Uvodnik

Spoštovane bralke in bralci, tako vroče zime, kot je bila letošnja, že dolgo ni bilo. Pa (sploh) ne samo zaradi toplega vremena. Za vse, ki se ukvarjamo s proučevanjem fenomena varnosti, se je v zimskih mesecih zvrstilo toliko dogodkov, da je vsak našel nekaj zase. Naj je šlo za afero v zvezi s prisluškovanjem obveščevalnih služb (na primer ameriške NSA) državnikom zavezniških držav, ukrajinsko krizo ali naravno katastrofo v Sloveniji, smo lahko vedno znova ugotavljali, da ima vse po malem opraviti z varnostjo, žal ne vedno z njenim zagotavljanjem, ampak tudi z zlorabljanjem mehanizmov, ki naj bi jo zagotavljali. Naše avtorice in avtorji se na dogajanje v tej zimi v prvi številki Varstvoslovja v letu 2014 seveda še niso mogli odzvati, ne dvomim pa, da bomo tudi o tem kmalu brali strokovne in znanstvene prispevke.

In kaj nam prinaša tokratna številka? Objavljamo pet člankov, prikaz monografije ter vsebinsko in avtorsko kazalo revije za leto 2013. Igor Bernik in Blaž Markelj sta se lotila proučevanja varovanja informacij pri uporabi mobilnih naprav. Verjetno so študenti tista populacija, ki najpogosteje posega po različnih mobilnih napravah, zato je njuna ugotovitev, da le-ti slabo poznajo načela varne uporabe mobilnih naprav, programske opreme zanje ter groženj in varnostnih rešitev, milo rečeno zanimiva, v resnici pa presenetljiva in predvsem skrb vzbujajoča. Ker je, kot trdita avtorja, pri mobilnih napravah meja med osebnimi in poslovnimi podatki popolnoma izginila, lahko informacijskovarnostna neosveščenost uporabnikov mobilnih naprav pomeni tudi večplastno tveganje in hkrati poseben izziv za strokovnjake. Poseben izziv prinaša tudi ekološki terorizem, ki se manifestira predvsem v smislu izrabe okolja za teroriziranje, teroriziranja okolja samega in taktike radikalnih okoljevarstvenikov. Toda glede na omejenost tovrstnih dejanj in glede na ugotovitve avtorjev prispevka, Maria Domjaniča in Bojana Dobovška, se zdi, da za enkrat ekološki terorizem predstavlja predvsem izziv v smislu poenotenja njegove definicije, zakonodaje na tem področju in preiskovalnih orodij za njegov uspešen (mednarodni) pregon.

Na izzive, tveganja in grožnje tako države kot posamezniki reagiramo z določenimi ukrepi. Prav posamezniki so že zdavnaj ugotovili, da se zgolj čakanje na državne organe, ko gre za zagotavljanje lastne varnosti, vedno ne izplača. Branka Lobnikarja in Kajo Kosec je zato zanimalo, ali in kako so se v zadnjih letih spremenili vedenjski vzorci pri samovarovalnih ukrepih, s katerimi si pomagajo prebivalci Slovenije. Avtorja ugotavljata, da se ljudje v svojem domačem kraju še vedno počutijo relativno varne, vendar kljub temu uporabljajo večje število varnostnih ukrepov kot desetletje poprej. Še posebej to velja za ženske, ki se počutijo bolj ogrožene kot moški in zato tudi pogosteje uporabljajo samovarovalne ukrepe. Brez določenih varnostnih ukrepov prav tako ne more preživeti nobena organizacija. Za sodobne organizacije je značilno, da se večina teh ukrepov nanaša na informacijsko varnost. Kaja Prislan in Igor Bernik v svojem prispevku ugotavljata, da se organizacije pogosto neučinkovito odzivajo na povečana varnostna tveganja, na kar vplivajo tako zunanji kot notranji dejavniki. Skorajda presenečata pa s trditvijo, da je učinkovitost informacijske varnosti vse bolj pogojena z neteh-

ničnimi ukrepi, za katerimi stoji usposobljen, dobro razvit in strateško naravnan varnostni management. Človeku se ob tem kar samo zastavi vprašanje, ali nismo v tej nebrzdani tehnološki evoluciji preveč stavili na stroje in zanemarili človeka?

Zadnji prispevek v tej številki se ukvarja z vse bolj aktualnim vprašanjem nacionalnih omejitev pri pravilih delovanja oboroženih sil v mednarodnih operacijah, ki slej ko prej privedejo tudi do vprašanja prekrškovne in celo kazenske odgovornosti vojakov na misiji. Avtorja Sabina Zgaga in Maj Fritz na primeru Slovenije in pripadnikov njenih oboroženih sil ugotavljata, da se glede kazenske odgovornosti lahko uporablja splošna slovenska kazenska zakonodaja (čeravno ne čisto brez pravnih in praktičnih vprašanj), medtem ko za prekrškovno odgovornost vojakov na misijah ni pravne podlage, saj se država gostiteljica svoji jurisdikciji za prekrške običajno odpove, slovenski Zakon o prekrških pa vsebuje le teritorialno načelo.

Za zaključek prve številke je Blaž Markelj pripravil prikaz monografije Igorja Bernika o kibernetski kriminaliteti in kibernetskem bojevanju, ki je bila letos izdana pri ugledni mednarodni založbi, Barbara Erjavec in Nataša Knap pa kazalo člankov ter vsebinsko in avtorsko kazalo revije Varstvoslovje za leto 2013.

Zahvaljujem se vsem, ki so prispevali k izidu številke, še posebej pa dolgoletnemu souredniku revije dr. Bojanu Dobovšku, ki zapušča uredništvo, saj se je spoprijel z novimi izzivi. Vljudno vabljeni k branju in pisanju za našo revijo.

Izr. prof. dr. Andrej Sotlar
Glavni in odgovorni urednik

VARSTVOSLOVJE,
let. 16
št. 1
str. 5–15

Zagotavljanje varnosti informacij z razumevanjem uporabnikovega ravnanja z mobilno napravo

Igor Bernik, Blaž Markelj

Namen prispevka:

Uporabniki različnih demografskih skupin vsakodnevno uporabljajo mobilne naprave v osebne in poslovne namene. Pri uporabi mobilnih naprav s pomočjo nameščene programske opreme in pri dostopanju do omrežij zanemarjajo varovanje informacij in večinoma ne delujejo v skladu s principi informacijske varnosti. Ob nevestni rabi mobilnih naprav je tveganje veliko. Ker so študenti velika skupina uporabnikov mobilnih naprav, ki vstopa v poslovni svet, smo izvedli raziskavo, kako le-ti uporabljajo mobilne naprave, koliko poznajo grožnje in uporabo možnih varnostnih zaščit. S tem znanjem organizacije lahko pripravimo na trenutne in prihajajoče informacijskovarnostne izzive.

Metode:

Predstavljene ugotovitve temeljijo na deskriptivnih dognanjih, izhajajočih iz pregleda virov in izvedene raziskave med študentsko populacijo ter analizirane s pomočjo statističnih metod.

Ugotovitve:

Študenti slabo poznajo načela varne uporabe mobilnih naprav, programske opreme zanje ter groženj in varnostnih rešitev. Glavne ugotovitve raziskave, izvedene 2012, pokažejo nizko stopnjo zavedanja in poznavanja groženj, ki pretijo uporabnikom mobilnih naprav ter nizko stopnjo uporabe varnostnih rešitev. Mobilne naprave postajajo mesto, kjer se shranjujejo in obdelujejo osebni in poslovni podatki. Pri mobilnih napravah je meja med osebnimi in poslovnimi podatki popolnoma izginila. Zato je pri uporabi mobilnih naprav priporočljivo spoštovati informacijskovarnostna priporočila in s tem zagotoviti ustrezno zaščito podatkov, do katerih imamo dostop.

Omejitve/uporabnost raziskave:

Znanstvene objave na temo, ki jo obravnavamo v prispevku, so redke. Navedb primerov širših razsežnosti zlorab iz prakse, preiskovanja kriminalitete in dejanskih sodnih obravnav pa je malo.

Praktična uporabnost:

Skozi izsledke ugotavljamo načine uporabe mobilne naprave, zavedanje groženj in uporabo varnostnih rešitev.

Izvirnost/pomembnost prispevka:

Menimo, da je delo na področju uporabe mobilnih naprav originalno in na izviren način obravnava predstavljeno problematiko.

UDK: 004.056:621.395.721.5

Ključne besede: mobilne naprave, grožnje, varnost, študenti

Ensuring the Security of Information by Understanding User Behaviour on a Mobile Device

Purpose:

Mobile devices are used every day by users from various demographic groups, both for personal and business purposes. Users neglect information security and generally do not operate according to the principles of information security while using the mobile devices by using the installed software and accessing networks. When using the mobile devices in unconscious manner the risk is high. Since the students are a very large group of users of mobile devices, we conducted a survey among them on how they use their mobile devices, and how much do they know of the threats and the use of possible security features.

Design/Methods/Approach:

The presented results are based on descriptive findings resulting from the review of resources and on the research conducted among the student population and subsequently analysed by statistical methods.

Findings:

Students have poor knowledge of the safe use of mobile devices, the software for them, threats and security solutions. The main findings of the survey, conducted in 2012, show low level of awareness and knowledge of threats to mobile security of smart phones and low level of utilization of security solutions. Mobile devices are becoming a place to store and process personal and business data. In the case of mobile devices the boundary between personal and business data is disappearing completely. Therefore, when using mobile devices it is advisable to observe safety information and recommendations in order to ensure adequate protection of the data to which we have access.

Research Limitations/Implications:

Scientific publications on the topic under discussion in this paper are rare. Allegations of abuse cases from practice, investigation of crime and the actual court case law is limited.

Practical Implications:

Through the results of the descriptive analysis and done research ways to use mobile devices are found, as well as the awareness of the threat and use of security solutions.

Originality/Value:

There is no access to comparative research, so the work on the use of mobile devices is original, since it addresses the issue presented in an original way.

UDC: 004.056:621.395.721.5

Keywords: mobile device, threats, security, students

1 UVOD

Zaradi naprednih razvitih mobilnih omrežij in mobilnih naprav[1] je možen stalen dostop do informacij v informacijskih sistemih, ki so potrebne za posamezne odločitve. Mobilne naprave s pomočjo mobilnih omrežij in različne programske opreme posameznemu uporabniku omogočajo nepozabno uporabniško izkušnjo (Greene, Tamborello in Micheals, 2013). Te niso priljubljene zgolj pri osebah, ki se gibljejo v poslovnem svetu, temveč celotni populaciji. Tako kot v realnem svetu, je za vzdrževanje stikov treba komunicirati; komuniciranje pa poteka prek družabnih portalov, tudi s pomočjo mobilnih naprav. Orodja, ki so namenjena dodatni zaščiti, pa so za uporabnike trenutno bolj ovira kot korist. Za mobilni dostop do kibernetskega prostora uporabljamo različne mobilne naprave, med katerimi so v zadnjem obdobju najbolj priljubljeni pametni telefoni. Po raziskavah podjetja International Data Corporation (2011) se v svetovnem merilu prodaja pametnih mobilnih telefonov povečuje za 55 % na leto. Raziskava, ki jo je leta 2011 objavila organizacija Ponemon Institute (2011) in je bila izvedena z namenom ugotoviti, kako dobro se uporabniki (državljani ZDA) zavedajo vprašanj varnosti in zasebnosti pri rabi pametnih telefonov, prikazuje, da uporabniki v večji meri (poleg telefoniranja) uporabljajo pametne telefone za prenose podatkov s spleta. Zanimivo je ekvivalentno število namena uporabe, največ izpraševancev ima pametne telefone tako za osebno kot poslovno rabo. Med mladimi pa je posebej zaželena neprestana povezanost s spletom in s tem omogočena dostopnost prenosa sporočil ali možnost uporabe številnih naprednih storitev družabnih omrežij (Facebook, Google Chat, Twiter idr.). Ker bodo le-ti v naslednjih letih aktivno vstopili v poslovna okolja in vanje prenašali svoje navade, menimo, da je za pripravo ustreznih strategij zagotavljanja t. i. mobilne varnosti v poslovnem okolju študentska populacija ustrezna testna skupina.

Programska oprema za mobilne naprave se prav tako razvija izredno hitro, predvsem z namenom privabiti uporabnike in povečati prodajo. Mladi prepogosto pozabljajo na pasti, ki jim pretijo, ko uporabljajo mobilne naprave, in tudi na potrebo po dodatni zaščiti, da bi se izognili pastem kibernetskega prostora. Tako je Ponemon Institute (2012) decembra 2012 objavil rezultate raziskave ugotavljanja tveganj v organizacijah, tako pri napravah kot informacijski infrastrukturi, ki jih uporabljajo končni uporabniki. Kot največje tveganje za varnost informacijske tehnologije in sistemov v organizacij je 70 % izpraševancev izbralo mobilne naprave. V rezultatih so primerjave za leto 2010, ko jih je tako odgovorilo le 9 %, za leto 2011 pa 48 %. Na drugem mestu v raziskavi iz leta 2012 (67 %) so mobilne aplikacije neznanega izvora, kar nakazuje na kontinuirano rast števila tistih, za katere mobilne naprave niso zgolj uporabno sredstvo, ampak tudi grožnja (varnostno tveganje) za informacijsko tehnologijo in sisteme organizacije.

1 *Med mobilne naprave uvrščamo predvsem naprave, ki imajo prilagojene operacijske sisteme, kot so iOS, Android, BlackBerry OS ali Windows mobile, in so prenosljive (mobilni telefoni, tablični računalniki itd.). V to kategorijo se lahko uvrsti vse naprave, ki se lahko prenašajo in pri katerih je dostop do interneta mogoč brez fizične povezave (tudi prenosniki, prenosne igralne konzole, industrijski čitalci itd.), medtem ko v skupino mobilnih telefonov spadajo tako mobilni telefoni, ki so namenjeni zgolj klicanju in pisanju kratkih sporočil, kot tudi pametni mobilni telefoni, ki predstavljajo sodobno komunikacijsko napravo, saj poleg klicanja prek mobilnih omrežij omogočajo še kopico dodatnih funkcij, ki so podobne funkcijam osebnega računalnika.*

Mobilna naprava je lahko tudi tarča programske opreme, ki se nenadzorovano namesti v napravo, kot je npr. škodljiva programska oprema in druge grožnje (*spyware*, *botnets*, *bluetooth connection* in okužbe v socialnih omrežjih (Leavitt, 2011)). Rezultati raziskave podjetja Lookout (2011) kažejo, da je bilo v drugi polovici leta 2011 povečano število groženj, temelječih na aplikacijah programa *malware*, predvsem v primerjavi s programi *spyware*; za 14 %. Poročilo Juniper Networks (2011) navaja, da se je od poletja 2010 za 400 % povečalo število mobilnih naprav, ki delujejo na platformi Android in so se okužile s škodljivo programsko opremo. V poročilu zasledimo tudi, da ima 85 % uporabnikov na svojem mobilnem telefonu neuporabno zaščito, saj si (nekateri) proizvajalci programske opreme za mobilne naprave dovolijo vgraditi »zadnja vrata« in potem brez vednosti uporabnika upravljajo nastavitve programske opreme na mobilni napravi ali pa le-ta samodejno pošilja podatke o tem, kje naprava je (npr. GPS lokacija). Tudi v poročilu Juniper Networks (2013) iz leta 2013 je navedeno veliko povečanje groženj mobilnim napravam. Poročilo je sestavljeno na podlagi enoletnega kontinuiranega spremljanja razvoja in pojavljanja groženj mobilnim napravam. Tako se je količina škodljive programske opreme od marca 2012 pa do marca 2013 povečala za 614 %.

Nepoznavanje delovanja programske opreme in zmožnosti, ki jih omogoča programska oprema mobilne naprave, povzroči, da postanemo potencialna tarča kibernetske kriminalitete. Zavedanje groženj in posledic, ki pretijo uporabnikom mobilnih naprav, je pomembno tudi zaradi zavedanja potrebe po zagotavljanju zadostne kibernetske zaščite. Nekatere zaščite bi dandanes morale biti uporabnikom samoumevne (npr. koda PIN za kartico SIM, zaklepanje povezave *Bluetooth* in zaklepanje mobilnih naprav), pa niso.

Med študenti slovenskih fakultet smo izvedli raziskavo z naslovom »Zavedanje groženj mobilnim napravam«. Namen raziskave je ugotoviti, v kolikšni meri se mladi zavedajo nevarnosti/groženj, ki jim pretijo, in kakšne varnostne rešitve uporabljajo. Cilji raziskave so bili pridobiti podatke o namenu, načinu in vrsti uporabe mobilnih naprav ter posledično o njihovem poznavanju načina rabe, groženj in zaščiti. S stališča poznavanja groženj in varnega upravljanja z mobilnimi napravami sklepamo tudi na uporabnikovo dovzetnost in poznavanje kibernetske kriminalitete.

2 METODA

Raziskava je bila izvedena s pomočjo spletnega vprašalnika, ki je bil objavljen na portalu »1ka« (www.1ka.si). Vprašalnik je bil aktiven 21 dni leta 2012. Študenti so bili o raziskavi/vprašalniku informirani prek elektorske pošte, Facebook profilov in osebno. Vprašalnik je sestavljen tako, da je mogoče ugotoviti, kako in s kakšnim namenom se uporabljajo mobilne naprave in katere vrste mobilnih naprav ter programskih rešitev se uporabljajo. V vprašalniku so vprašanja postavljena tako, da iz rezultatov dobimo vpogled v poznavanje in uporabo varnostnih rešitev ter poznavanje in zavedanje groženj, ki pretijo ob uporabi mobilnih naprav. Analiza podatkov je bila narejena s programskim orodjem SPSS. Obravnavali smo 281 izpolnjenih vprašalnikov.

Med izpraševanci je bilo največ starih od 21 do 25 let, sledi starostna skupina študentov do 20 let, 61,5 % žensk in 63,2 % takih, ki imajo zaključeno srednješolsko izobrazbo, 36,8 % je podiplomskih študentov.

Ugotavljali smo poznavanje načinov rabe mobilnih naprav. Ker pa način rabe izhaja tudi iz vrste naprave, smo ugotavljali, katere vrste mobilnih naprav uporabljajo izpraševanci. Tabela 1 prikazuje uporabo različnih tipov mobilnih naprav.

Tabela 1: Tip uporabljanih mobilnih naprav

Vzorec, $n = 282$	***n***	**%**
Klasični mobilni telefon in prenosni računalnik	79	28,01
Pametni telefon	76	26,95
Pametni telefon in prenosni računalnik	56	19,86
Klasični mobilni telefon	48	17,02
Klasični mobilni telefon, tablični računalnik in prenosni računalnik	9	3,19
Pametni telefon, tablični računalnik in prenosni računalnik	7	2,48
Klasični mobilni telefon in pametni telefon	4	1,42
Klasični mobilni telefon, pametni telefon, tablični računalnik in prenosni računalnik	1	0,35
Pametni telefon in tablični računalnik	1	0,35
Tablični računalnik	1	0,35

Iz tabele 1 je razvidno, da je največji odstotek tistih, ki istočasno uporabljajo klasični mobilni telefon (te danes v veliki meri tudi omogočajo povezavo v splet) ter prenosni računalnik; skoraj 27 % pa je takih, ki že uporabljajo pametni telefon. S skoraj 20 % pa jim sledijo izpraševanci, ki uporabljajo tako pametni telefon kot prenosni računalnik.

Tabela 2 prikazuje namen uporabe mobilne naprave. Več kot polovica (58,3 %) uporablja mobilne naprave v zasebne namene, medtem ko je četrtina takih, ki sočasno uporabljajo mobilne naprave v zasebne in službene namene.

Tabela 2: Namen uporabe mobilne naprave

Vzorec, $n = 216$	***n***	**%**
Samo za zasebne potrebe	126	58,3
Za zasebne in tudi službene potrebe	56	25,9
Za zasebne in službene potrebe	31	14,4
Za službene in delno tudi zasebne potrebe	1	0,5
Samo za službene potrebe	2	0,9

Glede na populacijsko strukturo izpraševancev (študenti) so bili takšni podatki pričakovani. Zaskrbljujoče pa je dejstvo, da je dokaj visok odstotek tistih, ki uporabljajo mobilne naprave za zasebne in službene potrebe, še posebno, če je to ista mobilna naprava. Problem nastane, ko kombiniramo med zasebnim in službenim (predvsem dostop do podatkov) ter s tem ne usklajujemo potrebe po

zagotavljanju zadostne kibernetske varnosti. Podoben primer najdemo tudi v raziskavi organizacije Ponemon Institute (2011), kjer je rezultat kombinacije osebne in poslovne rabe ravno tako velik (40 %). Iz obeh raziskav lahko trdimo, da je in bo (s prihodom novejših in naprednejših mobilnih naprav) težko postaviti ločnico med zasebno in profesionalno uporabo mobilnih naprav.

2.1 Ugotavljanje ogroženosti uporabnikov

Za zavedanje potreb po zagotavljanju zadostne stopnje informacijske varnosti pri uporabi mobilnih naprav je smiselno poznati grožnje. Tabela 3 tako prikazuje grožnje, ki jih izpraševanci poznajo.

