Računalniška kriminaliteta, mit o altruizmu

Miloš Lukman

Povzetek:

Namen prispevka:
Pri obravnavi računalniške kriminalitete se je potrebno zavedati posebnosti kiberprostora in njegovega vpliva na vedenje posameznikov. Na prvi pogled fizična in virtualna – kibernetska, kriminaliteta nimata veliko skupnega. Razlikujeta se po načinih storitve, storilcem ni potrebno imeti fizičnega stika z žrtvijo, prav tako so za vsako razvili svoje tehnike preiskovanja. Vendar so bili storilci kibernetske kriminalitete, v nasprotju s storilci iz fizičnega sveta, dolgo časa prikazani kot novodobni Robini Hoodi, tehnološki aktivisti, ki se borijo za pravičnost in so pripravljeni nesebično pomagati drugim. Statistična primerjava storilcev obeh kriminalitet pa osvetljuje storilce iz kibernetskega okolja v popolnoma drugačni luči. Izvedena je primerjava po starosti, spolu, izobrazbi, motivih, državljanstvu ter zaposlitvenem statusu domnevnih storilcev. V prispevku bom skušal osvetliti razliko med hekerji in storilci računalniške kriminalitete ter poiskati osnovne vzroke za deviantnost v kibernetskem prostoru.

Metodologija:
Primerjalna opisna metoda, deskriptivna statistika

Ugotovitve:
Večina opravljenih raziskav, ki obravnavajo storilce računalniške kriminalitete, predvsem populacijo hekerjev, navaja starost storilcev med štirinajstimi in petindvajsetimi leti. Obdelava statističnih podatkov pri nas izkazuje povprečno vrednost storilcev računalniškega kriminala 31,5 let. Če za statistično obdelavo uporabimo zgolj izrazito hekerska kazniva dejanja, je povprečna vrednost storilcev 27,7 let. Ostali primerjalni atributi ne izkazujejo bistvene razlike med storilci fizične in virtualne kriminalitete. Vsekakor izziv in znanje nista temeljni vodili kibernetskih storilcev, kot bi pričakovali po rezultatih opravljenih raziskav.

Omejitve/uporabnost raziskave:
Statistični rezultati ne predstavljajo absolutnega sodila o lastnostih storilcev kibernetskega kriminala, saj moramo na področju računalniške kriminalitete upoštevati veliko polje neidentificiranih kaznivih dejanj ter izredno selektivno prijavo zaznanih kaznivih dejanj s strani oškodovancev. Nekateri avtorji navajajo na en prijavljen incident celo 4000 poizkusov napadov na informacijske sisteme. Rezultati izkazujejo tudi veliko mero razpršenosti oz. variabilnosti, pa tudi število statističnih enot je premajhno, da bi rezultate lahko obravnavali kot popolnoma relevantne.

Praktična uporabnost:
Napovedovanje varnostnih pojavov na področju informacijske tehnologije je zaradi hitrega razvoja izredno težavno, edina stalnica je le človeška narava z vsemi svojimi dobrimi in slabimi lastnostmi. Zaradi tega bi bilo potrebno preusmeriti tehnicistično obravnavanje informacijske varnosti v človeški dejavnik. Veliko pozornosti bi morali usmeriti tudi v ozaveščanje mladih in jih pripraviti na odgovorno vedenje v navideznem svetu svetovnega spleta.

Izvirnost/pomembnost prispevka:
Prispevek podaja pregled statističnih podatkov domnevnih storilcev računalniške kriminalitete v primerjavi z izbranimi kaznivimi dejani storilcev fizične kriminalite.

Ključne besede: kriminaliteta, kibernetski prostor, statistična obdelava , informacijska varnost

1 UVOD

Kiberprostor predstavlja novo življenjsko dimenzijo, ki vpliva na človekovo duševno delovanje, vedenje in celotno osebnost. Hkrati ustvarja svojevrstno okolje za storitev kaznivih dejanj. Pri obravnavi računalniške kriminalitete se je potrebno zavedati posebnosti samega kiberprostora in njegovega vpliva na vedenje posameznikov. Na prvi pogled fizična in virtualna, kibernetska kriminaliteta, nimata veliko skupnega. Razlikujeta se po načinih storitve, storilcem ni potrebno imeti fizičnega stika z žrtvijo, prav tako so za vsako razvili svoje tehnike preiskovanja. Storilci kibernetske kriminalitete so bili, v nasprotju s storilci iz fizičnega sveta, dolgo časa prikazani kot novodobni Robini Hoodi, tehnološki aktivisti, ki se borijo za pravičnost in so pripravljeni nesebično pomagati drugim. Statistična primerjava storilcev obeh kriminalitet, pa osvetljuje storilce iz kibernetskega okolja v popolnoma drugačni luči. Karta o pravičnosti in moralnosti je izigrana. Mit o njihovem altruizmu je padel. Čas je, da se pričnemo zavedati, da se storilci računalniške kriminalitete ne razlikujejo od storilcev iz realnega sveta.

2 RAČUNALNIŠKA KRIMINALITETA

Računalniški kriminal ne predstavljajo le vdori v računalniške sisteme, temveč gre za izredno heterogeno skupino kaznivih dejanj, v katero so vključene tudi druge oblike kriminala: ponarejanje in goljufije, različne oblike kršitev avtorskih pravic, otroška pornografija, v nekaterih državah tudi vse oblike rasističnih in ksenofobičnih dejanj, vključno s sovražnim govorom. Posamezne pojavne oblike se med seboj prepletajo, včasih pa je težko določiti pravi motiv storilca. Slednje velja predvsem za računalniške vdore, pri katerih se je storilec le sprehodil skozi sistem. Posamezne oblike kaznivih dejanj so bile znane že pred prihodom računalnikov, kriminalci so zgolj izkoristili prednosti, ki jih prinaša informacijska doba, oblikovala pa so se tudi nova kazniva dejanja, katerih razvoj je pogojen z razvojem informacijske tehnologije. Dejansko je inkriminacija kaznivih dejanj vselej korak za storilci kibernetske kriminalitete. Geografska nedoločljivost interneta, konstantno dinamično spreminjanje spletnih vsebin in storitev ter neusklajena kazenska zakonodaja na področju kibernetske kriminalitete, predstavljajo dodatne ovire v boju proti kibernetskemu kriminalu. Grožnje iz interneta so usmerjene tako proti državam in njihovim institucijam, kot proti posameznikom.

Eno prvih razdelitev računalniških kaznivih dejanj je podal Carter (Carter, 1995). Opredeljuje štiri osnovne vrste računalniške kriminalitete: računalnik kot cilj napada, računalnik kot sredstvo, računalnik kot slučajno sredstvo ter kazniva dejanja v povezavi z razširjenostjo računalniške tehnologije. Večina sodobnih klasifikacij računalniške kriminalitete sledi njegovi razdelitvi. Podobno opredelitev kaznivih dejanj računalniške kriminalitete določa tudi evropska Konvencija o kibernetski kriminaliteti.

Tako Carter kot konvencija uvrščata v prvo skupino kazniva dejanja, pri katerih je cilj napada računalnik oz. informacijski sistem, pri čemer konvencija poimenuje skupino kot kazniva dejanja zoper zaupnost, celovitost in dostopnost računalniških podatkov in sistemov. Carterjeva opredelitev je morda v celoti nekoliko nedosledna, ker je v skupino uvrstil tudi vse napade na računalnike, vključno s krajo intelektualne lastnine, izsiljevanja na podlagi

pridobljenih različnih osebnih podatkov o žrtvi ter vse oblike tehno – vandalizma. Vdorov ne razlikuje po motivih storilcev in obravnava vse vrste enako. Kaznivo dejanje predstavlja vdor iz koristoljubja ali pa vdor, pri katerem je šlo zgolj za učenje oz. izziv napadalca. Enako je uvrstil napade, imenovane sprehodi skozi sistem, kjer storilec ne briše ali spreminja datotek v informacijskem sistemu in jih je opredelil kot kršitve lastnikove zasebnosti.

V skupino, kjer je računalnik uporabljen kot sredstvo, Carter uvršča predvsem kazniva dejanja ponarejanja in gre za podobno opredelitev kot za kazniva dejanja, ki so v evropski konvenciji o kibernetskem kriminalu uvrščena v kazniva dejanja, povezana z računalniki.

Naslednjo skupino pri Carterju predstavljajo kazniva dejanja, pri katerih računalnik ni ključen element za storitev kaznivega dejanja, je pa povezan s samo storitvijo. Do kaznivega dejanja bi prišlo tudi brez njega, vendar računalnik omogoča lažjo pot, hitrejšo obdelavo večje količine podatkov, s pomočjo informacijske tehnologije pa tudi uspešneje prikrijejo sledove svojega početja. Tipičen primer takih zločinov so kazniva dejanja v povezavi z otroško pornografijo, kjer tehnologija omogoča lažjo in hitrejšo izmenjavo inkriminiranega gradiva. Orodja za enkripcijo podatkov in anonimizacijo dodatno onemogočajo prestrezanje vsebine sporočil in odkritje izvora storilcev. Konvencija uvršča taka kazniva dejanja v skupino kaznivih dejanj povezanih s vsebino.

Carterjevo zadnjo skupino predstavljajo kazniva dejanja, ki jih vzpodbuja že sama razširjenost informacijske tehnologije. Tu gre predvsem za kršitev avtorskih pravic, kazniva dejanja pa so predvsem ponarejanje programskih produktov (piratstvo) in trgovina s ponarejeno programsko opremo. V omenjeno skupino sodijo tudi kraje računalniške opreme. Podobno konvencija razlikuje kazniva dejanja povezana s kršitvijo avtorskih in sorodnih pravic.

