UNIVERZITET U NIŠU
PRAVNI FAKULTET

Kompjuterski kriminalitet

(master rad)

Mentor :
Docent dr Darko Dimovski

Student :
Miloš Vidojković
Broj indeksa: 015/14 M-UP

Niš, 2015.

SADRŽAJ

UVOD

Prvi računar, nazvan ENIAC, pušten je u eksperimentalni pogon februara 1944. godine, da bi konačno bio završen tek 1946. godine. Njegova je osnovna funkcija bila da u ratne svrhe izračunava putanje artiljerijskih granata, a njegova izrada je koštala oko 400.000 tadašnjih dolara, što je u to vreme bila značajna suma, međutim on je opravdao tu cenu, jer je mogao da izračuna putanju granate, pet sekudi pre nego što pogodi metu.[1]

Neprestani razvoj tehnologije za proteklih sedamdeset godina od je od kompjutera načinio neophodnost u svim sferama života savremenog čoveka, a današnja cena kompjutera je skoro svima pristupačna, tako da se kompjuteri nalaze u skoro svakom domaćinstvu. Kao sredstvo koje ubrzava rad i informacije čini lako dostupnim, teško je zamisliti savremen život bez upotrebe kompjutera.

Nažalost pojava kompjutera i dalji razvoj tehnologije je doveo i do pojave novih oblika krivičnih dela i kao i do novih načina izvršenja istih. Način upotrebe kompjutera je primeren znanju prosečnog čoveka, tako da potencijalni izvršilac krivičnih dela može biti svako, a svetska upotreba interneta omogućuje da se dele vrše bilo gde u svetu.

Kriminalci iskorišćavaju ogromnu brzinu, jednostavnost i pre svega anonimnost, koje nam savremne tehnologije nude, kako bi izvršili različita krivična dela. To su najčešće napadi na kompjuterske sisteme i mreže, krađe identiteta i podataka drugih lica, distribucija pornografskog sadržaja dece, prevare, piraterija u oblasti kompjuterskih softvera i drugih kompjuterskih proizvoda itd.

Tehnološki razvijene zemlje su negde ranije, a negde kasnije zakonski odredila ova nova krivična dela. Uobičajeno je da se ova ova krivična dela nazivaju kompjuterska krivična dela. Međutim u Srbiji je prihvaćen termin visokotehnološki kriminalitet, a Krivičnim zakonikom Republike iz 2006. godine se ova krivična dela nazivaju i Krivična dela protiv bezbednosti računarskih podataka.[2] Većina zemalja je formirala i posebne državne organe radi suzbijanja ovih dela i pronalaženja njihovih počinilaca.

[1] Ž.Aleksić i M.Škulić ,*Kriminalistika*, Beograd,2004,str. 384.
[2] Glava XXVII KZ Republike Srbije

Zbog sve većeg značaja infomacione tehnologije i sve veće zavisnosti od upotrebe kompjutera u svakodnevnom životu neophodno je vršiti proučavanje karakteristika tzv. kompjuterskog kriminaliteta, jer se kompjuteri i informaciona tehnologija sve više koriste kao sredstvo za izvršenje postojećih oblika krivičninih dela, ali i za izvršenje novih oblika krivičnih dela.

Stoga, ovaj master rad je usmeren na proučavanje kompjuterskog kriminaliteta, njegovih počinilaca, domaće i međunarodne pravne regulative, a delom i na istraživanje kompjuterskog kriminaliteta u Republci Srbiji. Samim tim ovaj master rad se sastoji iz sledećih celina: Pojam kompjuterskog kriminaliteta, Karakteristike kompjuterskog kriminaliteta, Ciljevi, način korišćenja kompjutera pri kriminalnim aktivnostima i posledice kompjuterskog kriminaliteta, Vrste i odlike počinilaca kompjuterskog kriminaliteta, Konvencija o visokotehnološkom kriminalu Saveta Evrope sa dodatnim protokolom, Direktive EU o borbi protiv kompjuterskog kriminaliteta, , Međunarodne policijske organizacije i kompjuterski kriminalitet, Institucionalni okvir suprotstavljanja visokotehnološkom kriminalu u Republici Srbiji, Specifičnosti gonjenja za dela visokotehnološkog kriminala, Kompjuterska krivična dela u Krivičnom zakoniku Republike Srbije, Kriminološka tipologija kompjuterskog kriminaliteta, Posebni deo - istraživanje : "Visokotehnološki kriminal u Srbiji u periodu od 2006. do 2013. godine".

I Pojam kompjuterskog kriminaliteta

Jedan od najvećih problema kriminologije je i davanje jedinstvene definicije za nove oblike kriminaliteta, tako da ni kompjuterski kriminalitet nije izuzetak, iakopostojeviše definicija, ne postoji jedna definicija kompjuterskog kriminaliteta za koju bi rekli da je opšte prihvaćena. Teško je jednom definicijom obuhvatiti, sva krivična dela koja bi se mogla podvesti pod kompjuterskim kriminalitetom, zbog velike fenomenološke raznovrsnosti ovog oblika kriminalnog ponašanja. Kompjuterski kriminalitet je samo opšta forma kroz koju se ispoljavaju različiti oblici kriminalne aktivnosti, to je posebna vrsta kriminaliteta upravljena protiv kompjuterskih sistema u celini, ili jednom delu, na različite načine i različitim sredstvima u nameri da sebi ili drugom pribave kakvu korist ili da se nanese drugom šteta.[3]

U kriminološkoj literaturi postoji shvatanje da je kompjuterski kriminalitet deo privrednog kriminaliteta, ali i shvatanje da se radi o imovinskom kriminalitetu i da su kompjuterska krivična dela po svom karakteru najbliža imovinskim krivičnim delima. Najrasprostranjenija definicija u kriminologiji definiše kompjuterski kriminalitet kao skup svih delinkventnih ponašanja kojima se uređaji za elektronsku obradu podataka koriste kao sredstvo za postizanje kažnjivih radnji ili kao direktan cilj kažnjive radnje.[4]

Ministarstvo pravde Sjedinjenih Američkih Država je u Priručniku za krivično pravosuđe (eng. The Criminal Justice Resource Manual on Computer Crime) iz 1979. godine dalo prvu definiciju kompjuterskog kriminaliteta i po njoj kompjuterski kriminalitet predstavlja svaki nelegalni akt za čije uspešno krivično gonjenje je neophodno dobro poznavanje računarske tehnologije.

Radna grupa eksperata Ujedinjenih Nacija je na XI Kongresu prevencije krimaliteta i krivičnog pravosuđa održanom 2005. godine u Bangkoku na Tajlandu definisala kompjuterski kriminalitet tumačeći ga u skladu sa razmerama njegove rasprostranjenosti i opasnosti koja od njega potiče, kao opšti pojam koji obuhvata krivična dela koja se vrše pomoću kompjuterskog sistema ili mreže, u kompjuterskom sistemu ili mreži ili protiv kompjuterskog sistema ili mreže.

[3]Donn B.Parker.,*Fighting computer crime*, New York(USA), 1983, str.70.
[4]S.Konstantinović-Vilić, V.Nikolić-Ristanović,*Kriminologija*, Niš, 2003, str.178-179

Komisija Evropske unije je u Saopštenju datom 2001. godine odredila kompjuterski kriminalitet u najširem mogućem smislu, tako da se kompjuterskim kriminalitetom podrazumeva svako krivično delo koje na bilo koji način podrazumeva upotrebu informacionih tehnologija.[5]

Na prostoru bivše Jugoslavije, jedna od definicija koja je takođe vredna pažnje, jeste svakako ona koju je dao prof. dr Đorđe Ignjatović, prema kome kompjuterski kriminalitet predstavlja poseban vid inkrimisanih ponašanja kod kojih se računarski sistem pojavljuje kao sredstvo izvršenja ili kao objekat krivičnog dela, ukoliko se to delo na drugačiji način, ili prema drugom objektu, uopšte ne bi moglo izvršiti ili bi ono imalo bitno drugačije karakteristike.[6]

Jedna od naraširenijih i upotrebljivanih definicija je i da je kompjuterski kriminalitet predstavlja društveno opasnu pojavu, za čije se ostvarenje učinilac koristi, znanjima kompjuterske tehnologije, tako što se kompjuterski sistem shvaćen u najširem smislu, koristi kao sredstvo ili kao objekt kriminalnog napada ili kao i jedno i drugo.[7]

Iz obe definicije može se uočiti opseg kriminalnih radnji širok i da se pod kompjuterskim kriminalitetom smatra svaka kriminalna radnja koja koja se vrši uz pomoć kompjutera, kompjuterskih mreža i programa. Pored radnji koje su usmerene na pribavljanje protivpravne imovinske koristi, kompjuterski kriminal je obuhvata i aktivnosti koje su učinjene i iz drugih pobuda, kao što su stvaranje i distribucija virusa i malicioznog softvera, objavljivanje poverljivih ličnih i poslovnih podataka na internetu i sl.[8]

Prof. dr Vladimir Vodinelić je definisao kompjuterski kriminalitet u pravom (užem) i nepravom (širem) smislu ,tako da u užem smislu obuhvata kompjutersku prevaru sabotažu i špijunažu, dok se širem smislu odnosi na protivpravno prisvajanje kompjutera i njegovih komponenti krađom, proneverom i sl.[9] Po prof. dr Vidoju Spasiću kompjuterski kriminalitet predstavlja kriminalitet koji se vrši u digitalnom okruženju, i predstavlja specifičan oblik protivpravnog ponašanja u kome se kompjuterske mreže javljaju kao sredstvo, cilj, ili dokaz izvršenja krivičnog dela.[10]

---

[5]Izvor http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2001:0051:FIN preuzeto 20.07.2015. godine.
[6] Đ.Ignjatović,*Pojmovno određenje kompjuterskog kriminala*, Beograd, 1991, str. 142–143.
[7]B.Simonović,*Kriminalistika*, Pravni fakultet u Kragujevcu, Kragujevac, 2004, str. 665
[8] Ž.Aleksić i M.Škulić, *Kriminalistika*, Beograd, 2007, str. 46-63.
[9]N.Šarkić, D.Prlja, K.Damnjanović, V. Marić, V.Živković, V.Vodinelić, N.Mrvić-Petrović: Pravo informacionih tehnologija, Beograd, 2011, str.3.
[10]V.Spasić, *Aktuelna pitanja u oblasti sajber kriminala* (članak), Bilten sudske prakse Vrhovnog suda Republike Srbije broj. 1/2006, Beograd, str.107.

Imajući u vidu da su navedene značajnije definicije, koje kompjuterski kriminalitet definišu zastupajući različita gledišta , ipak je opšti utisak da ne postoji definicija koja je obuhvatila svu složenost i problematiku kompjuterskog kriminaliteta.

II Karakteristike kompjuterskog kriminaliteta

Bez obzira na nedostatak univerzalne definicije kompjuterskog kriminaliteta analizirajući navedene definicije lako se određuju njegove specifičnosti u odnosu na druge oblike kriminaliteta. U odnosu na tradicionalne oblike kriminaliteta, kompjuterski kriminalitet brzo menja forme i oblike ispoljavanja, granice među državama kao i vrstu oštećenog. Ova krivična dela vrše se prikriveno, često bez neke vidljive i bliske prostorne povezanosti učinioca dela i žrtve. Najčešće se teško otkrivaju, a još teže dokazuju, a dugo vremena ostaju praktično neotkrivena, sve dok oštećeni ne pretrpi neku štetu koja je vidljiva u kompjuterskom sistemu.[11]

Značajna odlika kompjuterskog kriminaliteta je dakle njegova **fenomenološka raznovrsnost i velika dinamika razvoja.**[12] Broj pojavnih oblika ispoljavanja kompjuterskog kriminaliteta je ogroman i u konstantom je porastu, upravo zahvaljući neprestanom razvoju tehnologije svakodnevno se pojavljuju nove i složenije forme kompjuterskog kriminaliteta. Kako kompjuterska tehnologija nalazi primenu u svim sferama života, mogućnosti zloupotrebe su veće iz dana u dan, i sada se javljaju znatno opasniji oblici kriminalnog ponašanja koji nisu bili ranije poznati u kriminalnoj i pravosudnoj praksi.

Druga bitna odlika **kompjuterskog kriminaliteta je da ne poznaje granice između država i kontinenata**. Ovoj odlici je naročito doprinelo širenje upotrebe interneta u svetu.Izvršilac može sa bilo kog mesta u svetu, napasti određenu kompjuterski sistem bez obzira gde se on nalazi, ovo omogućuje pre svega velika brzina rada kojom današnji računari raspolažu, tako da prostorni i vremenski okvir imaju mali značaj u većini oblika kompjuterskog kriminaliteta.

Kompjuterskim kriminalom bave se uglavnom lica koja vrlo dobro poznaju informacione tehnologije. U prvim godinama razvoja informacionih tehnologija, visoka stručnost bila je preduslov za rukovanje računarima, a samim tim to je dovodilo i do teškog razotkrivanja počinjenih krivičnih dela. Situacija je danas izmenjena, dostupnost i jednostavnost

[11] Igor Ž. Živkovski, *Otkrivanje i razjašnjavanje kompjuterskog kriminaliteta* ; članak ,2012, str.162-165.
[12] Alisdair A. Gillespie, *Cybercrime: Key Issues and Debates Florence*, Kentucky (USA), 2015,str.17.

u korišćenju računara, i širenje informatičke pismenosti omogućili su širokoj masi ljudi korišćenje računara, koji su neizbežni deo svakog poslovnog prostora i domaćinstva, a samim tim smanjeno je i vreme potrebno za sticanje neophodnih znanja i veština za izvršenje krivičnih dela kompjuterskog kriminaliteta.

Kako se radi o distancionim krivičnim delima vrlo je **mali i rizik otkrivanja počinioca**, a činjenica da se ova dela izvršavaju u informacionom okruženju, ovoj vrsti krivičnih dela daje određene osobenosti, a to je da se ova krivična dela vrše brže, lakše, na raznovrsnije načine i što je sa stanovišta kriminalaca značajno **anonimnije,** jer savremena informaciona tehnologija pruža i više nego idealne uslove počiniocima, da prikriju svoje kriminalne radnje.

Samim tim teško je prikupiti precizne podatke o rasprostranjenosti kompjuterskog kriminaliteta, o strukturi krivičnih dela kao i o njihovim posledicama, tako da je **tamna brojka ogromna**. Ona se prema nekim procenama kreće od 90% do 99%.[13] Jedan od osnovnih problema u sprečavanju i suzbijanju visokotehnološkog kriminaliteta je i činjenica da samo mali broj izvršenih krivičnih dela biva pribavljen i rasvetljen od strane policijskih i pravosudnih organa. Za tamnu brojku kompjuterskog kriminaliteta karakterične su dakle sledeće činjenice: mala verovatnoća otkrivanja;neurednost u izveštavanju o izvršenim delima; neodgovorna zaštita; porast broja računara uslovljava porast broja potencijalnih izvršilaca, teško pronalaženje materijalnih tragova izvršenog krivičnog dela.[14]

Prilikom različitih zloupotreba **samo mali broj oštećenih lica je i svesno da je bilo žrtva krivičnog dela**, pa tako i izostaje podnošenje krivične prijave, a ako i dođe do otkrivanja izvršenog dela, u većini slučajeva je već i prekasno da se preduzme neka odgovarajuća mera. Karakteristično je da i kada oštećeni otkriju da su bili žrtve krivičnog dela, oni često ne podnose prijavu i ne obaveštavaju nadležne organe. Kako su žrtve uglavnom finansijke institucije i privredni subjekti razlog ne neprijavljivanja je strah od gubitka poverenja kod poslovnih partnera, što dalje može dovesti do bankrotiranja. U velikom broju slučajeva rukovodioci oštećenih subjekata nastoje zataškati ova krivično dela i radije bi pretrpeti štetu nego da podnošenjem prijave reskiraju nesagledive posledice poljuljanog poslovnog poverenja.[15] Ukoliko bi kojim slučajem došlo do neovlašćenog prodora u informacioni sistem banke, i ukoliko bi se

13 D.Dimovski – *Kompjuterski kriminalitet*, Niš, 2010, str.205.
14 I.Feješ, *Kompjuterski kriminalitet – kriminalitet budućnosti, izazov sadašnjosti* – izlaganje na konferenciji, 2000, str. 378.
15 I.Feješ, *Kompjuterski kriminalitet – kriminalitet budućnosti, izazov sadašnjosti* – izlaganje na konferenciji, 2000, str. 378.

ova činjenica objavila, klijenti bi sa pravom strahovali da njihovi podaci nisu u dobrim rukama, i potražili bi drugog poslovnog partnera.

III Ciljevi, način korišćenja kompjutera pri kriminalnim aktivnostima i posledice kompjuterskog kriminaliteta

1. Ciljevi kompjuterskog kriminaliteta

Kako bi odredili ciljeve kompjuterskog kriminaliteta prethodno moramo odrediti osnovne pojmove. Kompjuterski sistemom možemo definistati kao svaki pojedinačni kompjuter ili kao grupu kompjutera koji su međusobno povezani ili uslovljeni, od kojih u zavisnosti od programa za upravljanje, jedan ili više njih, vrši automatsku obradu prikupljenih podataka. Kompjuterski podaci se definišu kao svako izlaganje činjenica, podataka ili koncepata u obliku koji je pogodan za njihovu obradu u kompjuterskom sistemu, uključujući tu i odgovarajući program na osnovu kojeg kompjuterski sistem vrši svoju funkciju. [16]

Dakle za potencijalne **ciljeve** kompjuterskog kriminaliteta možemo uzeti hardver, softver, programi, podaci, zaštita, usluge. Brojne aktivnosti koje mogu imati karakter kriminalnih radnji mogle grupisati na sledeći način: [17]

1. napad na hardver (uništenje, oštećenje ili otuđenje računarskog sistema ili njegovih komponenti),
2. napad na softver (uništenje, oštećenje, otuđenje i neovlašćena izmjena, objavljivanje ili korišćenje softverskih proizvoda),
3. napad na program (uništenje, oštećenje, otuđenje i neovlašćena izmjena, objavljivanje ili korišćenje programskih proizvoda),
4. napad na podatke (uništenje, oštećenje, otuđenje i neovlašćena izmjena, objavljivanje ili korišćenje podataka),
5. napad na zaštitu sistema (narušavanje ili probijanje sistema zaštite),
6. napad na usluge (neovlašćeno korišćenje informacionih resursa).

Kompjuterska tehnologija unela je nove i drastične promene u svim sferama savremenog života. Te promene su pored svojih pozitivnih strana donele i niz problema vezanih za pojavu i širenje računarskog kriminaliteta, raznih oblika, formi i vidova ispoljavanja i one se mogu svesti

16 Član 1. Konvencije o visokotehnološkom kriminalu, Savet Evrope, Budimprešta, 2001. god
17 Slobodan R. Petrović, *Kompjuterski kriminal;* Ministarstvo unutrašnjih poslova Republike Srbije : Uredništvo časopisa"Bezbednost" i lista "Policajac",Beograd 2000, str.45–46

na sledeće: nove forme vrednosti; koncentracija podataka; novi ambijent delovanja; nove metode i tehnike delovanja; sužavanje vremenske skale delovanja; širenje geografskog prostora delova; mobilnost; i stabilnost rizika.[18]

2. Način korišćenja kompjutera pri kriminalnim aktivnostima

Prema načinu na koji se kompujeteri koriste prilikom vršenja kriminalnih aktivnosti, možemo izvrštiti podelu gde se kompjuteri javljaju kao objekati napada, sredstva izvršenja, sredstva planiranja, rukovođenja ili prikrivanja kriminalnih aktivnosti i kao sredstva za obmanu.[19]

Kada su kompjuteri objekti napada, mogu biti predmeti različitih krađa poput krađa programa podataka, i komponenti, kao i objekti napada u slučaju kompjuterskih sabotaža.

Specifičnost načina korišćenja kompjutera kao sredstvo izvršenja kriminalnih radnji još jedna od osobenosti kompjuterskog kriminaliteta. Kompjuteri se mogu koristi radi krađe ličnih podataka. Za izvršenje koriste se o tehnike koje su vrlo usavršene i precizno osmišljene prilikom zloupotrebe podataka. Jedna od njih je i socijalni inženjering, odnosno sugestivna komunikacija i aktivna manipulacija koja za cilj ima navođenje potencijalnih žrtvi da odaju informacije o sebi, do kojih se da nije ovog metoda, dolazi tzv. hakerskim metodama.[20] To su podaci koju su pogodni za razne vrste zloupotreba poput, korisničnih imena i lozinki, podaci o jmbg, broju pasoša, lične karte, platne kartice i sl.

Kada se kompjuteri koriste kao sredstvo za planiranje, rukovođenje ili prikrivanje kriminalnih aktivnosti koje se najčešće sprovede od strane ogranizvanih kriminalnih grupa i terorista. Kriminalci kompjutere najčešće koriste radi pranja novca, vođenja dvostrukog knjigovodstva, ili radi obavljanja drugih protivpravnih bankarskih poslova. Podatke stvore ovim načinom korišćenja kompjutera, kriminalci štite kriptografskom metodom žaštite radi sprečavanja nedozvoljenog pristupa.

Zbog velike anonimnosti i prostorne udaljenosti, kompjuteri se uspešno koriste od strane kriminalaca pri kriminalni aktivnostima u kojima su žrtve predmet obmane, ucene, iznude i prevare.

---

18 D. Littlejohn Shinder, M.Cross,*Cybercrime* Burlington, MA, United States,2002, str. 2.

19 M.Budimlić, P.Puharić – *Kompjuterski kriminalitet – kriminološki,krivičnopravni, kriminalistički i sigurnosni aspekt* – Fakultet za kriminalistiku, kriminologiju i sigurnosne studije Sarajevo 2009. Godina,str. 10.

20 Nir Kshetri; *The Global Cyber Crime Industry - Economic, Institutional and Strategic Perspectives*, New York, USA,2010,str.10

Bez obzira na sve gore navedeno kompjuteri stoje na raspolaganju i organima gonjenja koji ih mogu koristiti radi kao sredstvo za za lakše otkrivanje,sprečavanje, dokazivanje krivičnih dela i indentifikaciju njihovih počinilaca.

3. Posledice

Posledice kod izvršenja ovih krivičnih dela su uglavnom imovinske prirode, ali mogu biti i nematerijalne prirode. Štete koje nastupaju su velike, često i nesagledive, i po nekom nepisanom pravilu veće nego što se čini na prvi pogled. Procenjuje se da je šteta prouzrokovana kompjuterskim kriminalitetom u 2014.godini je koštala svetsku ekonomiju preko 400 milijardi američkih dolara.[21] Štetu snose uglavnom sami oštećeni zbog veoma niskog stepena otkrivanja počinilaca. Osnovna podela štete je sledeća:

1. Finansijska šteta – koja nastaje kada učinilac vrši delo u cilju sticanja protipravne imovinske koristi pa tu korist za sebe ili drugog zaista i stekne ili je ne stekne, ali svojim radnjama pričini određenu štetu ; ili kada učinilac ne postupa radi sticanja koristi, ali ipak pričini finansijsku štetu;
2. Nematerijalna – ona može nastati npr. prilikom otkrivanja tajni, ili zahvaljući drugom indiskretnom postupanju;
3. Kombinovana – kada se npr. otkrivanjem određene tajne ili povredom autorskog prava istovremeno povredi nečije moralno pravo i istovremeno mu se prouzrokuje konkretna finansijska šteta.

IV Vrste i odlike počinilaca kompjuterskog kriminaliteta

Zbog velikog broja dela kompjuterskog kriminaliteta i različitih pobuda koje pojedince podstiču na njihovo vršenje, ne možemo sve počinioce podvesti pod jedinstven profil. Raspoloživi uzorci počinilaca, odnosno otkrivenih i gonjenih počinilaca još uvek su relativno mali i nedovoljno reprezentativni, da bi se iz njih proizveo neki opšti profil počinilaca.

U većini slučajeva radi se o mlađim muškarcima koji su visoko obrazovani, nisu ranije bili gonjeni i kažnjavani, imaju radno iskustvo i obezbeđenju egzistenciju i uglavnom sve vide kao izazov. Visoka stručnost omogućava stabilnu egzistenciju, sređene lične i porodične prilike

21 Center for Strategic and International Studies ,*Net Losses: Estimating the Global Cost of Cybercrime Economic impact of cybercrime II* ,Santa Clara USA ,2014,str.2

učinilaca, koji kao cenjeni članovi društva, ne izazivaju sumnju kod organa gonjenja. [22] Uglavnom se počinioci dele na one koje vrše dela radi sticanja imovinske dobiti i počinioci kojima novac nije prioritet, nego vide određen stepen izazova, uzbuđenja i zabave u prodiranju u sisteme i obaranju njihove zaštite. Kompletan kriminološki profil počinioca koji krivična vrše dela radi sticanja imovinske dobiti je sledeći :80% njih krivično delo vrši put; 70% njih je krivično delo izvršilo u predzeću u kome je zaposleno; starosti su između 19. i 30. godina; pretežno su muškog pola; veoma su inteligentni; zaposleni su i imaju dugogodišnje iskustvo u struci; kvalifikovaniji su i obrazovaniji nego što potrebe njihovog radnog mesta to zahtevaju; nisu osuđivani;sebe ne doživljavaju kriminialcima.[23]

Ovaj profil počinioca je čest u velikim poslovnim sistemima, poput finansijskih organizacija, banaka i centrala velikih kompanija. Dosadašnja iskustva ukazuju da se kompjuterskim kriminalitetom u bakarskim institucijama bave lica: koja su u 25% slučajeva osobe sa posebnim ovlašćenjima u kompjuterskom sistemu banke; programeri se javljaju u 18% slučajeva; službenici koji imaju pristup terminalima za isplatu novca su počinioci u 18 % slučajeva; blagajnici u 16 % slučajeva; operateri u 11 posto slučajeva; i lica izvan sistema poslovanja banke i korisnici usluga banke su zastupljeni u 12 % slučajeva.[24]

Počinioce krivičnih dela kompjuterskog kriminaliteta možemo podeliti na počinioce koji su motivisani isključivo na sticanje protivpravne dobiti, i na hakere kojima sticanje dobiti nije primarni cilj vršenja krivičnih dela. Počinioce koji krivična dela vrše radi sticanja protivpravne dobiti možemo podeliti na amatere i profesionalce. U okviru amatera kojih razlikujemo slabe i podložne pojedince, ljude sa porokom, i frustrirane pojedince, dok u okviru profesionalaca razlikujemo indivudalne profesionalne kriminalce, organizovane grupe i kriminalne organizacije.

1.1. Amateri

Amaterima pripadaju kriminalci koji imaju legano zanimanje, ali se povremeneno bave kompujterskim kriminalitet, i uglavnom ostaju neotkriveni. Kao izvršioce među amaterima razlikujemo frustrirane pojedince, slabe i podložne pojedince i ljude sa porokom.[25]

22 I.Feješ–Kompjuterski kriminalitet–kriminalitet budućnosti, izazov sadašnjosti– izlaganje na konferenciji;str. 377.
23 Slobodan R. Petrović ;Kompjuterski kriminal ; Ministarstvo unutrašnjih poslova Republike Srbije: Uredništvo časopisa "Bezbednost" i lista "Policajac",/ Beograd 2000,str.273-294.
24 Ž.Aleksić,M.Škulić, *Kriminalistika*, Beograd, 2002,str. 388-389.
25 D.Dimovski – *Kompjuterski kriminaliter*, članak–Niš, 2010, str.206.

Slabi i podložni pojedinci– ovoj grupi pripadaju počinioci koji su proizvodi njihove slabe ličnosti, a i slabih instrumenata kontrole. Njima je pružena mogućnost da nešto ukradu ili pronevere, a da nisu sagledali posledica toga čina, oni najčešće posle nekoliko usprešno obavljenih dela i sami prestaju sa bave kompjuterskim kriminalitetom. Zahvaljujući svom slabom karatkteru pripadnici ove grupe su često predmet manipulacije.

Ljudi sa porokom **–**Droga, alkohol, kocka, život iznad sopstvenih novčanih mogućnosti su faktori koji snažno motivišu počinioca da se bavi kompjuteskim kriminalitetom. Ovi počinici se najlakše otkrivaju i procesuiraju.

Frustrirani pojedinci **–**Ogrorčeni, nezadovoljni i razočarani pojedinci, predstavljaju tip kriminalaca koji su najopasniji po društvo. Osećaj da su prevareni, nepravedno zapostavljeni ili zaobiđeni, u njihovim očima opravdava svaku njihovu nezakonitu radnju i postupak, od krađa i pronevera do sabotaža i vandalističkog ponašanja.

1.2. Profesionalni kriminalci

Profesionalni kriminalci su lica kojima je bavljenje kriminalom jedino zanimanje i izvor zarade, imaju veliko iskustvo i predstavljaju veliku društvenu opasnost. U okviru ove grupe razlikujemo individualne kriminalce, organizovane grupe i kriminalne organizacije.

Individualni kriminalci **–** nastupaju samostalno i nezavisno u realizaciji svojih ciljeva. Mogu biti u kooperaciji sa drugim kriminalcima, ali uglavnom povremeno. Deluju u lokalu i nemaju razrađen dugoročni plan delovanja, zbog čega im je potencijal za izvršavanje krivičnih dela relativno ograničen.

Organizovane grupe **-** Predstavljaju skup pojedinaca koji radi ostvarenja svojih kriminalnih ambicija deluju zajedno. Grupe variraju od labavih udruženja do čvrstih udruženja sa jasno definisanim ciljevima. Ogranizovane grupe su lokalnog karaktera, ali sa izrađenom strategijom i taktikom. Potencijal za izvršenje krivičnih dela im varira, ali je shodno brojnosti i organizovanosti, daleko veći od individualnih kriminalaca, ali još ne toliki da bi posledice imale neki veći nacionalni efekat.

Kriminalne organizacije **–** Predstavljaju najviši oblik organizacije, odlikuju se čvrstom hijerarhijomm, strogom disciplinom, poslušnošću, lojalnošću uz izgrađenu dugoročnu strategiju i taktiku uz tajnost kao najznačaniji faktor opstanka.

Organizovani kriminal se stalno razvija i evoluira, i vrlo lako se prilagodio korišćenju informacionih tehnologija, koje se koriste kao alat za planiranje i kontrolu kriminalnih aktivnosti. Elektronski transfer novca omogućava lakše praćenje novca pribaljenog na protivpravan način, dok elektronska pošta omogućava lakšu komunikaciju kriminalaca. Sve ovo je znatno otežalo rad državnih organa, na praćenju i istraživanju rada kriminalnih organizacija, jer savremena tehnologija omogućava lakšu izmenu, modifikaciju i uništenje kompromitujućih podataka, koji jednim pritiskom na jedno dugme mogu biti izbrisani, a dokazi uništeni.