Tabela 3: Poznavanje groženj

	DA		NE	
	n	**%**	***n***	**%**
Kraja naprave (*n* = 246)	220	89,4	26	10,6
Okužba z malwareom (*n* = 236)	79	33,5	157	66,5
Okužba s spywareom (*n* = 239)	107	44,8	132	55,2
Okužba preko aplikacije (*n* = 243)	157	64,6	85	35
Phishing (*n* = 235)	68	28,9	167	71,1
Okužba z rootkitom (*n* = 229)	32	14	197	86
Drive By Downloads (avtomatični prenos aplikacije ob odprtju brskalnika) (*n* = 233)	103	44,2	130	55,8
Odtujitev podatkov (*n* = 234)	152	65	82	35
Okužba brskalnika, ki ob obisku določene spletne strani avtomatsko naloži malware in posledično aktivira reklamne vsebine in s tem onesposobi napravo. (*n* = 238)	117	49,2	121	50,8
Prestrezanje komunikacije (tudi prenosa podatkov) (*n* = 237)	137	57,8	100	42,2
Vdori prek Bluetootha (*n* = 238)	186	78,2	52	21,8
Virusi (*n* = 242)	201	83,1	41	16,9
Plačilne prevare (*n* = 239)	167	69,9	72	30,1
Avtomatsko oddajanje podatkov (*n* = 237)	132	55,7	105	44,3
Sledenje (*n* = 242)	189	78,1	53	21,9

Poznavanje in zavedanje posameznih groženj, ki pretijo uporabnikom pametnih mobilnih telefonov, je bistvenega pomena tudi s stališča informacijske varnosti. Ni presenetljivo, da je kraja med vsemi naštetimi na prvem mestu s skoraj 90 %. Vsekakor pa je presenetljivo dejstvo, da so grožnje, kot npr. *malware* in *spyware* ter okužbe z *rootkitom*, slabo poznane. Predvsem glede na dejstvo, da raziskave, kot so npr. Lookut (2011), Juniper Networks (2011) in McAfee (2013), v svojih poročilih opozarjajo na strmo povečanje okužb z omenjenimi grožnjami.

Zaradi zavarovanja pametnega mobilnega telefona pred raznovrstnimi grožnjami moramo poznati (vsaj) osnovne varnostne ukrepe (tabela 4). Izpraševanci odgovarjajo, da najpogosteje uporabljajo kodo PIN za kartico SIM, kar je tudi pričakovano. Tako varnostno rešitev vgradi v kartico SIM že tisti, pri katerem zakupite uporabo mobilne telefonije.

Tabela 4: Uporaba varnostnih rešitev

	Uporabljam		Poznam, vendar ne uporabljam		Ne poznam	
	n	%	*n*	%	*n*	%
PIN za SIM kartico (*n* = 212)	190	89,6	21	9,9	1	0,5
PIN za dostop do aplikacij na pametnem telefonu (*n* = 206)	44	21,4	117	56,8	45	21,8
Enkripcija podatkov (*n* = 206)	12	5,8	112	54,4	82	39,8
Avtentikacija ob uporabi določenih funkcij (*n* = 208)	27	13	90	43,3	91	43,8
Oddaljeno brisanje vsebin (*n* = 206)	14	6,8	84	40,8	108	52,4
Antivirusna zaščita (*n* = 207)	61	29,5	102	49,3	44	21,3
VPN povezava (*n* = 206)	14	6,8	84	40,8	108	52,4
Arhiviranje vsebin pametnega telefona (*n* = 205)	40	19,5	91	44,4	74	36,1
Centralni nadzor pametnega telefona (določanje politike uporabe) (*n* = 205)	13	6,3	83	40,5	109	53,2
Omogočeno sledenje pametnega telefona v primeru kraje (*n* = 207)	42	20,3	104	50,2	61	29,5
Izobraževanje (*n* = 204)	53	26	84	41,2	67	32,8

Skrbi dejstvo, da veliko izprašanih pozna možnost uporabe kode PIN za dostop do posameznih aplikacij na pametnem telefonu, vendar je ne uporablja (56,8 %). Pametni mobilni telefoni to omogočajo že v osnovi, uporabiti je potrebno le ustrezne nastavitve. Varnostno rešitev oddaljenega brisanja vsebine mobilnega pametnega telefona lahko uporabimo v primeru izgube ali kraje mobilnega pametnega telefona, vendar pozna to možnost samo 40 % izprašanih (a je niso oziroma je ne nameravajo uporabiti), 52 % izprašanih pa te varnostne rešitve sploh ne pozna. Naštete možnosti zavarovanja mobilne naprave bi uporabniki lahko pridobili z ustreznim izobraževanjem, ki je lahko splošno, za vse modele zavarovanja mobilnih naprav, ali specifično, usmerjeno v posamezne modele in določene programske rešitve. Glede na rezultate, več kot 42 % izpraševancev izobraževanje, kot varnostno možnost, pozna, vendar je ne uporablja; skoraj 39 % pa te rešitve ne pozna.

Ocenjevanje verjetnosti uporabe različnih načinov prenosa podatkov na pametnem mobilnem telefonu smo razdelili v tri skupine oz. faktorje. V te skupine smo umestili spremenljivke (uporaba načinov prenosa podatkov na pametnem

mobilnem telefonu), ki so jih ocenjevali na Likertovi lestvici od 1 do 5 (1 = Nikoli, 5 = Vedno). Izvedena faktorska analiza (tabela 5) z metodo glavnih komponent razvrsti spremenljivke v tri faktorje (pri pravokotni rotaciji Varimax z normalizacijo Kaiser). Prvi faktor smo poimenovali »Nezavarovana omrežja«. V okviru tega faktorja obstaja največja verjetnost uporabe brezplačnih nezavarovanih javnih omrežij, sledi uporaba domačega z geslom nezavarovanega omrežja in nato drugi načini prenosa podatkov. V okviru drugega faktorja, ki smo ga poimenovali »Zavarovana omrežja«, smo iskali pogostost uporabe zavarovanih omrežij pri prenosu podatkov. V sklopu tega faktorja najbolj pogosto uporabljajo domače brezžično omrežje, ki je varovano z geslom, sledi službeno zavarovano omrežje. Tretji faktor smo poimenovali »Internetni ponudniki«. V okviru tega faktorja je najbolj pogosta uporaba Internetnih modulov (ponudnikov) za prenos podatkov, sledi *Blutetooth* povezava.

Tabela 5: Faktorska analiza pogostosti uporabe različnih načinov prenosa podatkov

Faktorska analiza Prenos podatkov

Cronbachov koeficient alfa: 0,655 Kaiser-Meyer-Olkinova mera ustreznosti vzorčenja: 0,680					
F1: Nezavarovana omrežja					
Cronbachov koeficient alfa: 0,617					
Odstotek pojasnjene variance: 26,9 %	**F1**	F2	F3	Aritm. sr.	St. odkl.
Povprečna vrednost: 1,93; standardni odklon: 0,912	0,825			1,71	1,198
Drugo	0,718			1,65	1,016
Brezplačna javna brezžična omrežja, ki niso varovana z geslom (brezplačne javno dostopne točke)	0,579			2,30	1,263
F2: Zavarovana omrežja					
Cronbachov koeficient alfa: 0,568 Odstotek pojasnjene variance: 22,9 % Povprečna vrednost: 2,64; standardni odklon: 1,309					
	F1	**F2**	F3	Aritm. sr.	St. odkl.
Službeno brezžično omrežje, ki je varovano z geslom		0,828		2,00	1,456
Domače brezžično omrežje, ki je varovano z geslom		0,820		3,26	1,636
F3: Internetni ponudniki					
Cronbachov koeficient alfa: 0,348					
Odstotek pojasnjene variance: 18,6 %					
Povprečna vrednost: 2,94; standardni odklon: 1,095					
	F1	F2	**F3**	Aritm. sr.	St. odkl.
Modul ponudnika interneta (Mobitel, Simobil, Tuš idr.)			0,860	2,97	1,566
Bluetooth povezava			0,540	2,90	1,201

Stopnja zanesljivosti lestvice je izračunana s Cronbachovim koeficientom alfa, ki z vrednostjo 0,655 zagotavlja srednjo zanesljivost, skupna pojasnjena varianca vseh faktorjev pa je 68,4 % (tabela 5). Na podlagi predstavljenih ugotovitev in pregleda virov pa v nadaljevanju ugotavljamo načine zagotavljanja varnosti uporabnikom mobilnih naprav.

3 DISKUSIJA

Na podlagi teoretičnih spoznanj ugotavljamo, da sta uporaba in uporabnost mobilnih naprav v porastu, hkrati pa tudi informacijskovarnostne grožnje. Nameni uporabe mobilnih naprav so različni, najbolj pogost je v povezavi z možnostjo neprestane komunikacije in neprestane dostopnosti do informacij. Na področju programske opreme imamo številne aplikacije, ki omogočajo, da si uporabniki s pomočjo informacij, ki jih prenesejo iz kibernetskega prostora, olajšajo delo.

Pri vsej popularnosti mobilnih naprav se uporabniki premalo zavedajo, da morajo sami poskrbeti za njihovo varno rabo in zaščito podatkov, tako na napravi kot med prenosom le-teh. Poznavanje groženj, ki pretijo uporabnikom mobilnih naprav, in uporaba varnostnih ukrepov je zato bistvenega pomena. Iz poznavanja groženj izhaja uporaba potrebnih varnostnih rešitev, ob nepoznavanju groženj pa se pod vprašaj postavlja tudi posameznikovo poznavanje in uporaba varnostnih rešitev.

Predstavljene ugotovitve raziskave pokažejo, da izpraševanci slabo poznajo grožnje mobilnim napravam. Grožnje, ki jih poznajo, so splošne, medtem ko je poznavanje naprednih groženj, ki so na področju mobilnih naprav najbolj v porastu, slabo. Ravno tako je z uporabo varnostnih ukrepov. Najpogostejša je uporaba preprostih zaščitnih možnosti, ki jih na področju mobilnih naprav poznamo že dalj časa (npr. koda PIN), medtem ko je uporaba in poznavanje napredne zaščite nezadostno. Zanimiva je ugotovitev, da kljub poznavanju številnih nevarnosti, ki grozijo uporabnikom mobilnih naprav, ti še vedno ne verjamejo, da se lahko grožnja zgodi tudi njim. To pomeni, da nevarnosti zavestno zanemarjajo. Rezultati raziskave kažejo, da vprašani v največji meri uporabljajo mobilno napravo zato, da lahko komunicirajo z vrstniki. Programska oprema oz. načini uporabe pa se razlikujejo.

Uporaba mobilnih naprav se bo, glede na trenutne trende, povečevala še naprej. Vedno več bo naprednih aplikacij, ki bodo uporabnikom nudile hitrejši dostop do podatkov. Pri obilici raznovrstnih mobilnih naprav in programske opreme ne smemo pozabiti na pomen zasebnosti, varovanja informacij in vzpostavitve celovite kibernetske varnosti. V središče zagotavljanja omenjenega je treba postaviti izobraževanje in ozaveščanje uporabnikov. Uporabnike je potrebno seznaniti z varnostnimi načeli rabe mobilnih naprav, razširiti njihovo poznavanje raznovrstnih groženj in morebitnih posledic ob njihovi uresničitvi ter poudariti pomen zaščitnih ukrepov. Ko se grožnja enkrat uresniči, poti nazaj ni več, zato je treba za kibernetsko varnost poskrbeti že prej. To lahko večinoma storimo že z nekaj osnovnimi koraki uporabe tehničnih rešitev in znanja varne uporabe mobilnih naprav. Najbolj običajni ukrepi so redno zaklepanje naprave (s PIN-om, vzorcem, prstnim odtisom) (Mooney, Parham in Cairney, 2013), uporaba varnostnih reši-

tev (npr. antivirusni program), tudi tistih, ki so brezplačno dostopne na spletu, uporaba zaščitenih omrežij in kriptiranega prenosa podatkov (Teulf, Zefferer in Stromberger, 2013). Pri dostopanju do spletnih portalov in prenosu različnih aplikacij s spleta je potrebno uporabljati različna in varna gesla ter predhodno preveriti varnost mest in aplikacij, do katerih dostopamo.

Moderna tehnologija nam odpira vrata v svet dodatnih možnosti, ki jih nudi kibernetski prostor. Pri vsem tem pa ne smemo pozabiti na zdravo pamet uporabe moderne tehnologije, neprestano izobraževanje o uporabi le-te in se zavedati, da poleg dobrih stvari, ki jih tehnologija prinaša, vedno z njo prihajajo tudi nevarnosti.

LITERATURA

Greene, K. K., Tamborello, F. P. in Micheals, R. J. (2013). Computational cognitive modeling of touch and gesture on mobile multitouch devices: Applications and challenges for existing theory. V M. Kurosu (ur.), *Human-computer interaction: Interaction modalities and techniques* (str. 449–455). Heidelberg: Springer.

International Data Corporation. (2011). *IDC – Press release.* Pridobljeno na http://www.idc.com/getdoc.jsp?containerId=prUS22871611http://www.idc.com/getdoc.jsp?containerId=prUS22871611

Juniper Networks. (2011). *Malicious mobile threats report 2010/2011*. Pridobljeno na http://www.juniper.net/us/en/dm/interop/go

Juniper Networks. (2013). *Juniper Networks third annual mobile threats report.* Pridobljeno na http://www.juniper.net/us/en/local/pdf/additional-resources/3rd-jnpr-mobile-threats-report-exec-summary.pdf

Leavitt, N. (2011). *Mobile security: Finally a serious problem?* Largo: University of Maryland. Pridobljeno na http://www.computer.org/portal/web/computingnow

Lookout. (2011). *Lookout mobile threat report*. Pridobljeno na https://www.mylookout.com/mobile-threat-report

McAfee. (2013). *McAfee® labs threats report: Third quarter 2013.* Santa Clara: McAfee. Pridobljeno na http://www.mcafee.com/uk/resources/reports/rp-quarterly-threat-q3-2013.pdf

Mooney, J. L., Parham, A. G. in Cairney, T. D. (2013). Your guide to authenticating mobile devices. *Journal of Corporate Accounting & Finance, 24*(5), 51–68.

Ponemon Institute. (2011). *Second annual cost of cyber crime study: Benchmark study of U.S. companies*. Traverse City: Ponemon Institute. Pridobljeno na http://www.ponemon.org/local/upload/file/2011_2nd_Annual_Cost_of_Cyber_Crime_Study%20.pdf

Ponemon Institute. (2012). *2013 state of the endpoint.* Traverse City: Ponemon Institute. Pridobljeno na http://www.ponemon.org/local/upload/file/2013%20State%20of%20Endpoint%20Security%20WP_FINAL4.pdf

Teulf, P., Zefferer, T. in Stromberger, C. (2013). Mobile device encryption systems. V L. J. Janczewski, H. B. Wolfe in S. Shenoi (ur.), *Security and privacy protection in information processing systems* (str. 203–216). Heidelberg: Springer.

O avtorjih:

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

Blaž Markelj, predavatelj informacijske varnosti na Fakulteti za varnostne vede Univerze v Mariboru. Doktorski študent varstvoslovja. E-mail: blaz.markelj@fvv.uni-mb.si

VARSTVOSLOVJE,
let. 16
št. 1
str. 16–36

Sodobni ekološki terorizem

Mario Domjanič, Bojan Dobovšek

Namen prispevka:

Namen prispevka je predstaviti pojem ekološki terorizem ter problematiko razumevanja različnih definicij, ki ga opredeljujejo. Podobno kot pri pojmu terorizem se tudi pri ekološkem terorizmu, v nadaljevanju eko terorizem, soočimo z velikim številom definicij, ki eko terorizem opredeljujejo v treh oblikah, in sicer kot izraba okolja za teroriziranje, kot teroriziranje okolja ter kot taktiko radikalnih okoljevarstvenikov. Poleg tega skušamo v prispevku ugotoviti, ali je izraz eko terorizem primeren za označevanje aktivnosti radikalnih okoljevarstvenih skupin ali ne.

Metode:

Skozi analizo strokovne literature in intervjujev, opravljenih s slovenskimi strokovnjaki s področja ekologije, okoljske kriminalitete in terorizma, skušamo v članku predstaviti problematiko pojma eko terorizem.

Ugotovitve:

Preučevana tematika je kompleksna in široka ter preiskovalcem predstavlja nov izziv, saj se radikalni okoljevarstveniki povezujejo na način, ki se v določenih segmentih razlikuje od klasičnih terorističnih ali organiziranih kriminalnih skupin. Zaradi tega so v ZDA že sprejeli nekaj specifičnih zakonov, ki konkretno opredeljujejo in določajo zakonsko podlago za procesiranje dejanj eko terorizma, poleg tega pa si preiskovalci pri preiskovanju pomagajo tudi s klasičnimi orodji, kot so geografski informacijski sistem, orodje za določanje specifičnih tarč ter orodja za analizo povezav in analizo socialnih mrež.

Omejitve/uporabnost raziskave:

Pojav eko terorizma v Sloveniji in Evropski uniji je redek, zato je bilo zapleteno najti primerne kompetentne sogovornike, ki bi poznali obravnavano problematiko.

Praktična uporabnost:

Uporabnost je v predstavitvi različnih definicij, ki opredeljujejo pojem eko terorizem, saj je tematika nova in neraziskana. Članek vsebuje osnove za nadaljnje raziskovanje obravnavane problematike.

Izvirnost/pomembnost prispevka:

Slovenska strokovna literatura s področja eko terorizma je dokaj redka. Članek prinaša vpogled v problematiko ter informacije in dilemo o tem, kaj točno pojem eko terorizem predstavlja.

UDK: 343.3/.7:504

Ključne besede: ekološki terorizem, okoljski terorizem, ekološka kriminaliteta, radikalni okoljevarstveniki

Contemporary Ecological Terrorism

Purpose:

Similar to the concept of terrorism, that of ecological terrorism (henceforth eco-terrorism) is captured in a large number of definitions differing in three ways: first, as a use of the environment as a means of terrorizing, second, as a way of terrorizing the environment, and third, as a tactic employed by radical environmentalists. By separating the two concepts, terrorism and environmental terrorism, these three types of definitions of eco-terrorism can be divided between the two concepts, so that the concept of eco-terrorism relates to actions by radical environmentalists.

Design/Methods/Approach:

Numerous scientific articles have been analysed, and interviews with experts in the fields of ecology, environmental crime, and terrorism have been carried out.

Findings:

The topic at hand is complex and broad, representing a new challenge to the investigators because radical environmentalists form networks in a way which, in certain segments or aspects, differs from that of terrorist or organized-crime groups. As a result, the U.S. has already adopted a number of specific laws that concretely define and stipulate the legal grounds for processing acts of eco-terrorism. In addition, the investigators can also apply different conventional tools and methods, such as the geographic information system, a tool for the identification of specific targets, links analysis tools, and social networks analyzing tools.

Research Limitations/Implications:

Cases of eco-terrorism in Slovenia and the EU are rare, so it was difficult to find suitable competent interlocutors to know the issues under discussion.

Practical Implications:

The article presents various definitions of the concept of eco-terrorism, as the topic is relatively new and unexplored. It provides a starting point for further exploration of the issues addressed.

Originality/Value:

Slovenian literature in the field of eco-terrorism is scarce. This paper provides insight into the problems and thereto-related information while shedding light on the dilemma what exactly constitutes the concept of eco-terrorism.

UDC: 343.3/.7:504

Keywords: eco-terrorism, eco-terrorist, environmental terrorism, environmental crime, radical environmentalists.

1 UVOD

Preprostega odgovora na vprašanje, kaj označuje in predstavlja pojem eko terorizem, ni, zato bo pojem v drugem poglavju podrobneje razdelan. Odvisno od zagovornika, ki pojasnjuje pojem, lahko eko terorizem po eni strani označuje ra-

dikalne okoljevarstvene organizacije in skupine, po drugi strani pa naj bi pojem označeval državno oziroma gospodarsko uničevanje in izkoriščanje narave in okolja. Besedno vojno med eno in drugo stranjo izgubljajo radikalni okoljevarstveniki, saj s svojimi radikalnimi aktivnostmi sprožajo burne reakcije vlad, predvsem vlade ZDA, ki vidi eko terorizem kot eno največjih nacionalnih nevarnosti ter sprejema zakone in ukrepe za boj proti tako imenovanim eko teroristom (Buell, 2009). Podobno kot pri terorizmu gre tudi pri eko terorizmu za veliko težavo definiranja samega pojma. Težava se pojavi že pri definiranju osnove pojma, torej besede terorizem. Kljub večletnemu trudu strokovnjakov za terorizem še vedno ne obstaja poenotena, generalna definicija (Transnational Terrorism, Security & the Rule of Law, 2008). Terorizem smo na podlagi več različnih definicij, ki so analizirane v nadaljevanju, povzeli kot fizično ali psihično ustrahovanje ali napad na nedolžno civilno prebivalstvo s kakršnim koli namenom vplivanja na vlado ali druge državne institucije za doseganje storilčevih ciljev. Zelo podobno je tudi s pojmom eko terorizem. Definicij je veliko, med njimi pa lahko najdemo tudi povsem različne. Poleg tega se na vprašanje, kaj je eko terorizem, dobi skoraj toliko odgovorov, kot je definicij.

Najbolj pogosto se pojem eko terorizem uporablja za radikalne okoljevarstvene skupine, ki se poslužujejo kaznivih in terorističnih dejanj ter so dokaj nov, moderen pojav, ki je šele dobro v razvoju. Radikalni aktivisti v osnovi izhajajo iz okoljevarstvenih organizacij, kot so Greenpeace, Wilderness Society in podobne. Delijo si enako ideologijo o okolju in naravi, vendar so zaradi nezadovoljstva in neuspeha v nekem trenutku spremenili svojo taktiko iz mirne v radikalno oziroma/ali nasilno. Napade na raziskovalna središča, gradbena in gozdarska podjetja, farme, predelovalnice mesa in živalskih izdelkov ter ne nazadnje tudi ljudi priznavajo in jih javnosti posredujejo preko medijev in interneta, opravičujejo pa jih z izgovorom, da vse to počnejo zaradi reševanja nemočne narave in živali (Liddick, 2006).

Drugo plat pojma eko terorizma pa predstavljajo sami radikalni okoljevarstveniki, ki zagovarjajo svoja dejanja in trdijo, da je izraz eko terorizem plod lastnikov in odvetnikov velikih gospodarskih družb ter vladnih uslužbencev, ki na račun narave žanjejo velike dobičke. Z nastankom izraza eko terorizem so preiskovanje in preganjanje radikalnih okoljevarstvenikov umestili v sklop zakonov, ki preganjajo terorizem. Preiskovalci so tako dobili več pooblastil pri preiskovanju tovrstnih dejanj, radikalnim okoljevarstvenikom posledično grozijo višje kazni, gospodarstveniki in vlade pa so si s tem zaščitili svoje posle in dobičke (Smith, 2008).