Pri računalniški kriminaliteti predstavlja veliko težavo napačno vrednotenje teže storjenega dejanja s strani posameznika kot tudi družbe ter obsežno temno polje neodkritih kaznivih dejanj. Ocenjujejo, da je odkrita le desetina vseh napadov na računalniške sisteme. V oceno so bili vključeni vsi napadi oz. ogrožanja sistemov za nacionalno varnost, kot kibernetske kriminalne aktivnosti ter napadi na sisteme, ki povzročajo le nizko stopnjo ogrožanj (Borchgrave, 2000). Raziskava ameriškega obrambnega ministrstva, ki je bila izvedena s serijami testov, kjer so simulirali napade na informacijske sisteme vladnih organizacij pa opozarja tudi na nizko stopnjo poročanja o zaznanih napadih. V testih so izvedli 68.000 napadov, od katerih sta bili dve tretjini uspešni, zaznanih pa je bilo le 4 odstotke uspešnih vdorov. Samo 10 odstotkov teh vdorov je bilo tudi prijavljenih (Bosworth, Kabay, 2002). Korporacije nerade prijavljajo vdore v njihove informacijske sisteme, predvsem iz bojazni pred izgubo ugleda ter dolgotrajnimi preiskovalnimi postopki, običajni uporabniki pa napade pogosto povezujejo z motnjami v delovanju strojne in programske opreme.

Fenomenologija računalniške kriminalitete je bistveno enostavnejša kot iskanje vzrokov za njen nastanek. Ne glede na lokalno zakonodajo, so splošne pojavne oblike računalniške kriminalitete: vdori v informacijske sisteme, protipravno prestrezanje, motenje računalniških sistemov in podatkov, računalniške goljufije in ponarejanje, kršitve avtorskih pravic – piratstvo, zloraba naprav ter kazniva dejanja v zvezi z otroško pornografijo.

Resnični motivi storilcev računalniške kriminalitete so, v primerjavi z deklariranimi cilji in vrednotami, usmerjeni v pridobivanje materialnih koristi. Chantler v eni izmed svojih številnih raziskav poudarja, da kar 49 odstotkov hekerjev navaja kot prvenstvene motive: izziv, znanje in zadovoljstvo (Chantler, 1996). Rezultati statistične analize (podobno tudi tuje) pa nasprotujejo tej trditvi in kot glavni cilj kibernetskih storilcev prikazujejo koristoljubje. V

nadaljevanju bodo prikazani natančnejši podatki statistične analize, ki je bila prvenstveno usmerjena v lastnosti domnevnih storilcev.

2.1 Vzroki za pojav računalniške kriminalitete

Virtualni svet se razlikuje od resničnega in ustvarja novo digitalno skupnost. Morda na prvi pogled izgledata enako, vendar nista izenačena v doseganju psiholoških kvalitet. Navidezni svet ima že vnaprej določene oblike medsebojnega komuniciranja, ki postavljajo same po sebi tudi omejen nabor možnih oblik komuniciranja. Suler poudarja, da vse oblike računalniške komunikacije ne dosegajo enakega vpliva na psihološko zaznavanje posameznika ali skupine (Suler, 2005). Med temeljne psihološke značilnosti kiberprostora sodijo: omejeno in spremenjeno zaznavanje, anonimnost posameznikov, tekstovnost izražanja, začasna narava kiberprostora, zapisovanje in sledljivost posameznikovega ravnanja, interaktivnost, nezavedanje prisotnosti družbe ter virtualnost. Določene lastnosti virtualnega prostora morda same po sebi ne bi učinkovale na spremenjeno vedenje uporabnikov svetovnega spleta, vendar lahko njihova sinergija ustvari nepričakovane učinke, ki vplivajo na deviantno vedenje. Raziskovalci deviantnega vedenja v kibernetskem svetu se v grobem delijo na tiste, ki vidijo možne vzroke v vplivih okolja, sociološke teorije, in na drugo skupino, ki iščejo vzroke predvsem v osebnostnih lastnostih, kar predstavlja temelj vseh psihološko obarvanih teorij.

Določene sociološke teorije o vzrokih za računalniški kriminal označujejo anonimnost kot enega izmed najpomembnejših faktorjev. Anonimnost na internetu predstavlja ščit, ki preprečuje povezavo resnične uporabnikove identitete s podatki, ki se izmenjujejo po omrežju. Zasebnost in anonimnost sta v medsebojni povezavi. Ob tem se nam poraja vprašanje ali je skrivanje uporabnikove identitete v internetu zaželeno, ali morda prevelika stopnja anonimnosti vodi v deviantno vedenje posameznikov. Anonimnost, ki jo zagotavlja komunikacija preko računalnika, vzpodbudi številne zavrte želje v človeški duši, posamezne prikrite slabosti pa se okrepijo. Anonimnost kibernetskega okolja ostaja osrednja preokupacija psihologov in sociologov, ki preučujejo vedenje v virtualnem svetu.

Tehnološko zahtevna izsledljivost storilcev omogoča neovirano delovanje hekerjev, po drugi strani pa vse številčnejše in naprednejše tehnike za anonimizacijo zagotavljajo uporabo interneta brez razkritja identifikacijskih podatkov. Anonimizacija omogoča kriminalcem, da uporabljajo internet brez možnosti za ugotavljanje njihove identitete (Akdeniz, 2002).

Druge sociološke teorije iščejo vzroke za zlonamerna delovanja v nezavedanju prisotnosti družbe ter pomanjkanju socialnih vezi v računalniško posredovani komunikaciji, razosebljanju ter socialnemu učenju. Pri večini teorij gre za zmanjšanje samozavedanja, opuščanje posameznikovih notranjih meril ter zmanjšanje občutka za odgovornost.

Na vedenje storilcev računalniške kriminalitete vplivajo tudi določene osebnostne lastnosti. Nekateri psihologi vidijo vzroke za deviantno obnašanje predvsem v osebnostnih motnjah in pa tudi v duševnih boleznih. M. E. Kabay, Eric Shaw, Keven Ruby in Jerrold Post pripisujejo velik pomen osebnostnim motnjam v povezavi s pretirano narcisoidnostjo posameznikov (Bosworth,Kabay, 2002). V to skupino bi lahko šteli tudi teorije, ki dajejo močan poudarek možni povezavi med računalniško kriminaliteto in razvojno motnjo, znano kot Aspregerjev sindrom, ki se v lažji obliki pojavlja kot pervazivna razvojna motnja, v težji obliki gre pa za oblike klasičnega avtizma.

Določeni psihologi navajajo kot možen vzrok za računalniško kriminaliteto tudi motnjo z računalniško odvisnostjo (Suler,1997) oz. spletno zasvojenost kot ožjo obliko računalniške

odvisnosti. Pri spletni odvisnosti ne gre za odvisnost od samega interneta, temveč je v ozadju druga oblika odvisnosti.

3 STATISTIČNA ANALIZA PODATKOV O DOMNEVNIH STORILCIH KIBERNETSKE KRIMINALITETE IN PRIMERJAVA S STORILCI FIZIČNE KRIMINALITETE

Statistična obdelava posameznih kibernetskih kaznivih dejanj je izdelana na podlagi več lastnosti oseb osumljenih storitve kaznivih dejanj. Za statistično obdelavo sta izbrani dve populaciji storilcev. Populacijo kibernetske kriminalitete sestavljajo vsi osumljeni storilci po vseh členih kibernetske kriminalitete v Kazenskem zakoniku (uporabljeni so členi iz prejšnjega Kazenskga zakonika, *Ur. List Rs št. 95/2004*). Primerjalno populacijo predstavljajo vsi osumljenci po štirih členih kaznivih dejanj s področja premoženjske kriminalitete. Za omenjena štiri kazniva dejanja sem se odločil predvsem iz razloga, ker motivi storilcev v večini primerov ne odražajo posebnega odnosa do žrtve oz. oškodovanca, kar je primerljivo s kaznivimi dejanji, ki so storjena v kibernetskem prostoru.

V nadaljevanju bom večkrat uporabil pojem klasične kriminalitete. Tu ne gre za kriminalistično delitev deliktov, temveč predstavlja kriminal storjen na tradicionalen način in se navezuje na fizični, materialni svet.

Časovno obdobje statistične obdelave je 12 let. V okviru raziskave sem se odločil za uporabo že zbranih podatkov, ki jih vodi in obdeluje Policija, v okviru Ministrstva za notranje zadeve.

Pregled členov iz kazenskega zakonika ki sem jih uporabil za statistično obdelavo
(vsi statistični podatki se nanašajo na člene iz prejšnjega Kazenskega zakonika, Ur. List Rs št. 95/2004)

Kibernetska kriminaliteta:

- *Kršitev tajnosti občil*, 150. člen – 2. odstavek, 2.točka
- *Zloraba osebnih podatkov* – 154. člen, 2. odstavek
- *Neupravičena uporaba avtorskega dela* - 159. člen
- *Prikazovanje, izdelava, posest in posredovanje pornografskega gradiva* – 187. člen
- *Neupravičen vstop v informacijski sistem* – 225. člen
- *Vdor v informacijski sistem* – 242. člen
- *Izdelovanje in pridobivanje orožja in pripomočkov, namenjenih za kaznivo dejanje* – 309. člen, 3. odstavek

Primerjalni členi s področja klasične (fizične) kriminalitete:

- *Tatvina,* 211. člen
- *Velika tatvina* , 212. člen
- *Rop* - 213. člen
- *Roparska tatvina* - 214. člen

