Uvodnik

Spoštovane bralke in bralci!

Prihaja jesen in z njo tudi tretja številka revije Varstvoslovje. Zopet se bomo umaknili v zavetje toplih prostorov in sedli za računalnike, pri tem pa verjetno pozabili na varnost v kibernetskem prostoru. Na to nas bo spomnila večina prispevkov, ki je v prvem delu številke namenjena kibernetski kriminaliteti. Avtorja Aleksandar Ilievski in Igor Bernik v prispevku Boj proti kibernetski kriminaliteti v Sloveniji: organiziranost, način, pravna podlaga in njeno izpolnjevanje analizirata organiziranost in načine boja proti kibernetski kriminaliteti v Sloveniji, proučita pravne podlage za to področje in predstavita nacionalne statistične podatke o njenem uresničevanju. Pri tem izpostavita ključno vlogo Centra za računalniško preiskovanje pri preiskovanju kibernetske kriminalitete v Sloveniji in redko obravnavanje kibernetskih kaznivih dejanj v globalnem razcvetu kibernetske kriminalitete. V širšem kontekstu kibernetska kriminaliteta pomeni sodobno varnostno grožnjo v povezavi z ozaveščenostjo in delovanjem posameznika v kibernetskem prostoru. V prispevku Maje Dimc in Bojana Dobovška o percepciji kibernetske kriminalitete pri nekaterih uporabnikih interneta v Sloveniji in ZDA je izpostavljena problematika ozaveščenosti splošne javnosti na področju kibernetske kriminalitete v povezavi z njihovim preventivnim delovanjem v kibernetskem prostoru in odnosom do organov pregona, s ciljem opredelitve ključnih razlik med percepcijo, vedenjem in delovanjem posameznikov glede na njihovo fizično življenjsko okolje. Kibernetski sklop zaključuje prispevek Kaje Prislan in Igorja Bernika o socialno-psiholoških implikacijah kibernetskega terorizma, s katerim predstavita sinergijo učinkov nerealnih predstav o tehnologiji in terorizmu, realne sposobnosti in aktivnosti kibernetskih teroristov, hkrati pa opozorita na to sodobno grožnjo, ki je z vidika informacijske varnosti, predvsem na nacionalni ravni, ne smemo zanemariti. Kibernetski terorizem postaja vse pogostejša tematika medijev in polemičnih razprav. S senzacionalnim poročanjem namreč velikokrat povzročajo dramatične in nerealne asociacije na kibernetski terorizem, v smislu možnih scenarijev in posledic.

Drugi del številke izpostavlja del problematike poznomoderne družbe, kot so finančna kriminaliteta, staranje prebivalstva in kritične razdalje do neposrednega prenosa praks iz tujine, predvsem iz ZDA. Tanja Ahčan v prispevku Nadzor in regulacija bančnega sektorja: preventivni dejavnik boja proti finančni kriminaliteti opozori, da je finančna kriza razkrila številna odklonska ravnanja udeležencev globalnih finančnih trgov ter odprla množico kompleksnih pravnih in dejanskih vprašanj glede regulacije in nadzora finančnih trgov kot tudi uspešnosti kazenskega pregona odgovornih. Avtorica v prispevku ugotovi, da razloge za pomanjkljivosti oziroma šibkosti, katerih rezultat so bila odklonska ravnanja akterjev na finančnih trgih, ne gre iskati v normativni ureditvi *de lege lata*, temveč v pomanjkljivem nadzoru. Škodo finančne krize najtežje dojema starejša populacija, na kar opozorita Anton Toni Klančnik in Tinkara Pavšič Mrevlje v prispevku Kriminaliteta nad

starejšimi in izhodišča za varno staranje v Sloveniji. Ob prikazu projekcij staranja prebivalstva v naslednjih petdesetih letih izpostavita, da bo zagotovo prišlo tudi do povečanja kriminalitete nad starejšimi. Da bi bilo staranje v prihodnosti varnejše, preko statističnega pregleda opozarjata na najbolj rizična področja kriminalitete nad starejšimi. Rešitve iščeta v različnih preventivnih programih, usposabljanjih za delavce institucij, ki so v stiku s starejšimi žrtvami kaznivih dejanj, in programih psihosocialne in medicinske pomoči žrtvam. Drugi del številke zaključuje prispevek Igorja Areha s kritičnim razmislekom o Reidovi zasliševalski tehniki. Avtor opozori na vzpostavitev kritične distance do zasliševalskih tehnik, ki prihajajo predvsem iz ZDA. Ker je forenzična psihologija v Sloveniji slabo razvita, se tuje znanje s tega področja pogosto prenaša v naše okolje prenagljeno in brez poglobljenih strokovnih analiz, uporabniki tako prenesenega znanja pa so pogosto zavedeni. Pri tem opozarja, da današnja znanstvena dognanja in sodobni standardi varovanja človekovih pravic zavračajo uporabo Reidove tehnike, zato bi bilo treba tudi v slovenski preiskovalni praksi čim prej prevzeti in prilagoditi sodobne modele preiskovalnega intervjuvanja.

Številko zaključuje poročilo Maje Jere, Aleša Bučarja-Ručmana in Katje Eman o Nacionalni kriminološki konferenci Kriminaliteta, nered in družbeno nadzorstvo v času ekonomske krize – kriminološke refleksije, ki so jo 17. aprila 2013 organizirali člani Katedre za kriminologijo na Fakulteti za varnostne vede Univerze v Mariboru. Na konferenci je sodelovalo 18 predavateljev, ki so predstavili svoje poglede na dogajanje v Sloveniji v času krize kapitalističnega družbeno-ekonomskega sistema, sprememb demokratičnega političnega sistema in (pravne) države.

Zahvaljujeva se vsem, ki so sodelovali pri ustvarjanju številke, in vam želiva zanimivo branje.

Andrej Sotlar in *Bojan Dobovšek*
Urednika

Editorial

Dear readers

The fall has come and, with it, this year's third issue of the Journal of Criminal Justice and Security [Varstvoslovje]. From chilled nature we shall seek comfort in warm indoors and more frequently use computers and other electronic devices to pass the time. Protected against the cold, we should, nevertheless, not grow oblivious of the threats coming from cyber space; several papers from the first part of the current issue will see to that, drawing our attention to cybercrime. In Combating Cybercrime in Slovenia: Organization, Method, Legal Basis and its Implementation, Aleksandar Ilievski and Igor Bernik describe how Slovenia is tackling cybercrime. They focus on the legal framework put in place to combat it, use the national statistical data to demonstrate its implementation, highlighting the key role that the Center for computer investigation plays in investigating cybercrime, and point to the fact how rarely, indeed, the globally booming cybercrime is dealt with. In broad terms, it presents a modern security threat related to awareness levels and behaviours of individuals participating in cyberspace. The paper by Maja Dimc and Bojan Dobovšek discusses the perception of cybercrime in some internet users in Slovenia and in the United States, comparing the two very diverse and distant countries and showing the differences and similarities in awareness, preventive behaviours, and interaction with law enforcement. The cybercrime section of this issue ends with the paper authored by Kaja Prislan and Igor Bernik, giving an account of some socio-psychological implications of cyber-terrorism. They display the synergy of the effects of unrealistic notions about technology and terrorism, real skills, and activities of cyber terrorists, while warning us about this modern threat that, from the information security viewpoints, cannot be ignored, particularly not on the national level. Truly, cyber terrorism is becoming a frequent topic in debates and polemic discussions in the media, but on the other hand, sensational reporting often results in dramatic and far-fetched associations on cyber-terrorism made by the public, at least as regards possible scenarios and consequences.

The second section of this issue deals with some problems surging in late modernism, such as financial crimes and the aging population, emphasizing the importance of adopting a rather critical view of direct transfer of the practices from abroad, especially those from the U.S.

Paper Banking Sector Supervision and Regulation: A Preventive Factor in the Fight Against Financial Crime by Tanja Ahčan shows how the current financial crisis reveals numerous deviant behaviours of global financial market participants and brings to the fore a multitude of complex legal and factual issues regarding regulation and supervision of these markets, not to mention those related to effectiveness of criminal prosecutions of the responsible parties. She shows that the causes of the deficiencies or weaknesses resulting from deviant behaviours of financial market protagonists cannot be found in the legal framework, *de lege lata*, but can be attributed to both defective control and/or supervision. The

damage caused by the financial crisis is most difficult to perceive by the older population, as claimed by Anton Toni Klančnik and Tinkara Pavšič Mrevlje in their paper Crime against the Elderly and Guidelines for a Safer Aging in Slovenia. They show, by considering the projected aging of the population over the next fifty years, that there will certainly be an increase of crime against the elderly. To make ageing in the future safer, they present a statistical overview that defines the most risky facets of the crime against the elderly. Relevant solutions may also be sought for in various preventive programs, training programs for the staff of the institutions that come in contact with elderly victims of crime, and in programs of psychosocial and medical aid to the victims. This section of the current issue ends with a critical reflection on Reid interrogation techniques discussed by Igor Areh, who draws our attention to the need for establishing a critical distance towards interrogation techniques originating from abroad, mainly in the U.S. As forensic psychology in Slovenia is underdeveloped, foreign knowledge in this field is often transferred to our environment hastily and without any proper in-depth expert analysis, misleading even those who apply it. The author observes how current scientific knowledge and modern human rights standards reject the use of Reid interrogation techniques. It goes without saying Slovenian investigative practice should integrate modern models of investigative interviewing as soon as possible.

This year's fall issue concludes with a report on the National Criminological Conference: Disorder and Social Control in the Times of the Economic Crisis – a Criminological Reflection, held on April 17, 2013, as seen by Maje Jere, Aleš Bučar-Ručman, and Katja Eman. It was organized by the members of the Department of Criminology at the Faculty of Criminal Justice and Security, University of Maribor, hosting 18 speakers presenting their views on the events in Slovenia during the crisis of the capitalist socio-economic system, as well as those relating to the changes in the democratic political system, State, and the rule of law.

We thank all who participated in the creation of this issue and wish you a pleasant reading.

Andrej Sotlar and *Bojan Dobovšek*
Editors

VARSTVOSLOVJE,
let. 15
št. 3
str. 317–337

Boj proti kibernetski kriminaliteti v Sloveniji: organiziranost, način, pravna podlaga in njeno izpolnjevanje

Aleksandar Ilievski, Igor Bernik

Namen prispevka:

Številna poročila mednarodnih in nacionalnih organizacij iz zadnjega obdobja govorijo o hitrem in inovativnem razvoju kibernetske kriminalitete. V tem prispevku želimo analizirati organiziranost in način boja proti kibernetski kriminaliteti v Sloveniji, proučiti pravne podlage za to področje in predstaviti nacionalne statistične podatke o njenem uresničevanju.

Metode:

Splošne ugotovitve so oblikovane na podlagi pregleda literature, pregleda dejavnosti v Republiki Sloveniji, javnih, zasebnih in mednarodnih organizacijah, povezanih s kibernetsko in informacijsko varnostjo, pregleda zakonodaje ter dostopnih uradnih statističnih podatkov o kibernetski kriminaliteti.

Ugotovitve:

Ključno vlogo pri preiskovanju kibernetske kriminalitete v Sloveniji imajo Center za računalniško preiskovanje, Slovenski center za posredovanje pri omrežnih incidentih (SI-CERT) in Evropski center za kibernetsko kriminaliteto. V boj proti kibernetski kriminaliteti so vključene tudi druge državne, nepolicijske organizacije, zasebna informacijsko-varnostna podjetja, nevladne in mednarodne organizacije. Pravna podlaga za boj proti kibernetski kriminaliteti v Sloveniji je napredna in je del več nacionalnih in mednarodnih pravnih aktov. Največji problem, s katerim se srečujejo organi pregona, je redko obravnavanje kibernetskih kaznivih dejanj v globalnem razcvetu kibernetske kriminalitete, saj smo imeli v Sloveniji v zadnjih sedmih letih le nekaj obsodilnih obsodb.

Omejitve/uporabnost raziskave:

Prispevek proučuje boj proti kibernetski kriminaliteti v Sloveniji, vključujoč mednarodne organizacije, ki delujejo na območju države.

Izvirnost/pomembnost prispevka:

Na državni ravni še niso bili analizirani način, organiziranost in uspešnost boja proti kibernetski kriminaliteti. V prispevku izpostavljamo probleme, s katerimi se

srečuje Slovenija, in predlagamo priporočila za uspešnejši boj proti kibernetski kriminaliteti.

UDK: 343.9:004

Ključne besede: kibernetska kriminaliteta, omejevanje, institucije, pravna podlaga, Slovenija

Combating Cybercrime in Slovenia: Organization, Method, Legal Basis and its Implementation

Purpose:

Numerous recent reports by international and national organizations talk about the rapid and innovative development of cybercrime. In this paper we would like to analyze the structure and method of combating cybercrime in Slovenia, examine the legal basis regarding this field and present national statistics on its implementation.

Methods:

The general findings are reported on the basis of literature, reviews of the activities of individual state, public, private and international organizations related to cyber and information security, reviews of laws and further available official statistics in the field of cybercrime.

Findings:

The Center for computer investigation, SI-CERT and the European cybercrime center play a key role in the investigation of cybercrime in Slovenia. Additional non-police government organizations, private information-security companies, NGOs and international organizations are also included in the fight against cybercrime. The legal basis for the fight against cybercrime in Slovenia is advanced and is part of several national and international acts. The biggest problem faced by the law enforcement authorities is a rare approach to cyber criminal offenses during the global boom in cybercrime. For instance, there were only a few condemnatory convictions in Slovenia in the last seven years.

Research Limitations/Implications:

The paper examines the combat against cybercrime in Slovenia, including international organizations which are operating in the country.

Originality/Value:

The exact method, the organization and level of success of the fight against cybercrime have not yet been analyzed within a national framework. In this paper, we highlight the problems which Slovenia faces, and recommend more effective methods to fight against cybercrime.

UDC: 343.9:004

Keywords: cybercrime, limiting, institutions, legal basis, Slovenia

1 UVOD

Mednarodne in nacionalne organizacije beležijo hitro naraščanje števila kibernetskih napadov. Razvoj informacijsko-komunikacijskih naprav in njihovo spletno povezovanje ter gospodarska nestabilnost in neozaveščenost spletnih uporabnikov dodatno povečujejo možnosti škodljivih kibernetskih dejanj. Svetovni splet je na voljo tako običajnim spletnim uporabnikom kot tudi storilcem kaznivih dejanj v kibernetskem prostoru, ki z izkoriščanjem »odvisnosti« uporabnikov od spleta uresničujejo svoje cilje. Storitve, kot so nakupovanje, plačevanje blaga in storitev, pošiljanje datotek, elektronsko bančništvo, prenos podatkov in druge oblike poslovanja, ki potekajo prek interneta, povezovanje z mobilnimi napravami ter neomejen dostop in povezanost globalnega kibernetskega prostora, so sčasoma postale samoumevne in vsakdanje (Bernik in Prislan, 2012).

Boj proti kibernetski kriminaliteti je kompleksen, zato se organi pregona brez sodelovanja z mednarodnimi ustanovami, zasebnim sektorjem ter širšo javnostjo ne morejo uspešno boriti proti dejavnikom tovrstne kriminalitete (Brenner, 2007; Wall, 2007; Wall, 2007/2010). Specifičnost preiskovanja kibernetske kriminalitete zahteva od organov pregona poleg sodelovanja in izmenjevanja podatkov med institucijami na nacionalni in mednarodni ravni tudi dobro tehnološko opremljenost, strokovnost, poznavanje informatike in obvladovanje računalniških veščin. Institucionalna in pravna podlaga boja proti kibernetski kriminaliteti na evropski ravni sta Evropski center za kibernetsko preiskovanje, namenjen zaščiti evropskih državljanov in podjetij pred kibernetsko kriminaliteto, ki je začel delovati januarja 2013 (Europol, 2013), in Evropska konvencija o kibernetski kriminaliteti, ki državam podpisnicam daje pravno podlago za boj proti kibernetski kriminaliteti in je osnova za mednarodno sodelovanje (Rupnik, 2003).

V boj proti kibernetski kriminaliteti v Sloveniji in drugih evropskih državah so vključene številne organizacije na nacionalni in mednarodni ravni. V tem prispevku so analizirani načini, organizacija in uspešnost boja proti kibernetski kriminaliteti v Sloveniji. Predstavljamo organizacije in posameznike, ki delujejo na tem področju. Analiziramo njihovo delo, pravne podlage na nacionalni in mednarodni ravni ter uradne statistične podatke o številu kaznivih dejanj in pravnomočnih kazenskih sankcij na področju kibernetske kriminalitete.

2 KIBERNETSKA KRIMINALITETA

Kibernetski prostor ne pozna nacionalnih meja in zajema vse oblike digitalne dejavnosti. Zaradi kompleksnosti področja in različnih pogledov posameznih držav (še) nimamo univerzalno sprejete definicije kibernetske kriminalitete, čeprav so ta pojem do zdaj poskušale opredeliti številne organizacije in avtorji. Ob upoštevanju elementov, kot jih definira Konvencija o kibernetski kriminaliteti, jo Bernik in Meško (2011: 243) definirata kot: »Kibernetska kriminaliteta pomeni uporabo informacijsko-komunikacijskih tehnologij za izvedbo kaznivih dejanj.« Avtorja upoštevata tudi škodljiva in nemoralna dejanja v kibernetskem prostoru, ki niso nujno kriminalna in kazniva. Tudi Wall (2007: 28) pravi, da ni nujno, da

so dejanja inkriminirana in kibernetsko kriminaliteto definira kot »kazniva in škodljiva dejanja, ki vključujejo pridobitev ali manipulacijo s podatki zaradi določene koristi«. Na desetem kongresu organizacije Združenih narodov o preprečevanju kriminalitete in ravnanju s storilci (United Nations, 2000) je bila na delavnici, posvečeni kriminaliteti, povezani z računalniškimi omrežji, kibernetska kriminaliteta definirana v ožjem in širšem pomenu besede. V ožjem pomenu je kibernetska kriminaliteta »vsak protipravni način dela, ki se upravlja elektronsko in katerega cilj je motenje varnosti računalniških sistemov in podatkov, ki jih ta sistem obravnava«. Kibernetska kriminaliteta v širšem pomenu besede pa je definirana kot »vsako protipravno dejanje, ki se izvaja prek računalniških sistemov ali omrežja ali je kakor koli povezano z njimi.« V definicijo kibernetske kriminalitete se vključuje tudi uporaba računalnikov za izvajanje kaznivih dejanj. Dashora (2011: 240) definira kibernetsko kriminaliteto kot »kriminal, storjen na spletu, pri čemer se računalnik uporablja kot sredstvo ali cilj napada«. Tudi nekateri drugi (npr. Wilson, 2008; Yazdanifard, Oyegoke in Seyedi, 2011) podobno definirajo kibernetsko kriminaliteto.

V zadnjih letih so postale nelegalne in škodljive dejavnosti v kibernetskem prostoru zelo organizirane in inovativne (Bernik in Meško, 2011). Zato lahko na podlagi škode, števila storilcev kaznivih kibernetskih dejanj in njihovih žrtev govorimo o zelo uspešnem poslovanju (Anderson et al., 2012; Norton, 2011, 2012). Enotna univerzalna definicija, ki bi dala temeljna izhodišča za nadaljnje delo in poenotenje mednarodnega boja proti kibernetski kriminaliteti, je potrebna zaradi internacionalizacije problema in morebitne nevarnosti.

3 BOJ PROTI KIBERNETSKI KRIMINALITETI

Narava kibernetskega prostora in transnacionalnost kibernetskih dejanj sta zadosten izziv in pokazatelj kompleksnosti preprečevanja in zatiranja tovrstne kriminalitete. Zaradi potrebe po tehnološki opremljenosti, strokovnosti, znanjih o informatiki in obvladovanju računalniških veščin med preiskovalci kaznivih dejanj ter potrebe po mednarodnem sodelovanju in sodelovanju drugih vladnih in nevladnih organizacij in širše javnosti je boj proti kibernetski kriminaliteti bistveno bolj zapleten kot boj proti konvencionalni kriminaliteti (Bernik in Prislan, 2012; Broadhurst, 2006; Burns, Whitworth in Thompson, 2004; Wall, 2007).

Nadzor nad kriminaliteto, ki vključuje uporabo digitalne tehnologije in računalniškega omrežja, nalaga vzpostavljanje in delovanje novih mrež. Sem spadajo povezave med policijo in drugimi vladnimi organi, povezave med policijo in nepolicijskimi javnimi in zasebnimi organizacijami (npr. CERT in ISP), povezave med policijo in mednarodnimi organizacijami (npr. Europol-EC3, ENISA, Eurojust, CEPOL) ter povezava med policijo in spletnimi uporabniki (Brenner, 2007; Broadhurst, 2006; Wall, 2007, 2007/2010). (Ne)učinkovitost organov pregona je odvisna od številnih dejavnikov, kot so pomanjkanje standardne definicije kibernetske kriminalitete, težave pri preiskovanju kibernetske kriminalitete, nezmožnost pridobivanja in vzdrževanja tehnologije, potrebne za preiskovanje kaznivih dejanj zaradi velikih stroškov, težave z usposabljanjem zaposlenih

in pridobivanjem vodstvenih kadrov, zadolženih za preiskovanje, neustrezna zakonodaja itn. (Bossler in Holt, 2012; McQuade, 2006; Stambaugh et al., 2001). Empirične raziskave, opravljene med pripadniki organov pregona, zadolženimi za boj proti kibernetski kriminaliteti, kažejo, da organi pregona dejansko raziščejo zelo malo primerov kibernetske kriminalitete (Hinduja, 2004; Senjo, 2004; Stambaugh et al., 2001) in opozarjajo na pomanjkanje znanja, veščin in sposobnosti zaposlenih, pa tudi na pomanjkanje ustreznih tehničnih sredstev za preiskovanje tovrstne kriminalitete (Bossler in Holt, 2012; Burns et al., 2004; Davis, 2012; Hinduja, 2004; Holt, Bossler in Fitzgerald, 2010; Stambaugh et al., 2001). Navedene težave organov pregona omogočajo storilcem, da se kaznivih dejanj lotevajo brez strahu, kar povečuje »temno polje« njihovega delovanja.

Evropske države imajo zaradi razmeroma poenotenih standardov podoben način delovanja pri zatiranju in preprečevanju kibernetske kriminalitete. V Evropski uniji deluje več organizacij za mednarodno sodelovanje in izmenjavo podatkov. V Sloveniji boj proti kibernetski kriminaliteti poteka prek različnih nacionalnih in mednarodnih akterjev, ki različno vplivajo na povečanje nadzora nad kibernetskim okoljem.

4 BOJ PROTI KIBERNETSKI KRIMINALITETI V SLOVENIJI

Preden začnemo razpravo, bomo prikazali akterje, ki sodelujejo v boju proti kibernetski kriminaliteti v Sloveniji. Prikaz na sliki 1 je narejen na podlagi pregleda literature (Brenner, 2007; Enisa, 2011; Europol, 2013; Policija, 2010; RAND Europe, 2012; SI-CERT, 2013; Wall, 2007/2010) in poznavanja slovenskega prostora v boju proti kibernetski kriminaliteti.

4.1 Uprava kriminalistične policije

Policija kot državni organ, zadolžen za vzdrževanje reda in uveljavljanje nacionalne zakonodaje, ima v boju proti kibernetski kriminaliteti majhno, vendar pomembno vlogo (Wall, 2007/2010). Vloga policije se razlikuje od primera do primera. Pri svojem delu, torej preiskovanju domnevnih kršiteljev in zbiranju dokazov, policija običajno kombinira tradicionalne policijske metode z uporabo računalnikov (Sommer, 2004). Število tovrstnih kaznivih dejanj narašča pri nas in po svetu. Na področju preiskovanja kibernetske kriminalitete in računalniške forenzike slovenska kriminalistična policija usmerjeno deluje od leta 1999 (Policija, 2010). Leta 2009 je kriminalistična policija na novo organizirala to področje in ustanovila Center za računalniško preiskovanje ter štiri regijske oddelke (SKP Koper, Ljubljana, Celje in Maribor). V njih so zaposleni kriminalisti z odličnim znanjem informatike in računalništva, ki zaradi hitrega razvoja informacijske tehnologije (predvsem strojne in programske opreme) ter vedno novih načinov izvrševanja kaznivih dejanj skrbijo tudi za redno posodabljanje opreme (Strniša, 2010).

Računalniško preiskovanje obsega preprečevanje, odkrivanje, preiskovanje in dokazovanje kaznivih dejanj v kibernetskem prostoru in kaznivih dejanj, storjenih

Slika 1: Shematski prikaz organiziranosti boja proti kibernetski kriminaliteti v Sloveniji

z računalniško tehnologijo, ter zavarovanje računalniških podatkov, ki lahko kažejo na kazniva dejanja (Svetek in Kebe, 2003). Center in oddelki za računalniško preiskovanje pokrivajo tri glavna področja dela (Policija, 2010):

- preiskovanje kaznivih dejanj računalniške kriminalitete (zloraba osebnih podatkov, kršitev materialnih avtorskih pravic, napad na informacijski sistem, vdor v poslovno-informacijski sistem ter izdelovanje in pridobivanje pripomočkov, namenjenih izvedbi kaznivega dejanja);
- preiskave zaseženih e-naprav oz. e-podatkov (t. i. računalniška forenzika);
- strokovna pomoč pri preiskovanju drugih področij kriminalitete (kazniva dejanja otroške pornografije, spletne goljufije, rasne nestrpnosti na internetu, davčne utaje, korupcija, zlorabe e-bančništva itd.).

Toni Kastelic, vodja Centra za računalniško preiskovanje, pravi, da so pristop in metode preiskave odvisni predvsem od vrste kaznivega dejanja, načina storitve, informacij, ki so dosegljive forenziku, in tudi od tipa elektronske naprave. Najpogostejši prvi korak pri preiskovanju je izdelava istovetne kopije celotnega nosilca podatkov oz. tako imenovane forenzične kopije podatkov, kjer se nosilec podatkov kopira v celoti, od prvega do zadnjega bita. Pri izdelavi kopije se izračunajo kontrolne vrednosti, ki zagotavljajo integriteto kopiranih podatkov, torej istovetnost kopije z izvirnikom. Forenzik nato opravi forenzično analizo oz. preiskavo, katere cilj je odkritje digitalnih dokazov, in na koncu naredi zapisnik (Intervju s Tonijem Kastelicem …, 2012).

Hiter razvoj informacijske tehnologije zahteva sprotno in intenzivno izobraževanje ter dobro poznavanje računalniške programske in strojne opreme in novih pojavnih oblik kibernetske kriminalitete, njihovega odkrivanja in poznejšega

analiziranja (Broadhurst, 2006; Burns et al., 2004; Davis, 2012; Wall, 2007/2011). Ti dejavniki lahko močno vplivajo na učinkovitost dela kriminalistične policije. Slovenija je leta 2011 za povečanje zmogljivosti centra in oddelkov za računalniško preiskovanje od OLAF-a (Evropskega urada za boj proti goljufijam) prejela finančno pomoč. S projektom je slovenska policija povečala zmogljivosti regijskih enot za preiskovanje računalniške kriminalitete in izboljšala tehnično opremljenost kriminalistov, ki so bili poleg tega deležni tudi ustreznega izobraževanja. V letu 2011 sta bila izvedena nakup večje količine računalniške strojne opreme in licenc ter ustrezno strokovno usposabljanje (Policija, 2012).

4.2 Javne in zasebne nepolicijske organizacije

Javne in zasebne nepolicijske organizacije so lahko zelo koristne pri preventivnem in represivnem delovanju proti kibernetski kriminaliteti (Wall, 2007/2010). Organizacije spodbujajo oz. omogočajo mednarodno povezovanje, povečanje števila prijavljenih kibernetskih škodljivih dejanj, povečanje ozaveščenosti spletnih uporabnikov o pojavnih oblikah in potrebi po ustrezni zaščiti, kar je velika opora v boju proti kibernetski kriminaliteti.

Mednarodna organizacija CERT (Computer Emergency Response Team), ustanovljena leta 1998 na Carnegie Mellon University v Pittsburghu, je sodobna kombinacija med zasebno in javno organizacijo (Wall, 2007/2010). Od leta 1995 deluje tudi slovenski CERT (SI-CERT) – Nacionalni center za obravnavo varnostnih incidentov na internetu. CERT sprejema prijave zlorab, vdorov in okužb ter vseh drugih dogodkov, povezanih z računalniško in omrežno varnostjo. SI-CERT deluje v okviru javnega zavoda ARNES že od svoje ustanovitve (Akademska in raziskovalna mreža Slovenije)[1]. Delovanje centra je sestavljeno iz več faz (SI-CERT, 2013). Zagotovljeno je primerno delovno okolje in ustrezno usposobljeni zaposleni, ki so predpogoj za delovanje odzivnega centra. Z incidentom se začnejo konkretno ukvarjati in analizirati, ko ga zaznajo. Najpogosteje je to takrat, ko na naslov cert@cert.si prejmejo obvestilo o incidentu. Tega razvrstijo v eno od kategorij, naredijo analizo, primerno za kategorijo ali vrsto incidenta, in korelacijo med različnimi podatki o incidentu, drugimi incidenti ter sledovi, odkritimi v preiskavi. V fazi zamejitve, odstranitve in povrnitve zbirajo dokaze, omejujejo izpostavljenost sistemov in o incidentu po potrebi obvestijo skrbnike sistemov, ponudnike in druge CERT-centre. V končni fazi sledijo še sklepne dejavnosti z zbiranjem izkušenj, ki obravnavani incident povezujejo z drugimi obravnavanimi incidenti. SI-CERT se povezuje z drugimi akterji glede informacijske in omrežne varnosti doma in v tujini. Aktivno sodelujejo v evropski delovni skupini TF-CSIRT[2] in v svetovnem

1 *Javni zavod Arnes in Ministrstvo za pravosodje in javno upravo sta na podlagi sklepa vlade RS 31. maja 2010 podpisala sporazum o sodelovanju na področju informacijske varnosti. Sporazum določa, da Arnesov varnostni center SI-CERT pomaga pri vzpostavitvi vladnega Cert-centra (delovno ime Sigov-cert) in da do vzpostavitve novega centra tudi opravlja naloge koordinacije varnostnih incidentov za vse informacijske sisteme javne uprave (SI-CERT, 2013).*

2 *TF-CSIRT od leta 2000 združuje vse evropske odzivne CERT-centre.*

združenju »First« (Forum of incident response and security teams) ter v skupini nacionalnih odzivnih centrov, ki jo vodi ameriški CERT/CC (SI-CERT, 2013).

Slovenski odzivni center SI-CERT poleg opisane dejavnosti izvaja tudi projekt, ki se imenuje »Varni na internetu«. Zastavljen je dolgoročno in zajema široko področje informacijske varnosti. Dvig stopnje informiranosti o varni rabi interneta je glavni cilj projekta ozaveščanja slovenske javnosti. Njihove dejavnosti so usmerjene k doseganju ciljev (Varni na internetu, 2013): »Dvigniti stopnjo zavedanja ciljnih javnosti o različnih nevarnostih, ki so jim izpostavljene na spletu; poučiti uporabnike o varni uporabi spletnega bančništva; poučiti uporabnike o različnih oblikah spletnih prevar in jim ponuditi praktične rešitve, kako se zavarovati; ter informirati uporabnike o varstvu osebne identitete v socialnih omrežjih.«

Drugi projekt v RS je Center za varnejši internet SAFE-SI[3], ki združuje tri komponente: ozaveščanje o varni rabi interneta in novih tehnologij; telefonsko linijo za pomoč mladim in njihovim staršem, ki se znajdejo v težavah, povezanih z uporabo interneta, ter Spletno Oko − točko za anonimno prijavo nelegalnih spletnih vsebin (otroške pornografije in sovražnega govora). Dejavnosti centra so usmerjene proti štirim ciljnim skupinam: otrokom, mladostnikom, staršem in strokovnim delavcem (učiteljem, socialnim delavcem, vzgojiteljem). Cilj projekta je, da se med izbranimi ciljnimi populacijami s sprotnim zagotavljanjem preverjenih informacij in nasvetov za varno rabo novih tehnologij v Sloveniji doseže visoka stopnja ozaveščenosti o teh temah (Program Varnejši internet v Sloveniji, 2012).

V zadnjem času je veliko pozornosti usmerjene k ponudnikom internetnih storitev, ki lahko močno vplivajo na vedenje uporabnikov. Njihov vpliv je utemeljen na pravilih in pogojih, ki jih uporabniki morajo upoštevati, ter programski opremi, ki se uporablja in ki vpliva na zmanjševanje kibernetskega prestopništva (Wall, 2007). Ponudniki internetnih storitev izkoriščajo svoj položaj v komunikacijskih omrežjih in s tem ustvarjajo varnostne mehanizme na zadevnem področju. Slednji lahko zaznavajo in preprečijo različne kibernetske napade. Wall (2007/2010) pravi, da so ponudniki najbolj zanesljivi pri vzpostavljanju varnostnih sistemov v obliki filtrov SPAM. V Sloveniji deluje Sekcija slovenskih ponudnikov internetnih storitev (SISPA), kar omogoča sodelovanje in skupno reševanje problemov, povezanih z zaščito spletnih uporabnikov pred spletnimi grožnjami. Tovrstne organizacije, ki so se začele združevati tudi na mednarodni ravni (npr. Pan-European Internet Service Providers' Association), ponujajo pridobivanje pozitivnih izkušenj ter skupno iskanje načinov za uspešen boj proti kibernetski kriminaliteti.

4.3 Zasebna informacijsko-varnostna podjetja

Varen pretok informacij je danes en od osnovnih zahtev za stabilno in uspešno poslovanje organizacij. Uspešnost delovanja podjetij je v glavnem odvisna od

3 *Projekt Centra za varnejši internet SAFE-SI izvajajo Univerza v Ljubljani, Fakulteta za družbene vede, ARNES, Zveza prijateljev mladine Slovenije in Zavod MISSS (Mladinsko informativno svetovalno središče Slovenije), financirata pa ga »Generalni direktorat Connect« pri Evropski komisiji in Ministrstvo za izobraževanje, znanost, kulturo in šport (Program Varnejši internet …, 2012).*

njihovega informacijskega sistema (Bernik in Prislan, 2011). Informacijska varnost je samostojna poslovna funkcija podjetja, ki jo zagotavljajo vsi zaposleni v podjetju. O tem govori načelo o obvladovanju tveganj, ki ga je treba upoštevati tudi pri krepitvi informacijske varnostne kulture; načelo pravi, da je treba razpršiti odgovornost za njeno upravljanje tako, da skrb za upravljanje ne zadeva le vodstvenih kadrov, temveč postane naloga vseh zaposlenih v organizaciji, element vsakodnevnih dejavnosti in praks, tudi tistih, ki se na prvi pogled ne zdijo povezane z varnostjo (Chevreau, 2006).

V zadnjem času se je v Sloveniji pojavilo več podjetij, ki ponujajo storitve, povezane z zaščito in varnostnim preverjanjem informacijsko-komunikacijskih sistemov. V to skupino spadajo Sistemator, Hic Salta, SGbiro, Netis, Sibit, ATR.SIS, TrendNET, HERMES SoftLab, PRORANG, Simt, Team Intell, Palsit, S&T, MegaM, Virtua, Astec, D-NET, Viris, ACROS itn. Nekatera podjetja že imajo zaposlene certificirane računalniške forenzike. Podjetja najemajo zasebne forenzike, kadar sumijo, da je prišlo do izdaje poslovnih skrivnosti, nadlegovanja na delovnem mestu, zlorabe položaja ali notranjih informacij, uveljavljanja konkurenčne klavzule ali dokončnega izbrisa podatkov s trdih diskov (Banovič, 2007). Poleg tega se navedena podjetja ukvarjajo še z izobraževanjem zaposlenih o zaščiti in uporabi preventivnih ukrepov ter ustvarjanjem celovite varnostne politike in kulture v podjetjih (Prava ideja, 2010), kar je zelo pomembno z vidika informacijske varnosti.

4.4 Spletni uporabniki

Spletni uporabniki so najbolj izpostavljeni kibernetskemu tveganju in so pogosto žrtve kibernetske kriminalitete. S svojim ravnanjem in spletno kulturo lahko vplivajo na preventivno in represivno delovanje. V tem boju sodelujejo različne skupine uporabnikov, ki delujejo na določenem področju. Tak primer je skupina Anonymus, ki je, čeprav je znana kot kriminalna skupina, leta 2011 začela s spleta odstranjevati pedofilske vsebine in javno objavljati imena pedofilov (Anonymous napadel še pedofile, 2011).

Huey, Nhan in Broll (2012) ugotavljajo, da je lahko javnost pomemben partner organov pregona in zasebnih sektorjev pri varovanju kibernetskega prostora. Pri tem navajajo tri razloge za svoje trditve. Prvič, zaradi distributivne narave spletnega sveta lahko člani družbe postanejo »oči in ušesa« za zaznavanje kriminalnih dejanj; drugič, zaradi hitrosti informacij, ki jih zbira javnost, in mobiliziranja različnih oblik koristi, do katerih pogosto dostopajo hitreje kot najboljši organi pregona. Tretjo prednost vključevanja javnosti v civilne kiberpolicijske dejavnosti po njihovem mnenju predstavlja raznolikost posameznikov in skupin, kar omogoča dostop do široke palete koristi. Spletni uporabniki lahko z uporabo zanesljivih protivirusnih programov, požarnih zidov, filtrov antiSPAM, enkripcijo podatkov itn. ter predvsem z odgovornim in zavednim ravnanjem, ki je posledica poznavanj problematike, močno zmanjšajo svojo ranljivost in pogostost pojavljanja kibernetske kriminalitete. Prijavljanje kaznivih dejanj lahko policiji poveča motivacijo v boju proti kibernetski kriminaliteti in zoži njeno »temno polje«.

4.5 Raziskovalne in druge nacionalne organizacije

Raziskave na področju kibernetske kriminalitete so lahko učinkovite pri zagotavljanju novih načinov za odpravljanje težav, s katerimi se srečujejo državne in mednarodne institucije, ki si prizadevajo za povečanje nadzora nad kibernetskim okoljem. Prav temu služijo številne raziskovalne organizacije v Sloveniji, ki pri izvajanju svojih raziskovalnih dejavnosti ugotavljajo slabosti informacijskih sistemov, motive storilcev kaznivih kibernetskih dejanj, uporabnikove šibke točke idr. ter organom pregona in drugim organizacijam predlagajo ustrezne spremembe delovanja za učinkovitejšo preventivno in represivno delovanje na tem področju.

Pri nadzoru nad kibernetskim prostorom v Sloveniji sodelujejo številne organizacije. Ena od njih je Akademska in raziskovalna mreža Slovenije (ARNES) kot javni zavod, ki zagotavlja omrežne storitve raziskovalnim, izobraževalnim in kulturnim organizacijam, omogoča njihovo povezovanje in medsebojno sodelovanje ter sodelovanje s sorodnimi organizacijami v tujini (Arnes, 2012). Poleg ARNES-a se z raziskovanjem ukvarjajo tudi nekatere fakultete in inštituti (na primer Inštitut za informatiko, Laboratorij za telekomunikacije in Laboratorij za sistemske raziskave in informacijske tehnologije, Institut Jožef Stefan, Fakulteta za varnostne vede; Fakulteta za družbene vede, Fakulteta za elektrotehniko, računalništvo in informatiko itn.).

Naj omenimo še druge nacionalne organizacije, katerih dejavnosti so tudi zaščita in varovanje informacijskih, komunikacijskih in telekomunikacijskih omrežij. Te organizacije so (povzeto po Enisa, 2011): Informacijski pooblaščenec; Ministrstvo za visoko šolstvo, znanost in tehnologijo, Direktorat za informacijsko družbo; Ministrstvo za zunanje zadeve, Oddelek za informacijsko varnost in komunikacije; Agencija za pošto in elektronske komunikacije (APEK); Slovenska obveščevalno-varnostna agencija (SOVA); Ministrstvo za javno upravo, Direktorat za e-upravo in upravne procese; Urad Vlade RS za varovanje tajnih podatkov (UVTP) itn. Slovenija si z navedenimi organizacijami na državni in mednarodni ravni prizadeva uresničiti področno zakonodajo ter omogočiti spletnim uporabnikom varen kibernetski prostor.

4.6 Mednarodne organizacije za policijsko in pravosodno sodelovanje

Mednarodne policijske, pravosodne in druge organizacije so zaradi mednarodnega vidika kibernetske kriminalitete ključnega pomena. V Evropi delujejo štiri večje agencije za policijsko in pravosodno sodelovanje na področju kibernetskega (in drugega) prostora: Europol, ENISA, Eurojust in CEPOL, ki so v izjemno veliko oporo državam članicam pri njihovem boju proti čezmejni in organizirani kriminaliteti.

Europol je kot največja evropska policijska organizacija pristojen za reševanje hujših in organiziranih kaznivih dejanj na evropski ravni. Z zbiranjem in analiziranjem obveščevalnih podatkov, forenzično dejavnostjo in drugimi ukrepi pomaga državam članicam pri kazenskem pregonu (RAND Europe, 2012). V okviru

Europola od 11. januarja 2013 deluje Evropski center za kibernetsko kriminaliteto (EC3). Center ponuja delovno, tehnično in forenzično podporo državam članicam s strateško analizo. Cilj analize je učinkovitejše preprečevanje kibernetske kriminalitete, izboljšanje učinkovitosti kazenskega pregona, sodelovanje zasebnega sektorja v EU in določitev primerov dobre prakse ter ovir na poti k učinkovitejšemu mednarodnemu sodelovanju (Europol, 2013).

Evropska agencija za varnost omrežja in informacij (ENISA) je druga agencija, ki deluje na evropski ravni in je središče omrežne in informacijske varnosti EU, njenih držav članic, zasebnega sektorja in evropskih državljanov. V sodelovanju s temi skupinami izdaja agencija nasvete in priporočila o dobrih praksah informacijske varnosti, pomaga državam članicam pri izvajanju zadevne evropske zakonodaje ter si prizadeva za povečanje odpornosti evropske kritične informacijske infrastrukture in omrežij (Enisa, 2012).

Eurojust kot evropski pravosodni organ si prizadeva za izboljšanje učinkovitosti nacionalnih organov, pristojnih za preiskavo in kazenski pregon, pri obravnavi težjih oblik čezmejne in organizirane kriminalitete ter zagotavlja hitro in učinkovito sodno obravnavo storilcev kaznivih dejanj (Eurojust, 2012). Cilj delovanja organa je izboljšanje sodelovanja med evropskimi pravosodnimi organi in prek njih povezav z Europolom, kar vpliva na poenotenje pravosodnih standardov. Kazniva dejanja kibernetske kriminalitete obravnava Eurojustov oddelek za gospodarsko in finančno kriminaliteto (RAND Europe, 2012). Poleg navedenih organizacij na evropski ravni deluje tudi mednarodna organizacija CEPOL, namenjena usposabljanju delavcev, ki delajo na srednjih ali višjih ravneh v organih pregona na evropski ravni[4]. V CEPOL-u so do leta 2012 izvedli deset dejavnosti, povezanih s kibernetsko kriminaliteto, v katerih je sodelovalo 236 oseb (RAND Europe, 2012).