2. Hakeri

Razvitkom informacione tehnologije pojavio se novi tip specijalizovanog kriminalaca haker. Termin haker ima više značenja i prvobitno podrazumeva igrača početnika golfa, koji raskopava teren. Najprihvatljivije značenje je ono koje daje Oksfordski rečnik računarstva da je haker osoba koja neovlašćeno upada u tuđe, zaštićene sisteme. Haker je dakle, vrsta programera koja pravi manje-više korisne programe, ali obično loše dokumentovane i sa neželjenim uzgrednim efektima. Njihov motiv je često samo lična satisfakcija, ali ponekad i zlonamerno čine štetu ili kradu.[26]

Hakeri su osobe opsednute tehnologijom, i svaki aspekt njihovog života je njoj posvećen. Dnevno provede i po 16 časova za računarom, među njima dominiraju uglavnom muškarci, uglavnom se radi o licima sa visokom stručnom spremom, mada ponekad među njima ima i lica koja su svoje veštine stekla iz hobija.[27] Oni koriste kombinaciju tehničke genijalnosti i ljudske istrajnosti u želji da zasite svoju želju za znanjem.

Ova grupa počinilaca svoj užitak nalazi u samom izazovu probijanja zaštite sistema i upada u tuđi sistem.[28] Vole da pronalaze nedostatke u programima, a pogotovo u sistemima zaštite. Česti su primeri da sistem-administratorima hakeri putem elektronske pošte šalju savete kako da uklone uočene nedostatke.

Ova grupa počinilaca krivičnih dela kompjuterskog kriminaliteta je još uvek nepoznanica za svet psihologije, sociologije i kriminologije, za brojne autore razumevanje njihovog razvoja i motivacije postalo je jedno od glavnih polja njihovog interesovanja.Kriminolozi profil hakera sagledavaju na različite načina i analiziraju sa različitih aspekata neke o osnovnih karatkeristika

[26] V.Ilingvort - *Oksfordski rečnik računarstva*, Nolit, Beograd, 1990,str.93.
[27] M.Cetinić.,*Kompjuterska krivična dela i pojavni oblici*,Časopis Pravni život,broj 10, 1998,, str.266.
[28] M.Betts, *Portrait of a hacker*,Časopis Computer world , 25.novembar 1985 godina,str.56.

hakera su: da su oni skoro 100 % muškarci; slično računarskim programerima, hakeri su ekstremno bistri, skloni istraživačkom i logičkom razmišljanju i uvek su takmičarski raspoložen; po prirodi su radoznali; ne vole cenzuru jer to vodi jednoumlju; vole da vide sebe kao autoritete za računarom i nad bilo kim ko je povezan sa njom, što im daje osećaj moći i kontrole, dakle oni su zainteresovani za dobijanje osećaja moći, nego za posledice svojih radnji; imaju malo respekta prema onima koji ne znaju ništa o njihovoj omiljenoj temi kompjuterima.[29]

Tokom godina hakeri su kao deo svoje kulture razvili i poseban način komunikacije tzv. **leet speak**,[30] koji predstavlja šifrovanu formu pisanja, zamenjivanjem slova i brojeva, određenim simbolima koji liče na njih. Osnovna svrha pored komunikacije je isključivanje nepoželjnih lica i međusobno prepoznavanje hakera.Pored osnovne želje za znanjem pojavili su se i drugi pokretači poput novca ,tako da je sa već rasprostranjenim elektronskim bankarstvo, ubrzo došlo do prvih napada na banke i druge finansijske institucije.Osnovni motivi njihovog delovanja su: intelektualni izazov; radoznalost; avantura; zabava; osećaj svemoći; potreba za trijumfom; elitizam; osveta; prestiž; nadoknada osećaja manje društvene ili lične vrednosti.[31]

Hakere u skladu sa njihovim **motivima** možemo podeliti na kreativce, destruktivce i kriminalce. **Kreativcima** pripada najveći deo hakerske populacije u onom izvornom obliku, čine je hakeri, avanturističkog duha, enigmatičari, radoznalci, koji hakovanje doživljavaju kao jednu vrstu svog istraživanja, stučnog usavršavanja, samotestiranja i samodokazivanja, kome pristupaju bez ikakve zle namere i želje za posledicama. Većina hakera smatra svojom dužnošću da širi informacije i deli svoje znanje, takođe provaljivanje u tuđe sisteme radi istraživanja smatra opravdanim, ukoliko podatke ne krade i čini ih dostupnim drugim hakerima.[32]

To su programeri koji poseduju ogromno znanje, ali im ono nije dovoljno, jer struktura njihove ličnosti ne podnosi ograničenja i prepreke, koje sa uživanjem savladavaju. Ova vrsta hakera misi da su njihova nezakonita dela opravdana i etički prihvatiljiva.[33] Međutim, njihovo delovanje dovodi do finansijske štete i oštećenja sistema, ali softverske kompanije ih smatraju korisnim jer ukuzaju na slabosti sitema zaštite podataka.

[29]R. Chiesa ,S.Ducci,S.Ciappi - *Profiling Hackers: The Science of Criminal Profiling as Applied to the World of Hacking,* Boca Raton FL, United States, 2008, str.43-44.
[30]Preuzeto sa http://www.urbandictionary.com/define.php?term=leet+speak dana 10.07.2015. godine
[31]B. Sterling, *The Hacker Crackdown: Law and Disorder on the Electronic Frontier*, Bantam Books,Bantam, USA ; 1992, str. 170-182
[32]Preuzeto sa http://www.catb.org/jargon/html/ dana 09.08.2015.godine
[33]Preuzeto sa https://www.cs.berkeley.edu/~bh/hackers.html dana 09.08.2015. godine

Destruktivcima pripadaju hakeri kojima hakovanje predstavlja način zaispoljavanje lične agresije i frustracije, koja često dobija vandalističke oblike, nepotrebno menjajući podatke napadnutih sistema, posebno korišćenjem virusa.

Često ih zbog njihovih malicioznih namera nazivaju i krakerima (cracker). Oni poseduje tehnički talenat da u prodru u najsofisticiranije sisteme, ali njihova ličnost ne budi sumnju okoline. Ovu grupu čine uglavnom nezadovoljni radnici softverskih kompanija, obešenjaci i programeri. Većina njih počinje profesionalno da se bavi kriminalom, kada shvati da ima talenat za ozbiljnije poduhvate.

Kriminalci su hakeri čiji je jedini i osnovni motiv ostvarivanje protipravne imovinske koristi. Njima je jedini cilj da profitiraju od svojih veština i ne biraju šta, kada i zbog čega će da napadnu. Oni kao i klasični kriminalci deluju ili kao individualci ili u grupama.

V Konvencija o visokotehnološkom kriminalu Saveta Evrope sa dodatnim protokolom

1.Konvencija o visokotehnološkom kriminalu Saveta Evrope

Neophodnost međunarodnog povezivanja državnih organa je osnovni preduslov suprostavljanja kompjuterskom kriminalu. Srbija je ratifikovala Konvenciju o visokotehnološkom kriminalu Saveta Evrope u martu 2009. godine uz Dodatni protokol koji se bavi inkriminisanjem akata rasističke i ksenofobične prirode putem računara. Konvencija je doneta 23. novembra 2001.godine u Budimpešti, i pored Srbije ratifikovana je još od 31 države članice Saveta Evrope, a potpisale su je i Kanada, Japan, Južnoafrička Republika i SAD.

Osnovni ciljevi donošenja Konvecije su harmonizacija nacionalnih zakonodavstava u domenu materijalnopravnih odredbi u oblasti visokotehnološkog kriminala, uvođenje odgovarajućih procesnih instrumenata radi boljeg procesuiranja ovih krivičnih dela i uspostavljanje brzih i efikasnih institucija i procedura međunarodne saradnje.[34]

U preambuli same Konvecije naglašena je potreba za procesuiranjem počinilaca krivičnih dela visokotehnološkog kriminala, koja imaju međunarodni karakter. Unapređenje saradnje nadležnih nacionalnih organa jedan je od osnovnih prioriteta s ciljem suzbijanja visokotehnološkog kriminala. Konvencija se sastoji iz preambule, i četiri poglavlja: upotreba

[34]Preuzetohttp://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy%20project%20balkan/Strategic_priorities_conference/2467_Strategic_Priorities_V16_SRB_final_adopted.pdf. dana 10.08.2015. godine

termina, mere preduzimanja na nacionalnom nivou - materijalno i procesno pravo, međunarodna saradnja i završne odredbe.[35]

Evropske države među prvima shvatile neophodnost da stvaranja međunarodnog dokumenta koji bi regulisao pitanje kompjuterskog kriminaliteta, a sve veća opasnostodposledicakompjuterskogkriminaliteta, pospešila je nastojanja tvoraca Konvencije da se prevaziđu različita ograničenja u nacionalnim zakonodavstvima, koja dovode u pitanje, delotvornost pravne zaštite, zajedno sa međusobnim nastojanjima država da usklade svoja zakonodavstva u ovom pogledu.

Prvo poglavlje predstavlja skup definicija i osnovnih termina koji su korišćeni u Konvenciji. Drugo poglavlje Konvencije reguliše materijalne i procene odredbe na koje se potpisnice Konvecije obavezuju da će uvesti u svoje zakonodavstvo i nadležnost. Materijalnopravni deo je podeljen na sledeći način:

1. *Dela protiv poverljivosti, celovitosti i dostupnosti računarskih podataka i sistema*: nezakonit pristup; nezakonito presretanje; ometanje podataka;ometanje sistema; zloupotreba uređaja.
2. *Dela u vezi sa računarima:* falsifikovanje u vezi sa računarima; prevara u vezi sa računarima.
3. *Dela u vezi sa sardžajem:* dela u vezi sa dečijom pornografijom.
4. *Dela u vezi sa kršenjem autorskih i srodnih prava.*
5. *Drugi oblici odgovornosti:* pokušaj, pomaganje i podstrekavanje; odgovornost pravnog lica; sankcije i mere.

Konvencija je propisala minimum zajedničkih standarda prilikom inkriminisanja ovih krivičnih dela. Stvoren je osnov za saradnju između nadležnih organa država, kao i za ramenu iskustava. Konvencijom je isključen eventualni prigovor usled nedostatka dvostruke inkriminisanosti i u slučaju eventualne ekstradicije.

Za krivično delo ***nezakonitog pristupa*** podacima na računarima ili sitemu, potrebna je nemera učinilica da te informacije prisvoji, izmeni ili uništi. Tako da je državama potpisnicama ostavljena mogućnost da u svojim zakonodavstvima regulišu i posebne oblike ovog dela.

Nezakonito presretanje je krivično delo koje se sastoji iz namere presretanja prenosa podataka između dva računara.

35 Zakon o potvrđivanju Konvencije o visokotehnološkom kriminalu ("Sl. glasniku RS",br. 19. mart 2009.)

Krivična dela ***ometanje podataka*** i ***ometanje sistema*** se sastoji iz namere radi potpunog ili delimičnog brisanja, oštećenja, izmene sadržine, kompresije ili bilo kog drugog načina izmene podataka. Konvencija i ovde daje mogućnost državama da suze domet inkriminacije, odnosno da sa se krivičnim smatraju samo ona dela, gde je pričinjena veća šteta.

Zloupotreba uređaja je složeno krivično delo. Konvencija delo određuje kao svaku namernu, protivpravnu, proizvodnju, upotrebu, nabavku ili prodaju, kao i svaki oblik činjenja dostupnim i distribucije, bilo koje vrste uređaja, pod kojima se podrazumevaju i računarski programi pomoću kojih se mogu izvršiti krivična dela određena u Konvenciji. Imajući u vidu neodređenost ove odredbe, tvorci Konvecije ostavljaju mogućnost rezerve državama potpisnicama kada je reč o prodaji ili drugom načinu distribucije lozinki ili drugih podataka, pomoću kojih se mogu izvršiti krivična dela.

Falsifikovanje odnosi se samo na umišljajno, protivpravno brisanje, izmenu, ubacivanje ili sakrivanje podataka, koje rezultira izmenjenim sadržajem tih podataka, bez obzira na to, da li oni na ovaj ili onaj način dobijaju drugu svrhu ili smisao, ili postaju neupotrebljivi.[36]***Prevara***je određena kao umišljajno, protivpravno brisanje, izmenu, ubacivanje ili sakrivanje podataka, kao i svako drugo mešanje u rad sistema u cilju pribavljanja protivpravne imovinske koristi za sebe ili drugoga.

Konvencija o visokotehnološkom kriminalu obavezuje države potpisnice da kao krivično delo **dečje pornografije** inkriminišu sledeće radnje: proizvodnja dečije pornografije u svrhu njene distribucije preko računarskog sistema; nuđenje ili činjenje dostupnim dečije pornografije preko računarskog sistema; distribucija ili prenošenje dečije pornografije preko računarskog sistema; nabavljanje dečije pornografije preko računarskog sistema, za sebe ili za drugo lice; posedovanje dečije pornografije u računarskom sistemu ili na medijumima za čuvanje računarskih podataka.[37]

Konvencija je inkriminisala svako ponašanje uključujući i pribavljanje i posedovanje, što čini značajnu razliku u odnosu na bića sličnih krivičnih dela vezanih za kršenje autorskih prava putem računarske mreže. Tvorci Konvencije su na autoritativan način državama potpisnicama naredili da urede svoja zakonodavstva i da naj način doprinesu prevenciji dečje pornografije.

[36]L. Komlen Nikolić; *Suzbijanje visokotehnološkog kriminala*; Udruženje javnih tužilaca i zamenika javnih tužilaca Srbije, Beograd; 2010,,str.46.

37 Član 9. stv.1. *Zakon o potvrđivanju Konvencije o visokotehnološkom kriminalu* ("Sl. glasniku RS",br. 19.mart 2009.)

Konvencija i precizno reguliše šta se sve smatra pornografskim sadržajem , i definiše kao kao pornografski materijal koji vizuelno prikazuje :

1. maloletnika koji učestvuje u eksplicitno seksualnoj radnji;
2. lice koje izgleda kao maloletnik, koje učestvuje u eksplicitno seksualnoj radnji;
3. realistične slike, koje predstavljaju maloletnika koji učestvuje u eksplicitno seksualnoj radnji.[38]

Konvencija je podigla starosnu granicu po kojoj se decom smatraju sva lica do svoje 18. godine uz opciju daje države potpisnice pomerena na 16. godina. Kršenje ***autorskih i srodnih prava*** određuje u tri stava, i ne inkriminiše ih u skladu sa već postojećim međunarodnim ugovorima. Države potpisnice su obavezne da u sklada sa Konvencijom usvoje zakonske i druge mere, koju su neophodne kako bi se odgnovnorna lica kaznila za pokušaj ***izvršenja, podstrekavanja i pomaganja*** u izvršenju krivičnih dela visokotehnološkog kriminala. Takođe predviđene su mere koju su potrebne da bi se utvrdila ***odgovornost pravnih lica*** kao i mere za primenu odgovarajućih ***sankcija.*** Članovima 14-22 Konvencije regulisana su **procesna ovlašćenja** državnih organa prilikom istraživanja krivičnih dela visokotehnološkog kriminala.

Pored opštih odredbi koje nalažu državama potpisnicama Konvencije, da u svoja nacionalna krivična prava uvedu gore pomenuta krivična dela, velika pažnja usmerena je načinu prikupljanja podataka koji se nalaze u računarima ili prenosnim uređajima, kao i zaštiti osnovnih prava pojedinca garantovanih Evropskom konvencijom o ljudskim pravima iz 1950.godine, Međunarodnim paktom Ujedinjenih nacija o građanskim i političkim pravima iz 1966.godine i ostalim važećim međunarodnim dokumenatima o ljudskim pravima, koji sadrže načelo proporcionalnosti .[39]

Nadleži organi, u skladu sa Konvencijom, imaju pravo uvida i zaplene svakog računara ili nosača podataka, ukoliko postoje osnovi sumnje, da se tu mogu nalaziti nedozvoljeni materijali, kao i da od provajdera prikupljaju podatke, koji se odnose pre svega, na upotrebu interneta, telefona i kartica.

Konvecija predviđa i odredbe koje se tiču presretanja podataka, odnosno praćenja elektronske komunikacije, prevashodno one koje se obavlja putem interneta. Ova oblast Konvecije je i najosetljivija, jer je njome povređno jedno od osnovnih prava čoveka, a to je pravo

[38]Član 9. stv.2. *Zakon o potvrđivanju Konvencije o visokotehnološkom kriminalu* ("Sl. glasniku RS",br. 19. mart 2009.)
[39]Član 15. *Zakon o potvrđivanju Konvencije o visokotehnološkom kriminalu* ("Sl. glasniku RS",br. 19. mart 2009.)

na privatnost i pravo na prepisku, a Konvencija ne predviđa odgovarajuća ograničenja da takva prava neće biti zloupotrebljena. Kako se presretanje odnosi samo na teška dela, države imaju punu slobodu da same odrede kada će i u kojim slučajevima ovo pravo koristiti. Konvecija u čl.21.stv.3 određuje da: *" Svaka Strana ugovornica treba da usvoji zakonodavne i druge mere, neophodne da obavežu davaoca usluga da čuva u tajnosti sprovođenje svakog ovlašćenja predviđenog ovim članom i svaku informaciju u vezi sa tim."* Kada se imaju u vidu istrage za terorizam i zlostavljanje dece ovakva procedura je opravdana i prihvatljiva, međutim ni ovde nije predviđen mehanizam žaštite građana koji bi se zloupotrebom ovog stava našli na udaru vlasti određene zemlje.

Konvencijom nije predviđena ni obaveza provajdera da skladišti podatke o svojim korisnicima, koji bi možda kasnije bili od koristi nadležnim organima, i to zbog očigledne povrede prava na privatnost korisnika. Kako je Konvencija međunarodni instrument, države imaju mogućnost da prilikom ratifikacije izrade pravne propise koji bi nadomestili ove nedostatke.

Pitanje ***nadležnosti*** uređeno je članom 22. Konvencije koji u stavu 1. previđa da države imaju nadležnost za procesuiranje ukoliko je krivično delo izvršeno :

1. na njenoj teritoriji ;
2. na brodu pod zastavom te strane ugovornice;
3. u vazduhoplovu registrovanom u skladu sa zakonima te strane ugovornice;
4. od strane njenog državljanina, ako je delo kažnjivo po krivičnom zakonu zemlje gde je izvršeno ili ako je delo izvršeno na mestu izvan nadležnosti bilo koje države.

Po stavu 2. istog člana države imaju mogućnost da ne primenjuju pravila o nadležnosti u određenim slučajevima. Države potpisnice su obavezne da ukoliko ne izvrše ekstradiciju svog državljanina , da mu sude za dela koja su izvršena na teritoriji druge države potpisnice.

Treći deo Konvecije je posvećen **međunarodnoj saradnji**, gde predviđene odredbe uređuju načine radi prevazilaženja prepreka prilikom sprovođenja nacionalnog zakonodavstva za krivična dela koja po pravilu podrazumevaju učešće nekoliko zemalja, a često i pojedince iz više zemalja.

Većina odredbi Konvencije reguliše saradnju država koja sa se tiče eventualne razmene podataka za izvršena krivična dela, kao i ekstradicije počinilaca. U posebnim slučajevima može biti i uspostavljena i direktna saradnja između pravosudnih organa dve države, kao i Interpola,

bez ikakvog posredovanja organa izvršne vlasti. Države potpisnice Konvencije mogu tražiti jedna od druge sprovođenje istražnih radnji u slučaju kada :

1. ima osnova da se veruje da su odgovarajući podaci naročito podložni gubitku ili izmeni;
2. instrumenti, dogovori i zakoni inače nalažu brzu saradnju.[40]

Konvencija služi i kao osnov za ekstradiciju ukoliko države to pitanje nisu regulisale. Države neće biti obavezne da sprovedu ekstradiciju ukoliko postoji nedostatak dvostruke inkriminacije. Dodatni uslov da se ekstradicija može izvršiti, je da su krivična zakonima obe strane ugovornice kažnjiva zatvorskom kaznom od najmanje godinu dana ili težom kaznom.[41]

Konvencija predviđa osnivanje dežurne službe koja bi radila danonoćno sedam dana u nedelji (24/7), za čije potrebe države potpisnice moraju da uspostave u svojim policijskim službama jedinicu za saradnju, koja bi pružala trenutnu pomoć istragama ili postupcima u vezi sa krivičnim delima koja se odnose na računarske sisteme i podatke, ili radi prikupljanja dokaza u elektronskom obliku o krivičnom delu. Takva pomoć treba da obuhvati olakšavanje ili, ukoliko to domaće pravo i praksa dozvoljavaju, neposredno sprovođenje sledećih mera: davanje tehničkih saveta; zaštitu podataka; prikupljanje dokaza, davanje informacija pravne prirode i lociranje osumnjičenih.[42]

Konvenciju nažalost razvijene države nerado ratifikuju, do 2006. godine samo su Danska, Francuska, Norveška i SAD ratifikovale konvenciju. *I to zbog toga* što Konvencija obavezuje potpisnice na gonjenje počinioca i za ona dela koja nisu predviđena u njihovim zakonodavstvima, kao i zbog suviše širokog tumačenja nedozvoljenog sadržaja.[43]

[40]Član 31. stv.3. *Zakon o potvrđivanju Konvencije o visokotehnološkom kriminalu* ("Sl. glasniku RS",br.19. mart 2009)
[41]Član 24. stv.1. *Zakon o potvrđivanju Konvencije o visokotehnološkom kriminalu* ("Sl. glasniku RS",br. 19.mart 2009)
[42]Član 35.stv.1. *Zakon o potvrđivanju Konvencije o visokotehnološkom kriminalu* ("Sl. glasniku RS",br.19. mart 2009)
[43]L.Komlen Nikolić ; *Suzbijanje visokotehnološkog kriminala*; Udruženje javnih tužilaca i zamenika javnih tužilaca Srbije, Beograd, 2010, str. 51

2.Dodatni protokol

Dodatni protokol uz Konvenciju o visokotehnološkom kriminalu donet je 28. januara 2003. godine u ***Savetu Evrope*** u Strazburu i odnosi se u na inkriminaciju radnji rasističke i ksenofobične prirode učinjenih uz pomoć računara. Protokol inkriminiše ponašanja koje nije regulisala Konvencija, a koja se tiču širenja mržnje, netolerancije i netrpeljivosti putem računarskih sistema, prema rasnim, verskm, nacionalnim grupama i zajednicama.[44]

Širenje interneta i dostupnost računara postali su opasna sredstva za širenje pogubnih ideologija i stavova, poput veličanja nacizma, terorizma, poziva na linč pojedinaca i sl. Internet ne može blagovremeno kontrolisati, jer svaki korisnik smatra da ima pravo na izražavanje svog stava, tako da su zloupotrebe ogromne. Protokol je pre svega usmeren na inkriminaciju i kažnjavanje ovih ispada i obavezuje države potpisnice da u svoja zakonodavstva uvedu sledeća krivična dela:

1. širenje ili na drugi način činjenje dostupnim javnosti, preko računarskog sistema, rasističkog i ksenofobičnog materijala;
2. pretnja motivisana rasizmom i ksenofobijom;
3. uvreda motivisana rasizmom i ksenofobijom;
4. poricanje, značajno umanjivanje, odobravanje ili opravdavanje genocida ili zločina protiv čovečnosti;
5. pomaganje i podstrekavanje.[45]

Širenje ili na drugi način činjenje dostupnim javnosti, preko računarskog sistema, rasističkog i ksenofobičnog materijala podrazumeva svaku radnju kojom se ovakav materijal čini dostupnim javnosti korišćenjem računarskog sistema. Državama je ostavljena sloboda da odluče, da li ovakvi postupci povlače krivičnu odgovornost ili ne.

Pretnja motivisana rasizmom i ksenofobijom predstavlja stavljanje u izgled pojedincu ili grupi da će prema njima biti izvršeno neko krivično delo, koje je određeno u nacionalnom zakonodavstvu, pojedinici i grupe trebaju da se razlikuju po boji kože, raci, poreklu, nacionalnoj, verskoj ili etničkoj pripadnosti da bi delo imalo specifičan oblik predviđen protokolom.

---

[44]Član 1. Zakon o potvrđivanju dodatnog Protokola uz Konvencije o visokotehnološkom kriminalu koji se odnosi na inkriminaciju dela rasističke i ksenofobične prirode koja su izvršena preko računarskih sistema ("Sl. glasniku RS", Međunarodni ugovori br. 19. 2009.)

[45]Čl. 3-7. Zakona o potvrđivanju dodatnog Protokola uz Konvencije o visokotehnološkom kriminalu koji se odnosi na inkriminaciju dela rasističke i ksenofobične prirode koja su izvršena preko računarskih sistema ("Sl. glasniku RS", Međunarodni ugovori br. 19. 2009.godine)

Uvreda motivisana rasizmom i ksenofobijom poseduje elemente kao i prethodno delo, samo što se ovde radi o vređanju, a ne o pretnji. Protokol državama potpisnicama ostavlja i mogućnost stavljanja rezerve i ograničenja inkriminacije samo na one uvrede kojim se grupa ili pojedinac ponižavaju ili izvrgavaju podsmehu ili na uvrede kojima se širi mržnja.Poricanje, značajno umanjivanje, odobravanje ili opravdavanje genocida ili zločina protiv čovečnosti odnosi se na slučajeve koji su bili predmet odlučivanja od strane međunarodnih sudova od 1945. godine pa na dalje, i da je ovakav sadržaj na bilo koji način učinjen dostupan javnosti, odnosno većem broju ljudi.

Svaka država potpisnica treba da usvoji zakonodavne i druge mere, neophodne da bi se kao krivično delo u domaćem pravu propisalo namerno i protivpravno pomaganje i podstrekavanje na izvršenje nekog od dela propisanih u skladu sa ovim protokolom, sa namerom da ta dela budu učinjena.[46]

VI Direktive EU o borbi protiv kompjuterskog kriminaliteta

1.Direktiva Saveta Evropske zajednice o pravnoj zaštiti kompjuterskih programa

Evropska unija je donela više akata s ciljem suzbija kompjuterskog kriminaliteta. **Direktiva Saveta Evropske zajednice o pravnoj zaštiti kompjuterskih programa** od 14. maja 1991. godine predstavlja jedno od prvih rešenja u oblasti pravne zaštite kompjuterskih programa.

Direktiva je rezultat saradnje država članica, na smanjivanju razlika u svojim zakonodavstvima u cilju suzbijanja neovljašćenog umnožavanja kompjuterskih programa, koje je imalo negativan uticaj na funkcionisanje zajedničkog tržista. Pravna žaštita pružena je svakom fizičkom i pravnom licu koje potpada pod odredbe nacionalnih zakonodavstava u oblasti autorskog prava primenjivog na književna dela. Direktiva obavezuje države članice, da se kao nedozvoljena pravno sankcionišu tačno navedena ponašanja, i to:

1. stavljanje u promet kopije kompjuterskog programa, znajući da je kopija nedozvoljena ili imajući razloga za osnovanu sumnju u njenu nedozvoljenost;

[46]Čl. 7. *Zakona o potvrđivanju dodatnog Protokola uz Konvencije o visokotehnološkom kriminalu koji se odnosi na inkriminaciju dela rasističke i ksenofobične prirode koja su izvršena preko računarskih sistema* ("Sl. glasniku RS", Međunarodni ugovori br. 19. 2009.godine)

2. držanje iz komercijalnih razloga kopije kompjuterskog programa, znajući da je kopija nedozvoljena ili imajući razloga za osnovanu sumnju u njenu nedozvoljenost;
3. stavljanje u promet ili držanje u komercijalne svrhe svakog sredstva čija je jedina svrha da olakša nedozvoljeno uklanjanje ili neutralizaciju svakog tehničkog mehanizma eventualno napravljenog u cilju zaštite kompjuterskog programa.[47]

Članice su u obavezi da zaplene svaku nedozvoljenu kopiju kompjuterskog programa u skladu sa nacionalnim zakonom. Direktiva autorima obezbeđuje pravnu žaštitu za života i pedeset godina nakon smrti (ukoliko je reč o više autora, po smrti poslednjeg), pravnim licima i anonimnim autorima, rok zaštite teče od dana činjenja programa dostupnim. Autorom kompjuterskog programa smatra se fizičko lice , grupa lica i pravno lice.

2.Direktiva o čuvanju podataka koji su dobijeni ili obrađeni prilikom pružanja javno dostupnih usluga elektronske komunikacije ili javnih komunikacionih mreža

Direktiva o čuvanju podataka koji su dobijeni ili obrađeni prilikom pružanja javno dostupnih usluga elektronske komunikacije ili javnih komunikacionih mreža od 15.03.2006. godine doneta je s ciljem efikasnog otkrivanja i procesuiranja počinilaca, svih krivičnih dela, čije izvršenje ostavlja elektronske tragove. Direktiva je dopuna Direktive 2002/58 o obradi ličnih podataka i zaštiti privatnosti u oblasti elektronskih komunikacija.[48] Direktiva državama članicama u skladu sa članom 8. Evropske konvecije o zaštiti ljudskih prava i osnovnih sloboda daje pravo, da pod određenim uslovima ograniče prava građana s ciljem očuvanja javnog reda i mira, zaštite nacionalne sigurnosti, odbrane, i radi uspešnog procesuiranja počinilaca krivičnih dela i neovlašćene upotrebe sistema elektronske komunikacije.

Osnovni cilj Direktive je usklađivanje nacionalnih zakonodavstava država članica, koji regulišu obaveze davaoca javnih usluga komunikacija da čuvaju podatke koje u okviru obavljanja svoje delatnosti dobijaju i obrađuju, kako bi podaci bili dostupni u slučaju otkrivanja krivičnih dela i procesuiranja njihovih počinilaca. Direktiva se ne primenjuje na sadržaj elektronske komunikacije kao ni na informacije do kojih se dolazi korišćenjem elektronske

[47]Council Directive od 14. may 1991 on the Legal Protection of Computer Programs – Directive 91/250/EEC OJ no L122/42
[48]Preuzeto sa http://eur-lex.europa.eu/legal-content/HR/TXT/?uri=celex:32006L0024 dana 09.08.2015.godine

komunikacije, već samo na podatke o lokaciji i prometu pravnih i fizičkih lica koji su potrebni tačnu identifikaciju pretplatnika ili korisnika usluga.[49]

Direktiva vodi računa između poštovanja osnovnih ljudskih prava i potrebe efikasnog suprostavljanja kriminalu, vodeći se načelom srazmernosti i opravdanosti ograničenja prava građana. Pravo na pristup podacima imaju samo nadležni organi država članica u skladu sa sudskim postupcima uređenim domaćim zakonima.