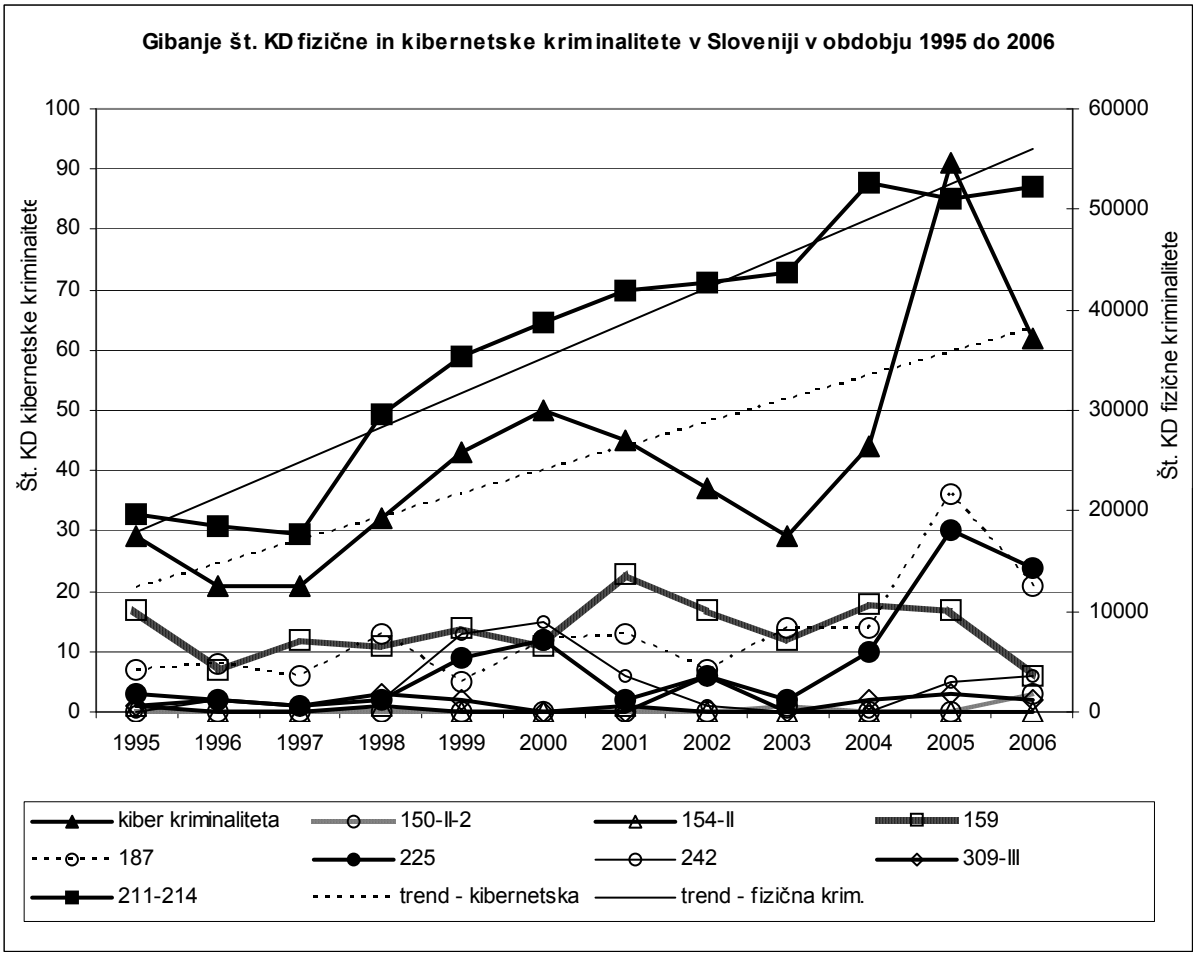
3.1 Splošen pregled števila kaznivih dejanj računalniške kriminalitete

V tabeli 1 so prikazana vsa kazniva dejanja po izbranih členih, ki so bila storjena v Sloveniji časovnem obdobju od leta 1995 do 2006. Statistično enoto predstavljajo vsa kazniva dejanja (po zgoraj navedenih členih), za katera je policija v navedenem obdobju na podlagi devetega odstavka 148. člena Zakona o kazenskem postopku vložila kazensko ovadbo ali poročilo v dopolnitev kazenske ovadbe. Skupno število storjenih kibernetskih kaznivih dejanj prikazanih

v tabeli je 504, kar predstavlja le 0,11 odstotka od skupne vsote vseh izbranih KD, prikazanih v tabeli. Kazniva dejanja ponarejanja kreditnih kartic statistično niso uvrščena med kibernetski kriminal, temveč med goljufije oz. tatvine, kar izkrivlja prikaz resničnega stanja na področju računalniškega kriminala v Sloveniji.

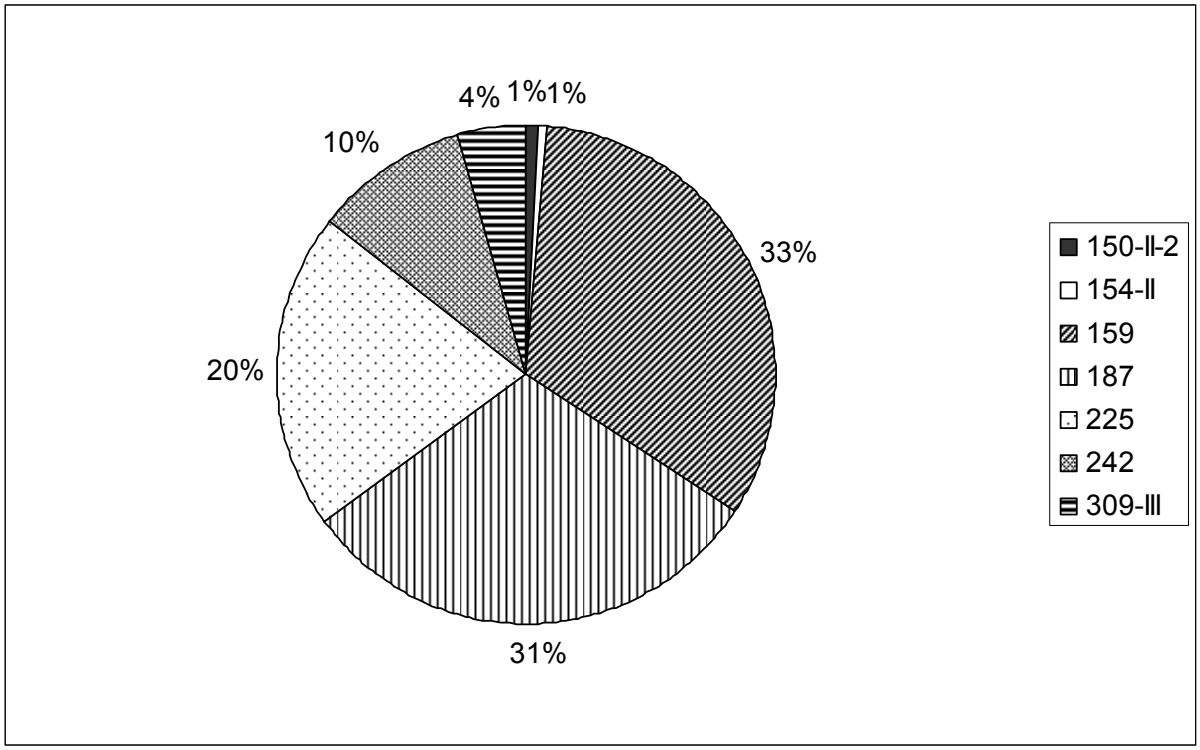
Tabela 1: Število kaznivih dejanj v obdobju 1995 do 2006 po posameznih kaznivih dejanjih (Vir: Policija, 2007)

leto	211-214	150-II-2	154-II	159	187	225	242	309-III	kiber	SKUPAJ
1995	19603	0	1	17	7	3	0	1	29	19632
1996	18383	0	0	7	8	2	2	2	21	18404
1997	17639	0	0	12	6	1	1	1	21	17660
1998	29648	0	1	11	13	2	2	3	32	29680
1999	35450	0	0	14	5	9	13	2	43	35493
2000	38738	0	0	11	12	12	15	0	50	38788
2001	41963	0	1	23	13	2	6	0	45	42008
2002	42697	0	0	17	7	6	1	6	37	42734
2003	43733	1	0	12	14	2	0	0	29	43762
2004	52614	0	0	18	14	10	0	2	44	52658
2005	51134	0	0	17	36	30	5	3	91	51225
2006	52310	3	0	6	21	24	6	2	62	52372
SKUPAJ	443912	4	3	165	156	103	51	22	504	444416



Slika 1: Gibanje števila kaznivih dejanj fizične in kibernetske kriminalitete v Sloveniji v letih 1995 do 2006 (Vir: Policija, 2007)

Slika 1 prikazuje gibanje števila kaznivih dejanj obeh vrst kriminalitete. V nasprotju s pričakovanji se trendna črta fizične kriminalitete dviga strmeje kot pri računalniški kriminaliteti. Potrebno je opozoriti na veliko polje neodkritih KD pri računalniški kriminaliteti in njeno sorazmerno nizko število enot, kar je treba upoštevati pri vrednotenju rezultatov. Majhno število statističnih povzroča tudi dokaj veliko nihanje krivulje, ki prikazuje skupno število kibernetskih KD. Močneje izstopata le kaznivi dejanji *Neupravičenega vstopa v informacijski sistem* in *Prikazovanja, izdelave, posesti in posredovanja pornografskega gradiva.* Ker novi kazenski zakonik inkriminira nekatera dejanja, ki se niso preganjala po prejšnjem zakoniku in posegajo v področje računalniške kriminalitete, lahko pričakujemo opaznejši dvig števila kaznivih dejanj v letu 2008.



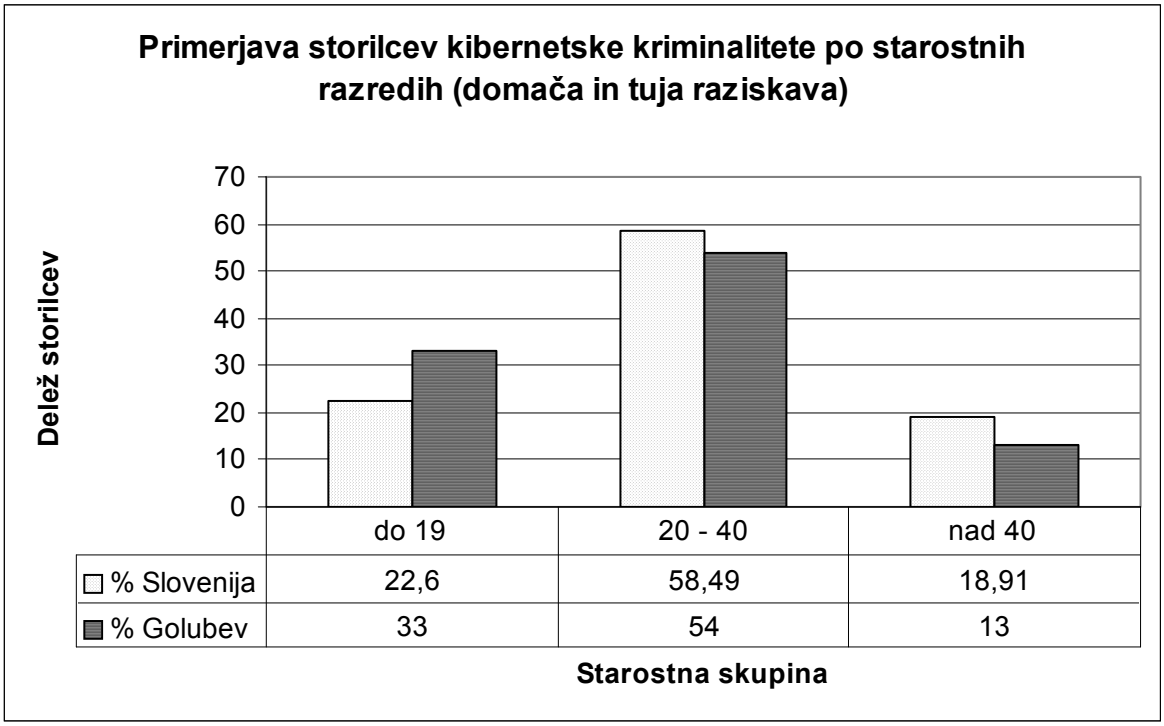
Slika 2: Deleži posameznih kaznivih dejanj računalniške kriminalitete (N=504, Vir: Policija, 2007)

