CYBER KRIMINAL

Mirjana Drakulić[1] Ratimir Drakulić[1],
[1]*Fakultet organizacionih nauka u Beogradu*

Sadržaj: *Globalne kompjuterske mreže stvorile su mogućnosti za nove oblike kriminala. U radu se prezentiraju oblici i aktivnosti borbe protiv cyber kriminala.*

1. UVOD

Globalne računarske mreže stvorile su mogućnosti za nove oblike kriminala. Pojavljuje se poseban, sufisticiran, prodoran, tehnički potkovan, beskrupulozan, opsednut, ponekad osvetoljubiv pojedinac [1] kome je teško suprotstaviti se a još teže zaustaviti ga. On sve češće ne želi da bude sam već mu je potrebno društvo, kao što mu je neophodna i "publika". Lakoća "vršljanja" cyber prostorom daje mu osećaj moći i neuhvatljivosti. Ovi osećaj nisu bez razloga, jer stavrno ga je izuzetno teško otkriti u momentu činjenja dela, što, uglavnom, predstavlja i "pravi" trenutak za njegovo identifikovanje i hvatanje. S druge strane, Internet koji je toliko ranjiv i nesiguran zbog ogromnog broja korisnika (računa se da je u toku 2004. godine broj korisnika Interneta narastao na (na dan 25. mart 2005. godine broj korisnika Interneta bio je 888,681,131, odnosno 13.9% ukupne svetske populacije), otvorenosti i neregulisanosti je i idealno skrovište kriminalaca različitog tipa.

U takvom okruženju i sa takvim pojedincima sve se češće pokušavaju izboriti ne samo mnoga nacionalna prava, međunarodne organizacije i asocijacije, već se uključuje i "privatni sektor" i korisnici ne bi li se ublažile negativne posledice i smanjili gubici koji nastaju zbog neomatanih kriminalnih aktivnosti. Tako na primer, finansijski cyber kriminal je Australiju u 2003. godini koštao preko 3,5 miliona dolara, a virusi, crvi i trojanci preko 2 miliona [11]. Sledeće godine finansijski cyber kriminal pada na 2 miliona dolara, ali su zato guvici od virusa narasli na preko 7 miliona. Ni Britanci nisu prošli bolje, njima je u 2003. godini finansijski cyber kriminal odneo preko 120 miliona funti, a virusi 27,8 miliona [12]. Privatnici i korisnici postaju naročito značajna grupa u stvaranju uslova za zaštitu privatnih kompjuterskih mreža i njihove povezanosti sa javnim, globalnim. Razvoj sigurne Internet infrastrukture ne može se zamisliti bez zajedničkih aktivnosti svakog od ovih aktera [2], tim više što cyber kriminal postaje globalni problem. A šta je on, u stvari?

2. CYBER KRIMINAL - POJAM I OBLICI

Trebalo je da prođe niz godina od pojave prvih oblika kompjuterskog kriminala do njegovog definisanja i taman su nastale neke svodne definicije kada se pojavljuje novi fenomen – cyber kriminal. Tako pokušavajući da se protumače razmere ovog kriminala i njegove opasnosti u dokumentu **Kriminal vezan za kompjuterske mreže** (*Crime related to computer networks*) sa Desetog kongresa Ujedinjenih Nacija posvećenog Prevenciji od kriminala i tretmanu počinioca od aprila 2000. godine [3] 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 međusobno povezanih uređaja kojima se vrši automatska obrada podataka (ili bilo kojih drugih funkcija)" kako je to definisano u **Konvenciji o cyber kriminalu** (*Convention on Cybecrime*) [4] Saveta Evrope onda je jasno da bez njih i kompjuterskih mreža nema ovog kriminala. On je kompleksan i čak ga smatraju kišobran-terminom koji pokriva raznovrsne kriminalne aktivnosti uključujući napade na kompjuterske podatke i sisteme, napade vezane za računare, sadržaje ili intelektualnu svojinu. Pri tome se

kompjuterske mreže odnosno informaciono komunikaciona tehnologija pojavljuje u višestrukoj "ulozi" [2], odnosno kao:

a) **Cilj napada** – napadaju se servisi, funkcije i sadržaji koji se na mreži nalaze. Kradu se usluge, podaci ili identitet, oštećuju se ili uništavaju delovi ili cela mreža i kompjuterski sistemi, ili se ometaju funkcije njihovog rada. U svakom slučaju cilj počinilaca je mreža u koju se ubacuju virusi ili crvi, obaraju sajtovi, upadaju hakeri, vršljaju "šunjala", vrši se "odbijanje usluga".

b) **Alat** –kriminalci od pamtiveka koriste kamen, nož, otrov, pištolj i slična oružja i oruđa a danas moderni kriminalci ne "prljaju" ruke koristeći mrežu u činjenju dela i realizovanju namera. Nekada ova upotreba mreže predstavlja potpuno novi alat, dok se u drugim prilikama već postojeći toliko usavršava da ga je teško i prepoznati (čak se spominju i dve varijante: nova dela sa novim alatima i stara dela sa novim alatima). Korišćenje ovog novog oružja naročito je popularno kod dečije pornografije, zloupotreba intelektualne svojine ili online prodaje nedozvoljene robe (droge, ljudskih organa, dece, nevesta, oružja i sl.).

c) "**Okruženje**" u kome se napadi realizuju. Najčešće to okruženje služi za prikrivanje kriminalnih radnji, kao što to veoma vešto uspevaju da urade pedofili, a ni drugi kriminalci nisu ništa manje uspešni.

d) **Dokaz** kao što se u klasičnom kriminalu pojavljuje nož, otrov, pištolj ili neko drugo sredstvo izvršenja dela, tako se i mreža i ICT mogu javiti u dokaznom postupku za cyber kriminal.

Istovremeno, kompjuterska mreža služi kao mreža za povezivanje raznih subjekata, ona je podrška i simbol. Naravno ova poslednja uloga je vezana za zastrašivanje, obmanjivanje, uplitanje.

Bitno je da je cyber kriminalu nesporno priznato "svojstvo" kriminala (pri tome ne treba zanemariti činjenicu da su se pored ovog pojavili i drugi termini: Internet kriminal, eKriminal, kriminal visokih tehnologija, mrežni kriminal, i sl.) kao "obliku ponašanja koji je protivzakonit ili će biti kriminalizovan za kratko vreme" [3]. S obzirom da postoje značajne razlike među zemljama ali i dokumentima međunarodnih organizacija i asocijacije to mala "ograda" na ponašanje koje će biti kriminalizovano u kratkom vremenu predstavlja presedan kojim se žele umanjiti posledice nesinhronizovanosti i neusklađenosti regulative.