V boju proti kibernetski kriminaliteti je poleg evropskih organizacij za policijsko in pravosodno sodelovanje prisotna še svetovna mednarodna organizacija Interpol, ki izvaja tudi dejanja, povezana s kibernetsko kriminaliteto. Interpolov program dela, ki je usmerjen v boj proti kibernetski kriminaliteti, je namenjen usposabljanju in spremljanju kibernetskih groženj. Njegovi cilji so spodbujanje izmenjave informacij med državami članicami, izvajanje usposabljanja za uveljavitev in vzdrževanje kibernetskih standardov, usklajevanje in pomoč pri izvajanju mednarodnih operacij, pomoč državam članicam v primeru kibernetskih napadov, razvoj strateških partnerstev z drugimi mednarodnimi organizacijami itn. (González, 2008).

5 USKLAJENOST MEDNARODNE ZAKONODAJE, NACIONALNA PRAVNA PODLAGA IN NJENO IZPOLNJEVANJE

Države z mednarodnimi in nacionalnimi pravnimi viri varujejo državljane pred škodljivimi vplivi digitalne družbe ter organom pregona omogočajo legalen boj

4 *Med 18. in 21. oktobrom 2011 je na Brdu pri Kranju potekal seminar CEPOL o kibernetski kriminaliteti (Uprava kriminalistične policije, 2011).*

proti kibernetski kriminaliteti. Prvi mednarodni pravni akt in pravni mehanizem za mednarodno sodelovanje pri kazenskem pregonu in poenotenju nacionalnih zakonodaj je Konvencija Sveta Evrope o kibernetski kriminaliteti[5] iz leta 2001 (Broadhurst, 2006). Konvencijo je 24. julija 2002 podpisala tudi Republika Slovenija (Council of Europe, 2013). Cilj konvencije je ustvariti skupno politiko držav podpisnic, ki bo varovala družbo pred kibernetsko kriminaliteto, med drugim tudi s sprejetjem ustrezne zakonodaje in spodbujanjem mednarodnega sodelovanja (Bernik in Prislan, 2012). Konvencija je vsebinsko razdeljena na štiri poglavja (Rupnik, 2003: 2–3): v prvem delu je opredeljen pomen nekaterih za razumevanje konvencije ključnih izrazov, drugo poglavje obravnava materialno in procesno kazenskopravno problematiko, tretje opredeljuje posamezne smernice mednarodnega sodelovanja, končne določbe v četrtem delu pa določajo načine podpisa, sprejetja in veljavnosti konvencije[6]. Kmalu zatem, ko je konvencijo o kibernetski kriminaliteti 8. septembra 2004 ratificiral državni zbor (Council of Europe, 2013), je Slovenija vključila smernice konvencije v svojo nacionalno zakonodajo. V Sloveniji veljajo poleg konvencije še drugi mednarodni pravni akti, ki se nanašajo na kibernetsko kriminaliteto, kot sta Konvencija WIPO o avtorskih pravicah[7] in Evropska konvencija o varstvu človekovih pravic in temeljnih svoboščin[8] ter drugi normativni akti, ki jih je podpisala RS in se lahko uporabijo v boju proti oz. za pregon kibernetske kriminalitete.

Kazenskopravni okvir zaščite in kibernetske varnosti državljanov je vsebovan v najpomembnejšem državnem pravnem aktu, torej v Ustavi Republike Slovenije (2006). Gre predvsem za varovanje človekovih pravic in temeljnih svoboščin, ki jih ogrožajo sodobne škodljive programske kode[9]. V slovenski kazenskopravni ureditvi so kazniva dejanja v kibernetskem prostoru regulirana s Kazenskim zakonikom Republike Slovenije. Kazenski zakonik obravnava vsa inkriminirana dejanja kibernetske kriminalitete. Kljub pogostemu spreminjanju evropske in slovenske zakonodaje o kibernetski kriminaliteti še vedno obstajajo nekatera

5 *Do konca leta 2012 je Evropsko konvencijo o kibernetski kriminaliteti podpisalo in ratificiralo 38 držav, tudi države, ki niso članice Sveta Evrope (ZDA, Japonska in Avstralija) (Council of Europe, 2013).*

6 *Konvencija določa tudi številne postopkovne pristojnosti, kot so iskanje in prestrezanje vsebine na računalniških omrežjih, in je vsebinsko razdeljena na (Bernik in Prislan, 2012) kazniva dejanja zoper zaupnost, integriteto in dostopnost računalniških podatkov in sistemov (vdor v računalniški sistem, protipravno prestrezanje in motenje podatkov ter sistemov, zloraba naprav) in kazniva dejanja, povezana s samim računalnikom (računalniško ponarejanje, računalniška goljufija, kazniva dejanja, povezana z otroško pornografijo, kazniva dejanja, povezana s kršitvijo avtorskih in sorodnih pravic).*

7 *Konvencija WIPO o avtorskih pravicah, imenovana tudi Internetna pogodba, temelji na Bernski konvenciji, najpomembnejši pogodbi mednarodnega avtorskega prava. Svetovna (univerzalna) konvencija o avtorskih pravicah (1952) je v Sloveniji začela veljati 5. novembra 1992 (Bogataj Jančič, 2008).*

8 *Konvencija WIPO o avtorskih pravicah je v Sloveniji začela veljati 28. junija 1994 (Kalčina, 2005).*

9 *Ustava Republike Slovenije (2006) v 35. členu – varstvo pravic zasebnosti in osebnostnih pravic; 37. členu – varstvo tajnosti pisem in drugih občil; 39. členu – varstvo osebnih podatkov in 60. členu – pravice iz ustvarjalnosti.*

nemoralna in škodljiva dejanja, ki niso kriminalizirana in kazniva[10]. Dejstvo je, da se tehnologija razvija hitreje kot pravo, vendar, kot pravi Peršak (2009: 196), je »prepoved tehnoloških iznajdb rešitev, ki ni sprejemljiva z vidika legitimnosti kriminalizacije«. Pomembni členi kazenskega zakonika z vidika kibernetske kriminalitete so (Kazenski zakonik [KZ-1-UPB2], 2012):

- 108. člen KZ-1-UPB2: terorizem;
- 139. člen KZ-1-UPB2: kršitev tajnosti občil;
- 140. člen KZ-1-UPB2: nedovoljena objava zasebnih pisanj;
- 143. člen KZ-1-UPB2: zloraba osebnih podatkov;
- 147. člen KZ-1-UPB2: kršitev moralnih avtorskih pravic;
- 148. člen KZ-1-UPB2: kršitev materialnih avtorskih pravic;
- 149. člen KZ-1-UPB2: kršitev avtorskim sorodnih pravic;
- 173.a člen KZ-1-UPB2: pridobivanje oseb, mlajših od petnajst let, za spolne namene;
- 176. člen KZ-1-UPB2: prikazovanje, izdelava, posest in posredovanje pornografskega gradiva;
- 211. člen KZ-1-UPB2: goljufija
- 212. člen KZ-1-UPB2: organiziranje denarnih verig in nedovoljeno prirejanje iger na srečo;
- 221. člen KZ-1-UPB2: napad na informacijski sistem;
- 235. člen KZ-1-UPB2: ponareditev ali uničenje poslovnih listin;
- 237. člen KZ-1-UPB2: zloraba informacijskega sistema;
- 247. člen KZ-1-UPB2: uporaba ponarejenega negotovinskega plačilnega sredstva;
- 248. člen KZ-1-UPB2: izdelava, pridobitev in odtujitev pripomočkov za ponarejanje;
- 251. člen KZ-1-UPB2: ponarejanje listin;
- 297. člen KZ-1-UPB2: javno spodbujanje sovraštva, nasilja ali nestrpnosti;
- 306. člen KZ-1-UPB2: izdelovanje in pridobivanje orožja in pripomočkov, namenjenih za kaznivo dejanje.

Pri pregledu uradnega prečiščenega besedila kazenskega zakonika iz leta 2012 opažamo posamezne razlike v primerjavi s Kazenskim zakonikom iz leta 2008; 173. člen je v obeh kazenskih zakonikih (KZ-1, 2008; KZ-1-UPB2, 2012) ostal nespremenjen in se glasi *spolni napad na osebo, mlajšo od petnajst let*, v zakoniku iz leta 2012 (KZ-1-UPB2, 2012) iz tega člena izhaja dodatni 173.a člen, ki se glasi: *pridobivanje oseb, mlajših od petnajst let, za spolne namene*. S členom v trenutno veljavnem zakoniku se inkriminira ne samo končni cilj storilcev (spolni napad), ampak tudi način pridobivanja oseb, mlajših od 15 let, prek komunikacijskih in informacijskih tehnologij. Poleg tega je prišlo do preimenovanja dveh členov – 237. člen (KZ-1, 2008) *vdor v poslovni informacijski sistem* je v uradno prečiščenem besedilu zakonika iz leta 2012 preimenovan v *zlorabo informacijskega sistema* (KZ-1-UPB2, 2012); 247. člen (KZ-1, 2008) *uporaba ponarejene kreditne ali druge bančne*

10 *Kazenski zakonik, ki je začel veljati 1. februarja 2008, je dodal še nekatera določila, predvsem o otroški pornografiji, s katerimi je posamezna dejanja opredelil kot kazniva (Bernik in Prislan, 2012).*

kartice pa se je preimenoval v *uporaba ponarejenega negotovinskega plačilnega sredstva* (KZ-1-UPB2, 2012).

V Sloveniji področje informacijske in kibernetske varnosti poleg Ustave in Kazenskega zakonika regulirajo tudi drugi zakoni (povzeto po Arnes, 2013): Zakon o elektronskih komunikacijah (109. člen), Zakon o varstvu potrošnikov (45.a člen), Zakon o elektronskem poslovanju na trgu (6. člen) in Zakon o varstvu osebnih podatkov (72. in 73. člen). Boj proti kibernetski kriminaliteti regulira tudi Zakon o kazenskem postopku (2012), ki opredeljuje način izvajanja predkazenskega in kazenskega postopka. Slednji v dveh členih (219.a in 223.a) ureja preiskavo elektronskih naprav ter zaseg in zavarovanje podatkov, kar je pomembno z vidika digitalne forenzike in pridobivanja digitalnih dokazov.

Čeprav ima Slovenski center za posredovanje pri omrežnih incidentih (SI-CERT) v zadnjem času več dela s preiskovanjem kibernetskih incidentov[11], je »temno polje« storilcev čedalje večje. Po besedah zaposlenih v slovenskem centru reševanje teh primerov na državni ravni že nekaj let poteka usklajeno. Težave nastanejo, ko zaradi narave interneta pride do napadov prek mednarodnega omrežja, saj so te preiskave navadno zapletene (Gabor, 2010). Po podatkih slovenske policije za obdobje 2005–2012 (Policija, 2006–2013) od leta 2005 beležimo nihanje števila kaznivih dejanj. V letu 2005 jih je bilo 52; leta 2006: 38; 2007: 113; 2008: 311; 2009: 114; 2010: 101; 2011: 276; 2012: 151. Kot je razvidno iz tabele 1, so se kazniva dejanja pretežno nanašala na napad na informacijski sistem.

Tabela 1: Število kaznivih dejanj kibernetske kriminalitete po letih (Vir: Policija, 2006–2013)

KD kibernetske kriminalitete	2005	2006	2007	2008	2009	2010	2011	2012
Zloraba osebnih podatkov	N/A	N/A	1	1	0	3	5	3
Zloraba informacijskega sistema	5	6	4	7	11	15	26	12
Kršitev materialnih avtorskih pravic	17	6	7	10	5	5	3	2
Napad na informacijski sistem	30	24	88	283	98	76	236	131
Izdelovanje in pridobivanje orožja ali pripomočkov za vdor ali napad na informacijski sistem	N/A	2	13	10	0	2	6	3
Skupaj	52	38	113	311	114	101	276	151

Opomba: kaznivo dejanje, v zdaj veljavnem zakoniku opisano kot »napad na informacijski sistem«, je bilo do leta 2008 opisano kot »neupravičen vstop v informacijski sistem«. Kaznivo dejanje »zloraba informacijskega sistema« se je do leta 2008 imenovalo »vdor v informacijski sistem«, v obdobju 2008–2012 pa »vdor v poslovni informacijski sistem«. N/A pomeni, da podatki o številu kaznivih dejanj niso na voljo.

Čeprav posamezna podjetja pravijo, da imajo dnevno več varnostnih incidentov (Bernik in Prislan, 2012), je število prijavljenih kaznivih dejanj relativno majhno in je v osemletnem obdobju ostalo skoraj konstantno. Neprijavljanje kibernetskih kaznivih dejanj spada med glavne težave v boju proti kibernetski

11 Iz poročila Slovenskega centra za posredovanje pri omrežnih incidentih SI-CERT (2013) je razvidno, da so v letu 2012 obravnavali več spletnih incidentov kot v letih 2010 in 2011 skupaj, in sicer 1.250.

kriminaliteti (Brenner, 2007; Wall, 2007, 2007/2010). Posamezna poročila in avtorji (AusCERT, 2005, 2006, 2010; Wall, 2007) navajajo, da je glavni vzrok, da uporabniki ne prijavljajo kibernetskih kaznivih dejanj, njihovo prepričanje, da je policija glede vloge pri zagotavljanju informacijske varnosti neučinkovita. Pojav neprijavljanja kibernetskih dejanj pa je razširjen po vsem svetu[12]. Poleg relativno majhnega števila kibernetskih kaznivih dejanj, kot je razvidno iz tabele 2, smo v Sloveniji dočakali le nekaj pravnomočnih obsodb.

Tabela 2: Število pravnomočno obsojenih polnoletnih oseb zaradi kibernetske kriminalitete po letih (Vir: Statistični urad Republike Slovenije, 2012)

KD kibernetske kriminalitete	2006	2007	2008	2009	2010	2011
Zloraba osebnih podatkov	0	0	0	2	3	6
Vdor v poslovni informacijski sistem	0	1	0	0	0	0
Kršitev materialnih avtorskih pravic	0	0	0	0	1	0
Napad na informacijski sistem	0	0	0	1	3	0
Izdelovanje in pridobivanje orožja ali pripomočkov za vdor ali napad na informacijski sistem	0	0	0	0	1	0
Skupaj	0	1	0	3	8	6

Opomba: Ker so prikazani razpoložljivi podatki do leta 2011, je v tabeli uporabljeno kaznivo dejanje »vdor v poslovni informacijski sistem«, ki se je v kazenskem zakoniku iz leta 2012 preimenovalo v »zlorabo informacijskega sistema«.

Največja izrečena kazen pri vseh pravnomočnih obsodbah je šest mesecev zapora (ni prikazano) (Statistični urad RS, 2012). V obdobju od leta 2009 do 2011 je bilo največ, enajst (11), pravnomočnih obsodb izrečenih za kaznivo dejanje »zloraba osebnih podatkov«; od teh sta bili dve zaporni kazni od enega do dveh mesecev, ena zaporna kazen od dveh do treh mesecev in osem zapornih kazni od treh do šestih mesecev. Drugo največkrat obravnavano kaznivo dejanje v tem obdobju je »napad na informacijski sistem«. Od štirih pravnomočnih obsodb sta bili izrečeni dve obsodbi na zaporno kazen do dveh mesecev, dve pa na zaporno kazen od treh do šestih mesecev. Za preostala tri kazniva dejanja (vdor v poslovni informacijski sistem, kršitev materialnih avtorskih pravic na internetu ter izdelovanje in pridobivanje orožja ali pripomočkov za vdor ali napad na informacijski sistem) je bila izrečena le po ena pravnomočna obsodba. Vse tri pravnomočne obsodbe so odrejale zaporne kazni od enega do dveh mesecev.

Dobra zakonska podlaga brez organizacij, sposobnih njenega izvajanja, ni dovolj za uspešen boj proti kibernetski kriminaliteti, niti z vidika generalne prevencije (Meško, 2002). Slovenske raziskave (Bernik in Meško, 2011; Dimc in Dobovšek, 2010) ugotavljajo, da je bilo več kot 50 odstotkov anketirancev že žrtev

12 *Halder in Jaishankar (2010) sta ugotovila, da je le 9,6 odstotka indijskih spletnih uporabnikov prijavilo kibernetska kazniva dejanja. Krone in Johnson (2007) sta ugotovila, da je težave, povezane s spletnim nakupovanjem, prijavilo približno 50 odstotkov avstralskih gospodinjstev; od tega 26 odstotkov banki, 21 odstotkov drugi agenciji in tri odstotke policiji. Raziskave, ki jih je v letih 2005, 2006, 2010 opravil Australia's Computer Emergency Response Team (AusCERT), so pokazale, da avstralska podjetja redko prijavljajo kazniva dejanja (le 30- do 35-odstotno).*

kakšnega kaznivega kibernetskega dejanja[13], približno toliko anketiranih pa je takšno dejanje zagrešilo[14]. Ob upoštevanju prikazanih uradnih podatkov res lahko govorimo o velikem »temnem polju« kibernetske kriminalitete, kar je z vidika slovenske kriminalne politike zelo neugodno, po drugi strani pa omogoča odlične razmere za delovanje kibernetskih storilcev.

6 SKLEP

Kot pravi Jurij Ferme, nekdanji direktor Uprave kriminalistične policije: »Boj proti kibernetski kriminaliteti zahteva od organov pregona velike vložke, tako finančne kot kadrovske, zato je treba poiskati načine za boljšo izmenjavo specifičnih znanj, metodologij in sistemov dela organov pregona na področju preiskovanja kibernetske kriminalitete in računalniške forenzike; pri tem je pomembno tudi sodelovanje med zasebnim in javnim sektorjem.« (Uprava kriminalistične policije, 2011)

Boj proti kibernetski kriminaliteti v Sloveniji poteka na več ravneh. Center za računalniško preiskovanje pri Upravi kriminalistične policije s svojim štirimi oddelki (SKP Koper, Ljubljana, Celje in Maribor) je zadolžen za preiskavo zaseženih e-naprav oz. e-podatkov in preiskovanje kaznivih dejanj kibernetske kriminalitete. Druga nacionalna organizacija, ki kot sestavni del javnega zavoda »Arnes« deluje v preiskavi kibernetskih kaznivih dejanj, je SI-CERT, ki je velika opora pri preiskovanju kibernetske kriminalitete, ne samo zaradi strokovnosti zaposlenih, temveč tudi zaradi povezanosti s sorodnimi mednarodnimi organizacijami, kar omogoča mednarodno povezovanje in izmenjavo podatkov. Januarja 2013 je v okviru Europola začel delovati Evropski center za kibernetsko kriminaliteto. Zagotavlja boljšo operativno podporo zmogljivosti za boj proti čezmejni kriminaliteti na ravni EU, specializirane strateške ocene in ocene ogroženosti, bolj osredotočena usposabljanja ter raziskave in razvoj, ki spodbujajo razvoj posebnih orodij za boj proti kibernetski kriminaliteti. V Sloveniji so poleg državnih in mednarodnih preiskovalnih organizacij prisotna tudi zasebna informacijsko-varnostna podjetja, ki opravljajo analize in skrbijo za obvladovanje kibernetskih tveganj.

Pravna podlaga kibernetske kriminalitete je v Sloveniji del različnih nacionalnih in mednarodnih pravnih aktov, pri katerih je razvidno permanentno spreminjanje in izboljšanje. Kljub napredni pravni podlagi se v času, za katerega je značilno hitro povečevanje kibernetske kriminalitete, v Sloveniji prijavlja in obravnava malo kaznivih dejanj, še manj pa se jih konča s pravnomočno obsodbo. (Ne) učinkovitost organov pregona je predvsem odvisna od razpoložljivih finančnih sredstev. Večja državna finančna spodbuda organom pregona bi pomenila večjo tehnološko opremljenost in njeno vzdrževanje, ustrezno in permanentno usposabljanje zaposlenih in pridobivanje vodstvenih kadrov, boljšo mednarodno

13 *Bernik in Meško (2011) ugotavljata, da je bilo 57,8 odstotka slovenskih spletnih uporabnikov žrtev okužbe z virusi; skoraj 25 odstotkov jih je doživelo nadlegovanje po e-pošti. Z drugimi dejanji kibernetske kriminalitete pa se je srečalo manj kot deset odstotkov anketiranih spletnih uporabnikov.*

14 *Dimc in Dobovšek (2010) ugotavljata, da je 54 odstotkov anketiranih slovenskih spletnih uporabnikov že zagrešilo kakšno obliko kaznivega kibernetskega dejanja.*

povezavo itn. Res je, da ima slovenska Uprava kriminalistične policije posebna pooblastila v boju proti kriminaliteti, vendar se policija brez sodelovanja z drugimi nacionalnimi in mednarodnimi organizacijami in njihove pomoči ne more ustrezno boriti proti kibernetskim prestopnikom. Slovenska organizacija CERT in zasebne informacijsko-varnostne preiskovalne organizacije so lahko izjemna opora organom pregona. Poleg tega, da poročilo agencije ENISA (2012) govori o potrebi po večjem sodelovanju med organizacijami CERT in organi pregona, ni veliko dokazov o sodelovanju med Upravo kriminalistične policije in slovenskim CERT-om. Povečanje števila konkretnih dokazov o učinkovitem in zavzetem delu organov pregona bi lahko izboljšalo sodelovanje in spodbudilo uporabnike kibernetskega prostora, da bi pogosteje prijavljali kazniva dejanja. Splošno razširjeno zaupanje v delo organov pregona ni samo pokazatelj zadovoljstva javnosti z njihovim delovanjem, temveč lahko močno vpliva na povečanje učinkovitosti pravosodnih organov v boju proti kibernetski kriminaliteti.

Za boljše razumevanje kibernetske kriminalitete in njene kriminološke opredelitve imajo raziskave na tem področju pomembno vlogo. Za nadaljnje delo avtorji predlagamo podrobno preučevanje povezanosti in sodelovanja med slovenskim Centrom za računalniško preiskovanje in drugimi nacionalnimi in mednarodnimi organizacijami ter preučevanje legitimnosti organov pregona kot možen vzrok njihove (ne)učinkovitosti. Tako se bodo podrobneje izpostavile težave, s katerimi se srečujejo slovenski organi pregona, in predlagala priporočila za učinkovitejši boj proti kibernetski kriminaliteti.

LITERATURA

Anderson, R., Barton, C., Bohme, R., Clayton, R., van Eeten, M., Levi, M. et al. (2012). *Measuring the cost of cybercrime.* 11th Workshop on the Economics of Information Security, Berlin, Germany. Pridobljeno na http://weis2012.econinfosec.org/papers/Anderson_WEIS2012.pdf

Anonymous napadel še pedofile. (22. 10. 2011). *Žurnal24.si.* Pridobljeno na http://www.zurnal24.si/anonymous-napadel-pedofile-clanek-138518

Arnes. (2012). *Predstavitev zavoda Arnes.* Pridobljeno na http://www.arnes.si/zavod-arnes/predstavitev.html

Arnes. (2013). *Neželena elektronska sporočila (spam) in slovenska zakonodaja.* Pridobljeno na http://www.arnes.si/pomoc-uporabnikom/varnostna-priporocila/nezelena-elektronska-posta-spam/zakonodaja.html

AusCERT. (2005). *Australian 2005 computer crime and security survey*. Pridobljeno na http://www.auscert.org.au/images/ACCSS2005.pdf

AusCERT. (2006). *Australian 2006 computer crime and security survey.* Pridobljeno na *http://www.auscert.org.au/images/ACCSS2006.pdf*

AusCERT. (2010). *Australian 2010/2011 computer crime and security survey.* Pridobljeno na https://cours.etsmtl.ca/log619/documents/divers/CSIsurvey2010.pdf

Banovič, Z. (1. 7. 2007). Stopiti na prste kiber kriminalcem. *Mojmikro.si*. Pridobljeno na http://www.mojmikro.si/preziveti/varnost/stopiti_na_prste_kiber_kriminalcem

Bernik, I. in Meško, G. (2011). Internetna študija poznavanja kibernetskih groženj in strahu pred kriminaliteto. *Revija za kriminalistiko in kriminologijo, 62*(3), 242–252.

Bernik, I. in Prislan, K. (2011). Proces upravljanja s tveganji v informacijski varnosti. V T. Pavšič Mrevlje (ur.), *Smernice sodobnega varstvoslovja: zbornik prispevkov* (str. 11). Ljubljana: Fakulteta za varnostne vede.

Bernik, I. in Prislan, K. (2012). *Kibernetska kriminaliteta, informacijsko bojevanje in kibernetski terorizem.* Ljubljana: Fakulteta za varnostne vede.

Bogataj Jančič, M. (2008). *Avtorsko pravo v digitalni družbi.* Ljubljana: Pasadena.

Bossler, A. M. in Holt, T. J. (2012). Patrol officers' perceived role in responding to cybercrime. *Policing: An International Journal of Police Strategies & Management, 35*(1), 165–181.

Brenner, S. W. (2007). Private-public sector cooperation in combating cybercrime: In search of a model. *Journal of International Commercial Law and Technology, 2*(2), 58–67.

Broadhurst, R. (2006). Developments in the global law enforcement of cybercrime. *Policing: An International Journal of Police Strategies & Management, 29*(2), 408–433.

Burns, R. G., Whitworth, K. H. in Thompson, C. Y. (2004). Accessing law enforcement preparedness to address internet fraud. *Journal of Criminal Justice, 32*(5), 477–493.

Chevreau, F. R. (2006). Safety culture as a rational myth: Why developing safety culture implies engineering resilience? V E. Hollnagel in E. Rigaud (ur.), *Proceedings of the Second Resilience Engineering Symposium* (str. 63–73). Pridobljeno na http://www.resilience-engineering-association.org/download/resources/symposium/symposium-2006(2)/Chevreau_R.pdf

Council of Europe. (2013). *Convention on cybercrime: Chart of signatures and ratifications*. Pridobljeno na http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG

Davis, J. T. (2012). Examining perceptions of local law enforcement in the fight against crimes with a cyber component. *Policing: An International Journal of Police Strategies & Management, 35*(2), 272–284.

Dashora, K. (2011). Cyber crime in the society: Problems and preventions. *Journal of Alternative Perspectives in the Social Sciences, 3*(1), 240–259.

Dimc, M. in Dobovšek, B. (2010). Perception of cyber crime in Slovenia. *Varstvoslovlje, 12*(4), 378–396.

Enisa. (2011). *Slovenia country report*. Pridobljeno na http://www.enisa.europa.eu/activities/stakeholder-relations/files/country-reports/Slovenia.pdf

Enisa. (2012). *The fight against cybercrime: Cooperation between CERTs and law enforcement agencies in the fight against cybercrime*. Pridobljeno na http://www.enisa.europa.eu/activities/cert/support/fight-against-cybercrime/supporting-fight-against-cybercrime

Eurojust. (2012). *Mission and tasks.* Pridobljeno na http://eurojust.europa.eu/about/background/Pages/mission-tasks.aspx

Europol. (21. 1. 2013). *New European cybercrime centre (EC3) opens at Europol*. Pridobljeno na https://www.europol.europa.eu/node/1899

Gabor, M. (2010). Informacijska varnost v 2009 in kaj prinaša 2010. V *Dnevi slovenske informatike: zbornik prispevkov.* Pridobljeno na http://www.tehnokratis.si/documents/Gabor-Informacijska-varnost-v-2009.pdf

González, T. S. (2008). *Interpol's role fighting cyber crime.* Pridobljeno na http://www.nyu.edu/intercep/lapietra/Interpol_Cyber.pdf

Halder, D. in Jaishankar, K. (2010). *Cyber crime victimization in India: A baseline survey report Centre for Cyber Victim Counseling* (CCVC). Pridobljeno na http://cybervictims.org/CCVCresearchreport2010.pdf

Hinduja, S. (2004). Perceptions of local and state law enforcement concerning the role of computer crime investigative teams. *Policing: An International Journal of Police Strategies & Management, 27*(3), 341–357.

Holt, T. J., Bossler, A. M. in Fitzgerald, S. (2010). Examining state and local law enforcement perceptions of computer crime. V T. J. Holt (ur.), *Crime on-line: Correlates, causes, and context* (str. 221–46). North Carolina: Carolina Academic Press.

Huey, L., Nhan, J. in Broll, R. (2012). 'Uppity civilians' and 'cyber-vigilantes': The role of the general public in policing cyber-crime. *Criminology & Criminal Justice, 13*(1), 81–97.

Intervju s Tonijem Kastelicem, vodjo Centra za računalniško preiskovanje. (30. 8. 2012). *Web-center.si*. Pridobljeno na http://web-center.si/forenzika/397-intervju-z-tonijem-kastelicom-vodjo-centra-za-racunalniko-preiskovanje

Kalčina, L. (2005). *Evropska konvencija o varstvu človekovih pravic in temeljnih svoboščin (EKČP) s Poslovnikom Evropskega sodišča za človekove pravice*. Ljubljana: Informacijsko dokumentacijski center Sveta Evrope pri Narodni in univerzitetni knjižnici.

Kazenski zakonik [KZ-1]. (2008). *Uradni list RS,* (55/08).

Kazenski zakonik [KZ-1-UPB2]. (2012). *Uradni list RS,* (50/12).

Krone, T. in Johnson, H. (2007). Internet purchasing: perceptions and experiences of Australian households. *Trends & Issues in Crime and Criminal Justice*, (330). Pridobljeno na http://aic.gov.au/documents/8/6/5/%7B8651CA28-C510-4B51-BA5E-EDF2F3665347%7Dtandi330.pdf

McQuade, S. (2006). Technology-enabled crime, policing and security. *Journal of Technology Studies, 32*(1), 32–42.

Meško, G. (2002). *Osnove preprečevanja kriminalitete*. Ljubljana: Visoka policijsko-varnostna šola.

Norton. (2011). *Norton cybercrime report*. Pridobljeno na http://us.norton.com/content/en/us/home_homeoffice/html/cybercrimereport/

Norton. (2012). *Norton cybercrime report*. Pridobljeno na http://now-static.norton.com/now/en/pu/images/Promotions/2012/cybercrimeReport/2012_Norton_Cybercrime_Report_Master_FINAL_050912.pdf

Peršak, N. (2009). Virtualnost, (ne)moralnost in škodljivost: normativna vprašanja nekaterih oblik kibernetične kriminalitete. *Revija za kriminalistiko in kriminologijo, 60*(3), 191–198.

Policija. (2006–2013). *Letna poročila o delu policije v letih 2005–2012*. Pridobljeno na http://www.policija.si/index.php/statistika/letna-poroila

Policija. (30. 7. 2010). *Kriminalistična preiskava računalniške kriminalitete slovenske policije v sodelovanju z ameriškim FBI – informacija z novinarske konference.* Pridobljeno na http://www.policija.si/index.php/component/content/article/35-sporocila-za-javnost/8923-kriminalistina-preiskava-raunalnike-kriminalitete-slovenske-policije-v-sodelovanju-z-amerikim-fbi-informacija-z-novinarske-konference

Policija. (2012). *Twinning projekti, evropske subvencije.* Pridobljeno na http://www.mnz.gov.si/si/policija_varnost_in_nadzor/svoboda_varnost_in_pravicnost/twinning_projekti_evropske_subvencije/

Program Varnejši internet v Sloveniji: javno letno poročilo. (2012). Pridobljeno na http://www.safe.si/uploadi/editor/1369051766Centerzavarnejsiinternet-letnoporocilo.pdf

RAND Europe. (2012). *Feasibility study for a European Cybercrime Centre*: *Final report.* Pridobljeno na http://www.rand.org/content/dam/rand/pubs/technical_reports/2012/RAND_TR1218.pdf

Prava ideja: Računalniški detektiv. (2. 2. 2010). *Rtvslo.si.* Pridobljeno na http://www.rtvslo.si/pravaideja/novica/127

Rupnik, A. (2003). *Konvencija o kibernetski kriminaliteti »Budimpeštanska konvencij*a«. Štirinajsta delavnica o telekomunikacijah VITEL, Brdo pri Kranju, Slovenija, 19. in 20. maj, 2003. Pridobljeno na http://www.ltfe.org/wp-content/pdf/Kiber_kriminaliteta.pdf

Senjo, S. R. (2004). An analysis of computer-related crime: Comparing police officer perceptions with empirical data. *Security Journal, 17*(2), 55–71.

SI-CERT. (2013). *Poročilo o omrežni varnosti za leto 2012.* Pridobljeno na http://www.cert.si/fileadmin/slike/si-cert/fokus/2013/SI-CERT_porocilo_2012.pdf

Sommer, P. (2004). The future for the policing of cybercrime. *Computer Fraud & Security*, (1), 8–12.

Stambaugh, H., Beaupre, D. S., Icove, D. J., Baker, R., Cassady, W. in Williams, W. P. (2001). *Electronic crime needs assessment for state and local law enforcement*. Washington: National Institute of Justice.

Statistični urad Republike Slovenije. (2012). *Polnoletni obsojenci (znani storilci) po spolu, kaznivem dejanju in glavni kazenski sankciji, Slovenija, letno.* Pridobljeno na http://pxweb.stat.si/pxweb/Dialog/varval.asp?ma=1360301S&ti=&path=../Database/Dem_soc/13_kriminaliteta/01_statistika_toz_sodisc/03_13603_obsojene_poln_osebe/&lang=2

Strniša, S. (31. 7. 2010). Vse več zlikovcev za računalniki. *Rtvslo.si.* Pridobljeno na http://www.rtvslo.si/crna-kronika/vse-vec-zlikovcev-za-racunalniki/235937

Svetek, S. in Kebe, J. (2003). Strategija računalniškega preiskovanja in analitske dejavnosti na področju kriminalitete. V M. Pagon (ur.), *Četrti slovenski dnevi varstvoslovlja: zbornik prispevko*v (str. 7). Ljubljana: Visoka policijsko – varnostna šola.

United Nations. (2000). *Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders,* Vienna, 10-17 April 2000. Pridobljeno na http://www.uncjin.org/Documents/congr10/4r3e.pdf

Uprava kriminalistične policije. (24. 10. 2011). *Na CEPOL seminarju so o kibernetski kriminaliteti spregovorili strokovnjaki iz 15 držav.* Pridobljeno na http://www.policija.si/index.php/component/content/article/267-prispevki/60771-na-cepol-

seminarju-so-o-kibernetski-kriminaliteti-spregovorili-strokovnjaki-iz-15-drav-?lang=

Ustava Republike Slovenije. (2006). *Uradni list RS,* (68/06).

Varni na internetu. (2013). *Cilji projekta.* Pridobljeno na https://www.varninainternetu.si/cilji-projekta/

Wall, D. S. (2007). *Cybercrime: The transformation of crime in the information age*. Malden: Polity.

Wall, D. S. (2007/2010). Policing cybercrimes: Situating the public police in networks of security within cyberspace. *Police Practice & Research: An International Journal, 8*(2), 183–205. Pridobljeno na http://www.google.si/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&ved=0CDEQFjAB&url=http%3A%2F%2Fwww.cyberdialogue.ca%2Fwp-content%2Fuploads%2F2011%2F03%2FDavid-Wall-Policing-CyberCrimes.pdf&ei=ePE2UtvmGdDHswbYx4DICw&usg=AFQjCNHtEHhy_jwjA61MUN_0OOTWC2INEg&bvm=bv.52164340,d.Yms

Wilson, C. (2008). *Botnets, cybercrime, and cyberterrorism: Vulnerabilities and policy issues for congress*. Pridobljeno na http://fas.org/sgp/crs/terror/RL32114.pdf

Yazdanifard, R., Oyegoke, T. in Seyedi, A. P. (2011). Cyber-crimes: Challenges of the millennium age. V D. Zeng (ur.), *Advances in electrical engineering & electrical machines* (str. 527–534). Berlin: Springer.

Zakon o kazenskem postopku. (2012). *Uradni list RS*, (32/12).

O avtorjih:

Aleksandar Ilievski, magister varstvoslovja, doktorski študent na Fakulteti za varnostne vede, Univerza v Mariboru. E-mail: ilievski.aleksandar86@gmail.com

Dr. Igor Bernik, docent za informacijsko varnost, predstojnik katedre za informacijsko varnost in prodekan za izobraževalno dejavnost, Fakulteta za varnostne vede, Univerza v Mariboru. E-mail: igor.bernik@fvv.uni-mb.si

VARSTVOSLOVJE,
let. 15
št. 3
str. 338–356

Percepcija kibernetske kriminalitete pri nekaterih uporabnikih interneta v Sloveniji in ZDA

Maja Dimc, Bojan Dobovšek

Namen prispevka:

Namen prispevka je analizirati problematiko kibernetske kriminalitete kot sodobne varnostne grožnje v povezavi z ozaveščenostjo in delovanjem posameznika v kibernetskem prostoru. Na podlagi empirične raziskave, izvedene v Sloveniji in Združenih državah Amerike, je izpostavljena problematika ozaveščenosti splošne javnosti na področju kibernetske kriminalitete v povezavi z njihovim preventivnim delovanjem v kibernetskem prostoru in odnosom do organov pregona s ciljem opredelitve ključnih razlik med percepcijo, vedenjem in delovanjem posameznikov glede na njihovo fizično življenjsko okolje (Slovenija in ZDA).

Metode:

Za potrebe prispevka je bila izvedena empirična raziskava, ki je vključevala dve skupini anketirancev, in sicer skupino posameznikov v Sloveniji ter skupino posameznikov v ZDA. Uporabljeno je bilo neeksperimentalno raziskovanje; za zbiranje podatkov je bil uporabljen anketni vprašalnik, s katerim smo merili poznavanje problematike, stališča in vedenje posameznikov v povezavi s pojavom kibernetske kriminalitete.

Ugotovitve:

Raziskava je pokazala pomembno razliko med ozaveščenostjo posameznikov in njihovim dejanskim varnostnim ravnanjem v virtualnem okolju, ki se v osnovi ne razlikuje glede na fizično lokacijo posameznika. Drugače pa je z občutkom varnosti, kjer se fizična lokacija preslika v virtualno okolje, saj so anketiranci živeči in delujoči v manjši državi (Slovenija) izrazili višjo stopnjo občutka varnosti v virtualnem okolju kot anketiranci živeči in delujoči v večji državi (Združene države Amerike). Poleg tega je bilo v okviru raziskave ugotovljeno, da obstaja nezaupanje in skepticizem glede usposobljenosti organov pregona za obravnavo primerov kibernetske kriminalitete, kar se odraža v potencialno manjši verjetnosti prijave in posledične obravnave kaznivih dejanj kibernetske kriminalitete. Z vidika ozaveščanja splošne javnosti s ciljem dosega visokega nivoja varnostnega ravnanja bi bilo potrebno povečati količino aktivnosti, povezanih z ozaveščanjem, hkrati pa bi se morali posvetiti tudi aktivnostim, ki bi zviševale stopnjo zaupanja v delovanje organov pregona.

Omejitve/uporabnost raziskave:

Omejitev raziskave izhaja iz načina zbiranja podatkov, saj je bila uporabljena metoda snežne kepe. Število udeležencev pri raziskavi je bilo dokaj majhno, zato bi bilo nadaljnje raziskave priporočljivo razširiti v smislu vključenosti večjega dela populacije.

Praktična uporabnost:

Rezultati raziskave imajo praktično vrednost na področju implementacije procesov preprečevanja kibernetske kriminalitete, in sicer primarno ozaveščanja splošne javnosti glede pomena lastne informacijske varnosti, saj je bil v okviru raziskave potrjen pomemben razkorak med znanjem in dejansko implementacijo osnovnih tehnik zagotavljanja informacijske varnosti.

Izvirnost/pomembnost prispevka:

Prispevek obravnava problematiko kibernetske kriminalitete in informacijske varnosti v Sloveniji in ZDA, pri čemer poskuša ugotoviti ključne razlike med varnostnim vedenjem in delovanjem posameznikov glede na fizično življenjsko okolje. Ugotovitve raziskave predstavljajo izhodiščno točko za nadaljnje raziskave pojavnosti kibernetske kriminalitete in implementacije informacijske varnosti.

UDK: 343.9:004

Ključne besede: kibernetska kriminaliteta, informacijska varnost, informacijsko-komunikacijske tehnologije, informacijska varnostna kultura

Perception of Cybercrime by Selected Internet Users in Slovenia and USA

Purpose:

The purpose of the article is to analyze the issue of cybercrime as a contemporary security threat as it relates to awareness levels and behavior of an individual in the cyberspace. Based on the empirical research performed in Slovenia and United States of America, the article discusses the issue of user awareness in the field of cybercrime, their consequent preventive behavior in the cyberspace, and their attitude toward law enforcement agencies with the aim of establishing the crucial differences between perception, knowledge and actual behavior of individuals based on their physical everyday environment (Slovenia and USA).

Design/Methods/Approach:

For the purpose of this article, an empirical research involving two groups of participants, a group of individuals from Slovenia and a group of individuals from the United States of America, was performed. Non-experimental research method was used; a survey questionnaire was used for collection of data regarding the level of familiarity, opinion and behavior of individuals as it relates to the issue of cybercrime.

Findings:

The research found an important discrepancy between the level of awareness regarding online safety and the actual behavior of individuals in the virtual environment, which does not differ due to the physical location of the individual. However, when it comes to the feeling of safety, the physical location of an

individual influences his/her feeling of safety while in cyberspace; namely, the research found that the participants living and working in a small country (Slovenia) are also feeling safer in the virtual environment than do the participants living and working in a large country (United States of America). Furthermore, in the framework of this research, we found a concerning level of distrust and skepticism regarding the investigative capabilities of law enforcement in the field of cybercrime, which results in potentially lower reporting rate and consequent lower level of prosecution cases. In terms raising the level of awareness of the general public with the aim of reaching a high level of safeguarding behavior, the level of activities related to awareness, as well as activities related to raising the level of trust in the capabilities of law enforcement, should be increased.

Research Limitations/Implications:

Research limitations are primarily due to the manner of data collection, since we used the snowball sampling method. Additionally, the number of participants if rather low; therefore, further research should be broadened in order to include a wider population range.

Practical Implications:

The research results have practical value in the field of the implementation of the processes of cybercrime prevention, and primarily in the field of raising the level of awareness of the general public regarding the importance of personal information safety, since our research confirmed a discrepancy between the level of knowledge and the level of actual implementation of the basic techniques of information safety assurance.

Originality/Value:

The article discusses the issue of cybercrime and information security in Slovenia and the United States of America. We attempted to find the key differences between safeguarding knowledge and behavior of individuals based on their physical living environment. The findings of the research represent a starting point for further comparison of the incidence of cybercrime and implementation of information security.

