Revija za kriminalistiko in kriminologijo / Ljubljana 62 / 2011 / 3, s. 242-252

Internetna študija poznavanja kibernetskih groženj in strahu pred kibernetsko kriminaliteto

Igor Bernik[1], **Gorazd Meško**[2]

Prispevek obravnava slovensko perspektivo poznavanja kibernetskih groženj in kibernetske kriminalitete z vidika dojemanja, zavedanja in strahu uporabnikov. S široko dostopnostjo in rabo informacijsko komunikacijskih tehnologij ter povezovanjem uporabnikov s pomočjo omenjenih tehnologij se je namreč odprl kibernetski prostor, ki ga mnogi izrabljajo kot prostor za izvajanje kriminalitete. Z večanjem števila uporabnikov se veča tudi število zlorab, žal pa se uporabniki vse premalo zavedajo nevarnosti na eni in možnosti uspešnega zoperstavljanja grožnjam na drugi strani. S pomočjo rezultatov spletne ankete, izvedene v marcu 2011, predstavljamo vpogled v dojemanje kibernetske kriminalitete in poskušamo razumeti strah pred njo. Rezultati ankete nam na podlagi statistične analize pokažejo, kako uporabniki dojemajo kibernetsko kriminaliteto. Ugotavljamo, da vprašani relativno dobro poznajo pojem kibernetske kriminalitete, vendar se bolj zavedajo medijsko izpostavljenih groženj. Pri tem ne gre zapostaviti dejstva, da so medijsko izpostavljene grožnje široko poznane, niso pa nujno tiste, ki ogrožajo varnost uporabnika, ter vsekakor povečujejo strah uporabnikov pred kibernetsko kriminaliteto. Zato na podlagi znanja in rezultatov predstavljamo glavne smernice, na podlagi katerih se, ob njihovem upoštevanju, zmanjša tveganje v kibernetskem prostoru. Smernice so osnova za boljše zavedanje o nevarnostih in vir napotkov za varnejšo rabo kibernetskega prostora. S tem pa se zaradi boljšega razumevanja groženj in poznavanja ukrepov proti njim zmanjša strah pred kibernetsko kriminaliteto. Spoznanja so praktično uporabna za preučevanje kibernetske kriminalitete in uporabnike kibernetskega prostora.

Ključne besede: dojemanje, zavedanje, strah, kibernetska kriminaliteta, informacijska varnost, Slovenija.

UDK: 343.3/.7: 004

1 Uvod

Strah pred kriminaliteto je danes ena izmed bolj raziskovanih tem v kriminologiji (Meško et al., 2006: 3), zato je poznavanje tovrstnega dogajanja potrebno tudi na področju kibernetske kriminalitete. Dojemanje ogroženosti in zavedanje o njej ter strah pred uporabo kibernetskega prostora so odvisni od posameznega uporabnika, vendar je razumevanje področja potrebno za raziskovanje in pripravo smernic varne rabe kibernetskega prostora. V postmodernih časih skoraj ni najti družbene refleksije, ki ne bi namenila posebne (če že ne kar osrednje) pozornosti negotovostim in iz njih vznikajočim bojaznim in tesnobi (Kanduč, 2005: 337). V tej študiji želimo ugotoviti mnenje ljudi o občutenju strahu pri rabi kibernetskega prostora. Uporabniki se v kibernetski prostor praktično stalno povezujejo oziroma so v njem povezani, saj so tehnologije – mobilne naprave, računalniki in internet – dostopne praktično povsod. Raziskovalci ugotavljajo, da strah pred kriminaliteto običajno presega dejansko stopnjo kriminalitete v družbi (Meško in Šifrer, 2008: 550). Mnogo ljudi se namreč kljub majhnemu številu zlorab boji uporabiti kreditno kartico v spletni trgovini, v realnem svetu pa jo z lahkoto oddajo v uporabo in izgubijo nadzor nad njo, bojijo se zlorabe podatkov, čeprav je na primer spletnih zlorab kreditnih kartic ali kraje identitete v Sloveniji relativno malo. Pa je teh primerov res tako malo ali se le ne pojavijo v medijih? Zelo hitro ugotovimo, da posamezni medijsko predstavljeni primeri povzročijo višjo stopnjo strahu, kot je dejanska ogroženost za morebitno viktimizacijo. Young (2007: 33) ugotavlja, da so množični mediji spektakularna mesta izključevanja: v javnost prenesejo zaporedje, pravičnost in vključenost (ozadje novice), pri tem pa namenoma poudarjajo napake, nepravičnosti in izključenost ter te elemente postavijo v ospredje. Menimo, da to velja tudi za dojemanje kibernetske kriminalitete, pri čemer pogosto pride do učinka, kot ga opisuje Cockcroft (2009: 13), da so novičarski mediji verjetno najbolj prodoren prostor obveščanja, saj s sprotnim načinom poročanja in dostopnostjo širokim množicam redko ne izkoristijo priložnosti za prilaščanje možnosti, da s fascinantnim poročanjem ne izzovejo presenečenj.

Mediji, zlasti novičarski, med katerimi pomemben delež poročanja o kibernetski kriminaliteti zavzemajo internetne

[1] Igor Bernik, docent in predstojnik Katedre za informacijsko varnost na Fakulteti za varnostne vede Univerze v Mariboru.

[2] Gorazd Meško, redni profesor za kriminologijo in dekan Fakultete za varnostne vede Univerze v Mariboru.

vsebine prek storitev web, Facebooka ali obveščanja s serijskimi pismi, te vsebine izkoriščajo za senzacionalistično poročanje. Táko poročanje pa mnogokrat izjemno vpliva na strah pred kibernetsko kriminaliteto. Žal pri tem zaradi vsebinsko pomanjkljivega poročanja ne ozaveščajo javnosti pred zaščito in potrebnimi ukrepi za zaščito posameznika, ampak jo odvračajo od resnega ravnanja. Mediji s svojim poročanjem pogosto ustvarjajo splošno mnenje in z miti o kriminaliteti upravičujejo socialne ukrepe, ki temeljijo predvsem na čustvenem odzivanju na poročanje o kriminaliteti. Ukrepe, predvsem represivne, argumentirajo z izražanjem strokovnih mnenj o kriminaliteti, družbeno nadzorstveni praksi ter obstoječih in pričakovanih institucionalnih in drugih odzivih na kriminaliteto (Meško, 2000: 305).

Vse več ljudi uporablja kibernetski prostor kot nekaj običajnega, vsakdanjega. Uporaba elektronskega poslovanja je tako postala nekaj vsakdanjega, tu pa je poudarjena varnost poslovanja. Zato so osrednja točka varovanja pri elektronskem poslovanju viri, ki imajo za njihovega lastnika določeno vrednost in mu omogočajo zmanjšati tveganje za izpostavljenost grožnjam (Gradišar in Lamberger, 2010: 30).

