# 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 komjuterski 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 kominkacionih 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 uredaji 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 ilegelnog preuzimanja muzickih 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. Kradu 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 sveobuvatna 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 sabotaže;
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 kriminala[9] navodi se da FBI i Nacionalni centar za kriminal belih kragni 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 sabotaža;
- 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
- phiching
- prisluškivanje
- praćenje e-konferencija
- prikačinjanje i analiza “cookies”.

Jasno je da veliki broj različitih klasifikacija sam po sebi pokazuje raznovrsnost ovih dela i kompleksnost njihovih pojavnih 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, Keyloger,...), trojanski konji (specijlni 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 goodina.


Slika 1. Zemlje koje su bile mete napada špijunaže[10]

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 Sajentološku 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 pritisnute 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 gigbajta 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 uzvrati 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 iza 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 prismotre, 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 Encycopedia - ''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 Sjedninjenoh 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 sto karakterise cyber prevare ja da one daleko dopiru zbog veličine Interneta kao tržista, da se brzo šire jer sa Internetom kao medijem sve se dešava mnogo brže, i niski troškovi izvodjenja 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 transkacija. 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 gradjana, a prevaratni su ostvarili dobit od oko 20 miliona dolara.

### *3.7. Krađa Internet usluga*

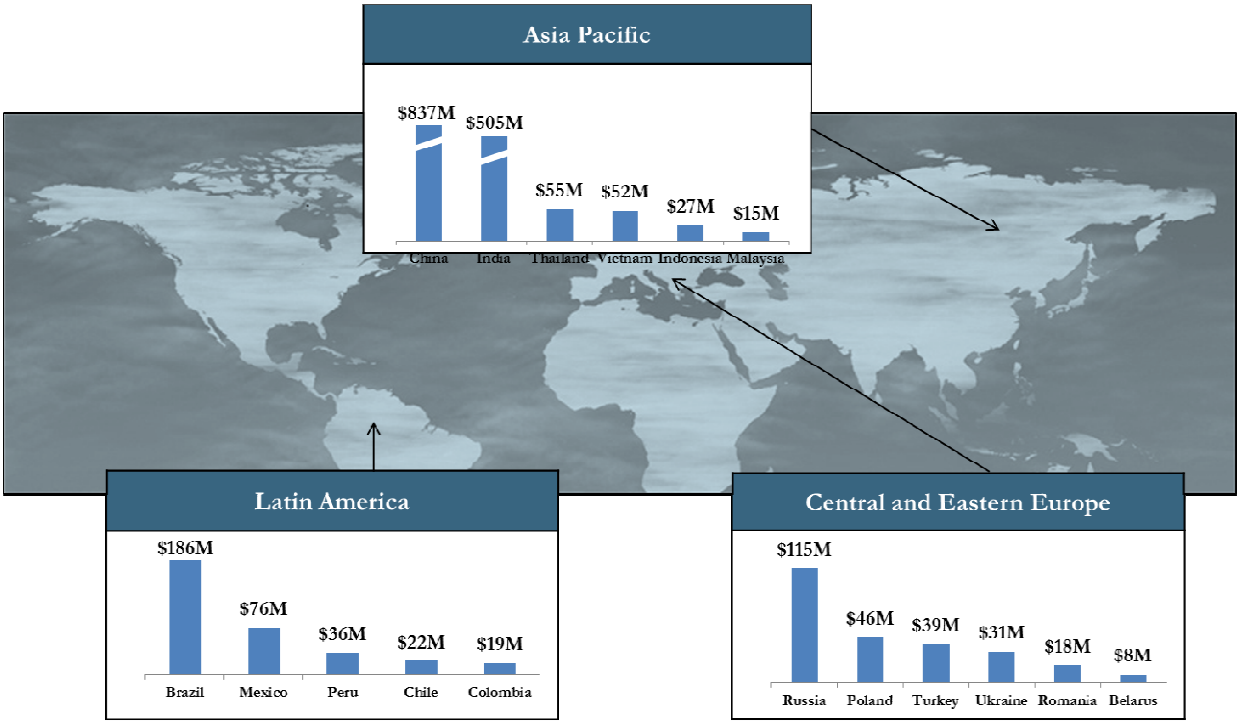
Krađa računarskih usluga, odnosno neovlašćeno korišćenje sistema, je veoma rasprostranjena pojava u oblasti informacione tehnologije, a cilj joj je da se za obavljanje privatnih poslova koriste tuđi računarski resursi. [14]