Slika 2 prikazuje deleže posameznih kaznivih dejanj v okviru kibernetske kriminalitete. Najštevilčnejše so kršitve 225. člena, *Neupravičena uporaba avtorskega dela, ki zajema 33 odstotkov,* sledita ji kaznivi dejanji *Prikazovanja, izdelave, posesti in posredovanja pornografskega gradiva (187. člen KZ)* ter *Neupravičen vstop v informacijski sistem(225. člen KZ).* Kaznivo dejanje *Vdora v informacijski sistem (242. člen KZ)* obsega desetino, 4 odstotni delež ima kaznivo dejanje *Izdelovanje in pridobivanje orožja in pripomočkov, namenjenih za kaznivo dejanje (309. člen KZ).* Hekerski kaznivi dejanji (225. in 242. člen) skupaj obsegata 41 odstotkov vseh KD računalniške kriminalitete.

3.2 Starost domnevnih storilcev računalniške in primerjalne kriminalitete

Po nekaterih že opravljenih raziskavah v svetu, je starost storilcev računalniške kriminalitete dokaj nizka. Golubev se sklicuje na ocene strokovnjakov Bilenchuka, Romanuka in Tsimbaluka, po katerih naj bi bilo 33 % storilcev mlajših od 20 let, 54 % je v starostni skupini 20 do 40 let, 13 % pa je starejših od 40 let (Golubev, 2003). Slika 3 prikazuje primerjavo Golubeve raziskave s podatki v Sloveniji. Obe raziskavi imata podobno grupirane podatke, pri katerih je najmočnejša skupina storilcev v skupini med 20 in 40 leti. Skupina do 19 let je

nekoliko šibkeje zastopana pri slovenskih osumljencih, primanjkljaj pa sta si enakovredno razdelili ostali skupini.

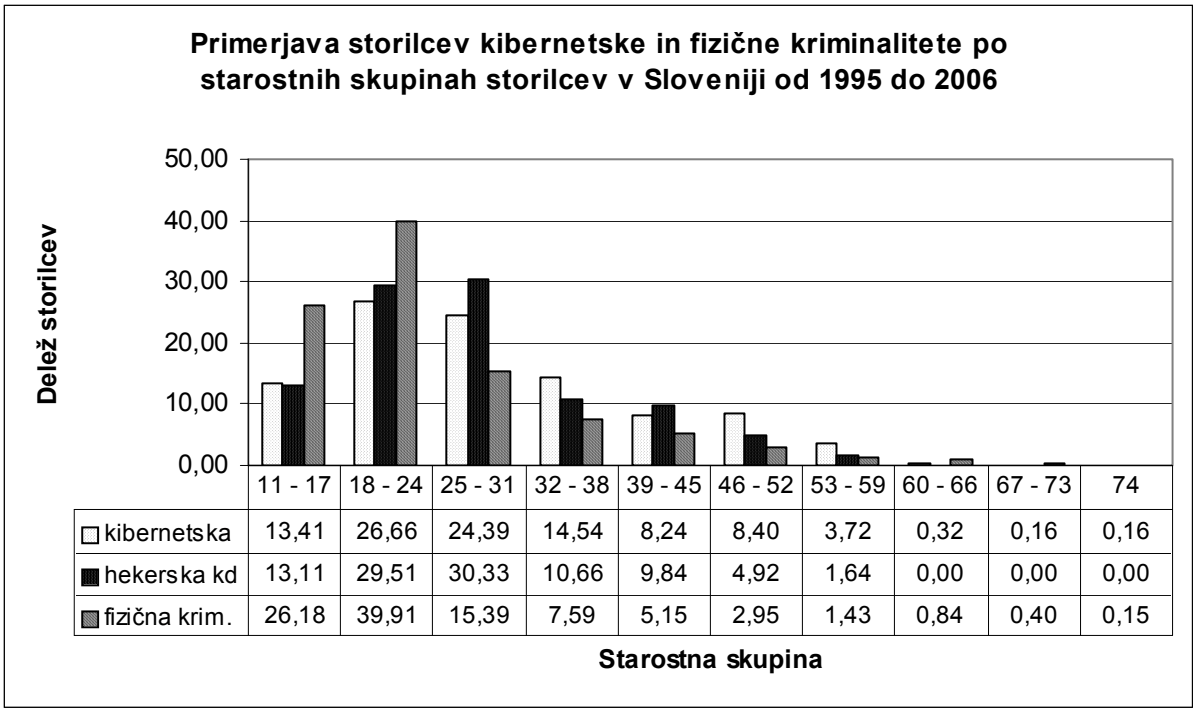


Slika 3: Primerjava rezultatov domače in tuje raziskave o starostnih skupinah storilcev računalniške kriminalitete (Vir: Policija, 2007 in Golubev, 2003)

Tabela 2: Primerjava statističnih vrednosti med kibernetsko in fizično kriminaliteto

	starost - kibernetska	*starost - fizična*
Povprečna starost	31,52758133	24,47794499
Mediana	29	21
Modus	22	17
Standardna deviacija	12,42485698	10,48553536
Varianca	154,3770711	109,9464518
sploščenost	0,281813678	3,605494837
Asimetrija	0,710235572	1,803780565
Najvišja starost	79	94
Število enot	707	159941

V tabeli 2 so prikazane nekatere statistične mere za obe populaciji storilcev. Povprečna vrednost storilcev kibernetske kriminalitete je 31,5 let in je precej višja kot pri storilcih fizične kriminalitete, kjer je 24,4 let. Standardni odklon je nekoliko višji pri storilcih kibernetske kriminalitete, sta pa pri obeh populacijah občutna, kar velja upoštevati pri interpretaciji rezultatov. Sploščenost oz. kurtoznost populacije je precej višja pri storilcih fizične kriminalitete, kar nakazuje na relativno razgibanost. Asimetrija osi je pri obeh populacijah pomaknjena v desno. Morda je zanimiva še mediana, ki je pri kibernetski kriminalitetei 29 let, pri storilcih fizične kriminalitete pa 21 let.



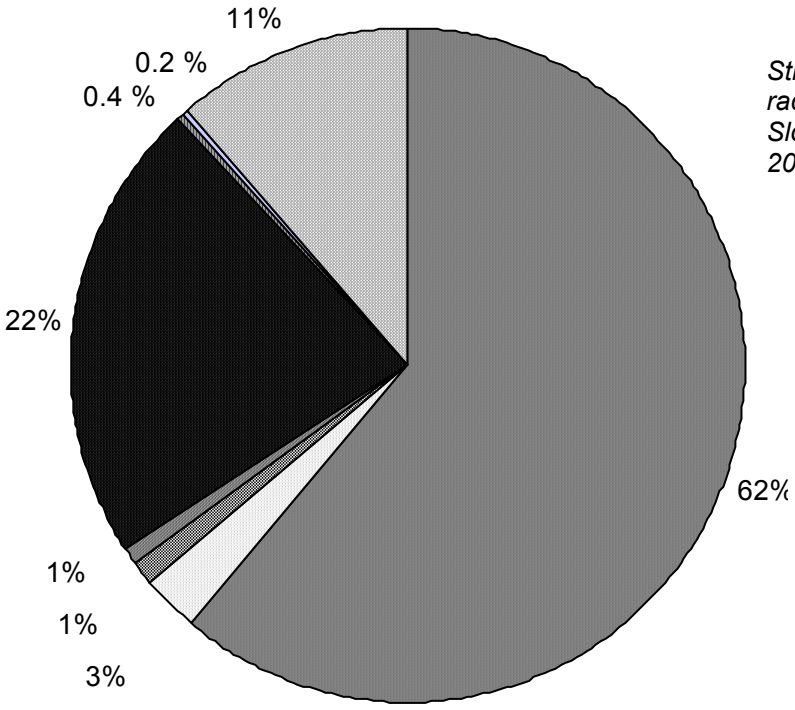
	11 - 17	18 - 24	25 - 31	32 - 38	39 - 45	46 - 52	53 - 59	60 - 66	67 - 73	74
kibernetska	13,41	26,66	24,39	14,54	8,24	8,40	3,72	0,32	0,16	0,16
hekerska kd	13,11	29,51	30,33	10,66	9,84	4,92	1,64	0,00	0,00	0,00
fizična krim.	26,18	39,91	15,39	7,59	5,15	2,95	1,43	0,84	0,40	0,15

Slika 4: Primerjava storilcev kibernetske in fizične kriminalitete po starostnih skupinah storilcev v Sloveniji v letih 1995 do 2006 (Storilci hekerskih kaznivih dejanj 225. in 242. člen so prikazani tudi ločeno, vir: Policija, 2007)