Od ustanovitve prve okoljevarstvene organizacije Sierra Club leta 1892 do danes je bilo, kot posledica izkoriščanja živali in narave, ustanovljenih mnogo različnih okoljevarstvenih organizacij in skupin. Z rastjo okoljevarstvenega gibanja se je sčasoma začel tudi razvoj okoljevarstvenikov in njihovih taktik, ki so postajale vse bolj radikalne. Sčasoma so se radikalne veje ločile od osnovnih organizacij in nadaljevale svojo »eko teroristično« pot z nasiljem in agresijo. Čeprav se eko teroristi razlikujejo od tradicionalnih teroristov, lahko vladam, podjetjem in splošni populaciji po vsem svetu povzročijo veliko težav in stroškov (Hoek, 2010; Metscher, 2005).

V nadaljevanju prispevka bomo opredelili pojem eko terorizem, katerega, kot že omenjeno, definicija ni povsem jasna. Predstavili bomo tudi značilnosti in delovanje radikalnih okoljevarstvenikov, katere lahko nekdo vidi kot ekološke teroriste in drugi kot borce proti ekološkemu terorju. Poleg osnovne predstavitve in definiranja pojma pa bomo v prispevku predstavili preiskovanje in preprečevanje omenjene problematike ter v zadnjem delu analizo opravljenih intervjujev z različnimi strokovnjaki s področja terorizma, ekološke kriminalitete in ekologije.

2 DEFINIRANJE POJMA EKO TERORIZEM

Nekateri strokovnjaki (Berkowicz, 2011; Omelchenko, 2011; Potter, 2009) ločujejo pojem eko terorizem od pojma okoljski terorizem, tako da eko terorizem uporabljajo kot pojem, ki opredeljuje radikalne okoljevarstvenike, in okoljski terorizem kot uničevanje narave s strani vojsk, držav, podjetij ali ljudi.

Na grobo lahko eko terorizem ločimo v tri oblike, s tem da se v prvi in drugi obliki definicije bolj nanašajo na okoljski terorizem, v tretji obliki pa se definicije nanašajo na eko terorizem:

1. izkoriščanje okolja za teroriziranje;
2. teroriziranje okolja;
3. teroriziranje kot okoljevarstvena taktika (Potter, 2009).

Uporaba izraza eko terorizem oziroma razvrščanje le-tega v eno od naštetih treh oblik je odvisna od tega, kdo in na kakšen način uporablja oziroma grozi, da bo uporabil nasilje za doseganje nekih ciljev.

2.1 Izkoriščanje okolja za teroriziranje

To obliko eko terorizma lahko razdelimo na dve področji. Pri prvem gre za izvajanje terorističnih dejanj za dosego političnih, verskih, ideoloških ali kakšnih drugih ciljev preko določenih taktik izrabe bioloških snovi ali uničevanja naravnih dobrin. Na primer kot eko terorizem bi lahko obravnavali napad z antraksom, zastrupitev vodnih virov, uničenje objektov za proizvodnjo ali distribucijo električne energije in podobno.

V drugem področju pa gre za tako imenovano okoljsko bojevanje. Pri tem gre za namerno uničenje, izkoriščanje ali izrabljanje okolja kot taktika bojevanja v času oboroženih spopadov, kot na primer uporaba agensa Orange v Vietnamski vojni, pri čemer je ameriška vojska s herbicidnimi mešanicami uničevala rastlinje v vietnamskih džunglah (Berkowicz, 2011). Drug primer te oblike eko terorizma je eno največjih razlitij nafte, ki jo je povzročila iraška vojska v Perzijskem zalivu in Kuvajtu med zalivsko vojno. V pol leta je iraška vojska po ukazu Sadama Huseina namerno povzročila izlitje več kot 900 milijonov litrov nafte. Pri tem so onesnažili več kot 700 kilometrov obale in 49 kvadratnih kilometrov kopna (Kostreba, 1999).

Pri izkoriščanju okolja za teroriziranje gre po navadi za teroristični napad neke teroristične skupine ali velike posege neke države za doseganje vojaških ali političnih ciljev oziroma za onesposabljanje oziroma uničenje nasprotnika ali druge države, kar lahko imenujemo tudi okoljski terorizem.

2.2 Teroriziranje okolja

Pri tej obliki lahko govorimo o povezavi pojmov ekološka kriminaliteta (pri čemer govorimo o pravno opredeljenih kaznivih dejanjih, družbeno nesprejemljivih dejanjih zoper naravo in o pretiranem, neopravičenem izkoriščanju naravnih dobrin in okolja) in eko terorizem. Gre za pretirano in nelegalno izkoriščanje naravnih dobrin in okolja. Gre tako rekoč za obsežno ekološko kriminaliteto, ki jo naravovarstveniki imenujejo »eko terorizem« držav in velikih gospodarskih korporacij, strokovnjaki pa to obliko poimenujejo okoljski terorizem (Potter, 2009).

Najbolj pogost primer pri tej obliki okoljskega terorizma je trgovanje z odpadki in nevarnimi snovmi. Podjetja in korporacije iz razvitih držav svoje odpadke nemalokrat z državno pomočjo izvozijo v države tretjega sveta. V današnjem času je zaradi strogih nadzorov in predpisov tega manj in so v to vpletene kriminalne združbe, v preteklosti pa so podjetja to pogosteje izvajala celo ob pomoči državnih organov. Znanih je več primerov odlaganja in skladiščenja strupenih odpadkov v državah tretjega sveta, saj to za podjetje lahko pomeni tudi do desetkrat manjši strošek in posledično večje dobičke. Tako je na primer 1988. leta norveško podjetje iz Filadelfije v Gvinejo pripeljalo 15.000 ton toksičnega pepela in ga skušalo prodati kot material za izdelavo opek. K sreči so norveški preiskovalni organi odkrili nelegalne aktivnosti in preprečili to dejanje (Liddick, 2011).

2.3 Teroriziranje kot okoljevarstvena taktika

Pri tej obliki gre za nasilna oziroma kazniva dejanja radikalnih posameznikov in skupin oziroma organizacij iz okoljevarstvenih krogov, ki skušajo s povzročanjem materialne škode ali ogrožanja oziroma napadanja ljudi preprečiti aktivnosti podjetij ali države, ki po njihovem mnenju škodujejo okolju. FBI definira eko terorizem kot »uporabo ali grožnjo z uporabo nasilja kriminalne narave proti nedolžnim žrtvam ali premoženju s strani okoljsko usmerjenih, subnacionalnih skupin, iz okoljsko-političnih razlogov ali z napadi simbolične narave, usmerjenih na nedolžno populacijo« (Federal Bureau of Investigation, 2003).

Tudi v enem od mnogih protiterorističnih zakonov, ki so bili predlagani in sprejeti v ZDA po terorističnih napadih 11. 9. leta 2001, »The terrorism act« iz leta 2003, najdemo definicijo eko terorista. Po tem zakonu je eko terorist tisti, ki namerno uničuje lastnino drugega z namenom vplivanja na javnost, da bi ta vplivala na tiste, katerih aktivnosti se štejejo kot okolju škodljive. Omenjeni akt je bil v senatu ZDA večkrat obravnavan, vendar uradno ni bil nikoli sprejet (Hoek, 2010).

Berkowicz v članku navaja več definicij eko terorizma različnih avtorjev. Tako definira eko terorizem po Vanderheidnu kot nelegalne taktike radikalnih okoljevarstvenih skupin, ki poskušajo tarčam, običajno podjetjem, ki povzročajo veliko okoljsko škodo, nanesti ekonomsko in materialno škodo, vendar pri tem fizično ne napadajo ljudi. V nadaljevanju navaja definicijo po Amsterju, ki pravi, da je eko terorizem odpor proti uničevanju naravne raznolikosti in divjega življenja. Nasilna dejanja nikoli niso usmerjena proti ljudem ali drugim živim bitjem, ampak je njihov namen uničiti stroje, orodje in opremo, ki uničujejo naravo (Berkowicz, 2011).

Prvi dve omenjeni obliki, izkoriščanje okolja za teroriziranje in teroriziranje okolja, lahko definiramo tudi kot okoljski terorizem, katerega dejavnosti imajo v večini primerov dolgoročni vpliv na okolje. Pri okoljskem terorizmu gre za kakršen koli nelegalen oziroma nedovoljen, obsežen poseg v naravo in okolje z namenom ustvarjanja dobička, pri čemer gre po navadi za teroriziranje okolja, ali z namenom terorističnega dejanja z izrabo okolja. Z nedovoljenim odlaganjem odpadkov, namernim izpustom olja v morje, s terorističnim napadom s kemičnim ali biološkim agensom, uničenjem jezu ali nekim podobnim dejanjem je povzročena škoda na okolju in naravi zelo obsežna, odpravljanje posledic pa dolgotrajno. Pri eko terorizmu pa gre za nedovoljene dejavnosti in napade lokalne narave. Tarča napada je lahko na primer točno določen laboratorij, živalska farma, industrijski objekt ali oseba. Pri tovrstnih napadih so posledice lokalizirane na konkretno tarčo ali žrtev napada, odpravljanje posledic napada pa običajno kratkotrajno. Ključna razlika med prvima dvema, torej okoljskim terorizmom, in zadnjo obliko, torej eko terorizmom, je, da ima eko terorizem bolj kratkoročne in lokalne posledice, medtem ko ima okoljski terorizem bolj dolgoročne in regionalne oziroma lahko celo globalne posledice. Pri okoljskem terorizmu gre za izkoriščanje narave in okolja le kot sredstvo za doseganje ciljev, medtem ko ideologija eko teroristov sloni na reševanju narave in čistem okolju (Berkowicz, 2011).

Obstaja več različnih definicij, ki eko terorizem pomensko drugače opredeljujejo. Ključni vprašanji pri definiranju pojma eko terorizma sta: »Kaj pojem eko terorizem dejansko opredeljuje?« ter »Ali sta pojma ekološki terorizem (angl. ecological terrorism) in okoljski terorizem (angl. environmental terrorism) pomensko različna?«. Kot je razvidno iz omenjenih oblik, ki pomensko razdeljujejo eko terorizem, vse tri vsebujejo neko vrsto terorja, kar pomeni, da imajo določen element terorizma. Definicija, in posledično umeščanje pojma v posamezno obliko, pa je odvisna od zagovornika in njegovega političnega prepričanja oziroma ideologije ter od tega, kaj želi z definicijo eko terorizma doseči. Nekateri avtorji skušajo bolj specifično opredeliti eko terorizem s tem, da ga ločijo od okoljskega terorizma, medtem ko drugi besedi okoljski in ekološki ne razlikujejo. Podobno kot pri definiranju terorizma tudi pri eko terorizmu ni enotne definicije in jo bo tudi zelo težko določiti, ne samo zaradi pogleda »za nekoga terorist, za drugega borec za pravice oziroma svobodo«, ampak tudi zaradi opredeljevanj povsem različnih nelegalnih, kaznivih ali nelegitimnih dejanj kot eko terorizem.

Zaradi lažje določitve razumevanja pojma eko terorizma bomo v nadaljevanju upoštevali delitev na eko terorizem in okoljski terorizem. Pri »okoljskem terorizmu« so dejanja načeloma obsojana z vseh strani. Po navadi se obravnavajo kot vojni zločini, klasična teroristična dejanja ali kriminalna dejanja. Eko terorizem radikalnih okoljevarstvenikov pa je nova tematika, katere definicija je še posebej nejasna, ravno tako pa njihova dejanja določen del družbe in celo nekatere države odobravajo, kar pa je sicer značilno tudi za tradicionalni terorizem. Pomemben element vseh dejanj, ki jih izvajajo radikalne okoljevarstvene skupine, je enak kot pri terorizmu, in to je psihološki učinek na širšo populacijo, preko katere vplivajo na vlado ali velike korporacije. Stopnja in količina nasilja, ki ga izvajajo radikalne okoljevarstvene skupine, je sicer majhna v primerjavi z nasiljem, ki ga izvajajo politični ali verski teroristi, dejstvo pa je, da radikalni okoljevarstveniki za dosego

svojih ciljev z izvajanjem kaznivih dejanj delujejo izven demokratičnega sistema (Long, 2004). Zaradi neuspeha oziroma zaradi ne dovolj hitrega uspeha tradicionalnih metod okoljevarstvenikov se nezadovoljni aktivisti pogosto odcepijo od okoljevarstvenih skupin in ustvarijo nove, bolj ekstremne skupine. V zadnjem času okoljevarstvene organizacije in posamezniki za dosego svojih ciljev uporabljajo vse bolj radikalna sredstva, kar posledično pomeni, da predstavljajo tudi vse večjo nevarnost. S svojimi kriminalnimi dejanji ustrahujejo in napadajo ljudi ter uničujejo lastnino države in podjetij, ki po njihovem prepričanju škodujejo naravi ali živalim. Zaradi določenih elementov, ki jih zajema taktika radikalnih okoljevarstvenikov, se v določenih pogledih njihova dejanja enačijo s terorizmom, zato tudi izraz eko terorizem.

3 EKO TERORIZEM KOT TAKTIKA RADIKALNIH OKOLJEVARSTVENIKOV

Eko terorizem je zelo sporna tematika. V prvi vrsti zaradi vseh definicij, ki obstajajo, in zaradi oblik, kaj vse lahko štejemo kot eko terorizem. Če pa se osredotočimo samo na radikalne okoljevarstvenike, ki jih povezujejo z eko terorizmom, pa na spornost tematike kaže tudi pogosto slišan citat »za nekoga terorist, za drugega borec za svobodo«, ki še posebej velja za eko terorizem. Okoljevarstveniki ter borci za pravice rastlin in živali pravijo, da izvajajo »direktno akcijo« za pomoč in reševanje okolja, ne glede na sredstva, medtem ko jih napadane vlade in podjetja označujejo kot eko teroriste (Liddick, 2006).

Dober primer, kako je lahko nekdo iz ene perspektive viden kot terorist in iz druge kot borec za živali in naravo, je Paul Watson s svojo skupino, ki delujejo kot Sea Shepherd Conservation Society (v nadaljevanju SSCS). Watson, ki je bil eden od soustanoviteljev skupine Greenpeace, je bil iz Greenpeace izključen 1977. leta. Razlog za izločitev je bil, po mnenju voditeljev Greenpeacea, njegovo nasilno dejanje med mirnimi protesti, ko je pobral in v morje zalučal kij enega od lovcev na tjulnje. Takoj po izločitvi leta 1977 je Watson ustanovil Earth Force Society, katere glavni cilj je bil zaustaviti lov na kite in tjulnje. Leta 1979 je Earth Force Society kupila svojo prvo ladjo, ki so jo poimenovali Sea Shepherd. Isto leto je Watson izvedel svojo prvo akcijo in prestopil mejo med okoljevarstvenikom in eko teroristom. Z ladjo Sea Shepherd se je zaletel v japonsko ladjo kitolovko Sierro in jo močno poškodoval ter ogrozil njeno posadko. Sierra se je umaknila v pristanišče, vendar je nikoli niso uspeli popraviti. Kmalu po incidentu na morju je bila na Sierro, ki so jo popravljali, postavljena bomba, ki je eksplodirala in ladjo poškodovala tako močno, da se je v desetih minutah potopila. Odgovornost za bombni napad in potopitev Sierre je prevzela Earth Force Society, ki se je kasneje leta 1981 preimenovala v Sea Shepherd Conservation Society (Hoek, 2010).

Watson s svojimi dejanji nemalokrat ogroža zdravje in življenje tako svoje posadke kot tudi tistih ljudi, ki so na napadenih ladjah. Na to kaže že potopitev ladje Sierra ter trčenje ali poškodovanje še vsaj devetih ladij, za katere je odgovornost prevzela organizacija Sea Shepherd Conservation Society. Podoben primer je tudi trčenje motornega čolna z ladje Sea Shepherd v japonski čoln s harpunami

za lovljenje kitov leta 2010. Motorni čoln ladje Sea Shepherd je bil uničen in je potonil, pri trčenju pa je bil močno poškodovan eden izmed članov posadke Sea Shepherd. Watson se s pripadniki SSCS sicer res bori proti nelegalnemu lovu na kite in tjulnje, kar mnogi vidijo kot reševanje morskih živali in narave, vendar pa jih zaradi njihovih dejanj, s katerimi nemalokrat povzročijo veliko škode, nekatera podjetja in države vidijo kot kriminalce in eko teroriste.

3.1 Značilnosti radikalnih okoljevarstvenih skupin

Radikalne okoljevarstvene skupine, kot so ALF[1], SSCS[2], Earth First![3], ELF[4] in podobne, nemalokrat s svojimi dejanji hodijo po tanki meji med terorizmom in kriminalom. Če pogledamo elemente, ki jih mora zajemati teroristično dejanje po Kharlamovi, vidimo, da bi omenjene skupine le pogojno lahko umestili v krog teroristov. Vendar pa je debata v strokovnih krogih zelo vroča in odprta (Kharlamova, 2011).

Chrystal Mancuso-Smith pojasnjuje večnamensko vlogo eko teroristov. Kot prvo je namen eko teroristov, da s svojimi nasilnimi in uničevalnimi dejanji bistvo okoljevarstva postavijo v ospredje in vzbudijo pozornost javnosti. Kot drugo eko teroristi upajo, da bodo s povzročanjem strahu in materialne škode prestrašili posameznike, organizacije, podjetja in vlade, ki s svojimi dejanji kakor koli škodujejo okolju. Poleg tega je končni in glavni namen eko teroristov povzročanje materialne škode in preprečevanje delovanja tistih, ki škodujejo okolju. Ter ne nazadnje, podobno kot tradicionalni teroristi, tudi eko teroristi hitro prevzamejo zasluge in odgovornost za incidente (Hoek, 2010).

1 *ALF – Animal Liberation Front – Pripadniki se zavzemajo za pravice živali ter nasprotujejo vsem oblikam raziskav na živalih in grobemu ravnanju z živalmi. Njihov cilj je reševanje živali iz okolij, v katerih so po njihovem mnenju zlorabljene. S svojimi dejanji povzročajo ekonomsko škodo vsem, ki na kakršen koli način izkoriščajo živali (Best in Nocella, 2005). Organizaciji ELF in ALF sta v zadnjih desetih letih skupaj povzročili za več 100 milijonov dolarjev škode. Skupni napadi aktivistov ELF in ALF so zelo uspešni, njihove tarče pa so v večini primerov državne ustanove in njihovi objekti (npr. urad za upravljanje z zemljišči, gozdna industrija ZDA, univerzitetni laboratoriji in podobno). Nemalokrat so žrtve njihovih napadov tudi gradbena podjetja, gozdarska podjetja ter trgovci terenskih vozil (Long, 2004).*

2 *SSCS – Sea Shepherd Conservation Society – Organizacijo je ustanovil bivši pripadnik Greenpeace Paul Watson. Skupaj s pripadniki SSCS in floto različnih ladij skušajo na različne nasilne in ne nasilne načine zaščititi morske živali. Njihove tarče napadov so predvsem lovci na kite, tjulnje ter morske leve.*

3 *Earth First! – Organizacija je bila ustanovljena z namenom zaščititi ameriške gozdove pred pretiranim izkoriščanjem. S sabotažami, ekotažami (»tree spiking«, »tree sitting«) in civilno nepokorščino so gozdarskim in gradbenim podjetjem preprečevali posek gozdov. Najbolj radikalni okoljevarstveniki so se ločili in ustanovili ELF (Keller, 2008).*

4 *ELF – Earth Liberation Front – Organizacija je nastala po modelu ALF. Njihov cilj je nanašanje finančne in gospodarske škode podjetjem, državam in organizacijam, ki po njihovem mnenju kakor koli ali s čimer koli škodujejo naravi in okolju. ELF je najbolj aktivna okoljevarstvena organizacija v ZDA na področju izvajanja »direktnih akcij«, vandalizma in kaznivih dejanj. Poslužujejo se različnih taktik, od uničevanja do požigov, uporabili pa so tudi že eksploziv in improvizirane bombe (Long, 2004).*

3.1.1 Organiziranost radikalnih okoljevarstvenih skupin

Za razliko od klasičnih terorističnih skupin, ki naj bi imele strogo hierarhijo in točno določeno linijo vodenja in poveljevanja, radikalni okoljevarstveniki oziroma eko teroristi niso preveč dobro organizirani. Nemalokrat se celo zgodi, da med posamezniki in skupinami, ki izvajajo kriminalna dejanja, ni skupne rdeče niti. Ideja je enaka, vendar nemalokrat nimajo enakega cilja, kaj dejansko želijo doseči s svojimi dejanji (Liddick, 2006).

Radikalni aktivisti delujejo znotraj anonimnih celic, ki niso geografsko omejene in v katere je običajno preiskovalcem zelo težko prodreti. Da nekdo postane pripadnik eko terorističnega gibanja oziroma radikalne okoljevarstvene skupine, mora preprosto podpirati njihovo idejo in izvajati kazniva dejanja v njenem imenu z namenom zaščite okolja in živali (The Inkerman Group, 2007). Celice so povsem samostojne in delujejo neodvisno od matične organizacije. Člani celic so zaradi varnostnih razlogov anonimni in med posameznimi celicami ni komunikacije. Zaradi anonimnosti in samostojnosti posameznikov so njihova dejanja močno odvisna od vidnih članov organizacije oziroma skupine, ki jim zagotavljajo podporo, usmeritve in seveda zelo pomembno propagando (Liddick, 2006). Vidni člani okoljevarstvenih skupin so ključni element za dosego cilja, ki se ga skuša doseči s kriminalnimi dejanji. Vidni oziroma javni sektor skupin so neke vrste politično krilo, ki je zadolženo, da po nasilnih napadih pride do političnih sprememb (Liddick, 2006).