UDC: 343.9:004

Keywords: cybercrime, information assurance, information communication technologies, information security culture

1 UVOD

Informacijsko-komunikacijske tehnologije (IKT) ključno vplivajo na delovanje sodobne družbe kot celote. Z razvojem interneta in svetovnega spleta se je razvil kibernetski oz. virtualni prostor, ki se vedno bolj prepleta s fizičnim prostorom. Skupaj s širjenjem funkcionalnosti svetovnega spleta se eksponentno povečuje količina uporabnikov[1] ter tudi vključevanje najrazličnejših naprav v kibernetski

1 *Število uporabnikov interneta se je, zaradi preproste uporabe in eksponentne rasti ponujenih informacij, od leta 2000 do leta 2012 v svetovnem merilu povečalo za 566 % in je v letu 2012 preseglo*

prostor in se dejansko premikamo v smeri omreženja celotne družbene infrastrukture[2]. Prednosti pa s seboj prinašajo tudi določene slabosti in ranljivosti, saj kot pravi Kanduč (v Kovačič et al., 2010: 1) »tehnologija povečuje družbeno in človeško moč in silo, obenem pa tudi odvisnost, nebogljenost in vsakovrstne utvare«.

Informacijsko-komunikacijska tehnologija je, v kombinaciji z delovanjem v kibernetskem prostoru, postala del vsakdanjega življenja, hkrati pa se delovanje organizacij in posameznikov v kibernetskem prostoru ni primerno prilagodilo. Prednosti IKT, kot so dostopnost, povezljivost, razširjenost, avtomatizacija ter seveda prostorska in časovna neomejenost, so lahko tudi največje pasti (Britz, 2009; Dimc, 2009; Taylor, Caeti, Loper, Fritsch in Liederbach, 2006; Wall, 2007). Ključne značilnosti kibernetskega prostora, kot so odsotnost mej, hitrost razvoja, anonimnost akterjev ter avtomatske metode, se hkrati uvrščajo med temeljne značilnosti kibernetskih groženj (Dunn, 2005). Ob tem pa virtualni vidik kibernetskega prostora deluje potencialno zavajajoče, saj se delovanje v takšnem okolju prepogosto dojema kot zgolj virtualno in posledično brez bistvenega vpliva na resnični svet. Shea (2004) tako poudarja, da elektronska naprava deluje kot vmesnik, zaradi katerega se zmanjša percepcija posledic dejanj, izvedenih v kibernetskem prostoru. Na neki način se torej zabriše meja med resničnim in fantazijskim ter ustvari »disinhibicijski učinek«, posledično uporabniki ne čutijo odgovornosti za svoja dejanja v kibernetskem prostoru, četudi gre za nasilno in v resničnem svetu nesprejemljivo vedenje (Suler, 2004). Kljub temu pa sta tako informacijsko-varnostna ozaveščenost in usposobljenost kot tudi človeški vidik informacijske varnosti še vedno le redko obravnavana (Dlamini, Eloff in Eloff, 2009).

Količina kibernetske kriminalitete narašča skupaj s količino ponujenih funkcionalnosti v kibernetskem prostoru in širjenjem uporabe interneta. Uporaba interneta v Sloveniji in ZDA je primerljiva, in sicer je v Sloveniji v letu 2012 internet uporabljalo 70 % prebivalcev (Raba interneta v Sloveniji, 2011), v ZDA pa 78 % prebivalcev (Miniwatts Marketing Group, 2013). V Sloveniji je število prijavljenih incidentov od leta 2008 do leta 2012 naraslo za skoraj 300 % (SI-CERT, 2012), medtem ko se število prijavljenih incidentov v ZDA v teh letih sicer ni bistveno spremenilo, le za dobrih 5 %, vendar pa se je povečala nastala finančna škoda (Internet Crime Complaint Center, 2008, 2012). Glede na populacijo v izbranih državah je število prijav primerljivo, in sicer v Sloveniji 0,14 %, v ZDA pa 0,09 %. Število prijavljenih napadov ribarjenja za podatki in goljufij je Sloveniji v enem letu naraslo kar za 100 % (SI-CERT, 2012), tudi v ZDA so takšne oblike kibernetske kriminalitete v porastu, in sicer je bilo v letu 2012 prijavljenih kar 14.141 primerov goljufij z uporabo elektronske pošte, pri čemer je prišlo do finančne škode več kot 4 milijone USD (Internet Crime Complaint Center, 2012).

V okviru predstavljene raziskave smo poskušali analizirati delovanje posameznika v kibernetskem prostoru glede na njegovo poznavanje in razumevanje

2,4 milijarde (Miniwatts Marketing Group, 2013).

2 *Gre za povezavo širokega spektra fizičnih naprav z internetom (npr. semaforji, elektronski prometni znaki, gospodinjski aparati itd.), kar poimenujemo »internet stvari«, ki omogoča dostop do oddaljenih podatkov in izvajanje fizičnega nadzora ne glede na lokacijo (Kopetz, 2011).*

pojava kibernetske kriminalitete, s tem povezano preventivno delovanje in odnos do organov pregona ter ugotoviti ključne razlike med vedenjem in delovanjem posameznikov v manjši državi (Sloveniji), kjer smo predpostavljali, da se uporabniki počutijo varnejše, in večji državi (ZDA), kjer smo predpostavljali večjo občutljivost posameznikov glede potencialnih nevarnosti. Ugotovitve raziskave predstavljajo izhodiščno točko za nadaljnje primerjave pojavnosti kibernetske kriminalitete in implementacije informacijske varnosti v prihodnosti.

Varnost v povezavi z informacijsko-komunikacijskimi tehnologijami običajno povezujemo s tveganji, pri čemer varnostno tveganje dejansko pomeni razmerje med tveganjem in nevarnostjo; posameznik je tisti, ki odloča o tveganju na podlagi lastne presoje, kar posledično vpliva na njegova dejanja (Rančigaj, 2010). V kibernetskem prostoru se posamezniki sicer zavedajo potencialnih tveganj, vendar jih v veliki meri ne percipirajo kot realne nevarnosti[3]. Posledično so varnostni incidenti v povezavi z informacijsko-komunikacijskimi tehnologijami v veliki meri rezultat neprimernega vedenja, neznanja, neozaveščenosti, ki pretvori obstoječo grožnjo v realno nevarnost.

Razvoj informacijsko-komunikacijskih tehnologij in oblikovanje sodobnega kibernetskega prostora nedvomno vpliva na družbene konstrukte in zaznavo stvarnosti, saj le-ta v kibernetskem prostoru ni niti lokacijsko niti časovno omejena. Ob tem se je treba zavedati, da ima danes posameznik, preko uporabe sodobnih tehnologij, možnost fizičnega, elektronskega ter tudi psihološkega vplivanja na stabilnost ključne informacijske infrastrukture in družbe kot celote (Hundley et al., 2007). Hkrati pa je zaščita sodobnih informacijsko-komunikacijskih tehnologij večplasten postopek (Markelj in Bernik, 2011), ki mora vključevati tako tehnične kot tudi sociološke vidike zagotavljanja varnosti.

Sodobna varnostna paradigma se osredotoča na tri ključne dileme, in sicer referenčne objekte varnosti (na koga se varnost nanaša), grožnje varnosti (kdo ali kaj to varnost ogroža) in varnostne mehanizme (kako varnost zagotavljati) (Liotta v Svete, 2005). V povezavi s sodobnimi tehnologijami ugotavljamo, da posameznik igra pomembno vlogo v vsakem od teh referenčnih objektov, saj se zagotavljanje varnosti nedvomno nanaša na posameznika, hkrati pa je ravno posameznik tisti, ki lahko namerno ali pa nenamerno predstavlja ključno varnostno grožnjo, zato je za zagotavljanje varnosti ključnega pomena okrepiti najšibkejši člen verige – posameznika. Ravno posameznik namreč predstavlja najpomembnejši del varnostnega procesa in »ključ do učinkovite stopnje informacijske varnosti« (Lobnikar, Prislan, Markelj in Banutai, 2012).

Pojem kibernetske kriminalitete je v uporabi že nekaj časa, vendar pa še vedno ni opredeljen dejanski obseg pojava, niti ni vzpostavljena enotna definicija, kar nedvomno negativno vpliva tako na preprečevanje kot tudi pregon (Gordon in Ford, 2006). Problematiko postavitve jasne definicije lahko pripišemo hitremu razvoju oblik kibernetske kriminalitete, ki se je v kratkem obdobju 20-ih let razvila od preprostih oblik zlorabe informacijsko-komunikacijskih tehnologij za

3 *Razliko med percepcijo tveganja in realno nevarnostjo Flaker (1994) zanimivo ponazori s primerom bananinega olupka, in sicer bananin olupek na tleh predstavlja grožnjo, da nam spodrsne in pademo, vendar pa olupek na tleh še ne pomeni, da nam bo na njem dejansko spodrsnilo (nevarnost). Tveganja in grožnje predstavljajo predpogoj za nevarnost, vendar pa to še ne pomeni dejanske nevarnosti.*

izvedbo tradicionalnih kaznivih dejanj do današnjih sodobnih kompleksnih visoko tehnoloških dejanj, izvedenih v celoti v kibernetskem prostoru. Definicije so tako dokaj splošne in poskušajo zajeti čim širši krog dejanj, ki bi jih lahko uvrstili v okvir kibernetske kriminalitete. Komisija evropskih skupnosti kibernetsko kriminaliteto opredeli dokaj ozko, in sicer kot »kazniva dejanja, storjena z uporabo elektronskih komunikacijskih omrežij in informacijskih sistemov ali proti takšnim omrežjem in sistemom« (Komisija evropskih skupnosti, 2007). Veliko širšo definicijo pa postavita Bernik in Meško, ki kibernetsko kriminaliteto opredelita kot »uporabo informacijsko-komunikacijskih tehnologij za izvedbo kaznivih dejanj« (Bernik in Meško, 2011).

Problematika preprečevanja in pregona kibernetske kriminalitete je močno povezana z virtualnim vidikom kibernetskega prostora, ki vpliva na percepcijo posameznika z vidika »virtualizacije« dejanj, izvedenih v kibernetskem prostoru. Posledično posameznik problematike ne vidi kot ogrožajoče, vse dokler se posledice ne odrazijo v fizičnem svetu. Strah pred kriminaliteto lahko vpliva na delovanje posameznika v fizičnem svetu (Meško, Petrovec, Areh, Muratbegović in Rep, 2006), le-to pa ne pomeni, da posamezniki občutek varnosti/nevarnosti dejansko prenesejo tudi v virtualno okolje. Namreč, v kibernetskem prostoru vsakdo predstavlja potencialno žrtev[4], vprašanje pa je, ali posamezniki grožnje tudi dojemajo na takšen način in kako le-to vpliva na njihovo delovanje v kibernetskem prostoru. Raziskava Eurobarometra je sicer pokazala, da uporabnike interneta skrbi kibernetska varnost, in sicer je kar 74 % sodelujočih izrazilo mnenje, da se je tveganje, da postanejo žrtev kibernetske kriminalitete povečalo v zadnjem letu, toda hkrati pa več kot polovica Evropejcev ne izvede primerih ukrepov za zaščito pred kibernetskimi kaznivimi dejanji[5] (Evropska komisija, 2012). Študija poznavanja kibernetskih groženj in strahu pred kriminaliteto v Sloveniji pa je pokazala, da se manj kot polovica ljudi strinja s tem, da je lahko »žrtev kibernetske kriminalitete vsakdo, ki uporablja računalnik«, kar nakazuje na nizko stopnjo ozaveščenosti ter hkrati tudi na dejstvo, da se za računalnikom mnogi počutijo varne, saj menijo, da kibernetski prostor nima stika z realnostjo in je ločen od realnega dogajanja (Bernik in Meško, 2011).

Kibernetski prostor predstavlja virtualno globalno okolje, zaradi česar zagotovitev sodelovanja organizacij na mednarodni ravni, opredelitev enotnih definicij pojmov, skupnih pravil delovanja in vzpostavitev sistema najboljših praks igra pomembno vlogo v boju proti kibernetski kriminaliteti. Ključna rešitev nedvomno leži v prevenciji, ki se mora osredotočiti na najšibkejši člen – povprečnega uporabnika. Ozaveščanje posameznikov na vseh ravneh je tako ključnega pomena za uspešno preprečevanje, omejevanje in tudi pregon kibernetske kriminalitete[6].

4 *Evropska komisija v svojem poročilu izpostavlja, da je dnevno približno milijon ljudi žrtev kibernetske kriminalitete. Poleg tega raziskava, izvedena s strani Evropske komisije v letu 2011, ocenjuje strošek kibernetske kriminalitete na svetovni ravni na 85 do 291 milijard EUR (Evropska komisija, 2012).*

5 *V raziskavi je sodelovalo cca 27.000 ljudi iz vseh držav članic EU (Evropska komisija, 2012).*

6 *Na področju kibernetske kriminalitete organi pregona praviloma delujejo zgolj represivno, in sicer je več kot 90 % primerov kibernetske kriminalitete obravnavanih na podlagi prijave posameznika ali organizacije (United Nations Office on Drugs and Crime, 2013).*

2 OPIS UPORABLJENE METODE IN VZORCA

V okviru raziskave problematike kibernetske kriminalitete kot sodobne varnostne grožnje v povezavi z ozaveščenostjo in vedenjem posameznika v kibernetskem prostoru je bilo uporabljeno neeksperimentalno raziskovanje družboslovnih pojavov, in sicer je tehnika zbiranja podatkov temeljila na metodi snežne kepe z uporabo elektronske pošte in socialnih omrežij. Pri uporabi metode snežne kepe naključno izberemo določeno število anketirancev, ki vprašalnik nadalje posredujejo svojim znancem; na takšen način se količina anketirancev veča kot snežna kepa ter učinkovito proizvaja vzorčno strukturo (Malhotra, 2002). Raziskava je bila izvedena v obliki elektronskih anketnih vprašalnikov z uporabo spletnega portala KwikSurveys (http://www.kwiksurveys.com). Oblikovana sta bila identična anketna vprašalnika, in sicer v slovenskem in angleškem jeziku. Anketna vprašalnika sta bila posredovana izbranim znancem preko elektronske pošte in socialnega omrežja, ki so ga nadalje posredovali svojim stikom. Prvi vprašalnik (v slovenskem jeziku) je bil tako posredovan posameznikom, ki živijo in delujejo v Sloveniji, drugi vprašalnik (preveden v angleški jezik) pa je bil posredovan posameznikom, ki živijo in delujejo v ZDA. Prvi vprašalnik je bil na razpolago 9 dni – v tem času je nanj odgovorilo 123 anketirancev, od tega so bili trije vprašalniki nepopolni, zato niso bili uporabljeni pri analizi. Drugi vprašalnik je bil odprt 11 dni – v tem času je nanj odgovorilo 81 anketirancev, pri čemer je bil en vprašalnik nepopoln in prav tako ni bil uporabljen pri analizi. V raziskavi je torej sodelovalo 200 anketirancev, pri čemer jih 40 % spada v skupino posameznikov živečih in delujočih na območju ZDA in 60 % v skupino posameznikov živečih in delujočih na področju Slovenije.

Omejitve raziskave izhajajo iz načina zbiranja podatkov, saj ne gre za preprosti naključni vzorec, ter iz velikosti obravnavanega vzorca, zato je treba te omejitve upoštevati pri generalizaciji podatkov. Razlog za tovrstno anketiranje je v predpostavki, da smo želeli v anketo vključiti aktivne spletne uporabnike, le-te pa je najlažje doseči z uporabo informacijskih tehnologij. Populacija anketirancev je tako vključevala posameznike na področju Slovenije ter posameznike na področju ZDA, ki aktivno uporabljajo internet. Na podlagi slednjega smo predpostavljali, da imajo anketiranci osnovno poznavanje informacijsko-komunikacijskih tehnologij. Anketiranje je bilo izvedeno v maju 2013, sodelovanje v raziskavi je bilo prostovoljno in anonimno.

Namen raziskave je analizirati ozaveščenost in delovanje posameznika v kibernetskem prostoru glede na njihovo poznavanje in razumevanje pojava kibernetske kriminalitete, s tem povezano preventivno delovanje in odnos do organov pregona ter ugotoviti ključne razlike med vedenjem in delovanjem posameznikov v posamični državi (Slovenija in ZDA) ter podati možnosti za izboljšavo področne problematike v Sloveniji. Anketni vprašalnik, oblikovan na podlagi preučene literature in obstoječih raziskav, je poleg splošnih demografskih podatkov vključeval naslednje vsebinske sklope: delovanje v kibernetskem prostoru, poznavanja varne rabe interneta in pojava kibernetske kriminalitete ter vedenje posameznika ob srečanju s kibernetsko kriminaliteto.

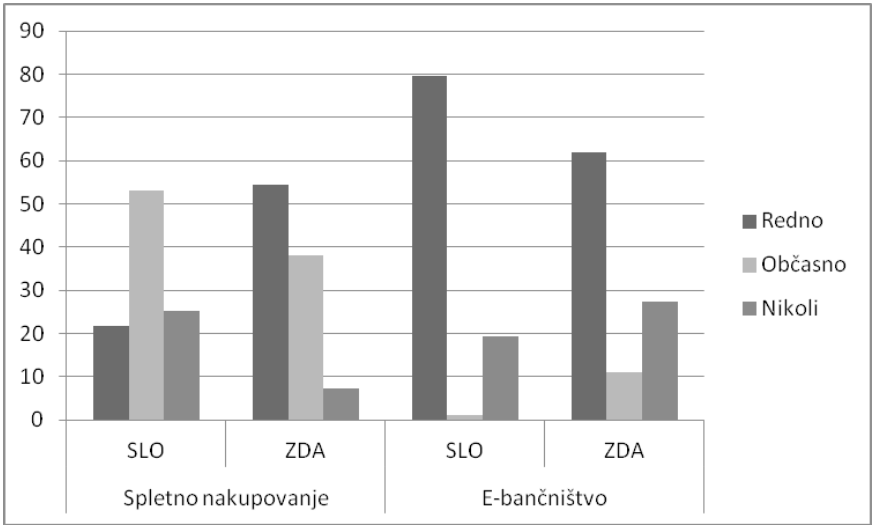
3 INTERPRETACIJA REZULTATOV RAZISKAVE

V nadaljevanju so prikazani rezultati analize zbranih podatkov, pri čemer smo se osredotočili na povezavo med znanjem oz. ozaveščenostjo, dejanskim vedenjem ter odnosom oz. percepcijo posameznika glede delovanja organov pregona na področju kibernetske kriminalitete v Sloveniji in ZDA. Analiza vključuje primerjavo med državama in povezavo na obravnavano problematiko pojavnosti, preprečevanja in pregona kibernetske kriminalitete.

3.1 Delovanje v kibernetskem prostoru

V okviru raziskave smo se najprej osredotočili na vprašanje delovanja posameznika v virtualnem prostoru, pri čemer nas je zanimala tako količina preživetega časa v kibernetskem prostoru kot tudi širina uporabljenih funkcionalnosti. V obeh skupinah anketirancev, torej tako skupini posameznikov, ki živijo in delujejo v Sloveniji (skupina SI), kot tudi skupini posameznikov, ki živijo in delujejo v ZDA (skupina ZDA), je količina časa preživetega v kibernetskem prostoru visoka, in sicer v obeh primerih cca 60 % anketirancev uporablja funkcionalnosti interneta več kot tri ure dnevno (skupina SI – 60 % in skupina ZDA – 66 %). Količina uporabe oz. preživetega časa v virtualnem okolju je torej v obeh skupinah primerljiva, nadalje pa nas je zanimalo, katere funkcionalnosti anketiranci uporabljajo.

Ena izmed najpogostejših oblik kibernetske kriminalitete je nedvomno kraja identitete, in sicer primarno kraja podatkov, povezanih z bančnimi računi (številke kreditnih kartic, dostopna gesla itd.), zato nas je najprej zanimalo, kako pogosto anketiranci uporabljajo spletne funkcionalnosti, ki vključujejo finančne prenose, in sicer smo se osredotočili na spletno nakupovanje z uporabo kreditne kartice in uporabo storitev e-bančništva (graf 1).



Graf 1: Spletne dejavnosti, povezane s finančnimi prenosi

V skupini SI največji odstotek (53 %) anketirancev izvaja nakupovanje preko spleta občasno[7], medtem ko največji delež anketirancev (55 %) skupine ZDA spletno nakupovanje izvaja redno[8]. Sklepamo, da gre v tem primeru za kulturne razlike in ne za odločitev, ki bi bila vezana na percepcijo večje ali manjše varnosti pri izvajanju spletnega nakupovanja. V nadaljevanju smo zato natančneje preučili povezavo med uporabo takšnih spletnih funkcionalnosti na eni strani ter poznavanjem pojavnih oblik kibernetske kriminalitete, občutkom lastne usposobljenosti glede spletne varnosti in občutkom varnosti v kibernetskem prostoru na drugi strani. E-bančništvo uporablja 81 % anketirancev skupine SI in 71 % anketirancev skupine ZDA, vendar pa je bistvena razlika v količini uporabe storitve, in sicer je pogostost uporabe e-bančništva višja v Sloveniji. V obeh primerih je uporaba e-bančništva široko razširjena, kar pripisujemo veliki stopnji zaupanja v varnost storitev, ki jih ponujajo bančne institucije.

Nadalje nas je zanimalo, ali je kakšna razlika v percepciji varnosti/nevarnosti kibernetskega okolja med obravnavanima skupinama, in sicer je raziskava pokazala, da imajo anketiranci v skupini SI močnejši občutek varnosti pri delovanju v kibernetskem prostoru, medtem ko se anketiranci v skupini ZDA čutijo bolj ogrožene, v okviru slednje skupine najvišji odstotek anketirancev meni, da kibernetski prostor ni preveč varen (57 %), medtem ko najvišji odstotek anketirancev v skupini SI meni, da je kibernetski prostor dokaj varen (39 %).

3.2 Poznavanje varne rabe informacijsko-komunikacijskih tehnologij in pojava kibernetske kriminalitete

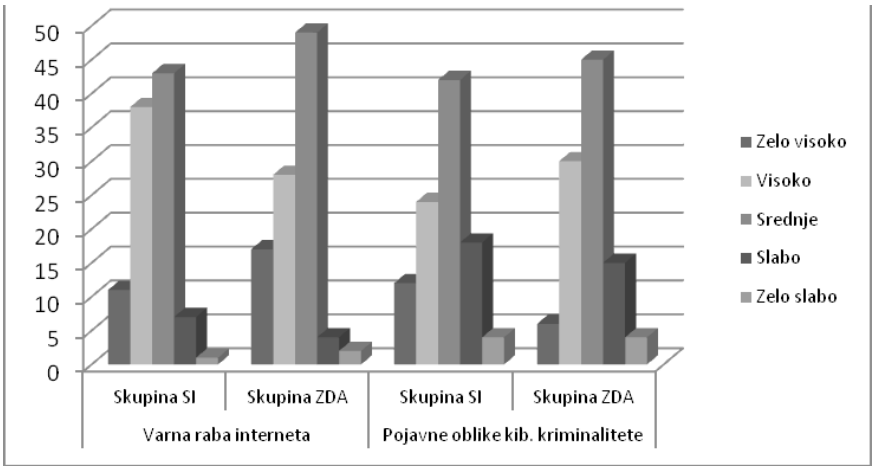
Kljub temu, da se jim kibernetski prostor na splošno ne zdi najbolj varen, anketiranci obeh skupin uporabljajo dokaj širok spekter funkcionalnosti, ki jih ponuja spletno okolje, zato nas je nadalje zanimalo, kako bi ocenili stopnjo svoje usposobljenosti na področju varne rabe informacijsko-komunikacijskih tehnologij ter stopnjo poznavanja pojava kibernetske kriminalitete v korelaciji s stopnjo uporabe funkcionalnosti, povezanih s finančnimi prenosi. Ob tem se zavedamo omejitve, povezane s problematiko definicije pojava kibernetske kriminalitete. V okviru raziskave smo se zato osredotočili na najširšo opredelitev, ki vključuje tako nove kot tudi tradicionalne oblike kriminalitete, ki so se prenesle v virtualno okolje.

Kot prikazano v grafu 2 se anketiranci v okviru obeh skupin v največji meri čutijo srednje usposobljene tako z vidika varne rabe interneta (43 % anketirancev skupine SI in 49 % anketirancev skupine ZDA) kakor tudi z vidika poznavanja pojavnih oblik kibernetske kriminalitete (42 % anketirancev skupine SI in 45 % anketirancev skupine ZDA).

Lastna ocena poznavanja/usposobljenosti je seveda lahko v veliki meri napačna, zato smo nadaljevali s konkretnimi vprašanji glede varnostnega ravnanja, in sicer smo se osredotočili na splošne oblike zagotavljanja varnosti, kot so nastavitve in menjava gesel ter varnostne nastavitve računalniškega sistema.

7 *Nekajkrat letno*

8 *Vsaj nekajkrat mesečno*



Graf 2: Ocena poznavanja/ usposobljenosti

Anketiranci obeh skupin so dokaj previdni v povezavi z uporabo gesel, in sicer jih velika večina uporablja različna gesla za različne storitve (npr. e-pošta, računalnik, socialno omrežje itd.); med anketiranci skupine SI kar 46 % sodelujočih uporablja drugačno geslo za vsako storitev, medtem je tako previdnih v skupini ZDA le 25 %, kjer največ anketirancev (57 %) sicer uporablja različna gesla, vendar pa ne drugačnega gesla za vsako storitev. Le 9 % anketirancev skupine SI uporablja isto geslo za vse storitve, medtem ko je ta odstotek v skupini anketirancev ZDA znatno višji, in sicer 19 %. Skupina anketirancev SI je torej bolj striktna glede uporabe različnih gesel, vendar pa varnostno delovanje žal odpove, ko se dotaknemo pogostosti menjave gesel, saj kar 50 % anketirancev skupine SI in 62 % anketirancev skupine ZDA gesla ne menjuje ali pa ga menja največ enkrat letno. Gesla je namreč priporočljivo redno menjati, sama pogostost menjave pa je odvisna od uporabljene storitve, za finančne storitve je tako priporočilo menjave gesla najmanj na dva meseca, ostala gesla pa na 3 do 4 mesece in ne redkeje kot na 6 mesecev (Granger, 2002).

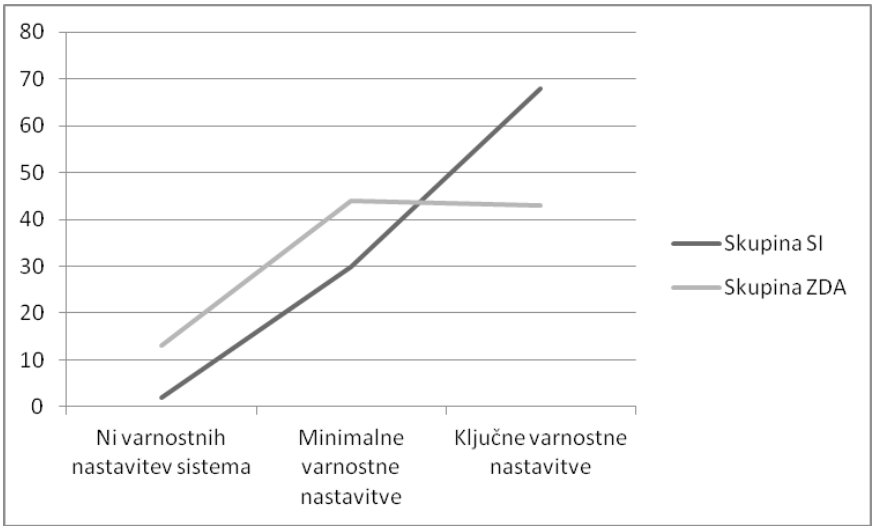
Z vidika varnostnih nastavitev računalniškega sistema smo anketirance povprašali, kakšne nastavitve imajo na lastnem sistemu oz. kako poskrbijo za varnost na svojem računalniku.

Kot prikazuje graf 3, so anketiranci skupine SI bolje poskrbeli za svoj računalniški sistem, saj velika večina (68 %) izvaja ključne aktivnosti za zagotovitev varnosti sistema (nameščen anti-virusni program, požarni zid, redno posodabljanje opreme itd.). Osnovnih varnostnih nastavitev sistema nima 2 % anketirancev skupine SI in 13 % anketirancev skupine ZDA. Pri tem je treba poudariti, da ni upoštevan tip uporabljene računalniške opreme glede na potencialne ranljivosti (npr. Apple).

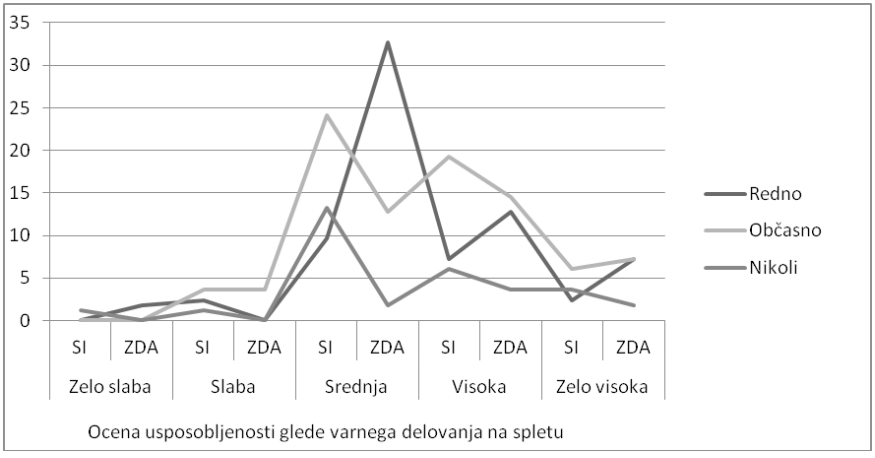
Glede na to, da je analiza pokazala dokaj visoko stopnjo zaupanja v storitve, ki jih ponujajo bančne institucije, smo se nadalje osredotočili na finančne prenose, povezane s spletnim nakupovanjem, v povezavi s čimer je opaziti porast primerov kibernetske kriminalitete v zadnjih letih. Zanimala nas je povezava med oceno stopnje usposobljenosti glede poznavanja varne rabe interneta in poznavanja

pojavnih oblik kibernetske kriminalitete na eni strani in stopnjo oz. pogostostjo izvajanja spletnih nakupov na drugi strani. Namreč, raziskava, izvedena v okviru EU, je pokazala, da »večina tistih, ki zaupajo spletnemu bančništvu in spletnemu nakupovanju, se počuti dobro obveščenih o kibernetski kriminaliteti« (Evropska komisija, 2012).

Graf 3: Varnostno ravnanje – nastavitve računalniškega sistema



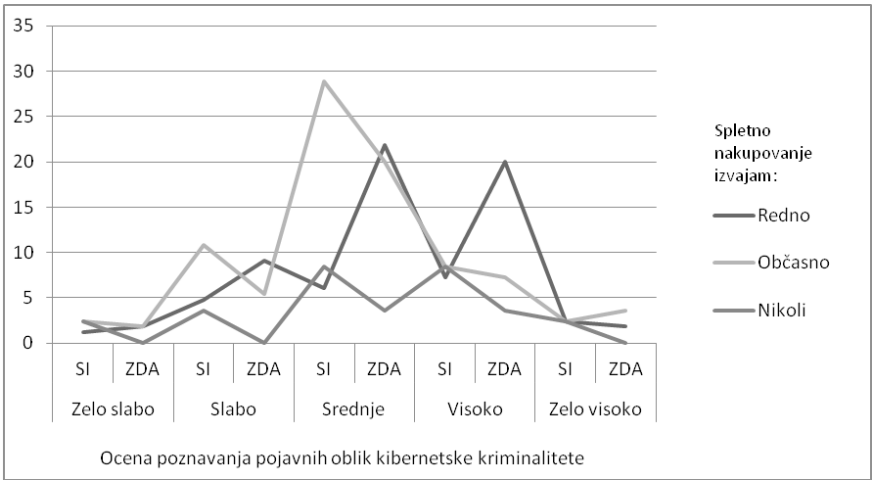
Graf 4: Uporaba funkcionalnosti spletnega nakupovanja v primerjavi z lastno oceno usposobljenosti glede varnega delovanja na spletu



Kot prikazuje graf 4, večina anketirancev skupine ZDA, ki redno uporablja funkcionalnosti spletnega nakupovanja z uporabo kreditne kartice, svojo usposobljenost glede varne rabe interneta ocenjuje kot srednje dobro, medtem ko v skupini SI najvišji odstotek tistih, ki redno uporablja takšno funkcionalnost, svojo usposobljenost ocenjuje kot visoko. Na splošno bi lahko v obeh primerih potrdili,

da se uporabniki, ki se odločijo za spletno nakupovanje, večinoma čutijo dovolj usposobljene tudi glede spletne varnosti.

V povezavi s poznavanjem pojavnih oblik kibernetske kriminalitete je analiza pokazala, da tako anketiranci skupine ZDA kot tudi anketiranci skupine SI, ki redno opravljajo spletne nakupe, svoje poznavanje pojavnih oblik kibernetske kriminalitete ocenjujejo kot srednje ali pa visoko (graf 5).



Graf 5: Uporaba funkcionalnosti spletnega nakupovanja v primerjavi z lastno oceno poznavanja pojavnih oblik kibernetske kriminalitete

Anketiranci v okviru obeh skupin ZDA in SI so torej v veliki meri prepričani v svojo usposobljenost glede varne rabe interneta in poznavanje pojavnih oblik kibernetske kriminalitete. Ob tem pa je zanimivo, da je večina anketirancev skupine ZDA, ki redno izvaja spletno nakupovanje (31 %), internet ocenila kot ne preveč varen, medtem ko je v skupini SI mnenje rednih spletnih nakupovalcev deljeno, in sicer med opcijama »ne preveč varen« (7 %) in »dokaj varen« (7 %).

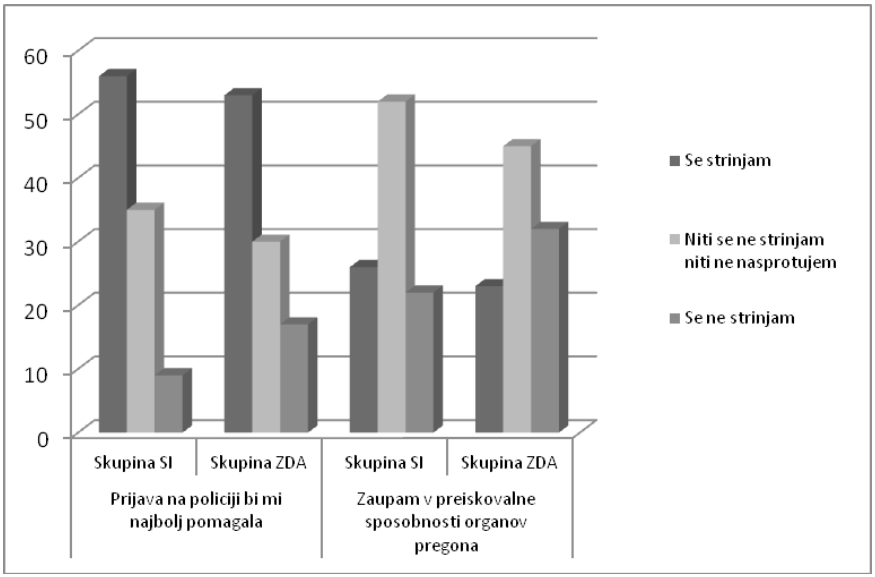
3.3 Vedenje posameznika ob srečanju s kibernetsko kriminaliteto

Uporaba funkcionalnosti informacijsko-komunikacijskih tehnologij nas spremlja na vseh področjih našega življenja in kot je pokazal prvi del raziskave, se anketiranci obeh skupin sicer zavedajo nevarnosti, pri čemer se bolj ogrožene počutijo anketiranci skupine ZDA, kar bi potencialno lahko pripisali manj varnemu fizičnemu okolju, hkrati pa do določene mere sicer delujejo varnostno, le-tega se bolj držijo anketiranci skupine SI, kar je zanimivo glede na dejstvo, da se anketiranci skupine ZDA počutijo bolj ogrožene, vendar pri svojem varnostnem ravnanju niso konsistentni. Obe skupini anketirancev pa se zavedata potencialnih posledic delovanja v virtualnem prostoru na fizični svet (v obeh skupinah več kot 80 % anketirancev meni, da dejanja v virtualnem okolju vplivajo na fizični svet).

Glede na to, da se anketiranci zavedajo potencialnih posledic virtualnega delovanja v fizičnem okolju, nas je nadalje zanimalo, kakšno bi bilo njihovo vedenje ob srečanju s kibernetsko kriminaliteto oz. s poskusom napada. Uporabili smo eno izmed najbolj razširjenih oblik poskusa kraja identitete, in sicer ribarjenje za podatki, pri čemer smo anketirancu predstavili situacijo, v kateri bi potencialno lahko postal tarča kraje identitete (prejeto elektronsko sporočilo z navodili za spremembo gesla s strani bančne institucije).

Večina anketirancev bi se uspešno obranila poskusa kraje identitete, še vedno pa se je bolj odrezala skupina SI, kjer bi se kar 92 % anketirancev pravilno odločilo in sporočila ne bi upoštevali oz. bi stopili v stik z odgovorno osebo, v skupini ZDA bi tako ravnalo 83 % anketirancev. Kraja identitete je zaradi finančnih posledic takšnega kaznivega dejanja v zadnjih letih pogosto obravnavana v medijih, zato takšen rezultat ni presenetljiv.

Nadalje nas je zanimalo, kakšen odnos oz. mnenje imajo anketiranci v povezavi z delovanjem organov pregona na področju kibernetske kriminalitete, in sicer smo se najprej osredotočili zgolj na prvi stik, torej prijavo kaznivega dejanja kibernetske kriminalitete. Večina udeležencev obeh skupin (več kot 50 % tako v skupini SI kot tudi v skupini ZDA) je mnenja, da bi ob srečanju s primerom kibernetske kriminalitete najbolj pomagala prijava na policiji, medtem ko jih tretjina ni prepričanih v učinek prijave. Večji problem predstavlja zaupanje v preiskovalne sposobnosti organov pregona, saj večina anketirancev ni vanje prepričana (približno polovica anketirancev v obeh skupinah), medtem ko slaba tretjina anketirancev v obeh skupinah ne zaupa preiskovalnim sposobnostim organov pregona (prikazano v grafu 6).



Graf 6: Odnos do organov pregona

4 RAZPRAVA

Skupaj z že omenjeno hitro rastjo števila uporabnikov sodobnih informacijsko-komunikacijskih tehnologij ne rasteta samo količina in popularnost ponujenih funkcionalnosti[9] (Kende, 2012), temveč tudi količina in raznolikost izvedenih dejanj kibernetske kriminalitete[10]. Predstavljena raziskava je pokazala primerljivo količino uporabe oz. preživetega časa v kibernetskem prostoru v obeh obravnavanih skupinah ter tudi široko uporabo ponujenih spletnih funkcionalnosti.

V povezavi z uporabo spletnih funkcionalnosti za izvajanje finančnih prenosov je na eni strani uporaba storitev, ki jih ponujajo kredibilne institucije (banke), široko razširjena v obeh skupinah, kar bi lahko pripisali veliki stopnji zaupanja v varnost storitev, ki jih takšne institucije ponujajo. Na drugi strani pa smo ugotovili, da se skupina SI še vedno bolj zanaša na fizični svet, medtem ko skupina ZDA preferira funkcionalnosti v celoti izvedene v kibernetskem prostoru, v kolikor se le-teh poslužuje. Seveda ob tem ne gre pozabiti, da storilci pogosto izrabljajo ravno zaupanje posameznika v kredibilnost in varnost poznane institucije (npr. PayPal) za izvedbo najrazličnejših zavajanj in prevar[11], zato je pomembno, da uporabniki prepoznajo potencialna tveganja in se pravilno odločajo ob srečanju z različnimi oblikami kibernetske kriminalitete.

Ena izmed najpogostejših oblik kibernetske kriminalitete je nedvomno kraja identitete, in sicer primarno kraja podatkov, povezanih z bančnimi računi (številke kreditnih kartic, dostopna gesla itd.), ki je tudi najbolj obravnavana v medijih, zato je bilo pričakovano, da se bodo ob podanem primeru poskusa napada ribarjenja za podatki udeleženci pravilno odločili, kar je raziskava tudi potrdila v okviru obeh obravnavanih skupin. Rezultat je v tem primeru skladen z ugotovitvijo, da se uporabniki, ki se odločijo za spletno nakupovanje, večinoma čutijo dovolj usposobljene tudi glede spletne varnosti in glede poznavanja pojavnih oblik kibernetske kriminalitete. Seveda pa takšne ugotovitve ne moremo posploševati na druge oblike kibernetske kriminalitete.

Glede na to, da so rezultati skupine ZDA na splošno pokazali širšo in bolj liberalno uporabo spletnih funkcionalnosti, lahko rezultat razlagamo na dva načina, in sicer, da se je skupina ZDA v virtualnem okolju preprosto udomačila, zaradi česar jih prisotnost potencialne nevarnosti ne ovira pri njihovem delovanju, ali pa lahko upoštevamo kulturne razlike in hitrost življenja, zaradi katere je uporaba informacijsko-komunikacijskih tehnologij neizogibna. Kulturne razlike po našem mnenju do določene mere vplivajo na količino uporabe funkcionalnosti informacijsko-komunikacijskih tehnologij, kar bi bilo smiselno dodatno preučiti v

9 *Julija 2010 je bila na primer naložena prva slika na takrat novo funkcionalnost – Instagram, dve leti kasneje je število naloženih slik naraslo na milijardo, ki jih je naložilo 50 milijonov uporabnikov (Kende, 2012).*

10 *Raziskava, izvedena leta 2012 v 24 državah sveta, ugotavlja, da je dnevno viktimiziranih kar 1,5 milijona posameznikov, pri čemer finančna škoda, povezana s kibernetsko kriminaliteto, znaša 110 milijarde USD na letni ravni (Symantec, 2012).*

11 *Eden izmed bolj popularnih načinov je ribarjenje za podatki (phishing), pri čemer storilci izrabijo zaupanje žrtve v kredibilen videz poslane pošte, da pridobijo želene podatke za nadaljnje zlorabe. V letu 2012 se je število takšnih napadov na svetovnem nivoju povečalo kar za 59 % v primerjavi z letom 2011 (RSA Security, 2012).*

nadaljnji raziskavi področja. Percepcijo varnosti pa lahko povežemo tudi s fizičnim okoljem življenja in delovanja v manjši oz. večji državi. Ljudje smo namreč fizična bitja in virtualno okolje na neki način še vedno predstavlja neznanko, zato se pravila fizičnega sveta v veliki meri poskušajo preslikati v virtualni svet. Prebivalci Slovenije se v svojem fizičnem okolju praviloma počutijo varnejše kot prebivalci ZDA, kar prenesejo tudi v virtualno okolje. Ob tem je zanimiva tudi visoka stopnja občutka usposobljenosti glede varne rabe interneta v okviru skupine SI, kjer se kar 49 % anketirancev čuti visoko ali zelo visoko usposobljene. Le-to bi potencialno lahko pripisali veliki količini ozaveščanja, izvedenega v zadnjem letu, ki se je osredotočalo primarno na potencialne zlorabe, povezane s finančnimi posledicami (npr. kraja identitete, prevare itd.)[12]. Ob tem pa je zanimivo dejstvo, da tako preprosta zaščita, kot je uporaba varnih gesel in njihova redna menjava, še vedno ni ukoreninjena v delovanje posameznika, saj velik del udeležencev[13] gesel ne menjuje redno (več kot enkrat letno). Raziskava je torej pokazala pomembno razliko med ozaveščenostjo posameznikov in njihovim dejanskim varnostnim ravnanjem v virtualnem okolju, ki pa se v osnovi ne razlikuje glede na fizično lokacijo posameznika.