2 Kibernetska kriminaliteta

Kaj pravzaprav razumemo pod izrazom kibernetska kriminaliteta? Česa naj se pravzaprav bojimo oziroma naj bi se bali? Ali kot pravi Wall (2009: 50), pri govorjenju o razširjenosti kibernetske kriminalitete manjka pojasnilo o tem, kaj je posebej "kibernetskega" na njej. Kazniva dejanja so določena v kazenskih zakonikih. Ljudje za odzivanje na kibernetsko kriminaliteto pričakujejo posebne, temu prilagojene zakone. Vendar je to nesmiselno, saj kazniva dejanja opredeljuje kazenski zakonik, ki omogoča pregon kaznivih dejanj, storjenih v kibernetskem prostoru, kot je na primer otroška pornografija, tatvina denarja z bančnih računov, goljufije, zlorabe in podobno. Še bolj zapleten je kontrast, da je med več sto tisoč incidenti, o katerih poroča kibernetska oziroma informacijska varnostna industrija vsako leto, relativno majhno število kazenskih pregonov (Wall, 2008: 56). Zaradi narave kibernetske kriminalitete se preganja malo kaznivih dejanj, povezanih s kibernetskim prostorom. Čeprav Završnik (2008: 330) navaja, da je mit o anonimnosti na internetu danes preteklost. Zato je iskanje krivcev na prvi pogled enostavno, zaradi zapletenosti in kompleksnosti tehnologij in globalnosti pa je odkrivanje storilcev kibernetskih kaznivih dejanj izjemno oteženo. Moč formalnega družbenega nadzorstva je v primeru vseh zapletenih kaznivih dejanj bistveno manjša kot v primeru vsakodnevne premoženjske in nasilniške kriminalitete. Odzivanje na kibernetsko kriminaliteto zahteva specializacijo in sposobnost zbiranja dokazov, da bi se storilci kibernetskih kaznivih dejanj ustrezno nadzorovali in kaznovali. Problem je v nedorečenosti, kaj je kibernetska kriminaliteta in katera dejanja naj se kaznujejo. Pomembno vprašanje je, ali je strah pred kibernetsko kriminaliteto upravičen in ali so ljudje dejansko ogroženi pred to vrsto kriminalitete in kaj je mogoče storiti, da se tveganje za viktimizacijo zmanjša.

"Najprimernejši pojem za poimenovanje kaznivih dejanj v zvezi z računalniki in njihovimi mrežami je po našem mnenju pojem kibernetična kriminaliteta. Ta pojem upošteva, da gre za kriminaliteto v zvezi z računalniki, ki je storjena v kiberkulturnem kontekstu (cyberspace)," navaja Završnik (2005: 249). Če povzamemo še definicijo Alshalana (2005: 12), ki pravi, da je kibernetska kriminaliteta skrita, da uporablja omrežja (v nefizičnem smislu) in občasno vodi k dobičku, in če upoštevamo elemente kibernetske kriminalitete, definirane z mednarodno Konvencijo o kibernetski kriminaliteti (Zakon o ratifikaciji Konvencije o kibernetski kriminaliteti in Dodatni protokol h Konvenciji o kibernetski kriminaliteti, ki obravnava inkriminacijo rasističnih in ksenofobičnih dejanj, storjenih v informacijskih sistemih (MKKKDP, 2004), lahko definicijo kibernetske kriminalitete pojmujemo takole: *"Kibernetska kriminaliteta pomeni uporabo informacijsko komunikacijskih tehnologij za izvedbo kaznivih dejanj."* Ob tem moramo poudariti, da med kibernetsko kriminaliteto prištevamo tudi škodljiva in nemoralna dejanja v kibernetskem prostoru, ki niso vedno kriminalizirana in kazniva (Peršak, 2009: 194). Posamezne elemente kibernetske kriminalitete obširno opisujeta Roche in Van Nonstrand (2008) ter podrobno navajata mnoge primere iz ameriške zakonodaje in sodne prakse. Dogajanje na področju kibernetske kriminalitete s pravnega in viktimološkega vidika v slovenskem prostoru obravnava Završnik (2005: 249) ter opredeli kibernetsko kriminaliteto in podobne pojave, psihološki in psihoanalitični fenomen v kibernetskem prostoru, skupnosti v kibernetskem prostoru, viktimizacijo in žrtve kibernetskega prostora, posebnosti storilcev kibernetske kriminalitete in nasilje v kibernetskem prostoru. Vsi ti elementi pa so v kibernetskem prostoru odvisni od dojemanja kibernetske kriminalitete, zavedanja o njej in strahu pred njo. Značilnih je nekaj mitov o kibernetski kriminaliteti (Wall, 2008: 47):

– kibernetski prostor omogoča kriminaliteto – internet ni varen, kibernetska kriminaliteta je vsepovsod;
– mit o vsemogočnih superhekerjih;
– heker lahko prevzame nadzor nad vašo identiteto;
– kriminalci v kibernetskem prostoru so anonimni in jim ni mogoče slediti ali jih izslediti;
– (kibernetski) kriminalci ostanejo nekaznovani;
– hekerji so postali del organiziranega kriminala;
– internet pokvari posameznike, ki običajno spoštujejo zakone, da jih pri rabi interneta kršijo.

Omenjeni miti zaradi slabega poznavanja področja in pogosto nestrokovnega poročanja medijev o kibernetski kriminaliteti še dodatno zastrašujejo uporabnike. Vse to pa nič ne pomaga pri dviganju njihove zavesti za varno delo v kibernetskem prostoru, ampak le povečuje strah uporabnikov. Dimc in Dobovšek (2010: 395) ugotavljata, da so "… nekatere vrste kibernetske kriminalitete tako razširjene, da so postale družbeno sprejemljive (na primer piratstvo)". Piratstvo v trenutno veljavnem slovenskem Kazenskem zakoniku KZ-1 (2008; v nadaljevanju KZ-1) ni opredeljeno kot kaznivo dejanje. V Sloveniji se pripravljajo spremembe zakonodaje. Predlog zakona o spremembah in dopolnitvah Kazenskega zakonika (KZ-1B, 2011) tudi piratstvo opredeljuje kot kaznivo dejanje, saj v poglavju Kršitev avtorskih sorodnih pravic 149. člen predlaga: "Tistega, ki neupravičeno reproducira, da na voljo javnosti, razširja ali da v najem eno ali več izvedb, fonogramov, videogramov, rtv-oddaj ali podatkovnih baz, katerih skupna tržna cena pomeni večjo premoženjsko vrednost, se kaznuje z zaporom do treh let." Kazenska zakonodaja se spreminja vsakih nekaj let in inkriminira nova kazniva dejanja, medtem pa se določena nova kazniva dejanja ljudem zdijo popolnoma sprejemljiva. Tako je tudi s kibernetsko kriminaliteto, v zadnjem času pa predvsem s spreminjanjem zavesti o piratstvu, ki pomeni kršenje avtorskih pravic. Večina mladih v Sloveniji piratstvo še vedno dojema kot nekaj povsem običajnega in sprejemljivega. Kibernetsko kriminaliteto je treba analizirati z vidika storilcev, žrtev in okoliščin kaznivega dejanja. Poleg tega je treba upoštevati tudi strah pred kriminaliteto, ki močno vpliva na zaznavanje negativnih pojavov in odzivanje ljudi nanje. Strah pred določenimi vrstami kriminalitete ne obstaja, če določenih virov ogrožanja ljudje ne poznajo, na drugi strani pa je senzibiliziranje ljudi z določenimi odklonskimi ravnanji vzrok za preburno odzivanje na grožnje informacijski varnosti (Završnik, 2010: 120). Strah pred (kibernetsko) kriminaliteto je povezan s posameznikovo oceno lastnega tveganja za viktimizacijo in oceno odprave škode, ki jo oseba utrpi z viktimizacijo (Meško et al., 2009: 293). Glede na to, obstaja neskladje med statistiko kibernetske kriminalitete (majhna zaznanost) ter vplivi medijev in osebnimi izkušnjami uporabnikov kibernetskega prostora.