3.1.2 Taktika in tarče radikalnih okoljevarstvenih skupin

Pomemben element vseh dejanj, ki jih izvajajo radikalne okoljevarstvene skupine, je enak kot pri terorizmu, in to je psihološki učinek na širšo populacijo, preko katere vplivajo na vlado ali velike korporacije. Stopnja in količina nasilja, ki ga izvajajo radikalne okoljevarstvene skupine, je sicer majhna v primerjavi z nasiljem, ki ga izvajajo politični ali verski teroristi, dejstvo pa je, da radikalni okoljevarstveniki za dosego svojih ciljev z izvajanjem kaznivih dejanj delujejo izven demokratičnega sistema (Long, 2004). V njihovem boju za okolje in živali mediji igrajo pomembno vlogo in so ključni za dosego ciljev vseh okoljevarstvenih organizacij, radikalnih pa še posebej. Mediji velikokrat s pozitivno interpretacijo dogodka sprožijo debato v širši množici in v strokovnih krogih, ali je za dosego zaščite okolja in živali upravičeno uporabljati tudi nasilno taktiko in izvajati kazniva dejanja (Liddick, 2006).

Vprašanja o tem, katera nasilna in kazniva dejanja so moralno dovoljena in katera so sporna v doseganju ciljev radikalnih okoljevarstvenikov, se pojavljajo tudi znotraj organizacij. Nekatere skupine zagovarjajo, da je dovoljeno samo uničevanje lastnine, kakršno koli ogrožanje ali napadanje ljudi pa je absolutno nedovoljeno. Spet drugi trdijo, da je za doseganje njihovega cilja, torej zaščite okolja in živali, dovoljeno posegati po kakršnih koli sredstvih, le da bodo uspešna (Liddick, 2006).

Liddick (2006: 72) je kazniva dejanja radikalnih okoljevarstvenikov razdelil v štiri skupine:

1. TIP I – manjša kazniva dejanja, ki ne povzročijo škode oziroma je škoda zelo majhna (do 10.000 USD), in ni nikakršnega ogrožanja ljudi.
2. TIP II – kazniva dejanja, pri katerih gre za veliko materialno škodo, vključno s požigi in manjšimi eksplozijami (nad 10.000 USD), vendar pri tem ni namena poškodovanja ljudi, obstaja pa posredna grožnja fizičnih poškodb ljudi.
3. TIP III – direktna grožnja ljudem, vključno z manjšimi fizičnimi napadi, brez resnih fizičnih poškodb.
4. TIP IV – fizični napad na osebo, pri katerem pride do fizičnih poškodb oziroma želijo napadalci fizično poškodovati napadeno osebo.

Posamezna kazniva dejanja po skupinah so predstavljena v tabeli 1.

TIP I	**TIP II**
• civilna nepokorščina • nedovoljen vstop na posest • protestiranje brez dovoljenja • osvobajanje ujetih živali • obešanje transparentov • blokiranje drvarskih poti • »tree sitting« • grafitiranje • onesposabljanje ključavnic • razbijanje oken	• uničevanje drvarske opreme • požiganje terenskih vozil • požiganje raziskovalnih laboratorijev • »tree spiking« • obsežno osvobajanje ujetih živali • uporaba molotovk • uporaba zažigalnih naprav
TIP III	**TIP IV**
• grožnje preko elektronske pošte • lažne bombne grožnje • telefonsko nadlegovanje in grožnje • pisemske pošiljke z britvicami • objavljanje osebnih finančnih podatkov • demonstriranje na zasebnem posestvu • grafitiranje zasebnih posestev • polivanje ljudi z barvo • obmetavanje ljudi z gnilo hrano • postavljanje mrtvih živali pred vrata zasebnih hiš	• fizični napad, pretepanje • umor • bombni napad • napad s fizičnimi poškodbami • napad, katerega namen je povzročitev fizičnih poškodb Lahko tudi: • biološki napadi • zastrupljanje vodnih rezervoarjev

Tabela 1: Vrste kaznivih dejanj (vir: Liddick, 2006: 73)

Svojo taktiko eko teroristi prilagajajo glede na tarčo, ki jo izberejo za svoj napad. Eko militantne skupine in posamezniki napadajo tako vladne in nevladne ustanove ter urade kot tudi zasebna podjetja in posameznike. Njihove potencialne tarče so vsi, ki so kakor koli vpleteni ali imajo koristi od aktivnosti, škodujejo živalim in okolju. Primarne tarče radikalnih okoljevarstvenikov so podjetja, ustanove, organizacije in posamezniki, ki neposredno izkoriščajo živali ter škodujejo okolju.

Najbolj pogoste primarne tarče militantnih okoljevarstvenikov so:

- urbanistična in gradbena podjetja ter posamezniki,
- podjetja in posamezniki iz gozdarske industrije,
- proizvajalci in trgovci športno-terenskih vozil,
- podjetja in posamezniki, kakor koli povezani s proizvodnjo, prodajo in distribucijo živalskih produktov (usnjarska, mesna, volnarska, ribja industrija),
- živalske raziskovalne ustanove in njihovi zaposleni,
- podjetja in univerze, ki se ukvarjajo z genetskim inženiringom,
- različne živalske farme in zavetišča, ki izvajajo poizkuse na živalih, ter njihovi zaposleni,
- lovski klubi in zveze,
- vladne ustanove, razna ministrstva, uradi in institucije s področja kmetijstva, gozdarstva, prehrane in drugo (Helios Global, 2008).

Sekundarne tarče radikalnih okoljevarstvenikov pa so podjetja in organizacije, ki so s primarnimi tarčami kakor koli povezane ali z njimi poslovno sodelujejo. Z izsiljevanji, grožnjami in napadi na sekundarne tarče skušajo aktivisti primarnim tarčam uničiti poslovne odnose oziroma ustrahujejo njihove poslovne partnerje (Helios Global, 2008).

Zaradi neuspeha oziroma zaradi ne dovolj hitrega uspeha tradicionalnih metod okoljevarstvenikov so se nezadovoljni aktivisti odcepili od okoljevarstvenih skupin in ustvarili nove, bolj ekstremne skupine. Progresivna radikalizacija okoljevarstvenih skupin se je pričela v Veliki Britaniji in se hitro razširila v ZDA ter kasneje tudi drugod po svetu. S svojimi kriminalnimi dejanji ustrahujejo in napadajo ljudi ter uničujejo lastnino države in podjetij, ki po njihovem prepričanju škodujejo naravi ali živalim. Zaradi določenih elementov, ki jih zajema taktika radikalnih okoljevarstvenikov, se v določenih pogledih njihova dejanja enačijo s terorizmom, zato tudi izraz eko terorizem.

4 PREISKOVANJE IN PREPREČEVANJE EKO TERORIZMA

Preiskovanje in preganjanje eko terorizma je v ZDA vroča tema, saj so ameriški organi pregona najbolj aktivni na področju domačega terorizma, kamor uvrščajo tudi eko terorizem. Domači terorizem je problem, ki ga v ZDA obravnavajo na zvezni ravni, zato za obravnavanje eko terorističnih dejanj upoštevajo na zvezni ravni sprejeto protiteroristično zakonodajo:

- Law against tree spiking (1988) – Napisan in sprejet kot odgovor na aktivnosti radikalnih aktivistov skupine Earth First!. Zakonu Drug Act of 1988 so dodali še amandma, ki je prepovedoval in kazensko obravnaval aktivnost »tree spiking«.
- Animal enterprise protection act of 1992 (v nadaljevanju AEPA) – Sprejet je bil kot odgovor na vse pogostejše napade radikalnih okoljevarstvenikov na zasebna, gospodarska in državna podjetja ter ustanove, ki pri svojem delu uporabljajo živali v izobraževalne ali raziskovalne namene,

za predelavo v hrano, v kmetijstvu, usnjarstvu in podobno. V njem so zapisali, da se kot zvezno kaznivo dejanje obravnava vsakršen napad, vandalizem, kraja ali oviranje dela oziroma proizvodnje, ki povzroči omenjenim podjetjem kakršno koli materialno škodo višjo od 10.000 dolarjev ali telesne poškodbe zaposlenih ali lastnikov.

- Antiterrorism and effective death penalty act of 1996 – Zakon se nanaša na vsa teroristična dejanja. Tako se po členih iz tega zakona kaznuje tudi radikalne okoljevarstvenike, ki s svojimi dejanji povzročijo eno ali več smrtnih žrtev. Zakon predvideva stroge kazni tudi za osebe, ki bi storilcem nudile usposabljanje ali osebje za teroristična dejanja.
- USA patriot act of 2001 (Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001) – Zakon je bil sprejet po terorističnih napadih na ZDA septembra 2001 z namenom preprečevati in kaznovati teroristična dejanja v ZDA in po svetu, izboljšati preiskovalna orodja, taktike in metodo organov pregona ter preprečevati pranje denarja. Eko terorizem se po tem zakonu preganja v poglavjih, ki opredeljujejo domači terorizem (Long, 2004).
- Animal enterprise terrorism act of 2006 (v nadaljevanju AETA) – Zakon je nadomestil AEPA in je zveznim oblastem razširil pooblastila za preiskovanje in boj proti eko terorističnim skupinam. AETA dopolnjuje zvezne kazenske predpise in določa kazniva dejanja poškodovanja ali zaviranja zasebnih, gospodarskih ali državnih podjetij in ustanov, ki pri svojem delu uporabljajo živali v izobraževalne ali raziskovalne namene, za predelavo v hrano, v kmetijstvu, usnjarstvu in podobno; uničevanja zasebne lastnine teh podjetij in osebne lastnine posameznikov, povezanih s temi podjetji, ter kakršne koli psihične ali fizične grožnje, grožnje s smrtjo ali resne fizične poškodbe posameznikov, povezanih s temi podjetji. Poleg tega je v AETA za razliko od AEPA kazniv tudi poizkus storitve prepovedanega dejanja in ne samo uspešno izvedeno dejanje, močno pa so se tudi povečale denarne in zaporne kazni za storjena dejanja (Bjelopera, 2012).

Za preprečevanje eko terorizma preiskovalci uporabljajo tradicionalne protiteroristične ukrepe, kot so zbiranje obveščevalnih podatkov (Open Source Intelligence, Image Intelligence in drugo) ter obdelava le-teh in preiskave že znanih storilcev ter osumljenih radikalnih okoljevarstvenikov. Po kaznivem dejanju, ki ga uvrščajo v sklop eko terorističnih dejanj, pa preiskovalci dejanje preiskujejo s klasičnimi kriminalističnimi taktikami in preiskovalnimi metodami (Deshpande in Howard, 2012). Kritiki boja proti eko terorizmu trdijo, da organi pregona pretiravajo in da je nevarnost s strani radikalnih okoljevarstvenikov preveč napihnjena ter da vlada s pregonom tako imenovanih eko teroristov pri ljudeh ustvarja »zeleni strah«. Enačenje kaznivih dejanj, kot sta vandalizem in uničevanje lastnine, s terorizmom je nesmisel in pretiravanje, radikalni okoljevarstveniki pa si ne zaslužijo etikete teroristov (Bjelopera, 2012).

V Evropski uniji do zdaj radikalni okoljevarstveniki še niso bili prav posebej aktivni. V Veliki Britaniji je sicer bilo zabeleženih nekaj napadov radikalnih okoljevarstvenikov, vendar so jih tam obravnavali kot posamezna kazniva dejanja.

Eko terorizem v obliki radikalnih okoljevarstvenih organizacij v EU ne predstavlja posebne nevarnosti, zaradi tega na tem področju ni sprejeta nikakršna posebna zakonodaja, ki bi obravnavala to problematiko. Ravno tako ni zaslediti, da bi katera od držav članic EU individualno sprejela pravni akt, s katerim bi predpisali posebno obravnavanje dejanj radikalnih okoljevarstvenikov v smislu eko terorizma.

4.1 Orodja za preiskovanje in preprečevanje eko terorizma

Pri preiskovanju radikalnih okoljevarstvenih skupin in aktivistov preiskovalci uporabljajo klasične preiskovalne metode in tehnike, vendar pa je samo preiskovanje tega področja zelo zapleteno, saj so aktivisti precej nepovezani, nastopajo anonimno ter po navadi niti javne osebe radikalnih skupin ne poznajo identitete aktivistov. Pri preiskovanju je ključna uporaba zanesljivih informatorjev, ki uspejo preiskovalcem pridobiti podatke o načinu storitve, storilcih, določenih nabavah sredstev in podobno. Pri združevanju in analiziranju podatkov si organi pregona pomagajo z orodji, ki so jim v pomoč tudi pri preiskovanju klasičnih terorističnih dejanj, kot so orodja za analizo povezav in analizo socialnih mrež, geografski informacijski sistemi ter orodja za določanje specifičnih tarč (Deshpande in Howard, 2012).

4.2 Primer Operacija Backfire

Operacijo Backfire so organi pregona izvedli z namenom razkritja in zajezitve grožnje, ki jo je s svojimi kaznivimi dejanji predstavljala ena od neznanih radikalnih okoljevarstvenih skupin. Različne pripadnike skupine z imenom »Družina« (angl. The Family) so v obdobju šestih let, v petih zveznih državah na severozahodu ZDA, povezali z dvajsetimi kaznivimi dejanji, s katerimi so povzročili več kot 40 milijonov dolarjev škode in uničili številna podjetja. Skupina se je prvotno predstavljala kot ena od celic organizacije Earth Liberation Front (ELF), kar so potrjevali tudi simboli ELF, ki so jih puščali na kraju kaznivih dejanj, vendar so pripadniki sčasoma ustvarili močno identiteto »Družine« in so izvajali akcije povsem samostojno in neodvisno od ELF, nikoli pa se niso povsem ločili od ideologije in ciljev ELF (Deshpande in Howard, 2012).

4.2.1 Sestava in organiziranost »Družine«

Organi pregona so v sklopu preiskave identificirali 18 oseb, povezanih z »Družino«, vendar je število članov znotraj »Družine« variiralo tako, da je pri posameznem kaznivem dejanju sodelovalo različno število ljudi. Člani skupine so si bili zelo različni, imeli pa so skupne lastnosti, ki so jih tesno povezovale. Skupno jim je bilo nezadovoljstvo z družbo, neupoštevanje pravnega sistema, sodelovanje na različnih protestih in zborih ter začetna predanost eden drugemu in skupnemu cilju varovanja narave (Department of Justice U. S., 2007).

Začetniki in idejni vodje »Družine« so bili Kevin Tubbs, William Rodgers in Stanislas Gregory Meyerhoff, ki so rekrutirali ostale člane in jih tudi usmerjali ter

izobraževali, kako storiti določeno kaznivo dejane. Pridobivanje radikalnih aktivistov jim je bilo olajšano zaradi promocije njihove ideje v imenu ELF, poleg tega pa so bili določeni člani med seboj močno povezani tudi osebno oziroma sorodstveno. Jedro skupine so predstavljali najradikalnejši aktivisti, kar je imelo za posledico evolucijo novih radikalnih aktivistov, saj so sčasoma pri kaznivih dejanjih začeli sodelovati tudi tisti pripadniki, ki se »Družini« v osnovi niso priključili z namenom izvajanja nasilja, agresije ali kaznivih dejanj, ampak preprosto zaradi ideje varovanja okolja in živali (Deshpande in Howard, 2012).

Pripadniki »Družine« so zelo dobro poskrbeli tudi za varnost in anonimnost ter izvajali vse potrebne preventivne ukrepe, da so se izognili razkritju s strani preiskovalnih organov. Natančno so načrtovali vsako izvedeno akcijo. Med pripravami in dejanji so nosili rokavice, maske ter zaščitne obleke. Zažigalne naprave so pripravljali v tako imenovanih »čistih sobah«, tako da na napravah niso puščali sledi. Vse dokaze so sprotno in temeljito uničili. Člani so izdelovali in uporabljali ponarejene dokumente ter veliko potovali med zveznimi državami, s čimer so se spretno izogibali preiskovalcem. Za medsebojno komunikacijo pa so uporabljali vzdevke, različne kode in številke ter ohranjali zapleteno varnostno mrežo medsebojnih odnosov in aktivnosti (Department of Justice U. S., 2007).

Člani so se med seboj sestajali na tako imenovanih »knjižnih klubih«, na katerih so si izmenjavali podatke ter posredovali informacije, ki so jih potrebovali za izvedbo kaznivih dejanj. Poleg izmenjave podatkov so na »knjižnih klubih« izvajali tudi določena usposabljanja, kot so neopazno opazovanje tarče, vlamljanje ključavnic, šifrirano komuniciranje, izdelava časovnih naprav za vžig zažigalnih sredstev in podobno (Department of Justice U. S., 2007). Preko »knjižnih klubov« so idejni vodje nove člane učili tudi o taktikah uporabe improviziranih eksplozivnih naprav, o različnih načinih netenja požarov ter o različnih vrstah sabotaž. Z omenjenimi taktikami so imeli namen uničiti ali poškodovati gospodarsko ali vladno lastnino. Po pričevanju nekaterih obdolženih pripadnikov »Družine« pa naj bi Rodgers in Meyerhoff načrtovala tudi radikalnejša dejanja, kot so uboji določenih vodilnih oseb gospodarskih podjetij, ki so bila tarča »Družine, vendar do izvršitve teh dejanj nikoli ni prišlo. Taktike skupine so temeljile na nizki tehnološki stopnji, za katere ni bilo potrebnega posebnega tehničnega znanja in za katere so bila sredstva in material lahko dostopna ter poceni, še vedno pa so z njimi naredili dovolj veliko in odmevno dejanje oziroma škodo. To je zmanjšalo logistiko in stroške ter olajšalo učenje novih članov in omogočalo »Družini«, da je dosegla veliko učinkovitost in kontinuiran izobraževalni cikel novih članov (Deshpande in Howard, 2012). Tajnost »knjižnih klubov« so člani »Družine« ohranjali tako, da so se sestajali na različnih krajih v več zveznih državah. Za sklic sestanka in komuniciranje so uporabljali skupne naslove spletnih elektronskih pošt, na katerih so napisali osnutek sporočila, ki je bil šifriran in nikoli poslan. Sporočilo je bilo običajno na spletu teden dni in vsak član je imel dostop do predala elektronske pošte, kjer je sporočilo lahko prebral. Vsi organizirani in izvedeni varnostni ukrepi ter anonimnost in molčečnost, ki so jih člani »Družine« izvajali, so pripomogli k visoki uspešnosti izvedenih kaznivih dejanj ter k dolgotrajni nerazkritosti s strani preiskovalcev (Department of Justice U. S., 2007).

Za »Družino« je bila ključna tudi medijska kampanja, s katero so prevzemali odgovornost in pojasnjevali svoje napade. Preko medijev so si širili krog privržencev, znotraj kroga radikalnih okoljevarstvenih gibanj pa so bili deležni velikih odobravanj. Medijske pisarne Animal Liberation Front in Earth Liberation Front so bile posrednik pri medijski kampanji, saj so tako aktivisti »Družine« ostali anonimni za medije, populacijo in ne nazadnje tudi za preiskovalce. Ravno sporočila o aktivnostih »Družine« pa so na koncu privedla do spora znotraj skupine, saj naj bi bil v enem od sporočil razkrit eden od aktivistov. Nesoglasja zaradi posredovanja vsebine sporočil medijem in posledično preiskovalcem so v »Družini« povzročila nekohezivnost in posledično površnost pri izvajanju varnostnih ukrepov (Deshpande in Howard, 2012).

4.2.2 Operacija Backfire

Med decembrom 1995 in oktobrom 2001 so aktivisti »Družine« povzročili vsaj dvajset požarov v petih zveznih državah ter porušili visokonapetostni električni daljnovodni stolp. S storjenimi dejanji so povzročili za več kot 40 milijonov dolarjev materialne škode. Preiskovalni organi iz posameznih zveznih držav so na začetku preiskave vsako od omenjenih kaznivih dejanj obravnavali posamezno, zbirali so forenzične dokaze, a si jih niso izmenjevali. Niti protiteroristična taktična enota FBI, ki je na zvezni ravni preiskovala storjena dejanja in jih je uspela na podlagi taktik, tehnik in postopkov, ki so jih storilci izvedli, grobo povezovati, ni imela mehanizma, ki bi omogočal posredovanje in izmenjavo informacij z lokalnimi preiskovalnimi organi (Deshpande in Howard, 2012).

Rezultat nepovezanih preiskav in neizmenjavanja informacij je bilo tavanje preiskovalcev v temi, da niso uspeli odkriti osumljencev, niti ni bila podana nobena obtožnica. Po petih letih neuspešnih preiskav se je leta 2000 zgodil preobrat. Preobrat je storil pomočnik državnega tožilca v Oregonu Kirk A. Engdall, ki je lokalnim in zveznim preiskovalcem predstavil skupne točke dejanj, poudaril pomembnost izmenjave podatkov ter skupne preiskave. Tako se je začela skupna preiskava, ki so jo poimenovali »Operacija Backfire«. Združitev ločenih preiskav in uporaba orodij, kot so SNA, analiza povezav, GIS in drugo, je preiskovalcem omogočila izrabiti vsa sredstva, s katerimi so potrdili ali ovrgli domnevne povezave med osebami in dogodki, združili forenzične dokaze ter bolje razumeli celotno eko teroristično mrežo, s katero so se soočali (Deshpande in Howard, 2012).