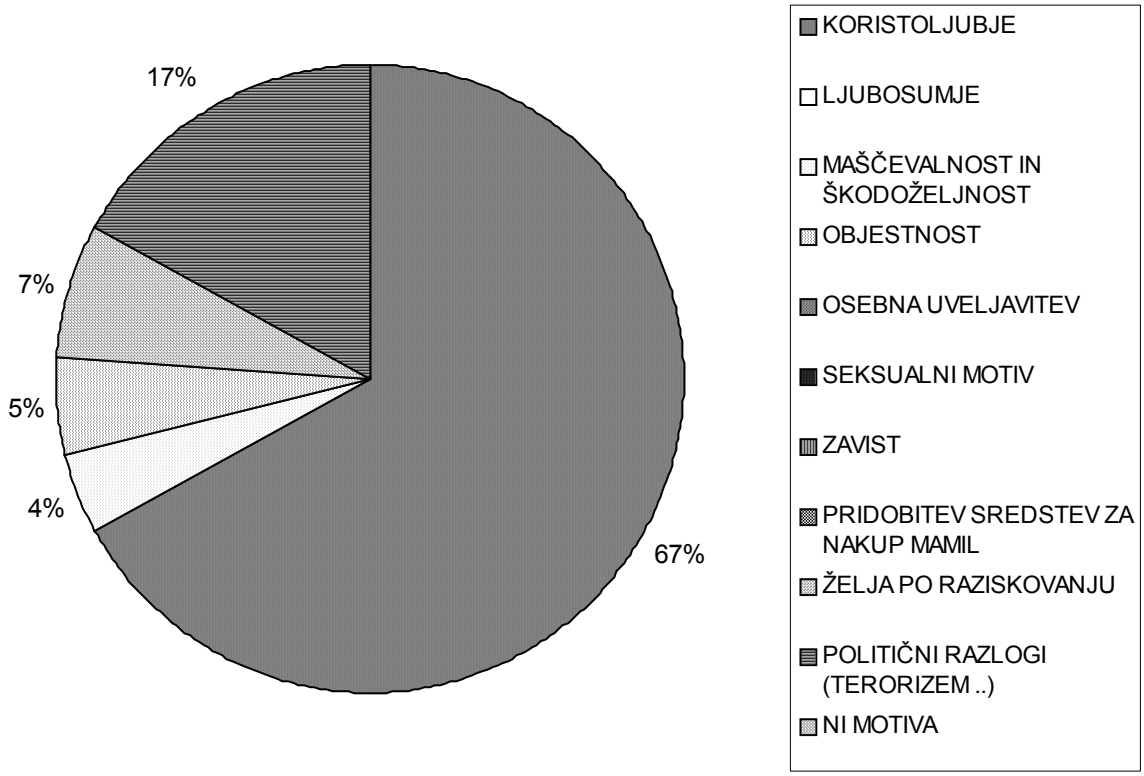
Slika 4 prikazuje porazdelitev osumljencev po ožjih starostnih razredih (velikost razreda je 7 let). Poleg populacije vseh storilcev kibernetske kriminalitete so prikazani ločeno tudi storilci hekerskih kaznivih dejanj (225. in 242 člen starega KZ). V nasprotju s predvidevanji je najštevilčnejši razred pri hekerski kaznivih dejanjih v starostni skupine 25 do 31 let, kar je višje kot pri skupni populaciji kibernetske in fizične kriminalitete, kjer je najmočneje zastopana starostna skupine 18 do 24 let.

3.3 Motivi domnevnih storilcev računalniške in primerjalne kriminalitete

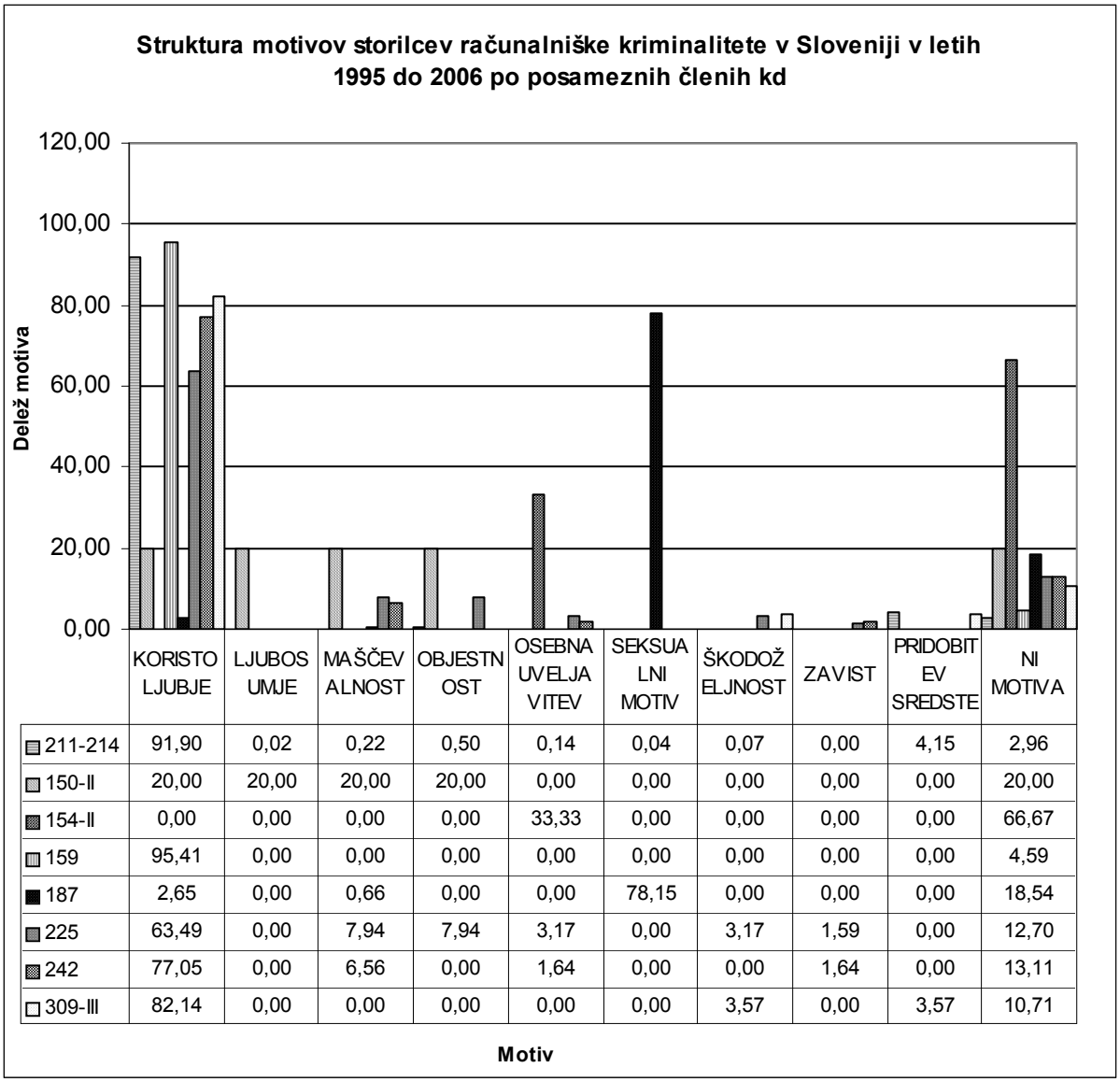
Poglavje o motivih storilcev računalniške kriminalitete morda najbolj razgalja njihovo pravo bit. Ne smemo enačiti vseh hekerjev s škodljivimi hekerji, saj bi prvi skupini naredili krivico. Drugo skupino lahko preprosto imenujemo kriminalci in s pravim hekerstvom nima nobene povezave. Slabo luč na prvo skupino mečejo prestopniki, ki svoje računalniške spretnosti ponujajo skupinam organiziranega kriminala. V nasprotju s prej omenjeno Chantlerjevo raziskavo je prevladujoč motiv koristoljubje. Slika 5 prikazuje delež motivov kibernetske kriminalitete v Sloveniji in rezultate raziskav Golubeva (Golubev, 2003). V obeh primerih izstopa motiv koristoljubja, Slovenija 62 %, Golubev 67 %. Pri slovenski populaciji je močno zastopan še spolni motiv, ki ga Golubev ne navaja. Gre za razliko o uvrščenosti kaznivih dejanjih v posamezno statistično raziskavo. Pri Golubevu je močno prisoten tudi politični motiv (17%), ki ga pri slovenski kaznivih dejanjih ni zaslediti. V tuji raziskavi je prisotna tudi želja storilcev po raziskovanju (7 %), pri domačih osumljencih tega motiva ni navedenega. Tuji storilci zagrešijo kazniva dejanja iz objestnosti v 5%, maščevalnost in škodoželjnost pa sta zastopani podobno v obeh raziskavah (Slovenija 3 %, tuja raziskava 4%). Pri slovenskih podatkih v 11 % odstotkih ni naveden motiv za storitev kaznivega dejanja.



Struktura motivov storilcev računalniške kriminalitete v Sloveniji v letih 1995 do 2006



Slika 5: Primerjava strukturnih deležev motivov storilcev računalniške kriminalitete – domača in tuja raziskava