D'Arcy s sodelavci (2009: 81) meni, da je za zmanjšanje neutemeljenega strahu pred kibernetsko kriminaliteto treba uporabnike ozavestiti, zato predlaga uporabo treh varnostnih ukrepov za zmanjšanje ogroženosti in strahu pred kibernetsko kriminaliteto:

– povečanje uporabnikovega poznavanja mogočih groženj,
– izobraževanje o varnosti in
– ozaveščanje uporabnikov o samovarovanju.

Enega izmed takih programov izvaja organizacija Enisa (2011), v Sloveniji pa so med bolj kakovostnimi in bolj dejavnimi ponudniki spletnih varnostnih storitev Safe.si (2011), Varni na internetu (2011) in Spletno oko (2011). Različna raven zavedanja o grožnjah in poznavanja načinov obrambe pred viri ogrožanja v kibernetskem prostoru se, kot ugotavljajo Bulgurcu et al. (2010: 526), odraža v obnašanju posameznika v kibernetskem prostoru.

Zavedanje o možnostih ogrožanja v kibernetskem prostoru in strah pred kibernetsko kriminaliteto sta odvisna od poznavanja virov ogrožanja pri posamezniku in od njegovega dojemanja groženj, ki prežijo nanj pri delu v kibernetskem prostoru. Poudariti velja, da najnovejše raziskave (Ponemon, 2011) kažejo veliko izpostavljenost kibernetski kriminaliteti in visoke stroške, ki so povezani z odpravljanjem posledic. Dejansko se stopnja kibernetskih napadov stalno povečuje oziroma so ti napadi bolj sistematično spremljani. Omenjena raziskava (Ponemon, 2011) ugotavlja kar 44-odstotno povečanje kibernetskih napadov v primerjavi z letom poprej. Zato je poznavanje stanja in zavedanje o ogroženosti nujno, če želimo zmanjšati vplive groženj na posameznika in podjetja. V nadaljevanju so predstavljeni rezultati raziskave, ki ugotavljajo uporabo računalnika, dojemanje virov ogrožanja in strah uporabnikov pred kibernetsko kriminaliteto.

3 Metoda

Z namenom, da bi bolje spoznali poznavanje, razumevanje in dojemanje kibernetskih groženj in strah pred kibernetsko kriminaliteto v Sloveniji, smo med slovenskimi uporabniki interneta izvedli spletno anketo. Vprašalnik je poleg splošnih podatkov o respondentih sestavljen iz dveh delov, in sicer iz vprašanj o poznavanju in razumevanju kibernetske kriminalitete in zavedanju o njej oziroma iz vprašanj o mogočih virih ogrožanja na internetu in o strahu pred kibernetsko kriminaliteto. Raziskavo o poznavanju kibernetske kriminalitete v Sloveniji, zavedanju o njej in strahu pred njo smo izvedli s spletno anketo (izdelana in izpolnjevana v Google docs) med uporabniki interneta marca 2011 (anketa je bila aktivna 15 dni). Ciljna populacija anketiranja so bili uporabniki spleta, ki iščejo informacije o njegovi varni rabi. Udeležence smo k sodelovanju povabili z objavo obvestila o izvajanju ankete na profilu Facebook Fakultete za varnostne vede in na forumu na straneh organizacije RIS (RisOrg, 2011). Statistična analiza podatkov je bila opravljena s pomočjo programa SPSS. Tabela 1 prikazuje značilnosti vzorca.

Tabela 1: Značilnosti vzorca anketiranih uporabnikov svetovnega spleta

Demografske značilnosti	ΣN = 277	N	%
Starost	manj kot 20	23	8,3
	21–30	214	77,3
	31–40	22	7,9
	več kot 40	18	8,3
Spol	ženske	184	66,4
	moški	93	33,6
Izobrazba	osnovnošolska	6	2,2
	srednješolska	203	73,3
	univerzitetna	48	17,3
	podiplomska	20	7,2
Regionalne skupine	1000 Ljubljana	96	34,7
	2000 Maribor	52	18,8
	3000 Celje	34	12,3
	4000 Kranj	31	11,2
	5000 Nova Gorica	15	5,4
	6000 Koper	17	6,1
	8000 Novo mesto	12	4,3
	9000 Murska Sobota	20	7,2

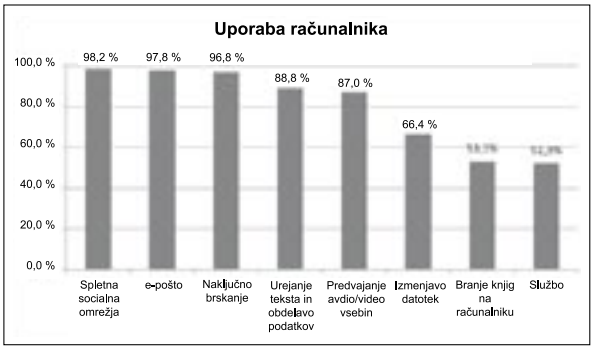
4 Rezultati

V nadaljevanju predstavljamo rezultate spletne ankete. Tabela 2 prikazuje časovno uporabo računalnika, graf 1 pa, da večina uporabnikov uporablja računalnik za sodelovanje v spletnih socialnih omrežjih, pošiljanje elektronske pošte in naključnega iskanja informacij na svetovnem spletu, in sicer tako na delovnem mestu kot doma.

Tabela 2: Dnevna uporaba računalnika

Čas rabe v urah	> 1	1–2	2–4	4–8	< 8
Računalnika	11,6 %	21,3 %	33,2 %	26,7 %	7,2 %
Interneta	20,9 %	26,7 %	31,4 %	16,6 %	4,3 %

Poleg tega približno polovico celotnega časa dela z računalnikom uporabniki porabijo v službi (52,3 odstotka), ostalo (47,7 odstotka) pa je uporaba za zasebne namene.