Rezultati dolgotrajne raziskave so se pokazali šele po tem, ko je preiskovalcem uspelo odkriti enega od storilcev, ki je dobro poznal organiziranost in delo »Družine«, kjer je tudi sam sodeloval pri mnogih nelegalnih aktivnostih, in za katerega so, glede na njegovo preteklost in osebnost, ocenili, da bi ga lahko prepričali v sodelovanje. Preiskovalci so na svojo stran pridobili radikalnega aktivista Jacoba J. Fergusona, ki je v izjavi podal podrobne podatke o storilcih, dejanjih, lokacijah ter taktikah (Department of Justice U. S., 2007). Preiskovalci so Fergusonovo vpletenost odkrili leta 2003, ko je »Družina« že prenehala izvajati svoje aktivnosti in se člani niso več sestajali. Ferguson je bil, v zameno za milejšo kazen, pripravljen sodelovati v preiskavi in se je v naslednjih dveh letih ozvočen sestajal s sostorilci ter snemal njihove obremenilne pogovore, ki so potrjevali Fergusonovo pričanje (Deshpande in Howard, 2012). Posnetki, ki so jih preiskovalci pridobili s

pomočjo Fergusona, so bremenili Kevina Tubbsa, Stanislasa Meyerhoffa, Kendalla Tankersleya, Williama C. Rodgersa, Daniela McGowana, Jonathana Paula, Darrena Thurstona in Chelseai Gerlach. Na podlagi močnih dokazov so preiskovalci leta 2005 izvedli prve aretacije, ki pa so pripeljale do novih priznanj in prič, ki so bile pripravljene pričati, ter posledično do novih dodatnih aretacij vseh vpletenih (Department of Justice U. S., 2007).

Organiziranost preiskovalcev v Operaciji Backfire je bila ključna za uspeh. Koordinacijskih sestankov so se udeleževali predstavniki državnega tožilstva, FBI, zveznega urada za alkohol, tobak in orožje, državnega gozdnega urada in lokalnih policij. Pod vodstvom Engdalla so si izmenjavali podatke ter se dogovarjali, katera služba, urad ali agencija bo izvedla katere postopke, kako in kdaj jih bo izvedla, kdo bo sodeloval ter kdo bo nosilec posamezne aktivnosti. Zaradi dobre organiziranosti in skupnega cilja razkritja vseh udeležencev v eko terorističnih dejanjih so vsi vpleteni delovali sinhronizirano in rezultat akcije je bil na koncu zelo uspešen (Deshpande in Howard, 2012).

5 EMPIRIČNI DEL

V empiričnem delu prispevka so bili glede na obdelano tematiko izvedeni intervjuji z različnimi strokovnjaki s področja terorizma, ekološke kriminalitete in kriminologije. Z namenom ugotoviti, kaj menijo slovenski strokovnjaki o pojmu eko terorizem ter o omenjeni problematiki, smo intervjuvancem zastavili sledeča vprašanja:

1. Kakšna je teroristična ogroženost v Republiki Sloveniji?
2. Kaj dojemate pod pojmom eko terorizem?
3. Osebne izkušnje oziroma poznavanje primerov terorizma/eko terorizma?
4. Kakšni so problemi pri preiskovanju terorizma/eko terorizma?
5. Predlogi za izboljšavo preventive in preiskovanja?

Ker je pojem eko terorizem še precej nejasen, smo želeli s prvim vprašanjem odpreti pogovor o terorizmu in nato v drugem vprašanju pričeti s specifično tematiko. Drugo vprašanje je bilo ključno za analizo, saj so intervjuvanci podali svoje videnje na obravnavano tematiko, s pridobljenimi ugotovitvami pa smo nato skušali potrditi ali ovreči podatke iz strokovne literature. Zadnja tri vprašanja zaradi različnih izkušenj in kompetentnosti intervjuvancev niso bila ključna za analizo. Vendar smo z njimi poskušali pridobiti dodatna mnenja, ki smo jih nato povezali in primerjali s tujo strokovno literaturo. Intervju je bil zastavljen polstrukturirano, kar pomeni, da je sogovornik odgovoril na zastavljeno vprašanje ter povedal svoje mnenje, nato pa smo s podvprašanji in z določenimi pojasnitvami nadaljevali pogovor.

V raziskavi vzorec predstavlja 5 intervjujev, ki so bili izvedeni februarja 2013 z vsakim intervjuvancem samostojno. Intervjuji so bili opravljeni s strokovnjakinjo za sredstva za množično uničevanje iz akademskih krogov, z dvema strokovnjakoma iz nevladnega področja iz akademskih krogov ter iz okoljevarstvene organizacije (skupina 1) ter z dvema predstavnikoma državnih preiskovalnih organov, ki predstavljata pogled preiskovalca na obravnavano tematiko (skupina 2). Dolži-

na intervjuja je bila približno 60 minut. Vsi intervjuvanci imajo večletne izkušnje na področjih ekologije, ekološke kriminalitete ali terorizma. Demografskih podatkov o starosti in spolu zaradi obljube intervjuvancem o anonimnosti raziskave ne navajamo.

Analiza intervjujev je pokazala, da sta ključni vprašanji, pri katerih smo se v pogovorih tudi najdlje zadržali, prvo in drugo. Odgovori na obe vprašanji nam kažejo kompleksnost in zapletenost določanja teroristične ogroženosti ter določanje pomena pojmu eko terorizem.

Pri prvem, »Kakšna je teroristična ogroženost v Republiki Sloveniji?«, smo dobili osnovni vpogled o prisotnosti grožnje terorizma v RS. Nanj je vseh pet intervjuvancev v prvi fazi odgovorilo enako, da Slovenija načeloma ni ogrožena oziroma da ocene kažejo, da je ta ogroženost zelo nizka. Vsi pa ob tem tudi poudarijo, da nizke ocene ne smemo podcenjevati, saj se vsak dan lahko zgodi kakšen napad, ki ga morda sploh ne pričakujemo.

Odgovori pri prvem vprašanju se razlikujejo v tem, da intervjuvana preiskovalca podata možne grožnje, ki po njunem mnenju predstavljajo najverjetnejšo nevarnost v RS. Eden od njiju kot največji grožnji vidi tranzit možnih teroristov skozi našo državo ter delovanje teroristov »samotarjev«, drugi pa nevarnost vidi v terorističnem napadu na neko tujo tarčo na našem ozemlju.

Intervjuvanka, strokovnjakinja za sredstva za množično uničevanje, pri tem vprašanju poudari, da je ogroženost relativna ocena, ki jo je zapleteno in zahtevno dejansko določiti. Opozori tudi na problem, ki ga vidi v nacionalnem varnostnem sistemu. Po njenem mnenju je enačenje verjetnosti z nejasnostmi groženj v sistemu nacionalne varnosti RS ključna pomanjkljivost sicer etablirane in znanstveno precenjene Resolucije o strategiji nacionalne varnosti RS. K temu se relativno »nevarno« kombinira splošno sprejet koncept: »Saj se nam ne more zgoditi nič takšnega, se ne bo zgodilo« namesto: »Ne sme se nam zgoditi nič takšnega, se ne sme zgoditi.« Iz odgovora je razvidno, da oseba problem terorizma vidi kot kompleksen problem, ki bi ga bilo treba obravnavati široko in večstransko ter rezultate take obravnave potem upoštevati pri pisanju dokumentov, kot je Resolucija o strategiji nacionalne varnosti RS.

Analiza prvega vprašanja nam pokaže, da dejanska ogroženost, kot kažejo tudi uradne ocene, v RS res ni velika, vendar pa vedno obstajajo možnosti, ki jih še posebej določita preiskovalca, da do nekega terorističnega dejanja dejansko pride.

Drugo vprašanje, »Kaj dojemate pod pojmom eko terorizem?«, se dotika konkretne obravnavane tematike eko terorizma. Intervjuvancem smo najprej prepustili, da so prosto podali svoje mnenje in ideje o eko terorizmu. V nadaljevanju smo jim podali tri delitve definicij eko terorizma, ki jih omenjamo v članku, ter nadaljevali pogovor z intervjuvanci na podlagi teh delitev. Odgovori so si bili bolj različni, nihče od intervjuvancev ni menil, da je izraz eko terorizem povsem primeren za dejanja radikalnih okoljevarstvenikov, se pa nekateri strinjajo, da njihova dejanja pogojno lahko predstavljajo neko vrsto teroriziranja. Štirje intervjuvanci se strinjajo, da je izraz eko terorizem primeren za izrabo okolja za teroriziranje. Strokovnjakinja za ekološko kriminaliteto ter eden od preiskovalec menita, da izraz eko terorizem za radikalne okoljevarstvenike ni primeren in njihova dejanja ne bi umestila vanj. Ista intervjuvanca se strinjata, da dejanja radikalnih okoljevarstvenikov ne ustre-

zajo kriterijem klasične definicije terorizma ter da gre za klasična kazniva dejanja kot so požig, vandalizem, fizični napad na osebo in podobno. Enačenje omenjenih dejanj s terorizmom in obravnavanje le-teh s strožjo protiteroristično zakonodajo se jima zdi pretirano. Strokovnjakinja za ekološko kriminaliteto meni, da ekološka kriminaliteta ni eko terorizem, ker je le-ta jasno definirana, medtem ko preiskovalec v določenem segmentu ekološko kriminaliteto vidi kot teroriziranje okolja in definira eko terorizem kot dejanja, ki povzročajo neko vrsto škode na okolju.

Okoljevarstvenik meni, da je eko terorizem pojem, ki je plod vlad in velikih korporacij, s katerim skušajo očrniti okoljevarstvenike, ki jim s svojimi dejanji nemalokrat preprečijo velike zaslužke na račun okolja. Drugi preiskovalec pa dejanja radikalnih okoljevarstvenikov, čeprav jih razume, pogojno vidi kot teroriziranje oziroma neka teroristična dejanja. Strokovnjakinja za sredstva za množično uničevanje pa v odgovoru na drugo vprašanje poda znanstveni pogled na problematiko. Če pojem opazuje s primerne akademske razdalje, se ji zdi primeren, če pa ga obravnava, o njem razmišlja zadostno in potrebno celovito, pa se ji zdi premalo natančno definiran in vse prej kot zadostno in potrebno celovit, celo neprimeren, in meni, da ga ne bi mogla uporabiti za katero koli od posameznih oblik eko terorizma, ki so opredeljene v strokovni literaturi. Povedala je, da izraz eko terorizem vsebuje različne nianse terorističnega dejanja, ter da se ji še najbližje pojmu zdi ofenzivna uporaba biološkega ali kemičnega agensa, ki lahko postane ekološki problem. Po njenem mnenju pogojno tudi radikalni okoljevarstveniki izvajajo neko vrsto terorja, vendar je izraz verjetno preveč radikalen. Analiza pokaže da so si v drugem vprašanju odgovori precej različni. Medtem ko nekateri radikalnih okoljevarstvenikov nikakor ne vidijo kot eko teroriste, drugi dopuščajo pogojno možnost, da se ta izraz za njih uporabi. Ravno tako se vidijo razlike pri uporabi pojma eko terorizem za ekološko kriminaliteto. Še najbolj se intervjuvanci strinjajo v primernosti izraza za izrabo okolja ali nekih bioloških ali kemičnih snovi v namen teroriziranja. Iz analize lahko povzamemo, da je dejansko največji problem ravno v definiranju eko terorizma in nadalje tudi v razumevanju in percepciji posameznih definicij in samega pojma.

Kot bistveno ugotovitev v analizi lahko navedemo, da pojem eko terorizem lahko vsakdo vidi drugače. Definicije, napisane v strokovni literaturi, so gledane s strani vsakega posameznega intervjuvanca lahko pravilne ali pa povsem napačne. In to nam dokazuje, da je definiranje eko terorizma, podobno kot definiranje terorizma, zelo zahtevno, zapleteno in problematično.

6 ZAKLJUČEK

Največja težava predstavljene problematike pojma eko terorizem je v njegovem definiranju in določanju njegove vsebine. Zaradi nenatančne definiranosti je problematično tako označevanje nekoga za eko terorista kot tudi sama obravnava storilca.

Eko terorizem je dokaj nov izraz, ki so ga takoj ob pojavu kot vzdevek pričeli uporabljati tako tisti, ki so želeli stigmatizirati okoljske aktiviste in aktiviste za pravice živali, kot tudi tisti, ki so želeli stigmatizirati državno in gospodarsko

»nasilje« nad naravo in živalmi. Okoljevarstveni aktivisti so hitro izgubili besedno vojno, tako da je izraz eko terorizem postal retorično orožje proti radikalnim aktivistom in včasih tudi proti ostalim okoljevarstvenikom, pobudnikom okoljskih reform. Dejstvo je, da radikalni okoljevarstveniki s svojimi dejanji izvajajo kazniva dejanja, povzročajo veliko materialno škodo, psihično ustrahujejo določen krog ljudi, a vendar je treba poudariti, da so radikalni okoljevarstveniki s svojimi dejanji včasih pripomogli tudi k upočasnjevanju onesnaževanja in izkoriščanja okolja. Nasilna dejanja radikalnih okoljevarstvenikov nikakor niso opravičljiva in so celo obsojanja vredna, vendar pa menimo, da je njihovo označevanje za eko teroriste preradikalno in pregrobo, čeprav v nekaterih segmentih njihova dejanja vsebujejo kriterije, ki določajo teroristično dejanje.

Treba je poudariti besede enega od senatorjev ZDA, ki je dejal, da je v današnjem času laže priti na naslovnice, če uporabiš izraz terorizem, vendar pa je včasih kriminal zgolj kriminal. Pravi, da če je potrebna slabšalna etiketa za radikalne okoljevarstvenike, naj bodo to kriminalci, vandali, saboterji, požigalci in podobno, ne pa teroristi (Smith, 2008).

Kljub temu, da so nekatera dejanja radikalnih okoljevarstvenikov nasilna in na neki način radikalni okoljevarstveniki lahko ustrahujejo in terorizirajo določen krog nedolžnih civilistov, je izraz eko terorist za njih pretiran. Izraz je nemalokrat izrabljen s strani vlad in velikih korporacij z namenom lažjega preganjanja okoljevarstvenikov in ščitenja svojih poslov ter dobičkov. Res je, da so nemalokrat dejanja »direktne akcije« kazniva in nelegalna, vendar pa okoljevarstvenike v ta dejanja privedejo neodzivnost in nereagiranje vladnih institucij na neopravičeno in pretirano onesnaževanje in izkoriščanje okolja. Če pogledamo tri osnovne razvrstitve, katere naj bi predstavljal pojem eko terorizem (izraba okolja za teroriziranje, teroriziranje okolja ter radikalne okoljevarstvenike), bi izraz eko terorizem lahko uporabili v primeru definiranja izrabljanja okolja za teroriziranje. Torej za teroristični napad z nekakšnim biološkim ali kemičnim agensom, ali s povzročanjem škode na okolju in naravi z namenom doseganja političnih ali vojaških ciljev. Za teroriziranje okolja izraz eko terorizem ni najbolj primeren, saj naj bi šlo v tem primeru za ekološko kriminaliteto, ki pa je dokaj natančno opredeljena z državnimi in mednarodnimi akti in tako tudi preganjana. Pri uporabi izraza eko terorizem kot taktiki radikalnih okoljevarstvenikov je določitev primernosti bolj zapletena. Dejanja radikalnih okoljevarstvenikov sicer zajemajo določene elemente, ki jih najdemo v definicijah terorizma, vendar ne vseh in ne popolnoma. Izraz zato ni povsem primeren in je za kazniva dejanja storjena s strani radikalnih okoljevarstvenikov pregrob.

Pojem ekološki terorizem je zelo kompleksen ter povzroča burne razprave o njegovi uporabi in pomenu. V prispevku smo predstavili le del problema, saj je globlji problem v miselnosti ljudi in čezmernem onesnaževanju okolja ter izkoriščanju narave in živali. Jasno je, da bi ljudje brez onesnaževanja in izkoriščanja narave danes težko preživeli, vendar pa bi bilo treba biti pri tem zmernejši, predvsem pa bi morale države in velike korporacije manj gledati na velike dobičke in bolj na okolje ter okoljsko politiko in pri tem upoštevati tudi mnenje ter predloge ljudi, predvsem okoljevarstvenikov.

LITERATURA

Animal enterprise protection act of 1992. (1992). *Public Law, 102–346.* Pridobljeno na http://www.nal.usda.gov/awic/legislat/pl102346.htm

Animal enterprise terrorism act. (2006). *S. 3880.* Pridobljeno na http://www.gpo.gov/fdsys/pkg/BILLS-109s3880enr/pdf/BILLS-109s3880enr.pdf

Antiterrorism and effective death penalty act of 1996. (1996). *Public Law, 104–132.* Pridobljeno na http://www.gpo.gov/fdsys/pkg/PLAW-104publ132/pdf PLAW-104publ132.pdf

Berkowicz, M. S. (2011). Eco-terrorism/Enviro-terrorism: Background, prospects, countermeasures. V H. Alpas, S. M. Berkowicz in I. Ermakova (ur.), *Environmental security and ecoterrorism* (str. 15–29). Dordrecht: Springer.

Best, S. in Nocella, J. A. (2005). *Behind the mask: Uncovering the animal liberation front*. Pridobljeno na http://www.pmpress.org/content/fmd/files/Behind_The_Mask.pdf

Bjelopera, P. J. (2012). *The domestic terrorist threat: Background and issues for Congress.* Congressional Research Service. Pridobljeno na http://www.fas.org/sgp/crs/terror/R42536.pdf

Buell, L. (2009). What is called ecoterrorism. *Gramma: Journal of Theory and Criticism, 16,* 153–166. Pridobljeno na http://dash.harvard.edu/bitstream/handle/1/4262048/1275004626-What%20Is%20Called%20Ecoterrorism.pdf?sequence=2

Department of Justice U. S. (2007). *Goverment's sentencing memorandum.* Pridobljeno na http://www.targetofopportunity.com/government_sentencing_memo.pdf

Deshpande, N. in Howard, E. (2012). *Countering eco-terrorism in the United States: The case of 'Operation Backfire'.* College Park: National Consortium for the Study of Terrorism and Responses to Terrorism. Pridobljeno na http://www.start.umd.edu/start/publications/Countermeasures_OperationBackfire.pdf

Federal Bureau of Investigation. (2003). *Terrorism 2002–2005.* Pridobljeno na http://www.fbi.gov/stats-services/publications/terrorism-2002-2005

Helios Global. (2008). *Ecoterrorism: Environmental and animal-rights militants in the United States.* Pridobljeno na http://www.exposeanimalrights.com/images/dhs-ecoterrorism-in-us-20081.pdf

Hoek, A. (2010). Sea Shepherd Conservation Society v. Japanese Whalers, the Showdown: Who is the real villain? *Journal of Animal Law and Policy, 3,* 159–193. Pridobljeno na https://journals.law.stanford.edu/sites/default/files/print/issues/hoek.pdf

The Inkerman Group. (2007). The war on ‚eco-terror': An analysis of the use of anti-terrorism legislation on activist movements in the UK & US. *The Inkerman monitor, 3*. Pridobljeno na http://www.google.si/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0CCgQFjAA&url=http%3A%2F%2Fwww.greenisthenewred.com%2Fblog%2Fwp-content%2FImages%2Finkerman_report_ecoterror.pdf&ei=Y0ILU7DZPKTQygPzzYLgDQ&usg=AFQjCNGHUwDhvvs-J3thkGNxZsNbLtWDkw&bvm=bv.61725948,d.bGQ&cad=rja

Keller, R. D. (2008). Earth First! V *Encyclopedia of environmental ethics and philosophy* (2nd ed., str. 221–223). Pridobljeno na http://davidkeller.us/publications/Keller-Earth_First%20EEEP.pdf

Kharlamova, G. (2011). Ecoterrorism: An ecological-economic convergence. V H. Alpas, S. M. Berkowicz in I. Ermakova (ur.), *Environmental security and ecoterrorism* (str. 31–37). Dordrecht: Springer.

Kostreba, L. (1999). Oil spill remediation efforts in the Middle East. *Restoration and Reclamation Review, 4*(3), 1–5. Pridobljeno na http://conservancy.umn.edu/bitstream/59292/1/4.3.Kostreba.pdf

Law against tree spiking. (1988). *H. R., 5210.* Pridobljeno na https://www.ncjrs.gov/pdffiles1/Digitization/143053NCJRS.pdf

Liddick, D. (2006). *Eco-terrorism: Radical environmental and animal liberation movements.* London: Praeger.

Liddick, D. (2011). *Crimes against nature: Illegal industries and the global environment.* Oxford: Praeger.

Long, D. (2004). *Ecoterrorism.* New York: Facts On File.

Metscher, R. (2005). *Ecoterrorism in the U. S.* Pridobljeno na http://knowyourthreat.com/resources/Ecoterrorism+in+the+US.Online.pdf

Omelchenko, A. (2011). Environmental lead contamination as eco-terrorism and a threat to ecosystems and public health. V H. Alpas, S. M. Berkowicz in I. Ermakova (ur.), *Environmental security and ecoterrorism* (str. 83–99). Dordrecht: Springer.

Potter, W. (7. 4. 2009). 3 definitions of eco-terrorism. *Green is the new red.* Pridobljeno na http://www.greenisthenewred.com/blog/eco-terrorism-definition/1671/

Smith, K. R. (2008). "Ecoterrorism"? A critical analysis of the vilification of radical environmental activists as terrorists. *Environmental Law, 38*(2), 537–576. Pridobljeno na http://www.supportdaniel.org/files/Ecoterrorism_critical_analysis.pdf

The terrorism act. (2003). *Act No. 5*. Pridobljeno na https://www.unodc.org/tldb/showDocument.do?documentUid=8877

Transnational Terrorism, Security & the Rule of Law. (2008). *Defining terrorism*. Pridobljeno na http://www.transnationalterrorism.eu/tekst/publications/WP3%20Del%204.pdf

USA patriot act. (2001). *Public Law, 107–56.* Pridobljeno na http://www.gpo.gov/fdsys/pkg/PLAW-107publ56/pdf/PLAW-107publ56.pdf

O avtorjih:

Mario Domjanič, mag. var. E-mail: mario.domjanic@gmail.com

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

VARSTVOSLOVJE,
let. 16
št. 1
str. 37–49

Spremembe samovarovalnih ukrepov pri prebivalcih Slovenije

Branko Lobnikar, Kaja Kosec

Namen prispevka:

Zagotavljanje varnosti in zagotavljanje občutkov varnosti vedno bolj postaja tudi naloga vsakega posameznika, ki vstopa v partnerski odnos s pluralnimi institucijami formalnega družbenega nadzorstva. Namen prispevka je bilo ugotoviti, ali so se pri prebivalcih Slovenije v zadnjem desetletju spremenili vedenjski vzorci na področju samovarovalnih ukrepov, pri čemer smo poskušali ugotoviti, ali na spremembe, če do njih sploh prihaja, vpliva posameznikova percepcija varnosti.