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 tudje 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 Daya, 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 piratsvta[16]

Microsoft istraživanje je pokazalo da je nezakonito poslovanje putem korištenja 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 mogucim 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 sluzbenika 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 vreba 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 menažeri bezbednosti.

### *3.10. Internet aukcije*

Aukcijske prevare na internetu danas su jedne on 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 krimniala 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 inzvanredne mogućnosti da se preko njega sprovode 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 finansijke probleme veoma često pribegavaju ovakovom 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 odredjene 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:

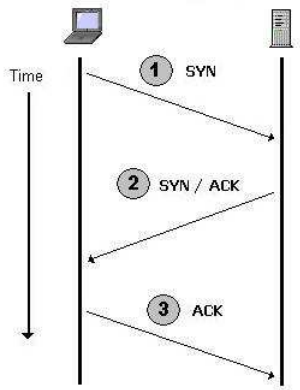
- ✓ keylogger može biti instaliran kada korisnik otvori datoteku u prilogu e-mail-a;
- ✓ keylogger može biti instaliran kada se datoteka pokrene iz otvorenog pristupa direktorijumu na P2P (Peer 2 Peer) mrežu;
- ✓ keylogger može da se instalira preko skripte veb stranice koja eksploatiše ranjivost pretraživača. 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 rukovanje[20]

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 telneta enkriptuje celokupan saobraćaj u komunikaciji između korisnika i servera.

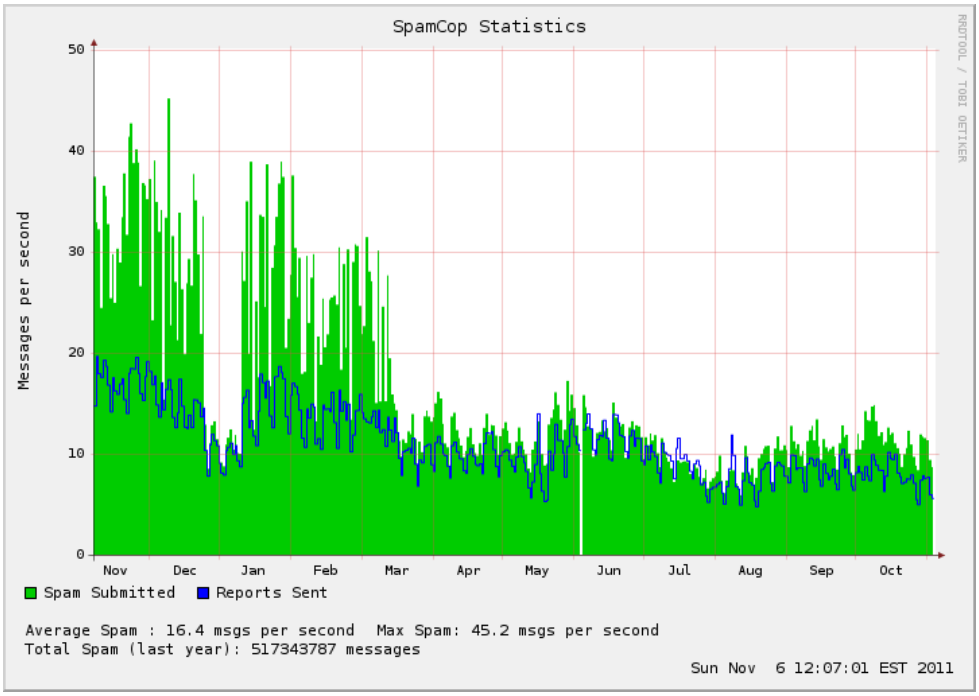
Pored prisluškivanja telnet sesija moguće je prisluškivati i sve ostale TCP/IP sesije koje ne koriste metode kriptovanja. Samim tim znači da je jedan od servisa koji je i doprineo velikoj popularizaciji interneta, e-mail, takođe ugrožen.