Graf 1: Uporaba računalnika

Uporabnikom se zdi uporaba računalnika pri delu, izmenjevanju podatkov in pregledu multimedijskih vsebin večinoma varna, pri direktni interakciji s spletom in izmenjevanju splošnih podatkov pa nevarna (tabela 3).

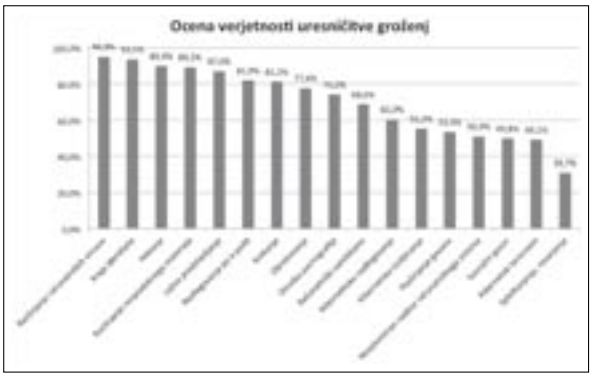
Tabela 3: Varnost rabe računalnika pri posameznih dejavnostih v kibernetskem prostoru

Raba računalnika je varna/nevarna pri:	Varna	Nevarna
internetnem izmenjevanju podatkov	61	216
prenosu glasbe/filmov	71	206
e-bančništvu	78	199
sprotnem sporočanju	82	195
spletnem nakupovanju	87	190
izmenjevanju e-pošte	102	175
naključnem brskanju po spletu	114	163
naključni rabi programov za prosti čas	134	143
igranju spletnih iger	141	136
naključni rabi poslovnih programov	162	115
namenskem brskanju po spletu	172	105
izmenjevanju poslovnih podatkov	173	104
delu	178	99
predvajanju glasbe/filmov	184	93
branju e-knjig/člankov	203	74
uporabi orodij Pisarne	229	48

4.1 Poznavanje kibernetskih groženj

Uporabniki so na vprašanja o poznavanju kibernetskih groženj odgovarjali pri vprašanjih z več mogočimi odgovori in izbiro vrednosti. Navedene so bile posamezne kategorije,

uporabniki pa so označili tisto, ki jo poznajo oziroma so bili vanjo vpleteni. Ko pogledamo, kako vprašani ocenjujejo grožnje varnosti informacij (graf 2), pa ugotovimo, da veliko vprašanih posamezne grožnje pozna.



Graf 2: Ocena verjetnosti ogrožanja

Osumljenci kaznivih dejanj kibernetske kriminalitete imajo po mnenju vprašanih nedokončano srednjo (25,6 odstotka), srednjo (38,3 odstotka) ali univerzitetno izobrazbo (34,4 odstotka). Glede na zaposlitveni status pa naj bi bili dijaki (14,8 odstotka), študentje (33,2 odstotka), zaposleni (26 odstotkov) ali nezaposleni (26 odstotka). Pri tem naj bi jih po mnenju vprašanih skupno kar 86,6 odstotka izhajalo iz srednjega družbenega sloja. Motivi storilcev so glede na oceno vprašanih prikazani v grafu 3.

Graf 3: Ocena motivov storilcev kibernetske kriminalitete

Poznavanje afer (tako domačih kot mednarodnih) s področja kibernetske kriminalitete, ki so bile odmevne v Sloveniji v zadnjem obdobju, je med vprašanimi dobro, saj 26 odstotkov vprašanih ni poznalo nobene od naštetih afer, poznavanje posamezne navedene afere pa je med 21,7 in 56 odstotki. Kar 82,7 odstotka vprašanih se je z aferami seznanilo po spletu, 63,9 odstotka od prijateljev, 61,2 odstotka na televiziji, na druge načine (strokovne revije, knjige, radio) pa manj kot 30 odstotkov.

Ugotavljamo, da uporabniki poznajo in uporabljajo zaščitno programsko opremo računalniških sistemov in komunikacij. Skoraj vsi (98,9 odstotka) navajajo, da uporabljajo požarne zidove (verjetno je pomembno dejstvo, da so vgrajeni v sodobne operacijske sisteme in jih je treba zgolj aktivirati), 94,9 odstotka pa jih uporablja protivirusne programe, ki jih tudi stalno posodabljajo (ali imajo nastavljeno avtomatsko posodabljanje). Druge posamezne, dodatne vrste zaščite, kot so na primer varnostni popravki operacijskega sistema, antispyware programe, kriptiranje vsebin in drugo, uporablja manj kot 20 odstotkov vprašanih. Čeprav se vprašani v veliki meri zadržujejo na spletu, pa relativno malo poznajo glavne spletne strani, ki v Sloveniji skrbijo za ozaveščanje uporabnikov o kibernetski kriminaliteti. Dobra polovica uporabnikov pozna spletne strani slovenske policije (56,3 odstotka) (www.policija.si) in strani nevladne organizacije Spletno oko (30,3 odstotka www.spletno-oko.si), vse ostale naštete spletne strani pa pozna 15,3 odstotka uporabnikov ali manj.

4.2 Dojemanje kibernetskih groženj – faktorska analiza

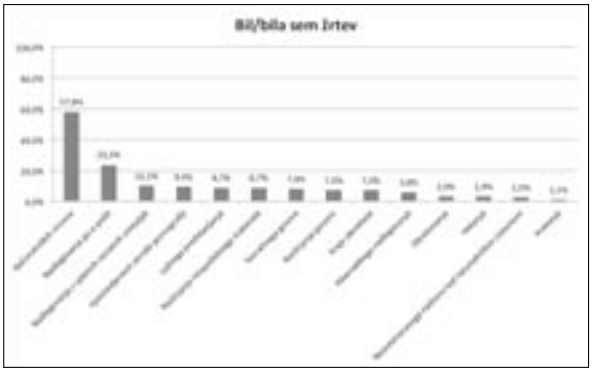
Strah pred kriminaliteto smo razdelili v tri skupine, vanje pa uvrstili posamezne spremenljivke, ki so jih vprašani ocenili na 5-stopenjski lestvici z vrednostmi od 1 do 5 (1 = me sploh ni strah, 5 = zelo me je strah). Izvedli smo faktorsko analizo (metoda glavnih komponent), s katero smo spremenljivke razvrstili na tri (pričakovane) faktorje s pomočjo pravokotne rotacije (Varimax z normalizacijo Kaiser). Rezultati so prikazani v tabeli 4.