Metode:

Za potrebe analize je bil pripravljen anketni vprašalnik, s katerim smo želeli ugotoviti, katere samovarovalne ukrepe in mehanizme posamezniki uporabljajo v svojem bivalnem okolju, zanimalo pa nas je tudi, katere od teh ukrepov so uporabljali pred desetletjem. V raziskavi, ki je bila izvedena v prvi polovici leta 2012, je sodelovalo 356 prebivalk in prebivalcev iz Slovenije, zbiranje podatkov pa je bilo izvedeno s pomočjo spletnega anketiranja (spletni portal SurveyGizmo). Kot metoda za zbiranje je bila uporabljena tehnika snežne kepe.

Ugotovitve:

Raziskava je pokazala, da se ljudje v svojem domačem kraju počutijo relativno varne. Iz rezultatov raziskave je razvidno, da prebivalci danes uporabljajo večje število varnostnih ukrepov kot pred desetimi leti. Največja odstopanja pri uporabi posameznih ukrepov so vidna pri ukrepih »dosledno zaklepanje vrat«, »dogovor s sosedi ali znanci, da spremlja vaše stanovanje v času odsotnosti«, »polno kasko zavarovanje avtomobila« in »dogovor s sosedi ali znanci, da praznijo poštni nabiralnik v času odsotnosti«. Najmanjšo uporabo samovarovalnih ukrepov je mogoče zaslediti pri ukrepu »uporaba video nadzora«, saj je velika večina ne uporablja oziroma si jo lahko privoščijo le redki. Ugotovili smo, da se ženske na splošno počutijo bolj ogrožene kot moški. Posledično tako pogosteje uporabljajo samovarovalne ukrepe.

Omejitve/uporabnost raziskave:

Pomanjkljivost raziskave je relativno majhen vzorec, kjer je razmerje med moškimi in ženskami nekoliko porušeno, omejitve pa izhajajo tudi iz metode zbiranja podatkov in starostne strukture vzorca. Kljub temu pa so rezultati raziskave uporabni kot izhodišče za nadaljnje raziskovanje.

Praktična uporabnost:

Rezultati raziskave nudijo odgovore na nekatera do zdaj redko analizirana, a pogosto postavljena vprašanja, ki zadevajo temo zagotavljanja varnosti s pomočjo samovarovalnih mehanizmov in ukrepov.

Izvirnost/pomembnost prispevka:

Gre za prvo tovrstno raziskavo v slovenskem prostoru, zato rezultati raziskave predstavljajo dodatek k obstoječim dejstvom in številnim kriminološkim viktimološkim raziskavam in raziskavam o strahu pred kriminaliteto.

UDK: 351.78(497.4)

Ključne besede: samovarovalni mehanizmi, strah pred kriminaliteto, varnost, preventivni ukrepi

Changes in Self-protective Behaviour in the Slovenian Population

Purpose:

Nowadays, ensuring safety is increasingly becoming a task of each individual trying to establish partnerships with pluralist institutions of formal social control. The purpose of this paper is to examine modifications of patterns in self-protective behaviours in Slovenia in the last decade to determine whether an individual's perception of safety affects these modifications.

Design/Methods/Approach:

For the purpose of this survey we prepared a self-conducted questionnaire to determine which self-protective measures and mechanisms were used by individuals in their living environment a decade ago and which are used today. The survey was conducted on a sample of 356 inhabitants of Slovenia in the first half of 2012. Data collection was carried out through a web survey using a snowball technique.

Findings:

The research has shown that people feel relatively safe in their living environment. Compared to their behaviour a decade ago, the respondents report increased use of security measures. Most differences are observed in the following self-protective behaviours: „consistent door locking", „arrangement with neighbours or acquaintances to monitor a person's home during their absence", „full car insurance", and "arrangement with neighbours or acquaintances to collect mail during the time of absence". We found that women generally feel more at risk than men. As a result, women are more likely to use self-protective actions.

Research Limitations/Implications:

A drawback of the research is the relatively small sample with an unequal men/women ratio, further restrictions resulting from the applied data collection methods and the age structure of the sample. Nevertheless, the research results are useful as a starting point for further research.

Practical Implications:

The survey results provide answers to some currently rarely analysed, but frequently asked questions concerning the topic of providing security through self-protective mechanisms and measures.

Originality/Value:

This study is the first of the kind in Slovenia, so its results represent a supplement to the existing findings in the field of criminological and victimological research and study of fear of crime.

UDC: 351.78(497.4)

Keywords: self-protective behaviour, fear of crime, safety, preventive measures

1 UVOD

Izbor okolja, v katerem bomo bivali, je pogojen z željami, potrebami, cilji, vrednotami, pričakovanji in osebnostnimi značilnostmi posameznika. Odločitev, kaj bo vplivalo na odločitev o kraju prebivanja, je odvisna od vsakega posameznika (Zupan, 2009). Življenje na podeželju lahko opišemo kot mirno in mnogokrat kot nasprotje hrupu in hitremu življenju urbanega vrveža. Občutek pripadnosti in občutek solidarnosti sta za človekovo osebnostno stabilnost zelo pomembna in to se na podeželju kaže tudi v obliki pomoči sovaščanu. Posledično se v takem okolju počutimo varneje, kar pa je tudi ena izmed osnovnih potreb posameznika kot družbenega bitja. Za razliko od podeželja so medosebni odnosi v urbanem okolju bolj odtujeni, manj pristni, bolj instrumentalni in interesno pogojeni. Haralambos in Holborn (2005: 106–117) zagovarjata stališče, da so družbe velikokrat zaznamovane tudi s številnimi negativnimi pojavi, ki so povezane z željo po hitrem in dobrem zaslužku, po hitrem vzpenjanju v hierarhiji politične, družbene in ekonomske moči. Te želje zmanjšujejo družbeno stanovitnost, socialno varnost in trajno organiziranost posameznih družbenih skupin. Vse to vodi v razkroj lokalnih skupnosti in družin ter več nestrpnosti in frustracij posameznikov in družbe. V situacijah negotovosti se razvijajo tudi možnosti za krepitev strahu pred tem, da bi postali žrtev kriminalitete. Namen prispevka je tako ugotoviti, ali so se pri prebivalcih Slovenije v zadnjem desetletju spremenili vedenjski vzorci na področju samovarovalnih ukrepov, pri čemer bomo poskušali ugotoviti, ali na spremembe, če do njih sploh prihaja, vpliva posameznikova percepcija varnosti.

2 SAMOVAROVALNO VEDENJE KOT NAČIN PREPREČEVANJA VIKTIMIZIRANOSTI IN KOT POSLEDICA STRAHU PRED VIKTIMIZIRANOSTJO

Strah pred kriminaliteto je pojem, ki ga je treba obravnavati interdisciplinarno, saj je vpet v različne dimenzije vsakdanjika, med katerimi sta tudi kakovost in količina življenja posameznika v povezavi z učinkovitostjo in produktivnostjo življenja

in vsakodnevnih obveznosti (Govekar, 2010). Živimo v času, kjer se soočamo z različnimi varnostnimi problemi in posameznik vedno bolj verjame, da so ti problemi vedno bolj pereči ter vedno manj obvladljivi. Vedno več študij kaže, da pa obstajajo določeni dejavniki (npr. bogastvo, zdravje, kakovost življenja), ki močno zmanjšujejo strah pred kriminaliteto (Meško, Petrovec, Areh, Muratbegović in Rep, 2006). Kljub temu se strah vseeno prepleta z množico strahov in negotovosti, ki se vsakodnevno zbujajo v nas. Jevšek (2007) ugotavlja, da je strah v osnovi le posameznikovo čustvo, ki ga uporabljamo, da se izognemo nevarnostim. Meško (1999a, 1999b) ugotavlja, da je eden izmed ključnih problemov merjenja strahu pred kriminaliteto v nejasnih opredelitvah določenih pojmov in da je merjenje odvisno tudi od vrste kaznivih dejanj na določenem območju. Ljudje se namreč veliko bolj bojijo kaznivih dejanj, kot so ropi, napadi ali posilstva, kot pa kriminalitete belega ovratnika ali premoženjske kriminalitete. Ugotavlja tudi, da je precej težko meriti čustvovanje posameznika, saj prihaja do vprašanja, ali bi potem zadovoljili kriterije ustreznosti, veljavnosti in objektivnosti.

Zaradi različnega mišljenja in vrste razlik med spoloma ta razlika pride do izraza tudi v načinu dojemanja kriminalitete. Raziskave kažejo, da je strah pred kriminaliteto najbolj prisoten pri skupinah ljudi, ki so na splošno bolj ranljive (ženske, starejši ljudje), čeprav policijske statistike kažejo, da sta ti dve skupini ljudi najmanjkrat viktimizirani (Policija, 2011). Vzrok za omenjeno neskladje so raziskovali številni kriminologi in ga poskušali razložiti na različne načine (Hanrahan in Gibbs, 2004). Ženske se običajno počutijo bolj ogrožene in bolj zaskrbljene kot moški, čeprav je uradno splošno potrjeno, da so žrtve kaznivih dejanj z znaki nasilja najpogosteje moški. Enako velja tudi za starejše ljudi, ki se počutijo mnogo bolj ogrožene, kljub temu da so mlajši pogosteje viktimizirani (Areh in Meško, 2003). Pri strahu pred kriminaliteto ne moremo niti mimo vpliva medijev. Svet se nam zdi poln nasilja, saj nam informacije o kriminalu prinašajo mediji vseh vrst – časopisi, televizija, predvsem pa internet. Mediji najpogosteje prinašajo le najbolj spektakularne informacije, kar se najuspešneje trži. Senzacionalistični prijem pri obravnavanju kriminalitete je vzrok, da se v naši predstavi izoblikuje podoba, da je nasilja desetkrat več, kakor ga je po statističnih podatkih. To pa samo še povečuje strah med ljudmi in občutek, da nikjer več nismo varni. To pa seveda vpliva na naše vedenje in mišljenje (Bučar-Ručman, 2009).

Ljudje za svojo varnost skrbijo na različne načine. Včasih z obzidji, dvižnimi mostovi, rešetkami, danes pa z vedno bolj naprednimi tehnikami mehanskega varovanja, saj je to ena najosnovnejših oblik varovanja lastnine in premoženja pred vlomilci (Sintal, 2012). Mednje štejemo večinoma sredstva, ki storilcem onemogočajo dostop do varovanega objekta ali njegove okolice. Njihova učinkovitost in kakovost sta odvisna od časa, ki ga storilec potrebuje, da napravo ali protivlomno sredstvo onesposobi. Tudi policija aktivno spodbuja samozaščitno vedenje prebivalcev. »Za boj proti kriminalu je policija, poleg represivnega dela, izoblikovala tudi preventivne programe, s katerimi želijo spodbuditi in dvigniti samozaščitni nivo posameznikov. Izkušnje kažejo, da lahko s preventivnim ravnanjem občutno zmanjšamo možnost vloma, ali celo odvrnemo storilca. Za preprečitev vloma so tako zelo pomembne mehanske, tehnične in fizične oblike varovanja.« (Policija, 2011)

Pod mehanska zaščitna sredstva štejemo predvsem protivlomna vrata, ograje, različne ključavnice, alarmne naprave, videokamere itd. Poleg mehanskega varovanja je pametno razmišljati tudi o tehničnem varovanju, kot dopolnilnem varovanju, oziroma dodatni zaščiti, za katero poskrbijo predvsem varnostne službe za ustrezno plačilo (Čas, 2012). Sistemi tehničnega varovanja so naprave, ki služijo za neposredno preprečevanje vlomov, ropov in drugih tatvin, kaznivih in škodljivih pojavov na področju premoženjske kriminalitete, saj storilce kaj hitro prestrašijo ali jim onemogočijo dostop do želenega zaklada. Med sisteme tehnične zaščite in varovanje objektov uvrščamo (Golob, 1997) protivlomne sisteme (sem spadajo ograje, rešetke, zaščitne mreže, sredstva za zaščito oken in vrat, ključavnice ter protivlomne omare, trezorji in blagajne), sisteme nadzora gibanja (postopki za identifikacijo in pristopno kontrolo), alarmne sisteme za odkrivanje in javljanje nepooblaščene prisotnosti ter sistemi za odkrivanje in javljanje požara ter sisteme video nadzora. Poleg mehanskega in tehničnega varovanja poznamo tudi različne oblike fizičnega varovanja, za katere skrbijo predvsem varnostne službe v skladu z zakonodajo na varovanem območju, za ustrezno plačilo, ki ga ne zagotavlja država (Čas, 2012). Še posebej je to pomembno za ustanove in posameznike, ki poslujejo z velikimi količinami denarja in drugimi predmeti visokih vrednosti. Za tako obliko varnosti skrbijo predvsem ustrezno strokovno usposobljeni varnostniki v skladu z Zakonom o zasebnem varovanju iz leta 2011 (Sotlar in Čas, 2011).

Zagotavljanje varnosti in zagotavljanje občutkov varnosti vedno bolj postaja tudi naloga vsakega posameznika. Iz podrejenega objekta varnostnih ukrepov vedno bolj postaja partner institucijam formalnega družbenega nadzorstva. Namen prispevka je bilo ugotoviti, ali so se v zadnjem desetletju pri prebivalcih spremenili vedenjski vzorci na področju samovarovalnih ukrepov, pri čemer smo poskušali ugotoviti, ali na spremembe, če do njih sploh prihaja, vpliva posameznikova percepcija varnosti.

3 UPORABLJENE METODE, OPIS POSTOPKA IN VZORCA

3.1 Postopek

Za potrebe raziskave je bil izdelan vprašalnik, s katerim smo želeli izvedeti pogostost uporabe samovarovalnih ukrepov pri prebivalcih. Tako je bila izdelana lista 19 možnih samovarovalnih ukrepov (seznam vseh teh ukrepov je predstavljen na sliki 1), kjer so lahko anketiranci odgovarjali, ali jih uporabljajo ali ne. Pri tem smo jih vprašali, ali so jih uporabljali v preteklosti (pred 10 leti) in ali jih uporabljajo zdaj. Poleg tega smo jim zastavili vprašanje, kako varno so se počutili v svojem bivalnem okolju pred 10 leti in kako varno se počutijo zdaj. Svoje odgovore so označevali na petstopenjski Likertovi lestvici, pri čemer je višja številka pomenila tudi višjo stopnjo občutka varnosti. Poleg navedenih vsebinskih vprašanj smo jim zastavili tudi nekaj demografskih, ki smo jih uporabili v analizi.

Zbiranje podatkov smo izvedli po metodi snežne kepe. Spletni vprašalnik je bil objavljen na spletnem portalu SurveyGizmo, s pomočjo obvestila preko elektronske pošte ter objave spletne povezave na družabnih omrežjih pa smo povabili

prebivalce Slovenije, da sodelujejo pri izpolnjevanju vprašalnika. Anketiranje je potekalo v obdobju med 28. julijem in 15. avgustom 2012.

3.2 Opis vzorca

V raziskavo je bilo vključenih 356 oseb, od tega 139 moških in 217 žensk. Povprečna starost moških anketirancev znaša 33,77, ženskih pa 28,88. Povprečna starost vseh anketiranih pa 30,84. Največ sodelujočih, kar polovica, jih ima srednješolsko izobrazbo, dobra tretjina višjo, visoko ali univerzitetno izobrazbo, ena šestina jih ima magisterij ali doktorat znanosti, le trije anketiranci pa so imeli v času izpolnjevanja ankete osnovnošolsko izobrazbo.

3.3 Omejitve raziskave

Omejitve, ki jih je treba upoštevati v raziskavi, se nanašajo na relativno majhnost vzorca. Rezultatov zaradi neuravnoteženosti in velikosti vzorca ne moremo posploševati na celotno populacijo, ker bi raziskava za izboljšanje verodostojnosti v prvi vrsti potrebovala večji vzorec, ki bi bil vsaj po spolu bolj uravnotežen. Poleg tega je treba upoštevati, da nekateri sodelujoči v raziskavi zaradi svoje trenutne starosti težko ocenjujejo obdobje pred desetimi leti. Čeprav smo anketirance spraševali o njihovih aktivnostih pri uporabi samovarovalnih ukrepov, je potrebno upoštevati, da se za uporabo samovarovalnih ukrepov po navadi ne odločajo posamezniki, ampak družine/skupnosti, v katerih živijo ti posamezniki. Kljub vsemu pa rezultati, po našem mnenju, pomenijo vsaj dobro izhodišče za nadaljnje raziskovalno delo.

4 ANALIZA IN INTERPRETACIJA REZULTATOV

Anketirancem smo na začetku postavili vprašanje, ki se nanaša na njihovo zaznavo varnosti v kraju, kjer prebivajo. Postavili smo jim dve vprašanji: naj ocenijo, kako varno so se počutili v svojem kraju bivanja pred desetimi leti in kako varno se počutijo v kraju, kjer prebivajo zdaj. Rezultati so predstavljeni v tabeli 1 v nadaljevanju.

Tabela 1: Primerjava ocene varnosti bivanja

		Povprečje	*n*	St. odklon	Standardna napaka povpr.
Par 1	V soseski, kjer sem živel pred desetimi leti, sem se počutil varno.	4,46	356	,701	,037
	V soseski, kjer živim, se počutim varno.	3,94	356	,931	,049

V tabeli 1 lahko vidimo, da je ocena občutka varnosti v obeh obdobjih nadpovprečna (na lestvici od 1 do 5, kjer 1 pomeni, da se anketiranci sploh ne strinjajo s trditvijo, 5 pa, da se s trditvijo močno strinjajo), pri čemer pa vidimo, da je ocena

za obdobje pred 10 leti višja, kot je ocena za čas, ko je potekalo anketiranje. Želeli smo ugotoviti, ali so razlike statistično značilne, zato smo izvedli primerjavo povprečij v parih (parni *t*-test). Rezultati analize so prikazani v tabeli 2 v nadaljevanju.

	Primerjalne razlike					*t*	df	*p*
	Povprečje	St. odkl.	St. napaka povpr.	95 % interval zaupanja				
				spodnji	zgornji			
PRED 10 LETI VS. DANES	,525	,883	,047	,433	,617	11,225	355	,000

Tabela 2: Primerjava razlik med ocenami varnosti bivanja pred 10 leti in zdaj

V tabeli 2 vidimo, da prihaja do statistično značilnih razlik v oceni varnosti bivanja pred 10 leti in zdaj ($t = 11{,}22$; $p = 0{,}000$). Anketiranci poročajo, da so se pred desetimi leti počutili varneje, kot se počutijo zdaj, razlike pa so tudi pomembne, saj je razlika med povprečnimi vrednostmi več kot 0,5. Lahko rečemo, da so anketiranci svojo varnost bivanja v soseski, kjer so živeli pred desetimi leti, ocenili z dobro 4 (ocena nekje med prav dobro in odlično), v času anketiranja pa so v povprečju ocenili stopnjo varnosti bivanja v svoji soseski s slabo 4. Pri tem pa je treba dodati, da je modus (najbolj pogosta ocena) pri obeh ocenah vedno 4.

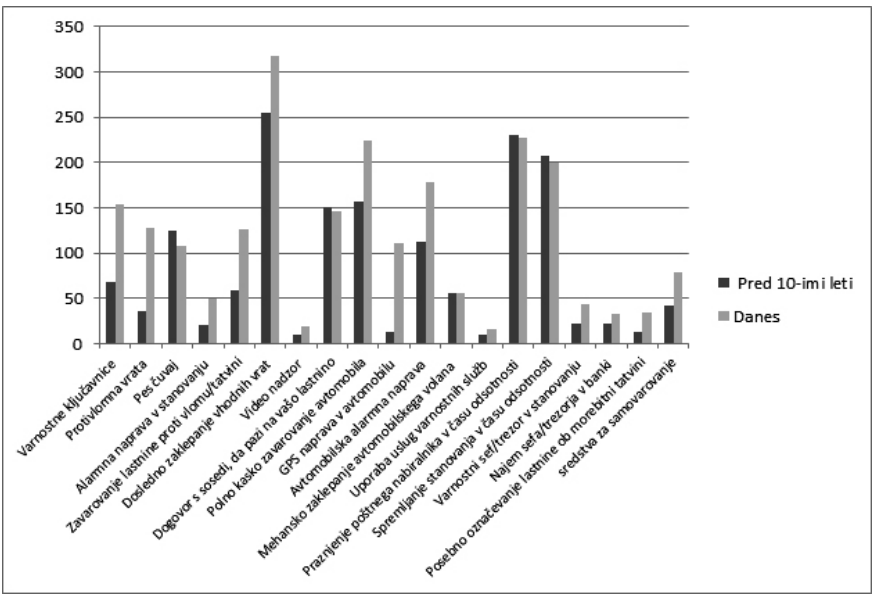
Zanimalo nas je, ali kraj bivanja vpliva na oceno varnosti. Zato smo opravili analizo variance (ANOVA) za odvisno spremenljivko »ocena varnosti bivanja v soseski pred 10 leti« ter »krajem bivanja pred 10 leti«. Pri opredelitvi kraja bivanja so anketiranci lahko izbirali med štirimi možnimi odgovori: vas, manjši kraj, manjše mesto, večje mesto. Analiza je pokazala, da med omenjenimi skupinami ne prihaja do statistično značilnih razlik v oceni varnosti bivanja ($p = 0{,}827$), kar pomeni, da kraj bivanja ni statistično značilno vplival na oceno varnosti bivanja. Enako analizo smo izvedli tudi za oceno varnosti v sedanjem kraju bivanja. Kraj bivanja se tudi v tem primeru ni izkazal za dejavnik, s katerim bi lahko pojasnjevali razlike v oceni varnosti bivanja ($p = 0{,}803$). Anketiranci se enako varno počutijo pri bivanju na vasi (povprečna vrednost = 3,9) ali pa v velikem mestu (povprečna vrednost = 3,97). Še najnižja povprečna vrednost je bila ugotovljena pri anketirancih, ki so bivali v manjšem kraju (3,8), vendar, kot rečeno, razlike niso statistično značilne. Rezultati naše raziskave tako ne potrjujejo prepričanj, da je občutek varnosti v mestu manjši kot na vasi.