### *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, spamerske 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 spama[21]

## *3.15. Phishing*

Phishing je oblik sajber-kriminala zasnovan na metodama društvenog inžinjeringa. 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.

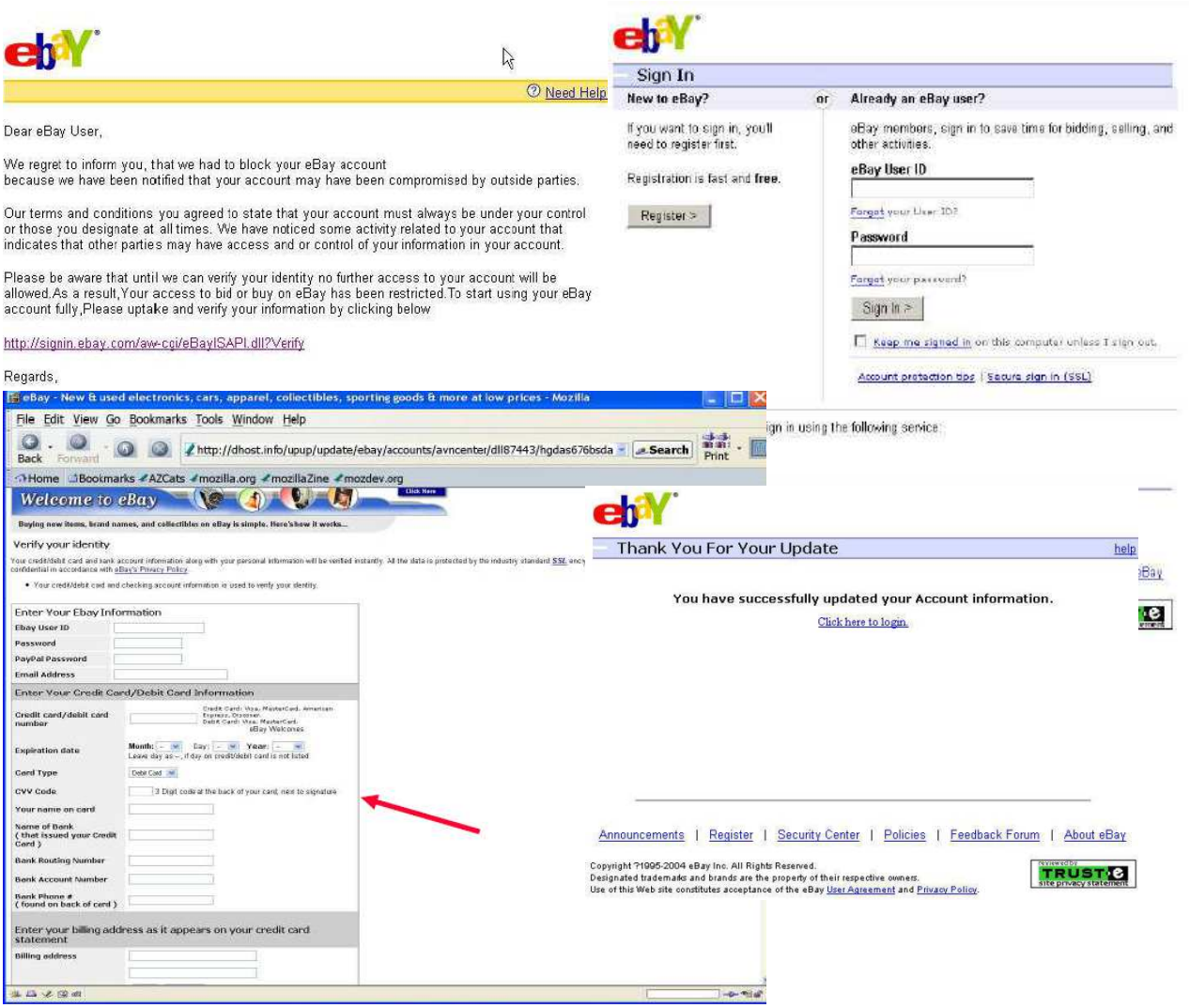
Sajber-kriminalci stvaraju savršene kopije komercijalnih web sajtova finansijskih insitucija. Oni potom nastoje da namame korisnike, koji naravno ništa ne sumnjaju, na sajt kako bi u lažnim formularima na sajtu ostavili svoje login podatke, šifru, broj kreditne kartice, PIN itd. Ove podatke sakupljaju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