Tabela 4: Faktorska analiza mogočih virov ogrožanja v kibernetskem prostoru

Cronbachov Alfa koeficient: 0,945 Kaiser-Meyer-Olkinov koeficient ustreznosti vzorčenja: 0,909					
F1: Neprimerno vedenje					
Cronbachov Alfa koeficient: 0,914 Odstotek pojasnjene variance: 53,833 Povprečna vrednost: 2,7092; standardni odklon: 0,92751					
	F1	F2	F3	Aritm. sr.	St. odkl.
Razširjanje govoric	,830			2,7619	1,0403
Lažno predstavljanje	,818			3,0586	1,0986
Sovražni govor	,729			2,5182	1,0092
Kraja identitete	,674			3,4908	1,0383
Spletkarjenje	,614			2,3650	0,8516
Otroška pornografija	,584			2,6423	1,0631
Kibernetski terorizem	,544			2,5927	1,0383
Klevetanje	,479	–,456		2,4396	0,9785
F2: Nadlegovanje					
Cronbachov Alfa koeficient: 0,901 Odstotek pojasnjene variance: 8,827 Povprečna vrednost: 2,3109 standardni odklon: 0,98861					
	F1	**F2**	F3	Aritm. sr.	St. odkl.
Nadlegovanje po e-pošti		–,891		2,1745	0,8502
Kibernetsko nadlegovanje (na primer soc. mreže)		–,887		2,2000	0,8407
Izsiljevanje v kibernetskem prostoru		–,802		2,2299	0,8961
Širjenje nespodobnega materiala po spletu	,370	–,460		2,4359	1,0123
F3: Aktivno ogrožanje					
Cronbachov Alfa koeficient: 0,875 Odstotek pojasnjene variance: 7,517 Povprečna vrednost: 3,0153; standardni odklon: 0,93113					
	F1	F2	**F3**	Aritm. sr.	St. odkl.
Krekerstvo			,932	2,7709	0,9075
Hekerstvo			,887	2,7766	0,9861
Neavtoriziran prevzem nadzora nad rač.			,639	3,1709	0,9840
Računalniški virusi			,607	3,6007	0,9763
Računalniški vandalizem, odtujitev			,589	2,7600	0,9804

V okviru prvega faktorja obstaja občutek možnosti viktimizacije oziroma strah pred mogočimi viktimizacijami v kibernetskem prostoru, pri čemer je na prvem mestu kraja identitete, sledijo lažno predstavljanje, razširjanje govoric, otroška pornografija, kibernetski terorizem, sovražni govor, klevetanje in spletkarjenje. Drugi faktor kaže, da se uporabniki bojijo tudi nadlegovanja pri uporabi kibernetskega prostora, pri čemer si viri ogrožanja sledijo takole: nadlegovanje po e-pošti, nadlegovanje v okviru socialnih omrežij, izsiljevanje in širjenje nespodobnega materiala na spletu. Tretji faktor kaže na dejavno ogrožanje, kjer so na prvem mestu računalniški virusi, sledijo neavtorizirani prevzem nadzora nad računalnikom, hekerstvo, krekerstvo in računalniški vandalizem oziroma odtujitev računalnika. Ti viri ogrožanja v kibernetskem prostoru so se pokazali kot veljavni v okviru preučevanega vzorca. Poleg tega je treba poudariti visoke vrednosti Cronbachovega Alfa koeficienta zanesljivosti, več kot 0,90, kar pomeni, da bi ponovitev take študije dala podobne rezultate.

Podatki o žrtvah posameznih ogrožanj v kibernetskem prostoru so predstavljeni v grafu 4.



Graf 4: Žrtve posameznih ogrožanj

Pri žrtvah posameznih kibernetskih ogrožanj lahko zaradi razširjenosti izvzamemo okuženost z virusi (57,8 odstotka) in nadlegovanje po e-pošti (večinoma SPAM in serijska pisma). Z drugimi elementi se je srečalo manj kot 10 odstotkov oseb (graf 4).

5 Razprava

Uporaba računalnikov, mobilnih naprav, njihovo povezovanje v internet in stalno izmenjevanje podatkov so postali stalnice našega vsakdana (Markelj in Bernik, 2011). Dostop do informacij in povezovanje med uporabniki se je s pojavom kibernetskega prostora popolnoma spremenilo, to pa pomembno vpliva na naše delo, komunikacije in obnašanje v družbi. Eno izmed osnovnih orodij za dostop v kibernetski prostor je računalnik, ki ga vprašani največ uporabljajo (graf 1) za dostop do spletnih socialnih omrežij, za e-pošto, brskanje po spletu in urejanje dokumentov. Visoki so odstotki za ogled avdio/video vsebin (87 odstotkov) na spletu, izmenjevanje datotek p2p (66,4 odstotka) in branja na računalniku (53,1 odstotka). Delež večinoma nelegalne izmenjave datotek in njihove rabe kaže na dojemanje sodobnih uporabnikov avtorsko zaščitenih vsebin, saj je splošno mnenje, da je vse, kar je dostopno po internetu, prosto, brezplačno. Ta odnos se prenaša tudi na branje na računalniškem zaslonu, kjer se jasno nakazuje, da prihajajoče generacije od tradicionalnega branja in spremljanja medijev prehajajo na branje in povezovanje v kibernetskem prostoru. Tako dejstvo, da velika večina (98,2 odstotka) uporablja spletna socialna omrežja, ni presenetljivo, ampak je posledica dejstva omenjenega prehoda iz tradicionalnega v kibernetski prostor.

Seveda se skladno s prenosom dela in podatkov v kibernetski prostor prenašajo tudi različne oblike kriminalitete. Pojavljajo pa se tudi nove oblike kriminalitete, na primer povezane s spletnimi socialnimi omrežji, saj na primer "količina osebnih podatkov, ki jih posamezniki izmenjujejo in objavljajo na internetu, hitro narašča, zlasti z vse večjo priljubljenostjo spletnih socialnih omrežij" (Dimc in Dobovšek, 2010: 395). Posebnih zaključkov iz rezultatov (tabela 3) glede na razpršenost ni moč izvesti, kar na neki način nakazuje, da je kljub znanju uporabnikov pri uporabi računalniških orodij in delu v kibernetskem prostoru zavedanje na področju informacijske varnosti relativno majhno. Primer je lahko e-bančništvo, ki se zdi večini nevarno, v resnici pa je zlorab pri spletnem bančništvu relativno malo, pa še te so večinoma posledica neodgovornega odnosa do sistemov dostopa do e-banke, ne pa posledica nezadostne ali neučinkovite zaščite, vgrajene v e-bančne sisteme. Ravno obratno pa je razumevanje uporabe računalnika pri delu, kjer večina meni, da drugi poskrbijo za ustrezno raven zaščite, pri tem pa pozabljajo na osnovno dejstvo, da pri današnjem delu večina zlorab izhaja iz nezavedanja ali brezbrižnosti ljudi, ki računalnike, priključene v internet, uporabljajo, saj z informacijskimi sredstvi večinoma ravnajo nevestno (McCullagh in Caelli, 2005: 336).

