtovima. Prevare su se dešavale najčešće u SAD. Novac koji su građani uplaćivali slan je u Rumuniju. Prevareno je oko 1000 građana, a prevaratni su ostvarili dobit od oko 20 miliona dolara.

3.7. Krađa Internet usluga

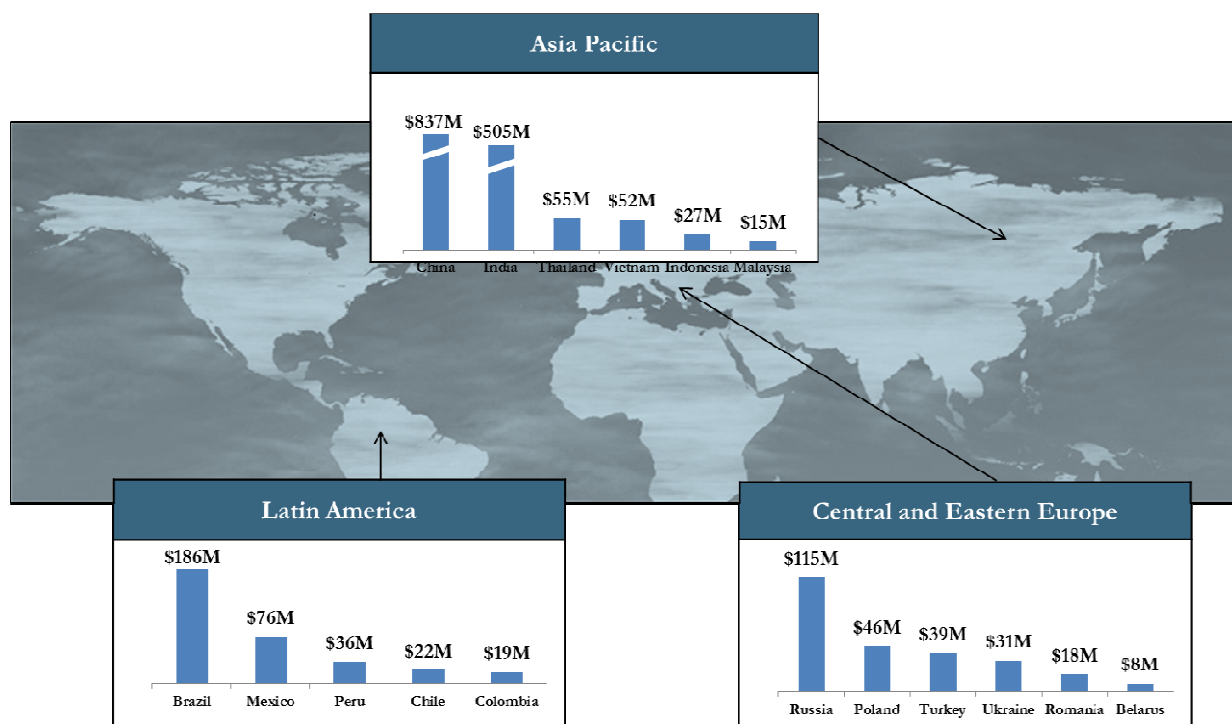
Krađa računarskih usluga, odnosno neovlašćeno korišćenje sistema, je veoma rasprostranjena pojava u oblasti informacione tehnologije, a cilj joj je da se za obavljanje privatnih poslova koriste tuđi računarski resursi.¹⁴

Ozbiljne pretnje dolaze od strane hakera, čije su česte mete računarski sistemi telefonskih kompanija. Upadom u ove sisteme hakeri, između ostalog, obezbeđuju besplatno korišćenje telefonskih usluga za pristup drugim računarima širom sveta. U novije vreme brojni su napadi na kućne bežične mreže. Mnogi koriste internet usluge od drugog pretplatnika tako da on nije svestan toga. Na internetu se mogu naći razni tutorijali kako izvesti ovaj napad i on ne zahteva veliko tehničko znanje.

3.8. Piratstvo softvera

Piratstvo softvera je korišćenje ili umnožavanje i distribucija softvera i programa koji nisu nabavljeni na legalan način. Tu se podrazumeva da pojedinci ilegalno kopiraju koriste ili preprodaju tuđe softvere. Softver može biti ekstremno vredan pri čemu onaj ko ima softver polaže ili podrazumeva izvesna vlasnička prava koja se ne razlikuju od prava na druge vrste dobara. Ilegalno kopiranje softvera je akt koji lišava vlasnika određenih legalnih prava, jer svaka ilegalna kopija ima potencijal lišavanja zakonitog vlasnika određene dobiti ili drugih pogodnosti koje je mogao ostvariti da ilegalna kopija nije bila napravljena.¹⁵

Microsoft je objavio rezultate Prve istraživačke studije o finansijskim učincima korišćenja piratskog softvera u okviru konkurentskog okruženja zemalja u razvoju. Kao podrška obeležavanju Play Fair Day, koji predstavlja globalnu inicijativu za promovisanje značaja korišćenja licenciranog softvera, ova studija potvrđuje štetu koju piratski softver prouzrokuje kompanijama koje se odluče na fer poslovanje.



Slika 2. Gubitak kompanija po zemljama koje rade po propisima zbog piratstva¹⁶

Microsoft istraživanje je pokazalo da je nezakonito poslovanje putem korišćenja piratskog softvera kreiralo neverovatnih 3 milijarde američkih dolara gubitaka godišnje među proizvođačima u Latinskoj Americi, Centralnoj i istočnoj Evropi i regionu Azijskog pacifika. U pojedinačnim zemljama Microsoft je bio u mogućnosti da odredi tačne gubitke među konkurentnim proizvođačima, pa je ta brojka u Brazilu 278 miliona USD, Rusiji 92 miliona USD, Indiji 344 miliona USD i Kini 863 miliona USD.

3.9. *Industrijska špijunaža*

U vreme velike konkurencije i stalnih inovacija, posedovanje prave informacije u pravo vreme osigurava kompaniji vodeći položaj na tržištu i stvara održivu konkurentsku prednost. Otvara se i mogućnost stvaranja velike baze podataka sa ciljem održavanja i povećavanja tržišnog učešća, kao i profita. Bitno je u pravo vreme otkriti šta konkurenti rade i šta nameravaju raditi. U tu svrhu pribegava se industrijskoj špijunaži. Razlog je jednostavan. Ekonomska špijunaža iziskuje mnogo manje troškove nego što je potrebno za ulaganje u sektor istraživanja i razvoja, štedi na angažovanju specijalizovanih stručnih kadrova i smanjuje tehnološki jaz u odnosu na konkurenciju. Ekonomska industrijska špijunaža predstavlja skup dobro planiranih i veoma stručno izvedenih aktivnosti u cilju pribavljanja poverljivih ekonomskih informacija, koje su od koristi za poslovne projekte firme ili zaštitu ekonomskih interesa svoje države.

Metode dobijanja informacija privatnog i komercijalnog tipa mogu se klasifikovati prema mogućim kanalima oticanja informacija:

- Akustička kontrola prostorije, automobila, neposredno čoveka;
- Kontrola i prisluškivanje telefonskih veza, preuzimanje faks-veze i modemske veze, mobilne i radioveze;
- Preuzimanje kompjuterske informacije, uključujući i radiozračenje kompjutera, nesankcionisano ulaženje u baze podataka i slično;
- Tajno fotografisanje i snimanje, specijalna optika;
- Vizuelno praćenje objekta;
- Nesankcionisano dobijanje informacija o ličnosti putem potkupljivanja ili ucene službenika odgovarajućih službi;
- Potkupljivanje ili ucenjivanje saradnika, poznanika, službenika ili rođaka, upoznatih sa prirodom posla;

Industrijska špijunaža često obuhvata tehnologiju ili robu koja ima i civilnu i vojnu primenu. Zbog bezbednosnih razloga, američke obaveštajne službe kontrolišu izvoz osetljive tehnologije pojedinim zemalja. Zbog toga mnoge američke kompanije moraju biti vrlo pažljive i štititi se od špijunaže, dok pokušavaju plasirati svoju robu i probiti se na nova tržišta. Između ostalog, posebna opasnost vrebava od insajdera, koji su spremni da prodaju poslovne tajne kompanije drugima. Takođe veliku opasnost predstavlja internet i njegova upotreba bez adekvatnih zaštitnih softvera u okviru preduzeća.

Metode i postupci industrijske špijunaže su na primer: "trojanski konj", izdaja, provala, korupcija, krađa industrijske tajne, prisluškivanje razgovora i telefonskih i drugih komunikacija i slično. Postoje takođe i neopreznosti u području bezbednosti industrijske tajne koje dovode do njenog otkrivanja (površnost kadrova, otkrivanje tajne neoprezom, komercijalna hvalisavost, tehničke konferencije i savjetovanja i sl.). Da bi se zaštitile poslovne tajne, poduzimaju se, pored postojećih zakonskih propisa i mera, posebne bezbednosne aktivnosti. Donose se sigurnosni programi koji su preventivno usmereni na sve moguće krizne tačke, o čemu brinu menadžeri bezbednosti.

3.10. Internet aukcije

Aukcijske prevare na internetu danas su jedne od najučestalijih prevara izvršenih preko interneta. Aukcija je proces kupovine i prodaje raznih stvari po principu ko da više (licitacija) gde ponuđač najviše cene dobija. Danas je Internet preuzeo proces aukcija u pravom smislu te reči.

Online aukcije su se pokazale kao vrlo unosan posao. Mnogi žive tako što kupuju i prodaju preko online aukcija. Milioni online aukcija dešavaju se svakodnevno i na njime se širom sveta nudi najraznovrsnija roba. Prodavci imaju svoj kutak koji mogu da posete milioni ljudi, a kupci imaju mogućnost da nabave sve što im je potrebno. Online aukcije pružaju mnogima mogućnost izvršenja najraznovrsnijih prevara. Ove aukcije uključuju prevare kao što su neisporučivanje robe, lažno predstavljanje, prodaju robe sa crnog tržišta i dr. Najpoznatiji aukcijski sajt u svetu je eBay.com, dok je kod nas limundo.rs.

3.11. Proizvodnja i distribucija nedozvoljenih i štetnih sadržaja

U ovu grupu sajber kriminala spadaju dečija pornografija, pedofilija, verske sekte, širenje rasističkih, nacističkih i sličnih ideja i stavova, zloupotreba žena i dece, manipulacija zabranjenim proizvodima, supstancama i robom (droga, ljudski organi, oružje).

Dečja pornografija je posledica eksploatacije, ili seksualnog zlostavljanja dece (osobe ispod 18 godina starosti). Može se definisati kao bilo koji vid prikazivanja, ili promovisanja seksualnog zlostavljanja dece, uključujući i pisane i audio zapise, koji se odnose na seksualne odnose sa decom, ili drugi vid seksualnog iskorišćavanja dece.¹⁷ Dečja pornografija je među najrasprostranjenijim vidovima kriminala na internetu. Dečju pornografiju šire pedofili radi pravljenja lične kolekcije, razmene materijala sa ostalim pedofilima, ili pravljenja novog materijala i dečije prostitucije.

Pedofilija je osećanje seksualne privlačnosti prema deci istog, suprotnog, ili oba pola. Pedofilija spada u najčešći oblik poremećaja ličnosti. Može biti heteroseksualna (dva puta češća) i homoseksualna. Heteroseksualni pedofili biraju djevojčice od 8 do 10 godina, dok homoseksualni pedofil bira stariji uzrast. Seksualno zlostavljanje dece predstavlja bilo koji vid eksploatacije djece mlađe od 16 godina u cilju seksualnog zadovoljavanja starije osobe.

U široj upotrebi, termin *pedofil* se najčešće koristi da opiše počinioca seksualne zloupotrebe deteta, mada statistika pokazuje da počinioci ne moraju nužno biti pedofili, niti da svaki pedofil zlostavlja decu. Takođe, postoje mnogobrojna uvrežena pogrešna mišljenja vezana za ovu pojavu. Među najčešća spadaju – da su zlostavljači uglavnom homoseksualni muškarci, da žene ne zlostavljaju decu, da je verovatnije da je dete žrtva njemu nepoznate osobe – kao i da je to nešto što se dešava negde drugde, a ne i kod nas.

Podaci o zlostavljanju dece su vrlo nesigurni, jer mnogi slučajevi ostaju neprijavljeni i nezabeleženi. Smatra se da čak 90 procenata dece koje je doživelo neku vrstu zloupotrebe nikad ne priča o svom iskustvu, bilo iz osećaja stida, ili iz straha za svoj ili život najbližih (često je slučaj da zlostavljač preti i zastrašuje dete, da bi ga sprečio da obelodani zlostavljanje).

U toku 2010. i 2011. godine policija je u akciji nazvanom "Armagedon" privela oko 45 osoba osumnjičenih za pedofiliju i posedovanje materijala sa sadržajem dečije pornografije.

Profil pedofila u Srbiji prilično je uopšten, te među privođenima i uhapšenima ima prosvetnih radnika, diplomiranih pravnika, sveštenika, fizičkih radnika, biznismena, novinara, lekara, nezaposlenih. Policijska akcija "Armagedon" je usmerena ka suzbijanju dečje pornografije koja se distribuira putem interneta i ima međunarodni karakter.¹⁸

Pored pornografske industrije, **sekte** čine jednu od najaktivnijih grupa na internetu. Reč „sekta” potiče od latinske reči „sequi”, što znači slediti. Sekta je manje organizovana religijska grupa predanih vernika, koja obično nastaje iz protesta protiv onoga u šta se pretvorila crkva. Za sve članove sekte karakteristično je da imaju čvrstu organizaciju i jedinstvene obavezne rituale. To su grupe koje se mogu prepoznati po svojoj manipulaciji usmerenoj na psihološku destabilizaciju svojih sledbenika, s ciljem da se od njih izvuče potpuna potčinjenost, smanjenje kritičkog duha, prekid sa opšte usvojenim porukama i koje sa sobom povlače opasnost za individualne slobode, zdravlje, obrazovanje, demokratske institucije. Život u sekti podrazumeva čvrstu identifikaciju sa grupom i vođom (telom i dušom).

Novi religijski pokreti-sekte, širom sveta, kroz zloupotrebu verskih prava i sloboda, šire paukovu mrežu u lovu na ljudske duše u koju se zapliće sve veći broj lakovernih. Verske sekte novog doba, nisu samo, kao što definicija kaže jeretički pravci izdvojeni od matice religije, nego i komercijalno-profitabilne organizacije, grupe sa političkim, pseudo-naučnim i psihoterapeutskim, kriminalnim pa i vojnim pretenzijama. Sektama se više ne bave samo mesne, matične verske zajednice, nego i zdravstveni radnici, pedagozi, pripadnici organa bezbednosti, sociolozi...

Delovanje sekti je raznovrsno, a kreće se od magijskih i proročkih sajtova do sajtova satanističkih organizacija. Nekoliko sajtova organizacija koje zvanično deluju kao sekte u svetu imaju krajnje kvalitetne materijale na svojim sajtovima i tehnički veoma dobro postavljene sajtove. Svako ko želi, lako će naći put u "bolji život". Na njihovim sajtovima su postavljeni edukativni materijali, E-mail liste, kalendari aktivnosti, sugestivne slike i slike sa "magijskim" značenjima za wallpaper, E-mail, štampu... Sekte očekuju mnogo od Interneta - i dobijaju. Članstvo na njihovim sajtovima je slobodno, za uzvrat će žrtva širiti spoznaju o postojanju i svevišnjem.¹⁹

Internet pruža izvanredne mogućnosti da se preko njega sprovede raznovrsne **propagandne aktivnosti sa negativnim predznakom**. Omogućava se najrazličitijim političkim, verskim, rasističkim, nacionalističkim, pa i terorističkim pojedincima, grupama, organizacijama i pokretima širom sveta da svoje poruke šalju preko cele planete. Ove aktivnosti se mogu realizovati preko sopstvenih web sajtova ili slanjem neželjene e-pošte.

Na internetu se takođe događa **manipulacija zabrenjenih proizvoda** što se većinom odnosi na alkohol, droge, oružje i ostale stvari koje su štetne a većina njih su zakonom zabranjene. Slike nasilja i ljudi s drogom u ruci se mogu svakodnevno naći na internetu pa su tako dostupne svima, naročito mladima na koje to ima negativan uticaj. Delimično zbog toga mladi dolaze u situaciju da probaju drogu, alkohol i druge stvari koje su zakonom zabranjene. Često na internetnu mogu pronaći i nelegalne trgovine ljudskim organima. Može se videti koliko koji organ košta. Ljudi koji imaju finansijske probleme veoma često pribegavaju ovakvom načinu rešavanja problema, ne znajući stvarne posledice po njih.

3.12. Nadgledanje E-pošte i praćenje e-konferencija

Nadgledanje se najčešće vrši uz pomoć nekih softverskih alata kao što keylogger i spyware. Spyware su softveri najčešće ugradjeni i kamuflirani u neke druge softvere a zadatak im je da bez znanja korisnika šalju podatke na unapred određene adrese. Keylogger-i su programi koji pamte sve što korisnik ukuca preko tastature. Oni mogu i da snimaju screenshot korisnika, kao i da peuzimaju e-mail, razgovore, e-konferencije i dr. sa računara na kom je instaliran. Većina modernih keylogger-a se smatra legalnim softverom. Programeri i prodavci nude dugačku listu slučajeva kojima je upotreba keylogger-a pravna i odgovarajuća:

1. Roditeljska kontrola: roditelji mogu da prate šta njihova deca rade na internetu, i mogu da se opredeljuju da budu obavešteni ako postoje pokušaji da se pristupi sajtovima sa sadržajem za odrasle ili na drugi način neprikladan sadržaj;
2. Ljubomorni bračni drugovi ili partneri mogu da koriste keylogger za praćenje postupaka njihove bolje polovine na Internetu ako su im sumnjivi za "virtuelne prevare";
3. Praćenje upotrebe računara za nerad, ili korišćenje radnih stanica posle radnog vremena;
4. Preko keylogger-a može se pratiti unos ključnih reči i fraza u vezi sa komercijalnim informacije koje bi mogli da ugroze preduzeće (materijalno ili na drugi način) ukoliko objavljeno;
5. Drugih razloga

Sve ovo omogućava zlonamernim korisnicima da iskoriste ogromne mogućnosti ovog softvera. Oni keylogger instaliraju na sledeći način:

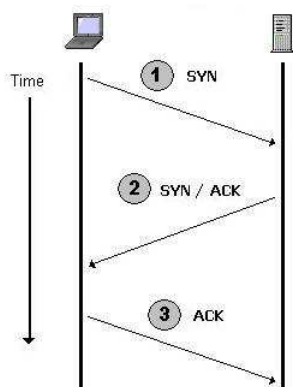
- ✓ keylogger može biti instaliran kada korisnik otvori datoteku u prilogu e-mail-a;
- ✓ keylogger može biti instaliran kada se datoteka pokrene iz otvorenog pristupa direktorijumu na P2P (Peer 2 Peer) mrežu;
- ✓ keylogger može da se instalira preko skripte veb stranice koja eksploatiše ranjivost pretraživača. Program će automatski biti pokrenut kada korisnik poseti zaražen sajt;
- ✓ keylogger može da se instalira od strane drugog zlonamernog programa koji je već prisutan na zaraženom računaru, ako je program u stanju da preuzme i instalira drugi malware na sistem.

3.13. Prisluškivanje

Sam metod prisluškivanja (eng sniffing) zasniva se na osnovnim principima rada mreže gde paketi putuju od jednog do drugog računara pokušavajući da stignu do svoje krajnje odrednice – računara kome se želi pristupiti.

U svakodnevnom radu i komunikaciji između dva računara najčešće korišćena komanda za prelaz sa jednog na drugi računrar putem mreže je komanda telnet, stim da se telnet ne uzima kao jedini vid pristupa ka nekom odredišnom računaru.

Način uspostavljanja veze između dva računara je sledeći



Slika 3. Trostruko rukovanje²⁰

Klijent šalje zahtev za otvaranjem konekcije (SYN). Zatim server odgovara sa tzv. SYN/ACK potvrdom da je zahtev za otvaranjem konekcije od strane klijenta prihvaćen i u trecem koraku klijent uspostavlja vezu sa serverom. Ovaj način uspostavljanja veze se zove trostruko rukovanje (3wayhandsahke).

Prisluškivanje (sniffovanje) je veoma popularna tehnika među hakerima, dokonim administratorima, kriminalcima, za sticanje potrebnih informacija. Sem toga računari komuniciraju putem kablova koji oko sebe stvaraju elektromagnetsko polje. Signale koji se šalju moguće je hardverski snimati i zatim kasnije analizirati.

Danas se sve manje koristi telnet kao servis za daljinsko pristupanje zbog njegove nesigurnosti. Umesto njega danas se koristi SSH (secure shell) servis koji za razliku od telnet enkriptuje celokupan saobraćaj u komunikaciji između korisnika i servera.

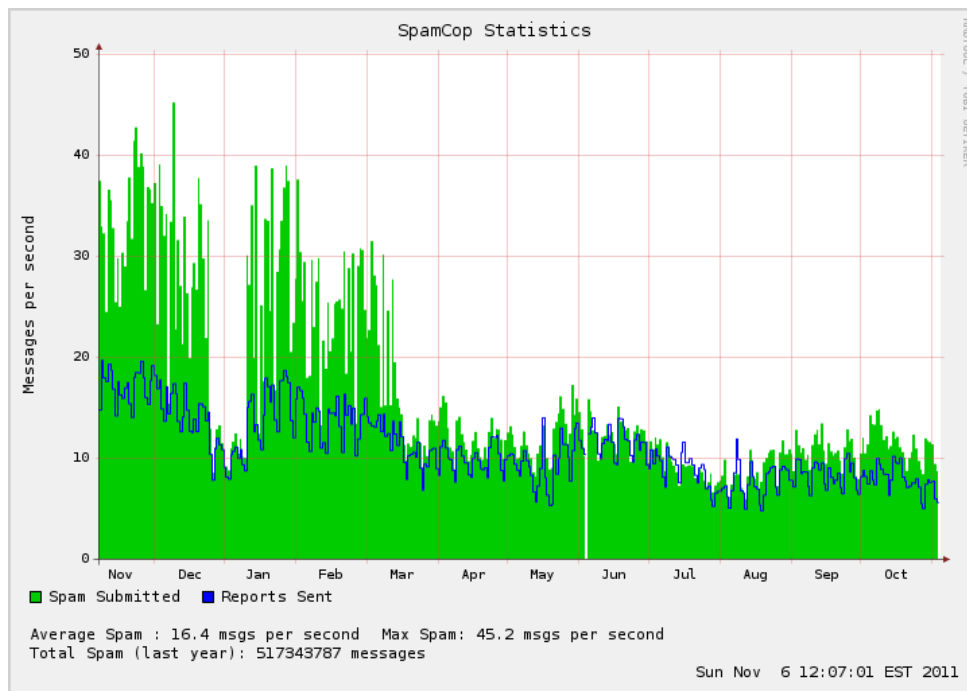
Pored prisluškivanja telnet sesija moguće je prisluškivati i sve ostale TCP/IP sesije koje ne koriste metode kriptovanja. Samim tim znači da je jedan od servisa koji je i doprineo velikoj popularizaciji interneta, e-mail, takođe ugrožen.

3.14. Spam

Spam je anonimna, neočekivana, masovna elektronska pošta. Ovu poštu u ogromnim količinama šalju spameri koji zarađuju novac od malog procenta primaoca koji kupe proizvod koji se reklamira u spam poruci. Spam se takođe koristi za phishing (obmanu) i širenje štetnog koda.

Tokom poslednje decenije, korišćenje i slanje spam poruka se raširilo. U početku, spam se slao direktno korisnicima kompjutera i bilo ga je lako blokirati, ali u godinama koje su usledile, brzo širenje interneta je omogućilo spamerima da jeftino i brzo šalju masovnu poštu, i to onda kada su otkrili da modemima individualnih korisnika može pristupiti bilo ko, sa bilo kog mesta u svetu, zbog toga što oni uopšte nisu bili zaštićeni. Drugim rečima, internet konekcije korisnika koji ništa ne sumnjaju mogu biti iskorišćene za spamovanje znatno većeg obima. To se dešavalo sve dok proizvođači hardvera nisu počeli da osiguravaju svoje uređaje, a filteri postajali sve veštiji u blokiranju spama. Pa ipak, spammerske tehnike su se uvek razvijale, ne samo u pogledu slanja spama, već i kao odgovor na razvoj filtera. Rezultat je tekuća bitka između spamera i onih koji nastoje da ih spreče, konstantno nastojeći da budu korak ispred u borbi sa spamom koji izaziva zakrčenje na autoputu informacija.

Prema izveštaju SpamCop-a prosečan broj spam poruka u jednoj sekundi je 16,4 dok je maksimalan broj spam poruka u sekundi iznosio 45,2 poruke.



Slika 4. Godišnji pregled protoka spama²¹

3.15. Phishing

Phishing je oblik sajber-kriminala zasnovan na metodama društvenog inženjeringa. Naziv phishing je namerna greška u pisanju reči fishing (pecanje), a podrazumeva krađu podataka sa kompjutera korisnika i kasnije korišćenje tih podataka za krađu korisnikovog novca.