V povezavi z delovanjem organov pregona na področju kibernetske kriminalitete je raziskava pokazala, da bi večina udeležencev sicer potencialno podala prijavo organom pregona, vendar pa večina v njihovo delovanje ni prepričana, kar je potrdilo ugotovitve drugih raziskav glede problematike zaupanja v preiskovalne sposobnosti organov pregona na področju kibernetske kriminalitete. Raziskava Urada Združenih narodov za droge in kriminal je tako pokazala, da velik del posameznikov na svetovnem nivoju ne prijavi primerov kibernetske kriminalitete, med glavne razloge med drugim spada tudi nizka stopnja zaupanja splošne javnosti v sposobnosti predstavnikov organov pregona (United Nations Office on Drugs and Crime, 2013). Ključnega pomena je torej, poleg aktivnosti, usmerjenih k ozaveščanju splošne javnosti glede problematike kibernetske kriminalitete in načinov varne rabe interneta, tudi ozaveščanje splošne javnosti glede pomena prijave kaznivih dejanj kibernetske kriminalitete in predvsem povečanje zaupanja v delovanje organov pregona tudi na področju visoko tehnoloških kaznivih dejanj.

Nivo znanja v kombinaciji z vedenjem posameznika predstavljata ključni dimenziji človeškega dejavnika v povezavi z zagotavljanjem informacijske varnosti in le z združitvijo obeh dimenzij je mogoče doseči visoko raven informacijske varnostne kulture (van Niekerk in von Solms, 2006). Podobno kot predstavljena raziskava namreč tudi druge raziskave kažejo občutno razliko med poznavanjem informacijskih groženj oz. stopnjo ozaveščenosti in dejanskim ukrepanjem; v zadnjih letih se je sicer izboljšalo razumevanje varnostnega vedenja – prva dimenzija, ni pa se spremenilo tudi varnostno vedenje posameznika – druga dimenzija (Rančigaj in Lobnikar, 2012). Slednje je potrdila tudi raziskava percepcije kibernetske kriminalitete v Sloveniji, ki je pokazala, da so, zaradi svoje virtualne narave in široke pojavnosti, določena dejanja, ki spadajo v okvir kibernetske kriminalitete, videna

12 *V letu 2011 je bil sprejet nacionalni program ozaveščanja o informacijski varnosti, ki ga izvaja Arnes s strokovno podporo SI-CERT v sodelovanju z Ministrstvom za izobraževanje, znanost in šport.*

13 *50 % skupine SI in 62 % skupine ZDA.*

kot sprejemljiva[14]. Ob tem je treba poudariti, da sta zaznavanje in interpretacija varnosti v veliki meri odvisna od splošne varnostne kulture; ko začne skupina kot celota moralno in socialno percipirati varnostne kršitve kot nesprejemljive in se posledično začne tudi varnostno obnašati, pride do prehoda od splošnega varnostnega zavedanja v varnostno kulturo (Lobnikar, Čaleta, Žaberl, Anžič in Rančigaj, 2009).

V okviru raziskave smo tako ugotovili, da so anketiranci precej samozavestni glede lastne usposobljenosti oz. poznavanja varne rabe interneta, vendar pa hkrati njihovo varnostno ravnanje ni zadostno predvsem z vidika konsistentnosti varne rabe. Pri tem naletimo na že prepoznano problematiko razlike med poznavanjem in dejanskim delovanjem v smislu »vem kako, a ne delam tako« (Rančigaj in Lobnikar, 2012), kar kaže na še vedno prenizko stopnjo informacijske varnostne kulture na področju uporabe funkcionalnosti informacijsko-komunikacijskih tehnologij v kibernetskem prostoru. Pomembno vlogo pri preprečevanju in omejevanju kibernetske kriminalitete namreč nedvomno odigra posameznik s svojim varnostnim ravnanjem v kibernetskem prostoru. Višjo stopnjo varnostnega ravnanja posameznika pa dosežemo z večjo ozaveščenostjo in poznavanjem oblik potencialnih napadov ter primernih odzivov/reakcij ob srečanju s kibernetsko kriminaliteto.

5 ZAKLJUČEK

Informacijsko-komunikacijske tehnologije predstavljajo nepogrešljiv del vsakdanjega življenja in delovanja, vendar pa se ob hitrem razvoju funkcionalnosti in razširjenosti kibernetskega prostora razumevanje in vedenje splošne javnosti nista primerno prilagodili. Kljub temu, da je nivo znanja oz. poznavanja pravil varne rabe interneta zadovoljiv, se le-to še vedno ne odrazi v varnostnem ravnanju posameznika v virtualnem okolju, kar je pokazala tudi predstavljena raziskava, saj že tako osnovno varnostno ravnanje, kot je redna menjava gesla, v veliki meri odpove. Problematičen je torej razkorak med ozaveščenostjo posameznikov in njihovim dejanskim varnostnim ravnanjem v virtualnem okolju, ki pa se v osnovi ne razlikuje glede na fizično lokacijo posameznika. Kljub temu se v povezavi z občutkom varnosti fizična lokacija dejansko preslika v virtualno okolje, saj so anketiranci živeči in delujoči v manjši državi (Slovenija) izrazili višjo stopnjo občutka varnosti v virtualnem okolju kot anketiranci živeči in delujoči v večji državi (Združene države Amerike). Dejstvo, da občutek varnosti bistveno ne vpliva na delovanje posameznika v kibernetskem prostoru, bi lahko pripisali virtualnemu vidiku kibernetskega prostora. V nadaljnjih raziskavah bi bilo zanimivo nadalje raziskati vpliv virtualnega vidika kibernetskega prostora tudi na vprašanje problematike percepcije viktimizacije, saj se, zlasti v primerih, kjer ni neposrednih finančnih posledic, velik del žrtev niti ne zaveda, da so bile

14 *Raziskava percepcije kibernetske kriminalitete je pokazala, da kar 65 % intervjuvancev razlikuje dejanje, izvedeno v virtualnem okolju, od dejanja, izvedenega v fizičnem svetu, pri čemer je večina mnenja, da je piratstvo programske opreme, filmov in glasbe družbeno sprejemljivo (Dimc in Dobovšek, 2010).*

izpostavljene kibernetski kriminaliteti (United Nations Office on Drugs and Crime, 2013). V povezavi z delovanjem organov pregona je problematičen predvsem skepticizem, povezan s percepcijo usposobljenosti predstavnikov organov pregona na področju kibernetske kriminalitete, in sicer je kar 75 % anketirancev izrazilo dvom v tehnično usposobljenost organov pregona. Slednje se potencialno lahko odraža v številu in verjetnosti prijave kaznivega dejanja kibernetske kriminalitete. Z vidika ozaveščanja splošne javnosti s ciljem dosega visokega nivoja varnostnega ravnanja bi bilo potrebno povečati količino aktivnosti, povezanih z ozaveščanjem, pri čemer bi se morali posvetiti tudi aktivnostim, ki bi zviševale stopnjo zaupanja v delovanje organov pregona. Le-ti bi morali preseči delovanje na represivni ravni in se usmeriti tudi v strateško obravnavo kaznivih dejanj kibernetske kriminalitete. Za vzpostavitev visokega nivoja varnostnega ravnanja posameznika v virtualnem okolju in posledično oblikovanje informacijske varnostne kulture na nacionalnem nivoju so ključnega pomena preventivne dejavnosti tako na nacionalnem kot tudi mednarodnem nivoju z namenom spremembe percepcije varnostnih kršitev v kibernetskem okolju in posledičnim povečanim varnostnim obnašanjem posameznika, s čimer bi presegli pozicijo »vem, vendar ne delam tako«[15].

LITERATURA

Bernik, I. in Meško, G. (2011). Internetna študija poznavanja kibernetskih groženj in strahu pred kibernetsko kriminaliteto. *Revija za kriminalistiko in kriminologijo, 62*(3), 242–252.

Britz, M. T. (2009). *Computer forensics and cyber crime*. New Jersey: Prentice Hall.

Dimc, M. (2009). Kriminaliteta v informacijski družbi. *Uporabna informatika, 17*(2), 101–105.

Dimc, M. in Dobovšek, B. (2010). Perception of cyber crime in Slovenia. *Varstvoslovje, 12*(4), 378–396.

Dlamini, M. T., Eloff, J. H. P. in Eloff, M. M. (2009). Information security: The moving target. *Computers & Security, 28*(3–4), 189–198.

Dunn, M. (2005). *A comparative analysis of cybersecurity initiatives worldwide.* Geneva: International Telecommunication Union. Pridobljeno na http://www.itu.int/osg/spu/cybersecurity/docs/Background_Paper_Comparative_Analysis_Cybersecurity_Initiatives_Worldwide.pdf

Evropska komisija. (2012). *Kibernetska kriminaliteta: državljane EU skrbi varnost osebnih podatkov in spletnih plačil.* Pridobljeno na http://europa.eu/rapid/press-release_IP-12-751_sl.htm

Flaker, V. (1994). Analiza tveganja. *Socialno delo*, *33*(3), 189–196.

Gordon, S. in Ford, R. (2006). On the definition and classification of cybercrime. *Journal in Computer Virology and Hacking Techniques, 2*(1), 13–20.

15 Posamezniki so namreč pogosto seznanjeni z osnovnimi varnostnimi tehnikami, vendar jih preprosto ne implementirajo (npr. uporaba varnih gesel, redna menjava gesel itd.).

Granger, S. (2002). *The simplest security: A guide to better password practices*. Pridobljeno na http://www.symantec.com/connect/articles/simplest-security-guide-better-password-practices

Hundley, R. O., Anderson, R. H., Bikson, T. K., Botterman, M., Cave, J., Neu, C. R. et al. (2007). *RAND: The future of the information revolution in Europe: Proceedings of an international conference*. Pridobljeno na http://www.rand.org/content/dam/rand/pubs/conf_proceedings/2007/CF172.pdf

Internet Crime Complaint Center. (2008). *2008 internet crime report*. Pridobljeno na http://www.ic3.gov/media/annualreport/2008_IC3Report.pdf

Internet Crime Complaint Center. (2012). *2012 internet crime report*. Pridobljeno na http://www.ic3.gov/media/annualreport/2012_IC3Report.pdf

Kende, M. (2012). *How the Internet continues to sustain growth and innovation*. Pridobljeno na http://www.internetsociety.org/sites/default/files/How%20the%20Internet%20continues%20to%20sustain%20growth%20and%20innovation.pdf

Komisija evropskih skupnosti. (2007). *Delovni dokument služb Komisije - Spremni dokument k sporočilo Komisije Evropskemu parlamentu, Svetu in Evropskemu odboru regij - Na poti k splošni politiki o boju proti kibernetskemu kriminalu*. Pridobljeno na http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52007SC0641:SL:NOT

Kopetz, H. (2011). *Real-time systems*. New York: Springer.

Kovačič, M., Modic, D., Rusjan, M., Selinšek, L., Šavnik, J. in Završnik, A. (2010). *Kriminaliteta in tehnologija: kako računalniki spreminjajo nadzor in zasebnost, ter kriminaliteto in kazenski pregon*. Ljubljana: Inštitut za kriminologijo pri Pravni fakulteti.

Lobnikar, B., Prislan, K., Markelj, B. in Banutai, E. (2012). Informacijskovarnostna ozaveščenost v javnem in zasebnem sektorju v Sloveniji. *Varstvoslovje, 14*(3), 345–363.

Lobnikar, B., Čaleta, D., Žaberl, M., Anžič, A. in Rančigaj, K. (2009). *Varnostna in organizacijska kultura v Slovenski vojski z vidika upravljanja s tajnimi podatki: končno poročilo raziskovalne skupine Fakultete za varnostne vede*. Ljubljana: Fakulteta za varnostne vede.

Malhotra, N. K. (2002). *Basic marketing research*. Upper Saddle River: Prentice Hall.

Markelj, B. in Bernik, I. (2011). Kombinirane grožnje informacijski varnosti pri rabi mobilnih naprav. V *Nove razmere in priložnosti v informatiki kot posledica družbenih sprememb, 18. Konferenca Dnevi slovenske informatike*. Ljubljana: Slovensko društvo Informatika.

Meško, G., Petrovec, D., Areh, I., Muratbegović, E. in Rep, M. (2006). Strah pred kriminaliteto – izzivi za raziskovanje. *Revija za kriminalistiko in kriminologijo, 49*(4), 346–353.

Miniwatts Marketing Group. (2013). *InternetWorldStats: Usage and population statistics*. Pridobljeno na http://www.internetworldstats.com/stats.htm

van Niekerk, J. in von Solms, R. (2006). *Understanding information security culture: A conceptual framework*. Johanesburg: Information Security South Africa. Pridobljeno na http://icsa.cs.up.ac.za/issa/2006/Proceedings/Full/21_Paper.pdf

Rančigaj, K. (2010). *Informacijska varnostna kultura v državni upravi* (Magistrsko delo). Ljubljana: Fakulteta za družbene vede.

Rančigaj, K. in Lobnikar, B. (2012). Vedenjski vidiki zagotavljanja informacijske varnosti. V I. Bernik in G. Meško (ur.), *Konferenca Informacijska varnost: odgovori na sodobne izzive, zbornik prispevkov.* Pridobljeno na http://www.fvv.uni-mb.si/konferencaIV/zbornik/Rancigaj_Lobnikar.pdf

RSA Security. (2012). *The year in phishing*. Pridobljeno na http://www.emc.com/collateral/fraud-report/online-rsa-fraud-report-012013.pdf

Shea, V. (2004). *Netiquette*. Pridobljeno na http://www.albion.com/netiquette/corerules.html

SI-CERT. (2012). *Nevarnost je odvisna od naše varnosti: Poročilo o omrežni varnosti za leto 2012*. Pridobljeno na https://www.cert.si/fileadmin/slike/si-cert/fokus/2013/SI-CERT_porocilo_2012.pdf

Raba interneta v Sloveniji. (2011). *Dostop do interneta ima 72 % slovenskih gospodinjstev*. Pridobljeno na http://www.ris.org/db/27/12187/Raziskave/Dostop_do_interneta_ima_72_slovenskih_gospodinjstev/?&p1=276&p2=285&p3=1318&db=160

Suler, J. (2004). The online disinhibition effect. *Cyber Psychology and Behavior, 7*(3), 321–326. Pridobljeno na http://www.samblackman.org/Articles/Suler.pdf

Svete, U. (2005). *Varnost v informacijski družbi*. Ljubljana: Fakulteta za družbene vede.

Symantec. (2012). *2012 Norton cybercrime report*. Pridobljeno na http://now-static.norton.com/now/en/pu/images/Promotions/2012/cybercrimeReport/2012_Norton_Cybercrime_Report_Master_FINAL_050912.pdf

Taylor, R. W., Caeti, T. J., Loper, K., Fritsch, E. J. in Liederbach, J. L. (2006). *Digital crime and digital terrorism*. New Jersey: Prentice Hall.

United Nations Office on Drugs and Crime. (2013). *Comprehensive study on cybercrime.* Pridobljeno na http://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf

Wall, D. S. (2007). *Cybercrime: The transformation of crime in the information age*. Cambridge: Polity Press.

O avtorjih:

Mag. Maja Dimc, predavateljica na področju kibernetske kriminalitete in informacijske varnosti, zaposlena na Ministrstvu za obrambo Republike Slovenije. E-mail: maja.dimc@gmail.com

Dr. Bojan Dobovšek, izredni profesor in prodekan na Fakulteti za varnostne vede Univerze v Mariboru. E-mail: bojan.dobovsek@fvv.uni-mb.si

VARSTVOSLOVJE,
let. 15
št. 3
str. 357–369

Socialno-psihološke implikacije kibernetskega terorizma

Kaja Prislan, Igor Bernik

Namen prispevka:

S prispevkom želimo predstaviti sinergijo učinkov nerealnih predstav o tehnologiji in terorizmu, realne sposobnosti in aktivnosti kibernetskih teroristov, hkrati pa opozoriti na grožnjo, ki je z vidika informacijske varnosti, predvsem na nacionalni ravni, ne smemo zanemariti.

Metode:

V prispevku je uporabljena deskriptivna metoda in metoda komparacije, s katerima smo analizirali predpostavke strokovnih in znanstvenih prispevkov na obravnavano tematiko. Z metodo sinteze spoznanj smo nadgradili trenutne teoretične pristope pri pojasnjevanju narave storilcev kibernetske kriminalitete in kibernetskega terorizma.

Ugotovitve:

Zaradi razvoja globalnega kibernetskega prostora je kriminaliteta pridobila povsem nove razsežnosti in priložnosti. Tako kot uporabniki sodobne tehnologije in klasični zlonamerni storilci v tem prostoru delujejo tudi kibernetski teroristi, katerih namen je s pomočjo tehnologije povzročiti čim večji strah in medijsko odzivnost. Psihološki učinki uporabe tehnologije prispevajo k temu, da kibernetski terorizem spremlja visoka stopnja nerazumevanja, posledično pa tudi strahu. Ker tovrstna kibernetska kriminaliteta nima urejene politične in pravne podlage, to skupaj z nerazumevanjem sodobne tehnologije, strahu pred njeno uporabo in možnimi zlorabami povzroča velik učinek zastraševanja. Čeprav kibernetski terorizem predstavlja resno grožnjo nacionalnim in organizacijskim informacijskim infrastrukturam, je njegovo udejanjanje v fizičnem okolju zgolj posredno. Teroristi sodobno tehnologijo za enkrat izkoriščajo predvsem kot orodje za pomoč pri načrtovanju napadov in ohranjanju lastnega obstoja.

Izvirnost/pomembnost prispevka:

Pomembnost prispevka se kaže v njegovi aktualnosti. Tako kot klasična kibernetska kriminaliteta tudi kibernetski terorizem postaja vse pogostejša tematika medijev in polemičnih razprav. S senzacionalnim poročanjem se velikokrat povzročajo dramatične in nerealne asociacije na kibernetski terorizem, v smislu možnih scenarijev in posledic. V prispevku predstavljamo njegove realne zmožnosti in temeljne značilnosti, izvirnost pa se kaže v njegovi pojasnjevalni in razlagalni vlogi.

UDK: 343.3/.7:004

Ključne besede: kibernetski terorizem, storilci, zastraševanje, psihološki vidiki

Socio-psychological Implications of Cyberterrorism

Purpose:

This paper intends to present the synergy between unrealistic notions about technology and terrorism and the cyberterrorists' real capabilities and activities. At the same time, the paper also points to the threat, which must not be neglected from the information security point of view, particularly at the national level.

Design/Methods/Approach:

The paper presents the use of descriptive and comparative methods, which were applied to analyse several assumptions found in professional and scientific publications in the relevant field. The synthesis method was then applied to consider the findings and upgrade current theoretical approaches in order to explain the nature of cybercrime and cyberterrorism perpetrators.

Findings:

Due to the development of global cyberspace, crime gained entirely new dimensions and opportunities. Apart from modern technology users and typical malevolent perpetrators, cyberterrorists, whose intention is to instigate as much fear and media attention as possible by using technology, are also operating in cyberspace. Psychological effects stemming from the use of technology contribute to the fact that cyberterrorism is characterised by a high level of misunderstanding and consequently fear. When considered in combination with the lack of understanding of modern technology, as well as the fear of its use and potential abuse, the fact that this type of cybercrime does not have a structured political and legal basis generates major intimidation effects. Although cyberterrorism represents a serious threat to information infrastructures owned by states and organisations, its actualisation in the physical environment is merely indirect. At the moment, terrorists mostly use modern technology as instrumentalities for planning attacks and preserving their own existence.

Originality/Value:

The importance of this paper is demonstrated by its up-to-date nature. Apart from traditional cybercrime, cyberterrorism is also becoming a subject of ever more frequent media attention and controversial debates. Sensationalist reporting often generates dramatic and unrealistic notions regarding cyberterrorism, as well as its potential scenarios and implications. This paper, however, presents the true capabilities and basic characteristics of cyberterrorism, while its originality is demonstrated by its explanatory and interpretative nature.

UDC: 343.3/.7:004

Keywords: cyberterrorism, perpetrators, intimidation, socio-psychological aspect

1 UVOD

Stalen tehnološki napredek in njegova splošna dostopnost oz. razširjenost sta v medsebojni kombinaciji privedla do različnih posledic, ki vplivajo na stanje in razvoj kriminalitete. Največja problematika, ki se je pojavila z vsakodnevno uporabo sodobne informacijsko-komunikacijske tehnologije (v nadaljevanju IKT) je zakonsko neurejen in geografsko neomejen kibernetski prostor, ki je glavni vzrok, da so poleg poslovne in socialne sfere kibernetski prostor odkrile tudi kriminalne skupine. Prvi poizkusi kibernetske kriminalitete[1] so bili primeri testiranja in preizkušanja lastnih sposobnosti posameznikov, z razvojem in napredkom tehnologije pa so se nevarno razvili tudi storilci v kibernetskem prostoru. Le-ti so danes največkrat organizirani v različne skupine, ki se povezujejo med seboj. Njihove aktivnosti so naravnane k skupnemu cilju skupine oz. združbe, najpogosteje pa gre za protipravno pridobivanje koristi ali javno odmevnost dejanj (United Nations Office on Drugs and Crime, 2010). V določenih skupinah je potreba po prevladi in načinu delovanja prerasla iz poslovne v politično motivacijo, da bi izzvala čim večjo medijsko pozornost in povzročila čim širšo družbeno škodo nasprotniku. V tem primeru govorimo o kibernetskem terorizmu. Politično in ideološko motivirana kibernetska kriminaliteta je pravzaprav ena izmed najbolj perečih področij sodobne družbe. Širša družbena motivacija, ki se uresničuje s pomočjo IKT, presega posamične interese, krši družbene norme, je v veliko primerih legalna, neopazna in v nekaterih kulturnih okoljih celo legitimna. Splošna dostopnost sodobne tehnologije je terorističnim organizacijam močno poenostavila načrtovanje lastnih aktivnosti in zagotavljanje življenjskega cikla. Anonimnost in komunikacijske prednosti tehnologije so privedle do razvoja novih in širitve obstoječih terorističnih celic. Kombinacija tradicionalnih terorističnih skupin s sodobno tehnologijo, organizirano kriminaliteto in hekersko subkulturo je privedla do drastičnega preoblikovanja delovanja in razvoja terorizma. Do selitve terorizma pa ni prišlo zaradi načrtovanja »elektronske vojne«, kot opozarjajo mediji, temveč zaradi neosebnosti uporabnikov in možnosti oddaljenega dostopa do informacijskih sistemov. Anonimnost, znotraj in zunaj teroristične organizacije, je članom poenostavila medsebojno komuniciranje, izogibanje organom pregona in rekrutiranje novih članov. Zaradi t. i. učinka deindividuacije[2] je širjenje in obstoj terorističnih organizacij veliko lažje, saj z zakrivanjem identitete pri uporabi tehnologije prihaja do porasta antisocialnega vedenja tudi v terorističnih vrstah. Ker kibernetski terorizem izziva veliko nejasnosti in nerazumevanja v smislu opredelitve, politične ureditve in zakonske podlage, ga tako v strokovni javnosti kot v širši družbi spremlja velika mera pod- in precenjevanja. Strah pred tehnologijo in terorizmom skupaj z dramatičnim poročanjem medijev povzroča v družbi veliko mero zastraševanja, kar pravzaprav uresničuje primarne cilje teroristov. Zanikanje in zavračanje njegovega obstoja, z neustrezno regulacijo in nadzorom, pa prav tako pripomore k obstanku terorističnih aktivnosti v kibernetskem prostoru.

1 *Kibernetska kriminaliteta pomeni uporabo informacijsko-komunikacijskih tehnologij za izvedbo kaznivih, škodljivih in nemoralnih dejanj v kibernetskem prostoru (Bernik in Meško, 2011).*

2 *Ali tudi »deindividualizacija«.*

1.1 Vzroki uporabe tehnologije v teroristične namene

Sodobno IKT so poleg klasičnih storilcev spretno izkoristile tudi teroristične organizacije, ki pri uporabi in zlorabi omenjene tehnologije ne zaostajajo za ostalimi storilci kibernetske kriminalitete. S selitvijo terorizma v kibernetski prostor in njegovo močno prisotnostjo na svetovnem spletu se je spremenila percepcija, razsežnost in agresivnost klasičnega terorizma, kot smo ga poznali. Glavna težava, s katero se srečuje mednarodna in strokovna javnost, je zaostanek varnostnih ukrepov in protiterorističnih aktivnosti za eksponentnim razvojem in preoblikovanjem terorističnih dejavnosti in njihovih pojavnih oblik. Odsotnost univerzalne oz. mednarodne definicije klasičnega terorizma in neustrezna normativna podlaga na tem področju takšen zaostanek še poglabljata. Trenutno imamo na voljo 18 univerzalnih mednarodnih pravnih aktov, ki se nanašajo na teroristične aktivnosti, nobeden izmed teh pa ne opredeljuje kibernetskega terorizma. Posledično pa pojav, ki ni pravno definiran, ni mogoče ustrezno kazensko in mednarodno preganjati ter obsoditi (Shiryaev, 2013). Kljub neenotni opredelitvi splošnega pojma »terorizem«[3] za njegovo pojavno obliko v kibernetskem prostoru, ob pregledu različnih definicij, predlagamo naslednjo definicijo: *»Kibernetski terorizem je naklepen, politično motiviran napad z uporabo IKT v kibernetskem prostoru za napad na druge informacijsko-komunikacijske sisteme (računalniški, informacijski sistemi, računalniški programi ali podatki) za nasilje nad cilji, ki se ne zoperstavljajo napadu. Pri tem se povzročajo panika, strah, javni odzivi velikih razsežnosti in potencialne smrtne žrtve.«*

Iz tega lahko razberemo, da teroristi pri zlorabi IKT uporabljajo enake tehnike in orodja kot storilci klasične kibernetske kriminalitete. Glavna težava, s katero se srečujejo pristojni organi, je torej prav razlikovanje med posameznimi oblikami kibernetske kriminalitete, ki je mogoče le na podlagi poznavanja identitete storilca in njegovega motiva. Ugotavljanje motiviranosti pa je izjemno problematično, saj so anonimnost, splošna razširjenost in dostop v kibernetski prostor z oddaljene lokacije glavni dejavniki sodobne tehnologije, ki storilcem omogočajo spretno zakrivanje identitete in izvora napada, prav tako pa so to glavni razlogi, zaradi katerih teroristi prisostvujejo v kibernetskem prostoru. Večina sodobnih terorističnih organizacij je sestavljena iz posameznih celic, ki so med seboj slabo povezane in so razpršene po večjem geografskem območju (US Army, 2007). Takšna struktura jim zagotavlja večjo varnost, vendar pa se zaradi tega pojavlja potreba po komuniciranju prek informacijskih medijev. Te razpršene skupine morajo biti medsebojno povezane, da lahko načrtujejo in izvedejo napade, pridobijo finančna sredstva in ponarejene dokumente. Obstoj in uspeh teh skupin je tako odvisen od dobre komunikacije, ki poteka mimo organov pregona, ki jih želijo odkriti (Rogers, 2003). In kibernetski prostor, predvsem internet, je orodje, s katerim lahko dosežejo te cilje. Je najverjetneje prvi množični medij, ki je omogočil zbiranje in povezovanje odtujenih oz. oddaljenih ljudi za izmenjavo mnenja in širjenje predsodkov. Zmožnost zaobiti

3 *Na splošno pa povsod velja, da terorizem pomeni sistematično in organizirano nasilno dejavnost skupin ljudi, ki so nedržavno ali državno organizirane s ciljem uničenja ali poškodovanja oseb in/ali premoženja, in to s političnimi, verskimi ali gospodarskimi nameni. Teroristična dejavnost je javna dejavnost, saj je usmerjena predvsem na vplivanje in oblikovanje javnega mnenja in na ustrahovanje širše družbene skupnosti (Newman et al., 2010).*

nacionalno zakonodajo je skupaj z elektronsko pošto in svetovnim omrežjem postala največji in najboljši medij za teroriste, ekstremistične skupine in aktiviste. Ta metoda komunikacije omogoča uporabniku zakrivanje prave identitete in skrivanje za izmišljeno oz. lažno (Crilley, 2004: 69), kar povečuje možnosti širjenja terorističnih skupin z rekrutiranjem novih članov. Takrat, ko se posamezniki, ki komunicirajo med sabo, ne poznajo (so anonimni), pride do t. i. deindividuacije, posledica česar pa je porast antisocialnega vedenja. Pri deindividuaciji popustijo posameznikove notranje zavore, zmanjša se sposobnost nadziranja lastnega ravnanja, kar je posledica zaznane anonimnosti. Različne študije ugotavljajo, da je zaradi anonimnosti večja verjetnost, da se bodo ljudje vedli agresivno (Peršak, 2009). Najnovejša različica teorije deindividuacije[4] trdi, da se bodo posamezniki obnašali deviantno, če socialna ali skupinska identiteta sprejemata oz. spodbujata takšno obnašanje in obratno (Williams, 2008: 145–146). Uporabniki kibernetskega prostora se namreč zavedajo »relativne oddaljenosti od drugih in relativne imunosti pred identifikacijo in sankcijami«. Prav tako je posameznik v kibernetskem prostoru popolnoma »gluh« oz. se ne zaveda pomena svojega dejanja in njegovih posledic v resničnem svetu (Hinduja, 2008: 392). Iz tega sledi, da anonimnost in deindividuacija sama po sebi sicer nista vzroka za deviantno obnašanje, lahko pa spodbudita k takšnim dejanjem posameznike, ki so iz takšnih ali drugačnih razlogov že nagnjeni k temu, vendar se v realnem svetu zaradi moralnih ali drugih zadržkov deviantnih aktivnosti ne bi poslu̇ževali. Vsekakor je kibernetski prostor močno pripomogel k zakrivanju identitete pripadnikov terorističnih organizacij, kar je njihov glavni način obstoja, in s tem povečal pripravljenost ljudi k priključitvi takšnim skupinam, saj je možnost odkritja v kibernetskem prostoru veliko manjša kot v fizičnem. Poleg zunanje anonimnosti pa svetovni splet zagotavlja anonimnost tudi znotraj same teroristične organizacije. Za slednje je značilno, da je notranja struktura razdeljena na posamezne dele, tako med posameznimi celicami kot tudi znotraj njih, v smislu hierarhije njenih članov. Novi člani in posamezniki, izvršitelji napadov, so pogosto izolirani od voditeljev in ključnih posameznikov v organizaciji. Takšna struktura terorističnih organizacij otežuje organom pregona pridobivanje ključnih informacij od ujetih članov te organizacije. Prav tako jim to onemogoča infiltracijo v jedro teroristične skupine (Rogers, 2003). Napad v kibernetskem prostoru oz. napad na določen informacijski sistem pa za napadalce predstavlja zelo nizko tveganje, saj obstaja majhna verjetnost, da bodo odkriti, prav tako pa lahko vstopijo ali zapustijo točko dostopa, kadar koli želijo. Če ob tem omenimo še nizko zavzetost oblasti za preganjanje tovrstne kriminalitete, lahko ugotovimo, da je tudi strah pred morebitnimi sankcijami skoraj ničen.

Poleg anonimnosti internet terorističnim skupinam daje možnost psiholoških učinkov na javnost z navideznim ojačevanjem[5] lastnih moči. Teroristična skupina, prisotna v kibernetskem prostoru, lahko z ustreznim znanjem pripravi lastno spletno stran, povezano z drugimi zelo obiskanimi spletnimi stranmi, kar daje uporabnikom občutek, da je skupina velika in močna, ne glede na njeno dejansko pojavno obliko. Pogosta razširjenost oz. prisotnost na spletu ustvarja vtis, da je organizacija takšna tudi v realnosti. In ker se uporabniki in družba odzivajo na

4 *Social identity theory of deindividuation – SIDE.*

5 *Ojačevanje je vojaški termin za povečevanje števila enot in moči.*

takšen pojav teroristične skupine na omrežju, se ji dejansko povečuje moč. V takšnem primeru se lahko obstoječa oblast in z njo represivni organi odzivajo na teroristične skupine, kot da so velike in mogočne. Oblast lahko zaradi tega postane izrazito avtokratična in poskuša omejiti uporabo ter razširjenost interneta s poseganjem v posameznikovo zasebnost. V takšnem primeru pa teroristi pravzaprav že dosežejo svoj cilj (Embar-Seddon, 2004: 17).

Eden izmed razlogov zlorabe tehnologije in uporabe interneta v teroristične namene pa je tudi razsežnost z napadom povzročenih posledic. Pri fizičnem napadu so posledice omejene na točno določeno lokacijo, medtem ko preostala skupnost dejanje le opazuje. Prav tako pa nasilje ni vedno najboljši način za doseganje političnih ciljev, saj je medijska pozornost usmerjena v samo dejanje in ne toliko v sporočilo teroristov, ki so ga želeli z dejanjem predati. Z uporabo interneta lahko teroristi s sporočilom dosežejo širšo skupnost, posledice pa niso tako dolgoročne in katastrofalne, da bi zameglile bistvo napada (Furnell in Warren, 2004). Prednost kibernetskega terorizma je tudi v tem, da je dejanje lahko sproženo na daljavo, prav tako pa ni potrebno ravnati z eksplozivom ali uresničiti samomorilsko misijo (Denning, 2000). Tehnike kibernetskega terorizma se močno razlikujejo od klasičnih terorističnih aktivnosti, saj so bolj sofisticirane in prikrite ter delujejo v popolnoma drugačnem okolju kot v preteklosti.

Temeljne oblike kibernetskega terorizma so (Ballard, Hornik in McKenzie, 2004: 59):

- Napad na informacijski sistem.[6] Glavni cilj je sprememba ali uničenje vsebine elektronskih datotek, računalniških sistemov ali podatkov, ki ga ta vsebuje.
- Uničenje ali poškodovanje kritične informacijske infrastrukture.[7] Sem so vključeni napadi na strojno in programsko opremo, stranska posledica pri tem je uničenje podatkov, glavni namen pa je poškodovanje informacijskega sistema oz. sistema, ki nadzira podatke v računalniškem okolju.
- Uporaba interneta in informacijskih sistemov za izvedbo klasičnega terorističnega napada.[8]
- Uporaba interneta za zbiranje finančnih sredstev za izvedbo nasilnih politično motiviranih akcij, za podporo drugih nasilnih dejanj ali za oglaševanje nasilne skupinske ideologije.[9]

Kadar je govora o kibernetskem terorizmu v pravem pomenu besede, gre za izvajanje zlonamernih vdorov in kibernetskih napadov na informacijske sisteme z namenom uničenja, spremembe, okvare ali zlorabe podatkov. Informacijski sistemi so lahko za teroristične skupine zanimivi zato, ker so najšibkejša točka razvitih družb. Računalniki nadzirajo dobavo električne energije, komunikacijo, letalski promet in finančne storitve. Uporabljajo jih za shranjevanje vitalnih

6 *Za napad se lahko uporabijo različne tehnike kibernetske kriminalitete: od širjenja zlonamerne programske opreme, kraja podatkov, onemogočanje delovanja sistemov in DOS napadov.*

7 *Kibernetski napadi v obliki vdorov, zasičenja strežnikov ali okvare sistemov.*

8 *V ta namen se med teroristi uporablja steganografija kot način za prenos skritih sporočil med pripadniki teroristične skupine. Največkrat se ta uporablja za prenos načrtov, širjenje priročnikov za načrtovanje napadov ali drugih ključnih informacij za izvedbo napada (Ballard et al., 2004: 59).*

9 *Za zbiranje finančnih sredstev se uporabljajo načini elektronskih prevar v obliki pharminga, phishinga, zlorabe kreditnih kartic, kraje identitete ipd.*

informacij, od zdravniških kartotek, poslovnih načrtov do kazenskih evidenc. Čeprav jim zaupamo, so ranljivi, predvsem zaradi slabe zasnove in pomanjkljive kakovosti nadzora nad nesrečami in napadi. Vendar pa se je pri tem treba zavedati tudi resnične moči in vpliva računalnikov na fizični prostor in okolje. Računalniki delujejo zaradi ljudi ali naprav, ki so priključene nanje. Da lahko računalnike povežemo s terorizmom, moramo zato razumeti njihove meje. Računalniki ne morejo neposredno ubiti ali poškodovati ljudi, lahko pa se povežejo z napravami ali sistemi, ki lahko vplivajo na fizično okolje. Zatorej obstaja posredno tveganje fizičnih okvar in neposredno tveganje ekonomskih poškodb. Kadar računalnike uporabimo kot orožje, se moramo zavedati, da so njihova dejanja posredna (Pollitt, 1997). Coleman (2003) navaja, da se neposredni stroški največkrat kažejo v izgubi prodaje med prekinitvijo, spletnih zamudah, prekinjenem dostopu za poslovne uporabnike, povečanih stroških zavarovanja, izgubi intelektualne lastnine, cenitev, stroških forenzike, sporih in izgubi kritičnih komunikacij v izrednem stanju. Med posredne posledice napada pa uvršča izgubo samozavesti in kredibilnosti finančnih sistemov, skrhane odnose in slabo globalno javno podobo, napete poslovne odnose, izgubo dohodkov strank v prihodnosti in izgubo zaupanja v vlado ter industrijo. Posledice se torej najpogosteje kažejo v ekonomski škodi. Ta pa lahko sproži veliko drugih posledic, ki so naštete kot posredne. Kibernetski terorizem lahko povzroči neposredno, vidno škodo, vendar pa je največkrat najhujša posredna škoda.

Za izvedbo sofisticiranih vdorov in napadov na informacijske sisteme teroristi potrebujejo relativno veliko znanja in spretnosti, zato se večina terorističnih skupin v kibernetskem prostoru ukvarja z naslednjimi aktivnostmi (prirejeno po Cohen, 2004: 150–151; Embar-Seddon, 2004: 16; Rogers, 2003): načrtovanje (zbiranje obveščevalnih podatkov, izvajanje analiz, koordiniranje članov in opreme); financiranje (zbiranje in prenos denarja, največji del finančnih sredstev pridobivajo v trgovini z drogo, belim blagom in orožjem, na spletu pa se sredstva velikokrat zbirajo in prenašajo prek dobrodelnih organizacij, donacij in skozi kraje ter zlorabe kreditnih kartic); koordiniranje (izdaja ukazov za izvrševanje akcij, časovno usklajevanje, določanje sestankov, dogovori o prevzemih naročenih pošiljk); politične akcije (povečevanje prepoznavnosti in medijske pozornosti z ustvarjanjem spletnih strani in prodajo terorističnih pripomočkov); rekrutiranje (pričakovana doba teroristične organizacije brez pridobivanja novih članov je manj kot eno leto, zato teroristične organizacije uporabljajo IKT in internet, da so bolj privlačne za mlajše morebitne kandidate ali t. i. mehke podpornike, ki javno in očitno izkazujejo podporo tem organizacijam); propaganda (preko spletnih strani teroristične skupine širijo svoje ideale in napačne oz. selekcionirane informacije s tem opravičujejo svoje akcije in ljudem prikazujejo svoje videnje sveta), ojačevanje (povečevanje moči enote brez dejanskega povečevanja števila njenih pripadnikov, saj je z uporabo interneta možno prikazati, da so veliko močnejše kot v resnici).

V največji meri teroristi uporabljajo internet kot podporo pri načrtovanju ali izvedbi klasičnih terorističnih napadov, vendar teroristični kibernetski napadi kljub temu predstavljajo povsem realno možnost. Zatorej je prva in najpomembnejša naloga preiskovalcev v primeru napada na informacijsko infrastrukturo prepoznati motiv in namen storilca. Mnogi primeri napadov se pod pojem terorizem ne morejo uvrstiti zaradi odsotnosti političnega ali socialnega motiva. Kljub temu pa

se zaradi potrebe po senzacionalnem poročanju velikokrat tudi najmanjše klasične napade na informacijske sisteme predstavlja kot terorizem. Do konca leta 2012 je bilo mogoče skupno zaznati več kot 31.000 prispevkov z opozorili na kibernetski terorizem, medtem ko v realnosti nismo uspeli zaznati nobenega klasičnega primera, posledično pa zato ne moremo govoriti o morebitnih žrtvah (Singer, 2012). Takšna situacija terorističnim organizacijam pravzaprav ne povzroča nobene škode, saj je njihov glavni namen ravno vplivanje na javno mnenje in povzročanje strahu v družbi[10] (Newman et al., 2010). Glede na to, da negativne osebne izkušnje s kriminaliteto praviloma (ne pa nujno) vplivajo na povečanje zaznane verjetnosti viktimizacije (Meško, Šifrer in Vošnjak, 2012: 80), lahko upravičeno domnevamo, da je zaradi preteklih negativnih izkušenj, ki jih ljudje pridobijo tudi od medijev, strah ob grožnji terorističnega napada izjemno velik. Kadar pa se ob tem omenja še možnost kibernetskega napada pa so občutki tesnobe in panični odzivi toliko večji. IKT že sama po sebi pri neveščih in neusposobljenih ljudeh izziva strah. Imenujemo ga tehnofobija in je odvisen od anksioznosti posameznika in njegove ozaveščenosti/usposobljenosti varno ravnati s tehnologijo (Gilbert, Lee-Kelley in Barton, 2003). Nepoznavanje tehnologije, njenega delovanja, morebitnih zlorab in posledic lahko hitro privede do prevelikega strahu in odpora ali pa ravno nasprotno, do malomarnosti in večje izpostavljenosti.

2 STRAH PRED KIBERNETSKIM TERORIZMOM

Ena izmed trenutno pogosteje raziskovanih tem v kriminologiji je strah pred kriminaliteto (Meško, Petrovec, Areh, Muratbegovič in Rep, 2006). Raziskovalci ugotavljajo, da strah pred kriminaliteto navadno presega dejansko stopnjo kriminalitete v družbi (Meško in Šifrer, 2008). Ko pomislimo na kibernetski terorizem, si predstavljamo najhujše, velikokrat pa si zamišljamo nemogoče scenarije, kar je posledica napačnega razumevanja pojava in strahu pred njim (Embar-Seddon, 2004: 18), vse skupaj pa se poglobi še zaradi slabih, redkih, vendar odmevnih izkušenj v preteklosti. Zelo hitro ugotovimo, da posamezni medijsko izpostavljeni primeri povzročijo višjo stopnjo strahu, kot sta dejanski ogroženost in možnost viktimizacije. Young (2007) ugotavlja, da so množični mediji spektakularna mesta izključevanja: v javnost prenesejo zaporedje, pravičnost in vključenost (ozadje novice), pri tem pa nalašč poudarjajo napake, nepravičnosti in izključenost ter te elemente postavijo v ospredje.