Od tega, koliko se ljudje zavedajo mogočih posledic, pa je odvisen tudi strah pred kriminaliteto. Meško in Šifrer (2008: 559) ugotavljata, da strah pred kriminaliteto ni odvisen od dejanskega obsega kriminalitete. Zaključimo torej lahko, da je strah pred kibernetsko kriminaliteto odvisen od posameznikovega zavedanja, kako se posledice dejanj v kibernetskem prostoru odražajo v njegovem življenju. Rezultati raziskave kažejo, da je poznavanje oblik kibernetske kriminalitete dokaj dobro, vendar pa uporabniki bolj poznajo medijsko izpostav-

ljene grožnje (graf 2) kakor pa tiste, pred katerimi bi se dejansko morali zaščititi. Te so računalniški virusi, kraja identitete, hekerstvo (primer slovenskih hekerjev pozimi 2010/11 (FT, 2011)), širjenje nespodobnega materiala (preiskava o vpletenosti člana parlamenta v širjenje nespodobnega materiala jeseni 2010 (RTVSLO, 2011)) in podobno. Manj poznane pa so javno manj izpostavljene grožnje, ki so pomemben faktor pri odgovornem obnašanju pri kibernetskih komunikacijah in zavedanju odgovornosti ter hkrati tudi pri razumevanju kibernetske kriminalitete in ogroženosti posameznika. Te grožnje pomenijo tudi strah posameznika pred mogočim ogrožanjem njegovega sistema in posledice, ki pri tem nastanejo. Omenjeno je posledica pomanjkanja znanja na posameznih področjih, ki izhaja iz dejstva, da je danes tehnologija dostopna prav vsakomur, postopki dela pa so poenostavljeni do te mere, ko uporabnik naprave in komunikacijske sisteme lahko uporablja brez vsakega predznanja in tako ne razume, kaj se v kibernetskem prostoru dejansko dogaja. Ker ne razume dogajanja, tudi ne uporablja ustrezne, vsaj nujno potrebne zaščite. Na ta način uporabniki kibernetskim kriminalcem pomagajo pri zlorabah oziroma s svojim neznanjem ali brezbrižnostjo pogojujejo svojo viktimizacijo. Glede na predhodne raziskave in podane ugotovitve je uspešna zaščita in s tem manjša ogroženost posameznika le v njegovem ustreznem in odgovornem obnašanju v kibernetskem prostoru.

O tem, da je žrtev kibernetske kriminalitete lahko vsakdo, kdor uporablja računalnik, se strinja 49,8 odstotka vprašanih. To nakazuje na majhno ozaveščenost, na neki način pa tudi na dejstvo, da se za računalnikom v zasebnem prostoru, stran od javnosti, mnogi počutijo varne in se jim zdi, da kibernetski prostor nima stika z realnostjo in je ločen od realnega dogajanja. Ocena vprašanih, kdo je po njihovem mnenju glavni storilec kaznivih dejanj v kibernetskem prostoru, je v primerjavi s policijsko statistiko (Policija, 2011) zanimiva, saj vprašani ocenjujejo, da so storilci kaznivih dejanj večinoma mladi izobraženi moški, ki imajo relativno visoko stopnjo izobrazbe (srednjo ali univerzitetno izobrazbo), izhajajo pa iz dokaj urejenih socialnih okolij; 72,6 odstotka vprašanih meni, da so glavni storilci moški v starostnem obdobju med 21 in 30 let (94,2 odstotka). Policijski podatki so delno drugačni, saj je porazdelitev starosti po statistiki osumljencev naslednja:

- 5 odstotkov je starih manj kot 16 let,
- 20 odstotkov je starih med 16 in 17 let,
- 35 odstotkov je starih med 18 in 23 let,
- 20 odstotkov je starih med 24 in 33 let,
- 20 odstotkov je starih več kot 33 let.

Med osumljenci se pojavlja 25,4 odstotka žensk. Na podlagi teh podatkov lahko sklepamo, da klasični stereotip mladega hekerja, ki ves čas preživi za računalnikom in ga socialno okolje popolnoma nič ne zanima, ni upravičen. Večina kibernetske kriminalitete ima po zadnjih raziskavah namen pridobiti materialne koristi (Ponemon, 2011), pri čemer so finančne izgube, predvsem podjetij, ogromne. Z vidika strahu pred kibernetsko kriminaliteto (tabela 4) je najbolj izpostavljena skupina "aktivno ogrožanje" posledično z materialno škodo kot rezultatom ogrožanja. Očitno je premoženjska ogroženost še vedno tista, ki posameznike najbolj skrbi oziroma najbolj prizadene, manj pa neprimerno obnašanje in nadlegovanje. Po pregledu statističnih elementov faktorske analize ugotavljamo, da spremenljivke ustrezno oblikujejo faktorje, ki so medsebojno povezani, zato je bila tudi izbrana metoda poševne rotacije. Opozoriti je treba na spremenljivki kibernetski terorizem in klevetanje, ki sta v F1: odklonsko vedenje, čeprav bi kibernetski terorizem lahko razvrstili tudi v aktivno ogrožanje. To je seveda odvisno od tega, kako uporabniki razumejo kibernetski terorizem, vsekakor pa gre za neprimerno vedenje. Spremenljivka klevetanje pa ima visoko vrednost tudi za razvrstitev v F2: nadlegovanje, vendar klevetanje le ne nadleguje posameznika direktno. Če še pogledamo vrednosti odstotkov variance, ugotovimo, da bi glede na vrednosti odstotkov pojasnjene variance lahko imeli le eno faktorsko strukturo, na primer strah pred kibernetsko kriminaliteto. Vendar je zaradi ujemanja spremenljivk znotraj posameznih faktorjev smiselno obdržati predstavljene faktorje.

Motivi storilcev kibernetske kriminalitete (graf 3) naj bi bili osredotočeni na izziv, maščevanje in dokazovanje napak, manj pa na rivalstvo, protest in medijsko pozornost. Rezultati mnenj so podobni poznanim dejstvom o odkritih storilcih in raziskavam v zadnjem obdobju (na primer GartnerGroup, 2011). Ugotavljamo, da se motivi storilcev od izziva dokazovanja selijo v smer pridobivanja materialne koristi. Rezultati naše raziskave kažejo, da vprašani večinoma ne razmišljajo o kibernetski kriminaliteti kot eni izmed glavnih groženj, ki bodo v prihodnje prežale na nezavedne uporabnike kibernetskega prostora, saj se kot motiva vse bolj pojavljata pohlep in denar. To sta tudi glavna vzroka sodobne kibernetske kriminalitete, zlasti kraje identitete, uporabe SPAM-a in bootnetov.