Članom 5. Direktive izvršena je kategorizacija podataka koji se skladište odnosno čuvaju i taksativno su podeljeni u kategorije i podkategorije.

U prvoj kategoriji nalaze se koji podaci su potrebni radi **pronalaženja i identifikacije izvora komunikacije**. Kod mobilne i fiksne telefonije čuvaju su sledeći podaci:

1. telefonski broj priključka sa kog poziv dolazi;
2. ime i adresa ukoliko je pretplantnik odnosno korisnik registrovan.

Kod pristupa, internetu,mobilnom internetu i elektronskoj pošti, čuvaju se sledeći podaci:

1. podaci o dodeljenom korisničkom imenu/imenima;
2. korisnicko ime i telefonski broj dodeljen svakoj komunikaciji s kojom se stupa u javnu telefonsku mrezu;
3. ime i adresa pretplatnika ili registrovanog korisnika kojem je u trenutku komunikacije dodeljena adresa internet protokola (IP), korisničko ime i telefonski broj.

Podaci potrebni radi otkrivanja **odredišta komunikacije** čuvaju se u drugoj kategoriji podataka. Kod mobilne i fiksne telefonije čuvaju su sledeći podaci:

1. birani broj ili brojevi i u slučaju koji uključuje korišćenje dodatnih usluga poput preusmeravanja ili prenosa poziva, broj ili brojevi na koje je poziv preusmeren;
2. ime ili imena i adresu/adrese pretplatnika ili registrovanog korisnika.

Kod mobilnog interneta i elektronske pošte, potrebno je sačuvati podatke o:

1. imenu primaoca usluge ili njegov broj telefona kome je upućen poziv putem usluge mobilnog interneta;
2. imenu i adresi pretplatnika, registrovanog korisnika ili podatke o korisničkom ime primaoca prema kome je komunikacija usmerena.

[49]L.Komlen Nikolić ; Suzbijanje visokotehnološkog kriminala; Udruženje javnih tužilaca i zamenika javnih tužilaca Srbije, Beograd; 2010,str. 64.

Direktiva u trećoj kategoriji podataka određuje koji se podaci čuvaju radi **utvrđivanja vremena, datuma i trajanja komunikacije**. Kod mobilne i fiksne telefonije čuvaju se podaci o datumu i vremenu početka i završetka komunikacije. Kod pristupa, internetu,mobilnom internetu i elektronskoj pošti, čuvaju se sledeći podaci:

1. vremenski okvir prijave i odjave pristupa korisnika internetu prema određenoj vremenskoj zoni, zajedno sa IP adresom, bilo da je statička ili dinamička, koju je komunikaciji dodelio davalac usluga pristupa internetu, kao i korisničko imenu pretplatnika odnosno korisnika;
2. vreme prijave i odjave od usluge elektronske poste ili usluge internet telefonije prema određenoj vremenskoj zoni.

Otkrivanje vrste komunikacije postiže se zahvljući podacima sadržanim u četvrtoj kategoriji. Kod fiksne i mobilne telefonije to je korišćena telefonskausluga, a kod elektronske poste i internet telefonije u pitanju je korišćena internet usluga.

Jedna od najvažnijih kategorija podaOtkrivanje komunikacijske opreme korisnika ili njihove navodne opreme,Kod fiksne telefonije čuvaju se telefonski brojevi sa kojih se poziva i koji su pozivani. Kod mobilne telefonije čuvaju se:

1. telefonski brojevi sa kojih se poziva i brojevi koji se pozivaju;
2. međunarodni identitet mobilnog pretplatnika stranke koja poziva i koja prima poziv;
3. međunarodni identitet mobilnog uredaja stranke koja poziva i koja prima poziv;
4. kod unapred plaćenih (pre-paid) anonimnih usluga, datum i vreme početka upotrebe usluge i oznaka lokacije sa koje je usluga aktivirana.

Kod pristupa internetu, elektronskoj posti i internet telefoniji čuvaju se podaci o telefonskom broju s kojeg se poziva u svrhu telefonskog pristupa ili digitalna pretplatnička linija ili druga krajnja tačka lica ko je započinje komunikaciju.

Direktiva u poslednjoj kategoriji reguliše koji su podaci neophodni za **otkrivanje lokacije opreme za mobilne komunikacije**.

Države članice su u obavezi da podatke čuvaju od šest meseci do dve godine od dana komunikacije.[50] Države mogu čuvati podatke i duže od predviđenog roka, ali uz obavezu

[50] Član 6. *Direktive Evropskog parlamenta i Saveta o čuvanju podataka koji su dobijeni ili obrađeni prilikom pružanja javno dostupnih usluga elektronske komunikacije ili javnih komunikacionih mreža*

obaveštavanja Komisije i druge države članice o razlozima produženja. Komisija može u roku od šest meseci u kome odobrava ili odbija nacionalne mere nakon ispitivanja da li su one preduzete kao sredstvo proizvoljne diskriminacije ili predstavljaju prikriveno ograničenje trgovine među državama članicama i stvaraju prepreku funkcionisanju unutrašnjeg tržišta.[51]

Direktiva reguliše i pravnu zaštite lica, čijji se se podaci prikupljaju i čuvaju i predviđena je obaveza preduzimanja potrebnih mera za svaki protivpravan pristup podacima koji se čuvaju i postupak utvrđivanja odgovornosti bilo u upravnom, bilo u krivičnom postupku. Sankcije u ovim slučajevima moraju po svojoj prirodi i težini biti srazmerne i takve da odvraćaju od daljeg kršenja zakona.

VII Međunarodne policijske organizacije i kompjuterski kriminalitet

1.Interpol

Međunarodna kriminalistička policijska organizacija (*fran.-Organisation internationale de police criminelle)*poznatija po svojoj telegrafskoj skraćenici Interpol je organizacija koja se bavi međunarodnom policijskom saradnjom. Osnovana je 1923. godine u Beču na međunarodnom kongresu Udruženja kriminalističkih policija i od 1989. godine sedište se nalazi u francuskom gradu Lionu. Osnovni cilj Interpola je:

1. da osigura i unapređuje najšire uzajamno pomaganje svih organa kriminalističke policije u granicama važećih zakona različitih država i u duhu Univerzalne Deklaracije o pravima čoveka Ujedinjenih nacija iz 1948. godine;
2. i da uspostavlja i razvija sve institucije koje mogu efikasno doprinositi prevenciji i represiji zločina i krivičnih dela iz opšteg prava.[52]

Interpolu okuplja policijske službe iz 190 zemalja, što ga čini posle Ujedinjenih nacija petom međunarodnom organizacijom po broju država članica u svetu. Njegova aktivnost izmedju ostalog podrazumeva i preduzimanje koraka ka suzbijanju kompjuterskog kriminaliteta. Interpol svoje aktivnosti vrši u koordinaciji sa nacionalnim policijskim službama preko Biroa za saradnju koji se nalaze u svakoj državi članici.

[51] Član 12. *Direktive Evropskog parlamenta i Saveta o čuvanju podataka koji su dobijeni ili obrađeni prilikom pružanja javno dostupnih usluga elektronske komunikacije ili javnih komunikacionih mreža*

[52] Član 2 Statuta Interpola - *Article 2 of The Constitution of the ICPO-INTERPOL adopted by the General Assembly at its 25th session* (Vienna - 1956). I/CONS/GA/1956(2008)

Vlada Singapura je Interpolu poklonila u septembru 2014. godine savremeni centar za borbu protiv kompjuterskog kriminaliteta, koji je počeo sa radom u aprilu 2015. godine. Centar se nalazi u Singapuru i predstavlja posebnu organizacionu jedinicu Interpola pod nazivom IGCI (eng. INTERPOL Global Complex for Innovation) u okviru koga je posebno Odeljenje za borbu protiv kompjuterskog kriminaliteta IDCC (eng. INTERPOL Digital Crime Centre) i Odeljenje za razvoj CIO (eng. Cyber Innovation and Outreach). U rad Centra su se uključile i mnoge IT kompanije koje su pomogle formiranje Centra i materijalno i kadrovski, tako centar ima već dve stotine i tridest zaposlenih stručnjanka iz više od pedeset zemalja od kojih su većina ranije bili zaposleni kao vodeći stručnjaci u kompanijama poput Kasperski, Majkrosof, Simens itd.

Osnovne aktivnosti Centra su da prikuplja i obrađuje podatke, procenjuje i upozorava nacionalne policijske službe na potencijalne krimalne pretnje, da oktriva krivična dela i njihove počinioce, da radi na prevenciji kompjuterskog kriminaliteta, da radi na jačanju međunarodne policijske saradnje, da pruža pomoć u veštačenjima i istragama nacionalnim policijskim službama, da pruža pomoć u obuci policijskih službenika, i da radi na razvoju novih tehnologija radi suprostavljanja kompjuterskom kriminalitetu. U okviru Odeljenja za borbu protiv kompjuterskog kriminaliteta IDCC danonoćno rade i dežurni timovi stručnjaka koji obaveštavaju nacionalne policijske službe o svakoj mogućoj kriminalnoj pretnji.

Od formiranja Centra Interpol je zajedno za nacionalnim policijskim službama sprečio više stotina hakerskih napada, oktrio više slučajeva kompjuterskih prevara i pronovera, i oktrio više slučajeva seksualne eksploatacije dece na internetu. Zahvaljući Centru odnosno Odeljenju za borbu protiv kompjuterskog kriminaliteta samo na Filipinima je u 2015. godini otriveno više organizovanih kriminalnih grupa koje su se bavile dečjom pornografijom i uhapšeno je preko sto osoba i zapljenjeno je preko hiljadu računara koji su sadržali eksplicitni seksualni sadržaj.[53] Procene čelnih ljudi Interpola su da će Odeljenje za borbu protiv kompjuterskog kriminaliteta sprečiti vršenje više hiljada krvičnih dela na godištnjem nivou i na taj način sprečiti sticanje protivpravne imovinske koristi u iznosu od preko pet milijardi evra. U prilog ovoj proceni ide I podatak , da je samo u aprilu 2015. godine u operaciji Simda Odeljenje za borbu protiv kompjuterskog kriminaliteta otkrilo kompjuterski virus koji je u višegodišnjem periodu napao preko 700 hiljada računara putem interneta i čija je svrha napada bila da od korisnika računara krade podatke o platnim karticama radi dalje zloupotrebe.

[53]INTERPOL Annual report 2014, INTERPOL General Secretariat, Lion , Fracuska, januar 2015. godine , str. 28

2.Evropol

Evropol je agencija Evropske unije koja je osnovana Ugovorom o Evropskoj uniji (EU) iz Mastrihta 1992. godine, i to Konvencijom Evropskog Saveta o Evropolu. Konvencija je stupila na snagu 1.oktobra 1998. godine. Evropol je počeo sa radom prvog jula 1999. godine, sa sedištem u Hagu, ipredstavlja specifičan vid saradnje policijskih službi država članica EU. Ciljformiranja Evropola je da poboljša saradnju policijskih službi i efikasnost nadležnih organa u borbi sa najtežim oblicima kriminala, koji pogađaju dve ili više država članica.

Glavni zadaci Evropol su lakša razmena informacija između država članica, operativna analiza, analitička obrada podataka o krivičnim delima, održavanje informacionog sistema i njegov razvoj, obavljanje složenih veštačenja i logističke pomoći kriminalističkim istragama policije.

Evropol nema ovlašćenja za hapšenje kriminalaca, već zahvaljući bazi podataka koju poseduje omogućava policijskim službama da kroz specijalizovan informacioni sitem imaju brz uvid, razmenu i obradu podataka. Informacionim sistemom Evropola policijske službe država članica su međusobno povezane, a deo infomacionog sistema su i države koje imaju potpisane sporazume sa Evropolom.

Baze podataka Evropola se odnose na podatke o osuđenim počiniocima krivičnih dela koja spadaju u nadležnost Evropola i licima koja su osumničena da su počinila krivična dela koja spadaju u nadležnost Evropola, kao i podatke za krivična dela i informacije o tome kada su i gde počinjena, sredstva koja bili korišćena ili mogla da budu korišćena za izvršenje krivičnih dela, policijske službe koje su se bavile delom ili slučajem, podatke o licima za koje postoji sumnja da su članovi kriminalnih organizacija, i podatke o presudama za krivična dela koja spadaju u nadležnost Evropola. Baze podataka se formiraju zahvaljući podacima koje dostavljaju policje zemalja EU i svih trećih država.

Ministarstvo unutrašnjih poslova Republike Srbije sarađuje sa Evropolom od 2009. godine i to na osnovu Zakona o potvrđivanju Sporazuma o strateškojsaradnji između Republike Srbije I Evropola.[54]

Jedna od glavnih oblasti delovanja Evropola je borba protiv kompjuterskog kriminaltiteta i tu svrhu osnovan **je Centar za borbu protiv visokotehnološkog kriminala** - European

54 "Sl. glasniku RS", br. 38 od 25. maja 2009.godine

Cybercrime Centre (EC3). Centar je počeo sa radom u januaru 2013. godine i ima zadatak da pomogne u zaštiti državnih organa, privrednih subjekata i građana od sve rastućeg kompjuterskog kriminaliteta u Evropskoj uniji, koji je posledica velike informacione pismenosti, razvijene informacione infrastrukture, elektronskog bankarstva i internet trgovine. Glavni oblasti delovanja Centra su :

1. borba protiv organizovanih kriminalnih grupa (pogotovo onih koje je bave finansijskim prevarama na internetu);
2. borba protiv dečje pornografije i seksualne ekspolatacije na internetu;
3. zaštite podataka od krađe;
4. i zaštita vitalnih informacionih sistema Evropske unije.

U skladu sa ove tri oblasti delovanja Centar pruža pomoć policijskim službama na sledeći način i to kao : obaveštajni i logistički centar; centralna baza podataka; centar za obuku; centar za veštačenje; centar za saradnju sa nevladinim sektorom i privredom.

Centar veliku pažnju usmerava i suzbijanju zloupotreba platnih kartica koje na nivou Evropske unije svake godine naprave štetu od milijardu i po evra, i Evropol je sproveo više uspešnih akcija na ovom polju[55]. Kako je upotreba platnih kartica raširena već skoro 20 godina na prostoru EU i kako je samo u 2011. godini ukupna vrednost plaćanja karticama bila preko 3000 milijardi evra, jasno je zašto ova oblast od posebnog značaja za Evropol.[56]Do zloupotrebe platnih kartica dolazi tako što izvršioci nabavljaju podatke sa kartica služeći se raznim metodama, a zatim te podatke prodaju, ili sami koriste. Samo 2011. godine u Evropskoj uniji bilo je 20.244 prijavljenih zloupotreba, što je skoro duplo više u odnosu na 2010.godinu, kada je bilo prijavljeno 12.383 zloupotreba.[57]

Centar je kao deo Evropola učinio dosta i u borbi protiv dečje pornografije i dosada je zahvaljući Centru razbijeno više kriminalnih grupa i uhapšeno na stotinepedofila. Poslednja u nizu uspešnih akcija Centra je kada u saradnji sa američkom federalnom policijom FBI i

55 Najpoznatija akcija Evropola protiv organizovanih kriminalnih grupa koje se bave prevarama i zloupotrebama kartica bila je "Plavi ćilibar" (eng. Blue Amber), u kojoj je učestvovalo preko 50 policijskih službi. U ovoj operaciji uhapšeno je preko 130 lica koja su u višegodišnjem periodu, zlopotrebom platnih kartica kupovala i preprodavala avio karte preko interneta i na taj način oštetila 38 avio kompanija i stekla protivpravnu dobit u iznosu od preko milijardu evra. Izvor http://www.computerweekly.com/news/4500248925/Police-arrest-130-in-global-anti-cyber-fraud-operation preuzeto dana 30.08.2015.godine

56 Europol – "*Public information version - Situation Report-Payment Card Fraud* "Luxembourg: Publications Office of the European Union god. 2012.godine str.4.

57 Europol – "*Public information version - Situation Report-Payment Card Fraud* "Luxembourg: Publications Office of the European Union god. 2012, str.8.

rumunskom policijom u februaru ove godine, spasao dvogodišnju bebu iz Rumunije koju je njen otac zlostavljao i slike i video zapise zlostavljanja postavljao i nudio radi prodaje na internetu.[58]

Centar je zaslužan i za formiranje Evropske finasijske koalicije za borbru protiv seksualne eksploatacije dece na internetu koja radi pod patronatom Evropske Komisije (eng. European Financial Coalition against commercial sexual exploitation of children online). Koaliciju čine predstavnici policijskih službi kao i predstavnici nevladinog sektora, privrede i istaknuti pojedinci koji se bore protiv zloupotrebe dece i njihove eksploatacije dece na internetu. Zahvaljući Centru i Koaliciji godišnje se obradi preko milion sumnjivih pornografskih sardžaja na internetu.[59]

Centar za borbu protiv visokotehnološkog kriminala bavi se i obaveštajnim aktivnostima, tako da u okviru centra radi i tim specijalizovan za prikupljanje informacija na internetu, njihovu analizu i prepoznavanje potencijalnih pretnji pobezbednostEU.

Po Digitalnoj Agendi Evropske Komisije za Evropske Uniju za 2020. godinu informaciona tehnologija je ključ privrednog razvoja i bezbednost na internetu je jedan od prioriteta obezbeđivanja tog razvoja.[60] Centar u cilju sprovođenja Agende intezivno sarađuje sa CERT-om (eng. Computer Emergency Response Team) koji predstavlja službu EU zaduženu za bezbednost organa Evropske Unije od pretnji koje dolaze sa interneta.

VIII Institucionalni okvir suprotstavljanja visokotehnološkom kriminalu u Republici Srbiji

Pravni okvir državnih organa nadležnih za borbu protiv visokotehnološkog kriminala uređen je Zakonom o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala (Sl. glasnik RS", br. 61/2005 i 104/2009), zakonom je uređeno obrazovanje, organizacija, nadležnost i ovlašćenja posebnih organizacionih jedinica državnih organa radi otkrivanja, krivičnog gonjenja i suđenja za krivična dela visokotehnološkog kriminala.

Visokotehnološki kriminal predstavlja vršenje krivičnih dela gde se kao objekat ili sredstvo izvršenja krivičnih dela koje su određena u zakonu javljaju računari, računarski sistemi, računarske mreže, računarski podaci, kao i njihovi proizvodi u materijalnom ili elektronskom

[58]Izvor https://www.europol.europa.eu/content/international-police-action-leads-rescue-22-month-old-romanian-sex-abuse-victim preuzeto dana 30.08.2015.godine
[59]Izvor http://www.europeanfinancialcoalition.eu/private10/images/document/2.pdf preuzeto dana 30.10.2015. god.
[60] European Commission , *Digital agenda for Europe* - European Commission Directorate-General for Communication Citizens information ; Luxembourg: Publications Office of the European Union, str.5

obliku. Računarski programi i autorska dela se smatraju proizvodima jer se mogu mogu upotrebiti u elektronskom obliku.

Zakon o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala primenjuje se radi otkrivanja, krivičnog gonjenja i suđenja za: [61]

1) krivična dela protiv bezbednosti računarskih podataka određena Krivičnim zakonikom;
2) krivična dela protiv intelektualne svojine, imovine, privrede i pravnog saobraćaja, kod kojih se kao objekat ili sredstvo izvršenja krivičnih dela javljaju računari, računarski sistemi, računarske mreže i računarski podaci, kao i njihovi proizvodi u materijalnom ili elektronskom obliku, ako broj primeraka autorskih dela prelazi 2000 ili nastala materijalna šteta prelazi iznos od 1.000.000 dinara;
3) krivična dela protiv sloboda i prava čoveka i građanina, polne slobode, javnog reda i mira i ustavnog uređenja i bezbednosti Republike Srbije, koja se zbog načina izvršenja ili upotrebljenih sredstava mogu smatrati krivičnim delima visokotehnološkog kriminala.

Više javno tužilaštvo u Beogradu je prema odredbama Zakona o javnom tužilaštvu ("Sl. glasnik RS", br. 116/2008, 104/2009, 101/2010, 78/2011 - dr. zakon, 101/2011, 38/2012 - odluka US, 121/2012, 101/2013, 111/2014 - odluka US i 117/2014) Zakona o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala, isključivo je nadležnoza krivično gonjenje svih krivičnih dela izvršenih putem visokih tehnologija.

U okviru Višeg javnog tužilaštva u Beogradu oformljeno je i Posebno odeljenje za borbu protiv visokotehnološkog kriminala koje čini posebni tužilac za visokotehnološki kriminal, zamenici tužioca, portparol, sekretar tužilaštva i ostalo tužilačko osoblje. Po zakonu, ali i po samoj prirodi stvari, prednost prilikom postavljenja imaju oni zamenici tužioca koji poseduju posebna stručna znanja iz oblasti informatičkih i radiodifuznih tehnologija .[62]

Posebno tužilaštvo za visokotehnološki kriminal je od osnivanja, odnosno od 2006. godine do osmog septembra 2015. godine, postupalo ili postupa u skoro šest hiljada predmeta u

[61] Član 3. *Zakona o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala* Sl. glasnik RS", br. 61/2005 i 104/2009
[62] Član 5. *Zakona organizaciji i nadleznosti drzavnih organa za_borbu protiv visokotehnoloskog kriminala*. Sl. glasnik RS", br. 61/2005 i 104/2009

okviru svoje nadležnosti. Odeljenje za borbu protiv visokotehnološkog kriminala Višeg suda u Beogradu nadležno je za sva suđenjenja u predmetima ovog tipa, dok je u postupku po pravnim lekovima nadležan Apelacioni sud u Beograd. Sudije Odeljenja za borbu protiv visokotehnološkog kriminala imenuje Predsednik Višeg suda u Beogradu iz reda sudija datog suda uz njihovu saglasnost.

Prednost imaju sudije koje poseduju posebna znanja iz oblasti informatičkih tehnologija. Osim toga, predsednik Višeg suda u Beogradu može u Odeljenje rasporediti i sudije drugih sudova upućenih na rad u taj sud, uz njihovu saglasnost.

U svakom slučaju, raspoređivanje traje najduže dve godine, a može biti i produženo odlukom predsednika Višeg suda u Beogradu, takođe uz pismenu saglasnost raspoređenog lica. Prednost u raspoređivanju konkretnih sudija u Odeljenje imaju nosioci sudijskih funkcija koji imaju iskustva u borbi protiv visokotehnološkog kriminala.

U okviru Ministarstva unutrašnjih poslova Republike Srbije radi suprostavljanja kompjuterskom kriminalitetu u okviru Uprave kriminalističke odnosno njene organizacione jedinice Službe za borbu protiv organizovanog kriminala formirano je Odeljenje za borbu protiv visokotehnološkog kriminala.

IX Specifičnosti gonjenja za dela visokotehnološkog kriminala

Krivična dela visokotehnološkog kriminala je izuzetno teško procesuirati i istražiti. Imajući u vidu da se radi o relativno novoj pojavi, sa transnacionalnim implikacijama, i da su države tek u protekloj deceniji prilagodile svoje zakonodavstvo, dolazi do niza problema u praksi. Međutim, u svim do sada predviđenim normativnim rešenjima ne postoji doslednost, a često ni minimum potrebne komplementarnosti, da bi se neko krivično delo protiv bezbednosti računarskih podataka uspešno procesuiralo.

Kao najvažniji problemi prilikom procesurianja dela visokotehnološkog kriminala izdvajaju se sledeći:

1. **Transnacionalni karakter –** Dela visokotehnološkog kriminala imaju izraženu nadnacionalnu dimenziju, te je na direktan ili indirektan način uključeno više država. Međutim, nedostak univerzalnog instrumenta međunarodnog prava u ovoj oblasti, značajno otežava međunarodnu saradnju. Jedan od najpoznatijih primera za ovaj problem, vezan je za dečju pornografiju i dogodio se u Austriji. Državljanin Austrije, je postavio sadržaj dečje pornografije

na internetu, koju su ostali pedofili mogli po novčanoj uplati da preuzmu. Server pomoću koga je nedozvoljen sadržaj postavljen bio je u Ruskoj Federaciji, a provajder servera ga je prijavio austrijskoj policiji, koja je pokrenula istragu i sprovela potrebna hapšenja. Većina lica koja su skinula sadržaj bila su iz Danske i Velike Britanije. Svim licima se sudilo u matičnim državama. Bez obzira na međudržavnu saradnju koja je u ovom slučaju bila besprekorna, postavilo se pitanje: "*Šta će se desiti, ukoliko određena država odbije saradnju iz formalno-pravnih ili političkih razloga*?" Ovo pitanje ukazuje na problem nepostojanja mogućnosti kažnjavanja počinilica, usled nedostatka pravnog instrumenta koji bi obavezao države na saradnju. Veliki je broj država čija zakonodavstva ne poznaju krvična dela visokotehnološkog kriminala, ili su dela inkriminisana na poseban način, ili svoje zakonodavstvo ne primenjuju. Takođe i zbog politike nekažnjavanja i neekstradicije određenih država bilo iz zakonskih ili političkih razloga za dela visokotehnološkog kriminala, određene države postaju sigurne države za počinioce krivičnih dela. Kako do danas ne postoji nijedan globalni instrumenti međunarodnog prava, koji bi regulisalao saradnju u ovoj oblasti, državama je ostavljeno da se protiv kompjuterskog kriminaliteta bore međusobnim bilateralnim sporazumima i regionalnim konvencijama, poput Konvencije Saveta Evrope. U budućnosti države će morati zbog neshvatanja društvene opasnosti koje visokotehnološki kriminal nosi, da sarađuju kako bi rešili nagomilane probleme, i moraće ubrzano da rade kako bi stvorili neophodnu proceduru, radi što bržeg reagovanja.

2. **Relativnost načela ignorantia iuris non excusat (** Nepoznavanje zakona nije izgovor) – Za izvršenje pojedinih krivičnih dela, kod počinioca uopšte ne mora postojati svest o onome što čine, kao i postojanje namere da se drugome naudi ili postojanje namere da se stekne određena protivpravna imovinska korist. Česti su primeri da korisnici "skidaju" sadržaje na internetu bez ikakvog znanja da su oni zaraženi kompjuterskim virusima, pa potom te iste sadržaje dalje prosleđuju svojim prijateljima i saradnicima, ili da prosleđuju sadržaje koje su primili u elektronskoj pošti, a koji su na protivpravan način pribavljeni. Kako u ovim radnjama društvena opasnost potpuno izostaje, o ovoj činjenici sudovi moraju voditi računa prilikom, odluke o poktetanju sudskog postupka.

3. **Obučenost pravosudnih organa –** Da bi pravilno postupali u postupcima, sudije, tužioci i ostali držani organi koji učestvuju u postupku moraju biti specijalizovani, ili se moraju specijalizovati u oblasti visokotehnološkog kriminala, jer je praksa pokazala da čak ni veštaci ne mogu predstaviti činjenice na takav način, koji bio razumljiv sudija koji ne poseduje nikakvo

predznanje iz infromacionih tehnologija i visokotehnološkog kriminala. Mnoge države su ovaj gorući problem pokušale da reše edukacijom svojih redovnih pravosudnih organa, ili uvođenjem specijalizovanih pravosudnih organa koji bi se isključivo bavili krivičnim delima visokotehnološkog kriminala. Uvođenje novih specijalizovanih pravosudnih organa je kvalitetnije i bolje rešenje, jer se na taj način stvaraju uslovi da se tužioci i sudije usredsrede na jednu oblast prava, uz naravno njihovo stalnu dodatnu edukaciju o svim segmentima viskotehnološkom kriminala, koji je procesuiranje počinilaca čini efikasnijim.

4. **Kako biti siguran, ko je počinilac krivičnog dela**? - Istražne radnje nadležnih organa, neće uvek dovesti do pravih počinilaca krivičnih dela. Specifična priroda ovih krivičnih dela, odnosno načina izvršenja, gde se upotrebljavaju informacione tehnologije, dolazi do izražaja prilikom indentifikacije počinilaca, i to najčešće zahvaljući IP adresi. Međutim, ne možemo sa apsolutnom sigurnošću tvrditi, da je vlasnik IP adrese i izvršilac krivičnog dela. Većina računarskih prevara je dovedena do tog nivoa savršenstva, da se olako upravlja tuđim računarima uspomoć drugih računara, a i česti su primeri da su druga lica, a ne vlasnik računara izvršioci krivičnih dela. Tipičan primer dolazi iz SAD-a m, gde je J.P. pravosnažno osuđen na zatvorsku kaznu u trajanju od pet godina, jer je poslao e-mail sa pornografskom slikom maloletnika. U ovom slučaju postojala je nedoumica policije, o tome da li postoji i odgovornost cimera osuđenog, jer se nije moglo sa pouzdanošću utvrditi da li je J.P. ili njegov cimer otvorio sporni e-mail nalog, da li je manipulisao putem Wi-Fi mreže nalogom koji nije bio zaštićen, i da je pronađeni CD sa pornografskim sadržajem pripadao njemu, a ne osuđenom J.P.-u.[63]

5. **Kako procesuirati počinioca koji koristi javne mreže? –** Teško je utvrditi počinioca koji je izvršio krivično koristeći javne WiFi mreže, koje su dostupne širokom krugu ljudi, npr. na aerodromima, autobuskim stanicama, trgovima, i drugim javnim mestima. Počinici se po pravilu brzo oslobađaju uređaja pomoću kojih su izvršili krivična dela, tako da čak i otkrivanje IP adrese, ne pomaže organima gonjenja, jer su počinioci, po pravilu, već odavno na bezbednoj lokaciji.