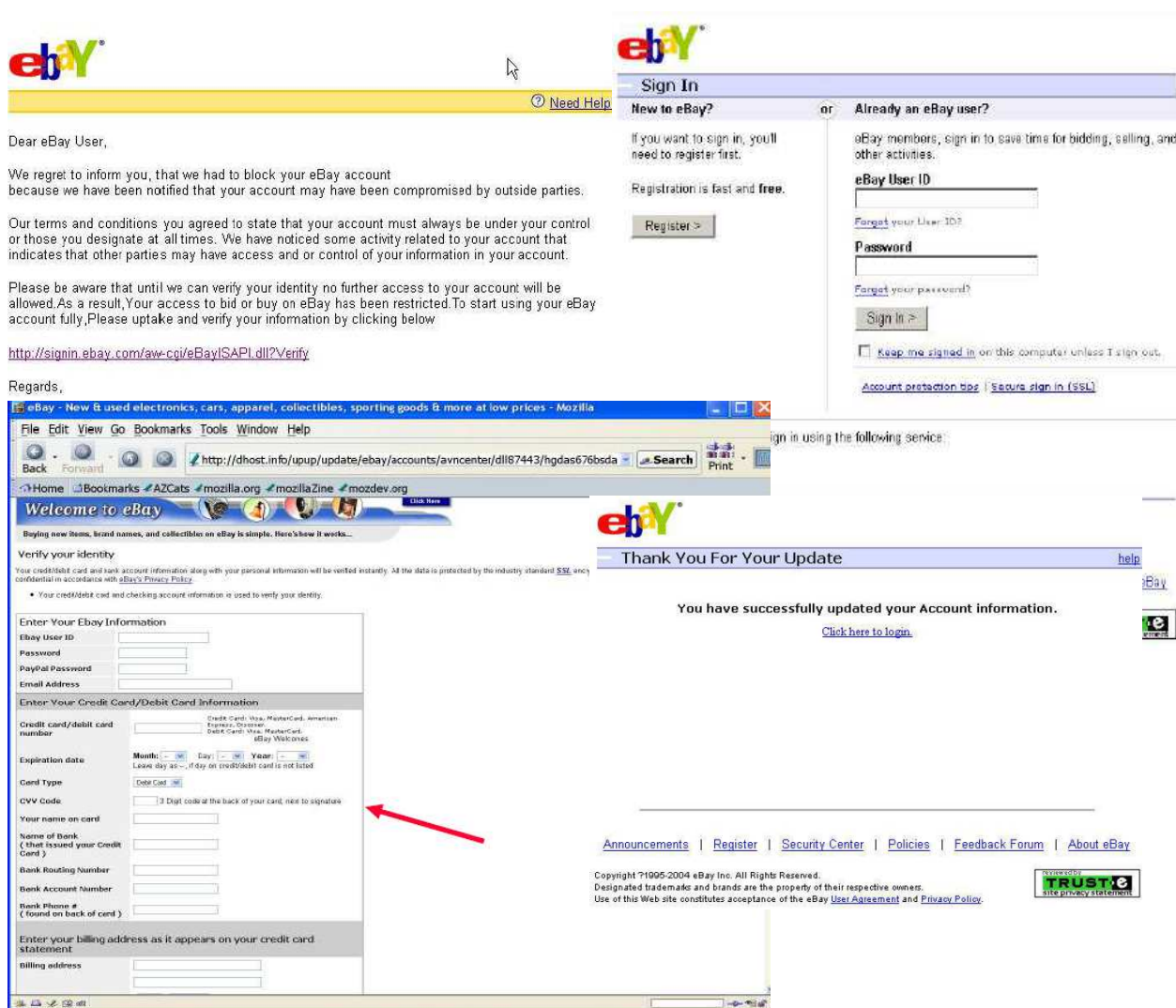
Sajber-kriminalci stvaraju savršene kopije komercijalnih web sajtova finansijskih insitucija. Oni potom nastoje da namame korisnike, koji naravno ništa ne sumnjaju, na sajt kako bi u lažnim formularima na sajtu ostavili svoje login podatke, šifru, broj kreditne kartice, PIN itd. Ove podatke sakupljaju phisher-i koji ih kasnije koriste za neovlašćeni pristup korisničkim nalogima.

Neke finansijske institucije sada koriste grafičke tastature, gde korisnik bira tastere pomoću miša umesto da koristi tastere na pravoj tastaturi. Ovo onemogućava phisher-e da sakupljaju poverljive podatke „hvatanjem“ unosa preko tastature, ali nema pomoći protiv takozvanih screenscaper metoda gde Trojanac pravi trenutni snimak korisnikovog ekrana i prosleđuje ga serveru kontrolisanom od strane autora Trojanca.

Postoji nekoliko različitih načina na koji se korisnici mogu odvesti na lažni web sajt.

- Spam e-mailovi, koji nalikuju prepisci sa legitimnom finansijskom institucijom.
- Agresivnije profilisanje, preciznije ciljana varijanta prethodno navedene metode: sajber-kriminalci usmeravaju phishing scam (prevaru) na korisnike nekog sajta (recimo Facebook) tražeći od njih da potvrde šifre, na primer.
- Instaliranje Trojanca koji menja host fajlove, tako da kada žrtva pokušava da pregleda sajt banke, ona biva preusmerena na lažni sajt.
- Pharming (preusmeravanje na lažni sajt), takođe poznat kao DNS poisoning.

- Spear phishing, napad na određenu organizaciju pri kome phisher traga za podacima jednog od zaposlenih a potom ih koristi kako bi ostvario širi pristup ostatku mreže.



Slika 5. Primer Phishing napada²²

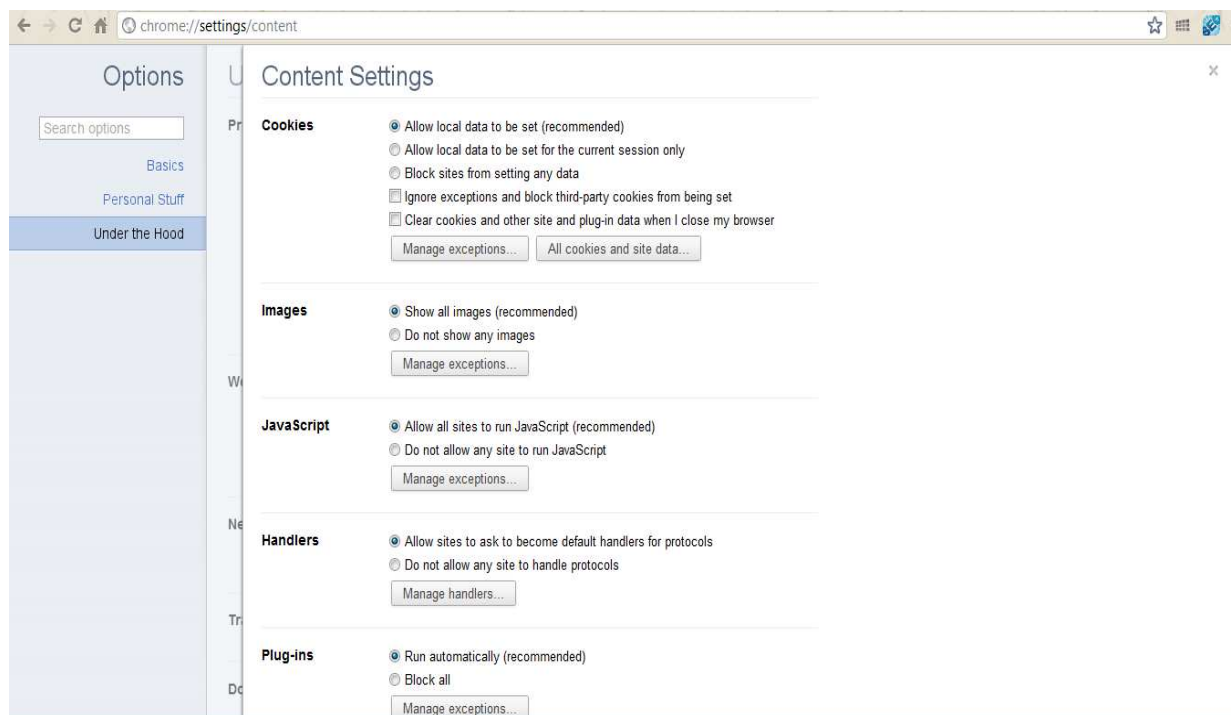
3.16. Analiza kolačića (cookies)

Kolačići su jedna od mnogih kompjuterskih tehnologija koje su napravile revoluciju u krstarenju internetom. To su mali tekstualni fajlovi koji se nalaze u računaru. Imaju više namena, a prvenstvena namena im je da identifikuju korisnika koji posećuje neku web stranu.

Kada korisnik poželi da otvori neku web stranu, njegov browser šalje serveru HTTP (HyperText Transfer Protocol) zahtev prema specifikaciji protokola. U odgovoru server vraća zahtevanu stranu, kojoj prethodi mali paket teksta HTTP odziv. U slučaju da server želi da snimi kolačić na korisnikov računar, odziv će u sebi sadržati i takav zahtev. Ako browser ima mogućnost korišćenja kolačića (a svi novi browseri imaju) i ako je uključeno korišćenje kolačića, server će snimiti kolačić na računar i koristiti ga pri sledećem otvaranju te strane. Naravno, pri sledećim posetama server može da promeni vrednosti koje kolačić sadrži, tačnije da ga ažurira ako je potrebno. Browser samo prima i šalje kolačiće u neizmenjenom obliku.

Informacije koje sadrži kolačić prvenstveno zavise od servera. Neke web strane mogu da prilagode prikaz prema korisnikovoj želji. Ako kolačić u sebi ne sadrži datum, onda je to takozvani „Session Cookie”, što znači da traje samo dok se ne zatvori browser. U ostalim slučajevima trajanje im je do datuma koji je upisan u njima.

Postoje dva tipa kolačića: „First Party” i „Third Party”. Prvi potiču sa istog servera čije strane korisnik posećuje. U drugom slučaju, kolačići dolaze s nekog servera sa strane koji na prvom sajtu ima ugrađen (engl. *embedded*) neki sadržaj. Korisnik može da izabere koji kolačić će da koristi a koji ne.



Slika 6. Podešavanje kolačića u GoogleChrome, Screenshot

Loše strane kolačića je „zasluga” kompanija za oglašavanje, koje upotrebljavaju kolačiće za istraživanje tržišta i programiranje ciljnog tržišta. Svako ko brine o svojoj privatnosti treba da zna da li može da je zaštititi ili ne. Kao i u drugim slučajevima, i sa kolačićima treba praviti kompromis – šta se dobija a šta gubi ako se kolačići onemoguće ili im se ograniči upotreba. Dakle, to je individualna stvar. Kod različitih sajtova upotreba kolačića različito se manifestuje. Kod nekih se ne gubi apsolutno ništa ako se isključe, a kod drugih nijedna strana neće se moći otvoriti.

Server obično zahteva postavljanje više od jednog kolačića. To mogu biti kolačići samo sa servera čija se strana otvara ili kolačići i sa drugog, eksternog servera (ili više njih).

Postoji mogućnost krađe kolačića preko nekog skript jezika (JavaScript ili JScript). Skript sakuplja kolačiće iz korisnikovog browsera i šalje ih na adresu zainteresovanog servera. Zatim zlonamerni korisnik može da analizira kolačiće i samim tim ugrozi korisnikovu privatnost.

4. PROFIL CYBER KRIMINALCA

Napadačem se smatra svako lice koje neautorizovano pokuša da pristupi podacima, sistemima ili infrastrukturi. U javnosti postoji neslaganje u vezi sa nazivom koji se upotrebljava za cyber napadače, tako da se paralelno koriste termini haker (hacker) i kreker (crecker). Istorijski gledano termin haker definiše osobu koja proučava informacione tehnologije u cilju ovladavanja novim znanjima, dok se krekerom nazivaju lica koja ta ista znanja koriste da bi vršila neautorizovan pristup mreži, sistemu ili podacima. Pojam haker u svom značenju opisuje osobu koja se bavi istraživanjem mogućnosti računara i njihovoj primeni u svakodnevnom životu. Pojam haker je prvi put pomenut sredinom 70-tih godina, kada su dva studenta sa MIT-a (Massachusetts Institute of Technology) koristeći trikove (hackove) ušli na Univerzitetski mejn frejm.

Tokom godina pojam haker je počeo da se vezuje za ljude koji neovlašteno ulaze (tačniji pojam je upadaju) na razne računarske sisteme i manje ili više uspešno pokušavaju da ovladaju sistemom. Takođe se pojavljuju različiti stavovi da li su hakeri u stvari loši (jer neovlašteno pristupaju raznim računarskim sistemima) ili su dobri (jer pokazujući da postoje propusti u sigurnosti i teraju za unapređenjem programa i sistema zaštite). S obzirom na to da je termin haker, iako delimično netačan, najčešće se koristi kao sinonim za napadača. Hakeri se po znanju dele na dve osnovne kategorije:

➤ *Script Kiddies*

U ovu kategoriju spadaju hakeri početnici koji koriste automatizovane alate (programe, skriptove - otuda i naziv Script Kiddies), koje su napisale stručnije "kolege", često bez razumevanja načina na koji rade, kao i bez poznavanja mogućih posledica po sisteme na koje se napadi usmeravaju. Ciljeve biraju po principu slučajnog uzorka na taj način što automatski pretražuju veliki broj sistema dostupnih na Internetu i provaljuju u one najslabije.

➤ *Profesionalci*

Hakeri profesionalci se odlikuju ekspertskim poznavanjem oblasti u kojoj deluju. Najčešće programiraju sopstvene alate, dok ciljeve biraju na osnovu interesa ili potrebe. Osim što rade kao "slobodni strelci", veliki broj kompanija i vladinih agencija ih zapošljava kao pomoć u obezbeđivanju mreža ili u cilju industrijske i vojne špijunaže i kontrašpijunaže. Hakeri se najčešće specijalizuju za jednu od tehnika, npr. za provaljivanje u web aplikacije ili operativne sisteme. U slučaju da je meta napada kompleksan sistem, hakeri se organizuju u timove u kojima je svaki član specijalizovan za određenu oblast.

Iako se po svom psihološkom profilu svrstavaju u asocijalne osobe, često nesposobne da se koncentrišu na uobičajene dnevne aktivnosti, hakeri poseduju natprosečnu upornost i koncentraciju kada je u pitanju rešavanje tehničkih problema, pamćenje nizova podataka i ovladavanje novim tehnologijama (Aspergerov sindrom). Činjenica je da u ovaj psihološki profil mogu da se svrstaju i pojedinci koji u svom delovanju nisu prešli na drugu stranu zakona, kao što su npr. tvorci današnjih računara, dobitnik Nobelove nagrade, ekonomista Vernon Smit i brojni drugi. Zabava, dokazivanje, znatiželja, osveta ili profit samo su deo palete motiva koji utiču na kriminalno delovanje hakera. Vrlo je bitno napomenuti da posledica upada, odnosno naneta šteta ne mora biti u direktnoj vezi sa motivom koji hakera pokreće. Posledice hakerskog upada (kao što je obaranje sistema ili brisanje podataka) u čijoj je osnovi zabava i znatiželja mogu biti podjednako ozbiljne kao posledice onog upada čiji je motiv osveta ili profit. Termin white hat, black hat i gray hat su izvedeni iz vestern filmova u kojima "loši momci" uvek nose crne šešire, dok "dobri momci" nose bele. U tom smislu, White Hat hakeri, iako vrše neautorizovan pristup

tudim sistemima, što je protivzakonito, ne oštećuju sistem ili podatke, već nakon uspešno izvedenog napada obaveštavaju administratora sistema o postojećem bezbednosnom propustu, kao i načinu na koji se propust može rešiti. Motiv koji ih pokreće je najčešće znatiželja. Black Hat hakeri su kriminalci koji koriste informacione tehnologije za ostvarivanje nelegalnog profita. Motivi koji ih pokreću su najčešće profit i samodokazivanje. U Gray Hat hakere spadaju oni koji po potrebi prelaze iz jedne grupe u drugu.

Dakle, ne može se govoriti o jedinstvenom profilu napadača. Najčešće su to nedelikventni, nenasilni, socijalno prilagodljivi pojedinci. To su po pravilu lica koja moraju da poseduju posebna stručna znanja i veštine u domenu visoke informatičke, računarske i kompjuterske tehnologije i kojima su ovakva tehnološka sredstva dostupna. Prema S. Petroviću današnjeg tipičnog kompjuterkog kriminalca moguće je portretisati kao uglavnom mladog, inteligentnog, visokomotivisanog, uzornog i poverljivog radnika, spremnog da radi prekovremeno, da istražuje i da se bori sa povremenim situacijama kad je potreban dodatni radni napor. Ima čvrsto izgrađenu logiku i odlično poznaje kompjuterski sistem, njegove mogućnosti i način korišćenja.²³

5. PRAVNA REGULATIVA CYBER KRIMINALA

Kao i kompjuterski kriminal i cyber kriminal iziskuje odgovarajuću pravnu regulativu. Na međunarodnom nivou najvažnije donešene regulative su:

- ✓ Konvencija Saveta Evrope o sajber kriminalu 2001.;
- ✓ Rezolucija UN o borbi protiv zloupotrebe informatičke tehnologije 2001. i 2002.;
- ✓ Konvencija Saveta Evrope o zaštiti dece od seksualne eksploatacije i seksualnog zlostavljanja 2007.;
- ✓ Direktiva EU o obradi ličnih podataka i zaštiti privatnosti u sektoru elektronskih komunikacija 2002.;
- ✓ Direktiva EU o čuvanju podataka koji su dobijeni ili obrađeni prilikom pružanja javno dostupnih usluga elektronske komunikacije ili javnih komunikacionih mreža 2006.;

Najvažnija međunarodna konvencija koja reguliše pitanje cyber kriminala je Konvencija o cyber kriminalu Saveta Evrope doneta 2001. godine u Budimpešti, a stupila je na snagu jula 2004. godine. Ona predstavlja vodič za države koje žele da razviju legislativu u borbi protiv cyber kriminala. Pored evropskih zemalja konvenciju su prihvatili i Japan, SAD, Kanada i Južna Afrika. Konvenciju prate brojni dokumenti doneti u okviru Saveta:²⁴

- Trust and Security in Cyberspace: The Legal and Policy Framework for Addressing Cybercrime (2002);²⁵
- Cyber-Rights & Cyber-Liberties, Advocacy Handbook for NGOs (2003);²⁶
- Racism Protocol to the Convention on Cybercrime (2003);
- The Protocol to the Cybercrime Treaty (2002);
- Additional Protocol to the Cybercrime Convention Regarding "Criminalization of Acts of a Racist or Xenophobic Nature Committed through Computer Networks";
- Report Revised draft of the Protocol on Racist Speech (2002);
- Background Materials on the Racist Speech Protocol ;
- Draft Protocol on Racist and Xenophobic Speech: Preliminary draft (2001);²⁷
- Second Protocol on Terrorism (2002).²⁸

Predmet konvencije o cyber kriminalu su krivična dela protiv tajnosti, celovitosti i dostupnosti računarskih podataka i mreža (neovlašćen pristup, oštećenje podataka, mreža, itd.), kompjuterska krivična dela (neovlašćeno unošenje, brisanje podataka, računarska prevara, krivična dela vezana za dečiju pornografiju krivična dela protiv povrede autorskih i srodnih prava sporedne odgovornosti i sankcije (pokušaj, pomaganje, podstrekavanje), odgovornost pravnih lica, sankcije, procesno pravo zaštita ljudskih prava oduzimanje sredstava izvršenja krivičnog dela, prikupljanje računarskih podataka u realnom vremenu, itd.

U borbi protiv cyber kriminala u Srbiji na snazi su dva zakona. Pored Krivičnog zakonika, tu je i Zakon o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala. Određivanjem institucija i mehanizama države koji će reagovati na

krivična dela cyber kriminala uspostavljen je u potpunosti uređen način i model institucionalne reakcije društva na ovu vrstu kriminala počev od otkrivanja i gonjenja učinilaca ovih dela, preko optuživanja, procesuiranja i na kraju osuđivanja onih učinilaca kojima je u sudskom postupku utvrđena krivica.

Članovi Krivičnog zakona koji se odnose na cyber kriminal su:

- Čl. 298 Oštećenje računarskih podataka i programa,
- Čl. 299 Računarska sabotaža,
- Čl. 300 Pravljenje i unošenje računarskih virusa,
- Čl. 301 Računarska prevara,
- Čl. 302 Neovlašćen pristup zaštićenom računaru, računarskoj mreži i elektronskoj obradi podataka,
- Čl. 303 Sprečavanje i ograničavanje pristupa javnoj računarskoj mreži,
- Čl. 304 Neovlašćeno korišćenje računara i računarske mreže,
- Čl. 208 Prevara,
- Čl. 185 Prikazivanje pornografskog materijala i iskorišćavanje dece za pornografiju,
- Čl. 199 Neovlašćeno iskorišćavanje autorskog dela ili predmeta srodnog prava,
- Čl. 225 Falsifikovanje i zloupotreba platnih kartica,
- Čl. 317 Izazivanje nacionalne rasne i verske mržnje i netrpeljivosti,

Sajber kriminal je stvorio potrebu za angažovanjem posebno tehnicki obučених stručnjaka, ali i reorganizacijom državnih organa. Zakona o organizaciji i nadležnosti državnih organa za borbu protiv visokotehničkog kriminala predviđa organizovanje i borbu protiv visokotehničkog kriminala i organizovanje i opremanje posebnih državnih organa koji će se baviti ovom oblasti. Organizovana je posebna služba u MUP-u, posebno tužilaštvo i posebno istražno i pretresno odeljenje Okružnog suda u Beogradu. Krivična dela iz oblasti visokotehnološkog kriminala su bila u isključivoj nadležnosti tih organa do 1.1.2010. godine. kada je ukinuto posebno odeljenje pri okružnom tužilaštvu u Beogradu. Danas te funkcije obavljaju:

- Dva zamenika višeg javnog tužioca koji su specijalizovani za borbu protiv visokotehnološkog kriminala,
- Služba za borbu protiv visokotehnološkog kriminala (deo MUP-a),
- Veće Okružnog suda za borbu protiv visokotehnološkog kriminala Okružnog suda u Beogradu.

Zakon se primenjuje radi otkrivanja i krivičnog gonjenja:

- ✓ Krivičnih dela protiv bezbednosti računarskih podataka,
- ✓ Krivična dela protiv intelektualne svojine, imovine i pravnog saobraćaja kod kojih se kao objekat ili sredstvo izvršenja javljaju računari, računarske mreže ili podaci, kao i njihovi proizvodi u materijalnom ili elektronskom obliku.
- ✓ Nastala šteta od preko 850.000 din ili je broj primeraka autorskih dela prešao 500 komada.

Dakle, Srbija već godinama razvija specijalizovane, ali ipak ograničene policijske i tužilačke kapacitete za borbu protiv cyber kriminala, koji su uspešni proporcionalno raspoloživim resursima i neuređenom zakonskom okruženju u kome rade. Nažalost, rad specijalizovanih istražnih službi, bez obzira na to koliko je kvalitetan, po prirodi je reaktivnog

karaktera i ne može da bude dovoljan ukoliko nije podržan mnogo ozbiljnijim radom na planu prevencije i sužavanja prostora za delovanje savremenog cyber kriminala. U ovom trenutku, teško je prepoznati institucionalizovan i organizovan napor države da bolje uredi ovu oblast, izgradi institucionalne kapacitete i podigne nivo svesti korisnika. Poredeći dostignuti stepen razvoja sa evropskim standardima, nema sumnje da Srbija ozbiljno kasni i da joj predstoji složen i obiman posao.

5.1. ORGANIZACIJA I NADLEŽNOST DRŽAVNIH ORAGANA U BORBI PROTIV KOMPJUTERSKOG KRIMINALA

Bezbednost informaciono-komunikacionih mreža je jedan od osnovnih preduslova za elektronsko poslovanje, a posebno za elektronsko plaćanje. Zaštita informacija je neophodna komponenta elektronskog poslovanja koja na željeni nivo redukuje opasnosti vezane za laku dostupnost i brzu razmenljivost ogromnih količina informacija. Brojne i raznovrsne potencijalne pretnje - opasnosti koje ugrožavaju informacione sisteme, a posebno one koji imaju karakter kriminalnih radnji, nedvosmisleno nameću potrebu izgradnje zaštite informacionih sistema. Jedan od segmenata zaštite od prevara i kriminalnih dela je i zakonska regulativa. U Republici Srbiji je u Krivičnom zakoniku u glavi dvadeset i sedam taksativno su nabrojana krivična dela protiv bezbednosti računarskih podataka, koja smo obradili u prethodnom poglavlju ovog rada, i koja uz ostala krivična dela vezana za visoko tehnološki kriminal svakako doprinose sprečavanju vršenja krivičnih dela iz ove oblasti.

U cilju sprovođenja Krivičnog zakonika vezano za oblast iz glave dvadeset i sedam s obzirom na specifičnost ovih krivičnih dela donet je Zakon o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala jula meseca 2005. godine⁴⁴.

5.1.1. Posebno tužilaštvo

Kako je članom 4. Zakona o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala predviđeno za krivična dela protiv bezbednosti računarskih podataka i krivičnih dela protiv intelektualne svojine, imovine i pravnog saobraćaja kod kojih se kao objekat ili sredstvo izvršenja krivičnih dela javljaju računari, računarske mreže i računarski podaci, za postupanje u predmetima navedenih krivičnih dela nadležno je Okružno javno tužilaštvo u Beogradu za teritoriju Republike Srbije. Obrazuje se posebno odeljenje za borbu protiv visokotehnološkog kriminala. Radom Posebnog tužilaštva rukovodi posebni tužilac za visokotehnološki kriminal, koga postavlja Republički javni tužilac iz redova javnih tužilaca i zamenika javnih tužilaca. Prednost imaju javni tužioci odnosno zamenici javnih tužilaca koji poseduju posebna znanja iz oblasti informatičkih tehnologija. Mandat posebnog tužioca je četiri godine i može biti ponovo postavljen. Posebni tužilac ima prava i dužnosti kao javni tužilac. Kada dođe do saznanja da se u jednom krivičnom predmetu radi o slučajevima predviđenim za nadležnost Posebnog tužioca, isti se pismeno obraća Republičkom javnom tužiocu zahtevajući od njega da mu poveri ili prenese u nadležnost taj predmet. Republički javni tužilac, na predlog Posebnog tužioca, donosi poseban akt o unutrašnjoj organizaciji i sistematizaciji radnih mesta u posebnom tužilaštvu uz saglasnost ministra za poslove pravosuđa.

5.1.2. Služba za borbu protiv visokotehnološkog kriminala

Članom 9 istog zakona je predviđeno da se obrazuje posebna služba za borbu protiv visokotehnološkog kriminala u okviru Ministarstva unutrašnjih poslova. Ministar unutrašnjih poslova po pribavljenom mišljenju Posebnog tužioca postavlja i razrešava starešinu Službe i bliže uređuje njen rad u skladu sa zakonom. Služba postupa po zahtevima Posebnog tužioca u skladu sa zakonom.

5.1.3. Nadležnost i organizacija sudova

Za postupanje u predmetima krivičnih dela iz oblasti visokotehnološkog kriminala za teritoriju Republike Srbije je nadležan Okružni sud u Beogradu. Za odlučivanje u drugom stepenu nadležan je neposredno viši sud . U okružnom sudu u Beogradu se obrazuje Veće za borbu protiv visokotehnološkog kriminala. Sudije u to veće raspoređuje predsednik Okružnog suda iz reda sudija tog suda uz njihovu saglasnost. Prednost imaju sudije koje poseduju posebna znanja iz oblasti informacionih tehnologija Sudije se raspoređuju u Veće najduže na dve godine a može im biti produžen mandate odlukom predsednika Okružnog suda u Beogradu.

5.1.4. Dosadašnja primena ovih zakona

Zakon je donet 2005. godine. Posebno tužilaštvo je formirano aprila 2007. godine Za krivična dela protiv bezbednosti računarskih podataka podignute su do sada optužnice 66 protiv 8 lica. Za krivična dela protiv intelektualne svojine u 2007. godini podignuta je optužnica protiv 95 lica .U toku 2008 godine Posebnom tužilaštvu za borbu protiv visoko tehnološkog kriminala podnete su krivične prijave protiv 166 lica, što predstavlja značajan porast u odnosu na prethodnu godinu. Zahtev za sprovođenje istrage stavljen je protiv 147 lica. Protiv 75 lica podignute su optužnice. U toku 2008 godine, policijski službenici Odeljenja za borbu protiv visokotehnološkog kriminala, SBPOK – a MUP-a Republike Srbije, od izvršilaca ovih krivičnih dela oduzeli su ukupno 53 računara i 48.400 kom. optičkih diskova, sa hiljadama neovlašćeno umnoženih autorskih dela u vidu filmova, muzika, softvera, računarskih igrica i drugih multimedijalnih sadržaja. U toku 2008 godine, na teritoriji Republike Srbije izvršeno je ukupno 1.313 krivičnih dela visokotehnološkog kriminala. U prethodnoj godini taj broj je uznosio 1.09545. Od osnivanja Posebnog tužilaštva za borbu protiv visokotehnološkog kriminala 55 lica je optuženo, 43 lica je pravosnažno osuđeno, a protiv 42 lica postupak je još uvek u toku. Pozitivnopravnim propisima RS, iz stvarne nadležnosti Posebnog tužilaštva izostavljan su krivična dela koja se odnose na zloupotrebu platnih kartica i internet pornografiju.