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 kaznivih dejanjih. Ukrepe, predvsem represivne, utemeljujejo z izražanjem strokovnih mnenj o kriminaliteti (Meško, 2000), ki v primerih kibernetskih napadov ali terorizma niso vedno objektivni in utemeljeni. V medijih je pogosto možno zaslediti opozarjanja na primere kibernetskega terorizma, bližajoče se elektronske vojne ipd. (npr. Spillius, 2012; Strand, 2012), ki

10 Teroristi zato, da bi izzvali strah in druge psihične odzive, izkoriščajo odmevnost svojega dejanja in sredstva množičnega obveščanja s prevzemanjem odgovornosti za teroristična dejanja, da bi tako izzvali širšo in večjo želeno reakcijo (Ledinek, 2005).

to sploh niso. Mnogi avtorji so pravzaprav mnenja, da še vedno nismo bili priča dejanskemu primeru kibernetskega terorizma (Cavelty, 2007; Conway, 2011; Stohl, 2007; Weimann, 2004). Zavedati se je treba, da kibernetski terorizem ni samo napad na vojaške ali vladne institucije, temveč ti napadi predstavljajo dejanje, izvedeno s pomočjo računalnikov, omrežja in storilcev kibernetske kriminalitete. Da lahko napad klasificiramo kot kibernetski terorizem, mora biti zasnovan tako, da povzroči strah ter vpliva na družbo in njeno izvršno oblast. Do danes je bila večina takšnih zaznanih napadov produkt storilcev brez političnega motiva[11] (Rogers, 2003). Takšne zmote zaradi slabega poznavanja področja in pogosto nestrokovnega poročanja medijev o kibernetski kriminaliteti še dodatno zastrašujejo uporabnike.

Poleg medijev, ki največkrat napačno uporabljajo pojem kibernetski terorizem, pa k nerazumevanju tega pojava prispevata še strah pred neznanim in pomanjkanje informacij oz. napačne informacije. Pojem kibernetski terorizem torej združuje dve sodobni obliki strahu (Ballard et al., 2004):

- strah pred napredujočo tehnologijo in
- strah pred terorizmom.

Tako tehnologija kot terorizem sta v sodobni družbi relativni neznanki. Uporaba tehnologije od posameznika zahteva ustrezno znanje in sposobnosti. Tisti, ki se tehnologiji niso prilagodili, niso sposobni normalnega funkcioniranja v sodobnem času, podprtem s tehnologijo. Motivacijo teroristov pa je težko razumeti in brez tega razumevanja se njihovi napadi zdijo brezčutni in naključni, kar pomeni, da vsakdo lahko postane tarča. Zatorej ni čudno, da pojem kibernetski terorizem pri ljudeh vzbuja strah (Embar-Seddon, 2004: 12). Ta pa spremlja vsakršen pojav, vezan na terorizem v kibernetskem svetu, ne glede na kateri ravni in v kakšni pojavni obliki se pojavi. Kibernetska kriminaliteta, katere del je tudi kibernetski terorizem, postaja vse pogostejša in aktualna tema medijev in mednarodne strokovne ter politične javnosti. Zaradi odmevnosti je strah pred kibernetskimi prevarami, zlorabami ali uničenjem povsem razumljiv, vendar v veliko primerih tudi nerazumen. Kibernetski terorizem je en izmed takšnih pojavov, ki kljub relativno redki uresničitvi povzroča močne in čustvene odzive. Slednje pa je pravzaprav glavni cilj terorističnih organizacij. S prisotnostjo v kibernetskem okolju zastrašujejo internetno populacijo, dejanska ogroženost kritičnih infrastruktur in uporabnikov pa pravzaprav zaradi pomanjkanja sodelovanja in interesa strokovne javnosti na tem področju ni znana.

3 RAZPRAVA

Anonimnost z možnostjo izogibanja odgovornosti ter strah pred terorizmom, tehnologijo in kibernetsko kriminaliteto, so glavni psihološki dejavniki oz. učinki, ki omogočajo razvoj in obstoj kibernetskega terorizma. Nejasnosti, povezane z

11 *Leta 1998 je tamilska gverilska skupina dva tedna »bombardirala« ambasade na Šrilanki s po več kot 800 elektronskimi sporočili na dan. V sporočilu je pisalo: »Mi smo spletni črni tigri in to počnemo, da bi prekinili vašo komunikacijo.« Obveščevalne službe so to označile kot prvi znani napad teroristov na državni računalniški sistem (Coleman, 2003).*

ureditvijo in nadzorom kibernetskega prostora, ter nedoslednost kaznovanja storilcev pa so glavni atributi sodobne tehnologije, ki privlačijo politično in ideološko motivirane storilce v relativno novo in neznano okolje. Možnost zakritja identitete pri posameznikih s politično uporniškim potencialom zmanjšuje notranje (moralne) zavore, kar terorističnim organizacijam olajšuje ohranjanje obstoja z rekrutiranjem novih, mlajših in tehnološko podkovanih članov. Poleg lažje komunikacije in organizacije kibernetski prostor teroristom olajšuje tudi doseganje zastavljenih ciljev oz. vizije, to je zastraševanje družbe. Strah pred kibernetskim terorizmom je posledica sinergije različnih dejavnikov strahu in je zaradi tovrstne kombinacije toliko večji in širši, saj ga ljudje navadno precenjujejo. Strah pred terorizmom je zaradi negativnih preteklih izkušenj še vedno zelo živ, s pridevnikom »kibernetski« pa je zaradi nerazumevanja sodobne tehnologije še toliko močnejši. K nerazumevanju tovrstnega pojava prispevata tudi neurejena politika in zakonodaja ter neobjektivnost oz. dramatičnost medijev pri poročanju o kibernetski kriminaliteti. Slednje pa daje terorističnim organizacijam en razlog več za implementacijo sodobne tehnologije v lastne aktivnosti.

Dejanska stopnja ogroženosti informacijskih sistemov pred terorističnimi skupinami, zaradi pomanjkanja interesa in volje ureditve tega področja, ni znana. Kljub neustreznemu razumevanju tovrstne teroristične dejavnosti pa grožnja hipotetično obstaja, zatorej predstavlja tudi dejavnik tveganja, predvsem za nacionalno informacijsko infrastrukturo. Pred tem ni izvzeta niti Slovenija, saj jo vključenost v mednarodno skupnost, politiko, organizacije in mednarodne akcije postavlja na seznam potencialnih tarč. Kibernetski terorizem je vsekakor pojav, s katerim se mora enotno in harmonično ukvarjati celotna mednarodna skupnost, ki naj uredi normativno in politično podlago za vsakršno nadaljnje preiskovanje, urejanje in nadzorovanje. Za učinkovitost pri doseganju takšnega konsenza pa je nujno potrebno sodelovanje različnih strok in področij, saj gre v primeru kibernetskega terorizma za izjemno kompleksen pojav, ki združuje največje družbene strahove. V boju proti tovrstni kriminaliteti morajo združiti svoje napore strokovnjaki z različnih področij, npr. psihologije, kriminalistike, informacijske varnosti itd. Dobro poznavanje narave problema in storilcev lahko pripomore k uspešnemu boju proti novi obliki terorizma. Treba je natančno analizirati razmišljanje storilcev, njihov način delovanja, način življenja, organizacijo in motive. Raziskava in analiza kibernetskega terorizma z namenom vpogleda v njegovo naravo je osnova vsakršnega nadaljnjega postopanja in urejanja tovrstne problematike. Nedavno je bil velik korak naprej storjen z mednarodnim projektom »Cyberterrorism project«, ki je izvedbo začel leta 2011 in poteka še danes. Njegov namen je raziskati stališča strokovnjakov, sprožiti multidisciplinarne razprave o problematiki in spodbuditi mednarodno ter medorganizacijsko sodelovanje. V nedavnih razpravah in raziskavah (mednarodna konferenca in raziskava med 118 strokovnjaki iz 24 držav, pri čemer so sodelovali tudi predstavniki iz Slovenije) o trenutnem stanju in mednarodni ureditvi kibernetskega terorizma, strokovnjaki ugotavljajo, da omenjen pojav spremljajo različne etične, politične, zakonske in tehnične ovire. S socialno-psihološkega vidika je največji problem v nerazumevanju narave tovrstne kibernetske grožnje, posledično pa je težko preprečevati in odkrivati grožnjo, ki ni enotno definirana. Zaradi odsotnosti ustrezne pravne

podlage pa je še težje identificirati potencialne storilce in določiti njihove motive. Večina strokovnjakov se strinja še, da je obstoj kibernetskega terorizma odvisen od stališč medijev oz. političnih razprav v določeni državi, saj omenjena dejavnika najbolj pospešujeta njegov razvoj (Cyberterrorism project, 2013). Iz tega sledi, da je odpravljanje strahu pred terorizmom pravzaprav protiteroristični ukrep, saj je strah gonilna sila vseh terorističnih organizacij. Na tem mestu je izobraževanje ljudi o rokovanju s tehnologijo, načinih zaščite in narave posameznih kriminalnih dejanj nujno potrebno za realizacijo takšnega cilja. Poznavanje lastnih ranljivosti in odgovorno vedenje v kibernetskem prostoru sta ključ do ustrezne informacijske varnosti posameznika. Pri sodobnem delu, kjer je stalna povezanost s kibernetskim prostorom nujna, večino zlorab »omogočata« ravno neznanje ali brezbrižnost ljudi, saj z informacijskimi sredstvi pogosto ravnamo nevestno (McCullagh in Caelli, 2005: 336). Boljše znanje, izkušenost, višja stopnja ozaveščenosti ter boljša zaščita računalnikov z elementarnimi programi in orodji za zaščito pomenijo manjše tveganje. Izobraževanje in usposabljanje glede 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. Nekaj strahu je sicer koristno, saj se s tem poveča pazljivost uporabnika pri delu z računalnikom, s tem pa se zmanjša ogroženost, zato tudi ni smiselno preveč zmanjševati strahu, saj lahko pride do nasprotnega učinka (Meško in Areh, 2003: 257).

Na nacionalni in organizacijski ravni je potrebno poskrbeti za sprejem in implementacijo celovite varnostne strategije: od tehnične zaščite do natančno določene osebne odgovornosti posameznikov in podjetij. Kibernetski storilci postajajo iz dneva v dan bolj izkušeni, uporabljajo številne tehnike, o katerih še nismo poučeni, zaradi česar je tudi obramba vedno korak za napadalci. Prav celovitost in pazljivost ter obravnavanje informacijske varnosti kot nedokončanega procesa je lahko edina obramba pred informacijsko-varnostnimi incidenti. V takšnem primeru bo informacijska varnost učinkovita, stroški okrevanja in prekinitve poslovanja pa minimalni. V primeru uresničitve dobro načrtovanega terorističnega napada na informacijski sistem se le-temu v celoti ne moremo uspešno zoperstaviti, zato je vse, kar lahko storimo to, da optimiziramo stanje varnosti, spoznamo grožnjo in smo nanjo pripravljeni. Kakršenkoli strah pred incidentom pa pri zoperstavljanju pomaga bolj malo.

LITERATURA

Ballard, J. D., Hornik, J. G. in McKenzie, D. (2004). Technological facilitation of terrorism. V A. O'Day (ur.), *Cyberterrorism* (str. 39–66). Aldershot: Ashgate.

Bernik, I. in Meško, G. (2011). Internetna študija poznavanja kibernetskih groženj in strahu pred kibernetsko kriminaliteto. *Revija za kriminalistiko in kriminologijo*, *62*(3), 242–252.

Cavelty, M. D. (2007). Cyber-terror: Looming threat or phantom menace. *Journal of Information Technology and Politics*, *4*(1), 19–36.

Cohen, F. (2004). Terrorism and cyberspace. V A. O'Day (ur.), *Cyberterrorism* (str. 149–151). Aldershot: Ashgate.

Coleman, K. (2003). Cyber terrorism. *Directions Magazine*. Pridobljeno na http://www.directionsmag.com/article.php?article_id=432

Conway, M. (2011). Against cyberterrorism. *Communication of the ACM, 54*(2), 26–28.

Crilley, K. (2004). Information warfare: New battlefields terrorists, propaganda and the internet. V A. O'Day (ur.), *Cyberterrorism* (str. 67–81). Aldershot: Ashgate.

Cyberterrorism project. (2013). Wales: Swansea University. Pridobljeno na http://www.cyberterrorism-project.org/about/

Denning, D. E. (2000). *Cyberterrorism: Testimony before the special oversight panel on terrorism committee on armed services U.S. House of Representatives*. Pridobljeno na http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html

Embar-Seddon, A. (2004). Cyberterrorism. V A. O'Day (ur.), *Cyberterrorism* (str. 11–21). Aldershot: Ashgate.

Furnell, S. M. in Warren, M. J. (2004). Computer hacking and cyber terrorism: The real threats in the new millennium. V A. O'Day (ur.), *Cyberterrorism* (str. 111–117). Aldershot: Ashgate.

Gilbert, D., Lee-Kelley, L. in Barton, M. (2003). Technophobia, gender influences and consumer decision-making for technology-related products. *European Journal of Innovation Management, 6*(4), 253–263.

Hinduja, S. (2008). Deindividuation and internet software piracy. *Cyberpsychology & Behavior*, *11*(4), 391–398.

Ledinek, I. (2005). Terorizem. *Varnostnik*, (8), 25.

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* (str. 336–357). Berlin Heidelberg: Springer-Verlag.

Meško, G. (2000). Miti o kriminaliteti v ZDA. *Revija za kriminalistiko in kriminologijo*, *51*(4), 305–313.

Meško, G. in Areh, I. (2003). Strah pred kriminaliteto v urbanih okoljih. *Revija za kriminalistiko in kriminologijo*, *54*(3), 144–152.

Meško, G. in Šifrer, J. (2008). Fear of crime in urban settings – an inquiry. *Varstvoslovje*, *10*(4), 550–560.

Meško, G., Šifrer, J. in Vošnjak, L. (2012). Punitivnost, viktimizacija in strah pred kriminaliteto pri študentih varstvoslovja – rezultati spletne ankete. *Varstvoslovje, 14*(1), 75–96.

Meško, G., Petrovec, D., Areh, I., Muratbegovič, E. in Rep, M. (2006). Strah pred kriminaliteto v Sloveniji in Bosni in Hercegovini – izidi primerjalne študije. *Revija za kriminalistiko in kriminologijo*, *57*(1), 3–14.

Newman, G. R., Clarke, R. V., Dobovšek, B., Ivanuša, T., Podbregar, I., Sotlar, A. et al. (2010). *Policijska dejavnost proti terorizmu: učbenik za vodilno osebje na policijskih postajah*. Ljubljana: Fakulteta za varnostne vede.

Peršak, N. (2009). Virtualnost, (ne)moralnost in škodljivost: normativna vprašanja nekaterih oblik kibernetične kriminalitete. *Revija za kriminalistiko in kriminologijo*, *60*(3), 191–198.

Pollitt, M. M. (1997). *Cyberterrorism – fact or fancy?* Pridobljeno na http://www.cs.georgetown.edu/~denning/infosec/pollitt.html

Rogers, M. (2003). The psychology of cyber-terrorism. V S. Andrew (ur.), *Terrorists,victims and society: Psychological perspectives on terrorism and its consequences* (str. 77–91). Chichester: Wiley.

Shiryaev, Y. (2013). *Cyberterrorism in the context of contemporary international law*. Warwick: Warwick school of law.

Singer, P. W. (2012). The cyber terror boogeyman. *Armed Forces Journal.* Pridobljeno na http://www.brookings.edu/research/articles/2012/11/cyber-terror-singer

Spillius, A. (12. 10. 2012). US at risk of 'cyber-Pearl Harbor'. *The Telegraph*. Pridobljeno na http://www.telegraph.co.uk/news/worldnews/northamerica/usa/9604794/US-at-risk-of-cyber-Pearl-Harbor-Leon-Panetta-warns.html

Stohl, M. (2007). Cyber terrorism: A clear and present danger, the sum of all fears, breaking point or patriot games? *Crime, Law and Social Change, 46*(4–5), 223–238.

Strand, P. (3. 10. 2012). America's cyber defenses: A digital Pearl Harbor? *CBN.News*. http://www.cbn.com/cbnnews/us/2011/december/americas-cyber-defenses-a-digital-pearl-harbor-/

United Nations Office on Drugs and Crime. (2010). *Cybercrime.* Pridobljeno na http://www.unodc.org/documents/data-and-analysis/tocta/10.Cybercrime.pdf

US Army. (2007). *A military guide to terrorism in the twenty-first century*. Kansas: TRADOC.

Weimann, G. (2004). *Cyberterrorism: How real is the threat? Special report*. Washington: United States Institute of Peace.

Williams, K. S. (2008). Using tittle's control balance theory to understand computer crime and deviance. *International Review of Law Computers & Technology*, *22*(1–2), 145–155.

Young, J. (2007). *The vertigo of late modernity*. London: Sage.

O avtorjih:

Kaja Prislan, mag. var., doktorska študentka na Fakulteti za varnostne vede Univerze v Mariboru.

Dr. Igor Bernik, docent, predstojnik Katedre za informacijsko varnost in prodekan za izobraževalno dejavnost na Fakulteti za varnostne vede Univerze v Mariboru. E-mail: igor.bernik@fvv.uni-mb.si

VARSTVOSLOVJE,
let. 15
št. 3
str. 370–384

Nadzor in regulacija bančnega sektorja: preventivni dejavnik boja proti finančni kriminaliteti

Tanja Ahčan

Namen prispevka:

Finančna kriza je razkrila številna odklonska ravnanja udeležencev globalnih finančnih trgov ter odprla množico kompleksnih pravnih in dejanskih vprašanj glede regulacije in nadzora finančnih trgov kot tudi uspešnosti kazenskega pregona odgovornih. V prispevku avtorica obravnava pozitivnopravno ureditev delovanja centralne državne bančne nadzorne oziroma regulatorne institucije. Predstavljene so naloge, pristojnosti in ukrepi Banke Slovenije, predvsem z vidika možnosti preprečevanja in odkrivanja finančne kriminalitete.

Metode:

Prispevek je teoretične narave, na podlagi deskriptivne analize *de lege lata* področja delovanja bančnega nadzornika in regulatorja, ki vključuje več pravnih področij, od državnopravne oziroma upravne ureditve, civilnega in gospodarskega prava do uporabnosti na kazenskopravnem področju.

Ugotovitve:

Nadzor in regulacija bančnega sektorja v Republiki Sloveniji temeljita na pravilih evropske zakonodaje in dobre prakse, ki jo oblikujejo mednarodne finančne institucije. Razloge za pomanjkljivosti oziroma šibkosti, katerih rezultat so bila odklonska ravnanja akterjev na finančnih trgih, ne gre iskati v normativni ureditvi *de lege lata*. Dosledna implementacija že uveljavljenih norm predstavlja preventivo v boju proti finančni kriminaliteti.

Izvirnost/pomembnost prispevka:

Problematika delovanja našega bančnega regulatorja in nadzornika, v povezavi z razlogi za izbruh finančne krize, je bila predvsem predmet razprav ekonomistov. Zaradi potrebe po morebitnih premišljenih reformah, predvsem v smislu preventivne vloge na področju finančne kriminalitete, pa je nujno, da se delovanje in ukrepanje državnega regulatorja celovito obravnava tudi s pravnega in kriminalnopolitičnega vidika.

UDK: 343.37

Ključne besede: finančna kriza, finančna kriminaliteta, regulacija, nadzor

Banking Sector Supervision and Regulation: A Preventive Factor in the Fight Against Financial Crime

Purpose:

The financial crisis revealed numerous deviant activities of participants in global financial markets, as well as raised a number of complex legal and actual questions regarding the regulation and supervision of said markets and the efficiency of criminal prosecution of those responsible. The paper deals with how the positive law regulates the activities of the central institution at state level responsible for banking supervision and regulation. The paper presents the tasks, responsibilities and measures of the Bank of Slovenia, particularly from the point of view of the possibility to prevent and detect financial crime.

Design/Methods/Approach:

The paper has a theoretical nature and is based on a descriptive *de lege lata* analysis of the activities of the banking supervisor and regulator, including several legal areas, from state law (or administrative set-up) to civil and commercial law, as well as the application in criminal law.

Findings:

The banking sector supervision and regulation in the Republic of Slovenia are based on the European legislation and good practice established by international financial institutions. The reasons for the imperfections or weaknesses of supervision resulting in deviant activities of the financial markets actors are not to be found in the legislative framework *de lega lata*. A consistent implementation of the already established norms represents a preventive factor in the fight against financial crime.

Originality/Value:

The activities of our banking regulator and supervisor, in connection with the reasons for the onset of the financial crisis, have been discussed mainly by economists. Given the need for well thought-out reforms, mainly in the sense of a preventive role in the area of financial crime, it is mandatory that the activities and measures of the state regulator are dealt with in their entirety also from the legal and crime policy view.

UDC: 343.37

Keywords: financial crisis, financial crime, regulation, banking supervision

1 UVOD

O finančni krizi se že skoraj polovico dekade piše in govori kot o naravni katastrofi. Z ekonomskega in pravnega vidika ni nobenega dvoma, da je bila sedanja finančna kriza posledica sistemskih pomanjkljivosti ter inovativnosti in odklonskih ravnanj udeležencev finančnih trgov. Stroka opozarja na pojav moralnega hazarda, na šibkosti sistemov vodenja in upravljanja korporacij (t. i. teorije »corporate governance«), na zlorabo temeljnega načela zaupanja med udeleženci, na enormne razsežnosti pohlepa vodilnih v finančnih institucijah v povezavi s črednim

nagonom investitorjev v smislu slogana »vsi delajo enako«. Podobno ugotavlja tudi Tomasic (2012), da je finančna kriza razkrila številne pomanjkljivosti glede vodenja in upravljanja finančnih institucij, korporacijske prevare ter šibko regulacijo in nadzor. Po petih letih razglabljanj o finančni krizi je mogoče povzeti, da je kljub številnim in dalj časa prisotnim indicem zatajila preventivna vloga nadzornikov in regulatorjev.[1] Izguba finančne stabilnosti lahko ustvari velike stroške za realni sektor, zato se finančna stabilnost obravnava kot javno dobro v pristojnosti institucije za nadzor finančnega sistema (Štiblar, 2010: 38). Schinasi (v Štiblar, 2010: 38) poudarja, da se morajo ustvarjalci ekonomske politike osredotočiti na preventivo, kontrolne preglede in identifikacijo potencialnih težav, preden škodijo gospodarskemu sistemu kot celoti. Ko sta raziskovala vzroke bančnih kriz, sta Caprio in Klingebiel (v Štiblar, 2010: 38) ugotovila, da je bil v 90 % primerov prisoten neprimeren bančni nadzor.

Z represivnega vidika je globalna finančna kriza razkrila vrsto pojavnih oblik gospodarske oziroma finančne kriminalitete, od različnih zlorab trga finančnih instrumentov, ki so bile posledica finančnih inovacij, do koruptivnih ravnanj odgovornih, ki so sprožili pravna in dejanska vprašanja kazenskega pregona. Bistvena značilnost dejanj in storilcev je, da gre za kriminaliteto belega ovratnika, torej kriminalna ravnanja privilegirancev, vplivnih poslovnežev na vodilnih položajih v bančnem lobiju, z razpredenimi formalnimi in neformalnimi mrežami poznanstev. Sutherland (2001) navaja, da je kriminaliteta belih ovratnikov običajno protipravno ravnanje tehnične narave in vsaj neposredno ne krši moralnih norm. Poleg tega so učinki oziroma posledice kriminalitete belih ovratnikov razpršeni v daljšem časovnem obdobju in na množico potencialnih žrtev, zato se prvotno zdi, da nihče ni oškodovan. Za finančne institucije, ki bi jih kazenski pregon potopil skupaj s storilci, pa je nastala angleška izpeljanka, namesto »too big to fail«, »too big to prosecute«.[2]

Izhajajoč iz pozitivnopravne ureditve, v prispevku obravnavam možnosti nacionalnega bančnega regulatorja in nadzornika, ki jih ima na področju preprečevanja finančne kriminalitete kot najhujše oblike odklonskih ravnanj udeležencev finančnih trgov. Iz pregleda danih normativnih okvirov je razvidno, da je imel naš bančni regulator vse preventivne vzvode v svojih rokah in da sta (bila) premalo učinkovita nadzor in regulacija tudi v naši državi.

1 *Januarja 2011 je bila nacionalna komisija v ZDA (Financial Crisis Inquiery Comission) ustanovljena, da razišče vzroke finančne in ekonomske krize. Po enem letu proučevanj, več kot 700 zaslišanih pričah in več milijonov strani prebranih dokumentov, je objavila končno poročilo (Federal Crisis Inquiery Commission [FCIC], 2011), v katerem je potrdila, da je bila kriza rezultat človeških dejanj in opustitev ter bi jo bilo mogoče odvrniti.*

2 *Morebitni kazenski postopki bi namreč korenito omajali splošno zaupanje komitentov v njihovo poslovanje in njihov poslovni ugled, kar bi (ponovno) destabiliziralo sektor.*

2 »BANČNIŠTVO KOT HRBTENICA SAMOSTOJNE SLOVENIJE«[3]

Štiblar (2010) je zagovornik državnega lastništva največjih slovenskih bank in meni, da bančni sektor v večinsko domači lasti, z domačimi bankirji, ohranja občutek monetarne in bančne suverenosti naše države tudi v krogu ostalih članic ekonomske in monetarne unije (v nadaljevanju EMU). Danes je slovensko bančništvo temelj ekonomske suverenosti neodvisne države, v prihodnosti pa naj varuje samobitnost, identiteto države v razmerah globalne konkurence (Štiblar, 2010: 15). Vprašanje pa ostaja, kakšen vpliv so imeli »državni« bankirji pri pojavu moralnega hazarda na naših tleh, v povezavi z menedžerskimi odkupi in podeljevanjem nezavarovanih kreditov pravnim osebam.[4]

Zaradi moralnega hazarda so odpovedali vsi bistveni dejavniki nadzora: upravljanje s finančnimi oziroma bančnimi tveganji, korporativna odgovornost, meni Dowd (2009). Podrobno utemeljuje, da je moralni hazard odigral glavno vlogo v dogodkih, ki so privedli do finančne krize, zato jo moramo pravilno razumeti, da bodo reforme ustrezno oblikovane in da bodo preprečile ponovno katastrofo. Hellmann, Murdock in Stiglitz (2000) pa navajajo, da pojav hazarda omogoča šele konkurenčno ravnovesje na prostem trgu, zato obstaja med akterji ter zakonodajalcem splošen konsenz o potrebi po določeni stopnji regulacije bank, ki naj vključuje minimalne kapitalske zahteve, učinkoviti nadzor bank in centralno regulatorno institucijo.

Upravljanje in vodenje bank je pomembna informacija sama po sebi, hkrati pa lahko eden ključnih dejavnikov njihove uspešnosti (Štiblar, 2010: 211).[5] Organisation for Economic Co-operation and Development – Organizacija za gospodarsko sodelovanje in razvoj (v nadaljevanju OECD) je objavila analizo, kakšen vpliv so imele na finančno krizo pomanjkljivosti oziroma slabosti upravljavskega sistema ali »corporate governance« in v zvezi s tem objavila poročilo. Iz analize izhaja, da so slabosti poslovodstva finančnih institucij v veliki meri prispevale k nastanku

3 *Štiblar (2010) piše, da je nastajanje samostojne Slovenije spremljalo tudi nastajanje slovenskega bančništva. Oboroževanje teritorialne obrambe in slovenskih sil je bilo financirano z »neuradnimi fondi« oz. nepovratnimi krediti; NLB je bila gospodarski subjekt s sorazmerno visoko kredibilnostjo in mednarodnim ratingom, ki je lahko delovala na mednarodnih finančnih trgih takoj po osamosvojitvi; prve finančne kredite za Slovenijo in druge finančne storitve je opravila NLB, ki je imela vlogo tudi na političnem oz. diplomatskem področju; odcepljanje od jugoslovanskega trga in transformacija slovenskega gospodarstva v 90. letih prejšnjega stoletja sta bila uspešna zaradi podpore bančništva.*

4 *Štiblar (2008) zatrjuje, da ni mogoče dati ocene, kakšno vlogo so imele naše banke v času finančne in gospodarske krize, vendar so po njegovem mnenju prispevale k »tajkunizaciji« slovenskega gospodarstva. Kritika se nanaša na financiranje kreditov menedžerjem za njihove notranje odkupe podjetij (managers buy out – MBO) v zameno za zastavo delnic teh gospodarskih družb ciljnega prevzema, kar je seveda posel z visoko tveganostjo. Moralno (etično) vprašanje pa se po mnenju Štiblarja nanaša na samo bistvo menedžerske prilastitve gospodarske družbe, saj najete kredite za nakup odplačujejo drugi.*

5 *Štiblar (2010) piše, da se za angleškim terminom dejansko skriva konflikt med različnimi interesi oz. cilji poslovanja gospodarske družbe, menedžmenta na eni in lastnikov na drugi strani. Gre za upravljanje, vodenje in obvladovanje družb. Teorija še ni razvila posebnega problemskega sklopa za »corporate governance« bančnega sektorja, temveč gre za splošno problematiko te teorije za primer delniških družb, ki so temeljna pojavna oblika bank. Teorija »corporate governance« naj bi vključevala tudi pravila in postopke za omejevanje delovanja menedžmenta.*

finančne krize, saj bi prav organi upravljanja oziroma vodenja morali predvideti in obvarovati institucije pred prevelikimi tveganji. Ugotovitve pa so pripeljale do odločitve, da je treba na novo proučiti in določiti temeljna načela na kritičnih področjih (Organisation for Economic Co-operation and Development [OECD], 2009).[6]

Štiblar (2010) dodaja, da je treba v našem bančnem sektorju upoštevati specifičnosti, ki glede teorije »corporate governance« veljajo za države v tranziciji ter hkrati posebnost majhnih držav. Pri tem povzame mnenje Berglofa in von Thaddena (v Štiblar, 2010), da je v tranzicijskih državah treba upoštevati posebnosti sistema vladanja v državi, uveljaviti transparentnost, zaščititi zunanje lastnike, a ne zgolj manjšinskih delničarjev, zaščititi upnike bolj kot lastnike, se usmeriti bolj na implementacijo kot sprejemanje zakonov, ki naj se sicer dopolnjujejo z namenom ustreznega razvoja finančnih trgov. Štiblar navede še eno posebnost obravnavane teorije za primer majhnih držav, ki jo izpostavita David in Mach (v Štiblar, 2010), in sicer gre za princip »vsi poznajo vse«, kar je značilnost tesnih medosebnih zvez. V zvezi s problematiko lastništva pa piše, da Gregorič in drugi (v Štiblar, 2010) opozarjajo, da postaja vprašanje »corporate governance« v tranzicijskih državah vse bolj pomembno zaradi nižje gospodarske rasti od pričakovane, kar je tudi posledica neustrezne implikacije teorije v praksi, saj je zunanji lastnik običajno država s svojimi neekonomskimi cilji.

Baselski odbor za bančni nadzor (Basel Committee on Banking Supervision) je že v novi kapitalski sporazum Basel II (Basel Committee on Banking Supervision, 2006)[7] povzel definicijo operativnega tveganja iz bančnih krogov, ki pravi, da je to »tveganje izgube zaradi neustreznih ali neuspešnih notranjih postopkov, ljudi in sistemov ali zaradi zunanjih dogodkov«, pri čemer naj bi taka definicija zajemala tudi pravna (zakonodajna, regulativna) tveganja (Majič, 2002: 3). Dobri upravljavski informacijski sistemi, učinkovit sistem notranjih kontrol ter kvalitetno načrtovanje rezervacij za nepredvidene situacije so bistvene sestavine uspešnega obvladovanja operativnih tveganj za banke (Majič, 2002: 3). Majičeva pojasnjuje, da je razlog, da je bilo treba poleg kreditnih in tržnih tveganj vključiti tudi operativna tveganja kot »ostala, druga« tveganja poslovanja bank, iskati predvsem v globalizaciji finančnih trgov oziroma storitev, vse bolj sofisticirani tehnologiji finančnega poslovanja (tveganja sistemskih napak, tveganja prevar, tudi zunanjih,

6 *Ključne ugotovitve in povzetke dobrih praks je posebna skupina OECD objavila v začetku leta 2010. Med drugim poudarjajo pomen dosledne implementacije pravil na nacionalnih nivojih, učinkovitejše upravljanje s tveganji ter izboljšanje pravil in postopkov upravljanja (board practices), vključno s sestavo upravnega organa, njegovo neodvisnostjo in strokovnostjo (OECD, 2010).*

7 *Basel II (2004 oz. 2006) oziroma novi kapitalski sporazum je priporočilo za oblikovanje politik in določa, koliko kapitala mora banka oziroma druga finančna institucija imeti glede na nivo finančnih in operativnih tveganj, s katerimi se sooča. Opredeljene so zahteve za upravljanje s tveganji in izračunom potrebnega kapitala, kar naj bi zagotavljalo stabilnost finančnih institucij in finančnega sistema. Sporazum je bil pripravljen s strani Baselskega odbora za nadzor bank in ni zavezujoč, služi kot podlaga za oblikovanje evropskih bančnih smernic v obliki direktiv, ki jih implementira tudi RS. Predhodnik Basel I iz leta 1988 je doživel kritike, ker ni upošteval v zadostni meri nekreditnih tveganj. Basel II (Basel Committee on Banking Supervision, 2006) temelji na treh stebrih: minimalne kapitalske zahteve, regulativni nadzor, tržna disciplina. Leta 2010 je bil sprejet Basel III (Basel Committee on Banking Supervision, 2010), ki vsebuje še strožja pravila poslovanja in nadzora, predvsem glede kapitalske ustreznosti bank, ki pa še ni začel veljati.*

vprašanja varnosti sistema), potrebi po stalnem vzdrževanju visoke stopnje notranjih kontrol in varnostnih sistemov, povezovanju subjektov, ki primarno opravljajo bančne storitve, v skupine, kjer prihaja do novih ogrožanj varnosti in transparentnosti delovanja sistema. Rotovnik (2003) zagotavlja, da mora biti upravljanje z operativnim tveganjem neločljivo povezano z organizacijsko kulturo banke, saj bodo le tako poslovne odločitve ali dejanja učinkovito ovrednotili operativno tveganje, ki je povezano z njimi. V drugem prispevku pa Rotovnik (2004) poenostavi problematiko operativnega tveganja in jo strne v enem stavku: »Kako dobro je vodena banka?« Na vseh poslovnih področjih, z vidika vseh tveganj in vključujoč vse sestavine (ljudje, sistemi, procesi).

Med temeljnimi načeli Odbora, ki jih podrobneje razčlenjuje Majičeva (2003), je opredeljena tudi vloga bančnih nadzornikov, ki morajo od bank zahtevati, da imajo vse navedene učinkovite sisteme za ugotavljanje, merjenje in spremljanje operativnih tveganj. Nadzorniki morajo ugotavljati ustreznost in učinkovitost metodologij, ki jih banka uporablja za presojo in obvladovanje operativnega tveganja, saj naj bi po baselskem sporazumu Basel II (Basel Committee on Banking Supervision, 2006) banke imele ustrezen kapital za kritje vseh tveganj svojega poslovanja.

3 NACIONALNI BANČNI REGULATOR IN NADZORNIK

Ključni temelj in predpogoj uspešnosti bančništva predstavlja centralna banka kot njegov regulator in nadzornik (Štiblar, 2010: 37). Delovanje Banke Slovenije (v nadaljevanju BS) ureja Zakon o Banki Slovenije ([ZBS-1], 2006), ki določa, da je BS centralna banka Republike Slovenije pravna oseba javnega prava, ki samostojno razpolaga s svojim premoženjem. Njene glavne naloge so oblikovanje in uresničevanje denarne politike ter denarnega nadzora, odgovornost za splošno likvidnost bančnega sistema, sodelovanje pri transakcijah na deviznih in finančnih trgih, sprejemanje v depozit sredstva bank in hranilnic, odpiranje računov bankam in hranilnicam, urejanje plačilnih sistemov. BS je neodvisna nevladna institucija, nadzor nad njenim poslovanjem pa izvaja Državni zbor RS, kateremu je dolžna poročati vsaj vsakih šest mesecev tako, da predloži poročilo o svojem poslovanju.

Razlogi, da so centralne banke kot nadzorniki zainteresirane za dobro poslovanje bančnega sistema, so po Štiblarju (2010) sledeči: interes za stabilnost finančnega sistema, katere ni mogoče doseči brez stabilnosti bančnega sistema; poslovne banke lahko preko odobritve kreditov vplivajo na količino denarja v obtoku; učinkovitost finančnega sistema je v veliki meri odvisna od učinkovitosti bančnega sistema; interes centralnih bank je zaščita deponentov zaradi obstoja asimetričnih informacij in nevarnosti širjenja panike v primeru zloma posamezne banke.

Naloge BS niso omejene le na ZBS-1 (2006), temveč so določene še v drugih predpisih, npr. o preprečevanju pranja denarja, bančništvu, potrošniških kreditih[8]

8 *BS opravlja tudi nadzor nad dajalci potrošniških kreditov, ki imajo dovoljenje po zakonu o bančništvu, in nad njihovimi posredniki ter je hkrati tudi prekrškovni organ (Zakon o potrošniških kreditih, 2010).*

ipd. Položaj BS se je spremenil z vstopom v EMU s 1. 1. 2007, saj je postala del Evropskega sistema centralnih bank (v nadaljevanju ESCB). Pri uresničevanju svojih nalog v celoti upošteva določila statuta ESCB in Evropske centralne banke (v nadaljevanju ECB). ZBS-1 (2006) določa tudi organa BS, ki sta Svet Banke Slovenije, ki določa denarno politiko in sprejema ukrepe za njeno izvajanje, in guverner Banke Slovenije.

3.1 Nadzor nad bankami po ZBan-1

V priročniku BS Proces ocenjevanja tveganj (Banka Slovenije, 2007) je uvodoma izpostavljena pomembnost vloge, ki jo imajo banke v nacionalnih ekonomijah, in zaupanje, ki ga imajo do teh institucij vlagatelji, zato morajo banke poslovati skrbno in varno ter vzdrževati primerno raven kapitala za zaščito pred tveganji, ki jim banka je ali bi jim lahko bila izpostavljena. V Strateškem načrtu BS za obdobje 2009–2012 (Banka Slovenije, 2008a) je zato opredeljeno, da nadzor nad poslovanjem bank temelji na pravilih evropske zakonodaje in dobre prakse za opravljanje bančnega nadzora, ki zajema predvsem preverjanje kvalitete upravljanja s tveganji[9], ki so jim banke izpostavljene, in usklajenosti poslovanja z veljavnimi predpisi, ki določajo minimalne standarde varnega in skrbnega poslovanja bank. Vsebinsko najobsežnejši zakon, na podlagi katerega BS izvaja nadzor nad bankami, je Zakon o bančništvu ([ZBan-1], 2010). BS opravlja nadzor nad bankami s spremljanjem, zbiranjem in preverjanjem poročil in obvestil bank ter drugih oseb, z opravljanjem pregleda poslovanja bank in z izrekanjem ukrepov nadzora. Pri tem lahko izreče naslednje ukrepe nadzora: priporočilo ali opozorilo, odredi odpravo kršitve, odredi dodatne ukrepe za uresničevanje pravil o upravljanju s tveganji, odvzame dovoljenje banki za opravljanje storitev, postavi izredno upravo, začne prisilno likvidacijo in sprejme odločitev o razlogih za stečaj. Pozornost BS je usmerjena v splošna in specifična tveganja, kompleksnost institucije, lastniško obvladovanje, kapital in možnost okužb v finančnem sistemu (Banka Slovenije, 2008a: 19).

Instrumenti nadzora in regulacije bank se lahko razdelijo v tri skupine: preventivni instrumenti (politika licenciranja, politika izdajanja soglasij za spremembo lastništva, politika izdajanja soglasij za člane upravnega odbora in organe upravljanja v banki, višina začetnega kapitala, izbira revizorjev, politika dajanja soglasij za statusne spremembe), korektivni instrumenti (nadzor upravljanja s tveganji in kapitalsko ustreznostjo, sistemi zgodnjega opozarjanja, javno objavljanje informacij, korektivni ukrepi do bank), represivni instrumenti (uvedba začasne uprave, stečaj in likvidacija banke) (Štiblar, 2010: 40).

9 *Vrste tveganj, kot so opredeljene v javnem delu priročnika Proces ocenjevanja tveganj (Banka Slovenije, 2007), so kreditno tveganje (vključno s tveganjem koncentracije, kreditnim tveganjem v listinjenju, preostalim tveganjem in deželnim tveganjem ter transfernim tveganjem), tržno tveganje (vključuje valutno tveganje), obrestno tveganje, likvidnostno tveganje, operativno tveganje (skupaj z IT tveganjem in pravnim tveganjem), strateško tveganje, tveganje ugleda, kapitalsko tveganje, tveganje dobičkonosnosti.*

3.2 Preprečevanje pranja denarja in financiranja terorizma

Režek (2002) med motivi za pranje denarja, ki je iskanje in uporaba metod za prikrivanje njegovega nezakonitega izvora ter poskus njegovega vključevanja v zakonite finančne in gospodarske tokove, navede tudi finančne organizacije (in druge udeležence v procesu), saj jim predstavlja pomemben vir zaslužka, visoka stopnja tveganja pri upravljanju z omenjenimi sredstvi pa le še povečuje dobičke iz te dejavnosti.[10]

Pristojnosti in dolžnosti BS na področju preprečevanja pranja denarja določa Zakon o preprečevanju pranja denarja in financiranja terorizma ([ZPPDFT], 2007). Bistvena novost ZPPDFT (2007) v primerjavi z Zakonom o preprečevanju pranja denarja ([ZPPDen-1], 2001) je uveljavitev pristopa, ki temelji na oceni tveganosti (Risk Based Approach). BS je tudi s sprejetjem novega zakona ostala pristojna za nadzor nad izvajanjem določb ZPPDFT (2007) v bančnem sektorju, na novo pa ji je dodeljena vloga prekrškovnega organa. Iz ZPPDFT (2007) izhaja tudi nova zadolžitev nadzornih organov glede izdaje priporočil oziroma usmeritev v zvezi z izvajanjem zakona. Iz Usmeritev pri izvajanju ukrepov na področju preprečevanja pranja denarja in financiranja terorizma (Banka Slovenije, 2008b) izhaja obveznost banke, da izdela analizo tveganosti, s katero oceni tveganost posamezne skupine strank, poslovnih razmerij, produktov in storitev z vidika morebitne zlorabe za pranje denarja ali financiranje terorizma, nato pa na tej podlagi izvaja ustrezne ukrepe. ZPPDFT (2007) namesto identifikacije stranke uvaja pregled stranke, ki obsega ugotavljanje in preverjanje istovetnosti stranke, ugotavljanje dejanskega lastnika stranke, pridobivanje zakonsko zahtevanih podatkov in redno skrbno spremljanje poslovnih aktivnosti stranke, pri čemer morata obseg in pogostost izvedenih aktivnosti ustrezati profilu tveganosti stranke.