6. Problem dokazivanja dela na sudu – Dokazi u elektronskom obliku se pred sudovima koriste već duži niz godina, ali ne postoji opšte prihvaćeno stanovište, šta se sve smatra elektronskim dokazima. Po najširem stanovištu elektronskim dokazima se smatraju svi podaci

[63] Preuzeto sa http://arstechnica.com/tech-policy/2007/04/child-porn-case-shows-that-an-open-wifi-network-is-no-defense/ dana 10.08.2015. godine

koji su sačuvani ili preneseni u elektronskom obliku (npr. slike, tekst, video, pošta, programi, virusi itd.). Stephen Mason iz Britanskog instituta za međunarodno i uporedno pravo predložio je sledeću definiciju: *"Elektronski dokazi su podaci, koji su kreirani, manipulisani, skladišteni ili kojima se komunicira uređajem, kompjuterom ili kompjuterskim sistemom, ili su preneti preko komunikacionog sistema, a relevantni su za sudski postupak."*[64] U svim zakonodavstvima elektronski dokazi su izjednačeni sa klasičnim dokazima, dok ni u krivičnim, ni u građanskim stvarima nisu uređena procesna pravila, za pribavljanje, izvođenje i čuvanje elektronskih dokaza. Ali bez obzira na to koliko su precizno definisane procedure prikupljanja elektronskih dokaza, mora se voditi računa o poštovanju prava privatnosti i zaštite podataka.[65]

7. **Efikasan sistem prevencije –** Vrlo malo napora se ulaže u prevenciju izvršenja krivičnih dela visokotehnološkog kriminala za razliku od napora usmerenih na otkrivanje krivičnih dela visokotehnološkog kriminala, njihovo istraživanje i otkrivanja, procesuiranje i sankcionisanja počinilaca. Određene sankcije, koje su bile izricane protiv počinilaca u pojedinim državama, pokazale su se kao krajnje neefikasne poput zabrane prilaska računaru, zabrane upotrebe interneta i o kazne kućnog pritvora. Takođe, nadležni organi uopšte ne preduzimaju mera radi sprečavanja recidivizma, gde bi umesto kažnjavanja, eventualnim mera podsticaja počinilaca putem društvenokorisnog rada, alternativnih sankcija i stimulisanja kreativnosti radili na odvraćanju počinilaca od ponovnog vršenja krivičnih dela.

X Kompjuterska krivična dela u Krivičnom zakoniku Republike Srbije

Kompjuterska krivična dela uvedena su u naše pravo usvajanjem Zakona o izmenama i dopunama Krivičnog zakona Republike Srbije 2006. godine. Zakon određuje pojam visokotehnološkog kriminala kao vršenje krivičnih dela kod kojih se kao objekat ili sredstvo izvršenja krivičnih dela javljaju računari, računarske mreže, računarski podaci, kao i njihovci proizvodi u materijalnom ili elektronskom obliku.

Zaključuje se da su usklađene i krivičnopravna i materijalnopravna zaštita autorskih prava, jer se po Zakonu o autorskim i srodnim pravima ("Sl. glasnik RS", br. 104/2009, 99/2011 i 119/2012), autorskim delima smatraju „naročito računarski programi u bilo kojem obliku njihovog izražavanja, uključujući i pripremni materijal za njihovu izradu, zatim muzička dela sa

[64] S. Mason ; *International electronic evidence ;* British Institute of International and Comparative Law, London UK ; 2008,str. 35.
[65] Fredesvinda Insa; *The admissibility of electronic evidence in Court – Fighting against high-tech crime* ; Journal of digital forensic practice volume I, issue 4; 2006; str. 285-289.

ili bez reči i pripremni materijal za njihovu izradu, zatim muzička dela sa ili bez reči, kao i filmska dela.[66]

Pojavni oblici kompjuterskog kriminaliteta u našem pravu su krivična dela koja su sadržana u XXVII glavi Krivičnog zakona RS (Krivična dela protiv bezbednosti računarskih podataka). To su sledeća krivična dela:

1. Oštećenje računarskih podataka i programa;
2. Računarska sabotaža;
3. Pravljenje i unošenje računarskih virusa ;
4. Računarska prevara ;
5. Neovlašćeni pristup zaštićenom računaru, računarskoj mreži, i elektronskoj obradi podataka;
6. Sprečavanje i ograničavanje pristupa javnoj računarskoj mreži;
7. Neovašćeno korišćenje podataka i programa.

1.Oštećenje računarskih podataka i programa

Kivično delo oštećenje računarskih podataka i programa ima tri oblika, od kojih su dva teža, a jedan osnovni.[67] Osnovni oblik postoji kada neko neovlašćeno izbriše, izmeni, ošteti, promeniili na drugi način učini nepotrebljivim računarski podatak ili program.

Radnja osnovnog oblika krivičnog dela određena je alternativno, tako da se može izvršiti na sledeće načine: brisanjem, izmenom, oštećenjem ili prikrivanjem računarskog podatka ili programa. Generalna klauzula određuje da se ovo krivično delo može učiniti i na drugi način, odnosno na način koji čini neupotrebljivim računarski podatak ili program.

Postojanje krivičnog dela podrazumeva da se neka od delatnosti koja ima karakter radnje izvršenja preduzima neovlašćeno, bez odgovarajuče dozvole. Krivično delo je dovršeno kada je usled preduzete radnje računarski podatak ili program postao neupotrebljiv.

Objekat radnje su računarski program ili računarski podatak, izvršilac može biti svako lice ali u praksi to su samo ona lica koje su stručno osposobljena za preduzimanje navedenih radnji. Ovo krivično delo se može izvršiti samo sa umišljajem. Za ovo krivično delo propisana je novčana kazna ili kazna zatvora do jedne godine.

[66]Član 2. Zakona o autorskim i srodnim pravima."Sl. glasnik RS", br. 104/2009, 99/2011 i 119/2012

[67] Član 298. KZ Republike Srbije ("Sl. glasnik RS", br. 85/2005, 88/2005 - ispr., 107/2005 - ispr., 72/2009, 111/2009, 121/2012, 104/2013 i 108/2014)

Teži oblik ovog postoji ukoliko je pričinjena šteta u iznosu koji je veći od 450.000 dinara. Propisana kazna zatvora za ovo krivično delo iznosi oko tri meseca do tri godine.Najteži oblik krivičnog dela određen je u stavu 3, i postoji ako je izvršenjem dela pričinjena šteta u iznosu preko 1.500.000 dinara, Predviđena kazna zatvora za ovo delo je od 3 meseca do pet godina.

Potrebno je naglasiti da se pod drugim načinima činjenja neupotrebljivim podrazumeva i činjenje nedostupnima, tako da se ovaj način inkriminišu i slučajevi delovanja raznih „trojanskih" ili „back door" programa koji služe kako bi se određeni programi sakrili u memoriji kompjutera, radi izvršenja pripremne radnje za neko krivično delo npr. računarsku iznudu.[68] Potrebno je takođe utvrditi tačno vreme i mesto izvršenja krivičnog dela, da li se radi o neovlaščenom izvršiocu i način na koji je izvršeno krivično delo. Takođe u stavu četiri ovog člana propisana je obavezna primena mere bezbednosti oduzimanja predmeta kojim je izvršeno ovo krivično delo.

Napad na internet stranice je tipičan način izvršenja ovog krivičnog dela i predstavlja redovnu aktivnost hakera, napadnuti su samo delovi sajta odnosno naslovna strana, na kojoj hakeri ostavljaju svoj potpis.

Oštećena lica uglavnom sama ili uz tuđu manje ili više stručnu pomoć, pokušavaju da povrate programe i podatke koji su predmet izvršenja ovog krivičnog dela jer im najčešće svakodnevno poslovanje. Na ovaj način se najčešće uništavaju neposredni dokazi, koji bi mogli dovesti do otkrivanja izvršioca, a nadležnim ogranima ostaju samo posredni dokazi koji nisu dovoljni za procesuiranje izvršilaca.[69]

2.Računarska sabotaža

Računarska sabotažaje kompjutersko krivično delo koje čini lice koje unese, uništi, izbriše, ošteti, izmeni, prikrije ili na drugi način učini neupotrebljivim računarski podatak ili program ili ošteti računar ili drugi uređaj za elektronsku obradu i prenos podataka sa namerom da onemogući ili znatno omete postupak elektronske obrade i prenosa podataka koji su od

[68] D.Prlja, M.Reljanović, Z.Ivanović, Krivična dela visokotehnološkog kriminala, Beograd, 2011, str 142.
[69] L. Komlen Nikolić, Suzbijanje visokotehnološkog kriminala; Udruženje javnih tužilaca i zamenika javnih tužilaca Srbije, Beograd; 2010 , str. 90.

značaja za državne organe, javne službe, ustanove preduzeća ili druge subjekte.[70] Izvršilac ovog krivičnog dela može biti bilo koje lice, a u pogledu krivice potreban je umišljaj.

Objekat napada računarska sabotaže je dvostruko određen. Kao prvo to može biti računarski podatak ili program, ali to može biti i računar odnosno drugi uređaj za elektronsku obradu podataka, ali ovde se mora raditi o posebnom svojstvu oštećenog. Svi objekti napada moraju da pripadati nekom državnom organu, nekoj javnoj službi ili drugim pravnim licima (kao što su npr. ustanove, preduzeća ili druge organizacije), dok u pogledu radnje izvršenja i ostalih obeležja bića ovog krivičnog dela nema razlike u odnosu na krivično delo oštećenje računarskih podataka i programa

Propisana kazna zatvora za ovo krivično delo je kazna zatvora od šest meseci do pet godina. Krivična dela računarska sabotaža i oštećenje računarskih podataka i programa su slična prema načinu izvršenja i posledicama koje mogu ostaviti, zbog čega nadležni organi moraju biti oprezni prilikom pravne kvalifikacije krivičnog dela.

Ova krivična dela se razlikuju po težini posledica koje prouzrokuju, jer su posledice krivičnog dela računarska sabotaža mnogo teže i imaju znatno širi spektar posledica i objekata i pravnih subjekata. [71]Posledice krivičnog dela računarska sabotaža su se manifestuju u znatnom onemogućavanju ili znatnom otežavanju funkcionisanja državnog organa za duži vremenski period, zajedno sa ogromnom materijalnom štetom i gubicima.[72]

Takođe kao poseban oblik izvšenja računarske sabotaže postoji i unošenje podataka i programa koji napadnuti podatak ili program čine neupotrebljivim ili za posledicu imaju oštećenje i uništenje podatka ili programa.

Primer iz sudske prakse Republike Srbije – KT VTK 03/2009

Presudom Okružnog suda u Beogradu po optužnici Posebnog tužilaštva KT VTK.br.3/09 od 16.07.2009. godine N.R. iz Vranja oglašen je krivim jer je 29. i 30. decembra 2008. godine u službenim prostorija "Veterinaske stanice Vranje a.d." u Vranju u nameri da znatno omete

[70] Član 299. KZ Republike Srbije ("Sl. glasnik RS", br. 85/2005, 88/2005 - ispr., 107/2005 - ispr., 72/2009, 111/2009, 121/2012, 104/2013 i 108/2014)
[71] Lj.Lazarević - *Komentar Krivičnog zakonika*, 2011.godina, Beograd, str.881
[72] L.Komlen Nikolić ; *Suzbijanje visokotehnološkog kriminala*; Udruženje javnih tužilaca i zamenika javnih tužilaca Srbije, Beograd; 2010, str.94

postupak elektronske obrade podataka od značaja za rad Regionalne kancelarije, Uprave za veterinu, Ministarstva poljoprivrede i šumarstva i vodoprivrede za Pčinjski okrug.

N.R. je nakon uručenja Rešenja o otkazu Ugovora o radu koji je imao sklopljen sa Regionalnom kancelarijom kao operater na poslovima unošenja relevantnih podatka, sa hard diska računara izbrisao podatke o obeleženim i evidentiranim životinjama, i registrovanim i evidentiranim domaćinstvima zajedno sa svim podacima propisanim Uredbom Vlade Srbije ,kao i podatkatke o evidentiranim životinjama koji se unose u AIR- Centralnu bazu podataka Ministarstva poljoprivrede i šumarstva i vodoprivrede Republike Srbije.[73]

3.Pravljenje i unošenje računarskih virusa

Krivično delo pravljenje i unošenje računarskih virusa ima svoj osnovni i teži oblik.[74] Osnovni oblik ovog krivičnog dela može učiniti lice koje napravi računarski virus u nameri da ga unese u tuđ računar ili računarsku mrežu, kod težeg oblika mora biti pričinjena šteta.

Računarski virus je računarski program ili neki drugi skup naredbi unet u računar ili računarsku mrežu koji je napravljen da sam sebe umnožava i deluje na druge programe ili podatke u računaru ili računarskoj mreži dodavanjem tog programa ili skupa naredbi jednom ili više računarskih programa ili podataka.[75]

Radnja izvršenja ovog dela je pravljenje virusa. Sudsko veće u svakom konkretnom slučaju mora utvrditi šta su to kompjuterski virusi, kako se prave, koje su njihove vrste i karakteristike, svrha i sadržina.[76]

---

[73]J.Matijašević, *Krivičnopravna regulativa računarskog kriminaliteta* ; Pravni fakultet za privredu i pravosuđe, Novi Sad 2013 str. 148-150

[74] Član 300. KZ Republike Srbije ("Sl. glasnik RS", br. 85/2005, 88/2005 - ispr., 107/2005 - ispr., 72/2009, 111/2009, 121/2012, 104/2013 i 108/2014)

[75] Član 112. stv. 3. tačka 20. KZ Republike Srbije ("Sl. glasnik RS", br. 85/2005, 88/2005 - ispr., 107/2005 - ispr., 72/2009, 111/2009, 121/2012, 104/2013 i 108/2014)

[76] Ministarstvo unutrašnjih poslova Republike Srbije je prvu krivičnu prijavu za krivično delo pravljenje i unošenje računarskih virusa podnelo 2010. godine protiv O.C. iz Beograda. O.C. je napravio virus tipa trojanac pod nazivom OMEA koji je imao funkcije slikanja aktivnog monitora zaraženog računara, snimanja kucanja karaktera na tastaturi, kao i funkcije postavljanja sadržaja na "zaraženi" računar i skidanja sadržaja sa računara preko IRC kanala.O.C. je predstavljajući se lažno kao Irena Miletić, Johan Meister i Dr Mayer, je slao virus kao dodatak tekstualnom delu mejla koji je bio poslat na preko 70 elektronskih adresa. Virusom je uspeo da zarazi tri nemačka državljanina. Jedan od zaraženih računara, pripadao je licu koje je klijent "Baden-Wurttemnerg" banke. O.C. je njegove podatke iskoristio da bi putem elektronskog naloga na sajtu banke, lažno prikazao da je on korisnik i vlasnik računa i doveo u zabludu službenike da na račun jedne banke u Beogradu, uplate iznos od 2.600 evra, sa svrhom

Neophodnu pomoć sudu odnosno sudskom veću mogu da pruže veštaci informatičke struke. Ovo delo se smatra svršenim samim momentom pravljenja ovakvog virusa u nameri da se on unese u tuđi računar ili računarski sistem, bez obzira da li se takva namera i ostvarila u konkretnom slučaju.

Za ovo krivično delo alternativno su predviđene novčana kazna i zatvor šest meseci. Ako je pak, ovako napravljeni virus i unet u tuđ računar ili računarsku mrežu čime je prouzrokovana šteta (bilo imovinska ili neimovinska) radi se o težem obliku ovog krivičnog dela za koje je propisana novčana kazna ili kazna zatvora od dve godine.

Za uspešno vođenje krivičnog postupka protiv izvršilaca krivičnog dela neophodno je pribaviti sledeće dokaze :

1. utvrditi vreme i mesto izvršenja krivičnog dela ;
2. pribaviti računarski virus;
3. oduzeti alate i uređaje pomoću kojih je virus napravljen ;
4. ustanoviti način na koji je računarski virus unet u tuđu računar ili mrežu ;
5. utvrditi nastupanje štete.[77]

4.Računarska prevara

Krivično delo računarska prevara ima jedan osnovni, jedan lakši i dva teža oblika.[78] U svakom obliku radnje krivičnog dela potrebno je da je radnja podobna da se njome utiče na rezultat elektronske obrade podataka i da je ona razlog drugačije elektronske obrade. Osnovni oblik dela čini svako lice koje unosi netačane podatak ili unese bilo kakav važan podatak ili ako lice na drugi način prikrije ili lažno prikaže podatak i tako utiče na rezultat elektronske obrade ili prenosa podataka u cilju pribavljanja protivpravne dobiti ili izazivanja štete. Netačan podatak je onaj podatak koji ne odražava istinito ono na šta se odnosi.

Propisivanjem ovog krivičnog dela, namera zakonodavca je bila usmerena ka zaštiti verodostojnosti i integriteta kompjuterskih podataka, koji se elektronski putem obrađuju ili se na ovaj način vrši njihovo prenošenje. [79]

---

uplate "pomoć prijatelju". Preuzeto sa http://www.blic.rs/Vesti/Hronika/188170/Prva-krivicna-prijava-za-unosenje-racunarskog-virusa-u-Srbiji preuzeto dana 01.08.2015. godine

77 D.Prlja, M.Reljanović, Z.Ivanović – *Krivična dela visokotehnološkog kriminala*, Beograd, 2011. str 156.

78 Član 301. KZ Republike Srbije Novi Sad

79 Lj. Lazarević - *Komentar Krivičnog zakonika* , Beograd 2011.godina, str.884

Radnja ovog krivičnog dela može se podvesti pod radnje falsifikovanja, krivotvorenja, dovođenja u zabludu oštećenog, sve u nameri da se sebi ili drugom pribavi protivpravna imovinska korist, odnosno da se drugome nanese kakva imovinska šteta.

Za postojanje krivičnog dela dovoljno je da je radnja izvršenja predzeta u navedenoj nameri. Tog trenutka smatra se da je delo izvršeno, nije neophodno da je nastupila imovinska šteta za neko lice. Za ovo krivično delo je propisana novčana kazna ili zatvor do tri godine. Zavisno od visine pribavljene protivpravne imovinske koristi za učinioca ili neko drugo lice, zakon razlikuje dva teža kvalifikovana oblika ovog krivičnog dela.

Za teži oblik ovog dela je propisana kazna zatvora od jedne do osam godina postoji kada je pribavljena imovinska korist u iznosu od preko 450.000 dinara. Ako je pak, na ovaj način pribavljena protivpravna imovinska korist u iznosu od preko 1.500.000 dinara, radi se o najtežem obliku računarske prevare za koji se propisana kazna zatvora od dve do deset godina.

Za privilegovani oblik računarske prevare propisana je novčana kazna ili zatvor do šest meseci postoji kada je radnja krivotvorenje podataka ili prikirvanja ili lažnog prikirvanja računarskih podataka preduzeta u nameri da se na ovaj način drugom licu nanese kakva šteta, ni ovde ne mora da nastupi šteta ali ona mora da postoji pobuda, odnosno unutrašnji pokretač učinioca na preduzimanju radnje izvršenja. Može se raditi o imovinskoj, ali u drugim vidovima neimovinske štete. Od značaja za svaku državu je elektronska obrada podataka jer elektronsko poslovanje postaje dominantan način rada privrednih subjekata i državnih organa. Elektronske transakcije su pogodne za razne vidove zloupotreba, a sa povećanjem njihovog obima povećava se i broj krivičnih dela. U ovoj oblasti od značaja je i Zakon o elektronskoj trgovini.[80]

Primer iz sudske prakse Republike Srbije – KTM 01/2009

M.C.-u je zahtevom za sprovođenje istrage je stavljeno na teret da je zajedno sa D.Č. protiv koga je razdvojen postupak, lažno prikazivao podatke u nameri da pribavi protivpravnu imovinsku korist, i time uticao na rezultat elektronske obrade podataka tako što je najpre nelegalno pribavio podatke sa platnih kartica , koje su izdate američkih banaka, a potom neke upotrebio za plaćanje prilikom kupovine preko interneta na sajtu www.comtradeshop.com tako što je maloletni M.C. predstavljajući se kao vlasnik kartica, naručivao razne proizvode i prilikom

[80]Sl.Glasnik RS br 41/2009 i 95/2013

plaćanja je koristio podatke koje je pribavio iz platnih kartica unosio u elektronski nalog preduzeća CT RETAIL D.O.O. i tako vršio plaćanje kupovine mobilnih telefona, oštetivši ga za iznos od 270.238,00 dinara.

Svi proizvodi bili su naručivani na fiktivno ime Miloš Dimitrijević sa adresom u Vranju i kao kontakt sa poštanskim dostavljačem DHL-om su koristili mobilni telefon na koji se javljao D.Č. i preuzimao robu koju su dalje delili između sebe.[81]

5. Neovlašćeni pristup zaštićenom računaru, računarskoj mreži i elektronskoj obradi podataka.

Ovo krivično delo ima osnovni i dva teža oblika ispoljavanja. Osnovno delo čine lice koje kršeći mere zaštite, neovlešćeno pristupi računaru ili računarskoj mreži.[82] Radnja izvršenja je pristupanje, ulazak, upad u tuđi računar ili računarsku mrežu , radnja mora biti preduzeta od strane neovlašćenog lica, dakle protivpravno i drugo, kršenjem predviđenih mera zaštite. Sve ove okolnosti moraju biti obuhvaćene umišljajem učinioca dela. Za ovo delo propisana je novčana kazna ili zatvor u trajanju do šest meseci.

Za prvi teži oblik, je propisana novčana kazna ili zatvor do dve godine, i to za lice za koje se utvrdi da je upotrebilo podatak koje je pribavilo, odnosno do koga je došlo neovlašćenim pristupom zaštićenom računaru ili računarskoj mreži. Ova upotreba može biti u bilo kojoj nameri ili za bilo koju svrhu i cilj.

Svako lice koje poseduje osnovno informatičko znanje može biti izvršilac ovog krivičnog dela, jer radi zaobilaženje postavljenih barijera koje onemogućavaju pristup zaštićenom računaru nije potrebnoveliko poznavanje informacionih tehnologija odnosno načina funkcionisanja računara i mreža, u prilog ovoj tvrdnji ide i činjenica da su na Internetu dostupni različiti programi i stranice sprecijalizovani za lako izvršenje ovog krivičnog dela.

Ukoliko je zbog preduzete radnje i upotrebe na ovaj način pribavljnog podatka došlo do nastupanja teških posledica za drugog, radi se o najtežem krivičnom delu ove vrste za koje je zakon propisao kaznu zatvora do tri godine. Za ovaj oblik je bitno da je nastupila teška posledica

81 J.Matijašević, *Krivičnopravna regulativa računarskog kriminaliteta* ; Pravni fakultet za privredu i pravosuđe, Novi Sad 2013 .godina, str.147-148

82 Član 302. KZ Republike Srbije ("Sl. glasnik RS", br. 85/2005, 88/2005 - ispr., 107/2005 - ispr., 72/2009, 111/2009, 121/2012, 104/2013 i 108/2014)

za drugog i da između nje i preduzete radnje upada u računarski sistem postoji uzročno–posledična veza.

U svakom konkretnom slučaju potrebno je precizno utvrditi koje mere zaštite su prekršene i na koji način, što predstavlja bitno obeležje ovog krivičnog dela. Neovlašćene pristupe u državne organe, institucije i preduzeća od javnih značaja obavljaju po pravilu hakeri, za koje ni jedna mera zaštite ne predstavlja nepremostivu prepreku. Do sada nije bilo napada na organe i institucije od javnog značaja Republike Srbije, što ne znači da ih neće biti.

U slučaju napada na njih, pravo postupanja imali bi pripadnici Vojnoobaveštajne agencije (VOA), Vojnobezbednosne agencije (VBA) i Bezbednosno informativne agencije (BIA) jer se radi o podacima koji mogu imati vojni, ekonomski ili službeni značaj, i mogu biti proglašeni tajnim.

U okviru **bezbednosne zaštite** Ministarstva odbrane i Vojske Srbije i Republike Srbije poslovi koje VBA i VOA, između ostalog obavljaju su: bezbednosna zaštita tajnih podataka; personalna bezbednost (bezbednosna provera lica i izdavanje bezbednosnih sertifikata za lica kojima je pristup tajnim podacima potreban radi obavljanja funkcije ili radnih dužnosti u VBA i VOA); industrijska bezbednost; bezbednosna zaštita informaciono-telekomunikacionih sistema i kriptozaštite.

U okviru **kontraobaveštajne zaštite**, VBA: otkriva, prati i onemogućava obaveštajno delovanje, subverzivne i druge aktivnosti stranih država, stranih organizacija, grupa ili lica usmerenih protiv Ministarstva odbrane i Vojske Srbije; otkriva, prati i onemogućava unutrašnji i međunarodni terorizam, ekstremizam i druge oblike organizovanog nasilja usmerenih protiv Ministarstva odbrane i Vojske Srbije; otkriva, istražuje i prikuplja dokaze za krivična dela kojima se ugrožavaju tajni podaci i krivična dela protiv bezbednosti računarskih podataka, propisana Krivičnim zakonikom, zakonom kojim se uređuje tajnost podataka, kao i drugim zakonima kada su navedena krivična dela usmerena protiv Ministarstva odbrane i Vojske Srbije; planira, organizuje i sprovodi kontraobaveštajnu zaštitu lica, objekata, aktivnosti i tajnih podataka Ministarstva odbrane i Vojske Srbije.

Ako su aktivnosti i dela iz stava 2. tač. 1), 2), 3) i 4) člana 6. Zakona o Vojnobezbednosnoj agenciji i Vojnoobaveštajnoj agenciji ("Sl. glasnik RS", br. 88/2009, 55/2012 - odluka US i 17/2013) usmerena prema Ministarstvu odbrane i Vojsci Srbije od lica koja nisu pripadnici Vojske Srbije i zaposleni u Ministarstvu odbrane, VBA svoje aktivnosti i

mere na planu njihovog otkrivanja, praćenja i onemogućavanja, odnosno istraživanja i dokumentovanja preduzima uz obaveznu saradnju sa Bezbednosno-informativnom agencijom ili policijom, sa kojima zajedno utvrđuje način daljeg postupanja.

Primer iz sudske prakse Republike Srbije – VTK 56/2007

Posebno odeljenje je protiv V.M. iz Beograda, podnelo istažnom odeljenju Okružnog suda u Beogradu. Predlog za preduzimanje istražnih radnji KT.vtk.br 56/2007 zbog osnovane sumnje da je u hotelu Stari Grad u Kragujevcu, koji posluje u okviru preduzeća Tourist games stari grad, neovlašćeno pristupio računarskoj mreži oštećenog preduzeća Yunicom iz Beograda čiji je bivši radnik, na način što je putem internet mreže hotela, probio mere zaštite preduzeća Yunicom za pristupanje e-mail serveru preko koga su zaposleni u preduzeću Yunicom koristili za elektronsku poštu, i neovlašćeno pregledaovao i skidao poštu zaposlenih u preduzeću Yunicom.[83]

6. Sprečavanje i ograničavanje pristupa javnoj računarskoj mreži

Krivično delo sprečavanje i ograničavanje pristupa javnoj računarskoj mreži ima osnovni i teži oblik .[84] Računarske mreže su objekat zaštite kod ovog krivičnog dela, i to one mreže koje su dostupne neodređenom broju lica, i koje se svakodnevno koriste za obavljanje fiansijskih transakcija, trgovine ili društvene mreže. Računarskom mrežom smatra se skup međusobno povezanih računara, odnosno računarskih sistema koji komuniciraju razmenjujući podatke.[85]

Osnovno delo čini svako koje lice je neovlašćeno sprečilo ili omelo pristup javnoj računarskoj mreži. Za ovo delo je propisana novčana kazna ili zatvor do jedne godine. Računarske mreže su objekat zaštite kod ovog krivičnog dela. Izvršilac ovog krivičnog dela može biti bilo koje lice, a mora postupati sa umišljajem. Krivično delo je svršeno kada je izvršena radnja kojom se ometa ili sprečava pristup javnoj računarskoj mreži, kao i kada delo izvrši službeno lice u okviru svoje dužnosti.

[83] J.Matijašević, ; Krivičnopravna regulativa računarskog kriminaliteta ; Pravni fakultet za privredu i pravosuđe, Novi Sad 2013, str.155.
[84] Član 303. KZ Republike Srbije ("Sl. glasnik RS", br. 85/2005, 88/2005 - ispr., 107/2005 - ispr., 72/2009, 111/2009, 121/2012, 104/2013 i 108/2014)
[85] Član 112. tačka 18. KZ Republike Srbije ("Sl. glasnik RS", br. 85/2005, 88/2005 - ispr., 107/2005 - ispr., 72/2009, 111/2009, 121/2012, 104/2013 i 108/2014)

U slučaju, da se kao učinilac javi službeno lice u vršenju službe, tada se radi o kvalifikovanom obliku ovog dela za koji je propisana kazna zatvora do tri godine.

Tužilaštvo radi valjanje kvalifikacije ovog krivičnog dela mora utvrditi nepostojanje pravnog osnova za sprečavanje ili ometanje pristupa javnoj mreži ,vreme, mesto, način izvršenja krivičnog dela i svojstvo mreže odnosno da li se radi o javnoj mreži. [86]

Ovde se, radi o jednom posebnom obliku krivičnog dela zloupotrebe službenog položajaod strane ovlašćenog službenog lica koje sprečava ili ometa drugom fizičkom ili pravnom licu nesmetani pristup i korišćenje javne računarske mreže. Za dokazivanje ovog oblika krivičnog dela, potrebno je utvrditi svojstvo službenog lica odnosno izvršioca i radnju koju je izvršio.

7. Neovlašćeno korišćenje računara ili računarske mreže

Ovo krivično delo čini svako lice koje neovlašćeno koristi računarske usluge ili računarsku mrežu u nameri da sebi ili drugom pribavi protivpravnu imovinsku korist.[87] Računarskom mrežom se u smislu člana 118. KZ tačka 18. smatra svaki skup međusobno povezanih računara koji komuniciraju razmenjući podatke.

Kod ovog krivičnog dela radnja izvršenja je određena kao svako neovlašćeno korišćenje računarskih usluga ili mreže. Objekat zaštite je savesnost i zakonitost u korišćenju kompjutera, kompjuterskih mreža od svih oblika zloupotrebe i nesavesnosti.

Posledica ovog dela se sastoji u povredi zaštićenog dobra. Ovo krivično delo može učiniti svako lice, a u pogledu krivice potreban je direktan umišljaj. Za ovo delo propisana je novčana kazna ili kazna zatvora u trajanju do tri meseca.

Organi gonjenja su u obavezi da oštećenom dostave ili učine dostupnim sve podatke koje poseduju o izvršiocu kako bi ostvario gonjenje. Za ovo krivično delo po stavu 2. gonjenje je jedino moguće preduzeti po privatnoj tužbi. Ovlašćena službena lica su dužna da u slučaju izvršenja ovog preduzmu u okviru svoje nadležnosti sve potrebne radnje i mere da prikupe sve dokaze, i da ukoliko postoje postoje osnovi sumje da je pored ovog dela izvršeno i drugo delo

[86] V.Urošević, S. Uljanović, Z.Ivanović -*Mač World Wide Webu : Izazovi visokotehnološkog kriminala*; Beograd, 2012, str 97.
[87] Čan 304. KZ Republike Srbije ("Sl. glasnik RS", br. 85/2005, 88/2005 - ispr., 107/2005 - ispr., 72/2009, 111/2009, 121/2012, 104/2013 i 108/2014)

krivično koje se goni po službenoj dužnost, primene ovlašćenja i odredbe koje se odnose na podnošenje krivične prijave.