Pri primerjanju rezultatov iz grafa 4 ter izobrazbe in starosti ugotovimo, da se vprašani z višjo stopnjo izobrazbe in/ali višjo starostjo manj bojijo kibernetetske kriminalitete. To je očitno posledica boljšega znanja in izkušenosti ter na podlagi tega višje stopnje ozaveščenosti ter boljše zaščite računalnika z elementarnimi programi in orodji za zaščito. Ljudje, ki več časa posvetijo resnemu delu z računalnikom in se zavedajo pomembnosti varnosti tega in vrednosti shranjenih podatkov, posvetijo del časa tudi njihovi zaščiti. Tako se kljub večji izpostavljenosti počutijo manj ogrožene. V Sloveniji je prijavljene in obravnavane kibernetske kriminalitete relativno malo (Policija, 2011). To pa ne pomeni, da se uporabniki manj bojijo oziroma da se groženj ne zavedajo in da ne upoštevajo

dejavnikov tveganja. Pri tem poudarjamo, da je manjša ogroženost iz kibernetskega prostora v Sloveniji tudi posledica slovenskega jezika, saj jezik aktivno obvlada le 2 milijona ljudi in je s tem vsebina pred globalnimi grožnjami že jezikovno "kriptirana".

Da bi zmanjšali možnost pojava kibernetske kriminalitete in drugih kibernetskih viktimizacij, IC3 (2010) predlagajo:

– previdnost pri odpiranju spletnih povezav, ki so jih dobili v e-pošti, predvsem iz neznanih spletnih naslovov. Na ta način se preprečijo nameščanje trojanskih programov, ribarjenje, škodljive kode, s čimer se zmanjša ogroženost računalnika in shranjenih podatkov;

– zavedanje, da z objavo zasebnih podatkov uporabniki omogočajo njihovo zlorabo. Taki podatki se lahko uporabijo za razumevanje uporabnikovega vedenja in načina dela, omogočajo pa tudi manipulacijo z uporabniki in prevzem identitete;

– preverjanje identitete osebe, ki od uporabnika želi pridobiti pomembne podatke (telefonsko preverjanje, povratno sporočilo);

– previdnost pri nameščanju dodatkov in aplikacij na računalnik in mobilne naprave. Če uporabnik ne pozna funkcij dodatkov in aplikacij, naj jih ne namešča, saj nekateri odpirajo vstop v sistem po omrežju in s tem omogočajo krajo osebnih in/ali poslovnih informacij;

– skrb za posodabljanje antivirusnih programov in požarnega zidu ter njuno stalno delovanje;

– gesla in PIN-kode se ne zaupajo nikomur. Preprečiti je treba možnost, da jih dobijo nepooblaščene osebe. Zelo je priporočljiva pozornost pri shranjevanju in upoštevanje zasebnosti pri njihovem vpisovanju;

– redno menjavanje gesel. Ta naj bodo dovolj kompleksna in naj ne bodo sestavljena iz splošnih z vami povezanih dejstev (imena, datumi rojstev, obletnice);

– uporabo zdravega razuma pri dostopu do kibernetskega prostora in povezovanju v njem. Ugodne ponudbe, milijonski zadetki na loteriji, ki od uporabnika za nadaljevanje postopka zahtevajo podatke ali nakazilo, so praviloma goljufija.

Izobraževanje in usposabljanje o nevarnosti kibernetske kriminalitete mora na vseh ravneh družbenega življenja postati del vsakdana, za usposobitev ozaveščenega posameznika, ki premišljeno in odgovorno uporablja internet brez strahu pred zlorabo. Določena mera strahu je sicer koristna, saj se s tem poveča pazljivost uporabnika pri delu z računalnikom, s tem pa se zmanjša ogroženost. Kljub temu pa ni smiselno preveč zmanjševati strahu, ker lahko pride do nasprotnega učinka (Meško in Areh, 2003: 257).

Ugotavljamo, da obstaja splošno pomanjkanje ozaveščenosti o kibernetski kriminaliteti in kibernetski zakonodaji med ljudmi, ki stalno uporabljajo informacijsko komunikacijske tehnologije tako za službene kot zasebne namene. Za zmanjšanje strahu pred kibernetsko kriminaliteto in dvig zavedanja o njenem obstoju morajo biti uporabniki seznanjeni z njegovimi pojavnimi oblikami, kot so na primer spreminjanje spletnih strani, nepooblaščen dostop do omrežja, kibernetsko nadlegovanje, internetne goljufije, kraja identitete, otroška pornografija, prestrezanje e-pošte, izdelava ponarejene e-pošte in kraja gesel.

Literatura in viri

1. Alshalan, A. (2005). Cyber-crime fear and victimization: an analysis of a national survey. Pridobljeno 13. aprila 2011, http://www.cse.msstate.edu/~dampier/study%20materials/NationalCrimeStats.pdf.
2. Bulgurcu, B., Cavusoglu, H., in Benbasat, I. (2010). Information security policy compliance: an numerical study of rational-based beliefs and information security awereness. **MIS Quarterly**, vol. 34, 523-A7.
3. Cockcroft, T. (2009). Late modernity, risk and the construction of fear of crime. V: G. Meško, T. Cockcroft, A. Crawford in A. Lemaitre (ur.), **Crime, Media and Fear of Crime.** Ljubljana: Tipografija, str. 13–26.
4. D'Arcy, J., Hovan, A., in Galletta, D. (2009). User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. **Information Systems Research**, vol. 20, str. 79–98.
5. Dimc, M., in Dobovšek, B. (2010). Perception of cyber crime in Slovenia. **Varstvoslovje**, 12(4), str. 378–396.
6. ENISA. (2011). Securing Europe's Information Society. Pridobljeno 21. aprila 2011, http://www.enisa.europa.eu/.
7. FT. (2011). Police shut down Mariposa hacker ring. Pridobljeno 11. julija 2011, http://www.ft.com/cms/s/0/f6960e5a-2711-11df-b84e-00144feabdc0.html.
8. GartnerGroup (2011). Security Risk Management. Pridobljeno 29. aprila 2011, http://www.gartner.com/technology/research/security-risk-management.jsp.
9. Gradišar, M., in Lamberger, I. (2010). Vpliv represivnih dejavnikov na zlorabe kreditnih in plačilnih kartic v Sloveniji. **Revija za kriminalistiko in kriminologijo**, 61(1), str. 28–36.
10. IC3. (2010). IC3 – Internet Crime Complaint Center. 2010 Internet Crime Report. Annual Report. Washington DC. NW3C – White Collar Crime Center. Pridobljeno 28. julija 2011, http://www.ic3.gov/media/annualreport/2010_ic3report.pdf.
11. Kanduč. Z. (2005). Postmoderne nevarnosti, bojazni in "dobri sovražniki"**. Revija za kriminalistiko in kriminologijo,** 56(4), str. 337–347.
12. Kazenski zakonik [KZ-1]. (2008). **Uradni list RS**, št. 55/08.
13. KZ-1B. (2011). Predlog zakona o spremembah in dopolnitvah Kazenskega zakonika. Pridobljeno 27. julija 2011, http://www.dz-rs.si/index.php?id=101&type=98&cl=K&mandate=-1&unid=PZ|E0DCFCF0B2BB10A0C12578A3004E5114.
14. Markelj, B., in Bernik, I., (2011). Kombinirane grožnje informacijski varnosti pri rabi mobilnih naprav. Nove razmere in priložnosti v informatiki kot posledica družbenih sprememb [Elektronski vir]: zbornik konference / 18. konferenca **Dnevi slovenske informatike, Portorož**, Slovenija, 18.–20. april 2011.