V nadaljevanju smo anketirance vprašali, ali so pred desetimi leti v stanovanju/hiši, kjer so bivali, uporabljali katerega od naštetih varovalnih mehanizmov oziroma samovarovalnih vedenj? Našteli smo 19 različnih stvari, anketiranci pa so lahko odgovorili z »DA« ali »NE«. Zatem smo za istih 19 samovarovalnih ukrepov/mehanizmov vprašali, ali jih uporabljajo zdaj. Rezultati so prikazani na sliki 1 v nadaljevanju.

Iz slike 1 je razvidno, da so anketirani pred desetimi leti varnostne ukrepe uporabljali le v manjši meri, pa še tu je med posameznimi ukrepi prihajalo do opaznih odstopanj. Še najbolj dosledno so zaklepali vrata in organizirali pobiranje pošte v času njihove odsotnosti, če pa k temu dodamo še dogovor s sosedi in kasko zavarovanje avtomobila, ki krije tudi tatvino, pa smo našteli tudi najbolj

pogoste samovarovalne aktivnosti pred desetletjem. Ugotovimo lahko, da se je frekvenca uporabe samovarovalnih ukrepov v zadnjem desetletju povečala. Pri vseh ukrepih, razen pri videonadzoru, se je frekvenca povečala, še najbolj opazno pri aktivnostih, ki niso povezana z investiranjem (na primer dosledno zaklepanje vhodnih vrat, dogovor s sosedi), ali pa so te investicije manjše (na primer nakup varnostnih ključavnic, zavarovanje škodnega primera ali pa nakup psa, ki je lahko tudi pes čuvaj).

Slika 1: Primerjava pogostosti uporabe samovarovalnih mehanizmov



Da bi ugotovili, ali prihaja do statistično značilnih razlik pri uporabi varnostnih mehanizmov oziroma ukrepov v preteklosti in danes, smo izračunali sumarno spremenljivko, tako da smo sešteli frekvence uporabe varnostnih mehanizmov pred desetimi leti in zdaj. Rezultat analize je prikazan v tabeli 3 v nadaljevanju, kjer vidimo, da je bila povprečna vrednost uporabe varovalnih mehanizmov pred desetimi leti 4,5, sedaj pa je 6,4.

Tabela 3: Primerjava pogostosti uporabe varnostnih mehanizmov (UVM)

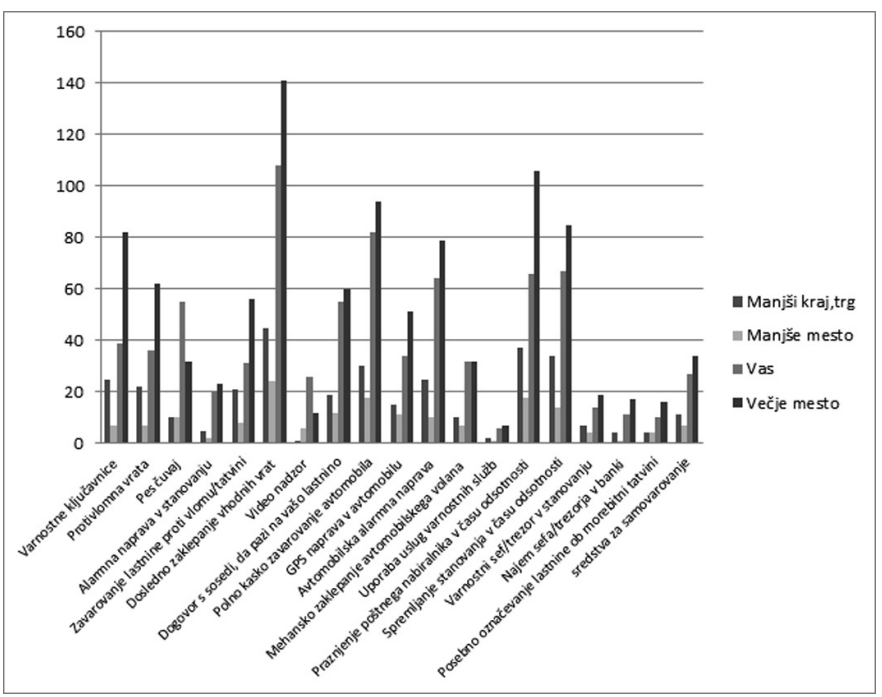
		Povprečje	*n*	St. odklon	Standardna napaka povpr.
Par 1	sum_UVM_pred_10 leti	4,5	356	2,371	,126
	sum_UVM_danes	6,4	356	3,200	,170

V tabeli 4 je prikazana tudi analiza statističnih razlik med pogostostjo uporabe samovarovalnih mehanizmov pred desetimi leti in danes. Ugotovimo lahko, da so razlike statistično značilne in da se je frekvenca uporabe samovarovalnih mehanizmov močno povečala (kar smo videli že na sliki 1).

Povprečje		Primerjalne razlike					*t*	df	*p*
		St. odkl.	St. napaka povpr.	95 % interval zaupanja					
				spodnji	zgornji				
Par 1	sum_UVM_ 10 let vs. sum_UVM_ DANES	– 1,873	2,767	,146	– 2,162	– 1,585	– 12,77	355	,000

Tabela 4: Primerjava razlik v pogostosti uporabe varnostnih mehanizmov (UVM)

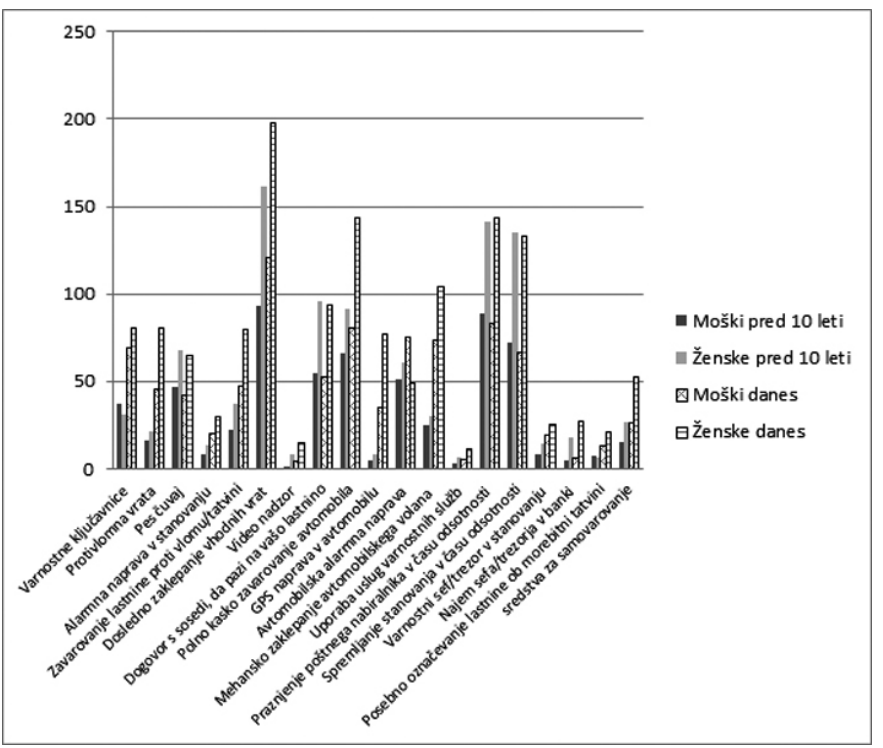
V nadaljevanju smo testirali predpostavko, da med občutkom varnosti in samovarovalnimi ukrepi obstaja statistično značilna povezanost. Rezultati so zanimivi. Ko smo izvedli analizo povezanosti (Pearsonov korelacijski koeficient) med občutkom varnosti in uporabo samovarovalnih ukrepov pred desetimi leti, nismo ugotovili statistično značilne povezanosti ($r = – 0,076$; $p = 0,125$). Sklenemo lahko, da uporabo samovarovalnih ukrepov pred desetletjem ne morem pojasniti s posameznikovo oceno varnosti bivanja v soseski. Pri analizi povezanosti uporabe samovarovalnih ukrepov in občutki varnosti v času anketiranja pa smo ugotovili statistično značilno in negativno povezanost ($r = – 0,189$; $p = 0,000$). Anketiranci, ki se počutijo manj varne v svojem bivalnem okolju, bolj pogosto uporabljajo samovarovalne ukrepe. Velja seveda tudi obratno: če se oseba v svojem bivalnem okolju počuti varno, bo tudi manj pogosto uporabila samovarovalne ukrepe. Na sliki 2 v nadaljevanju pa so predstavljeni rezultati primerjave uporabe samovarovalnih ukrepov med sedanjim krajem bivanja.



Slika 2: Uporaba samovarovalnih ukrepov glede na kraj bivanja

Anketiranci iz večjih mest najbolj pogosto uporabljajo samovarovalne ukrepe, najredkeje pa ljudje iz manjših krajev. Rezultat kaže na to, da v večjih mestih najpogosteje uporabljajo samovarovalne mehanizme. Razlike bi lahko pripisali dejstvu, da se ljudje v manjših krajih večinoma poznajo med seboj, si zaupajo, si pomagajo med seboj in se zato redkeje odločajo za uporabo dodatnih samovarovalnih mehanizmov (z izjemo najbolj običajnih in tudi najpogostejših). Je pa zanimivo, da je presenetljivo visoko stopnjo uporabe samovarovalnih ukrepov mogoče opaziti v vaseh. Rezultat bi lahko interpretirali tako, da bi strnjenosti naselja, kjer obstaja pristna interakcija med prebivalci (manjši kraj, trg), pripisali tudi odločitev za samovarovalne ukrepe. Na vasi te strnjenosti ni in vsak prebivalec mora sam poskrbeti za svojo varnost. Zato lahko opazimo zanimiv rezultat: vedenje prebivalcev na vaseh je zelo podobno prebivalcem v velikih mestih in odstopa od tistih, ki prebivajo v manjših krajih oziroma trgih.

Slika 3: Uporaba samovarovalnih ukrepov glede na spol – včasih in danes



V uvodu v prispevek smo omenili tudi razlike v ocenah ogroženosti glede na spol. Na sliki 3 so prikazani rezultati uporabe samovarovalnih ukrepov glede na spol anketiranega, in sicer za obdobje pred desetimi leti in za čas izvedbe anketiranja. Na sliki 3 lahko opazimo razlike v pogostosti uporabe samovarovalnih ukrepov. Ženske se na splošno počutijo bolj ogrožene kot moški ($t = 2{,}69$; $p = 0{,}007$; povprečje moški = 4,10; povprečje ženske = 3,83), kar je bilo tudi pričakovano. Pričakovali bi, da zaradi večjega strahu in hkrati večje skrbi za varnost v skupno-

sti ženske pogosteje uporabljajo samovarovalne ukrepe kot moški. Tako pregled pogostosti odgovorov kaže, da ženske pogosteje zaklepajo vrata in redno skrbijo za varnost in nadzor stanovanja v času odsotnosti.

5 RAZPRAVA IN ZAKLJUČEK

V prispevku smo analizirali spremembe na področju samovarovalnih ukrepov prebivalcev v zadnjem desetletju. Izhajali smo iz predpostavke, da je za lastno varnost vedno bolj odgovoren vsak posameznik sam in se to odraža tudi v njegovem samovarovalnem vedenju. Pravzaprav je samovarovalno vedenje prebivalcev osnovni pogoj za uspešno delo policije, zato policija tudi spodbuja tovrstno vedenje.

Rezultate raziskave bi lahko strnili v nekaj ugotovitev. Čeprav zasebnovarnostna industrija ponuja pisano množico možnih mehanizmov in ukrepov za samovarovalno vedenje, so med prebivalci še vedno najpogosteje uporabljeni klasični ukrepi od zaklepanja vrat, sosedska samopomoč in nadzor, uporaba varnostnih ključavnic ter zavarovanje nastanka potencialnega škodnega primera. Tisto, kar smo ugotovili, je, da prebivalci zelo redko uporabljajo usluge zasebnovarnostnih podjetij, video nadzor ali kakšno drugo visokotehnološko rešitev ali pa rešitev, ki ni povezana s tradicijo okolja, kjer prebivajo (na primer posebno označevanje lastnine proti tatvini, alarmna naprava v stanovanju, GPS naprava v avtomobilu). Ne glede na visoko stopnjo ocene varnosti v bivalnem okolju pa smo ugotovili, da je strah pred kriminaliteto začel vplivati tudi na samovarovalne ukrepe prebivalcev. Če pred desetimi leti nismo ugotovili povezanosti med občutkom varnosti in samovarovalnimi ukrepi, pa tega zdaj ni več – na uporabo različnih samovarovalnih ukrepov vpliva tudi občutek varnosti oziroma strah pred viktimiziranostjo. Pri tem smo zanimivo ugotovili, da kraj bivanja ne vpliva na analizirano vedenje, pri čemer najmanj samovarovalnih ukrepov zaznamo v manjšem kraju oziroma trgu – gre za skupnost, za katero je značilna fizična bližina, visoka stopnja medsebojnega poznavanja in tudi razvit občutek za pomoč. Gre za območje, kjer je neformalni nadzor skupnosti tisti, ki nadomešča samovarovalne aktivnosti, ki so bolj značilne za individualizirano mestno okolje ali pa redko poseljeno vaško okolje. Eden od zanimivih rezultatov raziskave je prav podobnost v uporabi samovarovalnih ukrepov med mestnim in vaškim okoljem, pri čemer kljub vsemu v mestnem okolju ugotavljamo tudi najpogostejšo uporabo samovarovalnih ukrepov.

Ne glede na pomanjkljivosti, ki izhajajo iz narave vzorca in vzorčenja, prinaša predstavljena raziskava nekaj zanimivih ugotovitev, ki jih je mogoče uporabiti tako v okviru preventivne dejavnosti institucij formalnega nadzorstva kot v okviru proučevanja vedenja ljudi v vedno bolj negotovem okolju. Ponovno se je namreč izkazalo, da se ljudje obrnejo k tehniki in samovarovalnim ukrepom takrat, ko nadzorstvene funkcije ne izvaja skupnost, v kateri živijo. Varnostna industrija sicer lahko promovira uporabo samovarovalnih ukrepov, tudi preko krepitve strahu pred kriminaliteto, vendar resničnega zaščitnega dejavnika ne predstavlja varnostna ključavnica ali dobro zavarovanje, temveč dobro delujoča skupnost, ki poskrbi za to, da se ljudje v njej počutijo varne. S tem pa upada tudi potreba po kaj več kot po doslednem zaklepanju vhodnih vrat, sosedski pomoči in samovarovalni skupnosti.

LITERATURA

Areh, I. in Meško, G. (2003). Strah pred kriminaliteto v urbanih okoljih. *Revija za kriminalistiko in kriminologijo, 58*(3), 256–264.

Bučar-Ručman, A. (2009). An overwiew of research on media reports about crime and insecurity issues in Slovenia. V G. Meško, T. Cockcroft, A. Crawford in A. Lemaitre (ur.), *Crime, media and fear of crime* (str. 79–103). Ljubljana: Faculty of Criminal Justice and Security.

Čas, T. (2012). *Zasebno varstvo: zasebno varovanje in detektivska dejavnost: študijsko gradivo za študente univerzitetnega programa FVV v Ljubljani.* Ljubljana: Čas – Zasebna šola za varnostno izobraževanje.

Govekar, E. (2010). *Stališča o kriminaliteti, nevarnostih, tveganjih in ogroženosti v sodobni družbi – javnomnenjska raziskava* (Magistrsko delo). Ljubljana: Fakulteta za varnostne vede.

Golob, R. (1997). *Sistemi zaščite in varovanja oseb in premoženja*. Ljubljana: samozaložba.

Hanrahan, K. in Gibbs, J. J. (2004). Fear of crime: Its meaning in the lives of elderly women. V C. T. M. Coston (ur.), *Victimizing vulnerable groups: Images of uniquely high-risk crime targets* (str. 83–96). Westport: Praeger.

Haralambos, M. in Holborn, M. (2005). *Sociologija – teme in pogledi.* Ljubljana: DZS.

Jevšek, A. (2007). Strah pred kriminaliteto in odnos do kaznovanja v kontekstu sodobnih nevarnosti, tveganj in negotovosti. V B. Lobnikar (ur.), *8. slovenski dnevi varstvoslovja*. Ljubljana: Fakulteta za varnostne vede.

Meško, G. (1999a). Občutki ogroženosti, strah pred kriminaliteto in policijsko preventivno delo. *Varstvoslovje, 1*(1), 30–34.

Meško, G. (1999b). Strah pred kriminaliteto – perspektive in dileme. *Socialna pedagogika, 3*(2), 99–108.

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.

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

Sintal. (2012). *Da alarm ne bo zatajil: redno vzdrževanje in prilagajanje sistemov tehničnega varovanja*. Pridobljeno na http://www.sintal-varnost.si/da-alarm-ne-bo-zatajil-redno-vzdrzevanje-in-prilagajanje-sistemov-tehnicnega-varovanja/

Sotlar, A. in Čas, T. (2011). Analiza dosedanjega razvoja zasebnega varovanja v Sloveniji – med prakso, teorijo in empirijo. *Revija za kriminalistiko in kriminologijo, 62*(3), 227–241.

Zupan, S. (9. 6. 2009). Prednosti in slabosti življenja v mestnem in podeželskem okolju. *Slonep.net.* Pridobljeno na http://www.slonep.net/pred-gradnjo/lokacija/novice/prednosti-in-slabosti-zivljenja-v-mestnem-in-podezelskem-okolju

O avtorjih:

Dr. Branko Lobnikar, izredni profesor za področje upravljanja varnostnih organizacij na Fakulteti za varnostne vede UM. Raziskovalno se ukvarja s področjem vedenja ljudi v povezavi z varnostjo ter z organizacijo in upravljanjem različnih varnostnih organizacij. E-mail: branko.lobnikar@fvv.uni-mb.si

Kaja Kosec, univerzitetna diplomirana varstvoslovka, študentka magistrskega študija na Fakulteti za varnostne vede.

VARSTVOSLOVJE,
let. 16
št. 1
str. 50–67

Dejavniki sprejemanja odločitev pri urejanju učinkovite informacijske varnosti v organizacijah

Kaja Prislan, Igor Bernik

Namen prispevka:

V preglednem znanstvenem prispevku analiziramo aktualne varnostne trende in sociološke ter psihološke ovire, s katerimi se sooča varnostni management, z namenom pojasniti dileme pri zagotavljanju informacijske varnosti. V času negotovih razmer v poslovnem okolju postaja informacijska varnost vse pomembnejši poslovni proces. Učinkovitost je pogojena z različnimi okoljskimi, strukturnimi in osebnostnimi dejavniki, ki jih je potrebno upravljati, če se želi ustrezno obvladovati tveganja, ki ogrožajo obstoj organizacij.

Metode:

Analiza varnostnih trendov je izvedena s pregledom aktualnih mednarodnih raziskav o trenutnem stanju informacijske varnosti. Prav tako je bil izveden pregled teorij, ki pojasnjujejo vpliv psiholoških dejavnikov na odločitvene procese. S sintezo ugotovitev smo izoblikovali predpostavke o vzrokih neracionalnih odločitev, teoretične pristope pa smo nadgradili z njihovo umestitvijo v organizacijsko in varnostno področje.

Ugotovitve:

Ugotavljamo, da organizacije funkcije informacijske varnosti ne razvijajo ustrezno. Pregled aktualnih raziskav je pokazal, da se organizacije pogosto neučinkovito odzivajo na povečana varnostna tveganja, saj jim to onemogočajo neugodne poslovne razmere, strokovna nepodkovanost in tradicionalna vodstvena mentaliteta, spremembe na področju varnostnih rešitev in kognitivne pristranskosti pri odločevalcih. Prav tako ugotavljamo, da je učinkovitost informacijske varnosti vse bolj pogojena z netehničnimi ukrepi, pri čemer največjo vlogo odigra usposobljen, dobro razvit in strateško naravnan varnostni management.

Praktična uporabnost:

Varnostni trendi, ki jih predstavljamo v prispevku, za večino sodobnih organizacij predstavljajo velik izziv pri doseganju poslovne uspešnosti. S prispevkom želimo opozoriti na sodobne varnostne dileme in prispevati k večji ozaveščenosti odgovornega managementa. Ponujamo tudi izhodiščne točke za učinkovito soočanje s kognitivnimi ovirami pri sprejemanju odločitev.

Izvirnost/pomembnost prispevka:

Prispevek je aktualen, saj analizira najnovejše raziskave o informacijski varnosti in na osnovi tega predstavlja sodobne trende. Prav tako je izviren, ker združuje spoznanja s področja psihologije tveganj in odločitev ter informacijske varnosti v organizacijski kontekst.

UDK: 004.056:005

Ključne besede: informacijska varnost, organizacija, varnostni trendi, psihologija tveganj, varnostni management, odločitveni procesi

Decision-making Factors Contributing to the Management of Information Security in Organisations

Purpose:

Information security is becoming an ever more important business process in this period characterised by uncertainty in the business environment. Its efficiency depends on various environmental, structural, and personal factors which need to be managed in order to adequately control all risks threatening organisations' survival. This paper analyses current security trends, as well as sociological and psychological obstacles in security management, with a view to clarifying different dilemmas related to the provision of information security.

Design/Methods/Approach:

The analysis of security trends was conducted on the basis of an overview of current international research on the present state of play in the field of information security. It also includes an overview of theories explaining the impact of psychological factors on decision-making processes. Assumptions regarding the reasons for irrational decisions were drawn by performing the synthesis of findings, while theoretical approaches were upgraded by placing them in the organisational and security fields.