5.2. PROPISI REPUBLIKE SRBIJE U OBLASTI KOMPJUTERSKOG KRIMINALITETA

Što se tiče naše države, možemo reći da smo se sa velikim zakašnjenjem uključili u oblast rešavanja ovog problema, te da je prvi korak načinjen donošenjem Zakona o izmenama i dopunama Krivičnog Zakonika Republike Srbije, kada je po prvi put izvršena inkriminacija krivičnih dela koja pripadaju oblasti kompjuterskog kriminala. To praktično znači da do donošenja ovog zakona, nije postojala zakonska regulativa u ovoj oblasti, te da su učinioci ovih krivičnih dela, bili izuzeti od krivičnog gonjenja, te da su slobodno bez bilo kakvih posledica mogli da vrše sve napred navedene oblike kompjuterskog kriminala. Kako je prema Krivičnom Zakoniku predviđeno : „ *Krivično delo je ono delo koje je zakonom predviđeno kao krivično delo, koje je protivpravno i koje je skrivljeno* „⁴¹ Određenost u zakonu je opšte obeležje svakog krivičnog dela. Određenost u zakonu znači propisivanje svih obeležja jednog krivičnog dela, određivanje njegovog bića. Dakle, tek 2003 godine uvodi krivična dela vezana za zloupotrebu kompjutera, a koja imaju zajednički objekt zaštite - bezbednost računarskih podataka odnosno informacionih sistema u celini i poverenja u istinitost ovih podataka. Dakle, osnovni materijalni zakon koji reguliše ovu oblast je Krivični Zakonik Republike Srbije , a nedavno je i ratifikovana Konvencija o visokotehnološkom kriminalu.

5.2.1. Krivično materijalno pravo

Krivično materijalno pravo predviđeno je prvenstveno Krivičnim Zakonom Republike Srbije . Krivični Zakonik Republike Srbije u delu koji nosi naziv „ Krivična dela protiv bezbednosti računarskih podataka“ predviđa sledeća krivična dela⁴². Prvo krivično delo ove vrste u našem pravu jeste: **Oštećenje računarskih podataka i programa**

Delo ima osnovni i dva teža oblika. Osnovno delo se sastoji u oštećenju, prikrivanju, neovlašćenom brisanju, izmeni ili na drugi način činjenju neupotrebljivim računarskih podataka ili programa. Delo se dakle može učiniti samo u odnosu na računarski podatak ili program koji pripada nekom fizičkom licu - pojedincu (kao napadni objekt) i to sa više alternativno predviđenih delatnosti. Cilj preduzimanja ovih delatnosti je onesposobljavanje za korišćenje u potpunosti ili delimično računarskih podataka (jednog ili više njih) ili programa.

⁴¹izvor : *Krivični Zakonik Republike Srbije*

⁴² izvor : *Krivični Zakonik Republike Srbije*

Posledica se dakle sastoji u povredi zaštićenog dobra. Delo može učiniti svako lice a u pogledu vinosti potreban je umišljaj. Za ovo je delo propisana novčana kazna ili zatvor do tri meseca. Prvi teži oblik ovog krivičnog dela postoji ako je preduzetom radnjom prouzrokovana šteta za neko lice u iznosu preko 450 000 dinara. Visina prouzrokovane štete je kvalifikatorna okolnost za koju zakon propisuje kaznu zatvora od tri meseca do tri godine. Najteži oblik ovog krivičnog dela za koji je propisana kazna zatvora od šest meseci do pet godina postoji ako je preduzetom radnjom prouzrokovana šteta u iznosu preko 1.500000 dinara.

Računarska sabotaza je drugo kompjutersko krivično delo u našem pravu za koje je propisana kazna zatvora od jedne do pet godina. Delo čini lice koje unese, uništi, izbriše, izmeni, ošteti, prikrije ili na drugi način učini neupotrebljivim računarski podatak ili program ili uništi ili ošteti računar ili drugi

uređaj za elektronsku obradu i prenos podataka sa namerom da onemogući ili znatno omete postupak elektronske obrade i prenosa podataka koji su od značaja za državne organe, javne službe, ustanove, preduzeća ili druge subjekte. Objekt napada kod ovog dela je dvojako određen. To je prvo, računarski podatak ili program (kao i kod prethodnog krivičnog dela) ali i računar

odnosno drugi uređaj za elektronsku obradu ili prenos podataka. No, ovde se mora raditi i o posebnom svojstvu oštećenog. Naime, ovi objekti moraju da pripadaju državnom organu, javnoj službi ili drugim pravnim licima kao što su ustanove, preduzeća ili druge organizacije. Inače u pogledu radnje izvršenja i ostalih obeležja bića ovog dela nema razlike u odnosu na prethodno krivično delo.

Pravljenje i unošenje računarskih virusa je krivično delo predviđeno u čl. 300 Delo ima osnovni i teži oblik. Osnovno delo čini lice koje napravi računarski virus u nameri da ga unese u tuđi računar ili računarsku mrežu. Radnja izvršenja je samo sačinjavanje, pravljenje virusa. Šta su to virusi, kako se prave, koje su njihove vrste ili karakteristike, svrha i sadržina predstavljaju pitanja koje sudsko veće mora da reši u svakom konkretnom slučaju kao faktičko pitanje. Delo je svršeno samim momentom pravljenja ovakvog virusa u nameri da se on unese u tuđi računar ili računarski sistem bez obzira da li je takva namera i ostvarena u konkretnom slučaju ili ne. Ako je pak ovako sačinjeni, napravljeni virus i unet u tuđi računar ili računarsku mrežu čime je prouzrokovana šteta (bilo imovinska ili neimovinska i to bez obzira u kom iznosu) radi se o težem obliku ovog krivičnog dela. Sledeće je krivično delo je **Računarska prevara**. Delo ima jedan osnovni, jedan posebni i dva teža, kvalifikovana oblika. Osnovno delo čini lice koje unese netačan podatak ili ne unese kakav važan podatak ili ko na drugi način prikrije ili lažno prikaže podatak i tako utiče na rezultat elektronske obrade ili prenosa podataka. Bitno je da je ova radnja falsifikovanja, krivotvorenja, dovodenja u zabludu oštećenog preduzeta u nameri da se sebi ili drugom pribavi protivpravna imovinska korist odnosno da se drugome nanese kakva imovinska šteta. Za postojanje krivičnog dela dovoljno je da je radnja izvršenja preduzeta u navedenoj nameri. Tog trenutka je delo svršeno. Nije potrebno da je u konkretnom slučaju u nastupila imovinska šteta za neko lice Poseban oblik računarske prevare za koji je propisana novčana kazna ili zatvor do dve godine postoji kada je radnja krivotvorenja podataka ili prikrivanja ili lažnog prikazivanja računarskih podataka preduzeta u nameri da se na ovaj način drugom licu nanese kakva šteta. Ta šteta ne mora da nastupi u konkretnom slučaju, ali ona mora da bude pobuda, unutrašnji pokretač učinioca na preduzimanje radnje izvršenja. Može se raditi o imovinskoj, ali i drugim vidovima neimovinske štete. Zavisno od visine pribavljene protivpravne imovinske koristi za učinioca ili neko drugo lice, zakon razlikuje dva teža, kvalifikovana oblika ovog krivičnog dela. Obliku računarske prevare za koji je propisana kazna zatvora od dve do dvanaest godina. **Neovlašćeni pristup zaštićenom računaru, računarskoj mreži i elektronskoj obradi podataka** ima osnovni i dva teža oblika ispoljavanja. Osnovno delo čini lice koje kršeći mere zaštite (preventivno - tehničke i druge mere) neovlašćeno pristupi računaru ili računarskoj mreži ili neovlašćeno pristupi elektronskoj obradi podataka. Radnja izvršenja je pristupanje, ulazak, upad u tuđi računar ili računarsku mrežu. Bitno je da je ova radnja preduzeta neovlašćeno, dakle protivpravno I drugo kršenjem predviđenih mera zaštite. Ove okolnosti moraju biti obuhvaćene umišljajem učinioca dela. Prvi teži oblik za koji je propisana novčana kazna ili zatvor do dve godine čini lice koje upotrebi podatak koji je pribavio, do koga je došao neovlašćenim pristupom zaštićenom računaru ili računarskoj mreži. Ova upotreba može biti u bilo kojoj nameri ili za bilo koju svrhu ili cilj. Ako je pak usled preduzete radnje upotrebe na ovaj način pribavljenog računarskog podatka došlo do nastupanja teških posledica za drugog (drugo fizičko ili pravno lice) radi se o najtežem krivičnom delu ove vrste za koje je zakon propisao kaznu zatvora od šest meseci do pet godina. Bitno je da je posledica i to teška (a to je faktičko pitanje za sudsko veće) nastupila za drugog i da između nje i preduzete radnje upada u zaštićeni računarski sistem postoji uzročno-posledična veza. **Sprečavanje i ograničavanje pristupa javnoj računarskoj mreži**. Delo ima osnovni i teži oblik. Objekt napada u ovom slučaju je javna računarska mreža. Osnovno delo čini lice koje neovlašćeno (dakle protivno postojećim propisima, protivzakonito) sprečava ili ometa pristup javnoj računarskoj mreži. Za ovo je delo propisana novčana kazna ili zatvor do 60 jedne godine. U slučaju da se kao učinilac javi službeno lice u vršenju službe tada se radi o kvalifikovanom obliku ovog dela za koji je propisana kazna zatvora do tri godine. Ovde se zapravo radi o posebnom, specijalnom obliku

krivičnog dela zloupotrebe službenog položaja službenog lica koje sprečava ili ometa drugom fizičkom ili pravnom licu nesmetani pristup i korišćenje javne računarske mreže. I poslednje delo je **Neovlašćeno korišćenje računara ili računarske mreže**. Delo čini lice koje neovlašćeno koristi računarske usluge ili računarsku mrežu u nameri da sebi ili drugom pribavi protivpravnu imovinsku korist. Predviđena je novčana kazna ili zatvor do tri meseca.

5.2.2. Konvencija o visokotehnološkom kriminalu

Ova konvencija je ratifikovana od strane Narodne skupštine Republike Srbije, I na taj način uveta u domaći pravni poredak. U samom uvodu ove konvencije, data su objašnjenja i razlozi donošenja⁴³. Kao osnovni razlog za donošenja ove Konvencije, države potpisnice navode: Sprovođenje zajedničke kaznene politika u svrhu zaštite društva od kiber kriminala, *inter alia* usvajanjem odgovarajuće legislative i unapređivanjem međunarodne saradnje; Saradnja između država i privatnih preduzeća u borbi protiv kiber kriminala I potrebu zaštite legitimnih interesa u korišćenju i razvoju informatičke tehnologije, jer efikasna borba protiv kiber kriminala zahteva povećanu, brzu i veoma funkcionalnu međunarodnu saradnju u krivičnim stvarima; U Konvenciji se navode osnovi donošenja ovog akta, kao što su: Duboke promene koje je donela digitalizacija, konvergencija i stalni trend ka globalizaciji kompjuterskih mreža; Rizici da se kompjuterske mreže i elektronske informacije mogu takođe koristiti za izvršenje krivičnih dela i da dokazni materijali koji se odnose na takve prestupe mogu biti uskladišteni u tim mrežama ili prenošeni preko njih; Dakle, osnovni cilj konvencije je sprečavanje dela usmerenih protiv poverljivosti, integriteta i dostupnosti kompjuterskih sistema, mreža i kompjuterskih podataka, kao i sprečavanja zloupotrebe tih sistema, mreža i podataka na taj način što će se predvideti kaznene mere za takva činenja kao što je opisano u ovoj konvenciji i što će se usvojiti mere dovoljne za efikasnu borbu protiv takvih krivičnih dela, na taj način što će se na ⁴³Izvor: Konvencija o visokotehnološkom kriminalu 61 unutrašnjem i međunarodnom nivou olakšati otkrivanje, istraga i gonjenje takvih krivičnih dela i što će se obezbediti uslovi za brzu i pouzdanu međunarodnu saradnju; Konvencija definiše sledeće termine Izraz **"kompjuterski sistem"** označava svaki uređaj ili grupu međusobno povezanih ili uslovljenih uređaja, od kojih jedan ili više njih, u zavisnosti od programa, vrši automatsku obradu podataka; Izraz **"kompjuterski podaci"** označava svako izlaganje činjenica, podataka ili koncepata u obliku koji je pogodan za njihovu obradu u kompjuterskom sistemu, uključujući tu i odgovarajući program na osnovu kojeg kompjuterski sistem vrši svoju funkciju; Izraz **"davalac usluga"** označava: Svako javno ili privatno lice koje korisnicima pruža svoje usluge na polju komuniciranja putem kompjuterskih sistema, I Svako drugo lice koje obrađuje ili skladišti kompjuterske podatke za račun takvih komunikacijskih usluga ili za račun korisnika takvog servisa. Izraz **"promet podataka"** označava sve kompjuterske podatke koji su u vezi sa komuniciranjem putem kompjuterskih sistema, a koje generiše kompjuterski sistem i koji čine deo lanca komuniciranja, u kojima se sadrže podaci o poreklu, odredištu, putanji, vremenu, datumu, veličini, trajanju i vrsti predmetne usluge. Krivična dela protiv **poverljivosti, integriteta i dostupnosti kompjuterskih podataka i sistema**. Nedozvoljeni pristup Svaka članica treba da usvoji takve legislativne i ostale neophodne mere da bi se bespravno pristupanje kompjuterskom sistemu kao celini ili nekom njegovom delu, kada se učini namerno, okvalifikovalo u njenom nacionalnom pravu kao krivično delo. Članica može da uslovi da delo mora biti učinjeno kršenjem bezbednosnih mera sa namerom pribavljanja kompjuterskih podataka ili sa nekom drugom nečasnom namerom, ili učinjeno u vezi sa kompjuterskim sistemom koji je povezan sa drugim kompjuterskim sistemom. Nedozvoljeno presretanje Svaka članica treba da usvoji takve legislativne i ostale neophodne mere da bi se u njenom nacionalnom pravu kao krivično delo okvalifikovalo bespravno presretanje prenosa kompjuterskih podataka koji nisu javne prirode, ka kompjuterskom sistemu, od njega ili unutar samog sistema, u šta spada i elektromagnetska emisija iz kompjuterskih sistema kojom se prenose takvi podaci, a kad je učinjeno sa namerom i uz pomoć tehničkih uređaja. Članica može usloviti da delo mora biti učinjeno sa nečasnim

namerama, ili učinjeno u vezi sa kompjuterskim sistemom koji je povezan sa drugim kompjuterskim sistemom. Ometanje podataka svaka članica treba da usvoji takve legislativne i ostale neophodne mere da bi se bespravno oštećenje, brisanje, kvarenje, menjanje ili prikrivanje kompjuterskih podataka okvalifikovalo u njenom nacionalnom pravu kao krivično delo, ukoliko se učini sa namerom. Članica može rezervisati pravo da uslovi da dela iz stava 1 moraju da rezultiraju velikom štetom. Ometanje sistema Svaka članica treba da usvoji takve legislativne i ostale neophodne mere da bi se u njenom nacionalnom pravu kao krivično delo okvalifikovalo bespravno i u većem stepenu ometanje funkcionisanja kompjuterskih sistema putem unošenja, prenošenja, oštećenja, brisanja, kvarenja, menjanja ili prikrivanja kompjuterskih podataka, ukoliko je učinjeno sa namerom. Zloupotreba uređaja Svaka članica treba da usvoji takve legislativne i ostale neophodne mere da bi se u njenom nacionalnom pravu kao krivično delo, ukoliko je učinjeno sa namerom i bespravno, okvalifikovalo sledeće: Proizvodnja, prodaja, nabavljanje radi upotrebe, uvoz, distribucija i drugi vidovi stavljanja na raspolaganje; Sredstava, što podrazumeva i kompjuterske programe, projektovane ili preuređenje prvenstveno u svrhu izvršenja nekog od navedenih dela; Kompjuterskih lozinki, šifri za pristup, ili sličnih podataka putem kojih se može pristupiti kompjuterskom sistemu kao celini ili nekom njegovom delu sa namerom da bude upotrebljen u svrhu izvršenja nekog od navedenih dela. Falsifikovanje koje je u vezi sa kompjuterima Svaka članica treba da usvoji takve legislativne i ostale neophodne mere da bi se u njenom nacionalnom pravu kao krivično delo okvalifikovalo unošenje, menjanje, brisanje ili prikrivanje kompjuterskih podataka koje rezultira u podacima koji nisu autentični, sa namerom da se učini da oni budu smatrani za autentične i da se sa njima u redovne svrhe postupka kao da su autentični, bez obzira na to da li su ti podaci direktno čitljivi i razumljivi. Članica može usloviti da postoji namera prevare, ili slična nečasna namera, da bi se ustanovila krivična odgovornost. Prevare koje su u vezi sa kompjuterima Svaka članica treba da usvoji takve legislativne i ostale neophodne mere da bi se u njenom nacionalnom pravu kao krivično delo okvalifikovalo nanošenje imovinske štete drugim licima kada se to učini bespravno i sa namerom, na sledeće načine: Bilo kakvim unošenjem, menjanjem, brisanjem ili prikrivanjem kompjuterskih podataka, Bilo kakvim ometanjem funkcionisanja kompjuterskih sistema, Sa namerom prevare ili drugom nečasnom namerom da se bespravno pribavi ekonomska dobit za sebe ili za druga lica Pored krivičnopravnih odredaba materijalnog karaktera koje sadrži Krivični zakonik Republike Srbije, oblast pravne zaštite prava intelektualne svojine, u okviru borbe protiv visokotehnološkog kriminala, regulisana je i **Zakonom o posebnim ovlašćenjima radi zaštite prava intelektualne svojine**. Ovim zakonom predviđena je odgovornost za privredne prestupe i prekršajna odgovornost pravnih lica za povredu prava intelektualne svojine. U pravcu kontrole proizvodnje, prometa, upotrebe i držanja robe kao i pružanja usluga kojima se povređuje pravo intelektualne svojine, posebna ovlašćenja poverena su pojedinim ministarstvima kroz inspeksijske službe (tržišna i turistička inspekcija pri Ministarstvu trgovine, turizma i usluga, poreski inspektorat i policija pri Ministarstvu finansija i dr.). Međutim, i ovde je učinjen jedan propust koji stvara dosta problema u primeni zakona. Naime, za jedan od subjekata privrednog poslovanja, samostalne trgovinske radnje, nisu predviđeni oblici odgovornosti. To u praksi znači da se radnje koje predstavljaju kršenje prava intelektualne svojine izvršene u poslovanju ovakvih subjekta privrednog prometa ne mogu brzo i efikasno sankcionisati kroz odgovornost za privredne prestupe, što one u suštini i jesu, već se moraju posmatrati kroz izvršenje krivičnog dela neovlašćenog iskorišćavanja autorskog dela ili predmeta srodnog prava. Ovo, sa jedne strane, podrazumeva angažovanje celokupnog mehanizma krivičnopravne zaštite koji je glomazan i ne naročito brz i efikasan u smislu ostvarivanja svrhe sankcionisanja zabranjene radnje, dok, sa druge strane, imajući vidu da naše krivično zakonodavstvo tek odskora predviđa odgovornost pravnog lica, nameće individualno sankcionisanje pojedinačne radnje jednog ili više fizičkih lica, čime se znatno otežava sankcionisanje nedozvoljenog ponašanja privrednog subjekta u privrednom i platnom prometu. Dakle, propisivanjem krivičnih dela koja se odnose na kompjuterski kriminalitet učinjen je prvi korak u suzbijanju ovih nedozvoljenih oblika ponašanja, međutim to nije dovoljno i da bi borba protiv visokotehnološkog kriminaliteta dala

određene rezultate potrebno je izvršiti I korenite promene u organizaciji i nadležnosti pravosudnih organa. To je učinjeno donošenjem Zakona o organizaciji i nadležnost državnih organa za borbu protiv visokotehnološkog kriminala jula meseca 2005. godine.

6. PIRATI NA MREŽI

Opasnost od velikog napada iz cyber-prostora danas spada u standardni repertoar govora, razvoja strategija i studija američke bezbedonosne politike. Već deset godina stižu upozorenja na “elektronski Perl Harbur” koji bi trebalo da bude izazvan “software-skombom na tržištu akcija” ili ispadom sistema sigurnosti letova koje može da prouzrokuje jedan hacker ili masivan napad tipa: Denial of Service (odbijanje pružanja usluga) na američku internet-privredu. Po navodima američkih obaveštajnih službi, u potencijalne protivnike koji se pripremaju na vođenje virtualnog rata u mrežama podataka spadaju Kineska narodnooslobodilačka vojska, islamski teroristi Osama Bin Ladena ili čak zaostala vojska Kube. Ono što se u ovim strateškim analizama nikad ne pominje, nasuprot svakoj horor vesti koje mediji vrlo rado objavljuju, uzrok je te nove trke u naoružavanju. Vojno osvajanje cyber-prostora nije počelo u avganistanskim planinama, ili na vojnim akademijama u Kini, već u samim Sjedinjenim Američkim Državama. Od početka 1990-tih godina, američka vojska je u svojim istraživačkim laboratorijama razvila elektronsko oružje za hacker-ski rat. A u “fabrikama ideja” postavljene su temeljne teorijske analize i konačno, u štabovima su napisane nove doktrine. Već više puta su američke specijalne jedinice izvodile cyber dejstva i poslednji je bio rat na Kosovu 1999. godine. Mnogo toga se do dana današnjeg čuva kao stroga tajna. Od onoga što je dostupno u javnim izvorima, može da se napravi sasvim zadovoljavajuća slika američkih cyber-ratnika, njihovog oružja i organizacije. A pri svemu tome se pokazuju unutrašnje protivrečnosti i teškoće koje su povezane sa takvom slikom rata, i ispostavlja se potreba da se razmisli o novim formama kontrole naoružanja na ovom polju. Dve razvojne linije – tehnička i strategijska – dovele su do aktuelnih napora SAD za vođenje rata na mreži. S jedne strane, vojna upotreba elektronike i kompjuterske tehnologije je prilično duga priča – ipak, kao što je poznato, prve kompjutere razvili su britanski i američki stručnjaci za prisluškivanje radi dekodiranja nemačke vojne komunikacije u Drugom svetskom ratu. Posle uvođenja radara, bežične komunikacije i elektronski upravljivih bombi, razvilo se i posebno polje takozvanog “elektronskog rata” ometanjem signala, elektronskim maketama (lažna vojna oprema) i oružjem koje traži signale i uništava odašiljače; tokom 1980tih godina razvilo se čak i takmičenje između “elektronskih kontramera” i “elektronskih kontra-kontramera”, a njihov cilj je bio da se elektromagnetni spektar koristi u potpunosti, a da se protivniku upravo to onemogući. Sredstva za tako nešto bili su oružani sistemi kao anti radarska raketa “HARM”, specijalni elektronski “borbeni avioni” kao što je EC-130H “Compass Call” ili EA- 6B “Prowler”, kao i visoko razvijena elektronika za komunikaciju bez ometanja i mogućnosti prisluškivanja. Ovaj razvoj, u situaciji nuklearnog zastrašivanja, politički nije bio posebno interesantan, i zbog toga je samo tehnološki forsiran. Dodajmo još i da su takve mere uvedene u “Operations Security” i bile su prisutne u vojnim obaveštajnim službama i izviđačkim jedinicama. Njihova posebna institucionalna uloga – da nisu podređeni komandantima jedinica u borbi – sprečila je razmišljanje o tome da li i kako se vođenje rata može iz osnova promeniti uz pomoć moderne elektronike. Da bi se to ostvarilo, bili su potrebni drugi uticaji na vantehničkim putevima. A ti uticaji su došli od istorijski obrazovanih mislilaca iz Pentagona, koji su predavali i

istraživali, poput Džona Arkvila (John Arquilla) sa Naval Postgraduate School u Montereyju, zatim Dejvida Ronfelda (David Ronfeldt) i Martina Libickog iz “fabrike misli” koja je bliska Pentagonu - Rand Corporation iz Santa Monike ili Dana Kuela (Dan Kuehl) sa National Defense University-a iz Vašingtona. Oni, a i drugi počeli su početkom 1990-tih godina da razmišljaju o društvenim, a time i vojnim promenama uslovljenim novim informacionim tehnologijama. U skladu sa neoliberalnim duhom vremena, prve studije su bazirane na novim menadžmentskim koncepcijama sa fleksibilnim organizacionim oblicima i “plitkom” hijerarhijom. Sa širenjem interneta i nastajuće diskusije o “informacijskom društvu”, koncept informacije dospao je u središte pažnje kao resurs. Ako postindustrijsko društvo i njena vojna sila nisu usmereni na ljude i mašine kao sredstvo produkcije ili destrukcije, tako se razmišlja, onda ciljevi napada vojnih operacija nisu više snaga protivnika, već njegovi sistemi obrade podataka. Institucionalizacija i operacionalizacija Time je “informacijski rat” dosegao status vojno strateške misli. Prve ideje i razmišljanja bile su postavljene već u 1970-tim godinama, ali konačan oblik dobile su tek 1990-tih godina u širokoj diskusiji o novim ciljevima, strukturnim principima i mogućnostima vođenja rata. Već 1992. godine napisana je prva strogo poverljiva direktiva Pentagona TS-3600.1 “Information warfare” sa kojim je počeo proces stalne organizacione i strateške reforme traje sve do dana današnjeg. Debata o vođenju informacijskog rata usidrila se vrlo brzo i organizaciono u vojnom aparatu. Posledica je bila osnivanje School for Information Warfare and Strategy na National Defense University u Vašingtonu 1994. godine, kao i postavljanje i obuhvatanje različitih jedinica za “informacijski rat”. Već godinu dana kasnije “Information warfare” postao je uzor za sve istraživačke i razvojne planove američke vojske. Avijacija i kopnena vojska su prvi postavili sopstvene stratejske predloge. Mornarica je 1995. godine postavila svoju instrukciju OPNAVINST 3430.26 za prebacivanje na informacijski rat, a u međuvremenu i marinski korpus raspolaže sa instrukcijom 3430.1 “Policy for information operations”.