15. McCullagh, A., in Caelli, W. (2005). Who Goes There? Internet Banking: A Matter of Risk and Reward, V: C. Boyd in J. M. Nieto Gonzalez (ur). **Information security and privacy: 10th Australasian conference, ACISP 2005.** Berlin Heidelberg: Springer-Verlag, str. *336–357*.
16. Meško, G. (2000). Miti o kriminaliteti v ZDA. **Revija za kriminalistiko in kriminologijo**, 51(4), str. 305–313.
17. Meško, G., in Areh, I. (2003). Strah pred kriminaliteto v urbanih okoljih. **Revija za kriminalistiko in kriminologijo**, 54(3), str. 144–152.
18. Meško, G., Hirtenlehner, H., in Vošnjak, L. (2009). Izkušnje s kriminaliteto in občutek ogroženosti v Linzu in Ljubljani – preskus kognitivne teorije strahu pred viktimizacijo. **Revija za kriminalistiko in kriminologijo**, 60(4), str. 292–308.
19. Meško, G., Petrovec, D., Areh, I., Muratbegovič, E., Rep, M. (2006). Strah pred kriminaliteto v Sloveniji in Bosni in Hercegovini – izidi primerjalne študije. **Revija za kriminalistiko in kriminologijo**, 57(1), str. 3–14.
20. Meško, G., in Šifrer, J. (2008). Fear of crime in urban settings – an inquiry. **Varstvoslovje**. 10(4), str. 550–560.
21. Peršak, N. (2009).Virtualnost, (ne)moralnost in škodljivost: normativna vprašanja nekaterih oblik kibernetične kriminalitete. **Revija za kriminalistiko in kriminologijo**, 60(3), str. 191–198.
22. Policija. (2011). Kriminaliteta. Pridobljeno 17. aprila 2011, http://www.policija.si/index.php/statistika/kriminaliteta.
23. Ponemon. (2011). **Second Annual Cost of Cyber Crime Study**: Benchmark Study of U.S. Companies, Ponemon Institute.
24. RisOrg. (2011). Raba interneta v Sloveniji. Pridobljeno 11. julija 2011, http://www.ris.org/
25. Roche, E. M., in Van Nonstrand, G. (2008). **Information Systems, Computer Crime & Criminal Justice**. Barraclough Ltd., Kalifornija.
26. RTVSLO (2011). Turk: Pri Magajni gre za zastraševanje. Pridobljeno 28. julija 2011, http://www.rtvslo.si/slovenija/turk-pri-magajni-gre-za-zastrasevanje-strajn-politicne- zarote-ni/243120.
27. SafeSi. (2011). SAFE-SI, varna raba interneta. Pridobljeno 11. aprila 2011, http://www.safe.si/.
28. Spletno Oko. (2011). Spletno Oko. Pridobljeno 3. maja 2011, http://www.spletno-oko.si/.
29. Varni na internetu. (2011). Varni na internetu. Od mene je odvisno vse. Pridobljeno 14. marca 2011, http://www.varninainternetu.si/.
30. Wall, D. S. (2009). The role of the media in generating insecurities and influencing perceptions of cybercrime. V: G. Meško, T. Cockcroft, A. Crawford in A. Lemaitre (ur.), **Crime, Media and Fear of Crime.** Ljubljana: Tipografija, str. 50–76.
31. Wall, D. S. (2008). Cybercrime, media and insecurity: the shaping of public perceptions of cybercrime. **International Review of Law, Computers and Technology**, 22(1-2), str. 45–63.
32. Young, J. (2007). **The vertigo of late modernity**. London: Sage.
33. Zakon o ratifikaciji Konvencije o kibernetski kriminaliteti in Dodatnega protokola h Konvenciji o kibernetski kriminaliteti, ki obravnava inkriminacijo rasističnih in ksenofobičnih dejanj, storjenih v informacijskih sistemih [MKKKDP]. (2004). **Uradni list RS**, (17/04).
34. Završnik, A. (2005). Kibernetična kriminaliteta – (kiber)kriminološke in (kiber)viktimološke posebnosti "informacijske avtoceste". **Revija za kriminalistiko in kriminologijo**, 56(3), str. 248–260.
35. Završnik, A. (2008). Boj za prevlado nad internetom – interno upravljanje in nadzorovanje. **Revija za kriminalistiko in kriminologijo**, 59(4), str. 321–338.
36. Završnik, A. (2010). Criminal justice systems` (over)reactions to IT security threats. V: BELLINI, Marcello (ur.). **Current issues in IT security** : proceedings of the interdisciplinary conference in Freiburg i. Br./Germany, 12.–14. maj 2009 (Interdisziplinäre Forschungen aus Strafrecht und Kriminologie, Bd. I 17). Berlin: Duncker & Humblot, str. 113–135.

Revija za kriminalistiko in kriminologijo / Ljubljana 62 / 2011 / 3, s. 242-252

Internet study of familiarity with cyber threats and fear of cybercrime

Gorazd Meško, Ph.D., Full Professor of Criminology and Dean of the Faculty of Criminal Justice and Security, University of Maribor, Kotnikova 8, 1000 Ljubljana, Slovenia.

Igor Bernik, Assistant Professor, Chair for the Information Security, Faculty of Criminal Justice and Security, University of Maribor, Kotnikova 8, 1000 Ljubljana, Slovenia.

The paper considers Slovene familiarity with cyber threats and cybercrime from the viewpoint of users' perception, awareness and their fear of crime. Wide access to and use of information and communication technologies and interactions of users by means of these technologies have opened the door to cyberspace, which has been misused by many for the commission of crimes. The increase of users has resulted in a growth of abuses but users are unfortunately rarely aware of dangers, on the one hand and, on the other, of possibilities of countering these threats effectively. The results of an internet survey carried out in March 2011 provide an insight into the perception of cybercrime and understanding of the fear of cybercrime. The findings of the survey, based on statistical analysis, show how respondents perceive cybercrime. It was established that respondents are relatively familiar with the notion of cybercrime but are more aware of threats highlighted by the media. In this connection, it must not be overlooked that these threats, which are widely known, do not necessarily represent a threat to the safety of users, although they nevertheless increase their fear of cybercrime. The paper provides principal guidelines, formulated on the basis of knowledge and research results, which, if taken into consideration, could curb risks in cyberspace. These guidelines provide a starting point for a larger awareness of dangers, as well as a source of instructions for the safer use of cyberspace. It is likely that better understanding of threats and greater knowledge of measures against them could reduce the fear of cybercrime. These findings have practical implications and are useful for the study of cybercrime, as well as for cyberspace users.

Key words: cybercrime, perception, awareness, fear of crime, information security, Slovenia

UDC: 343.3/.7: 004