3.3 Finančni konglomerati

Finančni konglomerat je skupina gospodarskih subjektov, ki so medsebojno kapitalsko povezani in obvladujejo celoto finančnih storitev, predvsem na področju bančništva, zavarovalništva ter trga vrednostnih papirjev.[11] Zaradi kompleksnosti pojava so združevanja subjektov na področju finančnih storitev prinesla tudi negativne vidike, s katerimi se ukvarjajo pristojni nadzorniki in ki naj bi bili posledica nezadostnega nadzora v preteklosti. Probleme pri ustanavljanju finančnih konglomeratov, kot navajata tudi Dierick (2004) in Skipper (2000), je mogoče deliti na problem regulatorne arbitraže, problem okužbe, moralni hazard, problem transparentnosti, konflikt interesov in zlorabo tržne moči. Do t. i. regulatorne arbitraže prihaja, ker ima vodilni subjekt v konglomeratu vpliv na ostale člane skupine, zato se lahko določene transakcije knjižijo v poslovnih knjigah

10 *Po podatkih Evropske skupnosti je za primeren zaslužek pripravljeno tveganje prevzeti kar 15–20 % bank (Šelih v Režek, 2002: 150).*

11 *Evropska zakonodaja določa, da mora biti najmanj en subjekt iz zavarovalniškega sektorja in najmanj en iz bančnega ali naložbenega (Direktiva 2002/87/ES, 2003), kar pomeni, da ni treba, da so v skupini zastopani vsi trije osnovni finančni sektorji.*

drugega subjekta in ne tistega, od katerega izvirajo oziroma pride do medsebojnih poslov zaradi izkoriščanja regulatornih razlik med posameznimi subjekti, ki so podvrženi različni normativni ureditvi in nadzoru. Transakcije tako le navidezno zadostijo nadzorniškim zahtevam, dejansko pa jih obidejo.[12] Za okužbo gre, ko se težave, ki pestijo en subjekt v skupini, prenesejo na ostale in ogrozijo finančno stabilnost skupine, lahko tudi celotnega finančnega trga, odvisno od moči in pomembnosti skupine. Najbolj tipičen primer moralnega hazarda v zvezi s konglomerati je povezan z velikostjo in pomembnostjo skupine za gospodarstvo izvorne države. Pridobi si lahko sloves, da je »too big to fail«, torej prevelik, da bi si lahko privoščili njegov zaton, zato se v javnosti in v skupini pričakuje, da bo zanj, v primeru nastanka težav, poskrbela in ga rešila država. Takšna percepcija pa znotraj skupine spodbuja bolj tvegano obnašanje oziroma poslovanje. Pomanjkanju transparentnosti prav tako botruje velikost konglomerata in njegova kompleksnost, kar povzroči, da nadzorniki in ostali udeleženci na trgu težje pridobijo natančne, predvsem pa jasne, podatke o strukturi konglomerata in vrsti tveganj, ki jim je izpostavljen, tudi zaradi razpršenosti le-teh znotraj konglomerata. Do konflikta interesov prihaja, ker konglomerat v odnosu do svojih strank nastopa v različnih vlogah, ki so med seboj nasprotujoče.

Zakon o finančnih konglomeratih ([ZFK], 2006) določa dopolnilni nadzor nad nadzorovanimi osebami, ki so del finančnega konglomerata[13], v skladu z zahtevami Direktive Evropskega parlamenta in Sveta 2002/87/ES (2003) o dopolnilnem nadzoru kreditnih institucij, zavarovalnic in investicijskih družb v finančnem konglomeratu. Cilji dopolnilnega nadzora po ZFK (2006) so predvsem: zagotoviti obvladovanje tveganj, ki so povezana s poslovanjem nadzorovanih oseb v finančnem konglomeratu, in s tem večjo stabilnost finančnega sektorja; ob sodelovanju pristojnih nadzornih organov in koordinatorja povečati učinkovitost nadzora nad nadzorovanimi osebami iz različnih finančnih sektorjev, kadar so le-te del finančnega konglomerata; povečati preglednost in varnost delovanja finančnega trga v Republiki Sloveniji kot sestavnega dela enotnega finančnega trga na območju držav članic Evropskih skupnosti, ki delujejo v okviru Evropske unije. Pristojni nadzorni organi za bančni sektor je BS, ki je tudi dolžna sprejeti ukrepe ob morebitnih ugotovljenih kršitvah, za določene kršitve, predvidene v ZFK (2006), pa nastopa tudi kot prekrškovni organ.

12 *Primer regulatorne arbitraže sta dvakratno oziroma večkratno štetje kapitala (double or multiple gearing – dvakrat se uporabi isti kapital za izkazovanje kapitalske ustreznosti) ali prekomerno finančno vzvodenje oziroma prekomerna uporaba dolžniškega kapitala (excessive leveraging – družba mati se prekomerno zadolžuje, ta dolg pa nato v obliki lastniškega kapitala vloži v hčerinske družbe).*

13 *V RS sta pri Ministrstvu za finance registrirana dva finančna konglomerata, to sta Skupina Triglav, ki je bila vpisana v register dne 24. 10. 2007, odločba pa izdana skoraj leto prej. Nadrejena oseba, ki je na vrhu finančnega konglomerata je Zavarovalnica Triglav, d. d., Ljubljana. Drugi pa je KD – AS, finančni konglomerat, vpisan 26. 10. 2010, odločba izdana 22. 9. 2010. Nadrejena oseba je KD, finančna družba, d. d., Ljubljana. Koordinator obeh je Agencija za zavarovalni nadzor, pristojni nadzorni organ, kot ga opredeljuje Zakon o finančnih konglomeratih v 16. točki 2. člena, pa BS.*

3.4 Hipotekarne in komunalne obveznice

Listinjenje (ang. Securitization)[14] je bila ena pomembnejših finančnih inovacij, ki je pripomogla k nastanku finančne krize. Proces listinjenja, po zelo skopi definiciji, pomeni zbiranje in združevanje podobnih si posojil v »pakete«, ki se nato financirajo s prodajo vrednostnih papirjev ali izdajo vrednostnih papirjev na podlagi kritnega premoženja. Podobno meni tudi Štiblar (2008), ki piše, da se je kriza začela v ZDA kot nepremičninska in se prenesla na finančna področja, s finančnih trgov pa nazaj v realno gospodarstvo, kjer se je z razraščanjem hipotekarnih posojil tudi začela. Ekonomisti sedaj ugotavljajo, da pretvorba osnovnega posojila denarja v vrednostne papirje v resnici nima naloge, da razprši tveganje, temveč da dejansko skrije tveganje osnovnega posla hipotečnega posojila in njegov izvor. Prodaja tveganj iz osnovnega posla povečuje likvidnost v sistemu in celotno posojilno aktivnost izmakne strogi kontroli centralnih bank (merila likvidnosti, solventnosti, Basel II) (Štiblar, 2008: 87). Splošno ureditev listinjenja za bančni sektor vsebuje ZBan-1 (2010), ki določa, da mora banka na podlagi ustreznih politik in postopkov ocenjevati in obravnavati tveganja, ki izhajajo iz poslov listinjenja, ne glede na vlogo, v kateri pri tem nastopa (investitor, originator, sponzor ali drugi udeleženec), vključno s tveganjem ugleda.

Listinjenje je lahko tudi proces izdajanja vrednostnih papirjev, zavarovanih s hipotekami.[15] Hipotekarna in komunalna obveznica sta vrednostna papirja visoke kreditne kakovosti, izdana pod pogoji iz Zakona o hipotekarni in komunalni obveznici ([ZHKO-1], 2012) in katerih kritje se zagotavlja na podlagi kritnega premoženja[16], njuni imetniki pa imajo ob stečaju izdajatelja prednostni položaj pri poplačilu iz tega premoženja. Hipotekarne in komunalne obveznice lahko izdaja samo banka, ki je pred tem od BS pridobila dovoljenje za njihovo izdajo v skladu z ZHKO-1 (2012). BS na podlagi tega zakona podeljuje tudi dovoljenje za opravljanje poslov skrbniku kritnega registra, ki je od izdajatelja ločena in neodvisna oseba. S pomočjo zakonskih načel, kot so kritno načelo, načelo zmanjšanja in odprave tveganj, načela ločenosti kritnega premoženja, dodatnega zavarovanja, prednostnega poplačila imetnikov hipotekarnih obveznic, predčasnega poplačila

14 Listinjenje je tudi »zloglasna« metoda institucij v t. i. sistemu senčnega bančništva, institucij, ki sicer izvajajo finančne storitve, vendar ne sodijo pod strogo bančno regulativo. Izraz senčno-bančni sistem je nastal leta 2007, ko ga je uporabil Paul McCully, direktor investicijskega giganta Pimco, izviral pa naj bi iz leta 1970, z razvojem skladov denarnega trga, katerih računi so funkcionirali kot bančni depoziti, niso pa bili podvrženi bančnemu nadzoru. Senčno-bančni sistem je potemtakem rezultat treh dejavnikov: povečanja konkurence nebančnih institucij, slabe regulacije in inovacij finančnih produktov. Ali obratno, prav osredotočenje regulacije na zdrav in stabilen bančni sistem je spodbujalo rast senčno-bančnega sistema. Podrobneje glej tudi http://ec.europa.eu/internal_market/finances/shadow-banking/index_en.htm.

15 Osnovna razlika med modeloma hipotekarne obveznice (mortgage bond) in modelom listinjenja (mortgage backed securities, MBS), ki se je razvil predvsem v anglosaškem pravnem sistemu, je v tem, da pri drugem modelu institucije, ki dajejo hipotekarna posojila, ne izdajajo hipotekarnih obveznic z namenom pridobivanja finančnih virov, torej zaradi refinanciranja kot v modelu hipotekarne obveznice, temveč hipotekarna posojila preprosto odprodajo posebnim finančnim institucijam.

16 Kritno premoženje hipotekarnih obveznic po ZHKO-1 (2012) so terjatve iz naslova hipotekarnih kreditov za stanovanjske in komercialne nepremičnine, sredstva nadomestnega kritnega premoženja, določenega z ZHKO-1 (2012) in izvedeni finančni instrumenti, ki jih izdajatelj sklene v zvezi s kritnim premoženjem.

in načelo omejitve izdajanja obveznic na banke, naj bi se zagotavljalo temeljno načelo varnosti hipotekarne obveznice oz. varnosti imetnikov hipotekarnih obveznic. BS ima torej tudi v primeru izdajanja navedenih vrednostnih papirjev široka nadzorna pooblastila.

4 RAZPRAVA

Nedvomno je prav zaradi finančne krize aktualno vprašanje, kakšne politične in sistemske rešitve je treba sprejeti (Hetzer, 2012: 250), da se situacija ne bi ponovila, čeprav vemo, da so gospodarska gibanja ciklična in da je imel poglavitno vlogo prav človeški faktor. Hetzer (2012) namreč meni, da je korupcija bistveno vplivala na razvoj dogodkov.

Pomen centralne nadzorne bančne institucije, ki sledi priporočilom stroke in tujim dobrim praksam, ni le v zagotavljanju varnega in transparentnega delovanja bančnega sektorja in finančne stabilnosti. Izkušnje obdobja po finančni krizi napotujejo na zaključek, da je tudi ključen dejavnik prevencije in boja proti finančni kriminaliteti.

Ugotovitev potrjujeta tako kratek prikaz pozitivnopravne ureditve v prispevku kot tudi pretekle izkušnje našega kazenskega pravosodja. Pred nekaj leti je potekal kazenski proces zoper podjetnika iz virtualne države, ki je preko koprske banke opral približno šest milijonov EUR, ker le-ta še ni imela vzpostavljenega sistema nadzora, kot ga zahteva ZPPDFT (2007). Podjetnik je račun odprl s ponarejeno potno listino, v imenu neobstoječe gospodarske družbe, s sedežem v mednarodno nepriznanem subjektu, situiranem na naftni ploščadi. Izrečena je bila oprostilna sodba, zasežen denar pa vrnjen na račun zagovornika, z blagoslovom Vrhovnega sodišča RS. Podobno sta pred leti povečanje oziroma pridobitev nadzora BS nad hranilno-kreditnimi službami razkrila poslovno in moralno sporne prakse, ki so jih poleg stečajnih senatov obravnavali tudi organi kazenskega pregona. Neuspešno, predvsem zaradi prepočasnega ukrepanja pristojnih institucij, zaradi domnevno protipravnih ravnanj stečajnih upraviteljev in ne nazadnje zaradi nepotrebnega spreminjanja kazenske zakonodaje. Kot piše Richard Schneider (2011), je bila prizorišče zločina tudi bančna skupina Hypo Alpe Adria. Zgodba še nima sodnega epiloga, avtor pa v knjigi opisuje trgovino z orožjem, pranje denarja, nakupe precenjenih zemljišč, načrtno izčrpavanje družb in »tajkunsko« privatizacijo velikih državnih podjetij ter podkupovanje politikov, pod skupnim nazivom »banka balkanske mafije«, ki je delovala tudi pri nas, dejanja pa naj bi razkril šele stečaj Vegrada in ne nadzorna bančna institucija.

V sporočilu za javnost BS poroča (Banka Slovenije, 2012), da je med izvajanjem nadzora[17] v bankah leta 2009 izdala 172 ukrepov, leta 2010 121 in leta 2011 263. V

17 *BS se je odzvala na kritike v medijih in v svojem sporočilu med drugim navedla, da je bil v obdobju po izbruhu krize od 2009 dalje največji poudarek v celostnih pregledih dan pregledu kreditnega tveganja, sledila sta likvidnostno in kapitalsko tveganje. Opravili so vrsto tematskih pregledov s področja preprečevanja pranja denarja, in financiranja terorizma, pregledi pa so zajemali tudi preglede družb v bančnih skupinah, menedžerskih odkupov, premostitvenih kreditov, upravljanja problematičnih naložb, kreditiranja določenih fizičnih in pravnih oseb ter projektnega financiranja.*

zadnjih dveh letih je BS podala Vrhovnemu državnemu tožilstvu RS eno pobudo za začetek kazenskega postopka, na Nacionalni preiskovalni urad so naslovili tri prijave suma kaznivega dejanja, na krajevno pristojno okrožno državno tožilstvo so podali tri ovadbe in na pristojno policijsko upravo eno obvestilo o nepravilnostih in eno obvestilo o sumu kaznivega dejanja. Skupno torej le devet neenotno poimenovanih aktov, brez pravno utemeljenega razloga za tako razlikovanje, ki so bili poleg tega posredovani različnim organom. Iz sporočila za javnost je tudi razbrati, da guverner zagovarja stališče, da BS ni preiskovalni urad, da njena naloga ni odkrivanje kaznivih dejanj, da nima dostopa do zaupnih dokumentov ipd., čeprav je v 231. členu ZBan-1 (2010) izrecno določeno, da sme (po določilih kazenske zakonodaje pa mora) BS zaupne informacije posredovati sodišču, državnemu tožilstvu ali policiji za potrebe kazenskega postopka.[18] V sporočilu so še zapisali, da so za odkrivanje notranjih prevar, goljufij in drugih kaznivih dejanj pri poslovanju banke pristojni organi odkrivanja in pregona.[19]

Hetzer (2012) pojasnjuje, da gre pri vprašanju kazenskega pregona odgovornih za finančno krizo za eno najkompleksnejših problematik gospodarskega kazenskega prava na sploh. Vendar dodaja, da je kazenski pregon nujen zaradi načel socialne pravičnosti in enakosti pred zakonom. S kompleksnostjo in zahtevnostjo kaznivega dejanja gospodarske kriminalitete se manjša verjetnost, da bo kaznivo dejanje sploh evidentirano kot sum, če pa že bo podan sum, se prav tako z večanjem kompleksnosti in zahtevnosti primera zmanjšuje verjetnost, da bo podana ovadba in kasneje na sodišču izrečena pravnomočna sodba; taka ugotovitev napotuje storilce gospodarske kriminalitete, da je za njih osebno ali njihovo združbo smiselno iskanje in izvajanje vedno novih in zapletenejših kaznivih dejanj (Hren, 2004: 508). Logično je torej, da BS kot najbolj strokovna in usposobljena bančna institucija v državi, s širokimi nadzornimi oziroma regulatornimi pooblastili, prva zazna protipravna ravnanja udeležencev na segmentu finančnega trga, ki jih nadzoruje, ter poslovodnih organov v bančnem sektorju. Zato je nujno, da že v začetni fazi, torej v fazi odkrivanja, sodeluje s policijo in tožilstvom, ki nato pridobita ustrezne sodne odločbe, bodisi za pridobitev zaupnih bančnih podatkov ali za hišno preiskavo.[20]

18 *Vsi državni organi in organizacije z javnimi pooblastili so dolžni naznaniti kazniva dejanja, za katera se storilec preganja po uradni dolžnosti, če so o njih obveščeni ali če kako drugače zvedo zanje. Obenem z ovadbo morajo navesti tudi dokaze, za katere vedo, in poskrbeti, da se ohranijo sledovi kaznivega dejanja in predmeti, na katerih ali s katerimi je bilo storjeno kaznivo dejanje, ter druga dokazila (145. člen Zakona o kazenskem postopku ([ZKP], 2012). Ovadba se poda pristojnemu državnemu tožilcu pisno ali ustno (147. člen ZKP, 2012). Opustitev ovadbe, da se pripravlja kaznivo dejanje in opustitev ovadbe kaznivega dejanja ali storilca, sta kaznivi dejanji po 280. členu in 281. členu Kazenskega zakonika ([KZ-1], 2012).*

19 *FSA (Financial Services Authority), britanska nadzorna in regulatorna finančna institucija, ima med zakonskimi cilji, ki jih zasleduje, zapisano, da je njena naloga tudi preprečevanje oziroma zmanjševanje finančne kriminalitete (reduction of financial crime). Britanci so pohiteli z reformami na tem področju, zato bo od aprila 2013 dalje finančni nadzor v pristojnosti nove institucije PRA (Prudential Regualtion Authority), ki bo delovala v okviru centralne banke (Bank of England), pod strožjimi pravili, ki naj bi preprečila ponovno krizo.*

20 *Po 214. členu ZBan-1 (2010) mora banka kot zaupne varovati vse podatke, dejstva in okoliščine o posamezni stranki, s katerimi razpolaga, ne glede na način, na katerega je pridobila te podatke. Po 5. odst. 156. člena ZKP (2012) lahko v primeru podanih razlogov za sum policija sama pridobi podatke o imetniku računa ali pooblaščenca od banke, vse ostale pa po odredbi preiskovalnega sod-*

Kakšna bo torej bodoča vloga našega centralnega bančnega nadzornika? Sprejet je nov baselski sporazum Basel III (Basel Committee on Banking Supervision, 2010), sprejeta je bila nova kapitalska direktiva (Direktiva 2010/78/EU Evropskega parlamenta in Sveta, znana tudi pod imenom Omnibus I), katere posamezna določila in zahteve smo morali prenesti v notranji pravni red. V evropskem prostoru že delujejo novi finančni nadzorniki in regulatorji, to so Evropski bančni organ (European Banking Authority, EBA), Evropski organ za vrednostne papirje in trge (European Securities and Markets Authority, ESMA) in Evropski organ za zavarovanja in poklicne pokojnine (European Insurance and Occupational Pensions Authority, EIOPA). Pravna ureditev delovanja evropskih nadzornikov in regulatorjev temelji na analizi napak in izkušenj, ki jih je razkrila finančna kriza. Pomembno je, da gre za neodvisne institucije, ki lahko koordinirajo aktivnosti nacionalnih nadzornikov, lahko pa tudi same prevzamejo neposredni nadzor v posamezni članici. Povzeti je torej mogoče, da z morebitnimi premišljenimi reformami v naši državi zaostajamo, pa čeprav bi bile le-te usmerjene zgolj v doslednejšo implementacijo že uveljavljenih pravil in okrepitev nadzora na kritičnih področjih, s poudarkom na preventivni vlogi BS.

LITERATURA

Banka Slovenije. (2007). *Proces ocenjevanja tveganj.* Pridobljeno na http://www.bsi.si/iskalniki/nadzorniska-razkritja-vsebina.asp?VsebinaId=5786&MapaId=831

Banka Slovenije. (2008a). *Strateški načrt Banke Slovenije za obdobje od 2009–2012.* Pridobljeno na http://www.bsi.si/banka-slovenije.asp?MapaId=1294

Banka Slovenije. (2008b). *Usmeritve pri izvajanju ukrepov na področju preprečevanja pranja denarja in financiranja terorizma*. Pridobljeno na http://www.bsi.si/zakoni-in-predpisi.asp?MapaId=251

Banka Slovenije. (2012). *Odgovor na članek, objavljen dne 29. 8. 2012, z naslovom »Zamujena leta guvernerja Banke Slovenije« v časopisu Dnevnik*. Pridobljeno na http://www.bsi.si/iskalniki/sporocila-za-javnost.asp?VsebinaId=15557&MapaId=137#15557

Basel Committee on Banking Supervision. (2006). *International convergence of capital measurement and capital standards: A revised framework – comprehensive version*. Pridobljeno na http://www.bis.org/publ/bcbs128.pdf

Basel Committee on Banking Supervision. (2010). *Basel III: A global regulatory framework for more resilient banks and banking systems*. Pridobljeno na http://www.bis.org/publ/bcbs128.pdf

Dierick, F. (2004). *European Central Bank: Occasional paper No. 20.* Frankfurt am Main: ECB.

Direktiva 2002/87/ES. (2003). *Uradni list EU*, (06/Zv. 4, L 35/1, 2003). Pridobljeno na http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=DD:06:04:32002L0087:SL:PDF

nika, na predlog državnega tožilca (1. odst. 156. člena). Seveda to ni ovira, da BS posreduje svoje ugotovitve, ki ne vsebujejo zaupnih podatkov, zadostijo pa standardu razlogov za sum, na podlagi katerih policija in tožilec predlagata izdajo sodne odredbe.

Direktiva 2010/78/EU. (2010). *Uradni list EU*, (L 331/120, 2010). Pridobljeno na http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2010:331:0120:0161:SL:PDF

Dowd, K. (2009). Moral hazard and the financial crisis. *Cato Journal, 29*(1). Pridobljeno na http://www.cato.org/sites/cato.org/files/serials/files/cato-journal/2009/1/cj29n1-12.pdf

Federal Crisis Inquiery Commission. (2011). *The report*. Pridobljeno na http://fcic.law.stanford.edu/report

Hellmann, T. F., Murdock, K. C. in Stiglitz, J. E. (2000). Liberalization, moral hazard in banking, and prudential regulation: Are capital requirements enough? *The American Economic Review*, *90*(1). Pridobljeno na http://individual.utoronto.ca/zheli/G31.pdf

Hetzer, W. (2012). Financial crisis or financial crime? Competence and corruption. V M. Edelbacher, P. Kratcoski in M. Theil (ur.), *Financial crimes, a threat to global security* (str. 217–267). Boca Raton: CRC Press.

Hren, M. (2004). Problemi gospodarske kriminalitete in korupcije v Republiki Sloveniji ter uspešnost oziroma neuspešnost pregona tovrstnih dejanj. V G. Meško (ur.), *Preprečevanje kriminalitete, teorija, praksa in dileme* (str. 496–511). Ljubljana: Inštitut za kriminologijo.

Kazenski zakonik. (2012). *Uradni list RS*, (50/12).

Majič, M. (2002). *Operativno tveganje: definicija, regulacija in merjenje*. Pridobljeno na http://www.bsi.si/nadzor-bank.asp?MapaId=163

Organisation for Economic Co-operation and Development. (2009). *The corporate governance lessons from the financial crisis.* Pridobljeno na http://www.oecd.org/daf/corporateaffairs/corporategovernanceprinciples/42229620.pdf

Organisation for Economic Co-operation and Development. (2010). *Corporate governance and the financial crisis, conclusions and emerging good practices to enhance implementation of the principles*. Pridobljeno na http://www.oecd.org/daf/corporateaffairs/corporategovernanceprinciples/44679170.pdf

Režek, D. (2002). Preprečevanje in odkrivanje pranja denarja. V D. Maver, B. Kečanovič in P. Mrhar (ur.), *Problematika odkrivanja in pregona gospodarske kriminalitete* (str. 149–162). Ljubljana: MNZ RS.

Rotovnik, T. (2003). *Operativno tveganje in Basel II – pripravljenost bank v Sloveniji na zahteve novega kapitalskega sporazuma*. Pridobljeno na http://www.bsi.si/nadzor-bank.asp?MapaId=163

Rotovnik, T. (2004). *Operativno tveganje z regulatorne perspektive*. Pridobljeno na http://www.bsi.si/nadzor-bank.asp?MapaId=163

Schneider, R. (2011). *Kraj zločina: Hypo Alpe Adria.* Mengeš: Ciceron.

Skipper, D. H. Jr. (2000). *Financial services integration worldwide: Promises and pitfalls*. Pariz: OECD.

Sutherland, E. H. (2001). Is »white collar crime« crime? V N. Shover in J. P. Wright (ur.), *Crimes of privilege, readings in white-collar crime* (str. 12–20). New York: Oxford University Press.

Štiblar, F. (2008). *Svetovna kriza in Slovenci*. Ljubljana: ZRC SAZU.

Štiblar, F. (2010). *Bančništvo kot hrbtenica samostojne Slovenije*. Ljubljana: ZRC SAZU.

Tomasic, R. (2012). The financial crisis and the haphazard pursuit of financial crime. V M. Edelbacher, P. Kratcoski in M. Theil (ur.), *Financial crimes, a threat to global security* (str. 177–204). Boca Raton: CRC Press.
Zakon o bančništvu. (2010). *Uradni list RS*, (99/10).
Zakon o Banki Slovenije. (2006). *Uradni list RS*, (72/06).
Zakon o finančnih konglomeratih. (2006). *Uradni list RS*, (43/06).
Zakon o hipotekarni in komunalni obveznici. (2012). *Uradni list RS*, (10/12).
Zakon o kazenskem postopku. (2012). *Uradni list RS*, (32/12).
Zakon o potrošniških kreditih. (2010). *Uradni list RS*, (59/10).
Zakon o preprečevanju pranja denarja. (2001). *Uradni list RS*, (79/01).
Zakon o preprečevanju pranja denarja in financiranja terorizma. (2007). *Uradni list RS*, (60/07).

O avtorici:

Tanja Ahčan, okrožna državna tožilka pri Okrožnem državnem tožilstvu v Ljubljani, dodeljena oddelku za gospodarsko kriminaliteto in študentka prvega letnika doktorskega študija na Fakulteti za varnostne vede Univerze v Mariboru.

VARSTVOSLOVJE,
let. 15
št. 3
str. 385–397

Kriminaliteta nad starejšimi in izhodišča za varno staranje v Sloveniji

Anton Toni Klančnik, Tinkara Pavšič Mrevlje

Namen prispevka:

Prispevek predstavlja statistiko kaznivih dejanj nad starejšimi (populacija nad 64 let) v letih od 2001 do 2011. Ob prikazu projekcij staranja prebivalstva v naslednjih petdesetih letih bo zagotovo prišlo tudi do povečanja kriminalitete nad starejšimi. Da bi bilo staranje v prihodnosti varnejše, prispevek preko statističnega pregleda opozarja na najbolj rizična področja kriminalitete nad starejšimi.

Metode:

Pregled statističnih podatkov policije v letih 2001 do 2011 in kratek pregled literature.

Ugotovitve:

Kriminaliteta nad starejšimi v Sloveniji se je v letih med 2001 in 2011 skoraj podvojila. Najpogostejša skupina kaznivih dejanj nad starostniki so premoženjski delikti (dobrih 80 %), sledijo kazniva dejanja zoper človekove pravice in svoboščine (dobrih 5 %), gospodarska kriminaliteta (skoraj 5 %) in kazniva dejanja zoper življenje in telo (skoraj 3 %).

Omejitve/uporabnost raziskave:

Prispevek prikazuje dostopne podatke o kriminaliteti nad starejšimi. Omejitve zaključkov so vezane na težko dostopne podatke o tem, kakšne so težave starejših pri prijavi kaznivih dejanj (ali da do tega sploh pride) in kakšne vrste pomoč jim je pri tem nudena (če sploh).

Praktična uporabnost:

S pregledom značilnosti kriminalitete nad starejšimi v zadnjem desetletju poznamo tvegana področja, na podlagi katerih je mogoče oblikovati (oziroma nadaljevati) različne preventivne programe, usposabljanja za delavce institucij, ki so v stiku s starejšimi žrtvami kaznivih dejanj, in pripraviti ustrezne programe psihosocialne in medicinske pomoči žrtvam.

UDK: 343.988-053.9

Ključne besede: kriminaliteta, starejši, starostniki, viktimizacija, Slovenija

Crime against the Elderly and Guidelines for a Safer Aging in Slovenia

Purpose:

This paper presents statistical data on criminal offenses committed against elderly citizens (population above 64 years of age) in years from 2001 to 2011. According to projections of population ageing in the next fifty years the number of elderly crime victims is expected to grow. In order to contribute to the efforts towards a safer aging of citizens the paper draws attention to the criminal offences that put the elderly at the biggest risk.

Design/Methods/Approach:

The paper is a review of police statistical data in years between 2001 and 2011.

Findings:

Crime against the elderly in Slovenia has almost doubled from 2001 to 2011. Property crime is the most common offense against the elderly (over 80%), followed by crimes against human rights and freedom (over 5%), economic crime (almost 5%) and offences against life and limb (almost 3%).

Research Limitations/Implications:

The paper presents accessible data on crime against the elderly. The limitations of findings are thus linked to data that are difficult to access: about the elderly's hardhips at reporting crime and what kind of help are they offered when they do.

Practical Implications:

By analysing the characteristics of crime against the elderly in the last decade we have recognised areas of vulnerability which provide important information needed to form (or continue) a variety of preventive programs, trainings for workers of institutions that encounter elderly victims of crime, and organize appropriate programs for psychological, social and medical help to victims.

UDC: 343.988-053.9

Ključne besede: crime, elderly, victimisation, Slovenia

1 UVOD

Še iz otroštva se spominjamo pravljic, ki so nam jih namenjali starši, učitelji, bližnji. V kontekstu tega prispevka naj spomnimo na pravljico[1] o kralju, ki je ukazal, da morajo njegovi podaniki pomoriti vse stare ljudi, ki ne morejo več delati, češ niso več za nobeno rabo. A v tem kraljestvu je živel tudi mladenič, ki je imel svojega očeta nadvse rad; prav zato je pred kraljevimi sli skril očeta pod velik čeber in mu skrivaj nosil hrano. Taisti kralj je imel hčerko edinko, ki jo je želel poročiti z najpametnejšim mladeničem v kraljestvu, in za to si je izmislil razne uganke. Omenjeni mladenič je razrešil vse uganke in bil spoznan za najpametnejšega mladeniča, ki naj bi se nato poročil s kraljično. Kralja je seveda zanimalo, od kod mu toliko znanja, a je mladenič kralju dal vedeti, da bi mu rad pojasnil, če se ne

1 *Gre za slovensko ljudsko pravljico z naslovom Pšenica – najlepši cvet (Brenk, 2004).*

bi bal stroge kazni. Kralj ga je prepričal, naj se ne boji, nato pa prisluhnil njegovi pripovedi o tem, kako ima rad svojega očeta, ki ga je hranil in vzgojil, zato ga je skril pred izvršitvijo kraljevega ukaza. Kralj je uvidel, da starostniki niso odvečni, da so mladim potrebni modrost, izkušnje in znanja starih ljudi, čeprav ne morejo delati. Kralj je svoj zastrašujoči ukaz spremenil in poudaril, da se naj vsakdo do starih ljudi vede spoštljivo, njihovi otroci pa naj bodo svojim staršem hvaležni ter naj zanje poskrbe do poslednje ure njihovega življenja.

Pravljice med drugim na otroka prenašajo modrost, napotke, nasvete in izkušnje ter koristijo tudi današnjim otrokom (Kucler, 2002). Iz predstavljene pravljice izhaja opozorilo, da je treba starostnikom posvetiti ustrezno pozornost, saj so pomemben del naše družbe. Ni zanemarljivo dejstvo, da ima proces staranja signifikanten vpliv na medgeneracijske odnose, tj. med generacijo mlajših oz. mladih na eni in starostnikov na drugi strani. Predvsem zato, ker so ravno mlajši tisti, ki bodo v času starosti poskrbeli za starejše.

Med družbami se starostna meja za določanje, kdo je *starostnik* oziroma *starejši* nekoliko razlikuje. Običajno jo definira starost ob upokojitvi, torej nekje med 60. in 65. letom. Trenutno večina razvitih držav upošteva kronološko starost 65 let. A življenjska doba se podaljšuje, z njo tudi delovna doba, kar bo kmalu lahko povzročilo spremembe pri določanju starejše populacije.

V zadnjih desetletjih se je starostna struktura prebivalstva v svetu precej spremenila. Prebivalstvo je vse starejše, najpogosteje omenjana razloga za to sta konstantno zniževanje rodnosti in podaljševanje življenjske dobe (Križman, 2010; Petek-Šter in Kersnik, 2004). Povečan delež starejše populacije povzroča številne spremembe, ki terjajo čimprejšnje ustrezne rešitve na več področjih: socialno varstvo, politike zaposlovanja, stanovanjska problematika idr., kar je bilo izpostavljeno tudi v Mednarodnem akcijskem načrtu o staranju (Križman, 2010).

Z rastjo starejše populacije se zvišuje tudi število starejših žrtev kriminalitete. Članek predstavlja podatke, ki služijo kot osnova za oblikovanje nadaljnjih ukrepov – od preventive do dela vseh služb, ki pridejo v stik s starejšimi žrtvami kaznivih dejanj.

2 DEMOGRAFSKI PODATKI O STAROSTNI SESTAVI PREBIVALSTVA IN OCENE

Iz poročila Združenih narodov o staranju svetovnega prebivalstva (Združeni narodi, 2001) izhajajo statistični kazalci in projekcije na obstoječo situacijo. V naslednjih 50-ih letih se bo pričakovana življenjska doba ljudi na globalni ravni povišala za 10 let, kar naj bi v letih 2045–2050 predstavljalo starost okrog 76 let, takratna pričakovana življenjska doba ob rojstvu pa naj bi dosegala povprečno 80 let v bolj razvitih in 71 let v manj razvitih regijah.

Tudi študija Statističnega urada RS (Vertot, 2009) zajema nazorne demografske podatke o starostni sestavi prebivalstva. Delež oseb v starosti nad 64 naj bi se v EU-27 povečal s 17,1 % na 30 % – število starostnikov naj bi se predvidoma od leta 2008 do leta 2060 povečalo s 84,6 milijona na 151,5 milijona. V Sloveniji naj bi se po projekciji prebivalstva EUROPOP10 delež prebivalcev nad 64 let do leta 2060

povečal s 16,5 % (leta 2015) na 31,6 %, delež tistih nad 79 let pa naj bi se potrojil: s 4,7 % na 12,7 % (Razpotnik, 2011).

Več kot očitna je napoved, da se delež starejših v populaciji vztrajno in postopoma povečuje. Ta podatek je izrednega pomena tudi z vidika varnosti, zaščite in skrbi za starostnike, saj predstavljajo heterogeno skupino z velikimi razlikami v zdravstvenem stanju, funkcionalnih zmožnostih in osebnostnih lastnostih. Pri zdravju posameznika je treba upoštevati tudi njegove številne razsežnosti in ga obravnavati v kontekstu z bolnikovimi izkušnjami, prepričanji in pričakovanji. Za starostnika je pravzaprav značilno zmanjševanje duševnih in telesnih sposobnosti, h katerim prispevajo normalen fiziološki upad in številne kronične bolezni ter stanja (Petek-Šter in Kersnik, 2004).

3 KRIMINALITETA NAD STAROSTNIKI

Starostniki so tako kot druge starostne skupine lahko žrtve kriminalitete psihološke, spolne in finančne narave. Ne glede na to, kakšne vrste so kazniva dejanja, kje so se zgodila (doma ali na javnem mestu) in kdo jih je povzročil (poznana oseba, družinski član ali neznanec), so starejši ranljiva skupina žrtev zaradi resnih telesnih, psihičnih in socialnih posledic viktimizacije.

Slovenska policija vodi statistiko žrtev kaznivih dejanj tudi glede na starost. Najstarejšo skupino predstavljajo žrtve nad 64 let, natančnejše klasifikacije za višjo starost ni. V Evropi ni enotnega načina beleženja tovrstne statistike. V Italiji, na primer, vodijo statistiko z upoštevanjem starostne meje 65 let, v Franciji 60 let, na Švedskem pa žrtve kaznivih dejanj po starosti ločujejo le na mladoletne in polnoletne (Giannini et al., 2013a).

Delež kaznivih dejanj nad starejšimi v Sloveniji narašča. Od leta 2001, ko je bil ta pod 5 %, je do leta 2011 narasel na 8 %. Odstotek je v primerjavi z nekaterimi državami še vedno nizek, saj je bilo starejših žrtev v Italiji v letu 2011 približno 12 %, v Franciji pa leta 2008 dobrih 12 % (tu je potrebno upoštevati, da francoska statistika vključuje posameznike od 60. leta dalje) (Giannini et al., 2013b).

V tabeli 1 so prikazani statistični podatki o oškodovancih kaznivih dejanj nad 64 let, razdeljeni po vrsti kaznivega dejanja in spolu. Gre za statistične evidence slovenske policije med letoma 2001 in 2011, torej za zaznana in obravnavana kazniva dejanja nad starejšimi. Glede na to, kako je statistika vodena, obstaja možnost, da je bila posamezna starejša oseba večkrat oškodovana v različnih letih in/ali v posamičnem letu, kot tudi, da je bila žrtev več različnih kaznivih dejanj v tem obdobju. Zagotovo pa teh primerov ni toliko, da bi to pomembno vplivalo na rezultate.

Podatki o številu oškodovancev kaznivih dejanj so bili združeni po vrsti kaznivih dejanj, upoštevajoč umeščenost kaznivih dejanj po posameznih poglavjih kazenskega zakonika. Pri tem naj spomnimo, da je v obdobju, obravnavanem v tem prispevku, prišlo do uveljavitve številnih sprememb v Kazenskem zakoniku RS [KZ] (1994). Pri obravnavi kriminalitete nad starostniki je predvsem pomemben nov Kazenski zakonik [KZ-1] (2008). Ta je začel veljati s 1. 11. 2008 in je na novo

definiral kar nekaj kaznivih dejanj, na primer *umor in uboj* iz poglavja zoper življenje in telo ter *nasilje v družini* iz poglavja zoper zakonsko zvezo, družino in otroke.

Nekatera kazniva dejanja (tabela 1) so združena v enotno skupino glede na njihovo vrsto, saj so kot takšna precej podobna:

- kazniva dejanja uboja, umora in povzročitve smrti iz malomarnosti – v vseh primerih gre za nasilno smrt;
- povzročitev lahke, hude in posebno hude telesne poškodbe – gre za povzročitev telesnih poškodb z različno hudimi posledicami;
- ogrožanje varnosti in grožnja – do spremembe kazenske zakonodaje se je določba imenovala ogrožanje varnosti, nato grožnja;
- tatvina, velika tatvina in zatajitev – gre za protipravno prilastitev tujih premičnih stvari;
- rop, roparska tatvina in izsiljevanje so protipravna prilastitev tuje premične stvari z elementi nasilja;
- oškodovanje tujih pravic, goljufija ter poneverba in neupravičena uporaba tujega premoženja – gre za spravljanje drugega v zmoto z lažnivim prikazovanjem/prikrivanjem okoliščin, prevaro oziroma zlorabo zaupanja;
- ostala kazniva dejanja; v to skupino je združenih več poglavij[2] iz kazenskega zakonika, ki so posamično zelo redko obravnavana.

3.1 Najpogostejša kazniva dejanja nad starejšimi

Pregled statističnih podatkov kaže, da je največ starostnikov (dobrih 80 %) oškodovanih s kaznivimi dejanji zoper premoženje – na leto jih policija v povprečju obravnava skoraj 4.000. Sledijo starejši oškodovanci s kaznivimi dejanji zoper človekove pravice in svoboščine (dobrih 5 %). Teh je na letni ravni povprečno 269. Gospodarska kriminaliteta nad starostniki predstavlja tretjo najpogostejšo skupino kaznivih dejanj (skoraj 5 %, približno 230 na leto), po pogostosti pa ji sledi skupina oškodovancev kaznivih dejanj zoper življenje in telo (skoraj 3% oziroma 143 primerov letno). Žrtve ostalih prikazanih kaznivih dejanj so manj pogoste, dosegajo največ 1,5 % žrtev, torej približno 70 obravnavanih primerov letno.

3.2 Razlike po spolu

Primerjava vseh starejših oškodovancev po spolu kaže, da je starejših žrtev kaznivih dejanj nekoliko več med moškimi (za približno 6 %). Starejši moški so veliko pogostejše žrtve kaznivih dejanj zoper življenje in telo (predvsem pri telesnih poškodbah, kjer je moških oškodovancev skoraj 50 % več), pogosteje pa so tudi obravnavani kot žrtve s področja kaznivih dejanj zoper človekove pravice in svoboščine (tudi do 25 % več moških na specifičnih kaznivih dejanjih).