Imajući sve to u vidu može se konstatovati da je cyber kriminal takav oblik kriminalnog ponašanja kod koga je cyber prostor okruženje u kome su kompjuterske mreže pojavljuju kao sredstvo, cilj, dokaz i/ili simbol ili okruženje izvršenja krivičnog dela. Pri tome se pod cyber prostorom, podrazumeva ili vrsta "zajednice" sačinjene od mreže kompjutera u kojoj se elementi tradicionalnog društva nalaze u obliku bajtova i bitova ili "prostor koji kreiraju kompjuterske mreže". Termin cyber prostor prvi je upotrebio Vilijam Džibson u naučnofantastičnoj noveli Neuromancer 1984. godine ("*Cyberspace. A consensual hallucination experienced daily by billions of legitimate operators, in every nation, by children being taught mathematical concepts... A graphical representation of data abstracted from the banks of every computer in the human system. Unthinkable complexity. Lines of light ranged in the non-space of the mind, clusters and constellations of data. Like city lights, receding …*"**).**

Ono je veštačka tvorevina koja zahteva visoku tehničku opremljenost, dobru informacionu infrastrukturu i koji je ničija i svačija svojina, u kome paralelno koegzistiraju virtuelno i realno i kod koga je komunikacija kolektivna. U takvom okruženju izuzetno je teško govoriti o nacionalnim razmerama kriminala i društvenoj opasnosti, bar ne u konvencionalnom smislu reči. Zato se ovaj kriminal svrstava u najizrazitiji oblik transnacionalnog kriminala protiv koga ni borba ne može biti konvencionalna. Pogotovo što društveni, socijalni i ekonomski kontekst ovog kriminala nije istovetan sa klasičnim transnacionalnim kriminalom jer za cyberspace važe druga pravila – što pokazuje Globalna studija o organizovanom kriminalu (*Global studies on organized*

crime) Centra za prevenciju od međunarodnog kriminala i Instituta Ujedinjenih Nacija za istraživanje interergionalnog kriminala [5].

Iako postoje brojne teškoće u definisanju ovog kriminala, kao što postoji i izražena 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 što se ni posledice više ne mere nekolicinama žrtava, niti desetinama i hiljadama dolara, dinara, evra, već šestocifrenim brojevima. Problemi nastaju i zbog novih elemenata za diferenciranje ovog od drugih oblika kriminala. Otuda je posebno pitanje koje su to vrste ovog kriminala.

3. TIPOVI CYBER KRIMINALA

Različiti dokumenti na različite načine klasifikuju oblike cyber kriminala. Tako u materijalu za "radionicu" o kriminalu na mreži desetog kongresa UN konstatuje se da postoje dve sub kategorije ovog kriminala [3]:

a) **cyber kriminal u užem smislu** - kao svako nezakonito ponašanje usmereno na elektronske operacije sigurnosti kompjuterskih sistema i podataka koji se u njima obrađuju;

b) **cyber kriminal u širem smislu** - kao 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.

U istom dokumentu navode se i konkretni oblici ovog kriminaliteta u skladu sa **Preporukom Saveta Evrope** i listom OECD-a iz 1989. odnosno 1985. godine. To su: 1) neautorizovani pristup kompjuterskom sistemu ili mreži kršenjem mera sigurnosti (haking); 2) oštećenje kompjuterskih podataka ili programa; 3) kompjuterske sabotaže; 4) neovlašćeno presretanje komunikacija od i u kompjuterskim sistemima i mrežama; i 5) kompjuterska špijunaža. Svaki od ovih oblika može se ukrštati sa svakim jer gotovo da ne postoji "čisti" oblik. Tako haking, pored neovlašćenog ulaska u kompjuterske sisteme i mreže, često obuhvata i uništenje podataka ili kompjutersku špijunažu (kao što je to slučaj sa upadima na veb sajtove i uništenje ili "prepravljanje" podataka na njima ili haking i trgovina pasvordima). Izmena kompjuterskih podataka i programa uključuje i "lansiranje" kompjuterskih crva i virusa što je najčešće praćeno zaustavljanjem rada kompjuterskog sistema, uništenjem podataka. U mrežama crvi i virusi se u većini slučajeva "razmenjuju" elektronskom poštom, a ne retko to čine i hakeri prlikom neovlašćenog pristupa.

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.

Njima se u novije vreme dodaju i dela podržana računarima. Ova dela obuhvataju "rasturanje" materijala ili samo njihovo posedovanje pri čemu se mreža koristi za postizanje boljih rezultata kriminala ili pokušaja izbegavanje pravde. U ova dela se ubrajaju razni nezakoniti i štetni sadržaji, kršenje autorskih i srodnih prava, prodaja zabranjene robe (oružja, kradene robe, lekova) ili pružanje nedozvoljenih usluga (kockanje, prostitucija). Najviše pažnje u ovoj grupi dela privlači dečija pornografija i distribucija raznih materijala Internetom [3].

Evropska konvencija o cyber kriminalu predviđa 4 grupe dela [4]:

a) **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;

b) **dela vezana za kompjutere** – kod kojih su falsifikovanje i krađe najtipičniji oblici napada;

c) **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;

d) **dela vezana za kršenje autorskih i srodnih prava** obuhvataju reprodukovanje i distribuciju neautorizovanih primeraka dela kompjuterskim sistemima.

Naravno, Konvencija pod kompjuterskim sistemom podrazumeva i kompjuterske mreže.

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

a) upade u kompjuterske mreže;

b) industrijsku špijunažu;

c) softversku pirateriju;

d) dečiju pornografiju;

e) bombardovanje elektronskom poštom;

f) "njuškanje" pasvorda;

g) "prerušavanje" jednog računara da elektronski "liči" na drugi kako bi se moglo pristupiti sistemu koji je pod restrikcijama; i

h) krađu kreditnih kartica.

Zavisno od tipa počinjenih dela cyber kriminal može biti:

a) Politički, koga čine:
   1. cyber špijunaža;
   2. haking;
   3. cyber sabotaža;
   4. cyber terorizam;
   5. cyber ratovanje.

b) Ekonomski:
   1. cyber prevare;
   2. haking;
   3. krađa Internet usluga i vremena;
   4. piratstvo softvera, mikročipova i baza podataka;
   5. cyber industrijska špijunaža;
   6. prevarne 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:

   1. dečija pornografija;
   2. pedofilija;
   3. verske sekte;
   4. širenje rasističkih, nacističkih i sličnih ideja i stavova;
   5. zloupotreba žena i dece.

d) Manipulacija zabranjenim proizvodima, supstancama i robama:

   1. drogom;
   2. ljudskim organima;
   3. oružjem.

e) Povrede cyber privatnosti:

1. nadgledanje e-pošte;
2. spam
3. phiching
4. prisluškivanje, snimanje "pričaonica"
5. praćenje e-konferencija
6. 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. U svakom slučaju to bi pored upada u kompjuterske sisteme i mreže, špijunaže, sabotaže, piraterije, bombardovanja elektronske pošte primanjem neželjenih poruka, "njuškanja" pasvorda, "prerušavanja" jednog računara drugim, bili i virusi, odnosno njihova proizvodnja i distribuiranje, kao i ceo skup nedozvoljenih i štetnih sadržaja od dečije pornografije do rasturanja verskih, rasističkih i sličnih sadržaja. Posebno su brojna dela diseminacije nedozvoljene robe ili pružanje nedozvoljenih usluga. Tome treba dodati i cyber sabotaže i terorizam, kao i krađu Internet vremena, usluga, indentiteta, razne zloupotrebe kreditnih kartica.