8. Pravljenje, nabavljanje i davanje drugom sredstava za izvršenje krivičnih dela protiv bezbednosti računarskih podataka

Krivično delo pravljenje, nabavljanje i davanje drugom sredstava za izvršenje krivičnih dela protiv bezbednosti računarskih podataka određeno je u članu 304a KZ Republike Srbije, i po njemu izvršilac ovog krivičnog dela je svako lice koje poseduje, pravi, prodaje ,nabavlja ili drugom licu daje na upotrebu kompjutere, kompjuterske sisteme, podatke i programe radi izvršenja krvičnih dela protiv bezbednosti računarskih podataka odnosno radi izvršenja krivičnih dela iz čl. 298. do 303. KZ. Za ovo krivično delo propisana je kazna zatvora u trajanju od od šest meseci do tri godine. Svi predmeti koji su korišećeni pri izvršenju ovog krivičnog dela se moraju oduzeti. Prvo krivično delo pravljenje, nabavljanje i davanje drugom sredstava za izvršenje krivičnih dela protiv bezbednosti računarskih podataka u Republici Srbije, je otkriveno i rasvetljeno 11.03.2015. godine po zvaničnom saopštenju Ministarstva unutrašnjih poslova Republike Srbije br. 100/11.[88]

Radnja izvršenja krivičnog dela može se sastojati u posedovanju, pravljenju, nabavljanju, prodaji ili davanju drugom kompjutera, sistema ili programa i podataka. Navedene radnje se preduzimaju radi izvršenja navedenih krivičnih odnosno radi pomoganja učiniocima koji vrše krivična dela iz čl. 298. do 303. KZ da ona postanu samostalna. Ova krivična dela su detaljno objašnjena i nije potrebna njihovo dodatno pojašnjenje.

Na gore navedeni način, zakonodavac je omogućio krivično pravnu žaštitu platnih kartica, ali i svih drugih objekata krivičnih dela iz grupe krivičnih dela protiv bezbednosti

[88] Pripadnici Ministarsva unutrašnjih poslova odnosno Službe za borbu protiv organizovanog kriminala su u saradnji sa Višim javnim tužilaštvom u Beogradu lišili su slobode Atilu Alaćana iz Subotice zbog osnova sumnje da je izvršio sledeća krivična dela protiv bezbednosti računarskih podataka: pravljenje i unošenje računarskih virusa, računarska prevara i pranje novca. Atila Alaćan je putem Interneta prethodno kupljeni kompjuterski virus, koji je sačuvao na servreru koji je zakupio, uneo u preko hiljadu računara širom sveta stvarajući botnet mrežu. Alćan je zatim putem zaraženih računara kojima upravljao sa svog servera na torent sajtovima postavljao zaražene fajlove koje je predstavljao kao filmove, koji su dalje upućivali na reklamu za internet stranicu koju je napravio Alćan, kako bi preko njega preuzimali navodno filmove, Atila Alćan je za ovu uslugu preko jedne kanadske kompanije naplatio preko sedamdeset hiljada američkih dolara. Preuzeto dana 02. 08. 2015. godine sa http://www.rts.rs/page/stories/sr/story/135/Hronika/857032/Uhap%C5%A1en+zbog+ra%C4%8Dunarske+prevare.hml

računarskih podataka i ujedno je izvršio inkriminaciju pripremnih radnji za vršenje ovih krivičnih dela, i to posebno krivičnih dela koja u sebi nose elemente krađe indentiteta.

9.Prikazivanje, pribavljanje i posedovanje pornografskog materijala i iskorišćavanje maloletnog lica za pornografiju

Krvično delo prikazivanje, pribavljanje i posedovanje pornografskog materijala i iskorišćavanje maloletnog lica za pornografiju određeno je članom 185. KZ. Ovo delo je određeno tako da ima četiri oblika i to:

1. U prvom obliku ovo krivično delo postoji ako lice maloletniku proda, prikaže ili javnim izlaganjem ili na drugi način učini dostupnim tekstove, slike, audio-vizuelne ili druge predmete pornografske sadržine ili mu prikaže pornografsku predstavu. Za ovaj oblik počinilac će se kazniti ili novčanom kaznom ili kaznom zatvora u trajanju do šest meseci.
2. U drugom obliku ovo delo čini svako lice koje iskoristi maloletnika za proizvodnju slika, audio-vizuelnih ili drugih predmeta pornografske sadržine ili za pornografsku predstavu. U ovom obliku zakonodavac je odredio samo zatvorsku kaznu u trajanju od šest meseci do pet godina.
3. Treći oblik postoji ukoliko se delo izvrši prema detetu. U ovom obliku zbog predmeta zaštite, zakonodavac je odredio samo kaznu zatvora i to na način što će se učinilac kazniti za prvi oblik zatvorom u trajanju od šest meseci do tri godine, a za drugi oblik zatvorom u trajanju od jedne do osam godina.
4. Poslednji četvrti oblik ovog krivičnog dela postoji kada lice za sebe ili drugoga, poseduje, prodaje, prikazuje, javno izlaže ,na elektronski ili drugi način čini dostupnim slike, video i audio zapise, ili druge predmete pornografske sadržine nastale iskorišćavanjem maloletnog lica. Za ovo delo predviđena je zatvorska kazna u trajanju od tri meseca do tri godine.

Iskorišćavanje kompjuterske mreže ili komunikacije, ili bilo kojih drugih tehničkih sredstava za izvršenje krvičnih dela protiv polne slobode prema maloletnom licu ili detetu. Krivični zakonik inkriminisao je u članu 185b. Postoje dva oblika. Kod prvog osnovnog oblika radnja izvršenja ovog krivičnog dela podrazumeva postojanje namere izvršioca da putem upotrebe kompjutera, kompjuterske mreže ili komunikacije dogovori sastanak sa maloletnikom i da se pojavi na

dogovorenom mestu korišćenjem računarske mreže ili drugih tehničkih sredstava. Za ovaj oblik predviđena je novčana kazna i kazna zatvora u trajanju od šest meseci do pet godina. Dok je u težem obliku postoji ukoliko je radnja izvršena prema detetu, i onda je predviđena zatvorska kazna u trajanju od jedne do osam godina.

XI Kriminološka tipologija kompjuterskog kriminaliteta

Kako postoje velike mogućnosti zloupotrebe kompjutera i informacione tehnologije, različiti su i oblici mogućeg proivpravnog ponašanja, tako da postoje i brojne klasifikacije krivičnih dela. Kompjuteri i informaciona tehnologija mogu poslužiti za izvršenje tradicionalnih oblika kriminaliteta ali i sasvim novih oblika kriminaliteta u vezi zloupotreba kompjutera, kompjuterskih sistema i mreža. U tradicionalne oblike kriminaliteta spadaju kompjuterske krađe, pronevere i prevare ,falsifikovanje. Novi savremeni oblici kompjuterskog kriminaliteta obuhvataju specifična krivična dela koja je jedino moguće izvršiti upotrebom kompjutera, kompjuterskih sistema i mreža. To su npr. hakovanje, stvaranje i distribucija virusa. Velike praktične mogućnosti koje pruža informaciona tehnologija, sa sobom nosi i opasnost od širenja i masovne upotrebe prisluškivanja, krađe poslovnih tajni, narušavanja privatnosti, a u poslednje vreme i realna opasnost od terorističkih akata.[89] Prof. dr V.Vodinelića je analizirajući ranije radove kriminologa i pravnika vezanih za kompjuterski kriminalitet, a trudeći se da pod pojmom kompjuterskog kriminaliteta obuhvati što više savremenih oblika kriminalnog delovanja podelio je kompjuterskog kriminalitet u četiri grupe:

1. neovlašćeno korišćenje računara,
2. manipulisanje računarima,
3. računarska špijunaža,
4. sabotaža računara.[90]

Ova podela je dovoljno široka tako da se njome može obuhvatiti većina krivičnih dela kompjuterskog kriminaliteta poput kompjuterskih krađa, prevara, pronevera, falsifikovanja, narušavanja privatnosti, špijunaža, terorizam, hakovanje, piraterija softvera,stvaranje i distribucija virusa. Ova krivična dela biće svaka ponaosob predmet posebnog razmatranja zbog svoje učetalosti u praksi.

[89] D. Jovašević, T. Hašimbegović , *Krivičnopravna zaštita računarskih podataka*,2008.godina; str.3.
[90] D.Jovičić, M.Bošković, *Kriminalistika metodika,* Banja Luka, 2002, str. 446–449

1. Kompjuterske krađe

Osnovno obeležje ovog dela je protivpravno oduzimanje tuđe pokrete stvari. Veoma su raznovrsni i promenljivi oblici u kojima se pojavljuje ovo delo, kao i načini njihove realizacije. Jedan od mogućih načina klasifikacije je i prema objektu koji se ovim delom prisvaja. U tom smislu u oblasti kompjuterskog kriminala postoje sledeći tipični oblici krađe:

1. Krađa računara i računarskih komponenti;
2. Krađa podataka;
3. Krađa računarskih usluga;
4. Krađa lozinki kodova i identifikacionih brojeva.[91]

U osnovi postoje dva načina realizacije ovog dela. Klasičan oblik koji podrazumeva fizički ulazak u prostorije i odnošenje računara i računaraske opreme i drugih stvari koje se protivpravano prisvajaju i drugi način, koji podrazumeva logički upad u računarski sistem i protivpravno prisvajanje računarskih podataka, kodova itd.

Ljudi su svesni vrednosti kompjutera i njegovih komponenti, pa su kompjuteri i ostali elektronski uređaji učestala meta današnjih lopova, kako je potražnja za kompjuterima sve veća krađe sve učestalije, jer se radi o robi koju lopovi brzo preprodaju.

U Velikoj Britaniji je u 2014. godini je prijavljeno da je ukradeno preko 183.523 kompjuterskih uređaja (laptopova, pametnih telefona, tableta i dr.). Najveći broj krađa je prijavljen u Mančesterskom upravnom okrugu i to 21.811, zatim u Zapadnom Jorkširu 17.120. Ogroman problem predstavljaju osetljivi lični i poslovni podaci koji se mogu naći na uređajima, tako da je Gradska uprava Glazgova u Škotskoj kažnjena sa 150.000,00 funti jer je nije preduzela neophodne mere kako bi zaštitila 74 laptop kompjutera koja su joj ukradena, na jednom od ukradenih laptopova nalazili su se podaci o bankovnim računima preko 6.000 stanovnika Glazgova.

Krađa podataka i trgovina njima, naročito onih podataka koji predstavljaju poslovnu i državnu tajnu, nije novijeg datuma ali je problem ogromnih razmera. Tehničke mogućnosti za krađu informacija pomoću kompjutera su ogromne. Internet nudi široke mogućonosti prodaje ili

[91]Slobodan R. Petrović,*Kompjuterski kriminal*; Ministarstvo unutrašnjih poslova Republike Srbije : Uredništvo časopisa "Bezbednost" i lista "Policajac",/ Beograd 2000.godina str. 117.

razmene ukradenih podataka. Zaštita od krađe podataka je neophodnost jer su informacije u današnjem vremenu ključ poslovnog uspeha, i ukoliko bi poverljivi podaci došli do konkurencije, mogli bijoj doneti odlučujuću prednost na tržištu.Upotrebom naprednih kriptoloških metoda, lopovima se omogućava sigurno prikrivanje prodaje podataka širom sveta, anonimnost koja vlada na internetu čini ga idealnim prostorom za prodaju ili trampu podataka.

Ketrin Arkuleta je u maju ove godine podnela ostavku na mesto šefa Savezne službe za upravljanje kadrovima SAD jer je otkriveno da su iz elektronske baze podataka te službe ukradeni podaci od preko 21,5 miliona ljudi, koji su u periodu od 2000. godine do danas konkurisali za posao u saveznoj administraciji. Podaci su naročito osetljivi jer su sadržali i bezbednosne provere ljudi, kao i podatke o zdravstvenom stanju.

Krađa računarskih usluga odnosno neovlašćeno korišćenje sistema, je jedan od najrasprostranjenijih vidova zloupotreva u oblasti informacione tehnologije. Iako krađa računarskih usluga spada u blaže oblike kompjuterske krađe, ipak štetne posledice koje može proizvesti nisu zanemarljive.

Cilj izvršenja ovog krivičnog dela je da se za objavljanje svojih poslova koriste tuđi kompjuterski resursi. Posledice koje mogu nastupiti su opterećenje rada poslovne mreže, usporavanje obavljanja redovnih poslova i neizvršavanja poslova. Učinioci su najčešće zaposleni ili bivši zaposleni koji imaju pristup do računarskih sistema i koji ga na ovaj način koriste da bi ostvarili dodatnu zaradu.

Ovo krivično delo najčešće čine hakeri, čije su mete telefonske kompanije i interent provajderi, oni na ovaj način obezbeđuju korišćenje njihovih resursa za sopstvene potrebe ili za izvršenje drugih krivičnih dela ili njihovo prikrivanje.

Krađa lozinki, kodova i identifikacionih brojeva je ista kao i krađa ključeva od automobila, jer su kodovi, lozinke i identifikacioni brojevi predstavljaju meru zaštite od trećih lica, i imaju cilj da spreče svaku nedozvoljenu radnju. Tako su hakeri u 2014. godini u Nemačkoj po podacima Nemačke Federalne Kancelarije za bezbednost ukrali lozinke za pristup elektronskoj pošti od preko 16 miliona ljudi i time ozbiljno ugrozili njihovu bezbednost i privatnost.[92]

[92] Preuzeto sa http://www.rtv.rs/sr_lat/evropa/milionska-kradja-lozinki-u-nemacko_454999.html dana 10.08.2015. godine

2. Kompjuterske prevare

Kompjuterske prevare su najrasprostranjeniji oblik kompjuterskog kriminaliteta, i susreću se u svakom delu privrednog poslovanja, koji može uticati na tokove robe i novca. Kompjuterske prevare su po svojoj prirodi najbliže privrednom kriminalitetu, a i u literaturi se, skoro bez izuzetka, ove pojave tretiraju kao pojavni oblik privrednog kriminaliteta. Kompjuterske prevare su najbrojnije u sledećim oblastima: finansijskog poslovanja, osiguranja, poreskih obaveza, socijalnog osiguranja, proglašavanjem stečaja, i pranja novca.[93]

Osnovno obeležje ovog dela je dovođenje nekog u zabludu, da bi se time pribavila protivpravna imovinska korist. Broj oblika kompjuterske prevare, kao i način njihove realizacije je praktično neograničen i u praksi se susreću kako one vrlo primitivne i grube, tako i one kod kojih učinioci ispoljavaju veliki stepen veštine i rafiniranosti.

Kompjuterske prevare predstavljaju najrašireniji vid kompjuterskog kriminaliteta, koji često prouzrokuje enormne štetne posledice. Kompjuterske prevare se vrše u nameri pribavljanja za sebe ili drugoga protivpravne imovinske koristi, s tim što se kod njih u zabludu ne dovodi ili održava neko lice, kao u slučaju običnih prevara, kod imovinskih krivičnih dela, već se ta zabluda odnosi na kompjuter u koji se unose netačni podaci, ili se propušta unošenje tačnih podataka, ili se na bilo koji drugi način računar koristi, za ostvarenje prevare u krivičnopravnom smislu.

Najpoznatiji oblik kompjuterske prevare je **nigerijska prevara** i ona spada u grupu prevara koja se vrši ulaganjem određene sume novca od strane prevarenog lica u određene poslove, naravno uz prethodno dato obećanje prevaranta da će se ostvariti znatno veća novčana dobit.

Ova vrsta prevare pojavila prvi put 80-ih godina prošlog veka i bila je povezana ubrzanim ekonomskim rastom Nigerije. Prevare su se uglavno vršile slanje poslovnih ponuda strancima za trgovinu ili eksploataciju nafte zahvaljući kojoj je Nigerija ekonomski ojačala.

Prevare su vršile slanjem lažnih poruka putem kompjuta odnosno elektronske pošte, i to o navodnim dobicima na igrama na sreću, i slanjem poruka vezanih za humanitarne priloge, poruke u vezi sa „ljubavnim i poslovnim ponudama“, preuzimanja nasleđa imovine najčešće nekih nepoznatih rođaka.

[93] J.Matijašević, *Krivičnopravna regulativa računarskog kriminaliteta* ; Pravni fakultet za privredu i pravosuđe, Novi Sad ,2013 str. 166.

Prevara se vršila početnim odabirom žrtve i njenim kasnijim ubeđivanjem metodama socijalnog inžinjeringa da unapred uplati određeni novčani iznos. Taj novčani iznos je u najvećem broju slučajeva neuporedivo manji od onog iznosa koji bi trebali da dobiju kao korist od nekog fonda, odnosno od pošiljaoca poruke. Elektronskom poštom se od primaoca tražila pomoć kojom bi došli do velikih novčanih iznosa, od par stotina hiljada do par desetina miliona dolara , a po uplati bi dobio određeni procenat od obećane zarade.

Prema državljanima Srbije koj su bili žrtve ovog oblika prevare, radnja izvršenja je izvedena na nekoliko načina: slanjem obaveštenja o lažnim dobicima igara na sreću nakon čega su žrtve uplaćivali određene sume novca da bi im se omogućilo podizanje nagrade, kao i slanjem obaveštenja o nasledstvu pomoću kojih su žrtve prevara metodama socijalnog inženjeringa navođene da poveruju da su nasledile određenu količinu novca, nakon čega su uplaćivali određene sume novca da bi im se omogućila isplata nasleđenog novca. [94]

3. Kompjuterske pronevere

Kompjuterska pronevera podrazumeva manipulaciju podacima s ciljem sticanja materijalne dobiti. Oblici kompjuterskih pronevera su podaci koji u informacionim sistemima reprezentuju dobra. Dobra predstavljena podacima su npr. novac, polaganje prava, radno vreme, kreditni rejting, bilansna stanja, lozinke, kodovi, identifikacioni brojevi i sl.

Pronevere putem kompjutera se teško otkrivaju, jer je često komplikovana kontrola i teško se dolazi do dokaza. Osnovno obeležje ovog dela je pribavljanje protivpravne imovnske koristi prisvajanjem vrednosti od onog kome su te vrednosti poverene. Kako je informaciona tehnologija kada je u pitanju privreda prvo uvedena u finansijske institucije, prve zloupotrebe su upravo učinjene u bankama ali u velikim poslovnim sistemima sa više hiljada zaposlenih. Kompjuteri i informaciona tehnologija su korišćeni u proneverama u kojima se vrši: falsifikovanje knjigovodstvene dokumentacije, ispostavljanje fiktivnih računa, ispostavljanje fiktivnih putnih naloga; kreiranje fiktivnih platnih spiskova, kreiranje fiktivne inventarske liste, kreiranje fiktivnih kupaca, veštačko povećanje zaliha robe, netačno prikazivanje gubitaka na

[94]V. Urošević, „*Nigerijska prevara u Republici Srbiji*“, Bezbednost – časopis Ministarstva unutrašnjih poslova Republike Srbije, Br. 3/2009, Beograd. str 145-156

robi, falsifikovanje kreditnih izveštaja, kreiranje lažnih finansijskih podataka i u dr. slučajevima.[95]

Ovaj oblik kompjuterskog kriminaliteta je široko raspostranjen u kategoriji kriminala belog okovratnika, jer uvođenjem tehnologije odnosno automatizacijom procedure za upravljanje platnim spiskovima, robom, prenosom robe između skladišta, potencijalni počinioci imaju veliki prostor delovanja.

Kompjuterske pronevere spadaju u grupu situacionih krivičnih dela, jer kod počinilaca ne postoji umišljaj pri izvršenju krivičnih dela, već se ova dela vrše, jer se pred počinicima ukazla „ dobra prilika", tako da bi bolja i učestalija neposredna kontola zaposlenih pogotovo u finansijskim institucijama u mnogome smanjila pronevere i krađe, jer bi se na ovaj način odvratio veliki broj potencijalnih počinilaca.

Jedna od najvećih pronevera odigrala se u Indiji 2009.godine. Indijska savezna policija uhapsila je predsednika upravnog odbora korporacije Satjam zajedno sa još trinaest osoba, korporacija je bila vodećih u sferi pružanja softverskih usluga u Indiji, vrednost provevere bila je preko 2,5 milijarde dolara, a rezultirala je konačnim gašenjem kompanije ove godine, otpuštanjem preko 20.000 zaposlenih i gubitka akcionara od preko 70 milijardi dolara. Sva uhapšena lica su osuđena na novčane i zatvorske kazne.[96]

4. Kompjutersko falsifkovanje

Osnovno obeležje ovog dela je stvaranje lažnih ili preinačavanje pravih predmeta, pomoću kompjutera, a sve radi pribavljanje protivpravne imovinske koristi. Tipični oblici korišćenja informacionih tehnologija radi falsifikovanja su: falsifikovanje dokumenata; falsifikovanje javnih isprava; falsifikovanje znakova za vrednost; falsifikovanje znakova za

[95]Slobodan R. Petrović; *Kompjuterski kriminal*; Ministarstvo unutrašnjih poslova Republike Srbije : Uredništvo časopisa"Bezbednost" i lista "Policajac",Beograd 2000, str. 131.

[96] Predsednik upravnog odbora je sa saučesnicima, falsifikovao odluke upravnog odbora i na taj način iz sredstava kompanije u višegodišnjem periodu proneverio preko 2,5 milijardi dolara, proneveri novac je uplaćivan na fiktivne firme i pojedince. Nadležni organi su u istrazi otkrili da je u jednom periodu korporacija isplaćivala plate 13.000 nepostojećih radnika. Proneverena sredstva kasnije su dalje korišćena za kupovinu akcija na berzi, i kupovinu preko 1000 nekretnina u Indiji inostranstvu na ime fiktivnih kompanija, kasnije su ustupana članovima porodica lica koja su učestvovala u proneveri. U proneveri ovih sredstava učestvovala je i amerčika revizorska kuća Pricewaterhouse Coopers koja je bila zadužena za upravljanje finasijskim sektorom korporacije Satjam i dvojica zaposlenih su osuđeni na zatvorske kazne jer su falsifikovali knjigovodstvenu i poslovnu dokumentacije.

obeležavanje robe; falsifikovanje novca; falsifikovanje potpisa; falsifikovanje žigova; falsifikovanje hartija od vrednosti.[97]

Pored navedenih predmeta falsifikovanja, informacione tehnologije omogućavaju i falsifikovanje elektronske pošte, koja predstavlja vrlo rasprostranje pojavu, odnosno da elektronska pošta ne dolazi od stvarnog pošiljaoca nego od nekog drugog.

Računari se pre svega koriste za falsifikovanje novca i putnih isprava,, preko 60% posto svih falsifikovanih novčanica i dokumenata otkrivenih u SAD je falsifikovano pomoću računara. Uprava za trezor SAD je zbog sve većeg broja falsikovanih novčanica više puta u poslednjih 20 godina morala da uvodi nove mere zaštite na novčanicama (vodene žigove, holograme, mikroštampa, nov papir za novčanice).

Računari se koriste i za falsifikovanje karti za prevoz, Mark Mason iz Donkastera u Engleskoj je u dvogodišnjem periodu od 2011.godine do 2013.godine falsifikovao preko 100 karata za prvu klasu britanskih železnica. Manson je u martu ove godine osuđen i nadoknadio je štetu železnici u ukupnom iznosu od preko 17.000 funti.

Falsifikovanje je jedan od društveno najrasprostranjenijh oblika kriminaliteta, posebno što sada informaciona tehnologija, zahvaljujući pre svega brojnim softverskim rešenjima, a i savremenim štampačima (danas čak i 3D štampačima) stvara izuzetno velike mogućnosti za realizaciju vrlo uspešnih falsifikata.

5.Narušavanje privatnosti pomoću informacionih tehnologija

Društveni i tehnološki napredak povezan je sa potrebama državnog aparata za povećanje bezbednosti i kontole pojedinaca. Do pojave interneta, mobilne telefonije i društvenih mreža, nadzor pojedinaca je predstavljao fizički posao, odnosno praćenje od mesta do mesta, intervjuisanje, posmatranje. Procenjuje se da je tajna policija Istočne Nemačke sarađivala je sa preko 500.000 saradnika informatora odnosno dostavljača, a imala je 10.000 zaposlenih samo na kontorli prepiske građana i prisluškivanju istih.[98]

Informaciona tehnologija omogućava akumulaciju ogromnog broja podataka o pojedincima. Podaci su akumulirani i skladišteni u elektronskim bazama, koje kasnije

[97]Peter J. Toren,*Intellectual Property and Computer Crimes (Intellectual Property usiness Crimes Series)* , New York USA, 2003, str. 6-41
[98]Preuzeto sa http://www.britannica.com/topic/Stasi dana 20.07.2015.godine

omogućavaju brzu obradu i pretragu. Razvijene države prednjače po upotrebi i razvoju tehnologija za široku kontrolu stanovništva i nadzor.

Utvrđeno je da sajtovi od 64. federalne službe SAD-a neovlašćeno uzimaju podatke lica koja ih koriste i vrše nadzor nad njihovom istorijom surfovanja po internetu. Bezbednosne službe država pod izgovorom bezbednosti svakodnevno narušavaju privatnost elektronske pošte građada. SAD su najdalje otišle po tom pitanju narušavanja privatnosti građana pa tako Nacionalna Sigurnosna Agencija SAD (NSA). Zahvaljući specijalizovanom softveru koji pretražuje sve mejlove koji su upućeni iz SAD-a ka inostranstvu i sve mejlove koju su upućeni u SAD iz inostranstva, koristeći kao kriterijum pretrage ključne reči (npr. bomba, oružje, napad itd.) svi mejlovi se potom skladište u slučaju neke dalje obrade ili potrebe.[99]

Sa sve boljim softverskim rešenjima vrši se prava invazija na privatnost građana, mada je masovna upotreba društvenih mreža to znatno olakšala.Ljudi ne razmišljajući ostavljaju gotovo sve svoje podatke na društvenim mrežama (ime, prezime, datum i mesto rođenja, podaci o zaposlenju, porodici, srodstvu, broj telefona, slike o svom domu, slike porodice i prijatelja, političke stavove itd.). U informaciono razvijenim zemljama o skoro svakoj osobi se skladište nekoliko stotina baza podataka od strane vladinih ustanova i velikih korporacija (nrp. Google. Yahooo , Amazon, Facebook , Vodafon, Orange, itd.). Usavršavanje biometrijskih dokumenata, upotreba platnih kartica, takođe olakšavaju stepen praćenja.

Ove baze podataka se često koriste u komercijalne svrhe, radi pronalaska određene kategorije potrošača, ili radi pronalska zaposlenih. Takođe se koriste u istragama državnih organa. Korporacija Google je tako podatke o svojim korisnicima prodavala specijalizovanim kompanijama za internet prodaju Amazon, Ebay, Paypal koji su ih kasnije koristili u komercijalne svrhe. Većina prikupljenih podataka može se upotrebiti radi ucene lica, jer određeni podaci predstavljaju tajnu i intimu lica (seksualno opredeljenje, politička pripadnost, tamna prošlost, zdravstveno stanje i sl.).

[99]Preuzeto sa http://www.theguardian.com/commentisfree/2013/aug/11/nsa-internet-surveillance-email dana 20.08.2015 godine.

6. Kompjuterska sabotaža

U praski su prisutni brojni oblici, kao i načini njihove realizacije ovog dela. Kompjuterske sabotaže se prema dosadašnjoj praksi uglavnom sastoje iz oštećenja ili uništenja kompjutera ili drugih uređaja za automatsku obradu podataka u okviru kompjuterskih sistema, ili delovanja počinilaca na informacije sadržane u memoriji kompjutera, na taj način što se brišu, menjaju ili se sprečava njihovo korišćenje. Sabotažom se može delovati na operativne mehanizme ili korisničke mehanizme koji su u pre svega u funkciji čuvanja podataka.[100] Osnovno obeležje ovog dela je prikriveno i podmuklo delovanje u vršenju službene ili radne obaveze, čime se nanosi šteta drugima.

Postoje dva osnovna oblika kompjuterske sabotaže i to logička sabotaža i fizička sabotaža.[101] Fizička podrazumeva fizičko oštećenje kompjutera i kompjuterske opreme, logička podrazumeva brisanje, oštećenje ili modifikaciju podataka, programa ili delova operativnog sistema.

Stvaranje i distribucija štetnih programa tzv. ***malware***[102] u nameri uništenja ili oštećenja podataka ili računarskih mreža spada u računarsku sabotažu. U štetne programe spadaju virusi, trojanci, crvi, bombe i droperi, veb preotimanje i stenografija.[103]

Virusi su programi koji utiču na program tako što rade uz osnovni program ili se nekontrolisano kopiraju u sistemu računara i time utiču na rad računara. Trojanci ili trojanski konji su programi koji se kriju u okviru nekog drugog programa, i aktiviraju se uz taj programi vrše neželjene radnje poput virusa u računaru. Crvi su programi koji se neprestano umnožavaju, i

---

100 Z.Cvetković – Kompjuterski kriminal – članak, 2011 god. ; str. 7-8.

101 Najpoznatiji primer logičke sabotaže vezuje se za iranski nuklearni program. Naime, izraelske bezbednosne snage su pokrenule operaciju pod širfrovavnim imenom "Myrtus" koja je za cilj imala da onesposobi iransko postrojenje za obogaćivanje uranijuma koje se nalaz i u gradu Nantancu. Operacija je brižljivo planirana, i trajala je nekoliko godina. Meta napada bili su softveri kompanije Siemens koji su upravljali postrojenjem odnosno centrifugama pomoću kojih se obogaćivao uranijum. Za potrebe ove operacje Izraelci su zajdeno sa američkim programerima izradili "stuxnet"crv koji po očekivanjima planera ove vojnoobaveštanje operacije trebao da toliko utiče na sistem postrojenja, da se troškovi obogaćivanja uranijuma povećaju do te mere, da se postrojenje učini nerentabilnim. Međutim akcija je do te mere bila uspešna da je u trogodišnjem periodu dok crv nije otkriven zahvaljujući izraelskih obaveštajcima prenet na više važnih kompjuterskih programa i sistema, koje je koristila iranska privreda. Zahvaljući ovom crvu Izraelci su veoma usporili iranski nuklearni program i izbegli nepotrebne ljudske žrtve koje bi bile neizbežne da je postrojenje napadnuto na konvencionalan način. Sabotaža je otkrivena 2010. godine. Izraelska strana nikada javno nije priznala da stoji iza sabotaže, smatra se da su u sabotaži učešće imali i američki obaveštajci, a da su u izradi crva učestvovali njihovi stručnjaci.Preuzeto sa http://www.nytimes.com/2010/09/30/world/middleeast/30worm.html?_r=0 dana 01.08.2015. godine

102 Preuzeto sa http://techterms.com/definition/malware dana 01.08.2015.godine

103 Preuzeto sa http://www.kaspersky.com/internet-security-center/threats/malware-classifications dana 01.08.2015. godine

opasni su jer mogu da se šire i na ostale računare u mreži. Droperi su programi kojima se skidaju i instaliraju virusi, bombe su programi koji aktiviraju određene viruse, koji mogu biti uspavani u sistemu računara. Stenografija se koristi radi skrivanja podataka o izvršenim krivičnim delima, i ona se koristi da se prostim vizuelnim pregledom, ne bi moglo utvrditi da je neko krivično delo izvršeno, već se zato moraju koristi posebni programi u računaru. Veb preotimanjem se korisnici lišavaju kontrole na internet pretraživačima ili sajtovima i preusmeravaju se na druge sadržaje.