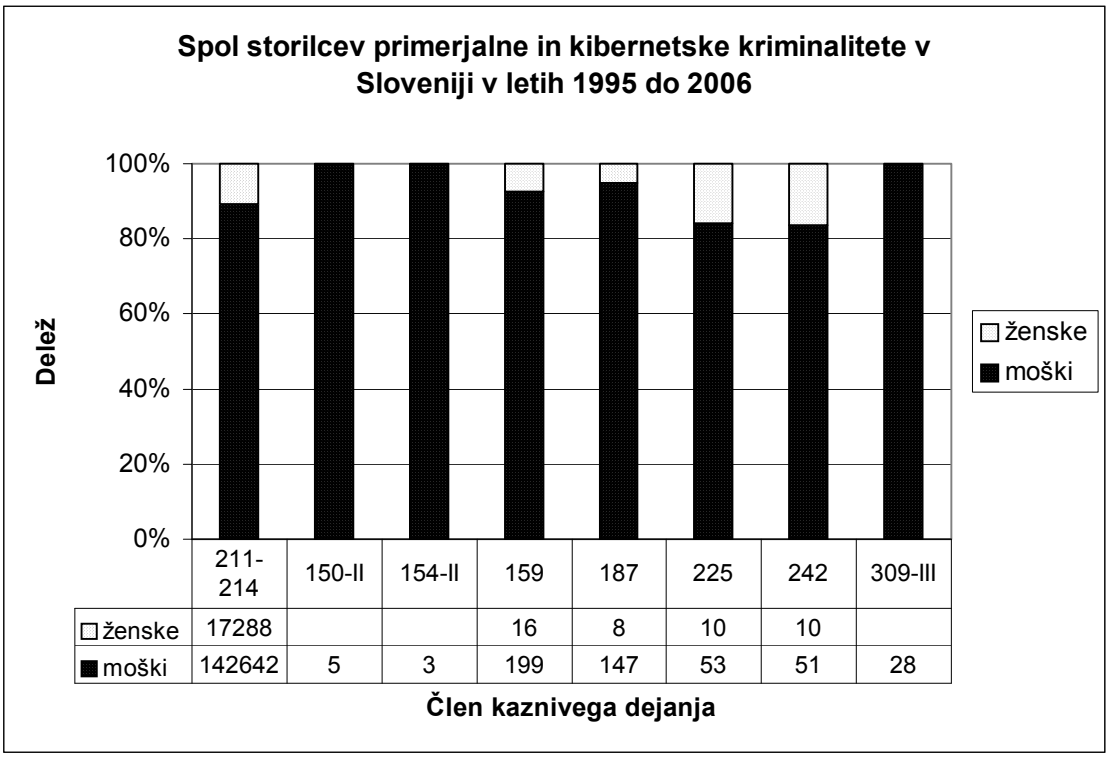


	KORISTOLJUBJE	LJUBOSUMJE	MAŠČEVALNOST	OBJESTNOST	OSEBNA UVELJAVITEV	SEKSUALNI MOTIV	ŠKODOŽELJNOST	ZAVIST	PRIDOBITEV SREDSTE	NI MOTIVA
211-214	91,90	0,02	0,22	0,50	0,14	0,04	0,07	0,00	4,15	2,96
150-II	20,00	20,00	20,00	20,00	0,00	0,00	0,00	0,00	0,00	20,00
154-II	0,00	0,00	0,00	0,00	33,33	0,00	0,00	0,00	0,00	66,67
159	95,41	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	4,59
187	2,65	0,00	0,66	0,00	0,00	78,15	0,00	0,00	0,00	18,54
225	63,49	0,00	7,94	7,94	3,17	0,00	3,17	1,59	0,00	12,70
242	77,05	0,00	6,56	0,00	1,64	0,00	0,00	1,64	0,00	13,11
309-III	82,14	0,00	0,00	0,00	0,00	0,00	3,57	0,00	3,57	10,71

Slika 6: Struktura motivov storilcev računalniške kriminalitete v Sloveniji v letih 1995 do 2006 po posameznih členih kd

Slika 6 in pripadajoča tabela prikazujeta deleže motivov domnevnih storilcev kibernetske kriminalitete v Sloveniji v obdobju 1995 do 2006 po posameznih členih. 150. in 154 člen, II odstavek, ne bom posebej analitično obravnaval, ker gre za minimalno število statističnih enot. Koristoljubje je prevladujoč motiv pri vseh kibernetskih kaznivih dejanjih, izjemo predstavlja le kaznivo dejanje *Prikazovanja, izdelave, posesti in posredovanja pornografskega gradiva* – 187. člen KZ RS, kjer je prevladujoč spolni motiv.

3.4 Spol domnevnih storilcev računalniške in primerjalne kriminalitete



	211-214	150-II	154-II	159	187	225	242	309-III
ženske	17288			16	8	10	10	
moški	142642	5	3	199	147	53	51	28

***Slika 7: Struktura storilcev primerjalne in kibernetske* kriminalitete v Sloveniji v letih od 1995 do 2006 po spolu**

Primerjava spolov storilcev se na prvi pogled ne razlikuje bistveno med posameznima vrstama kriminalitete (Slika 7). Chantler navaja v eni izmed svojih raziskav, da je le 5 odstotkov hekerjev ženskega spola. Pri nas je odsotek nekoliko višji in znaša 16,1 odstotek, če upoštevamo le hekerska kazniva dejanja (225. in 242. člen).

3.5 Izobrazbena raven in zaposlitveni status domnevnih storilcev računalniške kriminalitete in primerjalne kriminalitete

Pred pregledom statističnih podatkov moram opozoriti na metodologijo, ki sem jo izbral pri obdelavi statističnih podatkov o izobrazbi, statusu zaposlitve in delu, ki so ga opravljali storilci v času storitve kaznivega dejanja. Za relevantno primerjavo izobrazbe obeh populacij je potrebno izbrati enotno merilo. Idealno merilo bi predstavljala stopnja izobrazbe, vendar se policijska statistika vodil le po poklicih storilcev in ne po stopnji izobrazbe. Stopnjo izobrazbe sem nadomestil z ravnjo znanja, ki je potrebna za uspešno opravljanje nalog iz posameznega poklica. Raven znanja določa hierarhični položaj poklica v glavni poklicni skupini. Znotraj skupine so opredeljene še vrste znanja, ki določajo položaj poklica znotraj skupine. Podatke sem ustrezno prilagodil vsem poklicem, ki so se pojavili v statističnih podatkih. Za klasifikacijo sem uporabil uredbo Vlade Republike Slovenije o uvedbi in uporabi Standardne klasifikacije poklicev SKP-V2 (Uradni list RS, št. 16/2000), ki je dopolnila in spremenila Uredbo o standardni klasifikaciji poklicev iz leta 1997 (Uradni list RS, št. 28/97). Pretvorbo po SKP sem izbral, ker predstavlja obvezen nacionalni standard, ki se uporablja pri zbiranju, obdelavi in analizi podatkov na našem trgu dela. Priloga 1 prikazuje pretvorbo podatkov o poklicih, ki sem jo opravil po SKP-V2 (Statistični urad R S, 2000). Oviro pri obdelavi podatkov v tej skupini predstavlja tudi veliko število storilcev brez navedbe podatka o poklicu.

Pri statistični obdelavi podatkov ravni znanja sem izločil vse poklice, za katere ni opredeljena potrebna raven. Izločeni skupini sta skupina 1, v katero so uvrščeni zakonodajalci, visoki uradniki in menedžerji, ter skupina 9, v katero so uvrščeni vojaški poklici (Tabela 3).

Tabela 3: Standardna klasifikacija poklicev, glavne skupine poklicev, ravni znanja in stopnja izobrazbe, ki ustreza večini poklicev v skupini (Vir: Statistični urad R Slovenije, Metodološka pojasnila k SKP-V2)

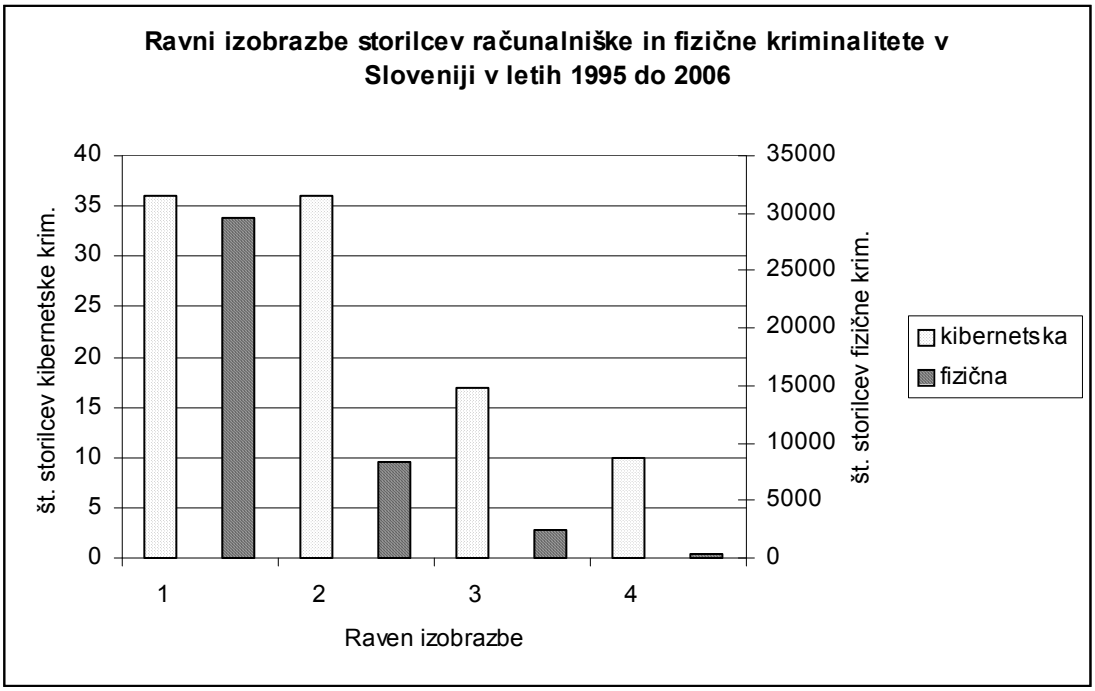
Glavna skupina poklicev		Raven znanja	Programi oz. stopnje izobrazbe, ki praviloma zagotavljajo usposobljenost za opravljanje večine poklicev v posamezni glavni skupini poklicev
1	Zakonodajalci/zakonodajalke, visoki uradniki/visoke uradnice in menedžerji/menedžerke	**-**	ni opredeljena raven znanja
2	Strokovnjaki/strokovnjakinje	**4**	programi do- in postdiplomskega univerzitetnega izobraževanja
3	Tehniki/tehnice in drugi strokovni sodelavci/druge strokovne sodelavke	**3**	programi srednjega[1] in postsrednjega izobraževanja brez univerzitetnih
4	Uradniki/uradnice	**2**	programi srednjega izobraževanja[1]
5	Poklici za storitve, prodajalci/prodajalke	**2**	programi srednjega izobraževanja[1]
6	Kmetovalci/kmetovalke, gozdarji/gozdarke, ribiči/ribičke, lovci/lovke	**2**	programi srednjega izobraževanja[1]
7	Poklici za neindustrijski način dela	**2**	programi srednjega izobraževanja[1]
8	Upravljalci/upravljalke strojev in naprav, industrijski izdelovalci/industrijske izdelovalke in sestavljalci/sestavljalke	**2**	programi srednjega izobraževanja[1]
9	Poklici za preprosta dela	**1**	izpolnjena osnovnošolska obveznost
0	Vojaški poklici	-	ni opredeljena raven znanja

Tabela 4 prikazuje število in odstotek posamezne ravni znanja (ne gre za stopnjo izobrazbe) obeh populacij storilcev kaznivih dejanj. Pri domnevnih storilcih fizične kriminalitete ima doseženo prvo raven izobrazbe skoraj tri četrine storilcev, pri kibernetski kriminalitete pa je število osumljenih s prvo izobrazbeno ravnijo dobra tretjina. Preko 90 % storilcev ima zaključeni prvi ravni izobrazbe in le slab odstotek četrto raven. Pri kibernetski kriminaliteti je takih storilcev desetina. Kibernetski storilci imajo torej višjo izobrazbeno raven kot storilci fizične kriminalitete. Povprečna izobrazbena raven populacije storilcev klasične kriminalitete je 1,35 ravni izobrazbe, standardni odklon je 0,633 ravni. Standardni odklon pri storilcih kibernetske kriminalitete je 0,97 ravni izobrazbe, povprečna vrednost ravni izobrazbe je 2,01 ravni. Povprečni osumljeni storilec kibernetske kriminalitete ima torej dokončano nekoliko višjo raven izobrazbe kot jo imajo osumljenci pri klasični kriminaliteti.