Ono što je nesporno je da je kompjuterski kriminal više vezan za aktivnosti pojedinaca, a kriminal vezan za kompjuterske mreže više je delo grupa i to organizovanih, profesionalizovanih pa sve češće i strogo specijalizovanih (npr. grupa pod nazivom *Phonemasters* postala je poznata zbog učestalih napada na američki Nacionalni informacioni centar o kriminalu i zato što je pored Amerikanaca uključivala i Kanađane i Švajcarce). Ove grupe su, s jedne strane, "tradicionalne" grupe organizovanog kriminala koje su se usavršile i osavremenile primenom informaciono komunikacione tehnologije i pripremile za "izlazak" na cyber scenu. S druge strane, javljaju se i posebne organizovane cyber grupe - cyber mafija. Ova mafija ima svoja pravila, drugačiji način ponašanja od konvencionalne mafije, kao što ima i specifično okružje. Njene aktivnosti su umnogome olakšane specifičnostima okruženja u kom deluju i oružja koja koriste. Okruženje je virtuelno, oružje je informaciono, a znanje je specijalizovano. Internacionalizam, transnacionalnost, multidimanzionalnost samo su neka od svojstava ovih grupa. Njihova organizaciona formula nije toliko jednostavna, ustaljena i jednoobrazna kao što je to slučaj sa drugim oblicima organizovanog kriminala što još više utvrđuje sliku njihove posebnosti.

4. REGULACIJA CYBER KRIMINALA

Kao i kompjuterski kriminal i cyber kriminal iziskuje odgovarajuću pravnu regulativu. 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. Paralelno sa tim i samoregulacija pokušava da se izbori sa ovom pojavom. Dakle, regulacija se odvija na više koloseka. Zanimljivo je da se mnogo više aktivnosti dešava na međunarodnom u odnosu na nacionalni i samoregulacioni plan. To je i donekle prirodno s obzirom na karakteristike dela i svojstva kriminalaca koji se njima "bave".

Najznačajniji i najbrojniji međunarodni akti doneti su u okviru Evropske Unije [6]: 1998. godine pod vođstvom Urliha Sieber-a sa Univerziteta u Virzburgu izrađena je posebna Studija o pravnim aspektima kompjuterskog kriminala u Informacionom društvu (*Legal Aspects of Computer-related Crime in the Information Society* – COMCRIME study) koja je obuhvatala i osnove cyber kriminala, kao višeg oblika. Ovaj akt u kombinaciji sa dokumentima sa Lisabonskog sastanka Evropskog saveta 2000. godine na kome se istako značaj tranzicije u konkurentnu, dinamičnu i na znanju zasnovanu ekonomiju predstavlja smernice za aktivnosti vezane za razumevanje fenomena cyber kriminala. Akcioni plan (*eEurope Action Plan*) iz iste godine vezan je za aktivnost obezbeđenja sigurnosti mreže i uspostavljanja saradnje zemalja članica i njihovog zajedničkog pristupa cyber kriminalu do 2002. godine. Iste godine donosi se i predlog Pravnog okvira odlučivanja vezanog za napade na informacione sisteme (*Proposal for a Council Framework Decision on attacks against information systems*). Godinu dana kasnije dokument je dopunjen sa

nedozvoljenim pristupom informacionim sistemima i nedozvoljenim ometnjama sistema i podataka. Doneta je 2000. godine i Direktiva o eletronskom poslovanju (*Directive on electronic commerce*) u kojoj se posebna pažnja posvećuje problemu zloupotreba [7]. Ta je godina i dalje "plodna" jer se donosi čitav set različitih akata od Odluke Saveta o sprečavanju dečije pornografije na Internetu, Konvencije o međusobnoj pomoći u krivičnoj materiji do Preporuke o strategiji za novi Milenijum u zaštiti i kontroli kompjuterskog kriminala [8]. Potom sledi akt kojim treba da se obezbedi sigurnije Informaciono društvo kroz sigurnost informacione infrastrukture i borbe protiv kriminala vezanog za kompjutere (*Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime*). Naravno sa tom godinom niti počinje niti se završava borba protiv kompjuterskog, cyber, odnosno kriminala visokih tehnologija. Tako je 1996. godine započela Zajednička akcija protiv rasizma i ksenofobije, 1997. doneta je Preporuka o anonimnosti subjekata na Internetu i Deklaracija o globalnim računarskim mrežama, 1998., sačinjen je Predlog o okvirima sprečavanja seksualne eksploatacije i trgovine ljudskim bićima. Par godina kasnije donosi se i poseban akt vezan za cyber kiminal (Communication on Cybercrime).

Nešto manje bile su aktivnosti OECD-a, UN i Saveta Evrope. Još 1983. godine u okviru OECD usvojena je Studija o međunarodnoj primeni i harmonizaciji krivičnog prava vezanog za probleme kompjuterskog kriminala i zloupotreba, tri godine kasnije izašla je minimalna lista u okviru dokumenta Kriminal vezan za kompjutere: analiza i pravna politika, a od 1999. godinu je obeležio ceo set priručnika za sigurnost informacionih sistema kojima se uspostavljaju pravila i osnov njenog postizanja.

Savet Evrope je krajem 1998. godine objavio početak pripreme na donošenju Konvencije o cyber kriminalu, čiji predlog je aprila 2000. godine pušten u proceduru javne rasprave. Ona je danas jedan od najznačajnijih dokumenata koji su pored evropskih zemalja prihvatili i Japan, SAD; Kanada, Južna Afrika. Konvenciju, koja je stupila na snagu u julu 2004., godine prate brojni dokumenti doneti u okviru Saveta: Trust and Security in Cyberspace: The Legal and Policy Framework for Addressing Cybercrime (2002.); Cyber-Rights & Cyber-Liberties, Advocacy Handbook for NGOs (2003.); 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 Zenophobic Speech: Prelimiary draft (2001.); Second Protocol on Terrorism (2002.). Nažalost među potpisnicima ovih akata nema naše zemlje.

U okviru grupe G8 od 1997. godine (kada je predložen Akcioni plan borbe protiv ovog kriminala, a usvojenog 1998.) na predlog ekspertske grupe za kooperaciju na polju pravde i unutrašnjih poslova ministri pravde i unutrašnjih poslova u više navrata su raspravljali o principima te borbe. Poslednji sastanak bio je u maju prošle godine na kom se, između osatlog, raspravljalo i o nužnosti međunarodne saradnje u sprovođenju istraga i hvatanju počinilaca, kao i prihvatanju standarda definisanih u kovenciji Saveta Evrope.