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 napada[22]

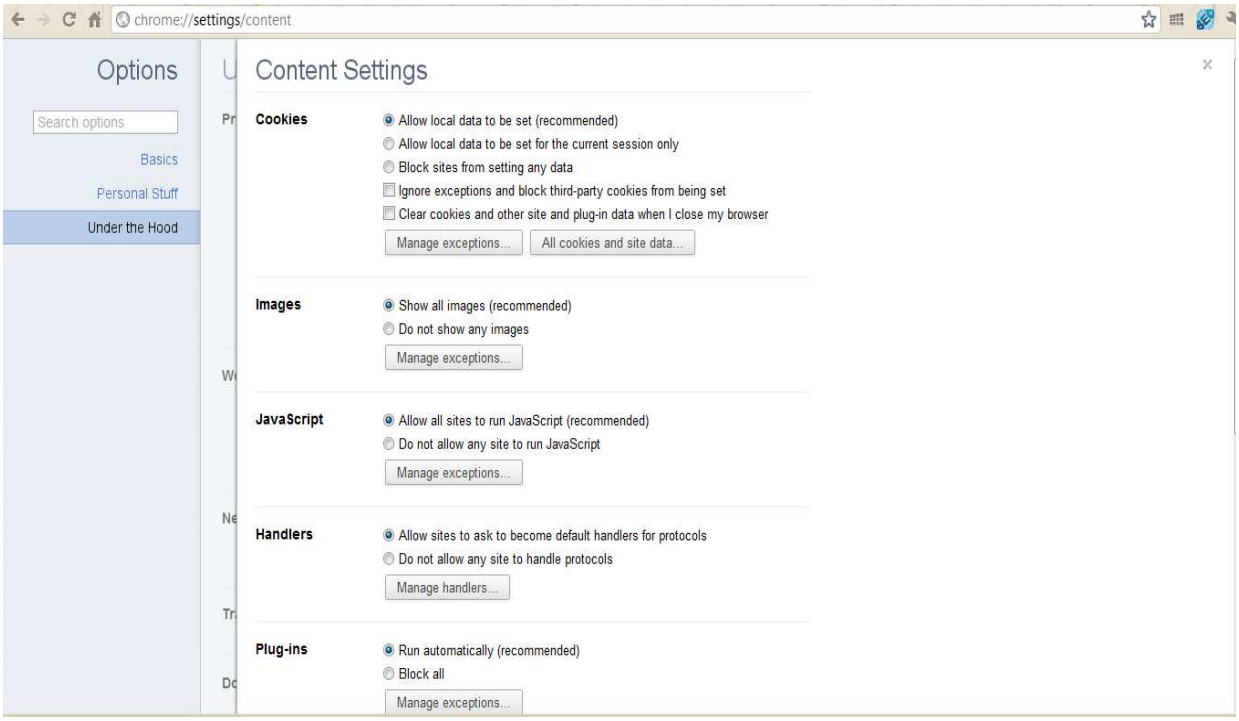
### *3.16. Analiza kolačića (cookies)*

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 koristiće 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 zaštiti 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.