[1] Zahtevana raven programa srednjega izobraževanja obsega poklicne, tehnične, strokovne in splošne programi srednjega izobraževanja

Tabela 4: Število in delež storilcev računalniške in fizične kriminalitete po ravneh izobrazbe V Sloveniji v letih od 1995 do 2006

raven izobrazbe	vrsta kriminalitete			
	kibernetska		klasična	
	število	odstotek	število	odstotek
1	36	36,36	29530	72,58
2	36	36,36	8318	20,45
3	17	17,17	2503	6,15
4	10	10,1	333	0,82
skupaj	99	100	40684	100

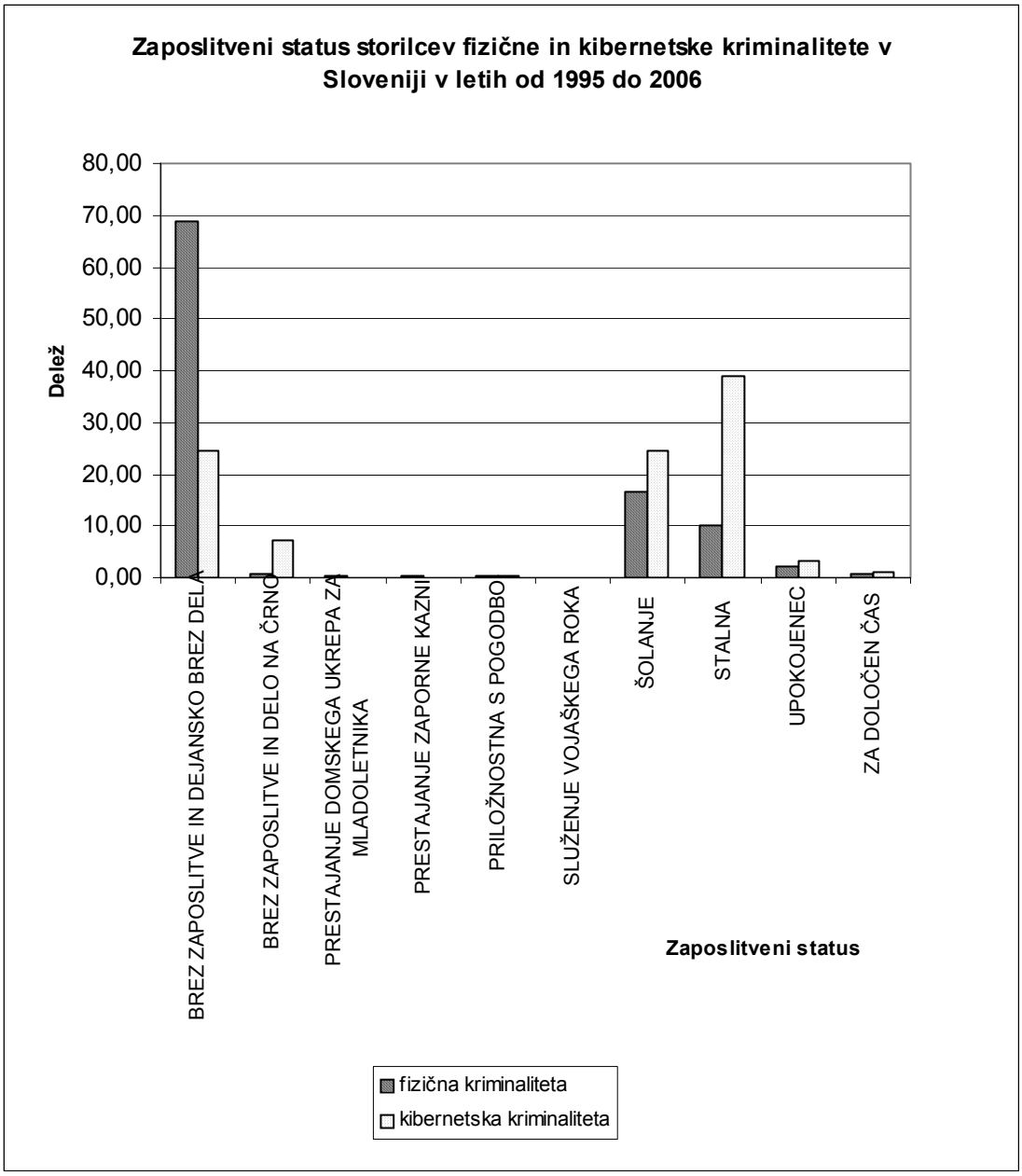


Slika 8: Izobrazba storilcev računalniške in fizične kriminalitete v Sloveniji v letih od 1995 do 2006 (Vir: tabela 4)

Slika 8 grafično prikazuje podatke iz Tabele 4.

Tabela 5: Zaposlitveni status storilcev fizične in kibernetske kriminalitete v Sloveniji v letih od 1995 do 2006

zaposlitveni status	vrsta kriminalitete			
	211-214	delež	kibernetska	delež
BREZ ZAPOSLITVE IN DEJANSKO BREZ DELA	56104	68,81	62	24,6
BREZ ZAPOSLITVE IN DELO NA ČRNO	660	0,81	18	7,1
PRESTAJANJE DOMSKEGA UKREPA ZA MLADOLETNIKA	255	0,31		0,0
PRESTAJANJE ZAPORNE KAZNI	165	0,20		0,0
PRILOŽNOSTNA S POGODBO	417	0,51	1	0,4
SLUŽENJE VOJAŠKEGA ROKA	26	0,03		0,0
ŠOLANJE	13487	16,54	62	24,6
STALNA	8317	10,20	98	38,9
UPOKOJENEC	1650	2,02	8	3,2
ZA DOLOČEN ČAS	454	0,56	3	1,2
SKUPAJ (ZNAN STATUS ZAPOSLITVE)	81535	100,00	252	100,0
NEZNANO	78406	78406		
DELEŽ (NEZNANO V CELOTNI POPULACIJI)	49,02	49,02		
ŠTEVILO STORILCEV SKUPAJ Z NEZNANO	159941	159941		



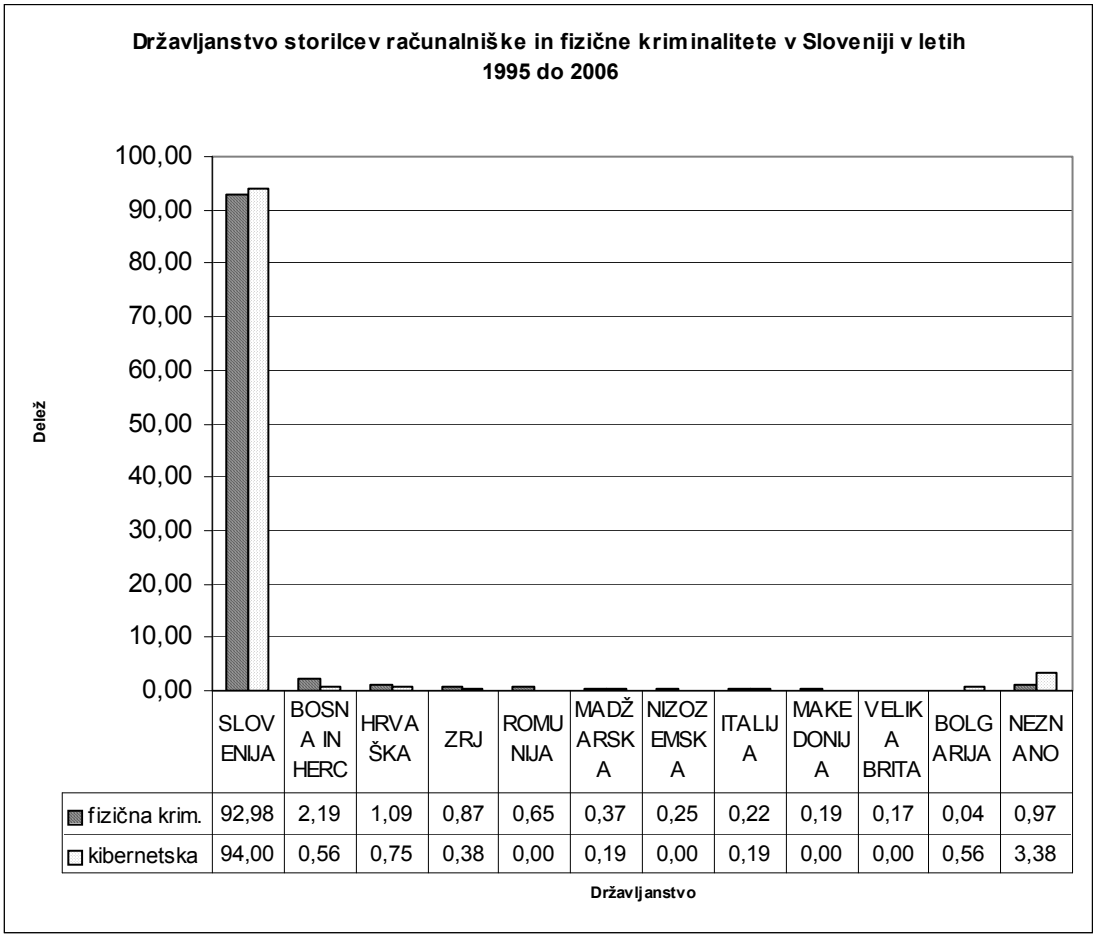
Slika 9: zaposlitveni status obeh populacij v Sloveniji v obdobju od 1995 do 2006 (Vir tabela 5)

Tabela 5 prikazuje zaposlitveni status storilcev kibernetske kriminalitete in populacije storilcev primerjalne kriminalitete v obdobju 1995 do 2006. Skoraj polovico osumljenih storitve kd pri klasični kriminaliteti ni imelo podatka o statusu zaposlitve oz. je bil neznan. Pri izračunu deleža teh podatkov nisem upošteval in sem uporabil le enote, kjer so bili ti podatki znani. Pri primerjalnih členih je status zaposlitve zelo močan kriminogeni faktor za storitev kaznivega dejanja, saj je izvršilo kaznivo dejanje dve tretjini oseb, ki niso imele zaposlitve in se tudi niso preživljale s stranskim zaslužkom. Kadar so brezposelne osebe opravljale delo na črno, se verjetnost storitve kaznivega dejanja močno zmanjša in pade celo pod en odstotek v deležu vseh storilcev, kjer so znani podatki o zaposlitvi. Čas šolanja je drugi najpogostejši zaposlitveni status in zavzema 16,65 odstotkov deleža pri storilcih z znanimi podatki. Vsak deseti stalno zaposlen izvrši kaznivo dejanje premoženjskega delikta. Ostali zaposlitveni statusi nimajo takega vpliva na storitev kaznivega dejanja. Pri storilcih kibernetske kriminalitete je delež storilcev, ki imajo zaposlitev skoraj 40 %, iz česar lahko zaključimo, da pri njih motiv koristoljubja ne izvira iz bitke za preživetje, temveč gre za izboljšanje njihovega

materialnega položaja. Le četrtini osumljencev računalniške kriminalitete storitev kaznivega dejanja tudi dejansko omogoča pridobivanje sredstev za preživljanje. Zaposlitveni status storilcev kibernetske kriminalitete torej ne opravičuje njihovih dejanj.