Pored toga ova organizacija donela je i: Recommendations for Enhancing the Legal Framework to Prevent Terrorist Attacks; Recommendations on Special Investigative Techniques and other Critical Measures for Combating Organized Crime and Terrorism; Recommendations for Sharing and Protecting National Security Intelligence Information in the Investigation and Prosecution of Terrorists and Those Who Commit Associated Offenses: Best Practices for Network Security, Incident Response and Reporting to Law Enforcement, i druge.

Ujedinjene Nacije, takođe, su imale brojne aktivnosti i donele odgovarajuće akte koji su direktno ili posredno bili vezani za rešavanje problema cyber kriminala. Pored njih određenim aspektima ili

tipovima ovog kriminala bave se i druge međunarodne organizacije kakva je WIPO, Međunarodna privredna komora, Svetska trgovinska organizacija, Azijsko pacifička organizacija za ekonomsku saradnju.

Materijalna prava postaju "besmislica" u odnosu na procesna koja treba da obuhvate sve postupke koji su vezani za krivične, građanske, upravne, arbitražne i druge poslove i aktivnosti. Ova prava treba da olakšaju istražnim i pravosudnim organima prikupljanje i realizovanje podataka o učinjenim delima i počiniocima. Istovremeno upravo ove odredbe trebalo bi da olakšaju institucionalizovanje saradnje koja se mora uspostaviti između odgovarajućih organa gonjenja različitih zemalja, kao i međjunarodnih policijskih organizacija. Otuda je Evropska Unija 2000. godine donela Konvenciju o međusobnoj pomoći u kriminalnoj materiji (*Convention on Mutual Assistance in riminal Metters*) kojom se predviđa ne samo saradnja već i usklađivanje pravnih i pravosudnih sistema zemalja članica. Saradnja se očekuje i sa relevantnim institucijama korisnika, organa za superviziju zaštite podataka, kao i industrije. Isticanje uspostavljanja efikasnosti, transparentnosti i ravnoteže među svim akterima koji treba da doprinesu odgovarajućoj borbi u sprečavanju ali i sankcionisanju cyber kriminala svakako je osnovni motiv ovog akta. Ni grupa G8 nije ostala po stani u rešavanju parktičnih pitanja kooperacije i inernacionalizacije aktivnosti vezanih za cyber kriminal. Uspostavljena je mreža koja 24 sata 365 dana u godini obezbeđuje adekvatnu primenu principa borbe protiv kriminala visokih tehnologija. Njima se pridružuju i zemlje nečlanice, čime se krug širi, a očekivani efekti treba da budu bolji. Uspostavljen je čak i ekspertski tim koji bi trebao da identifikuje metode i tehnike i definiše standarde koje se mogu primenjivati u borbi protiv cyber kriminala, kao i u pružanju pomoći specijalizovanim telima za njegovo otkrivanje. Taj tim čini Međunarodnu organizaciju za kompjuterske dokaze (*IOCE*) kao grupu kojoj su se priključili timovi iz Evropske Unije i njenih zemalja članica. Tako je uspostavljena mreža čiji je cilj olakšavanje realizacije programa istraživanja i praćenja ovog kriminala.

5. "NEPRAVNE" MERE

Adekvatnost i efikasnost regulacije ozbiljno se dovodi u pitanje ukoliko se ne obezbede i druge mere. Studije i ostali materijali sačinjeni u okviru međunarodnh organizacija i asocijacija, kao i odgovarajućih nacionalnih institucija predviđaju realizaciju mera u okviru stalnih konsultantskih procesa. Tako je na primer u okviru COMCRIME Studije predviđeno:

- formiranje posebnih jedinica specijalizovane policije na nacionalnom nivou;
- uspostavljanje saradnje između pravosudnih organa, industrije, organizacija potrošača i tela za zaštitu podataka;
- "ohrabrivanje" proizvodnje specijalizovanih proizvoda koji služe za povećanje sigurnosti kompjuterskih sistema i mreža.

Naravno, nikako ne treba zanemariti izuzetni značaj enkripcije kao osnovnog alata za obezbeđenje sigurnosti novih usluga, pogotovo kod elektronskog poslovanja, a koji treba do omogući efikasniju borbu protiv kriminala na Internetu. Ipak, uspostavljanje specijalizovanih jedinica za otkrivanje, praćenje i hvatanje cyber kriminalaca predstavlja pomak od koga se očekuje veća uspešnost i sigurniji izlazak u cyber prostor korisnika. Kao primer rada takvih tela predstavlja uspostavljanje "vrućih linija" između većeg broja zemalja od SAD, V. Britanije, Nemačke, Norveške, Austrije, Holandije do Irske, u okviru tzv. *Daphne* pograma i povezanih provajdera u Evropskom Forumu. Ove aktivnosti podržali su i eksperti koji su se u organizaciji UNESO-a sastali u Parizu 1999. godine radi dogovora o uspostavljanju konkretne mreže "vrućih linija" simbolično nazvanih "elektronska kula stražara". Njima treba dodati i ekipe okupljene oko projekta *Excalibur* koji je razvilo Švedsko obaveštajno odeljenje za kriminal i kojim se uspostavlja saradnja između policije Nemačke, Velike Britanije, Holandije i Belgije, zajedno sa Europolom i Interpolom.

Ove specijalizovane jedinice moraju se permanentno usavršavati kako bi mogle da se suprotstave veoma specijalizovanim kriminalcima. Tako Europol organizuje stalnu obuku svojih članova specijalizovanih grupa, a povremeno i posebne seminare za one koji su usmereni ka određenoj vrsti cyber napada. U novembru 2000. godine, na primer, jedan broj inspektora imao je višenedeljni seminar o specifičnostima dečije pornografije na Internetu i metodama i tehnikma otkrivanja "izvora", kao i načinima prikupljanja i obezbeđivanja dokaza. Slično se već godinama radi u okviru Interpola, a ni posebna grupa eksperata u okviru G8 nije ostala bez kontinuiranog usavršavanja. FBI je 2000. godine imao 16 specijalizovani stanica na teritorijama federalnih država sa preko 190 agenta grupisanih u jedinice od 3 – 4 inspektora. Njima treba dodati i brojne univerzitetske profesore i saradnike, kao i eksperte koji se nalaze u institutima, industriji, kompanijama i raznim drugim organizacijma i institucijama i koji se uključuju po pozivu za otkrivanje, praćenje i prikupljanje dokaza, ali i za pružanje konsultativnih usluga službenim jedinicama. Da bi se sagledale razmere ovog fenomena i identifikovale karakteristike pojavnih oblika formirani su posebni timovi za analizu (u FBI popularno nazvane *Computer Analysis and Response Teams* - CART, koji imaju trostruku ulogu – da pronalaze i analiziraju podatke neophodne za podršku FBI inspektorima, da budu tehnička i savetodavna podrška i da pomognu razvoju softverskih i drugih proizvoda za obezbeđivanje sigurnosti kompjuterskih sistema i mreža). Danas su to već brojne ekipe.