Saboteri imaju različite motive koju mogu biti, političkog, ekonomskog, vojnog, službenog ili privatnog tipa. Kako u privrednoj utakmici nema milosti, i često se ne biraju sredstva pa su i sabotaže kompjuterskih sistema, mreža, internet stranica konkurenata sve učestalije.

Programer motivisan osvetom, kažnjen je na kaznu zatvora od trideset meseci, jer je početkom 2008. godine u američkoj saveznoj državi Njujork, u kompaniji u kojoj je bio zaposlen odnosno u kompaniji MedicoHealth Solutions, pokušao da sabotira računarski sistem i da je u tome uspeo više od sedamdeset servera kompanije, bi bilo oboreno i neupotrebljivo. Na servirama koje je kompanija koristila, nalazile su se poverljive informacije o propisanim receptima i medicinskim podacima pacijenata, kao i važni finansijski izveštaji i računi i platni spiskovi svih zaposlenih.[104]

7. Kompjuterska špijunaža

Osnovno obeležje ovog dela je odavanje tajne, a osnovni oblik se sastoji u saopštavanju predaji ili činjenju dostupnim poverljivih podataka uz upotrebu kompjutera i informacione tehnologije. Obaveštajne službe se angažuju preko svojih pripadnika radi otkrivanja političkih, vojnih, ekonomskih i službenih tajni drugih zemalja. U Japanu je važeća filozofija: *„Zašto utrošiti 10 milijardi na istraživanje, kada se sa milion dolara može podmititi inžinjer konkurencije i vrlo brzo dobiti isti, ako ne i bolji rezultat.”*[105] Većina zemalja u javnosti ne

[104] Programer je zajedno sa još šestoro svojih kolega programera, trebao da bude otpušten kao tehnološki višak usled spajanja kompanije sa korporacijom UNIX, on je tri dana od dana otkaza napravio kompjuterski virus koji je trebao da sabotira računarski sistem. Šteta pričinjena kompaniji iznosila je između 70.000 i 120.000 dolara. Preuzeto sa http://www.informationweek.com/medco-sys-admin-pleads-guilty-to-computer-sabotage/d/d-id/1059395? dana 02.08.2015. godine

[105] Janusz Piekalkiewicz ;World history of espionage: : Agents, systems, operations, National Intelligence Janusz Piekalkiewicz ;World history of espionage: : Agents, systems, operations, National Intelligence Book Center, Washington USA 1998.god. str 341.

plasira podatke o svojoj ofanzivnoj aktivnosti, već samo o defanzivnoj aktivnosti svojih službi na polju kompjuterske špijunaže.[106]

Baze podataka u državnim ,vojnim, istraživačkim i mnogim drugim institucijama predstavljaju pravu riznicu tajnih podataka, čije je odavanje sada moguće učiniti na vrlo jednostavan način, objavljivanjem na internetum što potvrđuje slučaj Asanž i afera Vikilinks, kao i slučaj američkog oficira Snoudena koji je odao vojne tajne Pentagona. Takođe, elektronska pošta, je često meta napada, jer sadrži prepisku državnih službenika. Iza kulisa svetske politike, odvija se pravi **informatički rat**[107] u kome pored uobičajenih aktera Rusije i zemalja NATO-a, sve više učestvuje i Kina. Naime informacioni sistemi su postali prioritet u radu obaveštajnih službi pre svega zbog tehnoloških, vojnih, i ekonomsko-poličkih podataka. Opšte je poznata činjenica da vlade mnogih zemalja, svesne svoje zavisnosti od naprednih tehnologija, usmeravaju svoje obaveštajne službe ka pribavljanju naprednih tehnologija svim nepotrebnim sredstvima. Za upade u tuđe informacione sisteme radi krađe poslovnih tajni sve češće se koriste hakeri. Armija SAD veruje da će saradnja sa kompjuterskim hakerima i nadzor nad internetnom biti esencijalni u postizanju informacione superiornosti nad protivnikom.[108]

8. Kompjuterska pornografija

Objekat zaštite kod ovog protivpravnog ponašanja je dostojanstvo ličnosti i polna sloboda.[109]Maloletnici i deca su posebno zaštitećene grupe, pa samim tim organi gonjenja veliku pažnju poklanjaju sadržajima na internetu koji sadrže eksplicitne seksualne scene sa decom i maloletnicima. Uglavnom je ovo krivično delo u zakonodavstvima određeno tako da postoje njegova četiri ooblika i to: proizvodnja dečijeg pornografskog materijala, njegova prodaja, rasuturanje i činjenje dostupnim.

[106] SAD su objavile da 50 % država u svetu, iz fiskalnih prihoda finansira obaveštajne akcije prema SAD.
[107] Preuzeto sa http://lat.rtrs.tv/vijesti/vijest.php?id=135279 dana 02.06.2015.godine
[108] Do 2015. godine vojska SAD-a je oformila preko četrdeset timova za tzv. "sajber" ratovanje i Ukazom Senata SAD, Državni sekretar zadužen za odbranu,23. juna 2009. godine naredio je formiranje novog roda vojske Sajber komandu (United States ***Cyber Command*** - USCYBERCOM). Prevashodni cilj novog roda vojske pored obezbeđivanja nacionalne bezbednosti, je suprostavljanje kineskim hakerima koji su kompromitovali preko četrdeset tajnih projekata razvoja oružja Pentagona, i ukrali poslovne tajne od preko sto američkih korporacija samo u 2014.godini.[108] U poslednjoj poseti kineskog predsednika SAD, predsednik SAD Barak Obama najvio je da će do kraja 2015. godine uvesti sankcije svim kineskim pojedincima i kompanijama koji su izveli hakerske napade na SAD i izjavio da kineski hakeri predstavljaju jednu od najvećih špijunskih pretnji po bezbednost SAD-a. Preuzeto sa http://edition.cnn.com/2015/08/31/politics/china-sanctions-cybersecurity-president-obama/ dana 31.08.2015.godine
[109] V.Đurđić, D.Jovašević – *Krivično pravo: posebni deo*, Niš, 2013, str.79.

Upravo zbog činjenice da pornografski materijali teško vređa moral i da je postoji stalni rad nadležnih organa i borba za njihovo suzbijanje, neshvatljiva je činjenica da se tržiste pornografskog materijala neprestano širi. Ključni doprinos tome je dala kompjuterska tehnologija. Zahvaljući pre svega internetu pornografija je dostupna širom sveta u različiti oblicima poput slike, videa, teksta, animacije i sl.

Konvencija o visokotehnološkom kriminalu delo Dečija pornografija inkriminiše na sledeći način:

1. proizvodnja dečije pornografije;
2. nuđenje ili na drugi način činjenje dostupnim dečije pornografije putem računarskog sistema;
3. distribuciju ili emitovanje dečje pornografije putem računarskog sistema;
4. nabavljanje dečje porngrafije za sebe ili drugoga putem računarskog sistema;
5. posedovanje dečje pornografije na računarskom sistemu ili na medijumu za prenos računarskih podaaka.[110]

Masovnim širenjem upotrebe interneta došlo je do ekspanzije pornografskih sajtova, čija je upotreba svakodnevna čak i u zemljama poput Saudijske Arabije, Kine, Turske koje se i po današnjim merilima smatraju konzevativnim. Trgovina seksualno eksplicitnim sadržajima je jedna od najraširenijih i koriščenijih aktivnosti na internetu. Nedozvoljeni oblici pornografije, gde postoji upotreba dece postaju sve raširenij pogotovo u Aziji najviše u zemljama Indokine, gde pojedinci i pedofili željni zarade seksualno eksploatišu decu. Deca se najčešče namamljuju i obmanjuju nuđenjem velike sume novca da bi kao modeli nagi pozirali, mada su česti primeri da i roditelji za novac pedofilima prodaju decu. Takve slike ili video zapisi na posebnim sajtovima ili putem elektronske pošte dalje prosleđuju. Da pedofilske mreže i sajtovi predstavljaju pretnju koju treba otkloniti konstatovano je na više međunarodnih konferencija. [111]

[110]D.Prlja, M.Reljanović, Z.Ivanović – *Krivična dela visokotehnološkog kriminala*, Beograd, 2011. str.8.

[111] U januaru prošle godine Nacionalni istražni biro Filipina je sproveo akcijuje u glavnom gradu Manili i uhapsio jedanaest osoba, kod kojih je pronasao fotografije filipinske dece, uzrasta od 12 do 16 godina u kompjuterima. Lica su uhapšena u prostorijama dve firme, koje su bile registrovane kao call-centri, uhapšena lica su metodama socijalnog inžinjeringa ubeđivala lica da se pretplate na njihove sajtove koji su im omogućavali da uživo gledaju seksualno nasilje nad decom, takođe sajtovi su sadržali i dečije pornografske video zapise i fotografije. Po procenama policije zarađivali su dnevno i preko osam hiljada dolara kojoj je pronašao fotografije filipinske dece. Preuzeto sa www.blic.rs/Vesti/Svet/438405/Na-Filipinima-zbog-decje-pornografije-uhapseno-11-ljudi dana 01. 08. 2015. god

Internet je imao i uticaj na širenje i tržišta dečje pornografije. Uglavnom je reč o posedovanju, ali i širenju materijala na kojem su deca i maloletnici. Ova krivična dela su vrlo specifična jer se vršenjem krivičnih dela iz sfere seksualne zloupotrebe i ekspolatacije dece, vrše teška kršenja osnovnih ljudskih prava i sloboda. Trajno se remeti razvoj ličnostižrtve usled primene psihičkog nasilja, kao glavnog metoda rada. Same žrtve su u većini slučajeva u potpunosti bespomoćne i samim tim lako podložne različitim vidovima psihičke manipulacije.

U početku policija i nadležni organi su vrlo lako otkrivali počinioce, međutim danas se širenje ovog tipa pornografije vrši putem zašitićenih sajtova i slanjem kriptovanih poruka. Kako je prihod od dečje pornografije ogroman, kao izvršioci se pojavljuju i ostali kriminalci, a ne samo pedofili, tako da je nivo organizovanisti dignut na viši nivo, a grupe ljudi kojima je pornografski sadržaj dostupan su sve zatvorenijeg tipa.[112]

Kako se problemu dečje porgnografije nije posvećivao dovoljan stepen pažnje, danas imamo situaciju da je ova oblast u potpunosti pravno regulisana, i da je usmerena velika pažnja nadležnih organa o čemu svedoče i brojne policijske akcije.

9. Kompjuterska propaganda

Internet državama služi za kontrolu mass-medija i formiranje mišljenja javnog mnjenja. Internet propaganda može da posluži za izvršenje kriminalnih dela poput: pozivanja na nasilne prome ustavnog poretka; izazivanja nacionalne verske, rasne mržnje i netrpeljivosti; širenje laži ; podsticanja na agresivni rat.

Brojni korisnici putem računara koji su povezani različitim internet stranicama i društvenim mrežama mogu na taj načiin da vrše različite propagandne aktivnosti sa negativnim predznakom i to širenjem ideološke, rasne, verske, nacionalne, mržnje putem interneta omogućava najčešće terorističkim grupama da šire svoj uticaj.

Informacione tehnologije i internet su vrlo važno sredstvo državnih organa za konrolu javnog mnjenja i građana. Kontrola interneta i društvenih mreža je uobičajena aktivnost nadležnih organa u svim državama sveta, jer je internet postao neizbežno sredstvo u svim političkim akcijama i kampanjama.

Društvne mreže zauzimaju vrlo značajno mesto za vršenje propagadnih aktivnosti. Minstarstvo za informisanje Ukrajine je za potrebe propagadnog rata angažovalo više

[112]D.Ćirović, N. Janković, M. Lađević – *Cyber podzemlje u Srbiji*, Reporter broj od 16.11.2005.godine, str.12.

"volontera" čije je osnovni zadatak usklađivanje internet vesti na svim pro-ukrajinskim sajtovim, i komentarisanje novosti na svim značajnim internet sajtovima vezanim za situaciju na istoku Ukrajine, kao i obaranje informacionih sajtova proruskih separatista.[113]

Internet komentari na vestima najčitanijih internet stranicama, su jeftino sredstvo za forimiranje javnog menjenja i širenja određenih političkih ideja i poruka van granica zemlje događaja.[114]

Društvene mreže su se pokazale kao vrlo važno sredstvo za formiranje mišljenja javnog mnjenja pri političkim izborima i danas su neizostavni deo svake političke kampanja, pogotovo kod animiranja mlađih kategorija birača i neopredeljenih.[115]

Mnoge vlade država u strahu od masovnih protesta protiv vlasti cenzurišu vesti na internetu, i onemogućavaju korišćenje masovnih društvenih mreža. Od grupe demonstranata u Njujorku do pokreta svetskih razmera 2011. godine upravo zahvaljujući internetu i društvenim mrežama je nastao pokret „Okupirajmo Wall street" čiju su članovi protestvovali zbog sve većih društvenih nejednakosti. Državni organi su u strahu od širenja protesta cenzurisali društvene mreže i internet, tako da je korporacija Yahoo cenzurisala mejlove svojih korisnika vezane za protest, dok je upotreba Tvitera bila onemogućena u potpunosti.[116]

---

[113]Preuzeto sa http://www.bbc.co.uk/monitoring/ukraines-new-online-army-in-media-war-with-russia dan 01.08.2015. godine

[114] Vlada Izraela je otišla korak dalje pa je zbog urušenog ugleda, svojim studentima koji studiraju u Zapadnoj Evropi i Severnoj Americi, daje i do dve hiljade dolara kako bi na na društvenim mrežama potvrdo komentarisali politička dešavanja i vojne operacije u Izraelu. Zbog učestalih akcija izraelskih snaga bezbednosti u Pojasu Gaze i na Zapadnoj obali, u kojima se primenjuje nesrazmerna sila prema Palestincima, Izrael je izgubio simpatije javnog mnjenja u zemljama EU i Severne Amerkie koje su glavne zaštitnice Izraela, tako da je ova akcija smatrana kao nužnost radi povratka poljuljanog poverenja Preuzeto dana 02.08.2015. godine sa http://www.usatoday.com/story/news/world/2013/08/14/israel-students-social-media/2651715/

[115] Samo za potrebe predsedničke kampanje 2008. godine sadašnji predsednik SAD Barak Obama je na reklamiranje naloga na Facebook-u potrošio preko šesnaest miliona dolara. Tim Demokratske stranke SAD je ovim potezom obezbedio ipak veliku uštedu jer se putem društvenih mreža lakše vrši politički marketing, i lakše se vrši targetiranje birača po izbornim jedinicama u kojima je Barak Obama bio u zaostatku u odnosu na protivkandidata. Dok je 2012. godine u predsedničkoj kampanji za potrebe promovisanja na najmasovnijim društvenim mrežama potrošio deset puta više nego suprotni kandidat Mit Romni, odnosno preko 47 miliona dolara. U ovoj kampanji akcenat je stavljen na društvenu mrežu Twitter gde je Obamu pratilo preko 16.miliona ljudi, a na Facebook-u pravljenje su grupe koje su reklamirale Obamu pojedinim grupama birača poput vojnih vetera, penzionera, latino-amerikanaca i sl. Preuzeto sa http://www.pbs.org/newshour/bb/media-july-dec12-download_11-16/ dana 02.08.2015. godine

[116] Slično je postupila i Vlada u Turskoj kada je zbog protesta na trgu Taksim, premijer Erdogan zabranio upotrebu Tvitera, internet cenzura je zbog delikatne političke i bezbednosne situacije u Turskoj uobičajena slika. Protest na trgu Taksim se brzo proširio zahvaljujući društvenim mrežama, i na gradove u unutrašnjosti zemlje, bezbednosne procenu su bile da je u jednom trenutku bilo više stotina hiljada demostranata širom Turske i da bi se njihov broj i dalje povećavao. Pored Tvitera u Turskoj bila je onemogućena upotreba i drugih društvenih mreža kao i postavljanje video snimaka na sajtu Youtube o protestima. Demostranti su većinom bili studenti i omladina koja je je najveći korisnik pomenutih sajtova. Preuzeto sa https://en.wikipedia.org/wiki/Censorship_in_Turkey dana 02.08.2015. godine

10. Kompjuterski terorizam

Informacione tehnologije postaju uobičajen alat i meta terorista, informaciona tehnologija se sve više javlja kao sredstvo izvršenja krivičnog dela terorizma. Osnovno obeležje ovog dela je vršenje nasilja. Postoji više oblika i načina izvršenja ovog dela. Jedna od bitnih komponenti terorizma je i psihološko ratovanje, u kojem je ubijanje nevinih ljudi, civila opravdana mera zastašivanja kojom se prenose poruke putem savremene tehnologije čine dostupnim širokim svetskim masama, sa ciljem izazivanja panike i nesigurnosti, a sve radi ostvaivanja određenih političkih ciljeva. Terorizam je jedan od najvećih problema savremenog sveta, a zločini terorista su sve brutalniji.

Još daleke 1969. godine smatra se da je izvršen je prvi teroristički napad čija su meta bili računari od strane antiratne organizacije Beaver 55, u napadu uništen je centar za elektronsku obradu podataka hemijske kompanije Dow Chemical, koja je proizvodila bojne otrove, napalm i hemijsko oružje za potrebe rata u Vijetnamu.

Zahvaljujući informacionim tehnologijama terorističke grupe su danas lakše povezane, i omogućeno im je lakše regrutovanjenovih članova i širenje njihovih ideja. Delovanje terorističkih organizacija, danas nije više geografski ograničeno u okviru određene teritorije, niti su one više finansijski i politički zavisne od vlada pojedinih država.Terorističke organizacije u svoje redove primaju i hakere i druge IT stručnjake koji napadaju hardvere i softvere država, njihovih organa i raznih drugih privrednih organizacija. Zabeležena je i pojava da se terorističkih grupe koriste i uslugama posebne vrsta tehnoloških plaćenika, koji su bili pripadnici bezbednosnih i obaveštajnih službi zemalja istočne Evrope.

Američke bezbednosne agencije su objavile da je Osama Bin Laden koristio usluge IT stručnjaka i da je putem kriprovane elekronske pošte komunicirao sa pripadnicima terorističke organizacije Al Kaida, još 1998. godine američke službe bezbednosti su kod uhapšenog organizatora bombaških napada Vadiha El Hagea na američke ambasade pronašli računar sa kriptovanom elektronskom poštom koju je slao ostalim pripadnicima Al Kaide.[117]

[117]Teroristi su komunicarili elektronskom poštom, odnosno digitalnim slikama koje su kada bi se uvećale u pikselima sadražale uputsva o terorističkim aktivnostima. M.Zirojević – Upotreba novih informatičkih i komunikacionih medija u svrhe terorizma – Revija za bezbednost; Centar za bezbednosne studije, Godina II, br. 11/2008 Beograd. str. 4

Teroristi koriste informacione tehnologije radi ostvarivanja svojih ciljeva na sledeći način:

1. Koriste kompjutere kao alat, odnosno putem svojih internet stranica i foruma prikupljaju nove članove, informacije i novčana sredstva kojim finansiraju svoje operacije izdaju saopštenja javnosti.
2. Koriste kompjutere kao arhivu svojih članova, finansijera, planova, izveštaja, kretanja svojih članova, broja bankovnih računa, spisak pomagača itd.
3. Vrše neovlaćeni upad u sisteme službi bezbednosti i ostalih državnih organa, ali i privrednih subjekata i pojedinaca koji su predmet njihovog interesovanja.[118]

Kako se napadi terorista organizuju sa ciljem privlačenja medijske pažnje, internet je postao glavno sredstvo zapredstavljanje terorista. Sve aktivne terorističke ogranizacije imaju bar neki oblik pristustva na globalnoj mreži. Na internetu je aktivno preko 5.000 sajtova terorističkih organizacija, tako da je internet glavno sredstvo povezivanja terorističkih organizacija, i one na taj način koordinišu svoje aktivnosti, daju uputstva svojm članovima i simpatizerima, i sve češće pozivanju na nasilje što je učestala praksa radikalnih islamističkih organizacija koje pozivaju na Džihad sve muslimane.[119]

Internet stranice terorista su vrlo profesionalno urađene sa i sadrže uglavnom informacije o nastanku i delovanju terorističke grupe kojoj pripadaju, o političkim ciljevima grupe, istaknutim pripadnicima, važnim govorima, obaveštenja o aktivnostima, i audio i video prezentacije. Usled velikog rizika od otkrivanja svojih članova terorističke organizacije koje deluju u Siriji (Islamska država, Front Al-Nusra i dr.) ne regrutuju više svoje članove u Evropi i Severnoj Americi na tradicionalan način umesto u džamijama kao što je bila praksa ranijih godina, većinu radikalnih muslimana teroristi regrutuju jer aktivno koriste društvene mreže. Proces selekcije, prove i posmatranja novih članova je dug i smatra se da je oko 4.000 članova na ovaj način regrutovano i zapadnoevropskih zemalja, SAD i Kanade.[120]

---

[118] Douglas E. Campbell ─ *Computer Terrorism*, Syneca Research Group, Inc. Washington USA, 2011.godine str.13-17.

[119] M. Zirojević – *Upotreba novih informatičkih i komunikacionih medija u svrhe terorizma* – Revija za bezbednost ; Centar za bezbednosne studije, Godina II, br. 11/2008 Beograd, str. 5

[120] Većina boraca su mahom potomci iseljenika iz arapskih zemalja, i upravo je njihov povratak kući sa ratišta najveća bezbednosna pretnja po te zemlje. Preuzeto sa http://www.businessinsider.com/isis-is-revolutionizing-international-terrorism-2015-5 dana 10.10.2015. godine

Bez obzira što su informacione tehnologije dostupne teroristima, one su isto tako dostupne i svim ostalim ljudima i državnim organima, tako da nadležni organi imaju mogućnost da isprate svaku negativnu pojavu pa i aktivnost terorista.

11. Hakovanje (hacking)

Osnovnoobeležje hakovanja je narušavanje sistema zaštite i neovlaščeni upad u informacione sisteme. Reč hakinhg potiče iz engleskog jezika i slobodnim prevodom ima značenje čovek protiv kompjutera.[121]

Postoje više oblika realizacije ovog dela. Najčešće hakeri korišćenjem raznih metoda i tehnika pribavljaju sve informacije potrebne za uspešan upad u tuđji informacioni sistem, ili zahvaljujući unapred pripremljenim programima koji su napravljeni radi zaobilaženja uobičajenih parametara zaštite prodiru u tuđe informacione sisteme. Radi ostvarenja ovog dela potrebno je veliko predznanje iz matematike i elektronike.

Osnovne karakteristike hakinga su : neovlaščen pristup informacionom sistemu; nasilan pristup, odnosno probijanje sistema zaštite; pristup se realizuje upadom u informacioni sistem; potrebno je visoko profesionalno znanje radi ostvarenja upada; mesto napada je udaljeno od mesta napadača; haker čini i druga dela poput špijunaže, prevare, pronevere, krađe usluga, sabotažu, distribuciju virusa itd.; haker deluje samostalno ili u grupi.[122]

Najčešče posledice hakovanja su: narušavanje sistema zaštite; usporavanje ili blokiranje funkcija sistema; neovlašćen pristup, oštećenje, izmena ili uništenje podatka; ilegalna distribucija programa; krađa; širenje virusa.[123]

Najbolji primer koji pokazuje koliko su hakeri opasni dolazi iz Velike Britanije, programeri jedne banke su otkrili da su hakeri neometano više od dve godine preusmeravali manje novčane iznose na svoje račune, kada to su otkrili obavestili su ostale finansijske i bankarske institucije, a nadležni organi su ustanovili da se radi o hakerskoj grupi iz Rusije, koja je na ovaj način oštetila više od sto finansijskih i bankarskih institucija, u ukupnom iznosu od preko 650 miliona funti.[124]

---

[121]Preuzeto sa http://en.wikipedia.org/wiki/Hacker_%28computer_security%29 04.06.2015.godine
[122]M.Drakulić,*Osnovi kompjuterskog prava*, Beograd, 1996. god ; str 449.
[123]Slobodan R. Petrović ;Kompjuterski kriminal; Ministarstvo unutrašnjih poslova Republike Srbije : Uredništvo časopisa"Bezbednost" i lista "Policajac",Beograd 2000.godina, str.180.
[124] Preuzeto sa http://www.telegraph.co.uk/news/uknews/crime/11414191/Hackers-steal-650-million-in-worlds-biggest-bank-raid.html dana 10.08.2015.godine

Hakovanje je ozbiljan problem, jer posledice mogu biti velike. Postoji velika tamna brojka u otkrivanju ovih dela, jer i žrtve ne znaju da su bile predmet napada, u većini slučajeva i ne prijavljuju, a ciljevi napada nemaju ograničenja. Stvoren je veliki osećaj nesigurnosti, ali pojavom firmi koje su specijalizovane za bezbednost podataka donekle se stanje i popravlja.

12. Stvaranje i distribucija virusa

Ovaj oblik kompjuterskog kriminaliteta je nezaobilazan u svim kriminološkim podela. Osnovno obeležje dela je stvaranje i distribucija kompjuterskih programa - virusa, čija je isključiva namena nanošenje štete trećim licima.

Kompjuterski virus je program koji izvršava nedozvoljene radnje u sistemu korisnika bez njegovog znanja i dozvole. Da bi se određeni program smatrao kompjuteskim virusom on mora da:

1. se sam aktivira i da ubacuje svoj kod na mesto putanje za izvršavanje drugog programa.
2. se sam replicirati, odnosno da zameni druge startujuće programe, inficiranim kopijama virusnnih fajlova, virusi ovo mogu vršiti i na personalnim računarima i na serverima.
3. ima nosioca, kako bi se u kontaktu sa trećim licem mogao dalje prenositi.[125]

Postojedvaoblikaizvršenja ovog dela pri čemu prvi stvaranje virusa je uvek svesna radnja, dok distribucija može biti i nesvesna radnja.

Kompjuterski virusi mogu izvršiti različite promene u sisteme ali najčešće su: promena veličine programa; usporen rad programa i sistema; pogrešno izvršavanje programa; onemogućavanje rada sistema i činjenje ga neupotrebljivim; promene u datoteci programa; uništavanje sadržaja; kopiranje nepotrebnih i štetnih programa i informacija; smanjenje raspoloživog slobodnog prostora u sistemu i dr.[126]

Virusi nisu postajali do sredine 80-tih godina prošlog veka, prvi virusi nastali su u univezitetskim centrima u SAD. Masovna pojava virusa nastupila je širenjem informatičke pismenosti i upotrebe računara, i brzim razvojem tehnologije. Izrada virusa je zahvaljujući sve

[125] D.Prlja, M.Reljanović, Z.Ivanović – *Krivična dela visokotehnološkog kriminala*, Beograd, 2011. str 157.
[126] Slobodan R. Petrović ,*Kompjuterski kriminal*; Ministarstvo unutrašnjih poslova Republike Srbije : Uredništvo časopisa"Bezbednost" i lista "Policajac",Beograd 2000.godina, str. 185.

naprednijim softverskim rešenjima olakšana , tako da i lice prosečne informatičke obrazovanosti može kreirati virus. Smatra se da svaki računar na mreži dnevno napadne jedan virusni program ali programi internet zaštite poput Avasta, Nortona, Kasperskog to onemogućavaju, tako da ti napadi ostaju nama neprimećeni. Virusi mogu da izazovu katastofalne posledice pogotovo na sistemima od javnog značaja poput, sistema za upravljanje saobraćajem, osvetljenjem, distibucijom el. energije, da ne govorimo o sistemima u upotrebi odbrane i zdravstva. Po podacima antivirus kompanije Norton najrasprostranjeniji virusi svih vremena su :

1. MYDOM koji je od 2004. godine do sada napravio štetu od preko 38 milijardi dolara i smatra se da je napao preko 2 miliona računara. Ovaj virus je tipa crv i širio se putem elektronske pošte.
2. SOBIG.F je vrsta virusa-trojanca koji se neprestano umnožava i na taj način ometa rad sistema, ovaj virus je od 2003. godine napravio štetu u iznosu od preko 37 ilijardi dolara i smatra se da je napao oko 2 miliona računara.
3. I LOVE YOU je virus koji se širi putem elektronske pošte i to kao dodatak mejlu unutar dodatka je virus, koji su korisnici sami instalirali u svoje računare, ovaj virus je od 2000.godine napao oko pola miliona računa i napravio štetu od preko 15 milijardi dolara.
4. CORE RED je crv koji napada računare koji koriste Windows 2000 ili NT on napada ove računare zbog velikih nedostataka ovih operativnih sistema, smatra se da je od 2001. godine ovaj tip virusa napao milion računara i napravio štetu od 2.6 milijardi dolara.
5. SLAMER ili SAFIR je virus koji usporava rad mreže i napada provajdere do sada je napao oko 200 hiljada računara i napravio štetu od 1.2 milijarde dolara.

Radi uspešne odbrane od kompjuterskih virusa potrebno je povećati stepen zaštite i informatičke obrazovanosti svih korisnika radi uspešnije prevencije, takođe vrlo je bitno i korišćenje licenciranih antivirus programa. Radi uspešne prevencije potrebno je preduzeti sledeće mere i to: blokiranje uobičajenih sajtova nosioca virusa; blokiranje pošte ili fajlova sa više nastavaka tipa doc.jpg.vbs; redovno ažuriranje antivirus programa; redovno ažuriranje ličnih

i poslovnih datoteka; ne skidati neproverene programe i podatake sa inerneta; tretiranje svakog neočekivanog mejla kao sumnjivog.[127]

13. Piraterija softvera

Osnovno obeležje dela je korišćenje ili umnožavanje softvera koji je pribavljen na nelegalan način. Dva su osnovna oblika ovog dela korišćenje ilegalnih kopija i distribucija ovakvih kopija. Širenje upotreberačunara uslovilo je povećanje potražnje za programskim rešenjima radi podmirenje raznovrsnih potreba sve rastućeg broja korisnika.