6.1. Ratnici u mreži podataka

Tokom 1996. godine, stvarani su dodatni ključni dokumenti. Dva dana posle nove godine u Pentagonu, predsedavajući ujedinjenih šefova štabova predstavio je instrukciju CJCSI 3210.01 “Joint information operations policy”. Avgusta iste godine, kopnene snage su predstavile svoj novi priručnik za upotrebu na terenu, 100-6 “Information operations”, a u decembru je generalštab sastavio tajnu dopunu svoje direktive iz 1992. godine: S-3600.1 “Information operations”. Prema tada važećim predstavama američke vojske, “informacijski rat” je koncept koji obuhvata mnogo više od kompjuterskog napada. U srži sastoji se od ideje da se više ne osvajaju snage ili prostor neprijatelja, nego da se kontrolišu njegovi informacijski tokovi. Cilj je potpuna nadmoć u “informacionom polju”. Sredstva za tako nešto mogu biti i elementi psihološkog rata kao što su leci ili radioodašiljači, manevarske varke, “normalno” bombardovanje komunikacionih centara ili vodova kao i elektronski napadi. Ovako obuhvatan zahtev mogao je biti samo delimično ispunjen – previše je teško tačno poznavati jedan tuđi društveni sistem, čija tehnička infrastruktura ipak predstavlja samo jedan deo celine, i proceniti dejstva pojedinačnih intervencija u lancu. To važi do dana današnjeg, kao što je i jasno prepoznatljivo u aktuelnoj praksi. Vojno premeštanje u oblik “Command and control warfare”, čija je vojna doktrina takođe predstavljena 1996. godine, cilja dakle, na stari način, pre svega na uništenje komunikacionih infrastruktura neprijatelja, da bi borbene jedinice bile odsečene od

“glave” u komandnim centrima. Ovo je već isprobano u Zalivskom ratu 1991. godine: prvi irački ciljevi koje je SAD napala bili su repetitori, antene, telefonske centrale, mostovi kroz koje su prolazili komunikacioni kablovi. Mnoge iračke jedinice su na taj način bile odsečene od nivoa komande i postale su nesposobne za dejstvo. Dodatno su još bili napadnuti i irački komandni bunker. Konkretni naponi američke vojske, što se tiče ovog polja, do sredine 1990-tih godina usmerili su se, pre svega, na to da od hacker-skih napada kao i od protivnikovog prodiranja brane sopstvene informacijske mreže, senzore i komandne sisteme. Prioritet dobija ponovno uspostavljanje sistema u slučaju napada, pa je razvoj vojnog software-a bio usmeren ka tom cilju. Ovo s jedne strane ima i smisla, jer pre nego što se prodre u tuđe kompjutere da bi ih se pokvarilo ili uništilo, trebalo bi se temeljno zaštititi od kontraudara. S druge strane, generalna politika Klintonove administracije reflektuje upravo ovo težište, jer ona se od 1996. godine bavila sistematskom zaštitom američke infrastrukture od hacker-skih napada. U pozadini i pod velom stroge tajne, u oružanim snagama, započelo se sistematičnije s razvojem ofanzivnih koncepata. Prvi put je u direktivi S-3600.1 upotrebljen novi pojam “Napad na kompjuterske mreže” (Computer Network Attack-CNA). Ti napadi obuhvataju “operacije za prekid, odbijanje, oštećenje ili uništenje informacija koje se nalaze u računarima ili mrežama ili čak i samih kompjutera i mreža”. Do kraja 1990-tih godina, tekao je ovaj razvoj u tišini i osamljenosti vojnih tajnih službi kao i u istraživačkim laboratorijama, a pripadnicima oružanih snaga je još 1998. godine bilo zabranjeno da pojam “Ofanzivne kompjuterske operacije” koriste u javnosti. I u Kongresu se o programima nije otvoreno diskutovalo. Prilikom jednog saslušavanja u Senatu u vezi defanzivne strane informacijskog rata u junu 1998. godine, direktor CIA Džordž Tenet (George Tannet) je na pitanje da li su razvijane ofanzivne mogućnosti, odgovorio jednom rečenicom: “Mi uzimamo odgovornost za naš posao vrlo ozbiljno”. Istovremeno je i javna debata koja je vođena na website-u Vina Švartaua (Win Schwartau), www.infowar.com, bila u stvari niz popularnih objavljivanja, a različiti konceptualni članci iz stručnih vojnih časopisa kao i nekih reportaža iz štampe otišli su tako daleko da Pentagon više nije mogao da se drži politike čuvanja tajne. Takva politika je takođe sprečavala da komandanti borbenih jedinica mogu sebi predstaviti tačnu sliku kakve instrumente će u ovom novom polju imati na raspolaganju i kako da postupaju u svojim planovima primene. Objedinjeni šefovi štaba su već 1997.godine napravili brošuru za vojsku u kojoj je između ostalog pisalo: “Informacijski rat će biti primenjen na i u svim fazama i u celokupnom polju vojnih operacija i na svakom nivou vođenja rata”. Ovo prilično uopšteno uputstvo zahtevalo je jedno jasnije objašnjenje za komandante, pogotovu što su oni bili naviknuti na jasne operativne procedure. Ta objašnjenja predstavio je 9. oktobra 1998. godine, predsedavajući u generalštabu Henri Šelton (Henry Shelton) u obliku vojne doktrine JP 3-13 “Information operations”. Pored odbrane sopstvenih informacionih sistema i načina sprovođenja uputstvo opisuje “ofanzivne informacijske operacije” i koji se ciljevi biraju na strateškom ili taktičkom nivou, kakva je struktura organizacije i lanac komandovanja i način obaveštavanja o uspesima operacija. Uprkos sveopšte javnosti u vezi teme “informacijskih operacija” u američkim vojnim snagama, u oblasti kompjuterskih napada pretežno još uvek vlada tišina. Koje su tehnike na raspolaganju američkim cyber-ratnicima, e, to je najstrožija tajna. U “Joint doctrine for information operations”, u drugom tomu “ofanzivne informacijske operacije”, detaljno se upućuje na druge metode kao što su vođenje psihološkog rata, varke, elektronsko vođenje rata ili medijske aktivnosti, samo za oblast “Computer network attacks” uputstvo se nalazi na tajnom aneksu A “Supplemental information operations guidance”. Ipak, iz javnih izvora se mogu izvući određeni zaključci o tome s kakvim metodama rade informacijski ratnici. Traženje cilja: kako se

mogu obuhvatiti sve datoteke ove planete Najveći izazov u kompjuterskom ratu sastoji se u tome da se sakupi što više informacija i podataka o informacionom sistemu protivnika. To se radi uobičajenim načinom: špijunažom, elektronskim nadzorom telekomunikacija drugih država (signals intelligence) i procenom javnih izvora. Tu se nalazi i tesna povezanost sa tehnikama vođenja elektronskog rata. I ovde se ubacuju elektromagnetni signali u sisteme potencijalnog protivnika (electronic probing) da bi se dobile informacije o tome kako one funkcionišu . Air Force Information Warfare Center (AFIWC) radi takve procene u okviru projekta “sensor harvest”. Iznad svega toga neguje se oblast “funkcionalne mreže” u integrisanoj banci podataka u Pentagonu pod imenom “Constant web”, koja snabdeva podacima borbene trupe informacijama o komandnim mestima i mrežama neprijatelja. Za izabrane države se ovde identifikuju kritična čvorišta njihovih mreža i infrastrukture. A National Air Intelligence Center ima banke podataka o telekomunikacionim mrežama različitih država, National security Agency (NSA) održava jednu opširnu “adversaries” banku podataka i Joint Warfare Analysis Center bavi se takođe sličnim zadacima. Rad se često graniči sa Sizifovim poslom. Mnoge države za bezbedonosne potrebe koriste odgovarajuće kompjuterske sisteme, čiji način rada bez izvornog kôda (šifre) ne može da se otključa. Pri tome, su oni napisani u egzotičnim ili posebno razvijenim programskim jezicima. Jedan saradnik Pentagona izrazio se izuzetno tačno: “Tamo napolju (u drugim državama) postoji više od stotinu ideja za oružja informacijskog rata i ja bih rekao da za 98% od tih oružja nemamo saznanja neophodna za shvatanje sistema.” Ljudi ne mogu da kažu da neka određena zemlja koristi kompjuterski kod “X” na “Y” kompjuteru. Često su to računari napravljeni i razvijeni tamo, a software je takođe pisan u isto vreme. Pošto je veoma teško klasifikovati računarsko okruženje i detaljno ga opisati, isto je tako teško i definisati oružje koje može da se upotrebi protiv toga. Treba dodati još jednu otežavajuću stvar, da mnogi vojni i civilni ciljevi ne mogu striktno da se razdvoje. Mnoge vojne sile koriste satelitske kapacitete i kablove širokog opsega koji su iznajmljeni od strane civilnih telekomunikacionih ponuđača. Povrh svega toga, kompjuterski napadi će se vršiti ne samo protiv drugih vojnih snaga, već i protiv civilne infrastrukture, terorista ili kao kontranapad protiv cyber-napadača. Bez obzira što američke vojne snage imaju echelon-ski nadzor i tesnu saradnju sa obaveštajnim službama, one nisu u stanju da elektronski istraže sve moguće sisteme. U praksi se zbog toga ograničava opet na uobičajene sumnjivce: moguća vojna konkurencija, “banditske države” ili međunarodni teroristi. Čak i hacker-ski aktivisti mogu predstavljati izazov: kada je 1998. godine Electronic Disturbance Theater (EDT) protesta radi hteo da zauzme website Pentagona (jer je Pentagon podržao Meksičku vladu u intervenciji protiv pobune Čiapasa), hacker-i Defense Information System Agency su uzvratili udarac: oni su na website ugradili jedan Java-applet, koji je omogućio da se sruši Floodnet-Tool koji je koristio EDT, a time i web browser. Izbor ciljeva za napad i odgovarajućeg oružja sada više nije tehnički problem. Pošto ovakav način vođenja rata ne može da se poredi sa klasičnom tenkovskom bitkom ili strateškim bombardovanjem, komandantima nedostaje praktično iskustvo, koje im može pomoći u odlučivanju između obične bombe i cyber-napada. Otuda je Air Force Information Warfare Center (AFIWC) razvio niz simulacijskih potpora za informacijski rat, a korišćen je za obuku od strane 39. Information Operations Squadrona iz Hulburta na Floridi. Na takvom školovanju učestvuju, na primer, i članovi štaba iz Combined Air Operations Center-a iz Vičence u Italiji, a oni i dan danas vode NATO operacije na Balkanu. Pošto uspesi nekog cyber-napada ne mogu da se snime iz aviona ili sa satelita (da bi se video krater od bombe), AFIWC radi na razvoju sistema koji bi upravo te efekte mogli da vizualizuju. Jedan od tih sistema je SIMDAS, koji

omogućuje vrhovnom komandantu da prezentuje posledice cyber-napada, kao “hard kill” mere. Koristi se i u Joint Information Operations Center 5 (JOIC), a on se nalazi kao i AFIWC-u vazdušnoj bazi Kelly, San Antonio, u Teksasu. A i Naval Information Warfare Activity (NIWA) čija je centrala u NSA u Fort Meade u Merilendu, razvija jedan sistem za simulaciju i planiranje za pomoć komandirima na terenu pri napadu na komandne sisteme protivnika. Različite jedinice razvijaju i naprednije alate s kojima se automatski pravi spisak ciljeva za napad, a sistem planiranja vazdušnih snaga treba da bude gotov do kraja godine. Ovaj razvoj nosi sa sobom i određene probleme, jer ako se ne samo rat prebacuje u cyber-prostor, nego se sprovodi i implementacija software-a, onda se vrlo brzo može podleći fascinaciji novih tehnologija i mogu se iz vida izgubiti realni-stvarni i politički ciljevi rata. U krajnjem slučaju, u svakom ratu još uvek se radi samo o tome da se zauzme teritorija i da se tamošnjim vladarima ili narodu nametne svoja volja, a za tako nešto nije dovoljan cyber-rat, iako njegove apologete crtaju najlepše vizije o “elektronskom ratu bez krvi”. Cyber-napadi još uvek važe kao vrlo riskantno oružje, i to ne samo zbog toga što se ne mogu proceniti domino-efekti napadnutih sistema te na taj način napad na vojni sistem takvim okolnostima uvlači i štetu u civilnom sektoru, nego i zbog toga što se onda stvaraju međunarodni presedani. Upravo zbog toga, svaki pojedinačni kompjuterski napad mora da odobri predsednik SAD-a, i oni se izvode samostalno, bez saglasnosti saveznika iz NATO-a. Proći će još vremena dok cyber-oružje postane standardni element Air Tasking Order-a koji u svakom pojedinačnom slučaju određuje spisak ciljeva za napad. Oružja cyber-rata Koja su to uopšte oružja kojim su opremljeni američki cyber-ratnici? Pentagon ocenjuje napade na kompjuterske mreže kao “pasivne prislušne napade” (posmatranje – monitoring mreže ili dekodiranje), “insajderski napad” (slučajni ili namerni), kao i “hardware/ software distributivni napadi” (zlonamerna modifikacija sistema kod proizvođača ili u distribuciji) . Od tih stvari “prisluškivanje” i “insajder” već su davno poznati. Prislušne aktivnosti NSA, preko Echelon-skog sistema su opštepoznate i to po celom svetu, ali spadaju u značajno niži nivo ispod klasične špijunaže. Ubačeni agenti su stari način rada obaveštajnih službi, svejedno da li snimaju mikrokamerama tajna dokumenta ili to čine autorizovanim lozinkama. Otuda su pre svega interesantni “napadi na mrežu” i “distribicioni napadi”. Ovi drugi se sprovode u okviru standardizacija pravila, izvoznih kontrola ili preko tesne praktične saradnje između američkih kompjuterskih firmi i NSA, i u toj fazi se ne mogu opsluživati tj. reagovati. Ali, kako je i primećeno, oni su bili razlog za masovno korišćenje Open Source sistema kako u Rusiji i Kini, tako i u nekim evropskim državama. Uбудuće će se reagovati adekvatno pre svega na napade na mrežu (zovu ih još “hacker-sko vođenje rata”). Sredstva za to su raznovrsna, i crack-eri i hacker-i ih koriste često u civilnom sektoru: Virusi koji se kače na druge programe, “crvi” koji se sami šire, trojanski konji kao normalan program aktiviraju u pozadini neželjene aktivnosti, logičke bombe koje se mogu aktivirati sa velike udaljenosti. Tome možemo još dodati razne kôdove i pomoćne programe koji služe za savladavanje sigurnosnih prepreka neke kompjuterske mreže. Još jedna od mogućnosti su i Denial-of-service napadi, koji tako izbombarduje kompjuter upitima, da ne može da vrši svoju ulogu ili da se blokira mrežni opseg.

6.2. Odbrana od Američkog kriminala

NSA, koja je zadužena i za sigurnost i bezbednost kompjuterskih sistema nacionalnog bezbedonosnog aparata SAD, veoma pažljivo motri hacker-ske aktivnosti širom sveta i u toku je sa najnovijim alatima i trikovima. National Security Incident Response Center (NSIRC), koji je smešten u NSA, stvara centralnu banku podataka sa informacijama o problemima sa bezbednošću kompjutera. A njihov ogranak, Network Intrusion Analysis Capability, ima zadatak da “svoje mušterije” snabdeva sa detaljnim znanjem o hacker-skim tehnikama. Zvanično, ovo služi samo za odbranu od napada, ali to znanje se može naravno upotrebiti i u ofanzivnom smislu. Nije slučajno da borbene jedinice koje se bave informacijskim ratom imaju veoma bliske odnose sa NSA ili su čak tamo i smeštene. U NSA, od 1997. godine postoji Information Operations Technical Center (IOTC) u kojem specijalni ogranci iz tajnih službi i borbenih jedinica rade zajednički: P42 – Information Warfare Support Cell NSA-a, Critical Defense Technologies Division CIA-e i ogranak Pentagona J-33 “Special technology Operations”. J-33 upravlja sa desetinama “crnih programa” američke vojske i oprema specijalne timove za tajne operacije. Mora se poći od toga da su kompjuterski stručnjaci NSA-a u stanju da sa standardnim metodama hacker-ske scene izvrše kompjuterske upade na svim dostupnim mrežama. A ono što ove upade čini mnogo žešćim od upada hobi hacker-a su unutrašnji resursi koji za ovako nešto stoje na raspolaganju. Sakupljeno znanje o svim poznatim rupama u sigurnosnim sistemima povezano sa tehničkim informacijama o svim svetskim komunikacionim sistemima iz “Constant Web”-a – banke podataka, ogromnim mogućnostima njihovih računara za testove lozinki i otključavanja kao i odgovarajućim brojem osoblja, čini da je NSA daleko opasnija od “Script Kiddies”-a koji se prave važni, a njih obično političari koji nemaju pojma navode kao pretnju za nacionalnu bezbednost. Pored toga poznato je da je američka vojska već od kraja 1980-tih godina učestvovala u istraživanju i razvoju kompjuterskih virusa. Takve, više brutalne metode da se ometa neprijateljski kompjuterski sistem danas se ne uzimaju kao ozbiljni načini upotrebe, isto kao i “crvi” ili DOS napadi. Cilj cyber-ratnika je da se prodire u mreže, a da se to uopšte i ne primeti. Virusi i “crvi” su skoro neupotrebljivi u vojnom smislu, jer se njihovo širenje može vrlo teško ograničiti. Tome još treba dodati da je i imidž cyber-rata kao nekontrolisanog elektronskog pustošenja do sada suzdržavao komandante i političare da se takve mere odobre u većem obimu. Zbog toga su cyber-ratnici usmereni na to da svoje tehnologije predstave kao veoma precizno oružje. “Kada se diskutuje o vođenju rata u kompjuterskim mrežama, može se izleteti iz koloseka i razgovarati o virusima, “crvima” i programima koji se sami šire i svako misli da je to nešto kao oružje za masovno uništavanje i to bez ograničenja” – kaže pukovnik Dejvid Kirk (David Kirk), vršilac dužnosti komandanta Joint Operations Center-a. Premda se, za svaki slučaj, ovakvi scenariji takođe planiraju. Po izjavama saradnika iz Pentagona, kompletan ispad mrežnih sistema jedne države (koju bi prouzrokovale SAD), može da služi u jednoj zaoštrenoј kriznoj situaciji kao hitac upozorenja da se ta država ukroti. Pošto su cyber-napadi mere sa specijalnom tehnologijom, moraju se posebno odobravati. To znači da se moraju unapred davati podaci o ciljevima, sredstvima i eventualnoj kolateralnoj šteti. “Nacionalni zapovednici žele da budu sigurni da je sistem ili čvorište mreže tačno identifikovano” (onaj protiv koga se želi upotrebiti takva tehnologija), kaže pukovnik Kirk. Cilj tadašnjeg razvoja je da cyber-ratnici mogu u sledećih nekoliko godina da kažu svojim komandantima: “Mogu vam sa visokim stepenom sigurnosti reći da je rizik kolateralne štete X, da je rizik otkrivanja tehnologije Y i da je rizik za sisteme SAD-a Z”. Znači, pokušava se razviti tehnologija koja će izazvati tačno definisane efekte. Već 1997. godine u Joint Warfighter Science and Technology Plan-u, sa žaljenjem je

utvrđeno da za ofanzivni informacijski rat nedostaju pre svega još dve sposobnosti: brzo i automatski otkriti slabe tačke protivnika i fleksibilni sistemi napada koji mogu da se upotrebe protiv najrazličitijih kompjuterskih sistema. Generisan je, znači, razvoj “zalihe različitog novog oružja koje se bazira na usavršenim tehnologijama elektronski vođenog rata.” Upravo to se i do danas praktikuje. Odstranjuju se poznate tehnike vođenja elektronskog rata, pre svega ometanje odašiljača i lažna manevarska sredstva i vrše se pripreme za kompjutersko vođenje rata. Pri tome se isprobava veliki broj mogućnosti. Samo kod Information Warfare Battlelab (koji je smešten u Air Force Information Warfare Center [AFIWC] u San Antoniju), od osnivanja 1997. godine istraženo je više od 270 koncepata, a detaljnije se isprobava 37 koncepata. U Army Science and Technology Master Plan-u iz 1997. godine, poslednji koji je javno dostupan, može se naći još podataka o planiranim tehnologijama cyber-napada. U projektima koji su nazvani III.F07, III.F.09 i III.F.10 nalaze se tajne radnje za “elektronske napade na digitalnu komunikaciju”, i “napadi informacijskog rata – kao i odbrana” i “informacijski rat”. Po ovom planu, od kraja 1997. godine već postoje prototipovi s kojima se mogu izvesti napadi na postojeće komercijalne mreže, a od 1999. godine (američka) vojska je navodno u stanju da prekine i sve ostale komercijalne mreže. Do 2002. godine žele da budu u mogućnosti da tačno izabrana polja informacionog sistema potpuno onesposobe ili da ih ometaju, a do 2003. godine treba da bude moguće da se izvrši ciljani uticaj manevrima elektronske obmane i manipulacije podataka. Tek od 2004. godine očekuju se tehnologije koje će moći elektronski da unište informacione sisteme. Kako kaže Joint Warfighter and Science Technology Plan, tada treba da budu u pripravnosti sistemi za vođenje “integrisanog ofanzivnog informacijskog rata”. To sve izgleda veoma sporo, kada se posmatraju ti tako punim ustima izgovoreni info-rat govori, članci, knjige, strateški papiri jer oni se sastavljaju već deset godina. Brigadni general Džon Bejker (John B. Baker), nekada direktor Air Interlligence Agency i šef Joint Information Operations Center-a je još 1999. godine rekao: “Ako se radi o tome da pored čistog prisluškivanja prenosa podataka, manipulišemo i iskoristimo 'nule i jedinice' (onda je pred nama još dug put)”. Ali, ne treba da se zaboravi da se baš na napadima na informacijske mreže radi o potpuno novoj vrsti oružja i da se i drugi projekti naoružavanja delimično protežu i na 15 i više godina. Konstantan problem koji je ovde znatno oštrije izražen (u odnosu na druge projekte naoružavanja) je neverovatno brz razvoj informacione tehnologije upravo u civilnom sektoru. Jednom razvijeni ratni sistemi informacijskog rata mogu u stvarnosti da se koriste u veoma kratkom vremenskom periodu, i to pre nego što postanu neupotrebljivi zahvaljujući novim zaštitnim sistemima i upgrade-ovanju ciljeva. Sledeći problem koji može imati cyber-ratnik je da se njihove tehnike mogu koristiti u ograničenom obimu: ko je jednom bio napadnut, može da evaluiira svoje iskustvo i sa nešto stručnog znanja da se odbrani od drugog napada. Mnoga oružja za cyber-rat razvijaju se u okviru davno planirane modernizacije postojećih sistema za vođenje elektronskog rata. Srž elektronskog arsenala vazduhoplovstva (Air Force) je modifikovana verzija Lokidovog transportnog aviona C-130 “Hercules”. Specijalna verzija EC-130H sa oznakom “Compass Call” raspolaže sa tovarnim prostorom prepunim elektronike i raznim antenama s kojima se prisluškuju radio veze neprijateljskih trupa, da bi se posle evaluacije mogli ciljano uništiti. Uobičajeno je da se napravi slobodan prolaz bombarderima i to tako što se ometaju integrisani sistemi protiv-vazdušne odbrane. Srce uređaja je malo zastareli odašiljač i prijemnik sa tri modula za UHF frekvencije, jedan za VHF, jedan KY-58 satelitski sistem i dva KY-75-HF modula. Za sistematičnu primenu i protiv tehnološki visoko razvijenog neprijatelja ili protiv komercijalnih veza, sistem koji su prvobitno razvijali za analogne signale nije dovoljan. Dalji razvoj treba da ide na dva koloseka: s

jedne strane se za 2007. godinu planira Common Sensor avion koji će biti u stanju da nastupi i protiv digitalnih signala i to sistematično i da vodi zaista kibernetičke ratove iz vazduha. Projekti Information Warfare i Digital Communications Electronic Attack iz Science and Technology Master Plan-a vojske upravo se za to i izvode. Povrh toga, za elektronsko i digitalno uvođenje rata kao pojačanje treba da se koriste i bespilotne letilice koje će da presreću, automatski evaluiraju i ometaju signale protivnika. Upravljanje se vrši sa Compass Call-a ili sličnih raspoloživih aviona, kao na primer RC-7 Airborne Reconnaissance Low (ARC), RC-135V/W Rivet Joint ili RC-12 Guardrail, a njihov zadatak treba da preuzme novih 40 Common sensor sistema. Vazduhoplovstvo (US Air Force) upravo modernizuje glavni model Global Hawk, kopnene snage u istu svrhu razvijaju Tactical Unmanned Aerial Vehicle (TUAV). Još jedan dodatni modul za elektronsko vođenje rata treba da bude kompaktna stanica na terenu za prisluškivanje i elektronsko ometanje i pravljenje lažnih signala neprijatelju, a radili bi u saradnji i koordinaciji sa sistemima iz aviona. Uređaj može da stane u vozilo sa prikolicom, kao i u tovarni prostor transportnog aviona. Neki od defanzivnih sistema koji služe za zaštitu sopstvenih računara, može da se upotrebi i u ofanzivne svrhe. Air Force Information Warfare Center je razvio jedan program sa kojim se sumnjivim uljezima može staviti pečat – time bi uobičajene maskirne tehnike kao što je stalno menjanje korisničkog imena i lozinke postalo potpuno nedelotvorno. Pošto se praćenjem elektronskog traga hakera može doći do njegovog kompjutera, potrebno je pod određenim okolnostima upadati i u tuđe mreže, a onda treba da je moguće ubaciti i virus ili manipulirati podacima. Prve primene Već od sredine 1980-tih godina, američki hacker-i su pravili upade u kompjuterske mreže Varšavskog pakta. Saradnik CIA-e i NSA beleži po sopstvenim podacima – da su imali “značajne uspehe u penetraciji u tajne vojne kompjuterske sisteme Sovjetskog Saveza, kao i drugih država”. Tada se to pretežno radilo radi špijunaže. Tehnološki naponi su se tada koncentrisali na elektronsko vođenje raketa i ratnih aviona. U jednoj vojnoj akciji, prvi put su primenjeni kompjuterski upadi u okviru Uphold Democracy na Haitiu 1994. godine, kada su SAD vratile na vlast oborenog predsednik Bertrana Aristida (Bertrand Aristida). Mere je tada odobrio lično predsednik Klinton (Clinton). Posle toga je izvedeno nekoliko “relativno beznačajnih” kompjuterskih napada – barem po priči pripadnika američke vojske Washington Post-u. Mnogi od njih su služili pre svega kao nadzor nad protokom informacija protivnika. U mnogim drugim slučajevima stizali su predlozi od Pentagonovog odeljenja za “specijalne tehničke operacije” i razvijani su za ministra odbrane i predsednika. Ali, proces odobravanja je trajao tako dugo da više nisu mogli biti upotrebljavani. Rat NATO-a protiv Srbije za Kosovo se smatra, i to višestruko kao prvi pravi cyber-rat. Ovaj naziv je dobio pre svega zbog jakog učesća hacker-ske scene na obe strane, i to pre svega kao psihološke i političke rasprave na internetu. Često su crack-ovani website-ovi i punjeni sa podacima za ili protiv rata, a posle bombardovanja Kineske ambasade u Beogradu su se u virtualne rasprave uključili i kompjuterski frikovi iz Narodne Republike Kine. Povrh toga, izvođeni su napadi pre svega protiv NATO, Denial-of-service-attack i mail-server je bombardovan e-mail-ovima inficiranim virusima. Ali, ovo je više bila elektronska forma političkog divljaštva nego nešto što bi se nazvalo “rat”. Manje poznato je da su SAD elektronskim putem napale srpske protiv-vazdušne sisteme i to ne samo da su ih ometali, nego i ciljano manipulirali. Da bi to postigli, sa EC-130H Compass Call-a prisluškivali su visokofrekventne mikrotalasne podatke, onda su ih modifikovali i sa jakim predajnikom opet emitovali. Na kraju su operateri odbrambenih položaja na svojim monitorima videli ciljeve koji uopšte nisu postojali. Dalje, izvršen je napad na srpski telefonski sistem (fiksna mreža) da bi