Uspostavljanje saradnje između pravosudnih organa, industrije, raznih organizacija i asocijacija posebno se potencira od 1997. godine kada je u Vašingtonu održan sastanak ministara pravde i policije zemalja G8 i kada je utvrđeno 10 tačaka Akcionog plana borbe protiv cyber kriminala među kojima je posebno mesto posvećeno saradnji sa industrijskim sektorom koji dizajnira, razvija i proizvodi komponente globalnih mreža, ali i koji treba da bude odgovoran za izgradnju i primenu tehničkih standarda sigurnosti. Time je "pružena ruka" proizvođačima specijalizovanih hardverskih i softverskih proizvoda namenjenih sigurnosti. Komisija Evropske Unije je donela Odluku o posebnom programu razvoja (EU R&D Framework Programme, Internet Action Plan, i Programs STOP i Daphne) koji ima za cilj da utvrdi pravce borbe protiv pojedinaca i grupa okupljenih oko zloupotreba elektronskog poslovanja u okviru koga su brojni subjekti potencijalne i stvarne žrtve.

Možda najznačajnija aktivnost kojom se pokušava operacionalizovati saradnja između ovih aktera je formiranje EU Foruma koji obuhvata razne agencije, provajdere Internet usluga, operatore telekomunikacija, organizacija za ljudska prava, predstavnike korisnika, tela za zaštitu podataka i sve druge zainteresovane koji žele da se uspostavi saradnja u borbi protiv cyber kriminala na evropskom nivou.

Forum treba da omogući [6]:

a) razvoj dvadestčetvorosatne veze između državnih organa i industrije;

b) definisanje standardnih zahteva za koje provajderi treba da obezbede informacije o korišćenju Interneta;

c) izgradnju i primenu etičkog kodeksa sa definisanjem "dobrih poslovnih običaja" svih aktera, a posebno u međusobnim odnosima između državnih organa i industrije;

d) podspešivanje razmene informacija o trendovima kriminala visokih tehnologija između različitih pertnera, posebno u okviru industrije;

e) uspostavljanje posebnih koncerna za razvoj novih tehnologija;

f) razvoj menadžment mehanizama kojima se pruža zaštita, olakšava identifikacija i savladavaju pretnje vezane za informacionu infrastrukturu;

g) uspostavljanje čvršćih oblika ekspertske saradnje između različitih međunarodnih organizacija, tela i asocijacija (npr. Saveta Evrope i G8); i

h) razvoj principa saradnje (Memorandum of Understanding, Codes of Practice in line with the legal framework).

6. UMESTO ZAKLJUČKA - GDE SMO TU MI?

Naš cyber prostor nije ostao nedodirnut mnogim od oblika cyber kriminala. Za svega nekoliko godina "uspeli" smo da se popnemo visoko na rang listi opasnih i nesigurnih područja sa akterima kojima raste ugled u cyber podzemlju. Međutim, jedna grupa ovih počinilaca izgubila je predznak kriminalaca i svrstana je u heroje iako su njihove aktivnosti uveliko prevazilazile takve kvalifikacija. S druge strane, nespremnost pravosuđa i uspavanost prava olakšali su prelazak ovih pojedinaca u sferu "čistog" kriminala. To je ohrabrilo i mnoge druge koji su iz faze bojažljivih pokušaja prešli u drske i samosvesne kriminalce ubeđene da im niko ništa ne može. Takvu atmosferu prekinulo je nekoliko prijava istražnim organima koji pokušavaju da se uhvate u koštac sa novim oblicima kriminala i njima, često, nerazumljivim aktivnostima. Počele su i prve istrage i prikupljanje dokaza, a i prve tužbe našle su se pred sudovima u Beogradu, Pančevu i Nišu. Nažalost brojne su nedaće sa kojima se sreću sudije, tužioci i advokati zbog niskog nivoa, čak i elementarnog, znanja informatike što umnogome otežava i produžuje postupke koji, inače, iziskuju brzinu i spremnost da se u delićima sekunde spasu dokazi i identifikuju počinioci. Iako je pravna praznina koja je postojala u krivičnom zakonodavstvu popunjena izmenama i dopunama Krivičnog zakona Republike Srbije sa delima protiv bezbednosti računarskih podataka, to nije bilo dovoljno (preuzeta su rešenja Predloga Krivičnog zakonika SRJ iz 1999. godine, bez dopunjavanja sa novim krivičnim delima i oblicima inkrimnisanog ponašanja). Suočili smo se sa nekonzistentnošću sa drugim delima i sankcijama. Iako je ekspertski tim Saveta za državnu upravu Vlade Republike Srbije i UNDP-a u novembru 2002. godine izradio prvu verziju posebnog, lex specialis, Zakona o cyber kriminalu, ova verzija nije dalje otišla od nečije fioke. Poseban propust je što se u odredbe o organizovanom kriminalu nisu uvrstila i oblici cyber kriminala. Svemu ovome treba dodati i problemi u radu pravosudnih i policijskih organa, uvreženog mišljenja o nedodirljivosti izvršilaca, nepostojanja saradnje sa međunarodnim organizacijama, telima i asocijacijama, kao i nacionalnim institucijama drugih zemalja, nepostojanja posebnih specijalizovanih jedinica za istragu, specijalizovanih sudova za presuđivanje i serioznosti u radu provajdera, neuspostavljanja saradnje između subjektima koji bi trebalo da se izbore sa ovom pojavom, ipak se mora konstatovati da je koliko toliko pomereno sa "mrtve tačke" i da treba očekivati da se to nastavi kao organizovani, sistematizovani i kontinuirani rad. Kako i koliko će se to realizovati videće se već sa prvim presudama i formiranjem javnog mnjenja.