2 *Gre za poglavja kaznivih dejanj: zoper človečnost (14), volilno pravico in volitve (17), čast in dobro ime (18), človekovo zdravje (20), delovno razmerje in socialno varnost (22), pravni promet (25), uradno dolžnost, javna pooblastila in javna sredstva (26), pravosodje (28), splošno varnost ljudi in premoženja (30), varnost javnega prometa (31), okolje, prostor in naravne dobrine (32).*

Tabela 1: Število najpogostejših kaznivih dejanj nad starejšimi

KAZNIVA DEJANJA (zoper)	SPOL	2001	2002	2003	2004	2005	2006	2007	2008	2009	2010	2011	SKUPAJ		
													∑	*M*	%*
Življenje in telo	M	71	101	88	96	94	83	90	90	70	91	74	948	86,18	60,19
	Ž	51	55	64	63	60	48	49	53	62	64	58	627	57	39,81
	∑	122	156	152	159	154	131	139	143	132	155	132	1575	143,18	2,96
Uboj, umor, povzr. smrti iz malomarn.	M	2	7	-	4	3	3	7	2	2	3	4	37	3,36	52,11
	Ž	3	1	4	5	5	3	4	4	3	-	2	34	3,09	47,89
Telesne poškodbe	M	58	74	72	74	77	71	73	81	62	80	65	787	71,55	59,76
	Ž	39	49	54	49	51	35	42	44	54	62	52	531	48,27	40,32
Človekove pravice in svoboščine	M	103	128	124	157	131	154	167	160	158	148	163	1593	144,82	53,84
	Ž	97	88	117	111	106	150	173	173	113	127	111	1366	124,18	46,16
	∑	200	216	241	268	237	304	340	333	271	275	274	2959	269	5,57
Ogrožanje varnosti, grožnja	M	69	94	100	122	111	129	135	138	140	129	138	1305	118,64	55,39
	Ž	64	70	96	90	88	126	118	130	84	95	90	1051	95,55	44,61
Spolno nedotakljivost	M	1	-	1	-	-	-	1	-	-	1	-	4	0,36	8,33
	Ž	8	2	2	9	3	6	5	-	2	3	4	44	4	91,67
	∑	9	2	3	9	3	6	6	-	2	4	4	48	4,36	0,09
Posilstvo	M	-	-	-	-	-	-	-	-	-	-	-	-	-	-
	Ž	5	1	1	3	1	3	5	0	1	1	2	23	2,09	100
Spolno nasilje	M	1	-	-	-	-	-	-	-	-	-	-	1	0,09	11,11
	Ž	2	-	-	-	1	1	-	-	1	2	1	8	0,73	88,89
Zakonsko zvezo, družino in otroke	M	-	-	-	-	2	-	-	1	49	46	37	135	12,27	19,85
	Ž	1	1	1	1	1	-	-	22	188	186	144	545	49,55	80,15
	∑	1	1	1	1	3	-	-	23	237	232	181	650	216,67	1,22
**Nasilje v družini	M	-	-	-	-	-	-	-	1	48	45	37	130	43,33	20,21
	Ž	-	-	-	-	-	-	-	9	186	184	143	513	171	79,78
Premoženje	M	1552	1710	1600	2194	2135	2213	2212	1982	2130	2222	2873	22823	2074,82	51,96
	Ž	1272	1545	1495	1869	1772	1854	2268	2013	2114	2254	2644	21100	1918,18	48,04
	∑	2824	3255	3095	4063	3907	4067	4480	3995	4244	4476	5517	43923	3993	82,62

Tabela 1: nadaljevanje

Tatvina, velika tatvina, zatajitev	M	1197	1360	1309	1806	1809	1863	1827	1686	1786	1823	2041	18507	1682,45	51,13
	Ž	1016	1223	1239	1562	1459	1536	1894	1772	1782	1945	2258	17686	1607,82	48,87
Rop, rop. tatvina, izsiljevanje	M	19	19	17	20	18	29	17	18	34	28	13	232	21,09	37,66
	Ž	27	37	31	27	43	47	32	24	38	41	37	384	34,91	62,34
Goljufije, poneverbe	M	118	96	59	108	86	91	106	75	88	182	621	1630	148,18	56,34
	Ž	95	140	73	90	124	89	145	83	123	123	178	1263	114,82	43,66
Gospodarstvo	M	52	210	27	28	18	36	39	38	28	276	471	1223	111,18	48,17
	Ž	34	340	20	16	21	49	23	20	36	320	437	1316	119,64	51,83
	∑	86	550	47	44	39	85	62	58	64	596	908	2539	230,82	4,77
Poslovna goljufija	M	29	191	5	16	6	24	27	25	12	260	447	1042	94,73	47,39
	Ž	11	326	5	7	6	37	15	6	9	304	431	1157	105,18	52,61
Javni red in mir	M	11	20	29	23	17	19	23	28	25	18	18	231	21	34,74
	Ž	36	27	47	43	41	32	51	69	54	21	13	434	39,45	65,26
	∑	47	47	76	66	58	51	74	97	79	39	31	665	60,45	1,25
Ostalo	M	56	33	34	48	32	39	33	28	33	44	52	432	39,27	55,74
	Ž	28	30	30	41	27	39	20	36	32	27	33	343	31,18	44,26
	∑	84	63	64	89	59	78	53	64	65	71	85	775	70,45	1,46
SKUPAJ	M	1846	2202	1903	2546	2429	2544	2565	2327	2493	2846	3688	27389	2489,91	51,52
	Ž	1527	2088	1776	2153	2031	2178	2589	2386	2601	3002	3444	25775	2343,18	48,48
	∑	3373	4290	3679	4699	4460	4722	5154	4713	5094	5848	7132	53134	4883,09	100
% kaznivih dejanj nad starejšimi***		4,51	5,56	4,80	5,43	5,29	5,23	5,80	5,75	5,82	6,53	8,04			

Vir: Statistične evidence slovenske policije med letoma 2001 in 2011, pridobljeno s strani Oddelka za načrtovanje in analitiko Generalne policijske uprave.

* Odstotki v temnih poljih predstavljajo delež oškodovancev za posamezno kaznivo dejanje glede na število oškodovancev vseh predstavljenih kaznivih dejanj; odstotki v svetlih poljih predstavljajo odstotek žensk/moških žrtev po posameznem kaznivem dejanju oziroma skupini.

** Pri nasilju v družini se je pri izračunih upoštevalo obdobje treh let (2009–2011), ker je bilo to kaznivo dejanje v Kazenski zakonik umeščeno šele ob koncu leta 2008.

*** Odstotek kaznivih dejanj nad starejšimi glede na število vseh kaznivih dejanj v tistem letu.

Starejše ženske izrazito izstopajo kot žrtve kaznivih dejanj zoper spolno nedotakljivost in zoper zakonsko zvezo, družino in otroke, kjer so 4 do 11-krat pogostejše žrtve kot moški. Tudi pri obravnavi primerov kaznivih dejanj zoper javni red in mir prednjačijo ženske oškodovanke, katerih je skoraj enkrat več kot moških. Značilnosti dinamike nasilja in šibkejša fizična moč žensk so gotovo pomembni razlogi za opisane razlike. Mogoče jih je aplicirati tudi v skupini premoženjskih kaznivih dejanj z elementi nasilja, edini skupini s področja premoženjske kriminalitete, kjer so ženske pogostejše žrtve.

3.3 Trend kriminalitete nad starejšimi med leti 2001 in 2011

Predstavljeni podatki sicer kažejo, da je v letih 2003, 2005 in 2008 prišlo do rahlega upada števila starejših žrtev kaznivih dejanj, vendar pa kriminaliteta nad starejšimi narašča, še posebej po letu 2009. Število vseh kaznivih dejanj, katerih oškodovanci so starostniki, se je od leta 2001 (3.373 oškodovancev) do leta 2011 (7.132 oškodovancev) skoraj podvojilo.

Največji porast med predstavljenimi kaznivimi dejanji se je zgodil na področju gospodarske kriminalitete, in sicer v letih 2010 in 2011, visoko število tovrstnih obravnav pa je bilo tudi v letu 2002. V tem sklopu smo izpostavili zgolj kaznivo dejanje *poslovne* goljufije, ki je pravzaprav precej podobno kaznivemu dejanju goljufije, saj gre v obeh primerih za t. i. lažno prikazovanje oziroma preslepitev in za prikrivanje, da bo nekaj storjeno, pri čemer pride do oškodovanja tujega premoženja. Pomembna ločnica med kaznivima dejanjema pa je v tem, da je poslovna goljufija vezana na opravljanje gospodarske dejavnosti (npr. prodaje od vrat do vrat v imenu podjetij, predstavljanja različnih izdelkov, tudi preslepitve preko interneta z loterijskimi stavami ipd.). Porast gospodarske goljufije v omenjenih letih, ki je v primerjavi z obdobji najnižje obravnave tovrstne kriminalitete lahko tudi 70-kratna, lahko pojasnimo s poročili policije: v letu 2002 je policija preiskovala obsežen primer, v katerem so zaznali več kot tisoč kaznivih dejanj poslovne goljufije (Policija, 2003), v letu 2010 pa je bilo preganjanje gospodarske in finančne kriminalitete prednostna naloga policije (Policija, 2011). Ocenjujemo, da so ta dejanja tudi posledica gospodarske krize in s tem povezanimi socialno-finančnimi primanjkljaji posameznikov, ki so v želji po hitrem zaslužku vložena finančna sredstva pogostokrat izgubili (bili ogoljufani) v različnih prevarah in malverzacijah. Po drugi strani so tudi nekatere pravne osebe in samostojni podjetniki-posamezniki z goljufivimi nameni izkoristili sugestibilnost, stisko in bolezen ter zlorabili starostnikovo zaupanje.

Do velikega porasta, pa čeprav ne do take mere kot velja za gospodarsko kriminaliteto, je prišlo tudi na področju kaznivih dejanj zoper premoženje. Z manjšimi nihanji se je v letih od 2001 do 2011 število obravnavanih primerov skoraj podvojilo. Prevladujejo premoženjski delikti brez elementov (fizičnega) nasilja, kot so tatvine, velike tatvine in zatajitve, sledijo jim goljufije, oškodovanje tujih pravic ter poneverba in neupravičena uporaba tujega premoženja ter premoženjski delikti z elementi fizičnega nasilja: rop, roparska tatvina in izsiljevanje. Tudi sicer je premoženjska kriminaliteta najpogostejša, zato ta podatek na populaciji starostnikov

ne preseneča. Zagotovo pa je k porastu tovrstnih kaznivih dejanj prispevala gospodarska kriza, s svojim predvidljivim vedenjem (na primer dvigovanjem celotne pokojnine na banki) in slabšimi psihofizičnimi sposobnostmi pa so starejši občani zagotovo bolj izpostavljeni. Na tem mestu je smiselno spomniti na posebnost kazenskopravne ureditve v Sloveniji, po kateri se nekatera premoženjska kazniva dejanja[3], ki so izvedena med ali nad družinskimi člani, preganja le na njihovo zasebno tožbo. V praksi to pomeni, da že ob morebitni prijavi, da je premoženjsko kaznivo dejanje izvedel družinski član oz. ožji sorodnik, policija ne bo mogla izvajati dodatnih aktivnosti (zbiranje obvestil in dokazov, vrednotenje dokazov, ogled kraja dejanja, zaslišanje osumljenca, morebitne privedbe in pridržanja osumljenca, hišne preiskave idr.). Pri starejših posameznikih je taka ureditev lahko še posebej problematična, saj že sama prijava bližnjega od žrtve terja specifično psihofizično moč in sposobnosti, zasebna tožba pa je v tem pogledu še zahtevnejša.

Kazniva dejanja zoper človekove pravice in svoboščine starejših so tretja po vrsti glede na porast od leta 2001. Z manjšimi nihanji je število tovrstnih obravnavanih kaznivih dejanj naraslo za tretjino. Posebej smo izpostavili zgolj eno kaznivo dejanje, in sicer *ogrožanje varnosti*, ki se je po noveliranju kazenske zakonodaje preoblikovalo v kaznivo dejanje *grožnje*. Pri kaznivem dejanju ogrožanja varnosti je šlo za enostavno dikcijo o tem, da se kaznuje tistega, ki ogrozi varnost druge osebe z resno grožnjo, da bo napadel njeno življenje ali telo; pregon za to dejanje se je pričelo na predlog oškodovanca. Število teh kaznivih dejanj je med leti 2001 in 2011 naraslo za dobrih 70 % in predvidevamo lahko, da se bo ta trend nad starostniki nadaljeval. Vprašanje pa je, ali bodo statistični podatki po letu 2012 to tudi pokazali. Maja 2012 so namreč začele veljati spremembe vsebine tega kaznivega dejanja (135. člen Zakona o spremembah in dopolnitvah Kazenskega zakonika [KZ-1B], 2011), po katerem se pregon za ustrahovanje in resne grožnje začne na zasebno tožbo, na predlog pa, če grožnja vsebuje tudi verjetnost hude poškodbe. Kvalificirana oblika tega dejanja bo posledično najbrž večkrat zajela povzročitev telesnih poškodb in bo lahko kot taka pogosteje evidentirana kot povsem drugo kaznivo dejanje. Predvsem pa je potreben tehten premislek, kako v teh primerih sploh ustrezno zaščititi ranljive skupine ljudi – tudi starostnike. Takšna določba telesno in duševno celovitost starostnikov bolj ogroža, kot pa jih varuje in ščiti.

3.4 Nasilje nad starejšimi

Od vseh kaznivih dejanj nad starejšimi so zagotovo najtežje zaznana in poznana tista, ki vsebujejo elemente nasilja, zato je smiselno tu vsebino nekoliko poglobiti. Zakon o preprečevanju nasilja v družini (2008) definira več vrst nasilja: fizično,

3 *O tem govori 224. člen KZ-1 (2008): »Za kaznivo dejanje iz 204. (tatvina), 205. (velika tatvina), prvega, drugega, četrtega in petega odstavka 208. (zatajitev), 210. (odvzem motornega vozila), 211. (goljufija), prvega in drugega odstavka 215. (izneverjenje) in 220. člena (poškodovanje tuje stvari) tega zakonika, ki so bila storjena proti zakoncu ali osebi, s katero živi v zunajzakonski skupnosti, ali partnerju iz registrirane istospolne partnerske skupnosti, krvnemu sorodniku v ravni vrsti, bratu ali sestri ali drugemu krvnemu sorodniku v stranski vrsti do vštetega tretjega kolena, sorodniku po svaštvu do vštetega drugega kolena, posvojitelju ali posvojencu, rejniku ali rejencu ali proti drugim osebam, s katerimi živi storilec v skupnem gospodinjstvu, se pregon začne na zasebno tožbo.«*

spolno, psihično in ekonomsko nasilje ter zanemarjanje. Ker so nekatera kazniva dejanja kompleksna ali sestavljena (npr. tatvina s silo lahko pomeni roparsko tatvino), so umeščena v kombinaciji z drugo obliko nasilja:

- fizično nasilje: uboj, umor, povzročitev lahke, hude in posebno hude telesne poškodbe,
- zanemarjanje: povzročitev smrti iz malomarnosti,
- psihično nasilje: ogrožanje varnosti in grožnja,
- spolno nasilje (spolne zlorabe): posilstvo in spolno nasilje,
- psihično, fizično, ekonomsko nasilje in zanemarjanje: nasilje v družini,
- ekonomsko nasilje: tatvina, velika tatvina in zatajitev,
- ekonomsko, fizično in psihično nasilje: rop, roparska tatvina in izsiljevanje,
- ekonomsko nasilje: goljufija, oškodovanje tujih pravic ter poneverba in neupravičena uporaba tujega premoženja.

Našteta kazniva dejanja pogosto zajemajo tudi psihično nasilje, opravljajo pa se lahko v okviru družine, institucionalno in izven omenjenih okvirov (ad hoc kraji).

Do uveljavitve novega kaznivega dejanja *nasilje v družini* 1. novembra 2008 je bilo ugotavljanje vsebinsko in statistično ustreznih podatkov zelo oteženo. Do zakonskih sprememb je veljala inkriminacija[4] hude žalitve, grdega ravnanja, izvajanja nasilja oziroma ogrožanja varnosti, ki je bila pogojena z zaznavanjem teh nasilnih ravnanj v javnosti ali v družini[5], s še dodatnimi pogoji, da so ta dejanja povzročila pri drugih ljudeh ogroženost, zgražanje ali prestrašenost, da sta ga izvršili vsaj dve osebi ali pa je prišlo do hudega ponižanja več ljudi ali do lažje telesne poškodbe. Ti pogoji so bilo pogosto težko dokazljivi. Nova dikcija[6] se nanaša na grdo ravnanje, pretepanje, drugačno boleče ali ponižujoče ravnanje v družinski skupnosti oziroma v drugi trajnejši življenjski skupnosti, dodatno tudi z grožnjami o neposrednem napadu na življenje ali telo družinskega člana, z njegovim preganjanjem iz skupnega bivališča ter z zalezovanjem, prisiljevanjem k delu ali opuščanja dela kot tudi s spravljanjem v podrejen položaj z nasilnim omejevanjem enakopravnosti nad družinskim članom. Inkriminirano je tudi dejanje, ko je izvedeno proti (nekdanjemu) družinskemu članu po tem, ko je ta skupnost že razpadla, dejanje pa je povezano s to skupnostjo.

4 PREDLOGI IN ZAKLJUČEK

Še pred dobrimi desetimi leti je bilo število starejših žrtev kaznivih dejanj v Sloveniji relativno nizko v primerjavi z nekaterimi drugimi evropskimi državami. Se pa delež starejših žrtev naglo viša – število se je podvojilo in dosega približno

4 To inkriminacijo je vseboval Kazenski zakonik RS ([KZ], 2004) v kaznivem dejanju Nasilništvo po 299. členu.

5 Dopolnilen opis, da je to dejanje možno izvršiti »v družini«, je bila sprememba vnesena v Kazenski zakonik RS šele leta 1999 (Zakon o spremembah in dopolnitvah Kazenskega zakonika RS [KZ-A], 1999). Pred tem letom je bilo v praksi skoraj nemogoče najti zakonsko podlago za ustrezen pregon nasilja v družinskem okolju kot eno izmed oblik nasilja v družini.

6 Kaznivo dejanje se imenuje nasilje v družini, 191. člen KZ-1 (2008).

8 % vseh oškodovancev. Čeprav je to še vedno manj kot na primer v Italiji in Franciji, zahteva naraščajoča populacija starejših posebno pozornost. S staranjem prebivalstva je namreč pričakovati, da bo število kaznivih dejanj nad starejšimi hitro naraščalo.

Premoženjska kriminaliteta prevladuje med prijavljenimi kaznivimi dejanji (brez upoštevanja starostnih skupin oškodovancev); njen delež se giblje med 65 in 75 %. Zato ne preseneča, da premoženjski delikti predstavljajo največje tveganje tudi za starejše (za ženske predvsem tisti z elementi nasilja), v njihovi starostni skupini namreč ti presegajo 80 % vseh kaznivih dejanj. Ostala kazniva dejanja – med starejšimi sicer manj pogosta, a v velikem porastu – zajemajo področje *človekovih pravic in svoboščin*, kjer je delež med starejšimi v primerjavi s celotno populacijo žrtev rahlo višji, področje *gospodarske kriminalitete*, ki je med starejšimi polovico nižji, in področje *krvnih deliktov*, kjer posebnih razlik glede na ostale starostne skupine ni.

Prvi in zelo pomemben korak boja proti kriminaliteti je preventiva. Ker poznamo rizična področja kriminalitete nad starejšimi, lahko preventivne programe usmerimo prav tja. Preventivni projekt policije *Ne pozabite na varnost* (http://www.policija.si/index.php/dravljani-in-policija/preventivni-projekti/1152-ne-pozabite-na-varnost-?lang=), ki teče že od leta 2005, se osredotoča ravno na tista vedenja starejših občanov na javnih mestih in doma, ki se tičejo varovanja premoženja. V zadnjem ponatisu informativne zloženke pa je bilo dodano tudi poglavje o varnosti v prometu. Projekt je dobro zasnovan, saj nazorno prikazuje ne/varna ravnanja, ob predstavitvi starejši spoznajo tudi vodje njihovega policijskega okoliša, kar olajša morebitne prihodnje stike. Projekt je med starejšimi zelo dobro sprejet (M. Breznik, osebna komunikacija, 5. junij 2013), a bi ga veljalo ob večjih finančnih in kadrovskih možnostih izvajati pogosteje.

Da je premoženjska kriminaliteta med starejšimi tako pogosta, najbrž razlog ni le v manjši psihofizični moči le teh, temveč tudi lažje prepoznavanje (in s tem prijava) tovrstnih kaznivih dejanj. Psihični dejavniki, na primer sram, občutki krivde in strah, zagotovo vplivajo na manjše število prijav ostalih omenjenih kaznivih dejanj, zato bi bilo koristno izvajati preventivne projekte s tega področja, ki bi vsebovali tudi ozaveščanje (laične) javnosti. Nasilje nad starejšimi je nedvomno eno izmed teh. Starejši kaznivih dejanj z elementi nasilja največkrat ne naznanijo pristojnim službam (policiji, centrom za socialno delo). V tem prispevku prikazana statistika predstavlja le zaznane in obravnavane primere, ocenjuje pa se, da je sivo polje neprijavljenih kaznivih dejanj veliko večje. Predvsem zaradi dejstva, da so starejši zaradi pešanja psihofizičnih moči z leti vedno bolj odvisni od svojih najbližjih, ki so obenem tudi povzročitelji nasilja. Bojijo se, da bi se s prijavo njihova situacija še poslabšala.

Na tej točki je nujno poudariti, da kronološka starost 65 let ali več ne pomeni, da je oseba a priori žrtev nasilja oziroma oškodovanka kaznivih dejanj. Upoštevati je treba potek staranja (aktivno staranje, prehranjevalne navade, fizična in psihična kondicija, bolezni, socialni stiki, obseg socialne mreže ipd.), ki lahko posameznika naredi še posebej ranljivega (naivnost, zanašanje na rutinske navade, bolezenska stanja, fizična šibkost, težave s spominom, občutki sramu, čustvena prizadetost ob zlorabi zaupanja, izvajanju nasilja nad njimi, izguba samozavesti, sugestibilnost

idr.). To pa ni pomemben podatek le za oblikovanje preventivnih ukrepov, temveč tudi za ustrezno ravnanje v situacijah, ko do kaznivega dejanja nad starejšimi pride. So vsi delavci institucij, ki pridejo v stik s starejšimi žrtvami, zadostno usposobljeni za vodenje razgovorov, nudenje pomoči in skupno iskanje rešitev? Policija že nekaj let uspešno izvaja specifična usposabljanja policistov *Multiplikatorji pri obravnavi nasilja v družini* (Miklič, Klančnik in Sladič, 2012). Prednost in učinkovitost projekta multiplikatorjev je skupno usposabljanje z nevladnimi organizacijami, centri za socialno delo in državnim tožilstvom ter spoznavanje problematike nasilja preko igre vlog in neposredne izmenjave dobrih praks. Pa vendar bi bilo treba področje izobraževanj in usposabljanj posebej osredotočiti na že omenjene specifike starejših, prepoznavanje nekaterih bolezenskih znakov v starosti ter poznavanje in razumevanje omejitev le teh. Spominski sistem starejših, na primer, je zagotovo podvržen procesom staranja, vendar pa ustrezno komunikacijo in sodelovanje ovirajo predvsem predsodki mlajših o nezanesljivosti spominskega priklica starejših in morebitna prisotnost neurodegenerativnih obolenj. Rezultati raziskav namreč kažejo, da so starejši sposobni opisati dogodke in prepoznati storilca z enako natančnostjo kot mlajši odrasli, a so pri tem manj prepričani vase in hitro jih drugi označijo kot nezanesljive priče (Giannini et al., 2013b).

Predstavljeni podatki kažejo na specifike pri obravnavi starostnikov – žrtev kriminalitete in upoštevajoč dejstvo, da so poleg svoje ranljivosti in šibkosti podvrženi tudi mnogim (somatskim in psihičnim) zdravstvenim težavam, nudijo izhodišča za bodoče raziskave in ustrezne preventivno kurativne intervencije. Podroben pregled potrebujejo tudi sorodna področja, na primer prekrški z elementi nasilja (zmerjanja, nespodobno vedenje, kričanje ipd.) in udeležba starejših v cestnem prometu. Pri tem se moramo zavedati tudi, da dostopni podatki o prijavljenih kaznivih dejanjih ne dajejo vpogleda v težave, s katerimi se starejši srečujejo, da do prijave sploh pride (neinformiranost, strah, sram, težja mobilnost ipd.) in če se to zgodi, kakšna je obravnava teh primerov in ali sta starejšim pri tem nudena kakršna koli podpora in pomoč.

Grdo ravnanje s starejšimi ne pomeni le fizičnega in psihičnega nasilja, temveč tudi odsotnost ustreznega ukrepanja (World Health Organization, 2002). Brez tega lahko zloraba starejših poslabša njihovo psihofizično zdravje in s tem skrajša življenjsko dobo. Vodi lahko do depresij in zlorabe alkohola (Lipar, 2012). Posledično je delo s starejšimi v obliki preventivnih projektov, ustreznega ravnanja v primeru, da do kaznivega dejanja pride, ter naknadne psihološke, socialne in medicinske pomoči velikega pomena.

LITERATURA

Brenk, K. (2004). Pšenica – najlepši cvet. V A. Ilc (ur.), *Zlata čebelica* (str. 166–174). Ljubljana: Mladinska knjiga.

Giannini, A. M., Baralla, F., Cordellieri, F., Sgalla, R., Nardi, B., Ruggerini, M. G. et al. (ur.). (2013a). *National survey reports: Data about aged victims of crime*. Pridobljeno na http://www.access-guidelines.eu/index.php/en/

Giannini, A. M., Guariglia, C., Baralla, F., Cordellieri, P., Boccia, M., Sgalla, R. et al. (ur.). (2013b). *Guidelines: About aged victims of crime*. Pridobljeno na http://www.access-guidelines.eu/index.php/en/

Kazenski zakonik Republike Slovenije [KZ]. (1994). *Uradni list RS*, (63/94).

Kazenski zakonik Republike Slovenije [KZ]. (2004). *Uradni list RS*, (95/04).

Kazenski zakonik [KZ-1]. (2008). *Uradni list RS*, (55/08).

Križman, I. (2010). Uvodne besede. V N. Vertot (ur.), *Starejše prebivalstvo v Sloveniji* (str. 3). Ljubljana: Statistični urad Republike Slovenije.

Kucler, M. (2002). Pravljica kot socialnopedagoška intervencija. *Socialna pedagogika*, *6*(1), 21–46.

Lipar, T. (2012). Zloraba starejših in alkohol. *Kakovostna starost*, *15*(1). Pridobljeno na http://www.inst-antonatrstenjaka.si/tisk/kakovostna-starost/clanek.html?ID=1189

Miklič, N., Klančnik, A. T. in Sladič, A. (2012). Multiplikatorji pri obravnavi nasilja v družini. *Varnost*, *60*(2), 46–49.

Petek-Šter, M. in Kersnik, J. (2004). Obravnava starostnika v družinski medicini. *Zdravstveni vestnik*, *73*(10), 767–771.

Policija. (2003). *Poročilo o delu policije za leto 2002*. Pridobljeno na http://www.policija.si/images/stories/Statistika/LetnaPorocila/PDF/lp2002.pdf

Policija. (2011). *Poročilo o delu policije za leto 2010*. Pridobljeno na http://www.policija.si/images/stories/Statistika/LetnaPorocila/PDF/LetnoPorocilo2010.pdf

Razpotnik, B. (2011). *Projekcije prebivalstva za Slovenijo, 2010–2060: končni podatki*. Pridobljeno na http://www.stat.si/novica_prikazi.aspx?id=3989

Vertot, N. (2009). *Prebivalstvo Slovenije danes in jutri, 2008–2060: projekcije prebivalstva EUROPOP2008 za Slovenijo*. Ljubljana: Statistični urad RS.

World Health Organization. (2002). *The Toronto declaration on the global prevention of elder abuse*. Pridobljeno na http://www.who.int/ageing/projects/elder_abuse/alc_toronto_declaration_en.pdf

Zakon o preprečevanju nasilja v družini. (2008). *Uradni list RS*, (16/08).

Zakon o spremembah in dopolnitvah Kazenskega zakonika [KZ-1B]. (2011). *Uradni list RS*, (91/11).

Zakon o spremembah in dopolnitvah Kazenskega zakonika RS [KZ-A]. (1999). *Uradni list RS*, (23/99).

Združeni narodi. (2001). *World population ageing: 1950–2050.* Pridobljeno na http://www.un.org/esa/population/publications/worldageing19502050/

O avtorjih:

Anton Toni Klančnik, mag., višji kriminalistični inšpektor specialist v Oddelku za mladoletniško kriminaliteto na Upravi kriminalistične policije Generalne policijske uprave. E-mail: toni.klancnik@policija.si

Mag. Tinkara Pavšič Mrevlje, asistentka za področje psihologije v varstvoslovju na Fakulteti za varnostne vede Univerze v Mariboru. E-mail: tinkara.pavsicmrevlje@fvv.uni-mb.si

VARSTVOSLOVJE,
let. 15
št. 3
str. 398–407

Kritičen razmislek o Reidovi zasliševalski tehniki

Igor Areh

Namen prispevka:

Avtor želi opozoriti na vzpostavitev kritične distance do zasliševalskih tehnik, ki prihajajo predvsem iz ZDA. Ker je forenzična psihologija v Sloveniji slabo razvita, se tuje znanje s tega področja pogosto prenaša v naše okolje prenagljeno in brez poglobljenih strokovnih analiz, uporabniki tako prenesenega znanja pa so pogosto zavedeni.

Ugotovitve:

Zaradi razlik v zakonodaji Slovenije in ZDA se prisilne zasliševalske tehnike, kot je na primer Reidova, pri nas ne uporabljajo. Kljub temu pa lahko opazimo, da kar nekaj znanja kriminalistov izhaja iz zasliševalskih priročnikov, za katere velja, da so predvsem zbirke subjektivnih izkušenj avtorjev. Ti svoje priročnike agresivno tržijo in jih zavajajoče predstavljajo kot znanstveno utemeljene tehnike. Resnica je drugačna: priročniki temeljijo na nepreverjenih domnevah in na dvomljivih raziskovalnih ugotovitvah, obenem pa avtorji izkazujejo očitno nepoznavanje osnovnih psiholoških in metodoloških znanj.

Praktična uporabnost:

V prispevku so predstavljene glavne kritike tipičnega predstavnika prisilnih zasliševalskih tehnik – Reidove tehnike. Raziskave zadnjih desetletij kažejo, da je uporaba takšnih tehnik neupravičena, saj znanost njihovih ugotovitev ne potrjuje, ali pa jim celo nasprotuje. Pri preiskovalcih, ki so pod vplivom priročnikov, se pojavljata napihovanje samozavesti in neučinkovitost prepoznavanja zavajanja, hkrati pa se poveča tveganje za pojav izsiljenega priznanja. Zaradi naštetega bi bilo dobro, da se v praksi preneha z uporabo priročnikov.

Izvirnost/pomembnost prispevka:

Današnja znanstvena dognanja in sodobni standardi varovanja človekovih pravic zavračajo uporabo Reidove tehnike, zato bi bilo treba tudi v slovenski preiskovalni praksi čim prej prevzeti in prilagoditi sodobne modele preiskovalnega intervjuvanja.

UDK: 159.9:340.6

Ključne besede: zasliševanje, Reidova tehnika, kritična analiza, psevdoznanost

A Critical Review of Reid's Interrogation Technique

Purpose:

In Slovenia, forensic psychology is not a developed science and that may be one of the main reasons why coercive interrogation techniques are recklessly driven into a criminal investigation practice. The purpose of the paper is to critically evaluate Reid's interrogation technique in the context of forensic psychology.

Findings:

Coercive interrogation techniques like Reid's are not used in Slovenia due to legislation limitations, which in comparison with the USA essentially restrict psychological manipulation with a suspect. Nevertheless an important share of interrogation knowledge of criminal investigators comes from commercial interrogation manuals, which are scientifically recognised as subjective and as common sense knowledge based on personal experiences of their authors. Interrogation manuals are misleadingly presented as scientific work, although they are founded on mostly unconfirmed assumptions and dubious research results, besides authors show obvious lack of elementary psychological and methodological knowledge.

Practical Implications:

The main critiques of Reid's technique, which is the most noticeable representative of coercive interrogation techniques, are presented. Research done in the past decades shows that there is no scientific justification for applying such an interrogation technique. Results published in peer reviewed papers do not confirm assumptions and in some instances even disapprove claims which are presented in manuals. Criminal investigators who are using such knowledge have tendency to be over-confident and inefficient in recognition of deception, there is also a higher probability to extract a false confession during their work. Because of that it would be appropriate to stop using interrogation manuals of that kind.

Originality/Value:

On the base of today's scientific knowledge available and considering contemporary human rights standards, the use of Reid's interrogation technique (or even parts of it) is not justified. In Slovenia such an interrogation practises they should be completely rejected and new contemporary interrogation models of investigative interview should be considered.

UDC: 159.9:340.6

Keywords: interrogation, Reid's technique, critical analyses, pseudoscience

1 UVOD

Praktično znanje in njegova teoretična podlaga, ki naj bi bila potrebna za izvedbo učinkovitih zaslišanj, sta zajeta v množici zasliševalskih priročnikov, ki redno izhajajo predvsem v ZDA. Kopico bolj znanih in uveljavljenih si lahko delno ogledamo preko spleta in seveda tudi kupimo. V vseh so omenjene bolj ali manj podobne zasliševalske tehnike, ki so jih razvili izkušeni kriminalisti in jih oglašujejo

kot znanstvena dela, kar pa zagotovo niso. Avtorji priročnikov namreč izhajajo iz osebnih poklicnih izkušenj in lastne intuicije, v kar pogosto slepo verjamejo in se opirajo na raziskovalne ugotovitve dvomljive ali pa nepreverljive kakovosti (Gudjonsson, 2003).

Najbolj uveljavljen in vpliven zasliševalski priročnik sta zasnovala pravnika Fred Inbau in John Reid na začetku 40. let prejšnjega stoletja. Tehnika, ki je v njem opisana in je prvič izšla v obliki priročnika leta 1962, je danes poznana kot Reidova tehnika. Čez leta se je nekoliko spreminjala, tako da so se do njene zadnje izdaje leta 2011 nakopičile opazne razlike v priporočilih za izvedbo zaslišanj. Tako kot druge podobne tehnike izhaja iz domneve, da se storilci kaznivih dejanj upirajo priznanju zaradi sramu, krivde ali pa strahu pred kaznijo. Da bi vseeno prišli do priznanja, morajo zasliševalci uporabiti različne oblike psihološke manipulacije, pri tem pa ne smejo uporabiti telesnega nasilja ali groženj (Inbau, Reid, Buckley in Jayne, 2011). Cilj tehnike je tako doseči priznanje osumljenca, do tega pa lahko pridemo z zlomom osumljenčevega odpora in zanikanja ter z večanjem osumljenčeve potrebe po priznanju. V zadnji izdaji priročnika avtorji uporabljajo nekoliko drugačno retoriko in namesto kritiziranega lova za priznanjem, govorijo o tem, da je cilj zaslišanja spoznanje resnice. Kaže pa, da gre pri tem zgolj za kozmetične popravke, saj je tehnika še vedno izoblikovana tako, da služi prvotnemu cilju: pridobiti priznanje osumljenca brez pravih prizadevanj za spoznanjem resnice. Avtorji Reidove tehnike priporočajo tudi uporabo zavajanja in prevare, seveda v meri, ki je dopustna po ameriški zvezni zakonodaji.

Omenil sem, da je Reidova tehnika najbolj vpliven zasliševalski pristop, velja pa, da je tudi najbolj uporabljan pristop v Severni Ameriki, prevladuje namreč tako v policiji kot tudi v vojski (Kassin, Appleby in Perillo, 2011). Zasliševalska procedura navadno poteka tako, da se osumljenca pripravi na zaslišanje, brez da bi mu očitali storitev kaznivega dejanja. Namen priprave je, med drugim, vzpostaviti odnos in občutek zaupanja (Inbau et al., 2011).

2 IZVEDBA ZASLIŠANJA

Proces zaslišanja poteka v devetih korakih in zaslišuje se le osumljence, za katere so preiskovalci prepričani, da so storilci kaznivega dejanja (Inbau et al., 2011). Prepričanost v krivdo osumljenca je zelo problematična, saj so lahko zaradi nje preiskovalci pristranski. Če obstajajo trdni materialni dokazi, potem je zaslišanje, ki ima namen pridobiti priznanje, odveč. Če trdnih materialnih dokazov ni, kako so lahko preiskovalci prepričani v krivdo osumljenega? Poleg tega so policisti nagnjeni k temu, da v pogovorih z osumljenimi iščejo in najdejo znake, ki potrjujejo njihova prepričanja o krivdi osumljene osebe, vpliv te pristranskosti pa se z leti dela celo povečuje (Meissner in Kassin, 2002).

Zaporedje korakov pri izvajanju Reidove tehnike je takšno (Inbau et al., 2011):

1. Neposredno pozitivno soočenje: zasliševalec osumljencu pove, da je prepričan, da je on storilec. Če zasliševalec nima dokazov, se pretvarja, da jih ima. Če

je osumljeni pasiven, je to dokaz, da skuša zavajati. Zasliševalec nadaljuje s prepričevanjem, da je za osumljenca najbolje, da razkrije resnico.

2. Razvoj teme: zasliševalec preide iz obtoževalnega v empatični odnos in skuša pridobiti zaupanje. Sugerira več tem pogovora, ki imajo namen zmanjšanja občutkov krivde (minimalizacija teže dejanja) in da osumljencu možnost, da najde opravičilo za dejanje. Izbira teme pogovora je odvisna od osebnosti osumljenca. Če gre za čustvenega osumljenca, zasliševalec spodbudi pojavljanje obrambnih mehanizmov, kot so racionalizacija, minimalizacija in projekcija, s čimer osumljenca spodbuja, da prizna. Tako osumljencu npr. povedo, da bi v takšnih okoliščinah vsak storil takšno kaznivo dejanje, kaznivo dejanje prikazujejo kot manj resno, osumljencu predstavijo moralno sprejemljiv razlog za storitev kaznivega dejanja, za dogodek obtožijo druge osebe, vzbujajo občutke ponosa s hvaljenjem in laskanjem, poudarjajo, da so obtožbe pretirane ipd. Pri razumskih storilcih, ki ne izkazujejo občutkov krivde ali sramu, poskušajo npr. s tem, da ga čim prej ujamejo na laži, predstavijo mu pozitivne posledice priznanja, prepričujejo osumljenega, da je nesmiselno zanikati resnico ipd.
3. Obvladovanje zanikanja: večina osumljencev se upira priznanju in ponavljajoča se zanikanja je treba čim prej odpraviti, sicer je težje priti do priznanja. Zasliševalec to doseže tako, da ob zanikanju takoj prekine osumljenca. Med zanikanjem krivih in nedolžnih oseb je razlika v besednem in nebesednem vedenju. Zanikanje nedolžnih je intenzivno in spontano, pojavita se lahko jeza in ogorčenje. Zanikanje krivih je oklevajoče, neprepričljivo in naučeno. Nedolžne osebe pogosto gledajo zasliševalce v oči in se na stolu nagnejo rahlo naprej v togi, a odločni drži.
4. Premagovanje ugovorov: nedolžni osumljenci uporabljajo zanikanje, krivi pa ugovarjajo.
5. Pritegovanje in vzdrževanje pozornosti: ko se pri osumljencu pojavi pasivnost, mora zasliševalec zmanjšati osebno razdaljo med njima in pritegne osumljenčevo pozornost. To doseže tako, da primakne stol, se osumljenega rahlo dotakne, ga pokliče po imenu in ga gleda v oči. Osumljenec se počuti premaganega, je depresiven, zato je uporaba takšnih zvijač nujna, če želimo pridobiti njegovo pozornost in ga narediti sugestibilnega.
6. Obvladovanje pasivnosti: zasliševalec pokaže razumevanje in sočustvovanje z osumljenim ter ga spodbuja k priznanju. Pri tem skuša spodbuditi pojav občutkov krivde, zato govori o trpljenju žrtve, ki je večje, kot bi bilo, ker osumljeni ne obžaluje in prizna.
7. Predstavitev vprašanja dveh možnosti: osumljencu predstavimo dve možnosti oziroma dva verjetna motiva, ki naj bi ga napeljala v kaznivo dejanje. Obe možnosti sta obremenjujoči, vendar je ena predstavljena tako, da ohranja dostojanstvo, druga pa osumljenca prikazuje kot izrazito negativnega. Predstavitev dveh možnosti je vrhunec zaslišanja, ki ima namen spodbuditi priznanje. Ko osumljeni izbere ugodnejšo možnost, s tem delno prizna in se obveže k popolnemu priznanju.
8. Spodbujanje osumljenca, da navede podrobnosti: ko osumljeni, z izbiro ene od možnosti, poda delno priznanje, ga navajamo, da bi podal celovito priznanje. Pri tem mora navesti podrobnosti in svoje motive.

9. Pretvorba ustnega priznanja v pisno priznanje: do zapisa priznanja mora priti čim prej po zaslišanju, ker lahko osumljeni priznanje umakne, ko se zave njegovih posledic. Priznanje pridobimo s prosto in čim bolj natančno pripovedjo osumljenca ali pa s strukturiranim intervjujem.

3 ANALIZA TEHNIKE

Reidova tehnika temelji na osebnih izkušnjah njenega avtorja in njegovih sodelavcev. Temelji torej na opazovanju in zdravorazumskem sklepanju in ne na ugotovitvah verodostojnih znanstvenih raziskav. Zaradi tega takšno zaslišanje, kot ga predlaga Reid s sodelavci, ne more biti to, kar oglašujejo avtorji – sredstvo za pridobivanje resnice (Gallini, 2010). Tehnika temelji na neupravičenem posploševanju in nepreverjenih domnevah, ki jih avtorji zavajajoče predstavljajo kot veljavne znanstvene ugotovitve, kar pa zagotovo niso (Gudjonsson, 2003).

V množici nepreverjenih domnev je ena izmed najbolj problematičnih predpostavk o razliki v izkazovanju anksioznosti med krivimi in nedolžnimi osumljenci. Inbau et al. (2011) menijo, da lahko pri krivih osumljencih opazimo višjo anksioznost, ker so storili kaznivo dejanje in jih je strah posledic razkritja. To je razumno predvidevati, vendar pa okoliščine zaslišanja niso tako preproste, kot jih prikazujejo avtorji priročnika. Lažne obtožbe nedolžne osebe, nenehna soočenja z očitki zasliševalcev in izkazovanje nezaupanja, nenehno prekinjanje osumljenega, ko želi pojasniti, da je nedolžen ipd., vse to ustvarja dodatno anksioznost pri nedolžnih osebah, ki si jo lahko zasliševalci razlagajo kot znake zavajanja. Avtorji priročnika menijo, da je glavna razlika v anksioznosti nedolžnih in krivih osumljencev v trajanju anksioznosti. V nasprotju s krivimi osumljenci naj bi pri nedolžnih osebah anksioznost v teku zaslišanja počasi ugašala, a za to trditev ni nikakršnih raziskovalnih dokazov (Gudjonsson, 2003). Po vztrajnem iskanju v bazah znanstvenih člankov jih tudi avtor tega prispevka ni našel. Problematična je tudi ena izmed osnovnih predpostavk tehnike, po kateri so nedolžni osumljenci bolj pripravljeni sodelovati s policijo kot krivi osumljenci, saj je Vrij (2005) v raziskavah ugotovil ravno nasprotno.

Avtorji tehnike priporočajo uporabo psihološke manipulacije, kot sta zavajanje in laganje, kar je sporno tako z vidika etike kot tudi z vidika slovenske zakonodaje. Težko je verjeti, da Reidova tehnika z uporabo takšnih psiholoških manipulativnih tehnik omogoča učinkovito preiskavo kaznivega dejanja. Celo pisec prvega britanskega zasliševalskega priročnika John Walkley, ki je sicer veljal za pristaša Reida in Inbaua, je dvomil o učinkovitosti tehnike prisilnega zasliševanja, saj je ugotovil, da osumljeni navadno priznajo, ko se vzpostavi neko minimalno razumevanje in zaupanje med osumljenim in zasliševalcem (Walkley, 1990). Pri uporabi Reidove tehnike pa je med zaslišanjem težko vzpostaviti ali vzdrževati tak odnos, saj zasliševalec nenehno prekinja zagovor osumljenega z namenom, da zlomi njegov odpor.