prinudili komandante u Beogradu da sa svojim trupama na Kosovu komuniciraju preko mobilnih telefona, jer se mobilni telefoni lakše prisluškuju, pošto se ne mora imati direktan kontakt sa telefonskim kablovima. U Kosovskom ratu su se pokazali i problemi koje američka vojska još uvek ima sa vođenjem cyber-rata: strogo poverljiva operacija bila je još ranije pripremljena od strane Joint Information Warfare Center-a u saradnji sa komandantima u Evropi i to još onda kada su se događaji na Balkanu počeli zaoštrevati. Politička dvoumljenja sprečila su primenu odmah pri početku rata 24. marta, a odobrenje iz Vašingtona je stiglo tek nešto kasnije. Kada su onda cyber-ratnici sakupili sve potrebne informacije i pripremili sisteme, bombardovanjem terena je već bilo uništeno toliko mnogo da je bilo teško proceniti koji su zaista uticaj imali cyber-napadi. Naknadne procene su došle do zaključka da se moglo postići i više da su cyber oružja korišćena sistematičnije. Ljudi iz Pentagona procenjuju da je možda iskorišćeno deset posto mogućnosti. U jednom internom izveštaju mornaričkih jedinica, a koji je procurio u štampu, tvrdilo se čak da bi rat trajao upola manje da su informacijski napadi izvođeni bolje i opsežnije. Da se u informacijskom ratu ne radi samo o napadima na vojne mreže i podatke, dokazuje i saopštenje Newsweek-a u maju 1999. godine. Navodno je Bil Klinton ovlastio CIA-u da u okviru jedne Special technical operation upadne elektronski u banke u Rusiji, na Kipru i u Grčkoj da bi ispraznio inostrane račune predsednika Jugoslavije, Slobodana Miloševića. Potpuno u suprotnosti sa do sada navedenim akcijama, koje su usmerene protiv vojne sile jedne od zaraćenih strana, u ovom slučaju su pod američkom “paljbom” bili i civilni sistemi država koje nisu učestvovala u sukobu. Čak je i NATO partner Grčka bila izložena virtualnoj ‘prijateljskoj vatri’. Čak ni NATO saveznici nisu bili uključeni u ove planove. Kasnije se ispostavilo da je ova akcija očigledno bila stopirana od strane pravnika iz američke vlade, ali po jednom izveštaju United Press International-a, Amerika je upala u skrivena konta aktuelnog omiljenog neprijatelja, Osame Bin Ladena. Pošto je tajnim službama uspelo da prozru finansijsku mrežu islamističkog milionera, američki hacker-i su mogli da upadnu na račune i da preusmere novac ili da ugase račun. “Tri klika na tastaturi i nema ga” – rekao je jedan američki službenik UPI-u. Da li nečega ima u ovoj priči – treba sumnjati, jer postoje tesne veze između UPI i mračne sigurnosne firme iDefense-a koja je firma u direktnom podređenom položaju u odnosu na NSA i Pentagon. Džejms Adams (James Adams), bivši šef UPI-a, a danas direktor iDefense-a, više puta je javno prozvan zbog pogrešnih informacija. Po izjavama Chaos Computer Club-a, tehnički je moguće preko međunarodnog bankarskog sistema falsifikovati SWIFT doznake. Tajne službe kao što je NSA su u stanju to da izvedu. U svakom slučaju, priča skreće pažnju na realnu opasnost: cyber-napadi ne mogu se više nadzirati od strane parlamenta i javnosti kao što je slučaj sa normalnim ratovima, i civilni ciljevi su svakako predviđeni u ofanzivnim američkim doktrinama. Članovi odbora tajne službe Senata i predstavničkog doma SAD-a koji su na tajnoj sednici bili informisani o virtualnim napadima CIA-e na bankovne račune Miloševića, takođe su izrazili zabrinutost. Takva akcija protiv inostranih banaka ne da je prekršila mnoge međunarodne ugovore, nego bi mogla i ugroziti vodeću ulogu SAD-a u svetskom bankarskom poslovanju. Takođe, ovaj slučaj kršenja suvereniteta čak i savezničkih država je jedan opasan presedan i prosto poziva da se imitira, znači da se napadnu američke banke. Uostalom, SAD bi jednog hacker-a, koji bi pokušao nešto slično kod neke njujorške banke, označila kao cyber-teroristu. Problemi prihvatanja i problemi kadrova Izvan takvih spektakularnih pojedinačnih akcija, integracija cyber-ratnih planova u normalna vojna dejstva veoma sporo napreduje. Spomenuti Kosovo-breafing mornarice bio je interesantan jer je navodio i uzroke. Autor je opisao osoblje Information Operations Cell-a kao “vanredne ljude” ali je dopunio: “Imali su suviše male činove

i dolazili su iz pogrešnog miljea i nisu imali dovoljan uticaj na planiranje i sprovođenje akcija, kakav su trebali da imaju.” Za mnoge komandante su i sopstveni hacker-i još uvek jedna sumnjiva grupa koja sa uobičajenim fizičkim opterećenjem vođenja rata nema mnogo zajedničkog. Vođenje rata sa klikovima na mišu ili sa bespilotnim letilicama i bez realnog oružja za vojsku koja obožava heroje, telesnu disciplinu i angažovanje sopstvenog tela, još uvek je neuobičajena ako ne i neprijatna stvar. To što poreklo vođenja cyber-rata vodi iz tajnog aparata izviđačkih jedinica, takođe ne doprinosi tome da se informacijsko oružje posmatra kao još jedno “oružje sa police” kako je to rado formulisao general Ričard Majers (Richard Myers) koji je vodio odeljenje za kompjutersko vođenje rata u Space Command-u. Često su planovi za napad sa konvencionalnim oružjem već bili spremni, kada se neko seti i vojaka za informacijski napad, i da bi se i oni mogli nešto pitati. Tako se žale mnogi vojnici zaduženi za cyber-rat. Veliki deo posla u Air Force Information Warfare Center-u sastoji se sada u tome da unutar trupa propagiraju svoj know-how i njegove tehnologije. Za sada još uvek nedostaju jasne smernice delovanja za cyber-napade. Jer one do danas spadaju u nedovoljno precizno definisan prostor “informacionih operacija”, a planeri Pentagona imaju puno teškoća da postave uslove i pravila postupanja za takve intervencije. Svaki scenario, koji bi eventualno zahtevao upotrebu cyber-oružja, mora biti posebno razvijen i isto tako odobren. Sada se pravnici američke vojske bave time da li, i pod kojim okolnostima pravo naroda tako nešto uopšte dozvoljava. Paralelno s tim radi se na opsežnoj vojnoj strategiji za informacijski rat – Oplan 3600. Termin za završetak nije postavljen. Još jedan problem koji stalno pritiska je i nedostatak kadrova. Pentagonu nedostaju na svakom koraku kompjuterski eksperti, jer oni nalaze višestruko primamljivije poslove u privatnom sektoru. Neki ipak idu i drugim putem, jer cene radno vreme koje je regulisanije nego u Silikonskoj dolini ili podlegnu iskušenju da upadaju u tuđe računare a da pri tome ne budu zakonski gonjeni. Ali, to nije dovoljno da se pokrije potreba u ovoj oblasti. Vojsku jednim delom napuštaju i software-aši jer njihove ideje u škrtom aparatu često nailaze na zid. Jedan od primera je i Wheel Group koja danas pripada mrežnom gigantu Cisco Systems. Osnovali su je visokokvalifikovani kompjuterski eksperti Air Force Information Warfare Center-a (AFIWC), koji je 1998. godine vodio istragu kada su britanski hacker-i izvršili upade u Air Force Rome Laboratories i u Air Force Materiel Command. Tada su razvili “netsnifera” i nazvali ga “NetRanger”. Ovaj se nije dopao AFIWC-u, jer je tamo jedan drugi proizvod smatran za pravu stvar, i onda su kompjuterski frikovi napustili Air Force, tj. avijaciju i osnovali svoju firmu. A komercijalno rasprostranjen “NetRanger”, kasnije je koristio čak i od 609th Information Warfare Squadron. Da bi popravio ionako malobrojno osoblje u IT sektoru, Pentagon je u decembru 2000. godine počeo da poziva rezerviste sa kompjuterskim znanjem. Ukupno pet planiranih timova, takozvani Joint Reserve Information Operations and Informations Assurance Organizations treba između ostalog da budu upotrebljeni za sigurnost – bezbednost sopstvenih mreža kod operacija prisluškivanja ali i u svrhu kompjuterskih napada. Do 2007. godine treba da bude postavljeno 600 ljudi koji bi čak i u part-time aranžmanu radili za NSA ili Joint Information Operations Center. Da bi se zaobišla kratkotrajna uska grla, Pentagon je bio prinuđen da pojačano angažuje privatne firme. A tako nešto opet povećava troškove. Naravno da se mnoge firme motaju između mrežne zaštite, studije rizika, analiza i kompjuterskih napada, koji su de facto cyber-plaćenici za hacker-ske ratove SAD-a. Na primer, firma Sytex Inc. pomaže pri “analizi, pripremi i podeli podataka o informacijama relevantnih za cyber-rat” – jasno je rečeno, to znači: saradnja pri izboru ciljeva – meta za napad.

6.3.Digitalne slobodne ruke

Pretty Good Privacy (PGP) Sve ono što korisnici ne žele da saopšte dopisnicom nego stavljaju u koverat, trebalo bi da kôdiraju i na internetu, jer e-mail “protrči” kroz mnogo računara dok ne stigne na računar primaoca. Poruka se može pročitati na svakom od tih usputnih računara, a i sadržaj se može izmeniti tako da to ne primete ni pošiljaoc ni primalac. PGP kao program za kôdiranje i dekôdiranje je u ponudi, i to za skoro sve vrste računara, i što je bitno, besplatan je za privatnu upotrebu. Skraćenica PGP znači “Prilično dobra privatnost”. Ovaj software za kôdiranje i dekodiranje važi već godinama kao de facto standard za sigurnu komunikaciju na internetu, a i pomogao je da se probije američka zabrana kripto izvoza. Kod je izvezen preko knjiga i u Evropi je mukotrpno opet uskeniran, jer izvoz knjiga nije bio zabranjen. Policija i tajne službe još uvek ne mogu da “prisluškuju” PGP kôdirane mailove, pod pretpostavkom da ga korisnik ispravno koristi. Napad na poslednji kompjuter bi bio moguć velikom “strategijom prisluškivanja” i mogao bi da da pozitivan rezultat, jer se na matičnoj ploči nalazi tajni kôd. “Islednici” tada moraju samo da nađu tajnu lozinku. U međuvremenu postoji mnogo vezija PGP-a. Kritički raspoloženi stručnjaci preporučuju spartansku (osnovnu) verziju PGP-a 2.6.3. Taj program je besplatan na internetu zajedno sa grafičkom platformom kao mail PGP program (za Windows 95, 98, NT). Svejedno je koja se verzija koristi, tokom prvog koraka se automatski stvara jedan par kôdova. Kasnije se mogu stvarati dodatni kôdovi. Mora se izabrati kojim kriptografskim principom će se proizvesti kôd (ključ): RSA ili Diffie hellmann DSS. Korisnici 2.6x verzije mogu koristiti samo RSA kôdove (ključeve). Korisnici novijih verzija biraju po pravilu Diffie Hellmann DSS, jer se ovde mogu napraviti duži, a samim tim i sigurniji ključevi: na primer, jedan par RSA kôdova od 2048 BIT-a sa neograničenim trajanjem, a i jedan drugi par koji će biti validan samo dva meseca. Ovakve stvari povećavaju sigurnost. Onda se unosi kôdirana fraza, tj. tajna lozinka. Najsigurnija opcija je upotreba izmišljenog reda brojeva i slova. Minimum je osam znakova, i bilo bi preporučljivo da mogu da se pamte (bez pisanja na papiriću), jer ti znakovi moraju da se upišu prilikom dekôdiranja. Na kraju se par kodova generiše. Na sporim računarima ovaj postupak može trajati nekoliko minuta. Posle se javni kôd klikom na miša može poslati na internet, na jedan od takozvanih key servera. To su banke podataka u kojima se nalazi veliki broj javnih kodova (ključeva) i odatle se isti mogu koristiti. Po pravilu, računari međusobno razmenjuju ključeve ili se taj ključ eksportuje klikom na miša u jednu datoteku koja se može poslati i mail partneru ili se može javno staviti na raspolaganje na svom homepage-u. Kôdiranje principijelno funkcioniše tako da mail partner ima jedan par kodova iz javnog dela, a takođe poseduje i tajni kôd. Sa javnim kodom se poslati mail kodira, a primalac može da ga dekôdira samo uz pomoć tajnog ključa. Kodirati se mogu čitave datoteke kao i pojedini delovi teksta. Uz pomoć PGP-alata mogu se izabrati odgovarajuće datoteke. Dekôdiranje funkcioniše vrlo slično. Postoje takođe programi koji tajne kôdove memorišu na matičnoj ploči. Tako na primer postoji makro program koji se nalazi u Word dokumentima, koji ove kôdove pokušava da pošalje preko interneta. Sa napadačkim programima “Back Orifice” ili “Netbus” može se lako prisluškivati datoteka u kojoj je memorisan tajni kôd, iako je kôdirana i zaštićena lozinkom. Pre svega se jednostavne lozinke lako mogu provaliti automatskim isprobavanjem. Znači, preporučljivo je datoteku sa tajnim kôdom memorisati na disketu, a ne na matičnu ploču. Još sigurnije bi bilo tajne kôdove memorisati na čip karticu ili na neku sigurnu pokretnu spravicu. Remailer Mix-računari koji isključivo anonimizuju e-mail poruke zovu se remailer-i. Preko

jednog remailer-a moguće je poslati poruku u neku usenet grupu ili nekome lično poslati mail, a da primalac ne zna ime ili adresu pošiljaoca. Luc Donerhake (Lutz Donnerhacke) je donedavno u Jeni imao remailer , ali ga je zbog prevelikog opterećenja deaktivirao. Pseudoanonimni (takozvani anonimni) remailer-i su skoro iščezli sa interneta, oni anonimizuju poruke tako što jednostavno izmene ime i adresu i stave neku drugu adresu i ime. Pozitivno je bilo to što se preko ovih remailer-a mogao slati i odgovor (koji je i stizao). Negativno je to što su kod ovih remailer-a pravo ime i pseudonim bili na jednom mestu. Godine 1996., sajentologija je sudskim nalogom dobila pravo da prisvoji protokolne podatke finskog remailer-a "Penet". Navodno se jedan "Penet"-ov korisnik negativno izrazio o sajentolozima, naravno sa njihove tačke gledišta, i preko remailer-a je slao poruke u Usenet. Ali, na ovaj način policija je dobila i identitete ostalih 700.000 korisnika "Penet"-a. Potom je vlasnik Johan Helsingius zatvorio svoj remailer. Za zaista anonimne remailer-e postoje danas dva tehnička koncepta: oni koji koriste Cypherpunk remailer – koriste PGP, a Mixmaster remailer Lensa Kotrela (Lance Cottrel) koristi specijalno razvijen format za anonimizovanje. Sadržaji e-mail-ova se šifruju sa triple-DES. Paket header kao i triple-DES kod kôdiraju se RSA algoritmom. U međuvremenu postoje e-mail klijenti ili mixmaster frontends za anonimno slanje email-ova. Sa obe tehnologije rade "Private Idaho" i "Jack B.Nymble" na Windows-ima. Oba pretpostavljaju da je korisnik instalirao PGP, ali i na World Wide Web-u postoje neki homepage-ovi preko kojih se može direktno, uz pomoć Cypherpunk-a ili Mixmaster-a slati e-mail. Takav je, na primer, remailer projekat Orange . Pozitivno je ovde to što korisnik može sam da odredi preko kojih remailer-a će poslati svoj e-mail. Onda može i da proceni koliko vremena treba e-mail-u da stigne kod primaoca. Safeweb Software "Safeweb" kôdira kompletan web saobraćaj i na taj način štiti ličnu razmenu podataka. Engleski guru za zaštitu podataka, Sajmon Dejvis (Simon Davies), je entuzijasta što se tiče Safeweb-a: "Ova vrsta besplatnog software-a, kao i hushmail ili Freedom mreža poništiće sve napore vlasti". Treba napomenuti da saobraćaj ide samo preko računara Safeweb-a. Eksperti kritikuju da se na taj način nudi jedan jedini cilj u slučaju napada. Neke vladine službe mogu da se sprijatelje sa ovakvim software-skim alatima. Pre svega špijuni su tradicionalno uvek cenili što veću anonimnost: u jesen 2000. godine je služba anonimiranja stupila u savez sa američkom tajnom službom CIA. Pre dve godine uprava je pokrenula svoj rizični kapital u Q-tel firmi, da bi pretražila ove službe za anonimizovanje. Sada hoće i CIA da koristi Safeweb, da bi mogla da prikrije sopstvene aktivnosti na internetu. Za mnoge korisnike saradnja sa CIA-om nije baš potez koji uliva poverenje. Čak i 34-godišnjem šefu Safeweb-a Stivenu Hsu (Stephen Hsu) jasno je da će imati pad od 5% i to od najparanoidnijih korisnika, a doprinos Safeweb-a treba da se sastoji samo u tome da upravi obezbedi odgovarajući software. Sama CIA nije imala pristup web kompjuterima firme ili načinu rada software-a. Tehnologija koja se koristi u Safeweb-u zove se Triangle Boy. Svaki PC računar s tim može da se pretvori u jednu vrstu web servera, tako da korisnici mogu da posećuju web stranice a da ne ostavljaju tragove. Zahtev za željenim website-om se prosleđuje na website Safeweb-a i onda se uspostavlja veza. CIA je mogla da prikrije tragove ne samo u internet surf-ovanju, nego je mogla da uspostavi sigurne komunikacione veze za svoje ljude tako da su mogli bezbedno da komuniciraju sa CIA sedištem. Safeweb tehnologija je veoma zgodna i za neidentifikovano slanje poruka u druge države. Upravo ovu namenu je imao umu i Stiven Hsu kada je prošle godine kontaktirao CIA-u. Naravno, na ovaj način nisu slate samo propagandne poruke, nego su započeti i cyber-napadi, a da se ne otkrije odakle dolaze. Moglo bi se sada spekulisati o tome da li je pravi interes CIA-e bio da se crack-uje Triangle Boy i da se kompromituje njegova upotreba u javnosti. Ipak ovakve tehnike kao i

kriptografske metode otežavaju pravu delatnost tajnih službi: elektronsku proveru podataka. Međutim, bila bi dovoljna jedna presuda da se istražiteljima dozvoli pristup računarima koji vrše anonimizovanje. Naime, vlasnici tih računara vrlo verovatno mogu da dodele komunikaciji pojedinačnim korisnicima. Anonymizer Vrlo sličan Safeweb-u i veoma poznat je Anonymizer. Jednostavnim otvaranjem website-a u koji korisnik ubacuje jednu internet adresu, mogu da se anonimno koriste druge web stranice. Anonymizer radi kao običan proxy server. Ali odstranjuje sve lične informacije, kao i cookie ili IP adrese iz header-a web-upitnika . Ali, Anonymizer ne radi kao Safeweb sa više računara. Dovoljan je pristup na Anonymizer-ov računar da bi se došlo do korisnika. Ne postoji tehnička sigurnost. Korisnik mora verovati da Anonymizer neće sakupljati interesantne podatke. Napadač bi mogao da “presluša” komunikaciju između Anonymizer-ovog računara i korisnika i mogao bi čak da napravi analizu razmene podataka. Brzina konekcije je nešto sporija, ali kod brzih internet veza se to ne primeti. Crowds Ovaj projekat je prvi put predstavljen u leto 1997. godine. Suština ovog projekta je da se tragovi korisnika sakriju u World Wide Web-u. Tragovi pojedinca mešaju se s tragovima gomile korisnika: korisnik se pomeša u mnoštvo korisnika, a njegov prestup na neki web server dodeljuje se slučajnim odabirom nekog iz mnoštva, a ovaj onda može da prosledi pristup direktno na željeni server ili na nekog drugog slučajno izabranog iz mnoštva. Kada je pristup ostvaren, onda se prenosi preko slučajno izabranog člana iz mnoštva. Server polazi od toga da ima posla sa članom koji je želeo pristup. Navodno ni članovi mnoštva ne mogu da identifikuju onog koji je tražio pristup. Eksperti kritikuju da član mnoštva može da se smatra kao pošiljalac, s druge strane taj isti član s dobrim razlogom može uvek to porekne . Napadači ne mogu da “prisluškuju” podatke, jer su pristupi kôdirani simetričnim kriptosistemom. Ako napadač pravi analizu razmene podataka, kôdirani podaci se mogu povezati i posmatrati. Bez obzira na pozitivan izveštaj američke štampe o projektu, on se nije pokazao uspešnim. Do početka 2000. godine retko se koristi. Američke kripto-eksportne kontrole sprečavale su da se može u potpunosti koristiti i u Evropi. Ali i onda je bilo problema da se Crowds izvozi. Do danas nije dobilo značajnu podršku. Kod Crowds-a se pristup kanališe preko više računara – i u tome je njegova prednost. Na taj način Crowds preuzima recept uspeha samog interneta: pre samo nekoliko godina su mnogi smatrali da internet ne može da se cenzuriše. Konačno, tako je i bio organizovan – decentralizovano, tako da bi mogla opstati komunikacija između različitih tačaka i u slučaju nuklearnog rata. Ali, ako je unifikacija unutar jednog pravnog sistema, znači jedne države, i ide samo preko jednog centralnog čvorišta, onda može da se kontroliše. U međuvremenu se javlja više pokušaja da se stvori necenzurisana mreža, u kojoj bi se podaci mogli ekontrolisano razmenjivati. Što su sistemi decentralizovaniji, to su otporniji na pokušaje manipulacije. Napster Napster je najpoznatija berza za razmenu na internetu. Omogućava korisnicima brzo i jednostavnu razmenu muzičkih file-ova (pesama) na internetu. Da li su među tim file-ovima i muzička dela koja podležu pod zaštitu autorskih prava - to pre preuzimanja od strane Bertelsmana (Bertelsmann) nije provereno. Sistem je stvoren za fer upotrebu (fair use) i ne koristi nikakve kôdove. Pošto je Bertelsman blokirao nelicencirane i pesme sa zaštićenim autorskim pravima, pao je broj korisnika sa 15,5 na 12,1 miliona, znači za 3 miliona manje. Istraživanje je izveo Jupiter Media Metrix i to na korisnicima koji su Napster klijentom razmenjivali pesme. Gnutella Gnutella je malo teža za rukovanje od Napster-a, jer radi decentralizovanije nego Napster. Kod Gnutella-e je reč o Open-Source-Software-u za razmenu podataka. To se dešava u jednoj mreži računara koji međusobom razmenjuju razne pretrage. Kada korisnik pokrene pretragu, ona se sprovodi dalje na sve priključene računare. Zahtevi i

odgovori idu preko više računara i ne mogu se dodeliti nekoj određenoj IP adresi. Odgovori ipak sadrže IP adrese ponuđača podataka, što je preko provajdera vidljivo. Znači, anonimna razmena preko Gnutella-e nije moguća. Za Gnutella-u postoji više programa za primenu, takozvani klijenti. Tu spada Gnutella ili Toadnode za Windows, Mactella za Mac, MyGnut za BeOs, Hagelslag za Unix ili Java client furi. Onion Routing Po mišljenju izuzetno kritički raspoloženog profesora informatike iz Drezdena – Andreasa Ficmana (Andreas Pfitzmann), Onion Routing je jedini prihvatljivi koncept za anonimno surf-ovanje. Može da se koristi kao Napster ili Gnutella za prenos podataka, daljinskog logovanja i druge svrhe spajanja i razmene podataka. Kod Onion Routing-a podaci se mogu uglavnom anonimno razmeniti. Više računara je zaduženo za anonimizovanje. Komunikacija je kôdirana. Analiza razmene podataka je takođe ograničena. Ali, primaocu poruke je poznata adresa pošiljaoca. Sve u svemu, Crowds štiti od jačih napadača nego Anonymizer, a Onion Routing nudi još jaču zaštitu od Crowds-a. Istraživački projekat je sponzorisan od strane ministarstva odbrane SAD i istraživačke grupe DARPA takođe iz SAD. Prototip je dokazao da koncept funkcioniše. U fazi testiranja, mreža je bila ostvarena u proseku sa 50.000 poseta dnevno. Do početka 2000. godine nije bio dozvoljen izvoz software-a iz SAD koji sadrži kriptografske elemente. Od 28.01.2000. godine, prototip je offline i čeka na primenu. U inostranstvo, pak, ne treba da se izvozi zbog vojnog porekla. A ipak je Ulf Moler (Ulf Möller) na univerzitetu u Hamburgu iskopirao prototip. Kod Onion Routing-a, browser pravi konekciju sa prvim Onion Routing proxy serverom. Onda taj (proxy server) pravi anonimnu rutu, tj. konekciju kroz različite Onion Router-e sve do željenog servera. A pri svemu tome samo jedan Onion Router zna put do sledećeg servera. Pre nego što se podaci pošalju, oni se višestruko kôdiraju. Kôdiranje se sprovodi u slojevima oko podataka, pri tom svaki sloj sadrži adresu sledećeg Onion Router-a. Ovi slojevi su dali i ime projektu, jer koncept kodiranja liči na luk. Zaštitu od posmatranja pruža takozvani Dummy traffic ili prazan saobraćaj koji se obavlja između Onion Router-a. Ako se ovaj sistem malo koristi, onda ne pruža odgovarajuću zaštitu, jer tada mogu da se povežu krajevi komunikacionih kanala, preko razmenjene količine podataka. AN.ON Do sada predstavljene mogućnosti anonimnog surfovanja nisu zapravo zadovoljavajuće. Savezno ministarstvo (SR Nemačke) za privredu zahteva zbog toga razvoj službe za anonimnost. Projekat “AN.ON anonimnost u internetu” koji sprovode tehnički univerzitet iz Drezdena i nezavisni centar za zaštitu podataka iz Šlesvig Holštajna (Schleswig-Holstein), treba da razvije jednu uslugu preko koje bi bila kodirana internet komunikacija. A osnova bi bila mnoga nezavisna čvorišta, takozvani Mix proxy, i ne samo tajne službe, već i sami provider-i ne bi mogli saznati ko i šta radi na internetu. Svaki korisnik može samostalno da pokreće jedan Mix proxy, ako poseduje odgovarajuće široku internet konekciju. Software koji je razvijen u projektu treba u budućnosti da bude besplatno dostupan kao Open-Source, dakle krajnje pristupačan. Ministarstvo privrede želi pre svega da ukloni dosadašnje prepreke za e-commerce. Glavna prepreka je to što korisnici nemaju poverenja u mrežu. Korisnici bi trebalo da budu sigurni da pri on-line kupovini neće iza sebe ostaviti debeli informacioni trag. Nije ni čudo: porast trgovine preko interneta daleko je manji od onog što očekuje privreda. Po analizama ispitivača tržišta, odlučujući razlog leži u zabrinutosti korisnika u vezi sa sigurnošću poslovanja na internetu. Gostujući profesor informatike na slobodnom univerzitetu (Freien Universität) u Berlinu, Hens Federat (Hannes Federath), ima plastičan primer za to: “Zamislite da slučajno tražite medicinske informacije na internetu, jer neki vaši prijatelji pate od jedne teške bolesti. Istovremeno se informišete na nekom website-u nekog osiguravajućeg društva o najpovoljnijoj polisi životnog osiguranja. Obe stvari daju jedan profil, koji će biti procenjen i biće prodan zainteresovanim