3.6 Državljanstvo

Kibernetska kriminaliteta velja za kriminaliteto brez meja. Običajno si predstavljamo, da so naši strežniki napadeni večinoma iz tujih omrežij in tujih strežnikov ter s strani tujih hekerjev. Statistični podatki nasprotno dokazujejo, da večino vdorov v informacijske sisteme izvršijo slovenski državljani. Zmotne predpostavke o poreklu morebitnih napadalcev informacijskih sistemov pa sprejemajo celo vladne institucije in na napačni oceni ogrožanja zasnujejo celotne protiukrepe. Za primer bi lahko navedli poročilo podjetja Riptech iz leta 2002, ki v poglavju o kibernetskem terorizmu ugotavlja, da je bil le 1 odstotek napadov izvedenih iz držav, ki jih ameriško zunanje ministrstvo povezuje s terorizmom (Bendrath, 2003).



	SLOVENIJA	BOSNA IN HERC	HRVAŠKA	ZRJ	ROMUNIJA	MADŽARSKA	NIZOZEMSKA	ITALIJA	MAKEDONIJA	VELIKA BRITA	BOLGARIJA	NEZNANO
fizična krim.	92,98	2,19	1,09	0,87	0,65	0,37	0,25	0,22	0,19	0,17	0,04	0,97
kibernetska	94,00	0,56	0,75	0,38	0,00	0,19	0,00	0,19	0,00	0,00	0,56	3,38

Slika 10: Državljanstvo storilcev kibernetske in fizične kriminalitete v Sloveniji v obdobju od 1995 do 2006 (Vir: Policija, 2007)

Slika 10 prikazuje državljanstva storilcev kibernetske in fizične kriminalitete v Sloveniji v obdobju 1995 do 2006. Preko 90 odstotkov vseh storilcev obeh kriminalitet predstavljajo državljani R Slovenije, vsi ostali pa pri kibernetski kriminalitete zavzemajo manj kot odstotek. Za 3,38 odstotka kibernetskih storilcev ni podatka o njihovem državljanstvu.

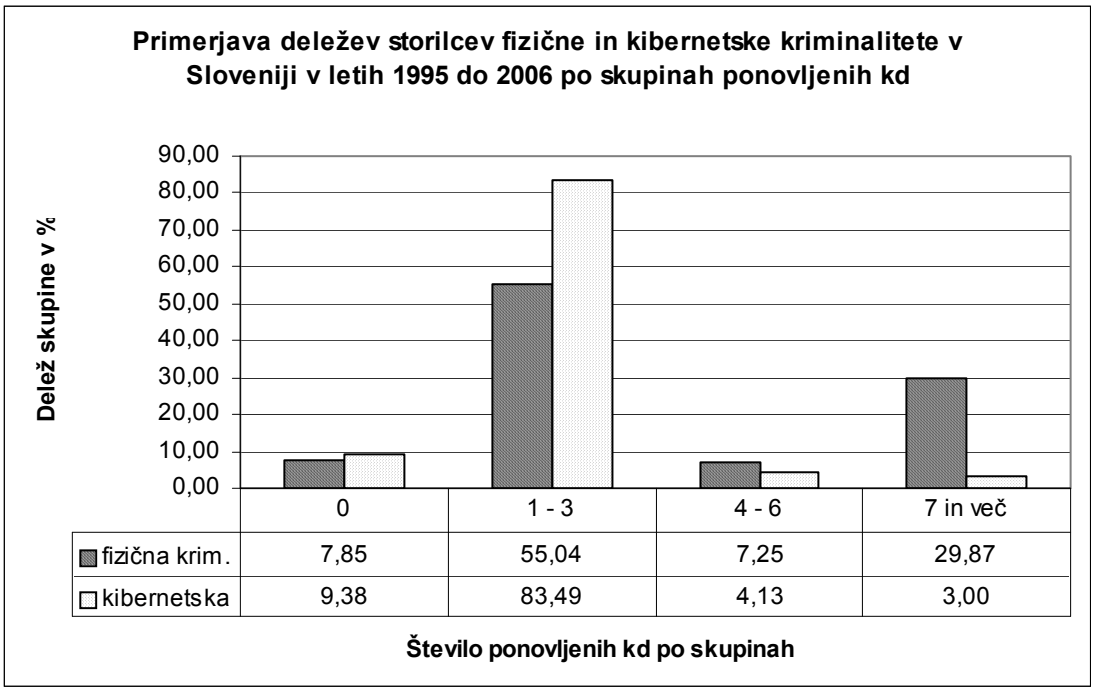
3.7 Povratništvo storilcev kibernetske kriminalitete in primerjava s storilci fizične kriminalitete

V tem sklopu naloge bom obravnaval recidivizem storilcev kibernetske kriminalitete. Ali so kibernetska kazniva dejanja enkratna, ali morda del ponavljajočega se vzorca deviantnega

vedenja? Primerjavo sem ponovno izvedel s storilci iz sveta fizičnega kriminala, s področja premoženjske kriminalitete. Podatke sem razdelil po skupinah. Prvi razred predstavljajo storilci brez ponovljenih kaznivih dejanj. Sledita dva vmesna razreda, vsak s tremi enotami ponovitev. Zadnji razred predstavljajo storilci s sedmimi in več kaznivimi dejanji.

Pri klasični kriminaliteti je delež storilcev v razredu z več kot sedmimi ponovljenimi kaznivimi dejanji občutno večji kot pri računalniški kriminaliteti. Malo ponovitev v razredu sedem in več kaznivih dejanj, lahko pripišemo sorazmerno mladi kibernetski kriminaliteti. Odstopanja so mogoča tudi zaradi majhnega absolutnega števila enot kibernetske kriminalitete.

Storilci računalniške kriminalitet kažejo močno nagnjenost k ponavljanju kaznivih dejanj, saj jih je le 9,38 odstotkov izvršilo le eno kaznivo dejanje. Delež je podoben kot pri primerjalni kriminaliteti, kjer je eno kaznivo dejanje izvršilo 7,85 odstotkov storilcev celotne populacije (Slika 10).



Slika 10: Primerjava deležev storilcev fizične in kibernetske kriminalitete v Sloveniji v letih 1995 do 2006 po skupinah ponovljenih kd

4 ZAKLJUČEK

Mit o altruizmu kibernetske kriminalitete lahko zavržemo. Tudi želja po novem znanju in izziv preizkušanja meja svojega tehničnega znanja ob vdorih v računalniške sisteme, nista prevladujoča motiva, pa čeprav storilci to zelo radi poudarjajo. Zaskrbljujoče je dejstvo, da se vse več hekerjev povezuje s skupinami organiziranega kriminala (Green, 2006), osnovni motiv njihovega delovanja pa postaja denar. Koristoljubje kot eden izmed najstarejših motivov očitno ne bo izumrl tudi v informacijski dobi. Večjo nevarnost kot izkoriščanje materialne koristi predstavljajo hekerski napadi na različno infrastrukturo (vodovodna omrežja in energetske sisteme), v zadnjem času pa celo na zdravje ljudi, ko so zlikovci na spletno stran foruma za bolnike z epilepsijo namestili program, ki lahko ob njegovem aktiviranju pri bolnikih, ki so občutljivi na svetlobne dražljaje oz. določene vzorce, sproži prave epileptične napade.

5 LITERATURA

Akendiz, Y. (2002). *Anonymity, democracy, and cyberspace - Part V: Democratic Process and Nonpublic Politics*, Social Resarch, 2002. Članek je dobljen 25.10.2006 na WWW:http://www.findarticles.com/p/articles/mi_m2267/is_1_69/ai_88584148

Borchgrave, A., Cilluffo, F., J., Cardash, S., Ledgerwood, M. (2000). Cyber Threats and Information Security Meeting the 21st Century Challenge. Washington, Center for Strategic and International Studies

Bendrath, R. (2003). *The American Cyber-Angst and the Real World – Any Link?,* The New Press, New York.

Bosworth, S., Kabay, ME. (et alt). (2002). *Computer Security Handbook*. John Wiley & Sons, 2002, str. 140 – 161.

Carter, D. (1995). Computer-Crime Categories: How Techno-Criminals Operate, The FBI Magazine, julij 1995. 02.04.2006 na WWW: http://www.lectlaw.com/files/cri.14.htm, 02.04.2006.

Chantler, N (1996). Risk: The Profile of the Computer Hacker. Doktorsko delo, Perth , Curtin University of Technology.

Greene, K. (2006). *Catching Cyber Criminals.* http:://www.techologyreview.com/read_article.aspx?id=16520&z=2588&p=1/ch=infotech;pridobljeno 23.10.2006.

Suler, J. (1997). *Computer and Cyberspace Addiction*. Selfhelp Magazine, http://selfhelpmagazine.com/articles/internet/cybaddict.html, pridobljeno 21.10.2006.

Suler, J. (2005). *The Psychology of Cyberspace* ,http://www.rider.edu/users/suler/psycyber/psycyber. html, 21.07.2006.