Za eno najbolj problematičnih zvijač, ki jih priporočajo avtorji Reidove tehnike, velja njihov nasvet, da v drugem koraku zaslišanja, pri razvoju teme, osumljenemu predstavimo moralno sprejemljiv razlog za storitev kaznivega dejanja. Če gre za

nedolžno osebo, ki je osumljena kaznivega dejanja in ji preiskovalec našteje kopico »neizpodbitnih« dokazov ter jo pred tem še odločno obtoži, potem je verjetno, da osumljeni v brezizhodni stiski prizna kaznivo dejanje. Bolje je namreč priznati in dobiti nižjo kazen, kot zanikati in zaradi navidezno trdnih obremenilnih dokazov dobiti hudo kazen (Gudjonsson, 2003).

Podobno velja za zvijačo, ki jo uporabljajo v sedmem koraku zaslišanja in jo imenujejo predstavitev dveh možnosti. Ta korak predstavlja vrhunec psihičnih pritiskov na osumljenca in zaradi njega ima tehnika upravičeno naziv prisilna zasliševalska tehnika. Osumljenca namreč prisilimo, da izbira med dvema negativnima posledicama domnevnega kaznivega vedenja, pri tem pa ni treba, da sta alternativi resnični. Ker je osumljeni potisnjen v prisilno izbiro, v stiski izbere tisto, ki je zanj ugodnejša oziroma manj obremenilna. Gudjonsson (2003) opozarja, da je to zelo nevarna tehnika, predvsem za osebe s podpovprečno inteligentnostjo, ki pa v policijski praksi predstavljajo pomemben delež osumljencev. Inbau et al. (2011) trdijo, da izkušeni zasliševalci dosežejo priznanje osumljencev v približno 80 % zaslišanj, med preostalimi 20 % osumljencev, ki ne priznajo, pa lahko pričakujemo majhen delež nedolžnih oseb. Menijo tudi, da v nobenem primeru uporabe prisilne izbire med dvema možnostma ne more priti do napačnega priznanja. Ravno v opisu sedmega koraka avtorji tehnike izkazujejo lahkomiselnost in nepoznavanje osnovnih psiholoških spoznanj, ki so ne samo v stroki, ampak tudi v širši javnosti znana že več desetletij (npr. raziskave Solomona Ascha s konformiranjem iz petdesetih let prejšnjega stoletja in standfordski jetniški poskus Philipa Zimbarda iz leta 1971).

V sklopu Reidove tehnike se uporabljata dve sporni orodji – minimalizacija in maksimalizacija, za kateri sta Kassin in McNall (1991) ugotovila, da sta tvegani zaradi verjetnosti pojava napačnih priznanj. Avtorji zasliševalske tehnike priporočajo uporabo maksimalizacije pri razumskih osumljencih, kar pomeni, da zasliševalec pretirava s težo obremenilnih dokazov in s težo kaznivega dejanja, iz česar lahko zaključimo, da priporočajo pridobitev priznanja z zastraševanjem. Nasprotno velja za tehniko minimalizacije, ki naj bi se uporabljala pri čustvenih osumljencih. Pri njej skuša zasliševalec z zvijačo pridobiti zaupanje osumljenca, nato pa si prizadeva priti do priznanja s pomočjo razumevanja, sočustvovanja, z ohranjanjem dostojanstva osumljenca, s pripisovanjem delne krivde žrtvi in z zmanjševanjem (minimalizacijo) teže posledic kaznivega dejanja. Avtorji sicer odsvetujejo zmanjševanje teže kazenskih, formalnih posledic kaznivega vedenja, a obenem priporočajo, da osumljencu sugeriramo misli, ki vodijo do občutka manjše resnosti kaznivega dejanja. Takšne sugestije pa povečujejo možnost pojava napačnega priznanja.

Da bi se zasliševalci lažje odločili, ali osumljeni govori resnico, jim avtorji tehnike ponujajo intervju z vedenjsko analizo[1], ki je po njihovem mnenju diagnostično orodje za prepoznavanje laži. Zasliševalci postavijo nekaj ključnih vprašanj, s katerimi preverijo vedenjske in besedne odzive osumljenih in tako ugotavljajo laganje osumljenca. Blair in Kooi (2004) sta primerjala vedenjske znake, ki naj bi bili pokazatelji zavajanja, z znaki, ki so se potrdili v raziskavah

1 *Behavior Analysis Interview (BAI).*

(npr. DePaulo et al., 2003), in ugotovila, da skoraj ni ujemanja med znanstvenimi ugotovitvami in trditvami avtorjev Reidove tehnike. Pomemben del omenjene tehnike, ki ga predstavlja intervju z vedenjsko analizo, tako nima znanstvene podlage, saj je z njim nemogoče razlikovati med iskrenimi in lažnivimi osebami (Kassin, Meissner in Norwick, 2005; Vrij, Mann in Fisher, 2006). Tako kot Reidova tehnika devetih korakov tudi intervju z vedenjsko analizo temelji na osebnih izkušnjah avtorjev tehnike in ne na rezultatih znanstvenih raziskav. Mimogrede, intervju z vedenjsko analizo temelji tudi na enaki nepotrjeni teoretični predpostavki kot poligrafiranje, da namreč zavajanje oz. laganje povzroča stresne odzive pri normalno socializiranih osebah. Raziskave kažejo, da ne obstajajo psihološki ali fiziološki znaki, ki bi bili pokazatelji laganja, kar pomeni, da sta obe tehniki znanstveno neverodostojni, saj je točnost razlikovanja krivih in nedolžnih oseb odvisna od pristranskosti ocenjevalcev, nizke veljavnosti in zanesljivosti tehnike ter od zmotno pozitivnih diagnoz (Leo, 2004). Pomenljivo je tudi to, da rezultati raziskav, na katere se sklicujejo Reid in njegovi sodelavci, niso bili nikoli javno objavljeni, tako da upravičeno dvomimo o njihovi verodostojnosti in njihovem obstoju (Leo, 2004).

Avtorji tehnike na lastni spletni strani zagotavljajo, da z njo ugotavljamo laž s 85 % točnostjo, vendar se pri dokazovanju verodostojnosti tega podatka sklicujejo na ugotovitve raziskave, ki ne zadošča niti najnižjim standardom izvedbe znanstvenih raziskav (Kassin, 2008). Raziskava (Horvath, Jayne in Buckley, 1994) je bila izvedena s pomanjkljivim eksperimentalnim nadzorom in je pristranska v korist točnosti Reidove tehnike. Neodvisne laboratorijske raziskave kažejo namreč bistveno nižjo točnost tehnike in v večini njih so ugotovili, da je z Reidovo tehniko nemogoče ločiti lažnive in iskrene osebe (Kassin, 2008). Vrij (2008) je v metaštudiji, ki je zajela 79 raziskav, ugotovil, da je pri laikih povprečna točnost ugotavljanja laži 54 %. Podobno je pregledal tudi študije, v katerih so ugotavljali točnost preiskovalcev, in v 31 raziskavah ugotovil povprečno točnost, ki znaša 56 %. To pomeni, da so preiskovalci pri ugotavljanju laži malenkost bolj točni kot laiki, očitno pa je eksperimentalno ugotovljena točnost daleč od 85 %, kot je zapisano na spletni strani avtorjev tehnike.

Uporaba in urjenje v izvajanju Reidove tehnike vodita k napihovanju samozavesti (Kassin in Fong, 1999) in k povečevanju pristranskosti preiskovalcev (Meissner in Kassin, 2002). Oboje predstavlja resno težavo za učinkovito izvajanje preiskav, saj so lahko kriminalisti pri ugotavljanju laganja zaradi tega celo manj točni kot laiki, čeprav so tudi slednji brez urjenja, tako kot policisti, nagnjeni k temu, da osumljence vidijo kot storilce, čeprav ni dokazov, ki bi to potrjevali (Kassin et al., 2005). Vzrok za napihovanje samozavesti in za neučinkovito ugotavljanje zavajanja, lahko najdemo v psevdoznanstvenih trditvah, ki zavajajo tiste, ki naj bi zavajanje ugotavljali.

Od 40. let prejšnjega stoletja so se zasliševalske tehnike zelo spremenile in danes zagotavljajo bistveno boljše varovanje osnovnih človekovih pravic, hkrati pa omogočajo bolj (etično) učinkovito opravljanje preiskovalnega dela. Vsaj 50 let stara Reidova tehnika, ki temelji na vzpostavljanju psihološkega nadzora nad osumljenim, na prevari in zvijači ter se oglašuje kot znanstvena, je bila nekoč dobro nadomestilo za predhodne zasliševalske prakse, ki so dovoljevale določene

oblike telesnega zastraševanja (Gallini, 2010; Kassin, 2008). Današnje raziskovalne ugotovitve v glavnem ne podpirajo trditev avtorjev Reidove tehnike ali pa jih celo zavračajo. Zato je uporaba Reidove tehnike v celoti, ali po delih, strokovno neupravičena in celo nedopustna, če upoštevamo tveganje za pojav napačnih priznanj, ki je preprosto previsoko za današnje standarde varovanja človekovih pravic.

Sodobni načini izvajanja zaslišanj stremijo k pridobivanju operativno uporabnih informacij in ne več k pridobivanju priznanj, zato se vedno pogosteje uporablja izraz preiskovalni intervju in ne več zaslišanje (Oxburgh in Ost, 2011). Tako je poglavitni cilj sodobnih zaslišanj ugotoviti kaj in kako se je nekaj zgodilo, manj pa je pomembno kdo, kaj in kje je storil kaznivo dejanje (Milne in Bull, 2006). Kaže, da bo britanski preiskovalni model intervjuvanja PEACE[2] v naslednjih letih najverjetneje povozil Reidov zasliševalski model v Severni Ameriki in Kanadi. Mnogi pa opozarjajo, da prehod iz prisilnega zasliševanja v preiskovalno intervjuvanje ne bo lahek, saj avtorji priročnikov o prisilnih tehnikah agresivno oglašujejo in tržijo svoje izdelke (Snook, Stinson, Tedeschini in House, 2010), kar še posebno velja za manj kritična družbena okolja z manj razvito znanostjo in nižjo družbeno ozaveščenostjo.

4 ZAKLJUČEK

Medtem ko je danes Reidova tehnika zavrnjena s strani znanosti in označena kot skupek etično spornih zdravorazumskih ugotovitev, ki so brez znanstvene osnove, v praksi še vedno ostaja kot vplivno zasliševalsko orodje. Slovenska zakonodaja v glavnem preprečuje njeno uporabo med zaslišanji, kljub temu pa je predvsem med informativnimi razgovori dovolj manevrskega prostora za uporabo nekaterih njenih komponent. Eden od razlogov za trdoživost omenjene tehnike prisilnega zaslišanja je gotovo v njenem agresivnem trženju, ki je učinkovito predvsem v državah z manj razvitim znanstvenim okoljem. Reidova tehnika je odigrala pomembno in koristno vlogo v času po drugi svetovni vojni, pred približno 20 leti pa se je začela era britanskih preiskovalnih intervjujev in skrajni čas je, da tudi v Sloveniji pustimo preteklost in ujamemo sedanjost.

LITERATURA

Blair, J. P. in Kooi, B. (2004). The gap between training and research in the detection of deception. *International Journal of Police Science and Management*, *6*(2), 77–83.

DePaulo, B. M., Lindsay, J. J., Malone, B. E., Muhlenbruck, L., Charlton, K. in Cooper, H. (2003). Cues to deception. *Psychological Bulletin*, *129*(1), 74–118.

2 *Kratica PEACE je okrajšava za angleške izraze Preparation and Planning (P), Engage and Explain (E), Account, Clarification and Challenge (A), Closure (C) in Evaluation (E).*

Gallini, B. R. (2010). Police 'science' in the interrogation room: Seventy years of pseudo-psychological interrogation methods to obtain inadmissible confessions. *Hastings Law Journal*, *61*(3), 529–580.

Gudjonsson, G. H. (2003). *The psychology of interrogations and confessions: A handbook*. Chichester: John Wiley & Sons.

Horvath, F., Jayne, B. in Buckley, J. (1994). Differentiation of truthful and deceptive criminal suspects in behavior analysis interviews. *Journal of Forensic Sciences*, *39*(3), 793–807.

Inbau, F. E., Reid, J. E., Buckley, J. P. in Jayne, B. C. (2011). *Criminal interrogation and confessions* (5th ed.). Gaithersberg: Jones & Bartlett.

Kassin, S. M. (2008). The psychology of confesions. *Annual Review of Law and Social Science*, *4*, 193–217.

Kassin, S. M. in Fong, C. T. (1999). »I'm innocent!«: Effects of training on judgments of truth and deception in the interrogation room. *Law and Human Behavior*, *23*(5), 499–516.

Kassin, S. M. in McNall, K. (1991). Police interrogations and confessions. *Law and Human Behavior*, *15*(3), 233–251.

Kassin, S. M., Appleby, S. C. in Perillo, J. T. (2011). Interviewing suspects: Practice, science, and future directions. *Legal and Criminological Psychology*, *15*(1), 39–55.

Kassin, S. M., Meissner, C. A. in Norwick, R. J. (2005). »I'd know a false confession if I saw one«: A comparative study of college students and police investigators. *Law and Human Behavior, 29*(2), 211–228.

Leo, R. A. (2004). The third degree and the origins of psychological interrogation in the United States. V G. D. Lassiter (ur.), *Interrogations, confessions, and entrapment*, (str. 37–84). New York: Kluwer Academic/Plenum.

Meissner, C. A. in Kassin, S. M. (2002). »He's guilty!« Investigator bias in judgments of truth and deception. *Law and Human Behavior*, *26*(5), 469–480.

Milne, R. in Bull, R. (2006). Interviewing victims of crime, including children and people with intellectual difficulties. V M. R. Kebbell in G. M. Davies (ur.), *Practical psychology for forensic investigations* (str. 7–24). Chichester: Wiley.

Oxburgh, G. in Ost, J. (2011). The use and efficacy of empathy in police interviews with suspects of sexual offences. *Journal of Investigative Psychology and Offender Profiling*, *8*(2), 178–188.

Snook, B., Stinson, M., Tedeschini, J. in House, J. C. (2010). Reforming investigative interviewing in Canada. *Canadian Journal of Criminology and Criminal Justice*, *52*(2), 215–229.

Vrij, A. (2005). Cooperation of liars and truth tellers. *Applied Cognitive Psychology*, *19*(1), 39–50.

Vrij, A. (2008). *Detecting lies and deceit: Pitfalls and opportunities*. Chichester: John Wiley & Sons.

Vrij, A., Mann, S. in Fisher, R. P. (2006). An empirical test of the Behaviour Analysis Interview. *Law and Human Behavior*, *30*(3), 329–345.

Walkley, J. (1990). *Police interrogation: A handbook for investigators*. London: Police Review Publishing.

O avtorju:

Dr. Igor Areh je docent za forenzično psihologijo na Fakulteti za varnostne vede Univerze v Mariboru. Do sedaj je objavil več kot 70 znanstvenih in strokovnih člankov ter drugih prispevkov, predvsem s področja verodostojnosti pričanja očividcev kaznivih dejanj. V praksi deluje kot sodni izvedenec s področja psihologije pričanja in kot svetovalec pri preiskovanju kaznivih dejanj. E-mail: igor.areh@fvv.uni-mb.si

Nacionalna kriminološka konferenca Kriminaliteta, nered in družbeno nadzorstvo v času ekonomske krize – kriminološke refleksije

17. aprila 2013 so člani Katedre za kriminologijo na Fakulteti za varnostne vede Univerze v Mariboru organizirali nacionalno kriminološko konferenco *Kriminaliteta, nered in družbeno nadzorstvo v času ekonomske krize – kriminološke refleksije*. Namen konference je bil zbrati prispevke, ki obravnavajo tematiko ekonomske krize v Evropi in Sloveniji ter njen vpliv na kriminaliteto, nered in družbeno nadzorstvo. Na konferenci je sodelovalo 18 predavateljev, ki so predstavili svoje poglede na dogajanje v Sloveniji v času krize kapitalističnega družbeno-ekonomskega sistema, sprememb demokratičnega političnega sistema in (pravne) države.

Uvodno predstavitev na konferenci je imela Alenka Šelih, ki je predstavila različne teoretične poglede na vpliv družbenih sprememb na razvoj kriminalitete. Ugotavlja, da je evropski prostor v 20. stoletju doživel štiri faze preobrazbe: prva so bili procesi demokratizacije po prvi svetovni vojni, druga procesi demokratizacije po drugi svetovni vojni in tretja procesi demokratizacije v 70. letih, s padcem avtoritarnih sistemov v Evropi (Španija, Portugalska, Grčija). Najobsežnejšo spremembo pa je predstavljal padec socializma in družbenopolitične spremembe v vzhodno- in srednjeevropskih državah. Pri tem je Alenka Šelih poudarila, da prehod iz socializma v kapitalizem ni samo sprememba sistema, temveč sprememba v produkcijskih razmerjih. Omenjene prehode, zlasti zadnjega, je avtorica pojasnila skozi različne kriminološke in sociološke teorije zahodnih in srednje- in vzhodnoevropskih avtorjev. Pogled, ki ga zagovarja avtorica, vključuje multikavzalni model razlage, ki ga poimenuje pristop šoka. Obsežne spremembe, ki so se zgodile, so prinesle šok za posameznika in družbo.

Zoran Kanduč se je dotaknil razvoja družb po drugi svetovni vojni, pri tem pa se je osredotočil na vprašanja razrednega boja. Pregled je začel s keynezianskim modelom in ga nadaljeval v obdobje *neoliberalizma*. Slednji je predstavljal kontrarevolucijo in vrnitev moči akterjem, ki so jo v 60. letih pričeli izgubljati. Takšna kontrarevolucija je v Sloveniji sovpadala z odcepitvijo in tranzicijo, ki je prinesla privatizacijo nekdanjega skupnega premoženja (zločin vseh zločinov), izkoriščanje in zatiranje. Kanduč je pri tem opozoril, da je prišlo (oziroma prihaja) do bizarne solidarnosti podrejenih do bogatašev. Ta je posledica ekonomske propagande, ki vključuje čaščenje bogatašev. Dobrodelnost slednjih, ki celi ravno

rane, ki jih povzročajo. Bogataši pa imajo na svoji strani tudi državo – še natančneje pravno državo, kjer je buržoazno pravo vir problema in ne njegova rešitev.

Benjamin Flander je opozoril na značilnosti in težave postmoderne družbe in na dejstvo, da je refleksija v družbi postmodernega kapitalizma v zatonu. Za postmoderne družbe je značilno delovanje dveh dejavnikov t. i. »dveh glavnih operaterjev«: velike pripovedi razsvetljenstva o emancipaciji in velike pripovedi neoliberalizma o učinkovitosti, funkcionalnosti in operativnosti. Znanstvena vednost deluje vedno bolj pod vplivom tržno-ekonomskih načel, ob tem pa na površje prihaja tudi kriza univerze. Tudi kriminološka vednost se dandanes legitimira s sklicevanjem na učinkovitost in uporabljivost. Za kriminološko vedo Flander zaključuje, da je mogoče identificirati tri središčne smeri: »demokratska kriminologija«, ki se nanaša na demokracijo, pravno državo, človekove pravice ipd.; »kriminološka doktrina zakona in reda«, ki vključuje neoliberalne/neokonservativne mutacije »demokratske kriminologije« – red, zakon, nadzor, varnost, kazen ipd. ter »znanost o kriminaliteti«, ki obsega aplikacijo naravoslovnih metod; pozitivistično-tehnicistične pristope. Pregled trenutnega stanja Flander zaključi z mislijo, da je »v t. i. demokratičnih državah kriminološka 'doktrina zakona in reda' bergla kriminalitetne in kaznovalne politike, znanstveno neoporečen štrik ji drži 'crime science', 'demokratska kriminologija' pa je bolj kot ne 'kalimero' kriminološkega diskurza«.

Gorazd Meško je predstavil prispevek o legitimnosti institucij formalnega družbenega nadzorstva v času družbenoekonomske krize v Sloveniji. Poudaril je, da je preučevanje legitimnosti policijske dejavnosti in pravosodnih institucij ključno na področju sodobne kriminologije in študij kazenskega pravosodja. Zaupanje v organe družbenega nadzorstva, predvsem v policijo, je še posebej izrazito in pomembno v kriznih razmerah, negotovosti, ekonomskih pretresih in posledičnih, negativnih vplivih na vsa druga področja (socialo, izobraževanje, kulturo). Legitimnost vključuje vprašanja o legitimnosti (sociološke in psihološke perspektive), vprašanja postopkovne pravičnosti, distributivne pravičnosti (enaka obravnava ljudi) in moralne kredibilnosti nosilcev oblasti. Pregled študij o legitimnosti v Sloveniji in svetu je pokazal, da je policija med organi formalnega družbenega nadzorstva najbolj pogosto proučevana institucija, pri čemer je najbolj v ospredju legitimnost policijskega dela. Meško ugotavlja, da je pomembno, da policija v okviru policijskega dela v skupnosti še naprej skrbi za ustvarjanje občutka varnosti, vendar za to ni edina odgovorna. Predstavil je tudi ugotovitve primerjalne študije o legitimnosti, ki je še v teku, in vključuje Rusijo, Romunijo in Slovenijo. Prve ugotovitve kažejo, da je cinizem do pravnega sistema in norm dokaj nizek, vendar pa so legitimnost, postopkovna in distributivna pravičnost, moralna kredibilnost ter podrejanje zakonom zaznani negativno – najslabše v Romuniji, sledi Rusija in Slovenija.

V drugi sekciji so bili predstavljeni trije prispevki, in sicer o kazenskopravnem odzivanju na gospodarsko kriminaliteto, o finančni krizi v povezavi s finančno kriminaliteto ter o vplivu ekonomske krize na gibanje ekološke kriminalitete.

Matjaž Jager se je v svojem prispevku osredotočil na kontradiktorno vlogo države na področju gospodarske kriminalitete. Predstavil je notranja protislovja kazenskopravnega odzivanja na gospodarsko kriminaliteto, na primer: država

ima permanentno dolžnost za krepitev gospodarstva, hkrati pa je pravna država regulator mehanizmov gospodarskega poslovanja – tako torej ovira in hkrati odmika ovire gospodarskim subjektom. Izpostavil je očitno imunost storilcev pred kazenskopravno intervencijo, pri čemer država daje vtis, kot da ne ve, kako se lotiti tega področja na način, da bo »volk sit in koza cela«. Po avtorjevem mnenju je to vprašanje politične volje. Opozoril je tudi na omejenost preventivnih aktivnosti na področju gospodarske kriminalitete, ki ostaja v pristojnosti Ministrstva za notranje zadeve, čeprav vsekakor sodi tudi na področje drugih ministrstev (Ministrstvo za gospodarski razvoj in tehnologijo, Ministrstvo za finance, Ministrstvo za izobraževanje, znanost in šport itd.).

Bojan Dobovšek in Boštjan Slak sta pripravila prispevek o povezavi med finančno kriminaliteto in finančno krizo, ki je po njunem mnenju vzročna – finančna kriza je posledica finančne kriminalitete in ne neke vrste katastrofa, ki se nam je »zgodila«, kot jo populistično zaznavamo, tudi po zaslugi poročanja medijev. Ravnanje nekaterih ekonomskih sektorjev, med katerimi izpostavita finančni sektor (omenjena sta tudi energetski in gradbeni sektor), avtorja označujeta kot finančno kriminaliteto, ki jo omogoča in varuje sistemska korupcija. Opozorita tudi na zmanjšan ali celo popolnoma odsoten nadzor nad institucijami, ki upravljajo velike vrednosti. Pomanjkljiv oziroma odsoten nadzor omogoča nekontrolirano, tvegano in tudi kriminalno vedenje teh institucij. Avtorja izmed možnih ukrepov za izboljšanje stanja poudarita pomen preventive, med represivnimi ukrepi pa predlagata razčlenitev kaznivih dejanj s področja finančne kriminalitete na posamezna manjša kazniva dejanja, kar omogoča lažje preiskovanje in dokazovanje, opozorita še na potrebo po večji specializaciji preiskovalcev in na pomen povračila škode v okviru kazenskih sankcij.

Katja Eman je v svojem prispevku predstavila ugotovitve o vplivu gospodarske krize na gibanje ekološke kriminalitete v Sloveniji. Najprej je pojasnila, da je primarni razlog za storitev ekološke kriminalitete dobiček – bodisi v obliki izogibanja stroškov ali preko prodaje naravnih virov. Na podlagi pregleda kriminalitetne statistike avtorica zaključi, da ni mogoče govoriti o izstopajočem porastu posameznih kaznivih dejanj zoper okolje, prostor in naravne dobrine na splošno, število tovrstnih kaznivih dejanj namreč iz leta v leto niha. Po opravljenih pogovorih s predstavniki institucij formalnega družbenega nadzorstva avtorica ugotovi, da slednji vendarle zaznavajo porast nezakonitega lova, ribolova, nezakonitega odlaganja odpadkov in tatvin lesa. Ugotovljen je torej dvojni vpliv ekonomske krize na gibanje ekološke kriminalitete v Sloveniji – tako pozitiven kot negativen. V pozitivnem smislu je propad gradbenih podjetij in s tem zapiranje gradbišč pripeljalo do zmanjšanja nezakonitega odlaganja gradbenih odpadkov, zmanjševanje proizvodnih kapacitet podjetij pa je prav tako vodilo v zmanjšanje izpustov v naravno okolje. S tega vidika torej ekološka kriminaliteta upada. Po drugi strani pa manjši podjetniki še vedno poskušajo znižati stroške obratovanja tako, da se poskušajo znebiti odpadkov na nezakonit način. Poleg tega se, zaradi neurejenosti odlagališč odpadkov, povečujejo tokovi odpadkov znotraj države in čezmejne pošiljke odpadkov. S tega vidika torej lahko govorimo o porastu ekološke kriminalitete.

V tretji sekciji so avtorji prispevkov razpravo o kriminaliteti, neredu in družbenem nadzorstvu prenesli na delo in učinkovitost organov pregona in nadzora, in sicer državno tožilstvo, policijo in zavode za prestajanje kazni zapora.

Tanja Ahčan je izpostavila pomembnost vloge državnih regulatorjev in nadzornikov pri preprečevanju in odkrivanju finančne kriminalitete, saj je finančna kriza razkrila številna odklonska ravnanja udeležencev globalnih finančnih trgov ter odprla množico vprašanj glede regulacije, nadzora in uspešnosti kazenskega pregona odgovornih posameznikov. Nadzor in regulacija finančnih trgov v Republiki Sloveniji temeljita na pravilih evropske zakonodaje in dobre prakse, ki jo oblikujejo mednarodne finančne institucije. Pri tem je avtorica opozorila, da šibkost regulacije in nadzora nista problem neustrezne strokovnosti in usposobljenosti posameznega nacionalnega regulatorja, ampak gre pri kaznivih ravnanjih udeležencev finančnih trgov za kriminaliteto belega ovratnika, vodilnih oseb finančnih lobijev. To pomeni, da gre pri neaktivnostih državnih nadzornikov bolj za vprašanje političnih in tudi kriminalnopolitičnih odločitev, zaradi česar je potrebno poseči po premišljenih reformah, predvsem v smislu preventivne vloge na področju finančne kriminalitete ter celovito obravnavanje delovanja in ukrepanje regulatorjev; ekonomskemu vidiku je potrebno dodati tudi pravni in politični vidik.

David Smolej je v predstavitvi prispevka z naslovom Učinkovitost policistov pri preiskovanju kaznivih dejanj v času ekonomske krize opozoril, da je ekonomska kriza do določene meje prizadela tudi slovensko policijo, predvsem na področju človeških virov, ki se ob upokojevanju policistov ne nadomeščajo. Avtor je izpostavil pomembnost odkrivanja in preiskovanja kaznivih dejanj (ki so v času ekonomske krize v porastu) kot ene izmed temeljnih nalog policije, kjer je pomembno, da policija postopa strokovno, zakonito in tudi učinkovito. Predstavil je rezultate analize ugotavljanja učinkovitosti dela policije, kjer je uporabil primerjavo statističnih podatkov policije s tožilstvom in sodišči v obdobju med 2007 in 2011. Ugotovil je, da se je v proučevanem obdobju odstotek preiskanih kaznivih dejanj s strani policije povečal za 3,2 % in odstotek podanih obtožb s strani tožilcev zmanjšal za 0,4 %. Avtor je v zaključku opozoril, da policijska statistika ne more biti (edino) merilo učinkovitosti in uspešnosti dela policije. Ker mora policija v času ekonomske krize delovati in izvajati svoje naloge ter ukrepe z manjšimi finančnimi in kadrovskimi viri, so se na to že odzvali odgovorni in spremenili zakonodajo, poenostavili postopke in zmanjšali administrativne ovire.

Lana Cvikl, Ana Oštir in Matjaž Ambrož so se dotaknili problematike slovenskega zaporskega prava z vidika pravil Evropskega sodišča za človekove pravice. Opozorili so na vedno iste izgovore vlad o proračunskih omejitvah, še posebej v času ekonomske krize, kadar so soočene z očitkom, da niso poskrbele za ustrezne bivalne pogoje v zaporih. Avtorji so poudarili, da nobene proračunske omejitve ne bi smele biti izgovor za zaporske razmere, ki kršijo elementarno človekovo dostojanstvo in pravice. Predstavili so analizo judikature Evropskega sodišča za človekove pravice z vidika položaja zaprtih oseb v Sloveniji in identificirali kritična mesta v slovenskem zaporskem pravu in praksi, ki bi lahko bila po primerih Mandić in Jović proti Sloveniji podlaga za nadaljnje obsodbe Slovenije pred tem sodiščem. Med najbolj relevantna in z vidika kršitve človekovih

pravic problematična področja spada 3. člen Konvencije, ki obravnava prepoved mučenja, nečloveškega in ponižujočega ravnanja. Čedalje bolj pomembne pravice so tudi pravica do zasebnega in družinskega življenja (8. člen), ki se uresničuje tudi z dovolj širokimi možnostmi korespondence in obiskov, nadalje svoboda izražanja (10. člen), ki vključuje tudi pravico do stikov z mediji in javno izražanje kritik zaporskega osebja, pravica do izpovedovanja vere ali prepričanja (9. člen) in ne nazadnje pravica skleniti zakonsko zvezo in osnovati družino (12. člen), vključno s pravico postati biološki starš. Avtorji so opozorili na pomembnost upoštevanja določil Konvencije ter spoštovanja človekovih pravic v slovenskih zaporih, ker je samo to rešitev pred novimi obsodbami Slovenije pred Evropskim sodiščem za človekove pravice.

Tema zadnje sekcije nacionalne kriminološke konference je bila kibernetska kriminaliteta.

Finančna kriza, mladi in kibernetska kriminaliteta je bil naslov prvega prispevka, avtorja Igorja Bernika. Opozoril je, da je v času finančne krize zaposlitev težko obdržati, še težje pa dobiti, pri čemer so mladi najbolj izpostavljena skupina, ker oboroženi z obilico znanja zaključujejo izobraževanja, na trgu dela pa zanje ni ustrezne perspektive. V iskanju možnosti in priložnosti za zaslužek se prav ti mladi hitro znajdejo v situacijah, ko postanejo žrtve kibernetskih prevar, saj s pridobljenim znanjem in spretnostmi veliko časa preživijo v kibernetskem prostoru, ne zavedajo pa se tveganj, ki sta jih razvoj in tehnologija prinesla. Znan je pojav zaposlitve mladih v organizacijah, ki se ukvarjajo s kibernetsko kriminaliteto (npr. spreminjanje kod v programih), pa čeprav o tem največkrat popolnoma nič ne vedo. Gre za primere hierarhično organiziranih kriminalnih skupin, ki so zelo pogoste v Romuniji, znani pa so tudi že primeri mladih iz Slovenije, ki so bili del takih združb (npr. primer mariborskih študentov računalništva in hekersko-kriminalne združbe Mariposa). Avtor je poudaril, da kibernetska kriminaliteta ni tehnično vprašanje, ampak je povezana predvsem s kulturo uporabnikov, zato je še toliko bolj pomembno izobraževanje in ozaveščanje ranljivih skupin, še posebej mladih.

Aleksandar Ilievski je predstavil svoj pogled na vpliv gospodarske krize na kibernetsko kriminaliteto, ki se je, glede na dostopne podatke, v obdobju krize drastično povečala. Vpliv krize na kibernetsko kriminaliteto je avtor proučil z vidika teorije rutinskih aktivnosti, ki (prenesena v polje kibernetske kriminalitete) predpostavlja, da je verjetnost napada v kibernetskem prostoru odvisna od motiviranosti storilca, ranljivosti žrtev in učinkovitosti kontrole nad tem prostorom. Avtor ugotavlja povečan motiv pri kibernetskih storilcih v času krize (visoka tehnična izobraženost storilcev in njihova brezposelnost), obenem pa večjo ranljivost uporabnikov spletnih storitev (številne spletne goljufije, prevare, okužbe s škodljivimi nezaželenimi programi). Specifika vizualnega prostora, mednarodna razsežnost in kreativni napredek kibernetske kriminalitete pa predstavljajo velik izziv za organe pregona, ki se v času krize za nameček soočajo še s pomanjkanjem finančnih sredstev za opravljanje svojega dela. Avtor poudari velik pomen ozaveščenosti uporabnikov o pojavnih oblikah in potrebi po ustrezni zaščiti, kar lahko pripomore k zmanjševanju ranljivosti in škode, ki jo utegnejo utrpeti uporabniki.

Prispevek Kaje Prislan se je nanašal na dinamiko protestnih gibanj v kontekstu tehnologije in spletnih storitev. Prislan ugotavlja, da so se množična gibanja v zadnjem desetletju zaradi vpliva sodobne tehnologije – zlasti interneta – spremenila v strukturi, organizaciji, komunikaciji in razširjenosti. Pri organizaciji aktivističnih organizacij in kolektivnih akcij aktivisti najpogosteje izkoriščajo spletna socialna omrežja. Uporabljajo jih za širjenje idej, sporočil, pozive, rekrutiranje podpornikov itd. Avtorica je predstavila tudi ugotovitve raziskave o vplivu spletnih socialnih omrežij na dinamiko protestov v Sloveniji. Zaključuje, da je pomembno vlogo odigralo omrežje Facebook, predvsem pri širjenju protestnih sporočil in pri pozivanju ljudi k aktivni udeležbi. Prav tako se je uporabljal za organizacijo aktivnih podpornikov, med splošno populacijo pa kot vir informiranja o preteklih in prihodnjih dogodkih.

Med glavnimi sporočili konference so organizatorji izpostavili potrebo po uravnoteženosti preventive in represije. Udeleženci konference so izpostavili problem, da so v veliki meri obsojeni manjši kriminalci, t. i. kurji tatovi, medtem ko je obsodb s področja velikega kriminala malo. Po besedah Alenke Šelih je razlog v tem, da je odkrivanje t. i. 'majhnega kriminala' najlažje, 'večji kriminal' pa je težje odkrivati in procesirati. Dodala je še, da organi pregona za odkrivanje primerov velikega kriminala vse do pred kratkim niso bili ustrezno usposobljeni. Prav tako je Zoran Kanduč še dodatno opozoril, da se povzročitelje primerov 'velikega kriminala' v medijih in družbi še vedno obravnava z vsemi častmi. Napočil je čas, da zopet obvelja osnovno načelo enakosti pred zakonom, zapisano v slovenski ustavi, temeljni listini človekovih pravic in svoboščin ter ne nazadnje tudi dolžnosti.

Maja Jere, Aleš Bučar-Ručman, Katja Eman

Splošno	Varstvoslovje je znanstvena revija, ki spodbuja interdisciplinarno razpravo in izmenjavo ugotovitev znanstvenega proučevanja varnosti, njenega zagotavljanja in ohranjanja ter tako prispeva k razumevanju delovanja skupnosti, organizacij in posameznikov, ki sodelujejo pri zagotavljanju varnosti.
Naslov prispevka	Naslov: velikost črk 14, **krepko**
Avtor(ji) prispevka	Naslovu sledi navedba avtorja (avtorjev) – samo ime in priimek. Ostali podatki: naziv, funkcija ter ustanove, kjer deluje(jo) se zapiše na koncu prispevka pod rubriko '**O avtorju(ih):**' (velikost črk 12).
Povzetek	Prispevku mora biti dodan povzetek. Povzetek naj vsebuje do 250 besed. Napisan naj bo jedrnato in jasno. Odraža naj le tisto, kar je obravnavano v prispevku. Napisan naj bo na naslednji način (namen, metodologija, ugotovitve in izvirnost so obvezne postavke; ostale postavke se lahko izpustijo, v kolikor gre za teoretični prispevek): **Namen prispevka:** Kateri so razlogi za pisanje prispevka in kateri so cilji raziskave? **Metode:** Kako so cilji doseženi? Katera je glavna metoda uporabljena za raziskavo? Kakšen je pristop in kakšno je teoretično področje prispevka? **Ugotovitve:** Katere so ugotovitve raziskave/prispevka? **Omejitve/uporabnost raziskave:** V kolikor je v prispevek vključena raziskava, mora ta del vsebovati predloge za nadaljnje raziskovanje in identifikacijo morebitnih omejitev raziskovalnega procesa. **Praktična uporabnost:** Kakšni so rezultati in praktična uporabnost prispevka, aplikacije ter zaključki? Vsi članki ne bodo vsebovali praktične uporabnosti – večina pa. Katere spremembe naj bi bile implicirane v praksi kot rezultat raziskave/prispevka? **Izvirnost/pomembnost prispevka:** Kaj je v prispevku izvirnega (novega)? Navedite, komu so ugotovitve raziskave/prispevka namenjene.
Povzetek v angleščini	Avtorji morajo oddati tudi prevod naslova in povzetka v angleščino. Za prevod povzetka prav tako velja omejitev do 250 besed. Postavke v angleškem jeziku so naslednje: **Purpose:** **Design/Methods/Approach:** **Findings:** **Research Limitations/Implications:** **Practical Implications:** **Originality/Value:**
Ključne besede	4–6 ključnih besed (navedene morajo biti tudi v angleščini – **Keywords**)
Besedilo	Prispevki naj bodo dolgi od 3.500 do 7.500 besed, napisani v MS Word formatu in pisavi Times New Roman, velikost črk 11, z 1,5 vrstičnim razmikom ter robovi: zgoraj – 3 cm, spodaj – 3 cm, levo – 2 cm, desno – 4 cm.
Strukturiranje besedila	Naslovi poglavij in podpoglavij naj bodo napisani z velikostjo črk 14, **krepko**. Primer: **1 UVOD** **2 POGLAVJE** **2.1 Podpoglavje 1** **2.1.1 Podpoglavje 2** **3 ZAKLJUČEK** **LITERATURA**
Literatura	Seznam literature naj vsebuje le v besedilu navedene vire, urejene po abecednem redu. Celotno navajanje literature mora biti v skladu s sistemom APA.
Navajanje literature	

Vrsta vira	**Literatura**	**Navajanje v besedilu**
Knjige en avtor	Newman, O. (1972). *Defensible space.* New York: Macmillan.	(Newman, 1972)

Knjige dva avtorja	Osterburg, J. W. in Ward, R. H. (2000). *Criminal investigation: A method for reconstruction the past* (3rd ed.). Cincinnati: Anderson Publishing.	(Osterburg in Ward, 2000)
Knjige trije do pet avtorjev	Smallbone, S., Marshall, W. L. in Wortley, R. (2008). *Preventing child sexual abuse, evidence, policy and practice*. Devon: Willan Publishing.	Prva navedba: (Smallbone, Marshall in Wortley, 2008) Naslednje navedbe: (Smallbone et al., 2008)
Knjige šest ali več avtorjev	Cooper, L., Eagle, K., Howe, L., Reims, H., Robertson, A., Taylor, D. et al. (1982). *How to stay younger while growing older: Aging for all ages*. London: Macmillan.	(Cooper et al., 1982)
Knjige avtor ni naveden	*Oxford essential world atlas* (3rd ed.). (1996). Oxford: Oxford University Press.	(Oxford essential world atlas, 1996)
Poglavja v knjigi oz. zborniku	Kornhauser, P. in Gostiša Kornhauser, A. (2006). Nasilje nad otrokom v družini. V J. Balažic in P. Kornhauser (ur.), *Zloraba in nasilje v družini in družbi, XII. spominsko srečanje akademika Janeza Milčinskega* (str. 83–97). Ljubljana: Inštitut za sodno medicino Medicinske fakultete.	(Kornhauser in Gostiša Kornhauser, 2006)
Članki v reviji (samo letnik)	Taylor, M., Holland, G. in Quayle, E. (2001). Typology of peadophile picture collections. *The Police Journal*, *74*, 97–107.	Prva navedba: (Taylor, Holland in Quayle, 2001) Naslednje navedbe: (Taylor et al., 2001).
Članki v reviji (letnik in številka)	Spaseski, J. (2009). Private security as an integral part of the single security system. *Varstvoslovje*, *11*(2), 305–315.	(Spaseski, 2009)
Gesla v enciklopediji	Pittau, J. (1983). Meiji constitution. V *Kodansha encyclopedia of Japan* (Vol. 2, str. 1–3). Tokyo: Kodansha.	(Pittau, 1983)
Članki v časopisu	Felc, M. (10. 7. 2009). Pojasnili tudi razloge za sodne zaostanke. *Delo*, str. 7.	(Felc, 2009)
Elektronski viri	**Knjige:** Standing, A. (2006). *Organised crime: A study from the cape flats*. Pridobljeno na http://www.issafrica.org/dynamic/administration/file_manager/file_links/GANGSFULL.PDF?link_id=3&slink_id=4122&link_type=12&slink_type=13&tmpl_id=3 **Članki v elektronski reviji:** Willison, R. (2006). Understanding the offender/environment dynamic for computer crimes. *Information Technology & People, 19*(2). Pridobljeno na http://www.emeraldinsight.com/Insight/viewPDF.jsp?contentType=Article&Filename=html/Output/Published/EmeraldFullTextArticle/Pdf/1610190203.pdf **Dokumenti in poročila:** Organization for Economic Co-operation and Development. (2001). *Trends in international migration: Continuous reporting system on migration*. Pridobljeno na http://www.oecd.org/dataoecd/23/41/2508596.pdf	(Standing, 2006) (Willison, 2006) Prva navedba: (Organization for Economic Co-operation and Development [OECD], 2001) Naslednje navedbe: (OECD, 2001)
Tabele, grafi in slike	Tabele naj bodo pripravljene v MS Word ali MS Excel formatu. Fotografije, grafični prikazi in slike naj bodo v jpg ali pdf formatu, široke največ 16 cm.	
Kam poslati prispevke	Prispevke naj avtorji pošljejo po elektronski pošti: rV@fvv.uni-mb.si	