stranama i možda će vam onda biti ponuđena nepovoljnija polisa životnog osiguranja.” Program Java Anon Proxy (JAP) već sada je dostupan besplatno, njega je u okviru projekta AN.ON razvio profesor Federat. JAP radi kao virtuelna mimikrija: komunikacioni podaci ne idu direktno na web server, nego preko takozvane Mix proxy kaskade. A pri tome se konekcija korisnika skriva među ostalim JAP korisnicima. Konekcija se može povezati sa jednim određenim korisnikom. Svaki korisnik bi mogao da bude onaj koji je pokrenuo konekciju. Na website-u piše: “Niko, ni neko ko stoji sa strane, ni koji drugi korisnik, čak ni onaj koji vrši uslugu anonimizovanja ne može razaznati koje konekcije upotrebljavaju određeni korisnici.” Po pravilu u jednoj kaskadi rade najmanje tri Mix proxy-a kojima upravljaju nezavisne institucije. Oni izjavljuju i obavezuju se da neće memorisati log-file-ove niti da će sa drugim koji rade sa Mix proxy-jima razmenjivati podatke koji bi mogli dovesti do toga da se može identifikovati određeni korisnik. Nezavisni kontrolni punktovi treba da garantuju da se prethodno preuzete obaveze i izjave poštuju. Najidealnije bi bilo, kako kaže Andreas Ficman, kada bi katolička crkva imala jedan proxy, politička partija drugi, univerzitet treći i robna kuća četvrti proxy – čak i proxy u inostranstvu bi doprineli većoj bezbednosti, jer korisnika je moguće identifikovati jedino kada bi svi koji upravljaju dozvolili prilaz proxy-u. FREENET Freenet je još radikalniji od AN.ON. On uspostavlja paralelni internet koji je otporan na cenzuru, anoniman je i omogućava efikasno objavljivanje i povlačenje informacija. Cilj je potpuno otklanjanje autorskih prava i slobodan pristup svim informacijama, i to za svakoga. 400 osoba sada rade (muškarci i žene za razvoj software-a) pod vođstvom škotskog studenta Jana Klarka (Ian Clark) na razvoju prototipa. Na potpuno decentralizovanoj mreži ne sme više biti centralnih kontrolnih čvorišta. To nije baš jednostavno. Klark i njegov tim imaju problema sa skaliranjem, efikasnošću i raspodelom opterećenja mreže i sa time se bore. Sistem će biti implementiran u Java-u, da bi se dobila platformska nezavisnost. Već sada simulacije pokazuju da je mreža relativno stabilna: čak do 20 čvorišta mogu ciljano da se zatvore i 30% može slučajno da ispadne a da mreža ne pukne. Korisnici se mogu osloniti na autentičnost primljenih podataka i sadržaj jedne datoteke je vezan preko jednog konkretnog zbira sa njihovim imenom. Iako se podaci još ne mogu ciljano tražiti. Peekabooby Projekat koji mnogo obećava a nije na nivou mreže nego na nivou (korisnika) klijenta: U proleće 2001. godine, američka hacker-ska grupa “Cult of the Dead Cow” (CDC) najavila je objavljivanje sopstvenog browser-a po imenu Peekabooby. Žele da ga predstave na hacker-skome kongresu DetCom u junu 2001. godine. Peekabooby ne da će kôdirati kompletan protok informacija između servera i browser-a, nego će raspodeljenim računanjem sprečiti identifikaciju korisnika. Korisnici mogu da kontaktiraju sa drugim Peekabooby korisnicima i na taj način treba da nastane posebna komunikaciona mreža. Unutar te mreže komunikacija je kôdirana – korisnici Peekabooby-a mogu sigurno da šalju čak i e-mail-ove. Peekabooby korisnici bi na ovaj način mogli da savladaju čak i firewall-ove. Peekabooby korisnici mogu i da traže informacije. Korisnik iz Kine bi uz pomoć ovog browser-a mogao da dođe do internet informacija koje je kineska vlada cenzurisala. Jedan računar izvan Kine bio bi “prolaz”: odavde bi mogli da se kôdiraju zahtevani podaci i šalju dalje kineskom disidentu. “Cult of the Dead Cow” postali su poznati kada su razvili alate za skoro neograničen prilaz tuđim Microsoft računarima: “Back Orifice” i “Back Orifice 2000”. Danas te programe koriste sistem administratori kao alat za daljinsko opsluživanje, a koriste ga i hacker-i.

7. The Kids are Out to Play

Ako postoji grupa osoba oko čije percepcije kao “zlih klinaca interneta” navodno postoji univerzalna saglasnost, onda su to tzv. “Script Kiddies”. Tako najčešće bivaju nazvani mladići koji, kao “cracker-i”, sebi obezbeđuju pristup tuđim računarima, naružuju website-ove i posredstvom Denial-of-Service-Attacs bacaju servere na kolena. Budući da pritom (navodno) ne koriste autentične programe koje su sami napisali već posežu za programima rasprostranjenim preko specijalizovanih IRC-kanala, Web i FTP-servera, pripisan im je atribut “script”, dok se “kiddies” odnosi na njihovo mladalačko doba. Najkasnije nakon DDos-napada na CNN.com, Yahoo!, eBay i druge vodeće komercijalne servise na internetu u februaru 2000. godine, o “Script Kiddies” se govorilo na sva usta. Do danas nije sa sigurnošću razjašnjeno ko je mogao nekoliko sati tako drastično nauditi nekima od svetskih servera koji su zasigurno najbolje čuvani i povezani najdebljim vodovima. Procene iznosa štete leže između 1,5 i 3 milijarde američkih dolara. Kao verovatni počinilac kasnije je optužen i izveden pred sud jedan Kanađanin koji je u trenutku čina imao petnaest godina, ali su eksperti ipak jedinstveni da on nije mogao biti jedini počinilac napada. Njegovo pravo ime nikada nije objavljeno zbog mladalačke dobi, ali je kao “Mafiaboy”, što je bio njegov internet pseudonim, ušao u istoriju mreže. Pretnja od strane “Script Kiddies”, poput “Mafiaboy” ili “Coolio” postala je udarni naslov na prvim stranicama novina i na večernjim vestima elektronskih medija, služeći organima gonjenja kao razlog više za zaoštavanje zakona protiv cyber-kriminala. Bivši britanski Ministar isnostranih poslova Robin Kuk (Robin Cook) otišao je čak toliko daleko, da je utvrdio da su “hacker-i” “gori od terorista”. Visoko rangirani državni službenici skicirali su situaciju u kojoj iz svojih dečjih soba u roditeljskim domovima tinejdžeri posredstvom kompjutera, modema i kopiranih software-a mogu dovesti do sloma kritične nacionalne infrastrukture: do gradova odsečenih od struje, do komešanja u bolnicama, finansijskim centrima i vojnim bazama, ili pak, u najmanjem slučaju do izbacivanja iz posla poslovnih servera na internetu i do državnih tajni u rukama neodgovornih mladića. Ipak i oni, koji bi to trebali bolje da znaju, pošto su trpeli i još uvek trpe ista ili slična demonizovanja, iskusni, pravi “hacker-i” iskazuju malo simpatija za klince. Oni koriste pojam “Script Kiddies” da bi se kao hacker-i jedne drugačije, starije etike razgraničili od njih. Oni ih preziru zbog podređenog nedostatka istinski dubokih znanja kompjutera i zbog toga što klinici svojim nepromišljenim delima daju vladama legitimaciju za širi spektar kriminalizovanja sigurnosno relevantnih kompjuterskih aktivnosti – u žargonu “hack-ovanja”. U pogledu ovog poslednjeg oni naprosto imaju pravo. Ipak, u istom momentu moramo dodati, da će stroži pripadnici policijskih i političkih krugova uvek pronaći razloge za zaoštavanje zakona i kaznenih praksi gonjenja. Moguće je da su takozvani “Script Kiddies” mnogo manje homogena i stereotipna grupa nego što bi želeli da nas uvere policija, mediji i stari hack-eri. Sa velikom verovatnoćom možemo reći da je potencijal štete koji oni reprezentuju mnogo manji od onog koji im se pripisuje. Sa tim iskazom ne treba da bude dovedeno u sumnju da mladi crack-eri čine zakonske prekršaje, da oni prouzrokuju lične i privredne štete, te da protiv takve, brojno rastuće pretnje nešto treba preduzeti. Ipak da li su “Script Kiddies” zaista takva “pošast društva”, izazov vrednostima društva? Ili su oni pre produkt istog tog društva koji ga tako proklinje? Možda je njihovo ponašanje simptomom grešaka koje leže suštinski dublje i široko su rasprostranjene, takoreći sistemski uslovljenih grešaka koje podstiču njihova (ne)dela? Slično kao i kod pitanja, da li kriminalca treba čisto individualno osloviti “krivim” za njegova dela ili su njega tek okolnosti načinile onakvim kakav je, takva pitanja nisu rešiva na opštoj moralnoj ravni. “Script

Kiddies” ovde ne treba da budu niti paušalno uzeti u zaštitu, niti razrešeni krivice, niti treba da bude replicirano negativnoj slici o njima koja bez daljnjeg već preovlađuje. Ako se tim fenomenom detaljnije pozabavimo, relativno brzo se dolazi do shvatanja da tih stereotipnih “Script Kiddies” ustvari i nema, nego ima pre svega klinaca sa nizom različitih stanovišta i motivacija koje povezuje samo jedno: naime, da veliki deo svog slobodnog vremena provode baveći se kompjuterima i mrežom. Najkasnije na tom mestu valja ad acta odložiti pojam “Script Kiddies” kao spolja nametnutu negativnu ocenu. Njih bi najpre, bez unapred utvrđenih moralnih vrednovanja trebalo videti kao ono što reprezentuju: kao relativno novu, tehnološku, neprilagođenu, do sada neposlušnu, ometačku i razornu omladinsku kulturu, pri čemu naglasak ipak leži na kulturi. Korene mladalačke hacker-ske kulture opisuje knjiga “Underground” (1997) iz perspektive mladih učesnika, istražujući njihove motivacione razloge. U toj knjizi se radi o mladim hacker-ima u Australiji, Sjedinjenima Američkim Državama i Engleskoj u periodu, od otprilike, 1988. do 1992. godine. Parametri su tada još bili sasvim drugačiji jer je “hack-ovanje”, upad u tuđe kompjuterske sisteme, služilo jednoj osnovnoj svrsi, naime zadobijanju pristupa u širom sveta rasprostranjenim elektronskim mrežama, što mladima tada uopšte nije bilo legalno omogućeno bez kreativnog zaobilaženja sigurnosnih mera. Događaji u vezi sa mail box-ovima poput “The Realm” u Melburnu ili chat sistemom “Altos” u Nemačkoj ipak predstavljaju nešto poput kopije budućeg razvoja situacije. Kao što nagoveštavaju priče u “Underground”-u, kod tih hacker-a ili cracker-a se s jedne strane radilo o tome, da pronađu vlastite puteve kroz upravo rastući svet mreže. Putem otimanja naloga korisnika i otvaranjem zadnjih vrata, oni su mogli poći putevima koji gotovo nikome nisu bili poznati, a njima su davali slobodu kretanja u internacionalnim mrežama, što se još uvek činilo potpuno utopijskim. Jedna važna motivacija bilo je i priznanje koje se sa uspešnim hack-ovanjem moglo steći u maloj, ali prefinjenoj hacker-skoj zajednici. Uz to dolaze i znatiželja, želja da se prisvoje tehnička znanja u postupku “uradi sam” i da se zaviri u svet odraslih. Minimalna etika sastojala se u tome da se tuđim sistemima ne pričinje šteta, da se sistem nijednog računara ne sruši, da se podaci ne obrišu i da se sebi ne obezbede nikakve finansijske dobiti. Važan je bio i Fair Play razmena informacija unutar zajednice – na primer znanja o zadnjim vratima i šifra-crack-metodama. Doduše, moralne granice su naprosto bile porozne, tako da je postojalo mnoštvo carding-a (prevara sa kreditnim karticama) i phreaking-a (zloupotrebe telefonskih konekcija), ali se istinski izazov sastojao u zadobijanju gospodarenja nad Unix-System-om. “Underground” pokazuje sliku mladića različitog porekla koji nisu kriminalno opredeljeni, ali su svakako spremni da prekorače određene granice legalnosti. Podvučene su i snažne veze sa drugim kulturama mladih, pre svega muzikom (indi rokom poput Midnight Oil), odnosno suprotnosti u odnosu na svet odraslih. Konflikt kultura i generacija, uključujući i uzajamna nerazumevanja, nije mogao biti veći – što je takođe element koji je do danas ostao takav. Tu je i svet sigurnosnih naloga sa vizit kartama, ulančeni elektronski kao i realni identiteti u čvrsto povezanim hijerarhijama i karijerama. Naspram njih stoje samo Slacker-tipovi, mladi koji deluju samo pod kriptičnim internet-pseudonimima (nadimcima, takođe nazvanim “handles”) iz kvartova u predgrađu Melburna ili Mančestera. Različite storije koje će se deset godina kasnije gotovo identično ponavljati vodile su ka postepenoj izgradnji protiv udara realnog sveta, a time i ka negativnom vrhuncu. FBI i tajne službe obraćaju pažnju na aktivnosti hacker-a. Spektakularni slučajevi dospevaju na naslovne stranice. Bivaju uvedeni novi anti-hacker-ski zakoni, krivci moraju biti pronađeni i kažnjeni za primer. Za današnje mladiće sam pristup internetu više nije problem, oni gotovo sa svih strana na njega bivaju ohrabrivani. Draž za ilegalne aktivnosti ili prostor za igru time ipak

nisu iščezli. Kao što je jedan sigurnosni ekspert sažeto formulisao, postoji jedna vrsta nove monete na internetu: zadnja vrata. U osnovi se pritom radi o istoj igri kao i pre deset godina: poći putevima koji su drugima neprohodni, nadmudriti profesionalne službenike sveta odraslih, dobiti "root" (administratorske privilegije) na tuđim serverima i pokazati insajderskoj zajednici da se, kako se u žargonu kaže, postalo "elitom", dakle da se pripada eliti istinskih službenih hacker-a. Ko sebi obezbedi pristup najvećem mogućem broju sistema (i, ukoliko nije oglašena na sva zvona, ta privilegija se zadržava na duže vreme), poboljšava svoj status u grupi. Najveća nagrada je etabliranje prihvaćenog *nom de guerre*, vlastitog internet nadimka, kao priznate marke u hacker-skoj zajednici. U svakom slučaju, taj cilj ne može biti postignut samo gomilanjem tesnih, domaćih, mirnih i tihih zadnjih vrata i pristupnih prava. Stoga važi da se kada se ukaže zgodna prilika, javno uspostavi jedan znak. Vandalske aktivnosti koje se najčešće pripisuju internet-zlikovcima, a verovatno su i stvarno počinjene sa njihove strane jesu Website-Defacement, takođe nazvan i WebGraffiti, odnosno DoS-napadi, tj. Distributed-DoS-Attacs. Prilikom "Distributed Denial of Service" napadima (DDoS), u osnovnom principu se radi o tome da se neki server bombarduje sa što je moguće većim paketima podataka, da bi mu se putem tog neželjenog saobraćaja zaustavila paleta internet veza koje mu stoje na raspolaganju, tako da "normalni" paketi podataka više ne mogu biti ispunjeni zahtevi web-servera od strane korisnika zainteresovanih za njegove usluge. Sa razvojem različitih oblika DDoS-napada usavršile su se metode za tu vrstu napada. Preko programa koje sadrže dotični kanali poput "Stacheldraht" ili "Tribal Flood Net" u ruke relativno neiskusnih korisnika dospevaju moćna oružja za napad, što posredstvom "Script Kiddies" samo daje krila medijskom hype-u. U stvari, mladi hacker-i ne žele da se vide označeni tim pojmom i mogu veoma nabusito reagovati kada osete da su nepravedno svrstani u tu kategoriju. To iskustvo je imao i Stiv Gibson (Steve Gibson), stručnjak za kompjutere čiji poslovni server je postao žrtva stalnog DDoS-napada. U slučaju koji je on sâm iscrpno dokumentovao na mreži, dogodio se DDos-napad od strane preko četiri stotine Windows-PC kompjutera raširenih širom sveta u kojem je napadač krišom uvukao male script-e (zване "Zombie" ili "Bot") i preko specijalnih IRC kanala razaslao ih njihovom "gospodaru". Povezanost Gibsonove firme GRC na internet bila je u potpunosti preplavljena ogromnim paketima podataka. Budući da napadi nisu prestajali, oštećeni se latio obaveštavanja podzemlja mreže. Zahvaljujući svojim sposobnostima kao starog hacker-a pošlo mu je za rukom da kao počiniooca identifikuje jednog trinaestogodišnjaka koji se pojavljivao sa nadimkom "Wicked" i da putem jednog foruma stupi u dijalog sa njim. "Wicked" je priznao da je prouzrokovao napade, jer je iz druge ruke čuo da ga je Gibson nazvao "Script Kid". On je preplavio njegovu konekciju sa mrežom da bi mu demonstrirao svoju moć. Gibson, koji je prošao kroz iskustvo katarze, zaključuje: - da je uprkos svim znanjima bio bez odbrane u odnosu na te napade, tako da je priznao "odustajem, ti si pobedio", - da osetljivost Misrosoft-sistema sačinjava jezgro nevolje kada "Zombies" bivaju preuzeti za DDoS-napade i da je sa novim generacijama, Windows 2000 i Windows XP situacija još više pogoršana, - da mu provajderi korisničkog računara ne mogu ili ne žele pomoći kada "Zombies" napadnu, tj. jednostavno zatvaraju oči i - da mu ni FBI nije mogao ili želeo pomoći. Tek nakon što je obelodanio svoj poraz i nakon što je svom protivniku mogao saopštiti da on navodnu izjavu u vezi sa "Script Kiddies" nikada nije izrekao, napadi "Wicked-a" su dobrovoljno prestali. Nakon toga se Gibson bacio na posao da razvije oruđe protiv DDoS-napada. Pri naruživanju website-ova koje je prikladno nazvano i "Web-Graffiti", radi se o tome da se obezbedi privremeni pristup nekom web-serveru i da se njegova homepage zameni sadržajima prema vlastitom izboru. Ta praksa je zadobila gotovo već epidemijske

razmere. Dnevno navodno šezdeset do osamdeset site-ova biva preuzeto i 'obeleženo grafitima'. Oni imaju najrazličitije sadržaje, ali iskazuju i neke zajedničke karakteristike: umetnici digitalnim sprejem ostavljaju signaturu svog imena, ime napisano u tipičnom hacker-skom žargonu koje se sastoji od slova, brojeva i znakova (na primer "Z3BR4 X", "Digi Almighty", "f0rpaxe"), žargon poput "XY rulez" ili "ownz", tj. "Soundso" preuzeo je kontrolu nad serverom. Mnogi takođe rade u grupama koje se pojavljuju pod imenima poput "PoizonB0x" ili "World of Hell". Ali često su nenasilni "shouts", tj. pozdravi vlastitoj zajednici, drugim grupama, a ponekad i poruke devojkama i hacker-skim veličinama poput Kevina Mitnika (Kevin Mitnick) i 2600-Magazine. Sastavni deo specifičnih napisa su obelodanjivanja opštih raspoloženja (Bier, Joints) a ponekad i političke poruke, grafikoni pa čak i Midi ili MPEG-podaci. Proteklih godina gotovo da nijedan popularan web-server nije ostao nenaružen takvim povremenim preuzimanjima, bio on server New York Times-a, NASA-e ili Bele Kuće. Što centralniji značaj neki server ima u javnom procenjivanju, utoliko je veća "cracker-ova" pobeda. Crack-ovanje servera poput New York Times-a do skora bi prouzrokovalo udarne naslove. Danas su ona toliko frekventna, da se mora raditi o istovremenom, koncentrisanom preuzimanju brojnih servera da bi se još privukla pažnja nekog od novinara. Interesantnije od pojedinačnih slučajeva su serije ili određeni konflikti. Tako postoje crack-erske trupe koje su se specijalizovale za preuzimanje servera iz vojno-industrijskog kompleksa. Druge pak favorizuju ciljeve među izabranim, velikim svetskim koncernima. U kontekstu političkih konflikata protivnički crack-eri međusobno ruše website-ove – kao nedavno US Amerikanci protiv Kineza, Palestinci protiv Izraelaca, Srbi protiv Hrvata i kosovskih Albanaca. Takve događaje mediji rado uvode u igru kao razgorevanje davno prognoziranih informatičkih ili cyber-ratova. Pritom jedno ipak nipošto ne bi trebalo da se previdi. Radi se "samo" o privremenom uništenju informacija na javno pristupačnom web-serveru koji biva promenjen ili načinjen nepristupačnim. Kritične aplikacije time ne bi trebalo da su pogođene, budući da one, što je jedno od osnovnih pravila svakog udžbenika bezbednosti, treba da cirkulišu drugim računarima koji nisu direktno povezani sa nekim web-serverom i trebali bi biti dodatno čuvani. Crack-ovanje web-servera jednog elektrifikovanog društva ne znači da se stekao pristup računaru sa čime bi se mogao srušiti dotični energetski sistem. Ipak, u medijskoj percepciji takvih događaja pomenuta razlika često biva (svesno?) zapostavljena. Kada se crack-eri, koji u stvari samo žele da publikuje svoj Web-Graffiti, spotiču preko banaka podataka sa informacijama o klijentima, informacijama o kreditnim karticama ili drugim osetljivim informacijama, onda se radi o značajnom nedostatku bezbednosne politike dotičnog preduzeća. Treba izričito reći da nije verovatno da neko na koga se odnosi oznaka "Script Kiddie", dakle početnik koji operiše samo sa unapred pripremljenim programima, može prodreti u jedan dobro čuvani sistem u kojem su zaključane sve poznate bezbednosne rupe. Čini se da je ipak lakše preko medija stvoriti 'žrtvene jarce', nego ozbiljno shvatiti bezbednost. Povrh toga, monokultura Microsoft-a predstavlja prividno idealno okruženje za aktivnosti "Script Kiddies" – na primer povredivost MS Outlook Express-a posredstvom virusa i crva koji su opremljeni sa virusnim Standard-Tool-Kits. Website "Alldas.de" u međuvremenu je jedini website koji još uvek objavljuje arhiv crack-ovanih website-ova. Intervjui sa Web-Graffiti atentatorima koji su tamo objavljeni izazivaju slutnju da je stadijum "Script-Kiddie" nešto poput prve stepenice na merdevinama učenja prilikom bavljenja temama kompjutera i bezbednosti. Sasvim drugačije nego što sugerišu medijski izveštaji, mladi crack-eri nisu bezuslovno fiksirani za karijeru tvrdokornih cyber kriminalaca ili cyber terorista. Mnogo radije oni potajno čeznu za poslom u kompjuterskoj industriji kao – iznenađenje – bezbednosni

eksperti, zvani i “White Hat Hacker” ili “Ethical Hackers”. Aktivnosti u podzemnom kompjuterskom svetu, a to je i među njima često upravo tako shvaćeno, služe sticanju reputacije među prijateljima, među proširenim krugom eksperata, a time kvazi pripremi u docnijem toku karijere. Njihovo kriminalizovanje ili čak izjednačavanje sa teroristima, može se uporedi samo sa slavnom poslovicom “topovima gađati vrapce”. Mladi prijatelji kompjutera, pogrešno nazvani “Script Kiddies”, često su pre idealistični mladi ljudi koji se vide konfrontirani sa svemoćnim institucijama države ili privrede. Nepoverljivi prema poštovanju autoriteta, oni smatraju da je legitimno počinuti zakonske prekršaje koji su u njihovim očima manji. Ono što se ranije označavalo kao vojno-industrijski kompleks, na internetu je udaljeno odmah iza ugla. Bez sasvim jasne svesti sa kim imaju posla, oni testiraju granice civilnog i vojnog interneta i izazivaju državnu moć. U svojim protiv-reakcijama ona nije nežna. Racije protiv petnaestogodišnjaka sa neuniformisanim, teško naoružanim agentima nisu retkost, pre svega u Severnoj Americi. Javno žigosanje kao kriminalaca i terorista, te dodeljivanje zatvorskih kazni šalju signal za zatvaranje redova u podzemlju. Tendencija je slična kao i u “Ratu protiv droge”. Ko zbog posedovanja jednog grama marihuane ide u zatvor godinu dana ili duže, sa velikom verovatnoćom se vraća u svet kao očvrsnuli kriminalac. Ubrzo nakon DDoS-napada na Yahoo! itd. Američki cyber kritičar Daglas Raškof (Douglas Rushkoff) napisao je da ga ti uspešni napadi ne ispunjavaju samo sa potajnom željom za nanošenje štete, nego da takođe ima naznaku o motivacijskim razlozima za te napade. To je rastuća komercijalizacija mreže koja prinuđuje da se od nje stvori sve sigurnije i bolje nadzirani prostor. Moguće je da se ti napadi sagledaju poput oslobađajućeg udara protiv konsekvenci komercijalizacije mreže, piše Raškof. Mladi se danas osećaju konfrontirani sa jednim višestruko regulisanim svetom u kojem vladaju potrošnja, robne marke i vlasti. Omladini pripada pobuna, isto kao i sazeo interes za seks i rastući osećaj za pravednost. Često korišćena predrasuda protiv mladih kompjuterskih čudaci glasi da su oni usamljeni tipovi, bez socijalnog života u “normalnom” svetu. Intervjui na “Alldas.de” jednako kao i knjiga “Underground” protivreče tom klišeju. Mladi kompjuterski čudaci su sasvim normalni mladići koji se interesuju za priznanje u grupi, za samopotvrđivanje i kontakt sa drugim polom. Njihovo demonizovanje i kriminalizovanje može značiti stvaranje stigmatizovanih autsajdera od nekih među najtalentovanijim i najznatiželjnijim ljudima u ovom društvu, ljudi koji mogu pružiti vredan doprinos, a zakoračivanje u normalan život im se nepotrebno otežava. Vredno je spomena da je godinu dana nakon DDoS-napada na CNN, Yahoo! itd. značajno popustila frekvencija medijskih izveštaja o “Script Kiddies”. Na udarnim kompjuterskim Newssites još se nalaze vesti o postupcima protiv pseudonima poput “Mafiaboy” ili “Coolio”, ali o zatvorskim kaznama na koje su oni konačno osuđeni ili nisu osuđeni, uprkos opsežnom istraživanju ne može se pronaći baš ništa. Jedan razlog može biti malaksavanje Dot-Com-Boom-a i da je samim tim opala i udarna vrednost takvih vesti. Jedan drugi razlog zvuči već nešto konspirativnije. Praktično sve visoko industrijalizovane zemlje u međuvremenu imaju drakonske zakone protiv cyber kriminala koji gotovo da i ne prave razliku između kriminalnih aktivnosti (krađa identiteta, prevara sa kreditnim karticama) i tipičnih “Script Kiddies”-aktivnosti. Na internacionalnoj ravni Evropski Savet, Evropska Unija, države G-8, vremenom su razrezali naredne internacionalne izdatke koji su zatrpali svaku jazbinu cyber kriminala, sasvim u smislu politike iz koje odsustvuje tolerancija. Javni otpor protiv takvog zakonodavstva koje preti odstranjivanjem mnogih građanskih prava u cyber prostoru, u liberalnoj štampi je minimalan, pa gotovo da čak i ne postoji. Kako god da se taj sklop – između zakonodavstva, buma i kraja

izveštavanja o “Script Kiddies” – mogao kauzalno sagledati, čini se, da “Script Kiddies” zasada odrađuju krivicu kao žrtveni jarčevi pretnje od interneta.