Termin piraterija softvera ušao je upotrebu 80-tih godina prošlog veka, a podrazumeva pojavu da pojedinci ilegalno kopiraju i koriste ili preprodaju tuđe programe. Izraz se obično koristi za krađu softvera koji prethodno namenjen prodaji. Softveri mogu biti izuzetno vredni, a zloupotrebom se oštećeni pre svega autori softvera, koji gube profit koji bi ostvarili da je softver pribavljen na legalan način, država je takođe oštećena, jer je lišena novca koji bi joj pripao po osnovu naplate poreza.

Motivi za pirateriju su različiti od ignorisanja zakona do sticanja profita. Sve raširenijom upotrebom piratskih verzija softvera dolazi do stagnacije softverske privrede koja do sada bila u višegodišnjem porastu, a samim tim smanjuju se i inovacije na ovom polju. Procenjuje se da Srbija izveze na godišnjem nivou softver u vrednosti od preko 200 miliona evra, ali je gubitak na ovom polju duplo veći usled piraterije. Kako softverski paket u proseku košta 50 eura, a svaki korisnik "skine" ,makar jednom mesečno jednu piratsku verziju nekog programa, jasno je da se radi o ogromnim finasijskim gubicima.

Procenat korišćenja piratskih softvera u svetu iznosi 42% od ukupnog broja softvera u upotrebi, u zemljama Evropske unije 33%, dok u Srbiji iznosi 70% sa trendom smanjenja.[128]

Upotreba piratskih softvera smatra se normalnom i ne postoji mehanizam sprečavanja, jer se inernet veze za skidanje takvih programa postavljaju svakodnevno, tako da softverske kuće pristaju na to da najprostije pakete svojih programa dele besplatno, dok je za naprednije dodatke koji poboljšavaju rad programa potrebna doplata.

[127] Z.Ivanović, D.Prlja, M.Reljanović–*Krivična dela visokotehnološkog kriminala*, Beograd, 2011. strane 168. i 169.
[128]Preuzeto sa http://www.politika.rs/rubrike/Ekonomija/Piraterija-odnosi-milijarde-dolara.lt.html dana 05.06.2015.godine

Čak i kompanija Microsoft to čini kako bi smanjila gubitke, jer po istraživanju njenih stručnih službni najveći problem predstavljaju pojedinci,odnosno individualni korisnici, a kako se piraterija teško dokazuje, jer se dokazi lako brišu, ovaj pristup se pokazao opravdanim jer je veći broj korisnika posle kupovao dodatke. Međutim bez obzira i na ovaj potez prodaja licenciranih programa je opala , tako da čini manje od 15% ukupnih prihoda kompanije, iako je u početku činila preko 70% prihoda. Novi operativni sistem Microsofta Windows 10, je pokušaj da se stane pirateriji na put, novi sistem prepoznaje nelegalne softvere i to svaki put kada računar koristi internet i tome obaveštava regionalne ili lokalne filijale kompanije, koje dalje obaveštavaju nadležne organe. Kompanija planira da sistem zaživi u preko 190 zemlja gde kompanija ima filijale ili predstavništva Sistem je zaživeo u SAD-u i Velikoj Britaniji gde se uveliko oduzimaju računari i propisuju kazne u iznosu od petsto funti.

Obični ljudi ne shvataju da se dosta vremena i sredstava ulaže u stvaranje programa, i da se na ovaj način finansijski obesmišljava rad programera. Piratskim pribavljanjem softvera neposredno šteti programerima i IT kompanijama, na isti način kao kada bi ukrali automobil. Američku ekonomiju piraterija jekoštala 200 milijardi dolara sume koja bi bila dovoljno za otvaranje 750.000 novih radnih mesta u privredi.[129]

XII Posebni deo - istraživanje

"Visokotehnološki kriminal u Srbiji u periodu od 2006. do 2013. godine."

Brz napredak i razvoj informacione tehnologije u poslednje dve decenije je, pored ogromnih prednosti koje su vidljive u svim sfrema života, doneo i nove oblike krivičnih dela, kao i nove načine za izvršenja postojećih. Republika Srbija je reagujući na ovakve pojave, ovu oblast uredila potrebnim normativnim odnosno zakonskim okvirom o kojem je bilo reči u ranijem delu rada. Imajući u vidu da naša zemlja nedovoljno brzo reaguje na društvene promene i ne prilagođava svoje pravosuđe novonastalim okolnostima, u oblasti visokotehnološkog kriminala opšti je zaključak da je reakcija države bila pravovremena i da Republika Srbija na ovom polju u potpunosti prati savremene tendencije u pravu i pravosudnoj praksi.

Osnivanjem specijalizovanih organa koji će se baviti istraživanjem, gonjenjem i sankcionisanjem krivičnih dela visokotehnološkog kriminala Republika Srbija (tada Državna

[129]Preuzeto sa http://www.poslovni.hr/hrvatska/privreda-sad-a-godisnje-gubi-vise-od-200-mlrd-dolara-zbog-piratstva-52710 dana 05.06.2015.godine

zajednica Srbije i Crne Gore) je bila među prvim državama u svetu koje su se na ovaj način suprostavile visokotehnološkom kriminalu.

Ratifikacijom Konvencije o visokotehnološkom kriminalu, Saveta Evrope i Dodatnog protokola uz Konveciju koji se bavi inkriminisanjem akata rasističke i ksenofobične prirode putem računarakao najnaprednijeg i sveobuhvatnijeg pravnog akta u ovoj oblasti i unošenjm odgovarajućih izmena u važeći Krivični zakonik i Zakonik o krivičnom postupku, Srbija je u potpunosti izvršila harmonizaciju svog zakonodavstva sa materijalnim i procesnim odredbama Konvencije, i na ovaj način pokazala svoju posvećnostu u suprostavljanju visokotehnološkom kriminalu kao deo šire međunarodne saradnje.

Implementacija donetih zakona na ovom polju se pokazala se izuzetno uspešnom, što za Republiku Srbiji i nije bio slučaj u prošlosti. Pratktično svi organi zaduženi za borbu protiv visokotehnološkog kriminala (Odeljenje za borbu protiv visokotehnološkog kriminala SBPOK-a, Odeljenja za borbu protiv visokotehnološkog kriminala Višeg suda u Beogradu, Posebno odeljenje za borbu protiv visokotehnološkog kriminala Višeg javnog tužilaštva u Beogradu) su od samog početka svog rada pokazali dobre rezultate u svom radu.

1. Predmet i cilj istraživanja

Kako je od osnivanja specijalizovanih organa za borbu protiv visokotehnološkog kriminliteta, prošlo relativno dosta vremena, koje možemo uzeti kao reprezentativno za istraživanje njihovog dosadašnjeg rada, za potrebe izrade ovog master rada sprovedeno je istraživanje u okviru Posebnog odeljenja za borbuprotiv visokotehnološkog kriminala Višeg javnog tužilaštva u Beogradu, organa koji je ujedno i najaktivniji u borbri protiv visokotehnološkog kriminala.

Predmet istraživanja je broj krivicnih prijava, podnetih optuznica i donetih presuda za krivicna dela kompjuterskog kriminaliteta Osnovni cilj ovog istraživanja je da se na osnovu prikupljenih podataka dođe do saznanja o obimu, strukturi i dinamici krivičnih dela visokotehnološkog kriminala, imajući u vidu da se radi o krivičnim delima novijeg datuma. Dobijeni podaci su takođe poslužili za analizu efikasnosti dosadašnjeg rada Posebnog odeljenja za borbu protiv visokotehnološkog kriminala.

2. Prostorni i vremenski okvir istraživanja

Prostorna granica istraživanja odnosi se na celu teritoriju Republike Srbije,a s obzirom da je od 2006. godine počela primena Zakona o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala (Sl. glasnik RS", br. 61/2005 i 104/2009), određeno je da za vremenski period istraživanja bude uzet period od 1. januara 2006.godine do 31. decembra 2013.godine.

3. Metode i hipoteze istraživanja

Radi sprovođenja istraživanja korištišćena je metoda analize podataka pribavljenog od Posebnog odeljenja za borbu protiv visokotehnološkog kriminala Višeg javnog tužilaštva u Beogradu.

U prijavi master rada navedene su sledeće hipoteze:

1. da su muškraci glavni počinioci krivičnih dela protiv bezbednosti računarskih podataka;
2. da su počinioci krivičnih dela protiv bezbednosti računarskih podataka punoletni;
3. da se svake godine beleži rast počinjenih krivičnih dela protiv bezbednosti računarskih podataka;
4. da su krivična dela protiv bezbednosti računarskih podataka , izvršena uglavnom od strane pojedinaca;
5. da su počinioci krivičnih dela protiv bezbednosti računarskih podataka , visokoobrazovana lica;
6. da su počinioci krivičnih dela protiv bezbednosti računarskih podataka , pripadaju srednjem sloju društva;
7. da su počinioci krivičnih dela protiv bezbednosti računarskih podataka zaposlena lica.

Za potrebe istraživanja upućen je zahtev kojim je od Posebnog odeljenja za visokotehnološki kriminal Višeg javnog tužilaštva u Beogradu zatražen uvid u podatke o broju osumnjičenih lica, okrivljenih lica, osuđenih lica za krivična protiv bezbednosti računarskih podataka, kao i podatke o broju predmeta po godinama, o broju pravosnažnih presuda po godinama, starosnoj strukturi osuđenih lica, obrazovnoj strukturi osuđenih lica, polnoj strukturi osuđenih lica, o radnom statusu osuđenih lica i o struktruri izvršenih krivičnih dela za period od 2006. do 2013. godine.

Međutim Više javno tužilaštvo u Beogradu, odnosno Odeljenje za visokotehnološki kriminal ne vodi evidenciju o podacima koji su zatraženi u Zahtevu za sprovođenje istraživanja, a pogotovo ne za period od 2006.godine do 2013.godine, jer je novi kompjuterski sistem evidentiranja predmeta i upisnika odnosno Standardizovana aplikacija za javna tužilaštva – SAPO u upotrebi od 2014.godine. Odeljenje za visokotehnološki kriminal ne vodi evidenciju ni o podacima koji se odnose na starosnu, obrazovnu i polnu strukturu, kao ni evidenciju o radnom statusu osuđenih lica.[130] Odgovorom na zahtev pruženi su samo podaci o broju predmeta po godinama i njihova klasifikacija po KT, KTR i KTN upisniku.

Na osnovu pribavljenog statističkog materijala od Posebnog odeljenja za visokotehnološki kriminal Višeg javnog tužilaštva u Beogradu iz gore navedenih razloga nije bilo moguće, proveriti tačnost svih navedenih hipoteza. Dobijeni podaci su poslužili za proveru tačnosti sledećih hipoteza:

1. da se svake godine beleži rast broja krivicnih prijava u posmatranom vremenskom periodu;
2. da su krivična dela protiv bezbednosti računarskih podataka, izvršena uglavnom od strane pojedinaca;
3. da broj počinilaca raste iz godine u godinu.
4. da je Posebno odeljenje za visokotehnološki criminal efikasno u svom radu.

4. Rezultati istraživanja

Za potrebe istraživanja Posebno odeljenje za visokotehnološki kriminal Višeg javnog tužilaštva u Beogradu dostavilo je samo podatke o ukupnom broju predmeta koji su kategorisani po upisnicima za period od 2006. godine do 8. septembra 2015.godine. Ukupan broj predmeta u datom periodu iznosi 5877, od kojih broj KT upisnika iznosi 1220 predmeta, KTR upisnika 3341, a ukupan broj KTN upisnika iznosi 1316.

Po članu 136. Pravilnika o upravi u Javnom tužilaštvu (Službeni glasnik RS", br. 110/2009, 87/2010 i 5/2012) evidencija upisnika za punoletne učinioce krivičnih dela "**KT**" upisnika sadrži osnovne podatke o punoletnim licima prijavljenih od strane policije ili drugih

[130] SAPO je centralizovani kompjuterski program za prikupljanje i obradu podataka, koji je uved u upravu javnih tužilaštava u Republici Srbiji kako bi podigao nivo efikasnosti njihovog rada i plod je IPA projetka koji finasira Evropska unija od 2008.godine, i njegovo Uvođenje je deo Nacionalne Strategije za reformu pravosuđa za period od 2013-2018 godine koju je Narodna skupština Republike Srbije usvojila 1. jula 2013. godine na sednici Sedmog Vanrednog zasedanja (Službeni glasnik Republike Srbije broj 9/10).

državnih organa, kao i od strane drugih lica ukoliko javni tužilac ili lice koje on odredi utvrdi da je iz priloženih dokaza ili na drugi način učinjeno verovatnim postojanje osnova sumnje da su izvršila krivična dela za koje se gonjenje preduzima po službenoj dužnosti, kao i osnovne podatke o primljenim obaveštenjima, preduzetim radnjama, odlukama tužioca i postupajućih sudova.

Evidencija upisnika za ostale krivične predmete "**KTR**" upisnika sadrži razne molbe, pritužbe, predloge, izveštaje i druge podneske državnih organa, pravnih lica i građana, kao i za vođenje napisa u javnim glasilima i upisivanje saznanja o događajima od značaja za rad javnog tužilaštva, za krivične prijave koje su nerazumljive, koje se ne mogu smatrati bilo kakvim izvorom saznanja o krivičnom delu ili učiniocu i koje su iz drugih razloga nepodesne za "**KT**" upisnik. **KTN** evidencija upisnika je evidencija nepoznatih počinilaca krivičnih dela.

Na osnovu objašnjenja značenja upisnika u Javnom tužilaštvu, vidimo da gore dati podaci, potvrđuju da je krivična dela kompjuterskog kriminaliteta, izuzetno teško procesuirati, jer je broj KT predmeta u Javnom tužilaštvu zastupljen sa svega 21% od ukupnog broja predmeta. Ovo znači da Posebno odeljenje za visokotehnološki kriminal, samo u ovim predmetima ima podatke o osumnjičenom, oštećenom, podnosiocu prijave i da je samo ovde izvršena tačna kvalifikacija krivičnog dela.

Grupa KTR upisnika je zatupljena u 57% slučajeva, i tužilaštvo u ovim predmetima, nema dovoljno podataka (kvalifikacija krivičnog dela, podaci o oštećenom, osumnjičenom i podnosiocu prijave) za dalje postupanje, već je potrebno prikupiti izveštaje od ostalih organa gonjenja, kako bi se naknadno odlučilo o daljem toku postupka.

Postupanje tužilaštva u KTN predmetima je ograničeno, jer ishod postupka u najvećoj meri zavisi od Ministarstva unutrašnjih poslova, to jest od otkrivanja indentiteta izvršioca krivičnog dela, i ovi predmeti su zastupljeni u 22% slučajeva. Ovi podaci, potvrđuju da su počinioci ovih krivičnih dela uglavnom anonimni, i da je tamna brojka kod ovih krivičnih dela izuzetno visoka.

1. Ukupan broj predmeta u vremenskom okviru istraživanja odnosno u periodu od 1. januara 2006. godine do 31. decembar 2013.godine, podeljen je u sledećoj tabeli po godinama.

Tabela br. 1 *Broj predmeta (KT,KTN, KTR) po godinama Posebnog odeljenja za visokotehnološki kriminal Višeg javnog tužilaštva u Beogradu.*

Godina	***Broj KT predmeta***	***Broj KTN predmeta***	***Broj KTR predmeta***	***UKUPNO (KT+KTR+ KTN)***
2006. godina	*19*	*/*	*/*	19
2007. godina	*75*	*11*	*68*	154
2008. godina	*110*	*14*	*60*	184
2009. godina	*91*	*42*	*114*	247
2010. godina	*116*	*13*	*443*	572
2011. godina	*130*	*28*	*502*	660
2012. godina	*114*	*65*	*609*	788
2013. godina	*160*	*243*	*558*	961
UKUPNO	***815***	***416***	***2354***	**3585**

Hipoteza "***da se svake godine beleži rast broja krivicnih prijava u posmatranom vremenskom periodu***" se u potpunosti može smatrati istinitom, na osnovu pribavljenih podataka koji su predstavljeni u Tabeli broj 1. U posmatranom vremenskom period ukupan broj predmeta u kojem je Posebno odeljenje za visokotehnološki kriminal Višeg javnog tužilaštva u Beogradu postupalo iznosi 3585, što možemo smatrati veoma reprezentativnim materijalom za proveru ove hipoteze. Čak i ukoliko bi kao početnu godinu istraživanja uzeli 2007. godinu i izuzeli podatke koji su prikazani u 2006. godini iz opsega istraživanja kao nereprezentativne, jer je u pomenutoj godini evidentirano samo 19 predmeta, pre svega zbog činjenice da je u toj godini Posebno odeljenje počelo sa radom, tačnost ove hipoteze, se ne dovodi u pitanje, a smanjenje broja predmeta ne utiče na uzorak istraživanja.

Ukupan broj predmeta za 2007. godinu u tužilaštvu iznosi 154, dok je za isti period u narednoj godini zabeležno 184 predmeta, iz ovih podataka vidimo povećanje u 2008. godini za čak 30%. U svakoj godini navedenoj u istraživanju se beleži rast broja predmeta u odnosu na prethodnu, najveći porast broja predmeta u Posebnom odeljenju zabeležen je u 2010. godini, gde je u odnosu na 2009. godinu broj predmeta uvećan za čak 131%. Da je rast broja predmeta iz godine u godinu konstantan, govori i podatak je broj predmeta u 2013. godini veći u odnosu na

2007.godinu za 524% , što govori da je tamna brojka kompjuterskog kriminaliteta izuzetno visoka.

2. **Ukupan broj predmeta po KT evidenciji upisnika za** period od 1. januara 2006.godine do 31. decembra 2013.godine, podeljen je po godinama i broju počinilaca u tabeli br.2.

Tabela br. 2 *Broj KT predmeta Posebnog odeljenja za visokotehnološki kriminal Višeg javnog tužilaštva u Beogradu po godinama i broju počinilaca*

Godina	***Broj KT predmeta***	***Broj počinilaca***
2006. godina	*19*	32
2007. godina	*75*	84
2008. godina	*110*	166
2009. godina	*91*	121
2010. godina	*116*	131
2011. godina	*130*	154
2012. godina	*114*	144
2013. godina	*160*	185
UKUPNO	***815***	***1047***

Drugu hipotezu da su krivična dela protiv bezbednosti računarskih podataka , izvršena uglavnom od strane pojedinaca, potvrđuju podaci prikazani u **Tabeli br.2.** Uvidom u Tabelu br.2 vidimo da je odnos ukupnog broja počinilaca i ukupnog broja KT predmeta za period od od 1.januara 2006.godine do 31.decembra 2013.godine iznosi 1,28 : 1, preciznije na jedan predmet odnosno krivično delo dolazi 1,28 počinilaca. U tabeli nema većih odstupanja u odnosu broja počinila i ukupnog broja KT predmeta za navedeni period, najmanji raspon zabeležen je u 2007.godini i iznoci 1,12 : 1 , dok je najveći raspon zabeležen u narednoj godini i iznosi 1,51 : 1. Iz ovih podataka vidimo da su krivična dela iz glave XXVII Krivičnog Zakonika Republike Srbije ("Sl. glasnik RS", br. 85/2005, 88/2005 - ispr., 107/2005 - ispr., 72/2009, 111/2009, 121/2012, 104/2013 i 108/2014) u navedenom periodu, u većini slučajeva uglavnom izvršena od strane pojedinačnih počinilaca, čije je potvrđena i tačnost druge hipoteze istraživanja.

Podaci iz ove tabele poslužili su i za proveru hipoteze "***da broj počinilaca raste iz godine u godinu***", koja se takođe na osnovu predstavljenih podataka nesumnjivo može smatrati

istinitom. Uvidom u Tabelu broj 2 vidimo da je ukupan broj počinilaca za KT predmete u 2006.godini iznosio 32, dok je u 2013.godini broj počinilaca iznosio 185 što je povećanje od skoro 500% Najveći kvantativni skok zabeležen je između 2007.godine i 2008.godine, kada je broj počinilaca sa 84 "skočio" na 166 što skoro rast od 100%, što nam govori da se radi o krivičnim delima sa ogromnom stopom rasta. Postoje vrlo mala odstupanja u rastu broja počinilaca iz navedene tabele, i ako 2009.godina beleži pad počinilaca u odnosu na 2008.godinu sa 166 na 121 i dalje možemo se smatrati da je rast broja počinilaca konstantan jer naredne godine beleže rast broja počinilaca ili je broj počinilaca približno isti, a i sama 2008.godina se može smatrati izuzetkom jer je broj počinilaca skoro duplo veći u odnosu na prethodnu godinu istraživanja.

3. U nedostatku materijala za istraživanje iz gore navedenih razloga, za potrebe izrade ovog master rada iskorišćeni su podaci iz publikacije "Visokotehnološki criminal - Praktični vodič kroz savremeno krivično pravo i primjeri iz prakse" izdatoj od strane Misije OEBS-a u Crnoj Gori u martu 2014.godine. Ovi podaci su prikazani u tabeli br.3 i odnose se na broj predmeta, lica, istraga, optužnih akata, i donetih presuda za krivično delo dečija pornografija iz čl. 185 KZ Republike Srbije, sve za period od 2010. do 2013.godine.

Tabela br.3 Broj predmeta, lica, istraga, optužnih akata, i donetih presuda za krivično delo iz čl. 185b KZ

Godina	***Broj predmeta***	***Broj lica***	***Istrage***	***Optužni akti***	***Presude***
2010. godina	*14*	*14*	*13*	12	10
2011. godina	*40*	*40*	*40*	40	35
2012. godina	*18*	*21*	*20*	20	14
2013. godina	*16*	*16*	*9*	5	4
UKUPNO	***98***	***91***	***81***	***77***	***63***

Podaci prezentovani u Tabeli br.3, takođe su potvrdili tačnost druge hipoteze istraživanja. Uvidom u tabelu vidimo da je odnos ukupnog broja predmeta i broja lica za krivično delo iskorišćavanje računarske mreže ili komunikacije drugim tehničkim sredstvima za izvršenje krivičnih dela protiv polne slobode prema maloletnom licu iz čl. 185b KZ, za period od 2010. do 2013.godine iznosi 1,08 prema 1. Raspon kretanja odnosa ukupnog broja predmeta i broja

počinilaca kreće se od najmanjeg 1,12 prema 1 do odnosa 1,68 prema 1 koji je ujedno i najveći. Ovi podaci nam nesporno ukazuju da postoje minimalna odstupanja u rasponu odnosa broja počinila i broja predmeta, a samim tim je i dodatno potvrđena hipoteza su izvršioci krivičnih dela viskotehnološkog kriminala u Republici Srbiji najčešće pojedinci.

U nedostatku podataka o strukturi izvršenih krivičnih dela jedino su podaci iz Tabele br.3 poslužili kao uvid u ***efikasnost rada Posebnog odeljenja za visokotehnološki kriminal***, a samim tim i proveru tačnosti poslednje hipoteze istaživanja. Na osnovu raspoloživih podataka za krivično delo prikazivanje, pribavljanje i posedovanje pornografskog materijala i iskorišćavanje maloletnog lica za pornografiju iz čl. 185 KZ, za period od 2010.godine do 2013.godine vidimo je ukupan broj predmeta 98, da je u 81 predmetu pokrenuta istraga dok su za 77 predmeta podneti optužni akti i u 63 predmeta su donete presude.

Analizirajući podatke po godinama rezultati rada Posebnog odeljenja za visokotehnološki kriminal su još impresivniji. U 2010. godini podneti su optužni akti u 12 predmeta, a presude su donete u 10, naredne godine donete su presude u 35 predmeta na osnovu optužnih akata podnetih u 40 predmeta, dok je u 2012.godini odlučeno u 14 predmeta od 20, a u 2013. godini donete su presude u 4 od 5 predmeta u kojima su podneti optužni akti. Ovi podaci govore da su u jednoj kalendarskoj godini donete prvostepene odluke u skoro 80% predmeta gde su podneti optužni akti što je daleko ispod proseka trajanja prvostepenog krivičnog postupka u Republici Srbiji koji iznosi 19 meseci.[131]

Pri analiziranju ovih podataka ne sme se zanemariti da se oni odnose na specifično krivično delo, gde su objekat zaštite maloletnici odnosno deca, pa je samim tim postupanje pravosudnih organa brže jer se vode načelom hitnosti.

Međutim, bez obzira na specifičnost krivičnog dela, ova hipoteza ide i u prilog stanovištu, da se ovom obliku kriminaliteta jedino efikasno možemo suprostaviti uvođenjem specijalizovanih pravosudnih organa. Na ovaj način se vrši i specijalizacija pravosudnog kadra koji je samim tim i stručniji za postupanje u ovim krivičnim delima, jer se na ovaj način stvaraju preduslovi da se tužioci i sudije usredsrede na jednu oblast prava, uz naravno njihovu kontinuiranu edukaciju o svim segmentima viskotehnološkom kriminala, koji procesuiranje počinilaca čine efikasnijim.

[131] Preuzeto sa http://www.mc.rs/upload/documents/NAJAVE/2014/CLJP/05-07-14_CLJP_Monitoring-rada-sudova-u-krivicnim-postupcima.pdf dana 10.07.015.godine op. citat

ZAKLJUČAK

Na osnovu prethodno iznetog, možemo zaključiti da ne postoji mogućnost apsolutne zaštite i da je svaki informacioni sistem izložen vrlo ozbiljnim rizicima. Smatramo najbolji način borbe protiv kompjuterskog kriminala u njegovoj prevenciji. Prevencija mora biti tako organozovana da odvrati potencijalne izvršioce kompjuterskog kriminala od izvršenja krivičnog dela, pri čemu polazna tačka moraju biti norme zakona koje se odnose na ovu grupu krivičnih dela.

Radi ostvarenja što adekvatnije zaštite i efikasnijeg mehanizma suprotstavljanja visokotehnološkom kriminalitetu, možemo da zaključimo najpre treba krenuti od poboljšanja zakonske regulative. U zakonskom tekstu mora se izgraditi što potpuniji krivičnoprocesni sistem reakcije na ovaj oblik kriminaliteta. Visokotehnološki kriminalitet kao transnacionalni društveni fenomen dovodi u pitanje osnovne vrednosti u najvećem broju savremenih država, zbog čega je od ključne važnosti sistem zaštite izraditi u skladu sa međunarodno prihvaćenim standardima koji su u praksi dali pozitivne rezultete. U tom kontekstu ključna stvar je razmena informacija između subjekata suprotstavljanja kriminalitetu na međunarodnom nivou, prikupljanje i razmena dokaznih materijala, kao i sprovođenje zajedničkih istraga agencija za sprovođenje zakona različitih zemalja.

Zakonodavstvo Republike Srbije vrlo dobro reguliše kompjuterski kriminalitet u materijalnom delu krivičnopravne materije, jer je u značajnoj meri usklađeno sa međunarodnim standardima. Međutim, potrebna su ozbiljna ulaganja u kadar, odnosno u lica koja su ovlašćena da postupaju u ovim predmetima. Potrebno je permanentno obrazovanje i usavršavanje u skladu sa svetskim tendencija u borbi protiv kompjuterskog kriminaliteta, kao i podizanje nivoa informatičke pismenosti ovih lica, sve u cilju njihovog efikasnijeg rada.

Ne sme se dozvoliti da sudije i tužioci da zbog nepoznavanja informacionih tehnologija, odugovlače sudske postupke, jer zbog specifičnosti krivičnih dela kompjuterskog kriminaliteta potrebno je brzo postupanje nadležnih organa radi otkrivanja počinioca i dokaza o izvršenim krivičnim delima.

Pored ulaganja u ovlašćena lica, paralelno se treba ulagati i u odgovarajuću opremu i infrastrukturu kojom bi se moglo odgovoriti na svaku eventualnu kriminalnu pretnju.

Kako je broj predmeta visoktehnološkog kriminalteta u Posebnom odeljenju Višeg javnog tužilaštva u Beogradu u konstantnom porastu trebalo bi izvršiti potrebne zakonske izmene

kojima bi se ono reformisalo. Reforme bi trebalo izvršiti na sličan način po kome su su formirana nova odeljenja tužilaštva za borbu protiv krivičnih dela korupcije u Novom Sadu, Kragujevcu i Nišu, odnosno potrebno je formirati novu mrežu pravosudnih i policijskih organa, jer bi se na taj način povećala efikasnost pravosudnih organa i pružio veći stepen pravne zaštite građanima od dosadašnjeg.

Radi suprostavljanja kompjuterskom kriminalitetu potrebno je produbiti međunarodnu saradnju, pre svega kroz implementaciju Konvencije o visokotehnološkom kriminalu Saveta Evrope sa Dodatnim protokolom.

Potrebno je i sa kriminološke strane radi uspešne prevencije dobro definisati profil izvršilaca krvičnih dela kompjuterskog kriminaliteta. Takođe treba raditi na prevenciji i na najnižem nivou u okviru privrednih i društvenih subjekata, a kako najveći broj izvršilaca kompjuterskog kriminala radi na poslovima veznim za informacione sisteme, potrebno je veliku pažnju posvetiti samom odabiru ličnosti koja će raditi na takvim poslovima. Fizičkim merama potrebno je zaštiti informacione sisteme od slučajnih oštećenja kompjuterske opreme, ali i od namernih oštećenja i neovlašćenih upada u prostorije u kojima se nalaze informacioni sistemi. Softverske mere zaštite treba da su usmerene ka sprečavanju neovlašćenog upada u informacioni sistem preko interneta i preko pristupnih jedinica unutra informacionog sistema. Što su važniji podaci koji se čuvaju u informacionom sistemu, to mere softverske zašite moraju biti veće.

Činjenica da je kompjuterski kriminalitet u sve većem porastu ukazuje na potrebu da savremeno društvo stalno usavršava mehanizme borbe protiv ove vrste kriminaliteta i to ne samo preventivnim merama već i kroz efikasnije otkrivanje i procesuiranje izvršenih krivičnih dela, kako bi se posredno preventivno uticalo na potencijalne izvršioce ovih dela, sve ove mere treba preduzeti organizovno,kontinuirano, sistematski i kao deo šire međunarodne saradnje bez koje nema većeg uspeha.