REFERENCE

[1] Cyberstalking, Anatomy of a Predator, www.cyberangels.org
[2] Robinson J., Internet as the Scene of Crime, International Computer Crime onference, Oslo, 2000., www.ccips.org
[3] Tenth United Nations Congress on the Prevention of Crime and the treatment of Offenders, www.oun.org
[4] Europena Committee on Crime Problems, European Committee of Experts on Crime in Cyber-Space, Draft Convention on Cyber-crime, April 2000., http://europa.eu.int
[5] United Nations office at Vienna, Global studies on organized crime, 1999., www.oun.org
[6] Communication from the Commission to the Council, The European Parliament, The Economic and Social Committee and Committee of the regions, Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime, http://europa.eu.int
[7] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain aspects of Information Society services, in particular electronic commerce, in the Internal Market, http://europa.eu.int

[8] The Prevention and control of organised crime: A European Union strategy for the beginning of the new Millennium (OJ 2000 C124, 3.5.2000).
[9] Legal Aspects of Computer-related Crime in the Information Society – COMCRIME, http://europa.eu.int/ISPO/legal/en/crime/crime.html.
[10] Australian Institute of Criminology, www.aic.gov.au
[12] Hi-Teh crime: The Impect to UK Business, www.nhtcu.org

KORISNI LINKOVI

A. **Council of Europe**

1. **Cybercrime Convention**
2. **Recommendation 95(13)**

B. **European Union**

1. **EC Cybercrime Communication and USG Response**
2. **EC Network Security Communication and USG Response**
3. **USG Statement at EU Cybercrime Forum meeting on data Retention**

C. **The "Group of 8" (G8) Major Industrial Democracies**

1. **Meeting of G8 Justice and Home Affairs Ministers, Washington, D.C., May 11, 2004**

D. **Other Fora**

1. **Assistant Attorney General Laura H. Parsky Speaks at the "The Major Challenges of Intellectual Property Protection" Conference in Rome, Italy on October 14, 2004"**
2. **OECD-APEC Global Forum: Policy Frameworks for the Digital Economy**
3. **OECD Releases Revised Culture of Security Guidelines**
4. **Fighting Cybercrime - What are the Challenges Facing Europe? The Transatlantic Perspective**
5. **Assistant Attorney General James K. Robinson Speaks at the International Computer Crime Conference in Oslo, Norway on May 29**
6. **Deputy Attorney General Eric Holder's welcoming remarks from the Vienna International Child Pornography Conference, September 29, 1999**
7. **Meeting of the Justice and Interior Ministers of The Eight, on December 9 and 10, 1997, in Washington, D.C., focusing on combatting high-tech and computer-related crime**
8. **Attorney General Janet Reno's Speech to Senior Experts Representing the G-7 on January 21, 1997**
9. **OECD Guidelines for Cryptography Policy**

A. Council of Europe

1. Cybercrime Convention

President's Message to the Senate on the Council of Europe Convention on Cybercrime (November 17, 2003).

Statement of Deputy Assistant Attorney General Bruce Swartz before the United States Senate Foreign Relations Committee, "Multilateral Law Enforcement Treaties" (June 17, 2004)."

- **Information Regarding Convention on Cybercrime (23 November 2001)**

  Text of Convention in HTML Format (signed 23 November 2001)

- **Explanatory Report to the Convention on Cybercrime (released 8 November 2001)**
- **Frequently Asked Questions about the Council of Europe Convention on Cybercrime (October 27, 2003)**
- **Additional Protocol to the Convention on Cybercrime Concerning the Criminalisation of Acts of a Racist and Xenophobic Nature Committed Through Computer Systems (released 7 November 2002)**

2. **Recommendation 95(13)**

- **Council of Europe Recommendation 95(13) relating to problems of criminal procedural law connected with information technology, Sept. 1995**

B. European Union

1Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime."

response to the Cybercrime Communication.

"Network and Information Security: Proposal for A European Policy Approach."

response to the Network Security Communication.

statement on behalf of the United States Government.

Some relevant links to the European Union Web sites follow:

http://europa.eu.int/information_society/topics/telecoms/internet/crime/index_en.htm

http://europa.eu.int/information_society/eeurope/news_library/new_documents/index_en.htm

http://europa.eu.int/comm/internal_market/en/dataprot/wpdocs/wpdocs_99.htm

http://europa.eu.int/comm/internal_market/en/dataprot/law/index.htm

http://europa.eu.int/ISPO/infosoc/telecompolicy/en/harmony.htm

http://europa.eu.int/comm/internal_market/en/dataprot/law/fechr.htm

C. The "Group of 8" (G8) Major Industrial Democracies

1. **Meeting of G8 Justice and Home Affairs Ministers, Washington, D.C., May 11, 2004**

Meeting of G8 Justice and Home Affairs Ministers (May 11, 2004)

D. Other Fora

1. **Assistant Attorney General Laura H. Parsky Speaks at the "The Major Challenges of Intellectual Property Protection" Conference in Rome, Italy on October 14, 2004**

- **Assistant Attorney General Laura H. Parsky Remarks before the "The Major Challenges of Intellectual Property Protection" Conference in Rome, Italy (October 14, 2004)**

2. **OECD-APEC Global Forum: Policy Frameworks for the Digital Economy**

Deputy Assistant Attorney General John Malcolm Remarks before the OECD-APEC Forum: Policy Frameworks for the Digital Economy, January 15, 2003.

Deputy Assistant Attorney General John Malcolm remarks before the OECD-APEC Forum: Policy Frameworks for the Digital Economy (January 15, 2003)

3. **OECD Releases Revised Culture of Security Guidelines**

• **OECD Calls for Culture of Security for Information Systems**

• **OECD Governments Launch Drive to Improve Security of Online Networks**

4. **Fighting Cybercrime - What are the Challenges Facing Europe? The Transatlantic Perspective**

Deputy Assistant Attorney General DiGregory's Remarks before the European Parliament on International Cooperation in Combating Cybercrime, September 19, 2000

- **Deputy Assistant Attorney General DiGregory's Remarks before the European Parliament (September 19, 2000)**

5. **Assistant Attorney General James K. Robinson Speaks at the International Computer Crime Conference in Oslo, Norway on May 29, 2000**

- **Remarks of James K. Robinson, Assistant Attorney General, Criminal Division, on the "Internet as the Scene of Crime" at the International Computer Crime Conference in Oslo, Norway (May 29, 2000)**

6. **Deputy Attorney General Eric Holder's welcoming remarks from the Vienna International Child Pornography Conference, September 29, 1999**

- **Remarks of U.S. Attorney General Eric Holder on "Combatting Ponography on the Internet" at the Vienna, Austria Intenational Child Pornography Conference (September 29, 1999)**

7. **Meeting of the Justice and Interior Ministers of The Eight, on December 9 and 10, 1997, in Washington, D.C., focusing on combatting high-tech and computer-related crime**

On December 9 and 10, 1997, Attorney General Reno convened a first-ever meeting on crime of her counterparts from The Eight (formerly known as the G-7 plus Russia) **10 Principles** and **10 Action Items** relating to high-tech crime.

- **Ministerial Communique as adopted December 10, 1997**, containing**10 Principles** and **10 Action Items** relating to high-tech crime.