7.1. Good Times

Good Times, klasični virus-hoax . Početkom decembra 1994. godine, na internetu je počeo da kruži jedan e-mail, čija prva rečenica je glasila: “Ovde je jedna važna informacija. Obratite pažnju na jedan fajl pod imenom 'Good Times'”. Nakon toga je kratki e-mail upozoravao da u America Online (AOL) cirkuliše jedan virus koji se širi putem e-mail-a. Ko god primi e-mail pod naslovom “Good Times” ne bi trebao niti da ga čita niti da ga sačuva. Radi se o jednom virusu koji bi pobrisao sve podatke sa hard diska, navodilo je dalje upozorenje na virus i zaključilo sa tim, da bi se to upozorenje trebalo “dalje poslati svim svojim prijateljima”, jer bi se na taj način i njima veoma pomoglo. Već nekoliko dana nakon prvog zajamčenog pojavljivanja upozorenja na “Good Times”, CIAC, koji pripada Ministarstvu energetike Sjedinjenih Država, u službenom izveštaju od 6. decembra obelodanila je da je “Good Times” e-mail šala, da takva vrsta virusa ne postoji te da stoga ne pretili ni opasnost od njega. Nije potrebno biti ekspert za kompjutere da bi se razumelo da se kompjuterski virusi ne mogu širiti posredstvom pukog otvaranja jednog e-mail-a. Virusi ili e-mail 'crvi' mogu biti skriveni u iscrpnim programima, koji sa e-mail-om bivaju poslani zajedno sa prilogom (attachment). Puki deo teksta jednog e-mail-a ne može pokrenuti takve događaje koji će izbrisati hard disk. Ipak, rasprostranjivanje virusa “Good Times” nisu sprečili niti relativno šaljivi karakter upozorenja na viruse, niti razjašnjavajuća obrazloženja AOL, administratora sistema, moderatora mailing lista, antivirus eksperata, firmi za zaštitu od virusa. Lažni virus-alarmi raširili su se na univerzitetskim mrežama, na mrežama vlada i firmi, infiltrirali su se u mailing liste, news-grupe, bulletin-board-ove, prokrstarili su Atlantik i vrlo brzo su bili prevedeni na različite jezike. Nakon prvog vrhunca epidemije u zimu 1994/95 učinilo se da su popustili, ali je uvek iznova dolazilo do novih pojava takvih alarma. Kao kod glasina, ogovaranja i sličnih poruka koje se održavaju u životu tako što u miru “pošte koja se prenosi šaputanjem” bivaju dalje prepričavane, sadržaj “upozorenja” se vremenom proširio. U jednoj varijanti to znači da je “Good Times” opasan zbog toga, što pri njegovom očuvanju biva aktiviran ACII-Buffer računara. Jedna varijacija na tu varijaciju okončava u tvrdnji da je “procesor izmešten u stanje beskonačnog binarnog proklizavanja n-te kompleksnosti”, što bi naposljetku vodilo ka uništenju procesora. Ni takva, očevidno pseudo-naučna zavaravanja nisu mogla da zaustave širenje “Good Times”-a. Usled toga je “Good Times” mutirao i ponovo se pojavio pod novim imenima, na pr. kao Irina, Deeyeda, a kasnije i kao Penpal Greetings, a na mreži je još i danas aktivan pod različitim identitetima, napokon i kao “It takes guts to say Jesus”. Uprokos svim prosvetiteljskim podsticanjima snaga uma, “Good Times” i njegovi sledbenici su otporni na svoje potpuno gašenje. Upozorenje na viruse je i sâmo postalo virus. Eksperti se spore oko toga sa čije strane je taj hoax (prevara) pušten u svet. U nekim izveštajima stoji da je “Good Times” istovremeno poslat od strane jednog AOL korisnika i jednog studenta. Međutim, ne postoji dokazivi, prvi izvor, kao što ne postoji ni pismo priznanja. Gotovo verodostojno, u smislu stvaranja legende, pojavila se teorija “spontanog nastanka” iz humusa interneta. Prema njoj bi se u naglašeno izokrenutom izveštaju moglo raditi o istinitom ili poluistinitom događaju. Prema jednoj drugoj varijanti postojalo je lančano pismo sa imenom “Good Times”. Da bi se ono prekinulo, neko je u svet pustio buvu da “Good Times” sadrži virus. Naprotiv, trebalo bi biti dokazivo, da je pre “Good Times”-šale postojalo lančano pismo nazvano “Good Luck”. U njemu je stajalo da bi dalje slanje tog lančanog pisma-e-mail-a donelo sreću

svima koji u tome učestvuju. Napad na racionalnost “Good Times” i slični načini obrade teksta ne sadrže nijedan kôd koji bi poput pravog kompjuterskog virusa mogao da pričini štetu podacima napadnute mašine ili samom hardware-u. Ipak upozorenja na viruse, koja su i sama postala virusi, prouzrokuju objektivne štete. Upravo u velikim organizacijama može opasti produktivnost, ukoliko je polovina zaposlenih u potrazi za virusom koji ne postoji. Administratori sistema trpe od bombardovanja e-mail-ovima zabrinutih korisnika, strepnje za njihove računare i rada koji je zbog toga nagomilan. Jedan takav lažni alarm se naročito na mailing listama može zakotrljati prema principu grudve od snega. I demantovanje upozorenja od strane moderatora liste koje ukazuje da se radi o hoax-u ponekad ne može zaustaviti lavinu. Pod određenim okolnostima demantovanje upozorenja samo još više skreće pažnju na hoax. Pod teretom priloga diskusiji prouzrokovanoj od strane hoax-a, e-mail server može da bude položen na kolena. Izvesno je da se može sporiti o tome, koliko velike štete u obliku gubitka produktivnosti nastaju posredstvom virus-hoax-a. Sigurno je samo da se uvek iznova pronade neko ko će nasesti na šalu i ponovo uhvatiti nit, te ponovo uspostaviti đavolji krug – ne postoji nijedna tobožnja tehnička “inекcija zaštite” protiv te vrste “virusa” poput one koju, primera radi, programi zaštite od virusa nude u odnosu na prave kompjuterske viruse. Kompjuterski virus je jedan program koji se može pripojiti drugom programu, čijim aktiviranjem on onda upravlja tako što utiče na dalje širenje virusa, ali ponekad nanosi i štetu podacima i obavlja druge uništavajuće procese. Nasuprot tome, upozorenje na virus koje je postalo virus ne inficira mašine, nego ljude. Korisnik sebe stvara domaćinom jednog programa koji sadrži jednostavno uputstvo za delovanje: “raširi me”. Samim tim, ta vrsta “virusa” u stvari nije tehnička tema. Uspeh te vrste počiva na usudnom “social engineering”-u tj. na nadmudrivanju razumskih barijera i igranjem na kartu praljudskih osobenosti poput strepnje, praznoverja i spremnosti na pomoć. Taktike onih koji prave virus-hoax imaju više veze sa reklamom, književnošću, psihologijom i grupnom dinamikom nego sa tehnikom. Da bi se poverovalo u njih i da bi se mogli dalje širiti, virus-hoax-i iziskuju određene setove pretpostavki. Relativno neiskusni korisnici kompjutera i interneta su ponajviše ugroženi od mogućnosti da dopuste da budu zaraženi lažnim upozorenjem na viruse. U hoax-viruse takođe se umešala klima virusne histerije koji su mediji poodavno stvorili. U jednom trenutku kompjuterski virusi su već osvojili naslovne stranice i to kada ih je još bilo relativno malo i kada većina ljudi još nije koristila lični računar, barem ne kod kuće. Moguće je da njihova atraktivnost kao medijske teme potiče odatle da virusi oslovljavaju duboko ukorenjene, iracionalne strahove – strah od epidemije koja se ne može kontrolisati, a izaziva iznenadne prekide funkcija u ljudskom organizmu koji se ne mogu objasniti, jer se o odgovarajućem pogonskom sistemu premalo zna. Ipak, pored podstrekivanja strahova virus-hoax-i bacaju i jedan mamac: onaj ko upozorenje pravovremeno pošalje dalje time postaje i omiljen kod svojih prijatelja, postaje spasilac zajednice. Upozorenja na viruse rado se odnose na autoritet, što znači da ih navode kao izvor istraživačkog rada neke od vodećih IT firmi ili službi za korisničku podršku nekih od vodećih internet provajdera. Naposletku, lažna upozorenja na viruse koriste određeno utišavanje glasa, tj. određen način pisanja i tipografske metode da bi u primaocu uspostavili stanje povećanog uzbuđenja u kojem se razum najčešće da nadmudriti. Oni često upotrebljavaju velika slova i mnoštvo znakova uzvika, što u e-mail etiketi odgovara urlanju u realnom svetu. Oni u primaocu često bude osećaj da je svedok jedne ekskluzivne, ali ekstremno važne informacije, utoliko što ukazuju na to da “za sada o tome niko ne zna”, ali je virus ipak “za dvadeset i četiri časa već inficirao milione kompjutera”. (Ne) logična posledica je da se deluje SADA, da se vest ODMAH mora dalje poslati SVIM PRIJATELJIMA. Upravo taj šematski

postupak koji se danas pre svega koristi pri e-mail spam-ovima u različitim varijacijama, virus-hoax u stvari čini lako prepoznatljivim. Onaj ko je jednom prozreo princip, semantičku i tipografsku konstrukciju takvih lažnih alarma, sa velikom verovatnoćom više nikada neće nasesti na to. A ko želi da bude sasvim siguran treba samo da pretraži jedan od anti-virus site-ova proizvođača ili univerziteta i da na potraži liste sa poslednjim pravim upozorenjima i poslednjim hoax-ima. Međutim, takav pristup koji se oslanja na činjenice upravo nije poenta ove stvari. Kada bi sve išlo sa racionalnim stvarima, "Good Times" bi izumro nakon dve nedelje. Univerzum Hoax-era Virus-hoax-i su programirani tako da nadmudruju razum, večnu sumnjalicu i poput trojanskog konja se ušuljaju u svet osećaja. Tamo oni umeju da pritisnu pravo dugme, da bi nas odobrovoljili da omogućimo njihovo umnožavanje. Utoliko je upozorenje na virus poseban tip jedne veoma raširene vrste poruka koji se viralno širi na internetu. U to se ubrajaju dalji hoax-i koji se odnose na kompjuterske teme, pozivi na humanitarne akcije, piramidalna-lančana pisma i preko e-mail raširene urbane legende (bajke velikih gradova). Viralni marketing, te umetnički i literarni e-mail hoax-i su posebni slučajevi, o kojima će još biti reči. Valja spomenuti i probleme u vezi sa prekrajanjima i kategorizacijom sa spamovima (pogledati članak "Postani bogat, srećan i sit" Florijana Šnajdera) i sa cyber-, odnosno informatičkim ratom (videti članak "Ratnici u mrežama podataka" Ralfa Bendrata). Čini se da su motivi hoax-a relativno jasni. Pri različitim formama hoax-a, u skladu sa njihovom definicijom, uvek se radi o momentu obmane. Neko sebi uzima slobodu da napakosti svojim bližnjima, utoliko što ih zavarava sa nečim što nije tačno ili ne postoji. Nagrada za te hoax-ere mogla bi biti oskudna radost, da pritom vide kako se 'patka' šiti mrežom. Mnogi hoax-i ipak imaju i dodatne motive. Oni su često komercijalne prirode kao na primer u slučajevima lančanih pisama, dok se kod nekih drugih može raditi o akcijama lične osvete, a drugi se opet usmeravaju u borbu Davida protiv Golijata, protiv moći režima ili velikih koncerna. Najkasnije od "Good Times"-a, e-mail hoax-i su postali deo folklora interneta koji više ne treba zanemarivati. Oni su neiskorenjivi poput spam-ova, ekstremno dosadni kada se pojavljuju u velikom broju, u najpovoljnijem slučaju su razveseljujući poput dobrog vica, a ponekad mogu imati i literarne kvalitete. Prvi virus-hoax datira u 1988. godine, a odaziva se na ime "2400 baud modem virus". Jedan upozoravač koji se predstavlja kao ekspert, iscrpno opisuje u tehničkom žargonu kako se virus navodno širi posredstvom takozvanog "Subcarrier"-a - kanala koji se "normalno koristi samo za protokolarnu razmenu između modema". Nakon dužeg testa autor dolazi do rezultata, da stariji "1200-baud-modem time" nije pogođen i stoga savetuje da se upotrebljava samo taj sporiji tip modema. Jedna od najlepših 'patki', što se tiče kompjutera i interneta bio je Internet-Cleaning-Day koji je pre nekoliko godina bio proglašen u mesecu februaru. E-mail počinje sa iznenađujućom tvrdnjom "kao što mnogi od Vas znaju, internet svake godine mora jednom dvadeset i četiri časa biti zatvoren zbog čišćenja". Radi se o tome, da bi mreža morala biti očišćena od "mrtvih e-mail-ova, neaktivnih FTP sajtova, Gopher sajtova i WWW sajtova" (kao kada bi štetne arterijske materije bile obložene na unutrašnjim zidovima i time ugrozile krvotok). Da bi Cash i Proxy mogli biti očišćeni na najvažnijim čvorištima, korisnici računara koji su stalno povezani sa internetom bi jedan dan trebali biti skinuti sa mreže a svaki fizički kontakt bi trebao biti otkaćen, da pri akciji čišćenja ne bi došlo do nenamernog brisanja podataka. Nažalost ne postoje informacije o tome, koliko WEB master-a se odazvalo pozivu. Jedan drugi internet-hoax za koji se čini da nikada nije izumro govori o e-mail porezu u Sjedinjenim Državama koji namerava da uvede Federal Communications Commission (FCC) u okviru jednog novog zakona. Široko rasprostranjeni su i hoax-i koji pozivaju na pomoć ženama pod talibanskim režimom ili na

spasavanje bolesnog deteta. U jednoj maloj privatnoj anketi obratio sam se ljudima koji su mi u prošlosti poslali te ili slične poruke. Jedno od saznanja koje sam stekao na osnovu odgovora jeste, da dalje slanje takvih e-mail-ova može biti bojažljivi pokušaj očuvanja kontakta. Pokušava se komunicirati sa većom grupom ljudi, sa kojima se inače ne održavaju permanentni kontakti. Pritom dalje poslati e-mail služi kao jedna vrsta vizit karte, neko se čini korisnim, pokazuje koje interese ima, nije samo “na” mreži, nego i “pri” mreži, deo jedne kontaktne mreže e-mail istomišljenika. Kako pokazuju odgovori, pretežno je reč o ponašanju početnika sa kojim se prestaje najkasnije tada, kada e-mail koji je jednom bio poslat u uverenju da se čini dobro, nakon šest meseci ponovo završi u vlastitom inbox-u. Mem je mem je mem Suštinska tačka hoax-fenomena je da se daljim slanjem upozorenja na viruse ili poziva u okviru kampanje zamišlja “community” u kojoj se želi osetiti pripadnost. Internet nam pruža osećaj da “nismo sami tu napolju”. Postojanje zajednice pretpostavka je za prihvatanje i dalje slanje tih e-mail virusa. I kreatori lažnih upozorenja i lančanih pisama međusobno na prikriveni način deluju sa zajednicom. Suštinski motiv je povezanost posredstvom mreže. Paralelno sa fazom brzog rasta interneta iz čuvanih zajednica istraživanja, vojske i ponekih privrednih pogona u širu javnost, u optičaju su različita teorijska stanovišta – od “kolektivne inteligencije”, preko “globalnog mozga”, pa do “mimetike”. Ona se odnose na one okolnosti koje omogućavaju virus-hoax-e i ne bi moglo biti slučajno, da te teorije svoje publicističke vrhunce slave upravo u fazi kada je “Good Times”-hoax doživljavao klimaks. Zajednica više nije ograničena na fizički svet, tračevi se više ne šire samo u kafeima, na zabavama i prilikom drugih društvenih dešavanja, već su elektronski ojačani i putem geografski raspršene zajednice interneta se ubrzano šire oko celokupne Zemljine kugle. Pokušaj evaluacije i razjašnjenja filozofskih i naučnih stavova koji leže iza pojmova kolektivna inteligencija, globalni mozak i mimetika prevazišao bi temu ovog članka. Napokon, mem-ovi su, kao pokušaj objašnjenja širenja e-mail hoax-a, vredni okretanja jedne stranice. Pojam Meme skovao je britanski istraživač evolucije Ričard Doukins (Richard Dawkins). Biološke pojmove gen i geneza on stavlja analogno razvoju ideja kao meme i memesis. Prema Doukinsu, meme su misli koje se oblikuju u jedinstva kojih se možemo sećati i koje odlikuje jedan fizički izraz. One bi bile prihvaćene od strane ljudi bez njihovog vlastitog učinka, tako da oni postaju domaćini tih meme-a. Upravo to se može reći i o virus-hoax-ima. Oni se mogu posmatrati kao set informacija koji vode računa o daljem vlastitom odgajivanju, a za to su im neohodni domaćini – mi ljudi. U ekonomiji pažnje oni egzistiraju u obliku e-mail inbox-a svakog pojedinog recipijenta. Tamo oni konkurišu mnoštvu drugih poruka: privatnim e-mail-ovima i onima koji se odnose na posao, pretplaćenim informatorima i mailing listama, spam-ovima. U toj naglašeno takmičarski orijentisanoj okolini, pre svega dva faktora odlučuju o tome da li ćemo otvaranje vesti uopšte smatrati vrednim truda. S jedne strane, to je adresa pošiljaoca i dotični naslov, sa druge. Budući da hoax-i najčešće funkcionišu uz pomoć trika da treba dalje da budu poslati prijateljima, oni ovde već beleže dodatni plus. A najviše uspešnih hoax-a imaju genijalno jednostavne naslove. E-mail pod naslovom “dobra vremena” (Good Times) ili “pozdrav od jednog prijatelja” (Penpal Greetings) rado se otvara, naročito ako stiže od nekog prijatelja. Isti mehanizam je uostalom na delu i prilikom pravih kompjuterskih virusa koji bivaju šireni posredstvom e-mail-a, kao na primer “I LOVE YOU”, odnosno “Homepage”. I u slučaju komercijalnih spam e-mail-ova naslovljavanja postaju sve rafiniranija. U poslednje vreme naslovi na primer glase “from John” (gotovo svako poznaje nekog ko se zove Džon), “information that you requested” (da li sam u poslednje vreme zatražio neku informaciju? Može biti...) ili “Re: Your Future” (tema koja je uvek interesantna). Ako je naslov shvaćen ozbiljno, e-

mail je dakle otvoren, tada se stvar zakuvava. Email virusi i e-mail 'crvi' počivaju na tome da se ujedno otvara još i dodatni attachment (i funkcioniše u e-mail okruženju koje dozvoljava izvođenje attachment-a). E-mail hoax-i počivaju na tome da bivaju dalje poslati, kada im se poveruje, ili se barem smatraju dovoljno interesantnim, da bi bili poslati drugima. Ono što nakon toga sledi u saglasju je sa Doukinsovom teorijom mema, darvinističkim iščitavanjem u oblasti ideja. E-mail hoax-i nastoje da pobude što je moguće snažnije osećaje – strepnja, seks, profit, usamljenost, odnosno želja za pripadnošću, želja za vrednošću, znatiželja, potreba za važenjem - koji u nama okidaju evolucionistički okidač i nagone nas da panično pritisnemo dugme: Forward... Kritičari mimetike ne slažu se sa time da je socijal-darvinističko učenje o evoluciji primenjivo na polju kulture. Oni argumentuju da se nalazimo u određenom periodu istorijskog razvoja civilizacije koji se u zapadnom svetu može identifikovati sa pojmovima kapitalizam i demokratija, a oni ipak ne mogu biti posmatrani kao istoznačni sa “prirodnim zakonitostima” evolucije. Napokon, prihvaćena pasivnost njima je trn u oku, budući da nas prema mimetici, parazitske meme koriste samo kao pasivne okidače . Hoax-politika Središnji mit interneta je takozvana Many-to-many komunikacija, komunikacija mnogih sa mnogima, koji raskida sa tradicionalnim modelom slanja sa jednog centralnog izvora vesti koje se emituju mnogim primaocima. Doduše, ta teza nije dokazana jer retko se radi o jednom jasnom linearnom sledu razvoja, pri čemu bi jedan sistem zamenjivao drugi, ali dalje slanje vesti u mrežama prijatelja i poznanika putem interneta, ponekad se činjenično pokazuje kao moćna komunikacijska mašina. Najznačajniji izraz te decentralizovane komunikacije danas su tehničke Pear-to-pear mreže (P2P) u stilu Napster-a ili Gnutella-e. Ali, Pear-to-pear ponovo pokazuje svoju moć i bez tehničke realizacije, kao na primer početkom 2001. godine u slučaju e-mail-a koji se ticao firme Nike, a obišao je ceo svet. Proizvođač sportske opreme ponudio je kupcima sprinterskih patika najvišeg kvaliteta mogućnost da robu personalizuju. Ukoliko za donekle uvećanu cenu poruče patike preko jednog website-a, na patiku će biti ušiven natpis prema vlastitom izboru. Kako kaže legenda, jedan američki student je poručio da mu ušiju reč “Sweatshop”. Taj pojam se odnosi na eksploatatorske prakse rada u fabrikama koje ne odgovaraju standardima zaštite radnika zapadnog sveta – a firma Nike je već godinama trpela prigovore da u najmanju ruku toleriše iste takve “Sweatshop” prilike u subkontrarnim proizvodnim pogonima trećeg sveta. Kada je Nike odbila da mušteriji ušije takav natpis razvio se kako interesantan, tako i zanimljiv e-mail dijalog između mušterije i firme, pri kojem je uobraženi ispitivač uvek iznova bio prinuđen na “verbalno hvatanje krivina” od strane odgovornog predstavnika firme. Taj e-mail dijalog pušten je na mrežu i raširio se sa tendencijama viralne zaraze. Nakon što sam po prvi put video, taj e-mail na jednoj mailing listi, u roku od nekoliko dana sam ga primio barem dvadeset puta sa različitih strana. Teško se može prosuditi koliko velika je činjenična šteta putem kampanje trkač nanesena imidžu Nike, ali se svakako radi o slučaju e-mail zaraze koji je naposljetku završio u etabliranim medijima i postao udarna vest širom sveta. Ipak, bilo bi pogrešno slaviti takav događaj kao dokaz za decentriranu, demokratsku moć interneta i time ga proglasiti apsolutno dobrim. Takvi “rezultati” P2P-komunikacija počivaju na određenim pretpostavkama koje se teško mogu kontrolisati i ne daju se generalizovati. Drugi e-mail hypes skorašnje prošlosti pre svedoče o zgražavanju, kao u slučaju jedne engleske službenice. Ona se uplela u razmenu erotskih e-mail-ova sa ljubavnikom kojeg je skoro upoznala. On je radio u jednoj velikoj firmi i celokupne rezultate razmene je prepun ponosa poslao dalje na adrese pet najboljih prijatelja u firmi. Njima se to učinilo toliko zabavno da su e-mail smesta dalje prosledili svojim svagdašnjim prijateljima, i tako dalje i tako dalje. U roku od dvadeset četiri časa, navodno je milion ljudi imalo došlo u

priliku da se naslađuje nenašminkanom diskusijom o oralnom seksu. Korišćenje Bottom-up-Power (mož odozdo) interneta za ambiciozni politički hoax, pošlo je za rukom birou za komunikacije Ubermorgen.com tokom američkih predsedničkih izbora 2000. godine. Ubermorgen.com se sastoji od Lucijusa Bernharda (Luzius Bernhard) – koji se pojavljuje i kao Hans Bernhard, Hans Ekstrem (Hans Etxtrem) i NET_Callboy – i partnerke LIZVLX, u svoje favorizovane taktike pored hoax-a ubraja i Šok-marketing i Drama-marketing. Ono što oni nazivaju “medijski-hack” predstavlja cilj i centar njihovog manevra obmanjivanja i konfrontacije: što pre je moguće dospeti na CNN. To im je uspelo u jesen 2000. godine sa projektom Voteauction.com, što je web platforma za licitaciju glasova birača prilikom predsedničkih izbora u Sjedinjenim Državama, a takođe i prilično slobodna interpretacija slobodne tržišne privrede. Jedan američki student prvobitno je programirao Voteauction.com kao protest protiv prakse finansiranja predizborne kampanje u Sjedinjenim Državama, u kojoj firme i lobiji različitih branši putem vlastitih izdataka pokušavaju da steknu uticaj na buduću politiku. Nakon sudske presude u državi Nju Jork, sajt su preuzeli Bernhard i partnerka, uspostavili su server izvan SAD i posredstvom e-mail kampanje počeli su da skreću pažnju na akciju. Sa argumentom da bi, ako je politika potkupljiva, od toga trebali da imaju profita i obični birači, Voteauction.com je brzo raspirio kovitlac publiciteta. Pažnja američkih sudova je u svakom slučaju pobuđena, koji su putem presuda i prekidanja domena pokušali da doskoče očevidno ilegalnoj delatnosti. Međutim, to je glasačkoj licitaciji (kasnije je mutirala u vote-auction.net, gde se i danas može pročitati lični doživljaj u obliku izveštaja) pribavilo još više publiciteta, a na završetku medijskog hack-a bilo je preko četiri stotine novinskih članaka i televizijskih izveštaja, kao i pet sudskih postupaka s tim u vezi, u različitim izbornim okruzima Sjedinjenih Država. Činjenično nije licitirao nijedan jedini birački glas, budući da je celokupna akcija od početka izgrađena kao lažnjak – ili Web-Hoax. Viralni marketing Zarazna moć virus-hoax-a i e-mail 'patki' napokon je zapažena i od strane onih koji se bave privredom. Od pre nekoliko godina već cirkuliše pomodni pojam “viralnog marketinga”. Njegova polazna tačka je da se izvesne grupe konzumenata, pre svega medijski i robno osvešćeni mladi pokazuju kao sve otporniji u odnosu na klasične forme reklamiranja. Stoga se započelo sa suptilnim brand-iranjem, sa događanjima poput clubbing-a i ravea, snowboard i skateboard dešavanja. Pritom je ultimativna ideja da sponzori više ne dovode svoj logo u vezu sa dešavanjem, već ono sami postaju dešavanje. Konzumenti treba da proizvedu kampanju vlastitim podsticajima, utoliko što će posegnuti za jedan od mamaca bačenih od strane firme i što će ga među sobom dalje deliti. U najpovoljnijem slučaju mamac, kao u slučaju “Flat Eric”, može i sam postati pop zvezda. Asocijacija sa nalogodavcem onda usledi na zadnja vrata jer nipošto ne sme delovati da je kampanja nametnuta: sve mora izgledati tako, ako da je jedan takav “medijski-događaj” u stvari činjenično proizveden od strane samih kupaca. Na sceni firmi za proizvodnju zaštite od virusa i software-a, viralni marketing biva shvaćen manje metaforično, a više praktično. Tamo već odavno ima sve više prigovora da pažnja koju mediji poklanjaju virusima i virus-histerija koja iz nje proizlazi, uopšte nisu toliko uzaludni. To doseže sve do okrivljavanja da su pravi virusi zapravo izuzeti iz medija, da bi se pravovremeno pripremila odgovarajuća digitalna zaštita (o tome vidi članak “Vi nas volite.txt.vbs” Janka Retgersa). Čak i najveće branše su već podlegle naklapanju kada se radi o tome, da se usisavanjem virus-hypes poput Melissa i I LOVE YOU, mreža korisnika povećava. Međutim, čini se da su oni koji posredstvom negativnog publiciteta pokušavaju da povećaju svoje učešće na tržištu najčešće mali autsajderi. Izveštaji na udarnim websites poput vnunet.com svedoče o takvim slučajevima, u kojima su firme širile upozorenja o navodnim epidemijama