Literatura

1. Aleksić Živojin , Škulić Milan: *Kriminalistika* - udžbenik, Beograd, 2004, godina
2. Babić Vladica *Kompjuterski kriminal: metodologije kriminalističkih istraživanja, razjašnjavanja i suzbijanja kompjuterskog kriminaliteta* , Sarajevo, 2009.
3. Backović Jakša, Stamenković Branko,Pavličić V.Adis, Paunović Bojana, *Viskotehnološki kriminal*, Podorica, 2014.
4. Bećirić Denis, *Visoko tehnološki kriminal*, članak - COBISS.SR-ID 139137036 ;2005. godina
5. Budimlić Muhamed, Puharić Predrag, *Kompjuterski kriminalitet – kriminološki, krivičnopravni, kriminalistički i sigurnosni aspekt*, Fakultet za kriminalistiku, kriminologiju i sigurnosne studije Sarajevo 2009.
6. Cetinić Marinka: *Kompjuterska krivična dela i pojavni oblici*, - članak ;Časopis Pravni život,broj 10, 1998 god.
7. Cvetković Zoran, *Kompjuterski kriminal – članak* COBISS.SR-ID92382466, 2011 god.
8. Čisar Petar, *Sistem za detekciju upada u mrežnu infrastrukturu* ; članak COBISS.SR-ID 198387468, 2013
9. Ćirović Danijela, Janković Nebojša, Lađević Milan, Cyber podzemlje u Srbiji - članak Reporter 16.11.2005.god
10. Dimovski Darko, *Kompjuterski kriminalitet*, članak – Niš. 2010 godina
11. Đurđić Vojislav i Jovašević Dragan – *Krivično pravo - udžbenik (posebni deo),* Beograd , 2006.
12. Đurđić Vojislav– *Krivično procesno pravo - udžbenik (posebni deo*) , Niš , 2007.
13. Đurđić Vojislav i Stevanović Čedomoir– *Krivično procesno pravo – udžbenik* (opšti deo) , Niš , 2007.
14. Feješ Ištvan: *Kompjuterski kriminalitet – kriminalitet budućnosti, izazov sadašnjosti* – izlaganje na konferenciji COBISS.SR-ID 159876620,2000 godina
15. Ignjatović Đorđe: *Pojmovno određenje kompjuterskog kriminala* - članak, Beograd, 1991.
16. Jovašević Dragan, Hašimbegović Tarik, Krivičnopravna zaštita računarskih podataka, Pravni informator br.6, 2003.god.
17. Jovičić Dragomir, Bošković Mićo, Kriminalistika metodika , Viša škola unutrašnjih poslova, Banja Luka 2002.godine
18. Komlen-Nikolić Lidija,Suzbijanje visokotehnološkog kriminala;Udruženje javnih tužilaca i zamenika javnih tužilaca Srbije, Beograd 2010
19. Konstantinović-Vilić Slobodanka, Nikolić-Ristanović Vesna: *Kriminologija - udžbenik*, Niš, 2003. godina
20. Lazarević Ljubiša, *Komentar Zakonika o krivičnom postupku* - knjiga; Beograd , 2011.
21. Lazarević Slobodan, *Hakeri*, Knjiga-komerc, Beograd 2000 .godina
22. Matijašević Jelena: *Krivičnopravna regulativa računarskog kriminaliteta* , Pravni fakultet za privredu i pravosuđe,Novi sad 2013
23. Milosavljević Milan, Grubor Gojko: I*straga kompjuterskog kriminala : metodološko-tehnološke osnove*; Beograd : Univerzitet Singidunum, 2009 Mirjana Drakulić: *Osnovi kompjuterskog prava* , Društvo operacionih istraživača Jugoslavije - DOPIS, (Beograd : Udruženje Nauka i društvo Srbije) 1996. god
24. Multidonatorski poverenički fond za podršku sektoru pravosuđa u Srbiji *-Funkcionalna analiza pravosuđa u Srbiji*, Beograd, 2014.godine

25. OEBS,*Visokotehnološki criminal - Praktični vodič kroz savremeno krivično pravo i primjeri iz prakse*", Misija OEBS-a u Crnoj Gori, Podgorica, 2014.godine.
26. Petrović Slobodan, *Kompjuterski kriminal*; Ministarstvo unutrašnjih poslova Republike Srbije : Uredništvo časopisa"Bezbednost" i lista "Policajac",Beograd 2000.godina,
27. Prlja Dragan, Reljanović Mario, Ivanović Zvonimir, *Krivična dela visokotehnološkog kriminala*, Beograd, 2011.
28. Putnik Nenad - *Sajber prostor i bezbednosni izazovi* – stručna monografija, , Beograd, 2009.Ranđelović Dragan, *Visokotehnološki kriminal*, Kriminalističko policijska akademija, Beograd 2013.godina
29. Ranđelović Dragan, *Visokotehnološki kriminal*, Kriminalističko policijska akademija, Beograd 2013.godina
30. Reljanović Mario; *Visokotehnološki kriminal* : pojam, regulativa, iskustva; članak - COBISS.SR-ID 147976972 ; 2007
31. Simonović Branislav,*Kriminalistika* - udžbenik, Pravni fakultet u Kragujevcu, Kragujevac, 2004. godina
32. Spasić Vidoje,*Aktuelna pitanja u oblasti sajber kriminala* –članak, Bilten sudske prakse Vrhovnog suda Republike Srbije broj. 1/2006, Beograd
33. Šarkić Nebojša Šarkić, Prlja Dragan, Damjanović Katarina, Marić Vladimir ,Živković Vesna, Vodinelić Vladimir, Mrvić-Petrović Nataša: *Pravo informacionih tehnologija*, Beograd, 2011.
34. Urošević Vladimir,*Nigerijska prevara u Republici Srbiji* ,Bezbednost – časopis Ministarstva unutrašnjih poslova Republike Srbije, Br. 3/2009, Godina LI, Beograd.
35. Urošević Vladimir,Uljanov Sergej, Ivanović Zvonimir- *Mač World Wide Webu : Izazovi visokotehnološkog kriminala*; ISBN 978-86-85445-19-4, Beograd, 2012
36. Vasić Dušan: *Zakonska zaštita elektronskih informacija i komunikacija u Srbiji : kritički osvrt na stepen normativne uređenost*i, članak - COBISS.SR-ID 513043388, 2008.
37. Vuletić Dejan, *Bezbednost u sajber prostoru* - knjiga,COBISS.SR-ID 192329996, Beograd, 2012.
38. Vuletić Igor : Primjenjivost tradicionalnih kaznenopravnih koncepata na računalni kriminal; članak - COBISS.SR-ID 516730556 ;2014.godina
39. Vodinelić Vladimir, *Metodika otkrivanja, dokazivanja i razjašnjenja računarskog kriminaliteta*,Priručnik br.4/90 Zagreb, 1990
40. Zirojević Mina, *Upotreba novih informatičkih i komunikacionih medija u svrhe terorizma* – Revija za bezbednost ; Centar za bezbednosne studije, Godina II, br. 11/2008, Beograd.
41. Živkovski Igor: Otkrivanje i razjašnjavanje kompjuterskog kriminaliteta ;članak COBISS.SR-ID 2012.godina.

Pravni izvori

1. Konvencija o visokotehnološkom kriminalu, Saveta Evrope, Budimprešta, 2001.god
2. Krivični zakonik Republike Srbije, *Sl. glasnik RS", br. 85/2005, 88/2005 - ispr., 107/2005 - ispr., 72/2009, 111/2009, 121/2012, 104/2013 i 108/2014*
3. Nacionalna Strategija za reformu pravosuđa za period od 2013-2018 godine koju je Narodna skupština Republike Srbije usvojila 1. jula 2013. godine na sednici Sedmog Vanrednog zasedanja, *Službeni glasnik Republike Srbije broj 9/10*
4. Pravilnik o upravi u Javnom tužilaštvu,*Službeni glasnik RS", br.110/2009,87/2010 i 5/2012*)

5. Zakon o autorskim i srodnim pravima.,*Sl. glasnik RS", br. 104/2009, 99/2011 i 119/2012*
6. Zakon o organizaciji i nadleznosti drzavnih organa zaborbu protiv visokotehnoloskog kriminala, *Sl. glasnik RS", br. 61/2005 i 104/2009*.
7. Zakon o elektronskoj trgovini,*Sl.glasnik RS br 41/2009 i 95/2013*
8. Zakon o potvrđivanju Konvencije o visokotehnološkom kriminalu,*Sl. glasniku RS",br. 19. mart 2009.*
9. Zakon o krivičnom postupku Republike Srbije *Sl. glasnik RS", br. 72/2011, 101/2011, 121/2012, 32/2013, 45/2013 i 55/2014*
10. Zakon o potvrđivanju dodatnog Protokola uz Konvencije o visokotehnološkom kriminalu koji se odnosi na inkriminaciju dela rasističke i ksenofobične prirode koja su izvršena preko računarskih sistema ,*Sl. glasniku RS", Međunarodni ugovori br. 19. 2009*.
11. Zakon o potvrđivanju Sporazuma o strateškoj saradnji između Republike Srbije i Evropola. *Sl. glasniku RS", br. 38 od 25. maja 2009.*
12. Zakona o Vojnobezbednosnoj agenciji i Vojnoobaveštajnoj agenciji, *Sl. glasnik RS", br. 88/2009, 55/2012 - odluka US i 17/2013*

Inostrani pravni izvori

1. DIRECTIVE 2013/40/EU OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA
2. Direktiva 2006/24 Evropskog parlamenta i Saveta o čuvanju podataka koji su dobijeni ili obrađeni prilikom pružanja javno dostupnih usluga elektronske komunikacije ili javnih komunikacionih mreža od 15.3.2006.godine
3. THE EUROPEAN COUNCIL, Council Directive od 14. may 1991 on the Legal Protection of Computer Programs – Directive 91/250/EEC OJ no L122/42
4. THE EUROPEAN PARLIAMENT AND OF THE COUNCIL COUNCIL ,DIRECTIVE 2011/92/EU OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL COUNCIL of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA
5. THE EUROPEAN PARLIAMENT AND OF THE COUNCIL COUNCIL ,DIRECTIVE 2009/136/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws
6. THE COUNCIL OF THE EUROPEAN UNION Framework Decision of 28 May 2001 on combating fraud and counterfeiting of non-cash means of payment (2001/413/JHA)

Strani izvori

1. Alisdair A. Gillespie - Cybercrime: Key Issues and Debates ISBN-13: 978-0415712200Florence, Kentucky, 2015.god
2. Betts Mitch. Portrait of a hacker - članak ; Časopis Computer world , 25.novembar 1985 god.
3. Bruce Sterling ; The Hacker Crackdown: Law and Disorder on the Electronic Frontier-knjiga, Bantam Books, USA; 1992.god

4. *Center for Strategic and International Studies*, Net Losses: Estimating the Global Cost of Cybercrime Economic impact of cybercrime II ; Santa Clara USA ,2014.
5. Douglas E. Campbell – *Computer Terrorism - knjiga* - Syneca Research Group, Inc.- Washington USA, 2011
6. Douglas Thomas; *Hacker Culture*; University of Minnesota Press, USA, Minneapolis, USA, 2002
7. Durham , Clifford, Ralph D. ; *Cybercrime : the investigation, prosecution and defense of a computer-related crime* ; North Carolina : Carolina Academic Press, Durham, 2006. god.
8. European Commission, *Digital agenda for Europe*, European Commission Directorate-General for Communication Citizens information ; Luxembourg: Publications Office of the European Union, 2014
9. Eoghan Casey, *Digital Evidence and Computer Crime : forensic science, computers and the Internet* , Academic Press, Burlington USA 2011.god
10. Europol, *European Cybercrime Centre (EC3); The European Financial Coalition against Commercial Sexual Exploitation of Children Online*, European Cybercrime Centre (EC3) – Hague, 2015
11. Europol – *"Public information version - Situation Report-Payment Card Fraud* ,Publications Office of the European Union, Luxembourg: 2012.god
12. Franklin Clark, Ken Diliberto, *Investigating computer crime*, Boca Raton, Florida USA .1996
13. Fredesvinda Insa; *The admissibility of electronic evidence in Court – Fighting against high-tech crime* - članak; Journal of digital forensic practice volume I, issue 4; 2006.god
14. Marco Gercke und Phillip W. Brunst *; Praxishandbuch Internetstrafrecht* - kniga Stuttgart: Kohlhammer, Stuttgart 2009.
15. Interpol ,Annual report 2014 – INTERPOL, INTERPOL General Secretariat Lyon , France,2015
16. Interpol,Supporting digital crime investigations – INTERPOL, INTERPOL General General Secretariat Lyon , France,2015
17. John, Muncie , Eugene. McLaughin – *The problem of Crime -knjiga– Second Edition* Open University and SAGE Publications Ltd, London, 2001.
18. Janusz Piekalkiewicz ;*World history of espionage:: Agents, systems, operations*, National Intelligence Book Center, Washington USA 1998
19. Kyung-shick Choi; *Risk Factors in Computer Crime*; El Paso USA, LFB Scholarly Publishing LLC 2010.
20. Parker B. Donn, *Fighting computer crime*, New York (USA)1983.god
21. Peter J. Toren,,*Intellectual Property and Computer Crimes (Intellectual Property usiness Crimes Series*, New York USA, 2003
22. Raoul Chiesa , Stefania Ducci, Silvio Ciappi - *Profiling Hackers: The Science of Criminal Profiling as Applied to the World of Hacking*, United States 2008.god.
23. Stephen Mason ; International electronic evidence - knjiga; British Institute of International and Comparative Law, London UK ; 2008. god.
24. Peter Stephenson; *Investigating computer-related crime*; Boca Raton, Florida USA ,CRC Press, 2000

Elektronski izvori

1. Aaron Brown, *Windows 10: Pirated operating systems will NOT get free upgrade,* preuzeto dana 10.08.2015. http://www.express.co.uk/life-style/science-technology/578050/Windows-10-pirates-pirated-operating-systems-free-upgrade-genuine-non-genuine-explained
2. Alexander Abdo, Patrick Toomey, *The NSA is turning the internet into a total surveillance system*, preuzeto dana 0.08.2015.godine http://www.theguardian.com/commentisfree/2013/aug/11/nsa-internet-surveillance-email
3. Associated Press, Israel to pay students to defend it onlinepreuzeto dana 02.08.2015. godine http://www.usatoday.com/story/news/world/2013/08/14/israel-students-social-media/2651715/
4. American Chemical Society, Dow Offices Vandalized, preuzeto dana 01.08.2015.godine http://pubs.acs.org/doi/abs/10.1021/cen-v047n048.p015a
5. Beta, Ostavka visoke zvaničnice SAD zbog krađe podataka 21,5 miliona ljudi ,preuzeto dana 10.08.2015.godine, http://www.blic.rs/Vesti/Svet/574539/Ostavka-visoke-zvanicnice-SAD-zbog-kradje-podataka-215-miliona-ljudi
6. Brian Harvey, *Computer Hacking and Ethics*, https://www.cs.berkeley.edu/~bh/hackers.html preuzeto dana 09.08.2015. godine
7. Council of Europe, *Action against cyber crime,* preuzeto dana 10.08.2015.godine http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy%20project%20balkan/Strategic_priorities_conference/2467_Strategic_Priorities_V16_SRB_final_adopted.pdf.
8. Council of Europe, *Convention for the Protection of Human Rights and Fundamental Freedoms* http://conventions.coe.int/treaty/en/Treaties/Html/005.htm preuzeto dana 09.08.2015.godine
9. Dario Kuntić, *Privreda SAD-a godišnje gubi više od 200 mlrd. dolara zbog piratstva* preuzeto dana 05.06.2015.godine http://www.poslovni.hr/hrvatska/privreda-sad-a-godisnje-gubi-vise-od-200-mlrd-dolara-zbog-piratstva-52710
10. Delegacijae Evropske Unije u Republici Srbiji i Kancelarija za saradnju sa civilnim društvom Vlade Republike Srbije, Monitoring rada sudova u krivičnim postupcima preuzeto dana 10. 07. 2015. godine http://www.mc.rs/upload/documents/NAJAVE/2014/CLJP/05-07-14_CLJP_Monitoring-rada-sudova-u-krivicnim-postupcima.pdf
11. Ellen Nakashima, *U.S. developing sanctions against China over cyberthefts,* preuzeto dana 30.08.2015.godine sanctions-against-china-over-cyberespionage/2015/08/30/9b2910aa-480b-11e5-8ab4-c73967a143d3_story.html
12. Eur Lex, *Communication from the Commission to the Council, the European Parliament and the Economic and Social Committee concerning a strategy for the Customs Union /**
13. *COM/2001/0051 final* */ preuzeto 20.07.2015. godine. http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2001:0051:FIN
14. Eur Lex, *Direktiva 2006/24/EZ Europskog parlamenta i Vijeća od 15. ožujka 2006. o zadržavanju podataka dobivenih ili obrađenih u vezi s pružanjem javno dostupnih elektroničkih komunikacijskih usluga ili javnih komunikacijskih mreža i o izmjeni Direktive 2002/58/EZ*, preuzeto dana 09.08.2015.godine http://eur-lex.europa.eu/legal-content/HR/TXT/?uri=celex:32006L0024

15. Europol, International police action leads to rescue of 22 month old romanian sex abuse victim, preuzeto dana 30.08.2015, https://www.europol.europa.eu/content/international-police-action-leads-rescue-22-month-old-romanian-sex-abuse-victim
16. European Financial coalition,*INHOPE 2012,Facts, Figures and Trends*,preuzeto dana 30.10.2015.god,http://www.europeanfinancialcoalition.eu/private10/images/document/2.pdf
17. Eric Bangeman, Child porn case shows that an open WiFi network is no defense, preuzeto dana 10.08.2015. godine http://arstechnica.com/tech-policy/2007/04/child-porn-case-shows-that-an-open-wifi-network-is-no-defense/
18. Joel D. Cameron, *Stasi*, preuzeto 20.07.2015.godine http://www.britannica.com/topic/Stasi
19. JOHN MARKOFF and DAVID E. SANGER, *In a Computer Worm, a Possible Biblical Clue*, preuzeto dana 01.08.2015. godine, http://www.nytimes.com/2010/09/30/world/middleeast/30worm.html?_r=0
20. John Dowell, *Technology Invading Privacy*, preuzeto dana 25.07.2015.godine https://www.msu.edu/~casechri/135/Chp3paper2.html
21. Kaspersky ,Malware Classifications http://www.kaspersky.com/internet-security-center/threats/malware-classifications ,preuzeto dana 01.08.2015. godine
22. Nepoznat autor, Malvare, preuzeto dana 01.08.2015.godine http://techterms.com/definition/malware
23. Nepoznat autor, Urban dictionary, preuzeto dana 10.07.2015. godine, http://www.urbandictionary.com/define.php?term=leet+speak
24. Nepoznat autor, Urban dictionary, 02.08.2015.godine http://www.urbandictionary.com/define.php?term=Torrent
25. Martin Evans , *Hackers steal £650 million in world's biggest bank raid*,preuzeto dana 10.08.2015.godine http://www.telegraph.co.uk/news/uknews/crime/11414191/Hackers-steal-650-million-in-worlds-biggest-bank-raid.html
26. Pamela Engel, *ISIS has mastered a crucial recruiting tactic no terrorist group has ever conquered*, preuzeto dana 10.10.2015. godine http://www.businessinsider.com/isis-is-revolutionizing-international-terrorism-2015-5
27. PBS NEWS, *Daily Download: Obama Spent 10 Times as Much on Social Media as Romney*,preuzeto dana 02.08.2015. godine http://www.pbs.org/newshour/bb/media-july-dec12-download_11-16/
28. Radio Televizija Republike Srpske, Informatički svjetski rat- digitalno naoružavanje http://lat.rtrs.tv/vijesti/vijest.php?id=135279 preuzeto dana 02.06.2015.godine
29. RT Vojvodine, Milionska krađa lozinki u Nemačkoj ,preuzeto dana 10.08.2015.godine http://www.rtv.rs/sr_lat/evropa/milionska-kradja-lozinki-u-nemacko_454999.html
30. RTS, Uhapšen zbog računarske prevare, preuzeto dana 02.08.2015. godine http://www.rts.rs/page/stories/sr/story/135/Hronika/857032/Uhap%C5%A1en+zbog+ra%C4%8Dunarske+prevare.html
31. Sharon Gaudin, *Medco Sys Admin Pleads Guilty To Computer Sabotage*,preuzeto dana 02.08.2015. godine http://www.informationweek.com/medco-sys-admin-pleads-guilty-to-computer-sabotage/d/d-id/1059395?
32. Stefan Despotović, *Srbija zemlja poljoprivrednika i informatičara*,preuzeto dana 04.06.2015. godine http://www.politika.rs/rubrike/Tema-nedelje/Izvoz-softvera-sve-unosniji/Srbija-zemlja-poljoprivrednika-i-informaticara.lt.html

33. Stefan Despotović, *Piraterija odnosi milijarde dolara*, preuzeto dana 05.06.2015.godine http://www.politika.rs/rubrike/Ekonomija/Piraterija-odnosi-milijarde-dolara.lt.html
34. Tal Kopan,White House readies cyber sanctions against China ahead of state visit , preuzeto dana 31.08.2015.godine http://edition.cnn.com/2015/08/31/politics/china-sanctions-cybersecurity-president-obama/
35. Tanjug, Na Filipinima zbog dečje pornografije uhapšeno 11 ljudipreuzeto 01.08.2015.godine, www.blic.rs/Vesti/Svet/438405/Na-Filipinima-zbog-decje-pornografije-uhapseno-11-ljudi .
36. Tanjug, *Prva krivična prijava za unošenje računarskog virusa u Srbiji* ,preuzeto dana 01.08.2015. godine, http://www.blic.rs/Vesti/Hronika/188170/Prva-krivicna-prijava-za-unosenje-racunarskog-virusa-u-Srbiji
37. Yana Lyushnevskaya, Ukraine's new online army in media war with Russia, preuzeto dana 01.08.2015.godine ,http://www.bbc.co.uk/monitoring/ukraines-new-online-army-in-media-war-with-russia
38. Warwick Ashford, *Police arrest 130 in global anti-cyber fraud operation*, preuzeto dana 30.08.2015. godine http://www.computerweekly.com/news/4500248925/Police-arrest-130-in-global-anti-cyber-fraud-operation

Ostali elektronski izvori

1. http://www.mup.gov.rs/
2. http://www.paragraf.rs/
3. http://lat.rtrs.tv
4. https://www.europol.europa.eu/
5. http://www.coe.int/web/portal/home
6. http://secitsecurity.com/
7. http://www.telekomunikacije.rs/
8. http://pravoikt.org/
9. http://www.datasolutions.rs/
10. http://www.virtualglobaltaskforce.com/
11. http://home.mcafee.com/?ctst=1
12. http://www.ucd.ie/cci/
13. http://www.webopedia.com

Sažetak master rada i ključne reči

Neprestani i nagli razvoj informacione tehnologije je pored svih prednosti koje je doneo čovečanstvu u svim oblastima života, doveo i do nastanka novog oblika kriminalnog ponašanja, odnosno do nastanka kompjuterskog kriminaliteta. Ovaj oblik kriminaliteta beleži ekspanziju kao nijedan do sada poznati oblik kriminaliteta. Sve učestalije zloupotrebe kompjutera i informacione tehnologije u Republici Srbiji poslužile su kao dodatan podstrek pri odabiru ove teme i izrade ovog master rada. Kompjuterski kriminalitet je kao negativna društvena pojava u ovom master radu sagledan i sa krimiološke i krivičnopravne strane radi dobijanja što bolje analize i potupnije slike ovog fenemona. Master rad se uključujući uvodna i zaključna razmatranja sastoji iz četrnaest celina.

Naslov master rada je "Kompjuterski kriminalitet".U delu rada kojim se obrađuje pojam kompjuterskog kriminaliteta, date su najrasprostranjenije definicije ovog fenomena, sa naglaskom da i dalje ne postoji jedinstvena i opšte priznata definicija među autorima. Rad dalje obrađuje kompjuterski kriminalitet analizirajući njegove osnovne karakteristike, kao i način upotrebe kompjutera i informacione tehnologije pri ovim kriminalnim aktivnostima, uz detaljnu obradu ciljeva i posledica ovog oblika kriminaliteta. Poseban deo rada usmeren je na kriminološku obradu vrsta počinilaca uz navođenje njihovih odlika.

Znatan deo rada posvećen je i međunarodnim dokumentima kojima je regulisan kompjuterski kriminalitet, odnosno na Konvenciju o visokotehnološkom kriminalu Saveta Evrope sa dodatnim protokolom, koja je ujedno i najznačajni pravni instrument na ovom polju, i na Direktive Evropske unije koje predstavljaju rezultat saradnje država EU na smanjivanju razlika u svojim zakonodavstvima u cilju suzbijanja i suprostavljanja kompjuterskom kriminalitetu.

U glavi VII predstavljenji su Interpol i Europol kao najznačanje međunarodne policijske organizacije i njihov dosadašnji rad u suzbijanju kompjuterskog kriminaliteta. Institucionalni okvir suprotstavljanja visokotehnološkom kriminalu u Republici Srbiji obrađen je u glavi VII koja predstavlja jedan od najznačajnih delova rada. Glava IX obrađuje sve specičnosti gonjenja za krivična dela visokotehnološkog kriminala, jer se ova dela izuzetno teško procesuiraju i istražuju, pre svega jer se radi o relativno novoj pojavi, sa transnacionalnim implikacijama, a i države su tek u protekloj deceniji prilagodile svoja zakonodavstva, tako da je u ovoj glavi obrađen niz problema do kojih dolazi u praksi. Centralni deo master rada razmatra kompjuterska

krivična dela u Krivičnom zakoniku Republike Srbije uz njihovu sveobuhvatnu analizu i navođenje primera iz prakse.

Najopširniji deo rada posvećen je kriminološkoj tipologiji kompjuterskog kriminaliteta u ovom delu obrađena su najučestalija krivična dela koja kriminolozi u svojim podelama pripisuju kompjuterskom kriminalitetu.

Za potrebe izrade master rada sprovedeno je i istraživanje u okviru Posebnog odeljenja Višeg javnog tužilaštva u Beogradu, osnovni cilj ovog istraživanja je da se na osnovu prikupljenih podataka o broju predmeta i počinilaca, dođe do saznanja o obimu, strukturi i dinamici krivičnih dela visokotehnološkog kriminala u Republici Srbiji a istraživanjem su potvrđene sledeće hipoteze:

1. da se svake godine beleži rast počinjenih krivičnih dela protiv bezbednosti računarskih podataka ;
2. da su krivična dela protiv bezbednosti računarskih podataka , izvršena uglavnom od strane pojedinaca.
3. da broj počinilaca raste iz godine u godinu.

Ključne reči master rada su kriminalitet, krivično delo, kompjuteri, informaciona tehnologija, hakeri, kompjuterski virusi, tužilaštvo.

The Abstract of the Master's Thesis and the Key Words

Despite numerous gifts that incessant and abrupt development in IT field has bestowed upon humanity, it has also brought about the inception of cybercrime. The expansion of this particular type of crime has surpassed that of all others thus far. The frequency of computer and IT misuse in the Republic of Serbia has served as an additional stimulus for choosing this topic as a master's thesis. In this master's thesis, cybercrime as a negative social phenomenon has been analyzed from the point of view of both criminology and criminal justice, and, as a result, a great insight into the issue has been gained. This master's thesis will consist of 14 chapters, including the introductory and concluding considerations.

Title master's work is "Computer criminality". In the section in which the notion of cybercrime is being dealt with, one shall find the most widely accepted definitions of this phenomenon, with an emphasis on the fact that there is still no single, generally accepted definition among the authors. This thesis will further deal with cybercrime by analyzing its main characteristics, as well as the methods in which computers and IT are used during such criminal

activities, while focusing at the same time on the analysis of the goals and consequences of this type of crime. A different section of this thesis will focus on the criminological analysis of the types of perpetrators, while also stating their characteristics.

A significant portion of this thesis shall be dedicated to the international documents that regulate cybercrime, i.e. The Council of Europe Convention on Cybercrime with additional protocol, which is the most significant legal instrument in this field, as well as on the EU Directives, which represent the results of the EU member states' collaboration on decrease in legislation differences in view of suppressing and opposing cybercrime.

In chapter VII, Interpol and Europol will be introduced as the most important international police forces; in addition, this chapter will discuss their achievements in suppressing cybercrime thus far. Chapter VIII will deal with the institutional framework of opposing high-tech crime in the Republic of Serbia. Chapter IX will focus on the specifications of the prosecutions for high-tech criminal offenses, as these deeds are usually not easily processed and investigated, mostly due to their being a relatively new phenomenon with transnational implications, and also, due to the fact that states have only adjusted their legislations during the last decade, which is why this chapter also deals with a number of problems that are experienced in real life. The central part of this thesis will, in addition to cybercrime offenses mentioned in Criminal Code of the Republic of Serbia, deal with their comprehensive analysis and real-life examples.

The greatest portion of this thesis is dedicated to the criminological typology of cyber criminality. In this part, the most frequent criminal offenses ascribed to cybercrime by criminologists are analyzed.

For the purpose of this thesis, a research has been conducted within the Special Division of the High Prosecutor's Office in Belgrade. The main goal of this research was to understand the extent, structure and dynamics of high-tech criminal offenses, based on the gathered information on the number of cases and perpetrators. As a result of the research, the following hypotheses have been corroborated:

1. That, every year, there is an increase in the number of committed offenses against computer data security;
2. That criminal offenses against data security have mostly been committed by individuals;

3. That the number of perpetrators has been increasing year after year.

In this master's thesis, the **key words** are: criminality, criminal offense, computers, IT, hackers, computer viruses and prosecutor's office.

Biografija studenta

Student - kandidat za odbranu master rada, Miloš Vidojković rođen je dvadeset i petog novembra 1988. godine u Ljubljani, Republika Slovenija.

Osnovnu školu "Ljupče Nikolić", kao i prirodno-matematički smer Aleksinačke gimnazije završio je u Aleksincu. Osnovne akademske studije na Pravnom fakultetu, Univerziteta u Nišu, upisao je školske 2007/2008 godine i iste završio 16. aprila 2014. godine i time stekao zvanje diplomirani pravnik. Za vreme studija bio je aktivni član više studentskih i omladinskih organizacija i učesnik više seminara i konferencija od kojih se izdvaja IV ELSA Ex-Yu Konferencija pod nazivom "Građanska neposlušnost kao jedno od osnovnih ljudskih prava" održana u Budvi 2012. godine.

Iste godine po diplomiranju upisao je master studije na Pravnom fakultetu, Univerziteta u Nišu, studijski smer "Pravo unutrašnjih poslova".

U periodu od jula 2014. godine do maja 2015. godine radio je kao pomoćnik javnog izvršitelja Zorana Bogdanovića, imenovanog za područje Privrednog suda u Nišu i Višeg suda u Nišu. Od maja 2015. godine pa do danas je upisan u Imenik advokatskih pripravnika Advokatske komore u Nišu, kao pripravnik advokata Olivera B. Injca iz Niša.

Tečno govori engleski jezik.