8. **Attorney General Janet Reno's speech to Senior Experts representing the G-7 on January 21, 1997**

- **Janet Reno's speech to Senior Experts representing the G-7 on January 21, 1997**

9. **OECD Guidelines for Cryptography Policy**

- **Preface**
- **Recommendation of the Council Concerning Guidelines for Cryptography Policy**
- **Guidelines for Cryptography Policy**
- **Report on Background and Issues of Cryptography Policy**

Criminal Division
U.S. Department of Justice
Computer Crime Research Center (CCRC)
http://www.crime-research.org/
Computer Hacker Latest News Stories
http://computerhacker.newstrove.com/
Corporate Crime Reporter
http://www.corporatecrimereporter.com/index.html
Council of Europe
Convention on Cybercrime: Budapest, Nov. 23, 2001
http://conventions.coe.int/Treaty/EN/CadreListeTraites.htm
Critical Infrastructure Assurance Office
http://www.ciao.gov/
CyberAngels
http://www.cyberangels.org/index.html
Cybercop Portal
https://cybercop.esportals.com/
Kevin Manson, Co-Founder, Cybercop Portal.

Cybercrime: A Collection of Web Resources
http://www.wjin.net/index.php

Cybercrime.Gov
http://www.cybercrime.gov/

Cybercrimes
http://cybercrimes.net/index.html

Cyber Criminals Most Wanted LLC
http://www.ccmostwanted.com/

Cyberthreat: Protecting U.S. Information Networks
http://usinfo.state.gov/journals/itps/1198/ijpe/ijpe1198.htm

DigiCrime, Inc.
http://www.digicrime.com/dc.html

FindLaw's Cyberspace Law : Computer Crime
http://www.findlaw.com/01topics/10cyberspace/computercrimes/sites.html

High Technology Crime Investigation Association (HTCIA)
http://htcia.org/

High Tech Crime Network
http://www.htcn.org/

How to Report Internet Crime
http://www.usdoj.gov/criminal/cybercrime/reporting.htm

ILook Investigator ©
http://www.ilook-forensics.org/

Information Security Oversight Office
http://www.archives.gov/isoo/

Internet Fraud
http://www.internetfraud.usdoj.gov/

Internet Fraud Complaint Center (IFCC)
http://www.ifccfbi.gov/

Internet Fraud Watch Site
National Fraud Information Center
http://www.fraud.org/ifw.htm
Internet ScamBusters Ezine
http://www.scambusters.org/

McWhortle Enterprises (SEC Scam Site)
http://www.mcwhortle.com/
National Cyber Security Partnership (NCSP)
http://www.cyberpartnership.org/

National Fraud Information Center
Internet Fraud Watch Site
http://www.fraud.org/
National Intrastructure Protection Center (NIPC)
http://www.nipc.gov/

Nigerian Fraud E-Mail Gallery
http://potifos.com/fraud/

Operation Cyber Sweep (FBI)
http://www.fbi.gov/cyber/cysweep/cysweep1.htm
Police Officer's Internet Directory
Computer Crime Directory
http://www.officer.com/c_crimes.htm
Royal Canadian Mounted Police Information Technology Security Branch
http://www.rcmp-grc.gc.ca/tsb/index.htm
Security-Focus.Com
http://www.securityfocus.com/
http://www.takedown.com/
TechTV Cybercrime Page
http://www.techtv.com/cybercrime/
University of Dayton School of Law Cybercrimes Page
http://cybercrimes.net/
www.cybercrime.gov
http://www.usdoj.gov/criminal/cybercrime/index.html

50 Ways to Protect Your Information Assets When Cruising the Internet
http://www.all.net/journal/50/cybercop.html
Agencies, Companies Urged To Set Guidelines for Fighting Cyberterrorism
http://www.govexec.com/dailyfed/1102/110102td1.htm
Analysis of the Jurisdictional Thresholds for Prosecuting Cyber Crimes in the United States at the State Level
http://www.ists.dartmouth.edu/TAG/ajt/osi-juris-project.htm
Assessing the Risks of Cybercrime, Cyber War, and Other Cyber Threats
http://www.csis.org/tech/0211_lewis.pdf
Best Practices for Seizing Electronic Evidence
http://www.secretservice.gov/electronic_evidence.shtml
CIO Cyberthreat Response and Reporting Guidelines
http://www.csoonline.com/response/index.html
Clinton Addresses Cyberterrorism
http://www.epic.org/security/infowar/clinton-infowar-199.html
Clinton Pushes National Cyberterrorism Center
http://www.govexec.com/dailyfed/0199/012799t2.htm
Combating Cybercrime: FBI's InfraGard Program Promotes Security Awareness

http://www.infragard.net/library/combating_cybercrime.htm
Computer Attack and Cyber Terrorism: Vulnerabilities and Policy Issues for Congress
http://www.fas.org/irp/crs/RL32114.pdf
CRS report by Clay Wilson, October 17, 2003.

Computer Crime
http://www.state.nj.us/sci/
Computer Crime and Comprimised Commerce
http://www.aph.gov.au/library/pubs/rn/2003-04/04rn06.pdf
Computer Crime and Security : LC Science Tracer Bullet TB 94-1, March 1994
http://lcweb2.loc.gov/sctb/
Congress Pressing Case Against cyber-Criminals
http://www.freep.com/money/tech/mwend12_20030912.htm
Corporate America Now on Front Lines of War on Terror
http://er.lib.msu.edu/alpha_all.cfm?type=Electronic%20Journal&letter=C
Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime
http://europa.eu.int/ISPO/eif/InternetPoliciesSite/Crime/CrimeCommEN.html
The European Commission is participating in a number of initiatives aiming at making communications networks like the Internet safer from criminal activity. January 26, 2001. (Last checked 01/05/04)

Critical Infrastructure Protection:,br> **Efforts of the Financial Services Sector to Address Cyber-Threats**
http://www.gao.gov/new.items/d03173.pdf
CSI/FBI Computer Crime and Security Survey
http://www.gocsi.com/awareness/fbi.jhtml
8th or 2003 survey
7th or 2002 survey
CyberAge Stalking
http://www.llrx.com/features/cyberstalking.htm

Cyber Crime...and Punishment:
Archaic Laws Threaten Global Information, December 6, 2000
http://web.archive.org/web/20020611051642/
http://www.mcconnellinternational.com/services/CyberCrime.htm
Cyber Crime Pays a Call
http://charitychannel.com/article_11865.shtml
Cybercrime, Transnational Crime, and Intellectual Property Theft
http://www.house.gov/jec/hearings/03-24-8h.htm
Cybercriminals Threaten Economic, Personal Safety
http://www.freep.com/money/tech/mwend20_20030320.htm