virusa, a za ta upozorenja se naposljetku ispostavilo da su drastično preterana. Vrhunac ironije nastaje kada, kao što se već događalo, software za zaštitu od virusa i sam proizvodi lažna upozorenja na viruse. Opravdano upozorenje manjeg proizvođača na 'crv' koji se nalazi na homepage - virus-skener renomiranog proizvođača treba pogrešno da identifikuje kao virus, te da nakon toga pošalje upozorenje na virus. Na kraju se čini da ni sami programi za zaštitu od virusa više nisu zaštićeni od virus-hoax-a. Jedan izdavač knjiga sebi može pripisati sumnjivu slavu koja se sastoji u zastupanju klasičnog virus-hoax-a kao sredstva za podsticanje prodaje proizvoda koji nema veze sa kompjuterom. Godine 1996. na ekranima se pojavilo upozorenje na viruse pod naslovom "Irina" . Jedan istraživač virusa prepoznao je sličnost sa "Good Time" hoax-om, raširivši svoje saznanje na odgovarajućim bulletin board-ovima. Prema jednim engleskim dnevnim novinama, radilo se o PR-Gag-u koji je dospeo na stranputicu. Izdavaču Penguin Books palo je na pamet da na web-u objavi roman pod naslovom "Irina". Tadašnji direktor Electronic Publishing-a imao je zadatak da lažno upozorenje na viruse "Irina" pošalje izabranim časopisima, svakako bez spominjanja Penguin Books i njihovog projekta interaktivne knjige. Kao pošiljalac upozorenja na viruse naveden je profesor Eduard Predo (Edward Prideaux) sa (nepostojećeg) "College of Slavonic Studies in London". Pojam "viralnog marketinga", tri mladića iz Holandije shvatila su previše doslovno. Oni su priznali krivicu za slanje homepage 'crva' u svet . Iskoristili su feature koji je u međuvremenu postao široko poznat, naime da Microsoft Outlook putem jednog API može pokrenuti druge programe za izvođenje Scripts. "Homepage" je funkcionisao tako da bi korisnik koji klikne na attachment HOMEPAGE.HTML.VBS, između ostalog, otvorio četiri prozora Internet Explorer-a koji vode ka porno-site-ove. Nije poznato da li su autore i činjenično povezivali poslovni interesi sa tim porno-site-ovima. Prema njihovim vlastitim izjavama oni su se samo nadali da će sa svojim crvom započeti karijeru u stvarima viralnog marketinga i da će ljudima moći da pokažu "radost da se na mreži bude zloban". E-Mail-Hoaxes u umetničkoj sceni na mreži Kao što se moglo i očekivati, e-mail hoaxes su u umetničkoj sceni na mreži stekli veliku popularnost. Hoax-i imaju veliku tradiciju pre svega u književnosti. Rasprave iznošene u prepisci između rivalskih frakcija, članci i pamfleti potpisani lažnim imenima i vesti širene u klevetničkoj nameri, određivali su međusobne sporove generacija umetnika, izazivajući u njihovim krugovima velika talasanja – pri čemu su pojedinci izvan tih krugova na te provokacije najčešće ostajali u potpunosti hladni. Tako se odvijala i elektronski ubrzana komunikacija umetničke scene na mreži u drugoj polovini devedesetih godina. Ta faza donela je ponovno oživljavanje neokonceptualizma oslonjenog na mrežu, pri kojem se često činilo da je komunikacija važnija od produkcije umetničkih dela. To u svakom slučaju nije prigovor, već stav. U doba burnog razvoja čisto nastavljanje kretanja duž razvojnih linija novih ideja čini se važnije nego ustrajavanje na jednom pronađenim istinama. Pod tim stanovištem valja sagledati budni interes za hoax-taktike u umetničkoj sceni na mreži, pri čemu je navođenje lažnog identiteta u e-mail-ovima i širenje lažnih činjenica pod takvim pokrivenim-identitetima, jedan od najomiljenijih načina postupanja. Onaj nepoznati Hoaxer, koji je na mailing listi Syndicate pokušao da inscenira sukob između teoretičara medija Herta Lovinka (Geert Lovink) i aktiviste mreže, odnosno ICANNspecijaliste Ted Bajfilda (Ted Byfield), odviše opušteno je shvatio hoax-taktiku. U svakom slučaju, gotovo niko nijedne sekunde nije poverovao u to. Jednostavno se nije uklapalo u profil ličnosti tih prepređenih zvezda scene na mreži, da jedan drugom javno nabacuju prejake izraze poput "seronjo". Pošiljalac takođe nije bio zaista vešto prikriiven, već je lako putem analize e-mail uzglavlja identifikovan od strane anonimnog Šveđanina koji mu je odgovorio na mail. Mnogo više truda

uložio je Hoaxer koji je preuzeo e-mail identitet umetničkog kritičara i teoretičara Timoti Drakrija (Timothy Druckrey), kao i pisca i umetnika Marka Amerike, šaljući pod njihovim imenima priloge na mailing liste koji su se činili prikladni da izazovu nezadovoljstvo i da formiraju raspoloženje protiv Drakrija i Amerike. Protiv njih ili protiv Hoaxer-a radila je činjenica da i Drakri i Amerika neguje krajnje individualni stil pisanja koji uprkos očevidnog truda nije mogao biti zaista verodostojno imitiran. Uprkos tom nedostatku “mnogo buke ni oko čega” imalo je barem izvesnu literarnu auru. Da su male, tesno povezane zajednice na mreži naročito prikladne kao ciljevi hoax-a, pokazao je onaj hoaxer koji je 1999. godine diskreditovao odluku za dodeljivanje nagrade umetničkog festivala medija Ars Electronica . Tada se radilo o e-mail-u koji je na udarne mailing liste poslat tačno početkom festivala, pobudivši privid da je poslat kao protestna nota od strane četiri od pet članova žirija nagrade Prix Ars u kategoriji .net umetnost. Prestižna nagrada je 1999. godine dodeljena je poslovnom sistemu Linux. Četiri navodna člana žirija žalila su se da je glasanje petog člana žirija bilo izmanipulisano u interesu sponzora festivala. Festival su sponzorirala velika IT-preduzeća koja su planirala, tako se moglo pročitati u obaveštenju, da ponude i samu Linux distribuciju, pa su stoga podmitili jednog člana žirija da bi još više favorizovali Linux-Hype. Premda su u potpunosti pali sa neba, ti prigovori su igrali na kartu očekivanog ponašanja u zajednici na mreži i nesputanog priključivanja na Linux-Hype koji je tada dosegao svoj prvi vrhunac sa rezultatom da je proključala kuhinja za zakuvavanje tračeva u umetničkoj sceni na mreži. Jednom probuđenu sumnju više nije moglo u potpunosti da odstrani iz sveta ni prikrivanje hoax-a na Telepolis-u. Gotovo legendaran je kombinovani e-mail i web-hoax koji je početkom 1996. godine inscenirala grupa umetnika Etoy sa “Digital Hijack”-om. Etoy je najpre uz pomoć software robota analizirala pet najfrekventnijih internet pretraživača da bi ustanovili koji pojmovi za pretragu bi najčešće bili u opticaju, odnosno kako ti pojmovi moraju biti aktivirani u izvorni kôd wesite-a, da bi u redosledu (ranking) mašine za pretragu bili što je moguće više pozicionirani. Tada je redosled funkcionisao na temelju principa koji su bili doista jednostavni. Odgovarajući pojam za pretragu morao bi se javljati što je moguće češće, svakako u tekućem tekstu a ne jednostavno pedeset puta ponovljen u HTML-Tag-u na početku opisa stranice. U skladu sa zadobijenim rezultatima, Etoy je programirao website koji je često sadržavao pojmove za pretragu poput “sex” i “Porsche”, sa ciljem da, ukoliko je moguće, dospe među prvih trideset izlistavanja neke pretrage. Kada bi oni što pretražuju stigli na Etoy-site, uz pomoć Refresh Metatag-a koji je u unapred programiranim intervalima bez ikakvog učinka korisnika, pozivao nove stranice. Korisnici bi “ostali zarobljeni” u njihovom website-lavirintu. Na taj način, Etoy grupi je pošlo u rukom da za svega nekoliko meseci “otmu” milion i po korisnika. Sa pratećom e-mail kampanjom i za to adekvatnom, ekstremnom retorikom o “digitalnoj otmici”, Etoy je dospela u tada veoma uticajni Wired-Magazine i dobila je prvu nagradu u kategoriji umetnosti na festivalu Ars Electronica . U sličnom duhovnom ambijentu odvijale su se i akcije grupe RTMark, koja se specijalizovala za dizajniranje lažnih website-a političara i firmi, i najstojići da plimu poseta skrene prema tom site-u balansiranjem između činjenica i fikcije. Hit Banting (Heath Bunting) i Rejčel Bejker (Rachel Baker) su nastojali da lansiraju upravo praktične ludorije koji su preko svog servera irrational.org, između ostalog, izdavali i lažne studentske legitimacije iz Meksiko Sitija, nagovarali surfere na živčiranje svojih sugrađana putem policijskih web kamera, a zajedno sa ruskim umetnikom Aleksejem Šulginom (Alexej Shulgin) dodeljivali su “zlatne internet medalje” najnemaštovitijim korisničkim Homepages. Umetnički par Jodi dizajnirao je website koji se igrao sa korisničkim strahom od browser-crash-a, virusa i rušenja sistema. U jednom

ranijem radu Jodi se i eksplicitno pozvao na omaž “Good Times” hoax-u. Zajedno sa Vukom Ćosićem, umetnikom koji živi u Sloveniji, Banting, Beijker i Šulgin su mogli zahtevati da se pojam net.art oblikuje u istom tom rukopisu i da odlučujuće utiču na ranu umetnost na mreži. Čini se da je njihov poslednji zajednički hoax da su se – izuzimajući Jodi – od otprilike 1999. godine deklarirali kao “retired net.artists”, takoreći rano penzionisani umetnici mreže. Ono što povezuje pomenute umetnike moglo bi biti okarakterisano kao uspešni viralni marketing na mreži. Bez prisustva na uobičajenim instancama pogonskog sistema umetnosti, oni su sebi stvorili publiku čisto putem komunikacije na mreži, a samim tim i izvesan stepen slave. Rasipanje medijalnih virusa koji se poput trojanskog konja uvlače u sisteme koji prerađuju informacije korisnika, povećalo je njihovu vrednost na mreži – bolje rečeno na engleskom “net value” - kao umetnika. Na sličan način je u poslednjih par godina “Netočka Nezvanova” (koja se docnije pojavila) postala ekstremno poznata osoba na mreži – po dobrom kao i po lošem. Pod pseudonimom Netočka Nezvanova (Netochka Nezvanova) koji je pozajmljen iz jednog romana-fragmenta od Dostojevskog, pomenuta osoba je razvila sasvim ličan e-mail stil. Po promenljivim korisničkim adresama i domenima poput “god-emil”, “m9ndfukc” i napokon “relativno” konstantnim domenom “integrer”, svoje e-mail-ove ona je formatirala tako, kao da su prošli kroz ludo zabavni program mešanja slova. Prema zakonitosti koju je bilo teško prozreti, pojedinačna slova bi bila zamenjena drugim znakovima ASCII-kôdovima poput uzvičnika, zareza, zagrada i brojeva. Rezultat je ponekad podsećao na programski kôd, a nekad opet na prirodni jezik pri čemu je ovaj potonji bilo teško razlučiti. Samo onaj ko se upustio u taj kôd i potrošio mnogo vremena na njegovo dešifrovanje mogao je isfiltrirati nešto poput značenja iz mail-ova Netočke Nezvanove. Sa tim e-mail stilom ona se vrzmala oko brojnih mailing lista i njihove moderatore dovodila do napada besnila. U svojim najlošijim danima bombardovala je mailing liste sa tucima takvih vesti, što je dovodilo do isključenja niza foruma. Pri okršajima koji su se pritom razgoreli, mnoge muške mail moderatore ona je rado psovala kao “mail korporativni fašisti”, što ih je samo još više izluđivalo. Pri delimično visokom broju dnevnih post-ova, razumljiv je bes moderatora i učesnika na listama. Ono što ipak začuđuje jeste stepen neprijateljstva koji provocira takav stil komunikacije. Premda njeni e-mail-ovi nisu sadržali virus i nisu iznosili upozorenja na viruse, čini se da njena tehnika na suptilan način oslovljava virus-paranoju. Oni su se pojavljivali kao neka vrsta prljavštine na forumima koji su u stvari predodređeni za racionalnu diskusiju – haotične zbirke ASCII-znakova siglaniziraju opasnost od subverzije i zaraze zajedno sa strahom od onoga što se ne može identifikovati. Muškarce određenog karakternog sklopa njene poruke doista mogu dovesti do ivice ludila, pa se utoliko njihov paušalni prigovor i ne čini sasvim neutemeljen. Pritom se Nezvanova e-mail-ovi u stvari veoma lako mogu identifikovati, pa samim tim i profilirati bez ikakvog posebnog truda. Ali, pri detaljnijem uvidu, oni sadrže zaista suptilne vesti koje se često na dekonstruktivan način odnose na prethodnu poštu i uokviruju se sa ASCII-grafikom i indirektnim komentarima. Čitljivi redovi koji su tu između moduluju i variraju određene teme, poput “umetnost mašina”, “memepool” i druge zanimljive reči insajderske kulture na mreži. Putem konsekventnog prikrivanja vlastitog identiteta, Netočka Nezvanova je stvorila umetničku ličnost u kojoj je postala ultimativna hoax-kraljica mreže. Njeni e-mail-ovi bude asocijacije, kao da negde na mreži postoji neka veštačka inteligencija koja permanentno reciklira novosti, meša značenja, izaziva konflikte i sa proročkim kvalitetima dešavanjima na mreži daruje čaroliju koja se inače tako retko može osetiti u uobičajenoj fiksiranosti na korist i produktivnost mreže

8. ZAKLJUČAK

U ovom radu sagledan je pojam i vrste cyber kriminala. Već prilikom pokušaja njegovog definisanja, uočile su se prve teškoće. Naime, ma koliko se svako pojmovno određenje cyber kriminala na prvi pogled činilo adekvatnim, vrlo brzo se uočavalo da je ovaj oblik kriminalnog delovanja toliko složen, da je vrlo teško iskazati u jednoj definiciji njegovu specifičnost, sadržajnost i značenje za društvenu zajednicu.

Razmatrajući posledice cyber kriminala, očigledno je da se isti razlikuje od svih drugih oblika kriminalnog delovanja po stepenu opasnosti u odnosu na napadnuta dobra. Ova konstatacija je još više došla do izražaja kada se shvatilo da mnoge kriminalne aktivnosti potpomognute uticajem oblika cyber kriminala postaju još opasnije i štetnije. Tanka linija razdvajanja sajber kriminala, sajber terorizma i rata u sajber prostoru danas je potpuno izbledela; ima indicija da neke zemlje vide kriminalne i terorističke grupe kao korisne saveznike i da su već pokazale spremnost da tolerišu, ohrabruju, pa čak i usmeravaju pojedince i grupe da napadaju neprijateljske ciljeve. Sve veća zavisnost nacionalnih ekonomija i državne uprave od kritične ICT infrastrukture, njena uzajamna i prekogranična povezanost sa drugim infrastrukturama, u okruženju brojnih pretnji i rizika, kao imperativ nameću potrebu za sistematskim rešavanjem problema suprotstavljanja syber napadima velikih razmera.

Od prvih pojavnih oblika, početkom 90-ih, do danas mnoga su međunarodna tela posvetila pažnju ovom kriminalu. Pored međunarodne sve je učestalija i nacionalna regulacija cyber kriminala, odnosno nekih od njegovih oblika. Zanimljivo je da se mnogo više aktivnosti dešava na međunarodnom u odnosu na nacionalni plan. Nije za pohvalu to što Srbija, iako je još 2005. pristupila, a u martu 2009. i ratifikovala Konvenciju o visokotehnološkom kriminalu Saveta Evrope, još uvek nije implementirala sve obaveze koje je tim činom preuzela.

Ipak, ohrabruje činjenica da Srbija, kao i mnoge države postaju svesne ove pojave i da su u svom pozitivnom krivičnom zakonodavstvu predvidele pojavne oblike cyber kriminala kao posebna krivična dela. Poslednjih godina zemlje širom sveta ubrzano donose strategije za sprečavanje zloupotreba Interneta, a članice EU su takođe odlučile da unaprede sudsku i policijsku saradnju tako što će formirati jednu agenciju za cyber kriminal koja bi mogla da bude pridružena Europolu, policijskoj agenciji EU. Na pomolu je podudarnost interesa velikih sila da se cyber criminal obuzda. Industrijska špijunaža je međutim nešto drugo i to je već postao središnji problem između Kine i SAD. Ipak, ono što je nasušna potreba danas je međunarodni sporazum o osnovnim pravilima ponašanja u cyber prostoru. Ono što predstavlja dodatni problem u suzbijanju cyber kriminala je problem građanskih prava i sloboda, jer iole savršeni softver za nadzor kriminalaca proizvodi i "kolateralnu štetu" – narušava privatnost i nedužnih.

Sa druge strane, ohrabrujeće je i to što se u sve većem broju naučnih i stručnih radova pažnja posvećuje upravo ovom obliku kriminalnog ponašanja. Na taj način dolazi do razotkrivanja mnogih specifičnosti cyber kriminala, a istovremeno se otvara mogućnost suprotstavljanju njegovim oblicima od strane društvene zajednice.

Literatura

- [1] APIS Security consalting, Kompjuterski kriminalitet,
<http://www.apisgroup.org/sec.html?id=29> 14.11.2011.
- [2] Arsenin Aleksandar, Sekte na internetu,
<http://www.internetservis.co.rs/virtuelnodetinjtvo/3.php?idtxt=28> 17.11.2011
- [3] Babović Miloš, Kompjuterska prevare i Internet prevara, Članak objavljen u zbirci, Symorg 2004.
- [4] Bellamy William, TCP Port 80 - HyperText Transfer Protocol (HTTP) Header Exploitation
http://www.cgisecurity.com/lib/bill/William_Bellamy_GCIH.html#ClintonWong
15.11.2011
- [5] Chik B. Waren, Challenges to Criminal Law Making in the New Global Information Society, www.law.ed.ac.uk/ahrc/complaw/docs/chik.doc 13.11.2011.
- [6] Cyber-Rights & Cyber-Liberties, Advocacy Handbook for NGOs <http://www.cyber-rights.org/cybercrime/> 17.11.2011
- [7] Declan McCullagh, Beefed-Up Global Surveillance
<http://www.wired.com/politics/law/news/2002/02/50529> 17.11.2011.
- [8] Dr, Mirjana Drakulić, mr Ratimir Drakulić, Cyber kriminal, Fakultet organizacionih nauka, Beograd
- [9] Dr Dragan Prija , Kompjutersko pravo – slajdovi sa predavanja, Beograd, 2011.
www.prlja.info
- [10] Dr Dejan Simić, Slajdovi sa predavanja Tehnike zaštite u računarskim mrežama, FON, Beograd.
- [11] Đukić Bratislav, *Nigerijske email prevare otuđile preko 2 miliona dolara u Srbiji i Hrvatskoj* <http://www.inforepublic.org/2010/02/03/nigerijska-email-prevara-odnijela-preko-2-miliona-dolara-u-srbiji-i-hrvatskoj/> 16.11.2011.
- [12] Encyclopedia of cyber crime,
<http://www.scribd.com/doc/20262442/Encyclopedia-of-Cyber-Crime> 15.11.2011.
- [13] European committee on crime problems,
<http://www.cdt.org/international/cybercrime/020107coe.pdf> 17.11.2011.
- [14] Internet World Stats, <http://www.internetworldstats.com/stats.htm> 13.11.2011.
- [15] Global Play Fair Day, Full BRIC Country Study,
<http://www.microsoft.com/presspass/presskits/antipiracy/Default.aspx> 15.11.2011.

- [16] Necin Goran, Armagedon za srpske pedofile, <http://www.internetservis.co.rs/virtuelnodetinjtvo/3.php?idtxt=28> 17.11.2011.
- [17] Petrović R. Slobodan, Policijska informatika, Kriminalističko-policijska akademija, Beograd, 2007.
- [18] Petrović Slobodan, *Kompjuterski kriminal*, MUP R. Srbije, Beograd, 2000.
- [19] Revealed: Operation Shady RAT <http://www.mcafee.com/us/resources/white-papers/wp-operation-shady-rat.pdf>
- [20] Robinson J., Internet as the Scene of Crime, International Computer Crime onference, Oslo, 2000., www.ccips.org 15.11.2011.
- [21] Sexual Abuse of Children on the Internet: A New Challenge for INTERPOL, <http://unesdoc.unesco.org/images/0011/001147/114734eo.pdf> 17.11.2011.
- [22] SpamCop Statistics, <http://www.spamcop.net/spamgraph.shtml?spamyear> 15.11.2011.
- [23] Symantec, Cybercrime Report for 2011, http://www.symantec.com/content/en/us/home_homeoffice/html/cybercrimereport/ 13.11.2011.
- [24] Tenth United Nations Congress on the Prevention of Crime and the treatment of Offenders, www.oun.org 13.11.2011.
- [25] Trust And Security In Cyberspace: The Legal And Policy Framework for Addressing Cybercrime <http://www.internetpolicy.net/cybercrime/020800cybercrime.pdf> 17.11.2011.
- [26] Webopedia, http://isp.webopedia.com/TERM/C/cyber_crime.html; Koenig D., *Investigation of Cybercrime and Technology-related Crime*, <http://www.neiassociates.org/cybercrime.htm> 15.11.2011.
- [27] Frank Patalong, "PeekaBooty"; Jetzt kommt der Hacker-Browser, Spiegel Online, 8.5.2001, <http://www.spiegel.de/druckversion/0,1588,132661,00.html>
- [28] <http://www.cspam.com> (18) <http://www.visi.com/~drow/spam> (19) <http://ga.to/mmf>
- [29] <ftp://ftp.de.pgpi.com/pub/pgp> ili preko Network Associates, Inc.
- [30] <http://www.rafael-seifert.de/goodtime.htm>
- [31] Chik B. Waren, Challenges to Criminal Law Making in the New Global Information Society, www.law.ed.ac.uk/ahrc/complaw/docs/chik.doc 13.11.2011.
- [32] Internet World Stats, <http://www.internetworldstats.com/stats.htm> 13.11.2011.
- ¹ Symantec, Cybercrime Report for 2011, http://www.symantec.com/content/en/us/home_homeoffice/html/cybercrimereport/ 13.11.2011.

[33] ¹ Webopedia, http://isp.webopedia.com/TERM/C/cyber_crime.html; Koenig D., *Investigation of Cybercrime and Technology-related Crime*, <http://www.neiassociates.org/cybercrime.htm>

[34] APIS Security consulting, Kompjuterski kriminalitet, <http://www.apisgroup.org/sec.html?id=29> 14.11.2011

[35] Dostupno na <http://www.scribd.com/doc/20262442/Encyclopedia-of-Cyber-Crime> 15.11.2011.

[36] Dostupno na <http://www.mcafee.com/us/resources/white-papers/wp-operation-shady-rat.pdf> 15.11.2011.

[37] Babović Miloš, Kompjuterska prevare i Internet prevara, Članak objavljen u zbirci, Symorg 2004.

[38] Dostupno na <http://www.inforepublic.org/2010/02/03/nigerijska-email-prevara-odnijela-preko-2-miliona-dolara-u-srbiji-i-hrvatskoj/> 16.11.2011.

¹ Petrović R. Slobodan, Policijska informatika, Kriminalističko-policijska akademija, Beograd, 2007.

[39] Global Play Fair Day, Full BRIC Country Study, <http://www.microsoft.com/presspass/presskits/antipiracy/Default.aspx> 15.11.2011.

[40] Sexual Abuse of Children on the Internet: A New Challenge for INTERPOL, <http://unesdoc.unesco.org/images/0011/001147/114734eo.pdf> 17.11.2011.

[41] Necin Goran, Armagedon za srpske pedofile, <http://www.internetservis.co.rs/virtuelnodetinjtvo/3.php?idtxt=28> 17.11.2011.

[42] Arsenin Aleksandar, Sekte na internetu, <http://www.internetservis.co.rs/virtuelnodetinjtvo/3.php?idtxt=28> 17.11.2011

[43] Dr Mirjana Drakulić, mr Ratimir Drakulić, Cyber kriminal, Fakultet organizacionih nauka, Beograd,

Dostupno na <http://www.internetpolicy.net/cybercrime/020800cybercrime.pdf> 17.11.2011

Dostupno na <http://www.cyber-rights.org/cybercrime/> 17.11.2011.

Dostupno na <http://www.cdt.org/international/cybercrime/020107coe.pdf> 17.11.2011.

Dostupno na <http://www.wired.com/politics/law/news/2002/02/50529> 17.11.2011.