Cyber Protests: The Threat to the U.S. Information Infrastructure
http://www.nipc.gov/publications/nipcpub/cyberprotests.pdf
Cyber-Predators
http://library2.cqpress.com/cqresearcher/
Cyber Security Perception Straw Poll
http://www.staysafeonline.info/news/NCSACyberSecurityStrawPerceptionPollReport.pdf
Cybersecurity Spending Estimated to Grow to $7.1 billion by 2009
http://www.govexec.com/dailyfed/0305/031705p1.htm
Cyberstalking

http://www.aic.gov.au/publications/tandi/tandi166.html
Cyberstalking: A New Threat for Law Enforcement and Industry
A Report from the Attorney General to the Vice President, August 1999
http://www.usdoj.gov/criminal/cybercrime/cyberstalking.htm
CyberStalking: Are You at Risk?
http://www.securityworld.com/library/workplacetech/cyberstalking.html
Cyber-Stalking:
Obsessional Pursuit and the Digital Criminal
http://www.crimelibrary.com/criminology/cyberstalking/
Defending America's Cyberspace: National Plan for Information Systems Protection (Government Document) The White House: Office of the National Coordinator for
Electronic Crime Needs Assessment for State and Local Law Enforcement
http://www.ncjrs.org/pdffiles1/nij/186276.pdf
http://www.ncjrs.org/txtfiles1/nij/186276.txt
Electronic Crime Scene Investigation: A Guide for First Responders
http://www.ncjrs.org/pdffiles1/nij/187736.pdf
http://www.ncjrs.org/txtfiles1/nij/187736.txt
Electronic Frontier: The Challenge of Unlawful Conduct Involving the Use of the Internet
http://www.cybercrime.gov/unlawful.htm
FBI Congressional Statement on Cybercrime, Feb. 16, 2000
http://www.fbi.gov/congress/congress00/cyber021600.htm
FBI Congressional Statement on Cybercrime, Feb. 29, 2000
http://www.fbi.gov/congress/congress00/vatis022900.htm
FBI Congressional Statement on the National Infrastructure Protection Center, March 1, 2000
http://www.fbi.gov/congress/congress00/vatis030100.htm
FBI Congressional Statement on the National Infrastructure Protection Center, March 8, 2000
http://www.fbi.gov/congress/congress00/vatis030800.htm
FBI Congressional Statements: 2002
http://www.fbi.gov/congress/congress02.htm
Federal Guidelines for Searching and Seizing Computers
http://www.usdoj.gov/criminal/cybercrime/search_docs/search.htm
http://www.usdoj.gov/criminal/cybercrime/supplement/ssgsup.htm
Federal Law Officers Weigh Online Privacy Issues
http://www.govexec.com/dailyfed/0101/011201td.htm
Government Grants Scam
Hack Attacks
http://www.govexec.com/features/0897s2.htm
Hacktivism! Taking It Off the Streets, Protestors Are Acting Up Online
http://www.sfbg.com/SFLife/34/28/lead.html
Half of Americans Fear Terrorists Might Mount Successful Cyber-Attacks
http://www.pewinternet.org/reports/reports.asp?Report=100&Section=ReportLevel1&Field=Level1ID&ID=437
Identity Theft Epidemic Consumes Money, Time
http://www.freep.com/money/tech/mwend8_20030908.htm
Internet Auction Fraud Report
http://www1.ifccfbi.gov/strategy/AuctionFraudReport.pdf
Internet Crimes Against Children
, see Missing/Exploited Children

Internet Fraud Complaint Center

Internet Fraud Complaint Center
Annual Fraud Report, 2004
http://www.ifccfbi.gov/strategy/2004_IC3Report.pdf
Internet Sex Crimes Against Minors: The Response of Law Enforcement
Missing/Exploited Children

Lessons Learned by Consumers, Financial Sector, Firms, and Government Agencies During the Recent Rise of Phishing Attacks,br> http://www.treas.gov/offices/domestic-finance/financial-institution/cip/pdf/fbiic-fsscc-report-2004.pdf
Michigan Computer Crime Units Created
Michigan State University Cybersecurity Institute
http://www.ccs.msu.edu/
National Cyber Security Partnership Task Force
Report on Security Across the Software Development Lifecycle
http://www.cyberpartnership.org/init-soft.html
National Infrastructure Protection Center
Advisory on E-Commerce Vulnerabilities, December 1, 2000
http://www.nipc.gov/warnings/advisories/2000/00-060.htm
National Strategy to Secure Cyberspace
http://www.whitehouse.gov/pcipb/cyberspace_strategy.pdf
Phishing Activity Trends Report, Oct. 2004
http://www.antiphishing.org/APWG_Phishing_Activity_Report-Oct2004.pdf
Practices for Securing Critical Information Assets
http://www.infragard.net/library/pdfs/securing_critical_assets.pdf
Profits Embolden Hackers
http://www.techweb.com/wire/story/TWB19980323S0013
Progress and Challenges in Securing the Nation's Cyberspace
http://www.dhs.gov/interweb/assetlibrary/OIG_CyberspaceRpt_Jul04.pdf
Prosecuting Intellectual Property Crimes Manual
http://www.cybercrime.gov/ipmanual.htm
Protecting America's Freedom in the Information Age
http://www.markletaskforce.org/
Protecting your Trade Secrets in the Computer Era
http://www.berrymoorman.com/articles/1199rahprottradesec.html
Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations
http://www.cybercrime.gov/searchmanual.htm
Securities Fraud Looms as Dark Side of Internet Growth
http://usinfo.state.gov/journals/itgic/1097/ijge/gj-10.htm
Security Directors on Computer Crime (article)
http://www.cj.msu.edu/~outreach/security/secdir.html
Seven Simple Computer Security Tips for Small Business and Home Computer Users
http://www.infragard.net/library/seven_tips.htm
Software is the New Tool for Catching Crooks
http://www.govexec.com/dailyfed/0100/012700t4.htm
Spam, Phishing and Fraud on the Net
http://www.llrx.com/features/spam.ppt
Special Report on "Phishing"
http://www.usdoj.gov/criminal/fraud/Phishing.pdf
State and Local Law Enforcement Needs to Combat Electronic Crime (NCJ 183451)
http://www.ncjrs.org/pdffiles1/nij/183451.pdf
http://www.ncjrs.org/txtfiles1/nij/183451.txt
State Cybercrime Legislation in the United States: A Survey
http://web.archive.org/web/20010802194821/
http://www.richmond.edu/jolt/v7i3/article2.html
Study on Legal Issues Relevant to Combating Criminal Activities Perpetrated Through Electronic Communications
Tougher Computer Crime Laws Needed
http://www.govexec.com/dailyfed/0100/012500b3.htm

United Nations Manual on the Prevention and Control of Computer-Related Crime
http://www.uncjin.org/Documents/irpc4344.pdf
U.S. Customs Debuts Cybersmuggling Center
http://www.govexec.com/dailyfed/1000/100400j1.htm
U.S. Department of Justice Criminal Division
Computer Crime and Intellection Property Section (CCIPS)
War Provokes Hackers to Launch Attacks on Web
http://www.freep.com/money/tech/mwend27_20030327.htm

Why Hackers Escape
Organized, Well-Financed Criminals Stay a Step Ahead of the Law
http://news.com.com/2009-1017-912708.html?tag=fd_lede