Findings:

The authors find that organisations are not developing the function of information security in an adequate manner. The overview of current research shows that organisations are often inefficient in their response to higher security risks, since they are prevented from doing so by unfavourable business conditions, lack of expertise, traditional management mentality, changes in the field of security-related solutions and cognitive bias found in decision-makers. The authors also find that the efficiency of information security is ever more dependent on non-technical measures, whereby trained, well-developed and strategically-oriented security management plays a crucial role.

Practical Implications:

For the majority of modern organisations, security trends presented in this paper represent a great challenge in terms of achieving business success. This paper wishes to draw attention to contemporary security-related dilemmas and raise the awareness of responsible management. The paper also provides several starting points enabling an efficient confrontation with cognitive obstacles in the course of decision-making.

Originality/Value:

This paper is up-to-date, as it analyses the latest research into information security and uses such analysis to present contemporary trends. It is also original, since it combines findings from the fields of the psychology of risk and decision-making, as well as from information security, and places them in organisational context.

UDC: 004.056:005

Keywords: information security, organisation, security trends, psychology of risk, security management, decision-making processes

1 UVOD

Trenutno stanje v poslovnem okolju, ki zajema npr. velika poslovna tveganja, finančno negotovost in bolj pogoste ter nevarne grožnje, je varnostno funkcijo povzdignilo med pomembnejše skrbi organizacij. Negotovost glede ogroženosti in preživetja poslovnih entitet je vse večja, saj so razmere v medorganizacijskih odnosih in zunanjem okolju zelo nepredvidljive. Celovita varnost organizacijskega okolja je zato nujen pogoj, ki prispeva k njihovi stabilnosti, pri tem pa takšnega cilja ni mogoče doseči brez učinkovite informacijske varnosti, ki je pomemben del varnostne funkcije. Agresivna implementacija tehnoloških novosti v poslovne entitete, ki se kaže kot vse pogostejši organizacijski trend, z namenom izboljševanja in poenostavljanja poslovnih funkcij, sicer poveča produktivnost podjetij in optimizacijo njihovih procesov, obenem pa povzroči situacijo, v kateri se grožnje in ranljivosti povečajo. Zaradi stalnih sprememb na področju kibernetskih groženj in tehnoloških tveganj klasični varnostni mehanizmi postajajo neuporabni, varnost pa ob stagnaciji ostane neuresničen organizacijski cilj. Pri zagotavljanju učinkovitost informacijske varnosti so zato organizacije vse pogosteje primorane uporabljati nekonvencionalne pristope povezane z netehničnimi aspekti in strateškimi/upravljavskimi kompetencami.

1.1 Varnostna funkcija v organizaciji

Varnostna funkcija je specifična organizacijska veja in področje, ki je ni mogoče obravnavati in ocenjevati na enak način kot ostale poslovne ukrepe in aktivnosti. O tem, kdaj je organizacija v celoti ali njeno določeno področje varno, je zelo težko govoriti, saj je varnost abstraktno stanje, ki ga je težko izraziti s konkretnimi in točnimi podatki. Trček (2006) navaja, da je varnost stanje minimalnih tveganj in da stanje absolutne varnosti ne obstaja, saj bodo vedno prisotna določena tveganja, ki jih ne moremo obvladati ali predvideti. Varnostna funkcija je v organizaciji podporne narave, saj omogoča nemoteno izvajanje vsakodnevnih poslovnih aktivnosti. Vsaka organizacija, še posebej v času gospodarske nestabilnosti, pa zahteva racionalnost pri razporejanju razpoložljivih virov za podporna področja, ki morajo prispevati k izpolnjevanju organizacijskih ciljev. Kadar je varnost učinkovita, izpolnjuje zastavljene cilje na gospodaren način in s tem prispeva

k razvoju organizacije. Tako kot varnostna funkcija nasploh je tudi informacijska varnost zelo obsežno in abstraktno področje, ki za zagotovitev učinkovitosti zahteva interdisciplinaren in timski pristop ter različne sposobnosti varnostnih strokovnjakov (Ivanc, 2013; Whitman in Mattord, 2008; Thomson in Solms, 2006). Gre za večnivojski sistem, kamor vključujemo postopke managerske, tehnične/operativne in procesno politične narave, ki se nanašajo na področje preprečevanja in odkrivanja groženj ter okrevanja po morebitnih incidentih (Allen in Westby, 2007; Sethuraman in Adaikkappan, 2009). Celovita varnost je v največji meri odvisna od razvitega varnostnega managementa, ki je pristojen za sprejemanje odločitev o varnosti. Uspeh oz. izpolnjevanje zastavljenih organizacijskih ciljev se v relativno veliki meri povezuje z managersko upravljavskimi funkcijami (Peters in Waterman, 1982; Vila, 1994; Vršec, 2013), kot so razvoj organizacije, načrtovanje in definiranje organizacijskih ciljev, odzivanje na nepričakovane situacije, način in sposobnost vodenja, upravljanje s kadrovskimi viri, njihov razvoj in nadzor ter organizacijske vrednote. Pri tem je zelo pomembno, da organizacija določi in izbere pravo strategijo, kajti ukrepi so lahko učinkoviti, vendar še vedno neracionalni in neuspešni, kadar jih organizacija ne potrebuje in pri tem zasleduje napačne cilje (Afonso, Schuknecht in Tanzi, 2006). Tudi Stewart (2012) navaja, da je upravljanje organizacije uspešno, kadar ima natančno določeno strategijo razvoja, načrt zagotavljanja varnosti pa je skladen z organizacijskimi cilji. Učinkovitost managementa se močno povezuje z ustrezno klimo in kulturo v organizaciji ter splošnim vedenjem zaposlenih. Iz tega je razvidno, da so pogoji oz. kriteriji ocenjevanja uspešnosti in učinkovitosti informacijske varnosti relativno nedoločeni in povezani z zelo abstraktnimi stanji, kar ustvarja veliko nejasnosti.

Zaradi heterogenosti in vpliva različnih dejavnikov informacijske varnosti ni mogoče učinkovito urediti na preprost in nenačrtovan način. V praksi se organizacije pri optimizaciji varnosti informacij in odpravljanju groženj srečujejo z različnimi dilemami. K temu poleg razmer v organizaciji in zunanjem poslovnem okolju močno pripomorejo sodobni varnostni trendi, ki ustvarjajo paradoksalne varnostne situacije, ter kognitivni miselni procesi, ki vplivajo na njihov proces odločanja in načrtovanja.

2 VARNOSTNI TRENDI

V praksi na informacijsko varnost vplivajo številne situacije, ki proces ovirajo ali onemogočajo. Med takšne situacije štejemo npr. pomanjkanje finančnih virov in strokovnega znanja ali njihovo neracionalno razporejanje; paradoksalne situacije med varnostjo in funkcionalnostjo informacijskih sistemov (oz. zahteva po sprejemanju kompromisov med poslovnimi in varnostnimi potrebami); stalne spremembe na področju varnostnih storitev in tehničnih rešitev; in kognitivne pristranosti oz. miselne ovire, ki se pojavljajo pri odločevalcih. Teoretično sicer obstaja idealna situacija, v kateri so izvedeni vsi ustrezni postopki za zagotovitev optimalne informacijske varnosti: varnostni management je razvit in zavesten, tehnični oddelek je ozaveščen in na voljo, tehnologija je posodobljena, izvajajo se ustrezne meritve učinkovitosti, postopki so dokumentirani, predpisani in nadzo-

rovani, ukrepi pa upoštevajo zahteve in potrebe uporabnikov ter poslovnih procesov. Praktično pa je takšna situacija v realnem poslovnem okolju težko dosegljiva, saj se poslovne situacije nenehno spreminjajo, naklonjenost vodstva varnostnemu področju stalno niha, spreminja pa se tudi struktura tehničnih oddelkov in njihove pristojnosti/odgovornosti. Odločitve pri načrtovanju informacijske varnosti so torej pogojene z različnimi organizacijskimi dejavniki, ki variirajo ter so odvisni od vsake organizacije in managementa posebej. Se pa vsa podjetja soočajo z eksponentnimi spremembami, ki jim je težko slediti in jih razumeti. To za tehnično in strokovno nepodkovane odločevalce ustvarja dileme pri izpolnjevanju zahtev po učinkoviti in uspešni informacijski varnosti hkrati.

Vprašanje o učinkovitosti informacijske varnosti je tesno povezano s sodobnimi (varnostnimi in tehnološkimi) trendi, ki med strokovnjaki sprožajo polemike glede njihovih prednosti in slabosti. Varnostni management se zaradi potrebe po optimizaciji stroškov vse pogosteje odloča za prenos odgovornosti za informacijsko varnost k tretjim specializiranim subjektom (ali t. i. izkoriščanje zunanjih virov (ang. outsourcing) varnostnih funkcij), prenašanje podatkov v oblak in eksponentno integracijo mobilne tehnologije in z njimi povezanih aplikacij v delovne procese. Omenjenih ukrepov se organizacije poslužujejo predvsem zaradi potrebe po optimizaciji stroškov (Järveläinen, 2012; Markelj in Bernik, 2011).

Outsourcing se v času naraščajočih groženj in zahtev po učinkovitosti varnosti kaže kot najpogostejša praksa. S tem se sicer določena tveganja prenesejo na zunanje organizacije, vendar se posledično s tem povečujejo druga tveganja in grožnje. Prenos varnostnih funkcij iz organizacijskega v zunanje okolje zelo pogosto vodi tudi v zmanjševanje delovne sile za zagotavljanje informacijske varnosti znotraj organizacij, kar še posebej ogroža varnost zaupnega informacijskega kapitala – manj zaposlenih pomeni manj znanja in manj nadzora. Posledice tega se kažejo v povečani ranljivosti podjetij in večjih možnostih za napake (Fullbrook, 2009). Zato se organizacije pri sprejemanju odločitev o vzpostavljanju varnostnega sistema ne smejo držati samo načela zniževanja stroškov in izogibanja odgovornosti, temveč morajo upoštevati prednosti investicij v lastne varnostne zmogljivosti, ki so neotipljive in nefinančne narave (Hriberšek in Ribič, 2013).

Poleg outsourcinga se organizacije vse pogosteje poslužujejo storitev računalništva v oblaku, kjer gre za prenos podatkov v oblak, s tem pa se zmanjšajo stroški informacijske tehnologije in vzdrževanja. Poleg prednosti takšnega ukrepa pa se vzporedno pojavlja vprašanje informacijske varnosti, saj ni natančno določeno, kdo vse lahko dostopa do informacij in kje natanko se podatki oz. del oblaka s podatki nahaja (Markelj in Bernik, 2011). Takšne storitve zmanjšujejo nadzor nad upravljanjem informacijskega kapitala. V oblaku shranjene informacije so lahko brez vednosti lastnika dostopne različnim subjektom, zaradi česar je težko zagotoviti njihovo zaupnost in celovitost (Thomson, 2011). Ker pa je poslovanje neke organizacije odvisno tudi od dobaviteljev, poslovnih partnerjev pogodbenih izvajalcev in navsezadnje tudi od konkurence, so sestavni del poslovnega informacijskega sistema tudi podatki teh zunanjih dejavnikov (Vršec, 2013). Zaradi tega je stopnja varnosti v zunanjih, povezanih oz. partnerskih okoljih prav tako izjemno pomembna. In kadar se organizacija odloči za prenos podatkov ali storitev, organizacijska varnost postane odvisna od stanja varnosti v okoljih, na katera organizacija sama nima vpliva.

Organizacije skušajo poenostaviti delovne procese tudi s pomočjo mobilne tehnologije, ki postaja organizacijski trend, od katerega so podjetja vse bolj odvisna. Kot napovedujejo raziskave, bodo v prihodnosti najnevarnejše kibernetske grožnje usmerjene ravno v ranljivosti mobilne tehnologije (Internet security threat report,[1] 2012; TMT global security study: Raising the bar,[2] 2011), saj je v trenutnem kontekstu najmanj zaščitena in najbolj ranljiva. Razlog je v tem, da se zelo hitro razvija, medtem ko se njeni zaščiti, zaradi razširjenosti in enostavne uporabe, ki zmanjšujeta občutek tveganja, namenja izjemno malo pozornosti, tako z vidika politične ureditve kot tehnične zaščite. Vse pogosteje je mogoče zaznati tudi trend vnašanja osebnih mobilnih naprav, ki jih zaposleni koristijo v zasebnem življenju, v organizacijo in delovno okolje za izpolnjevanje službenih obveznosti (BYOD[3]). To ustvarja situacijo, v kateri se združujejo zasebne in poslovne aktivnosti uporabnika, kar povečuje možnosti za zlorabe in ranljivosti v organizacijski strukturi (Sjouwerman, 2012).

Težnja organizacij slediti spremembam in tehnološkemu razvoju je zelo velika, vendar pa nepremišljena implementacija tehnoloških novosti v organizacijsko strukturo ni primeren odziv na povečana varnostna tveganja. Dobre varnostne odločitve morajo biti podprte s trdnimi argumenti – analizami prednosti in slabosti. Ker pa je učinkovitost varnosti težko merljivo področje in velikokrat tudi neustrezno definirano, v praksi pogosto prihaja do izbire neutemeljenih varnostnih ukrepov, odločitve pa temeljijo na občutkih in netočnih informacijah.

Z informacijsko varnostjo povezane nepravilne odločitve so pogosto posledica tega, da organizacije ne izvajajo ustreznih postopkov ugotavljanja dejanskega stanja (Centre for Internet Security, 2010). Slagell (2010) ugotavlja, da je analiziranje tveganj zelo redka organizacijska praksa, na podlagi katere bi organizacije sprejemale odločitve. Če pa tovrstne analize že izvajajo, so pri tem prepuščene same sebi in lastnemu (pogosto omejenemu) znanju, analize pa so medsebojno neenotne, nedosledne in neprimerljive. Glede na dejstvo, da organizacije pogosto trpijo za pomanjkanjem strokovnega znanja, volje in finančnih virov, medtem ko so storitve varnostnih svetovalcev za veliko organizacij finančno prezahtevne, je omejeno poznavanje stanja logična posledica. To potrjujejo tudi študije, ki poročajo o stagnaciji poizkusov ocenjevanja informacijske varnosti v praksi (Mimoso, 2009). Raziskave ugotavljajo, da podjetja sicer aktivno razvijajo informacijsko varnost, vendar varnostne zmogljivosti podjetij nazadujejo od leta 2008, saj 65 odstotkov organizacij ne analizira stanja informacijske varnosti (Global state of information security survey: Eye of the storm,[4] 2012) oz. je to ocenjevanje neučinkovito in neustrezno razvito (Info Security, 2011). Odsotnost točnih in aktualnih informacij

1 *Podjetje Symantec je analiziralo informacijskovarnostne incidente v 200 državah in pri tem zabeležilo skupno 5,5 milijonov zlonamernih napadov na informacijske sisteme. Dnevno so obravnavali 4.595 primerov, pri čemer je bilo vsak dan zaznanih povprečno 82 primerov napadov na organizacije. Takšni napadi so se kazali v obliki t. i. »ciljanih napadov« z namenom vohunjenja za zaupnimi podatki (ang. ATP – advanced persistent threat), kjer gre za kombinacijo različnih groženj (npr. kombinacija socialnega inženiringa in zlonamerne programske opreme, vstavljene v informacijski sistem organizacije) (Internet security threat report, 2012).*

2 *Mednarodna raziskava opravljena v 138 organizacijah.*

3 *BYOD – Bring Your Own Device*

4 *Raziskava izvedena med 1.836 pripadniki informacijskovarnostnega managementa v 64 državah.*

o trenutnem stanju varnosti in ogroženosti ali napačne informacije, ki so posledica neustreznih postopkov ugotavljanja dejanskega stanja, vodijo v nepravilne odločitve, ki temeljijo na predvidevanjih (Pironti, 2007). Zaradi pomanjkanja informacij o dejanskem stanju varnosti se podjetja na viktimizacijo v praksi najpogosteje odzivajo z odpravo posledic prvotne viktimizacije; s povečanjem fizične varnosti, zmanjšanjem privlačnosti tarče in nadzorom dostopa (Lamm Weisel, 2005; Global state of information security survey: Changing the game,[5] 2013), ki so klasični in nezadostni ukrepi pri zagotavljanju celovite in strateško usmerjene varnosti. Najpogosteje torej uporabljajo situacijsko prevencijo, najmanj pa se v praksi uporablja socialna strategija, s katero bi ugotavljali dejanske vzroke viktimizacije in poskušali uvajati dolgoročne spremembe, saj to zahteva veliko časa in truda.

Odločitve o investiranju v razvoj varnosti so v domeni vodstvenega kadra, ki (tudi) informacijsko varnost zelo pogosto povezuje s finančno koristjo varnostnih ukrepov in z idejo, da je varnost strošek. Zaradi vse večjih finančnih omejitev morajo odgovorni za upravičevanje investicij v področje varnosti njeno učinkovitost prikazati s hitrimi in točnimi rezultati (Ashraf, 2005; Pironti, 2007). Ker pa informacijska varnost v primeru učinkovitosti daje rezultate v obliki neuresničenih groženj, jo je težko dokazati s konkretnimi (finančnimi) podatki. Kadar so implementirani ukrepi učinkoviti, je zelo zahtevno izmeriti njihov vpliv na varnostne incidente oz. oceniti, koliko je organizacija pridobila s tem, da se nepoznane grožnje niso uresničile. Neuresničitev neke grožnje lahko vodi v prepričanje, da grožnja sploh ne obstaja (Burton in Stewart, 2009), kar privede do dodatnih, neupravičenih varčevalnih ukrepov. Iz tega razloga je informacijska varnost tisto področje v organizacijah, kjer se v kriznih časih zelo pogosto agresivno zmanjšujejo investicije. To pa je še eden izmed mnogih dejavnikov, ki povečuje varnostna tveganja (Knopik in Zhan, 2010). S tem informacijska varnost postaja najbolj ogroženo varnostno področje v organizacijskih strukturah. Nasprotno pa mora biti urejanje tovrstnega področja naloga vsake organizacije, saj uporaba IKT[6] v prihodnosti ne bo upadla (trendi kažejo ravno nasprotno), prav tako pa lahko upravičeno pričakujemo nadaljnji razvoj groženj in tveganj. Za učinkovito upravljanje se morajo organizacije zavedati, da je varnost dolgoročna investicija, ki ne prinaša dobička, temveč preprečuje izgubo (ENISA, 2012).

Tako ugotavljamo, da lahko poizkusi (hitrega) prilagajanja sodobnim varnostnim trendom in tehničnim novostim brez trdne argumentacije vodijo v povečane ranljivosti. To se navadno zgodi takrat, kadar organizacije tega ne počno premišljeno in analitično ter novosti uvajajo na podlagi priporočil prodajalcev, ki imajo lahko dvomljive namene. Pri zagotavljanju učinkovitosti informacijske varnosti je zato v primeru načrtovanja in vzpostavljanja varnostnih načrtov potrebno upoštevati prednosti in slabosti sodobnih trendov informacijske varnosti ter razumeti tveganja, ki jih povzroča implementacija takšnih ukrepov (kot npr. prenos odgovornosti na zunanje subjekte). Predvsem pa mora vsaka organizacija poiskati in tako poznati odgovor na dve temeljni vprašanji:

5 *Analiza 9.300 podjetij v 128 državah je pokazala, da ima zgolj 42 odstotkov organizacij proaktivno informacijskovarnostno strategijo, medtem ko imajo preostale pomanjkljive varnostne načrte (ali pa jih sploh nimajo) in se na grožnje odzivajo pretežno reaktivno.*

6 *Informacijsko-komunikacijska tehnologija.*

- kakšno je trenutno varnostno stanje in
- kakšen je načrt za prihodnost?

Kadar se informacijska varnost načrtuje strateško in dolgoročno (kar je tudi pogoj njene učinkovitosti) mora odgovorni varnostni management jasno in natančno določiti operativne, taktične in strateške varnostne cilje. Ti morajo biti osnovani na točnih informacijah o aktualnih varnostnih ukrepih in njihovih vplivih na upravljanje ogroženosti. Na takšen način se lahko identificirajo stopnja njihove združljivosti s poslovnimi zahtevami, učinkovitosti ter varnostne vrzeli, ki jih je treba urediti v prihodnosti. Organizacija mora vedeti, kaj si želi in iz kakšne situacije bo pri doseganju ciljev tudi izhajala. Želena varnostna situacija v prihodnosti pa mora biti zastavljena racionalno in predvsem izvedljivo, saj lahko pretiran idealizem in optimizem, tako kot ravnodušnost in ignoranca, povečata obstoječa tveganja. Poznavanje trenutnega varnostnega stanja, varnostnih potreb in zmogljivosti so torej nujni pogoj učinkovitosti informacijske varnosti. Brez razumevanja omenjenih področij so neracionalne odločitve s prekomernimi in nepotrebnimi ukrepi neizogibna posledica!

3 DEJAVNIKI SPREJEMANJA ODLOČITEV

Na varnostno situacijo v organizacijskem okolju vplivajo zunanji, organizacijski in osebnostni dejavniki. Finančna kriza, varnostni in tehnološki trendi so situacije, ki jih uvrščamo v področje zunanjih in organizacijskih dejavnikov. Te lahko upravljamo zgolj do določene mere oz. se nanje lahko zgolj odzivamo s pravilnimi in racionalnimi odločitvami. Na racionalnost teh odločitev vplivajo tudi osebnostni in psihološki dejavniki, ki se pojavljajo pri tistih, ki so pristojni za njihovo sprejemanje. Informacijska varnost je tako kot tehnična tudi kriminološka in psihološka tema in jo je kot takšno potrebno obravnavati, če se želi zagotoviti celovit pristop pri njenem pojasnjevanju. Zajema različne psihološke vidike, od delovanja in osebnostnih značilnosti storilcev, vedenja in odnosa zaposlenih pri uporabi tehnologije, odnosa vodstva do varnostne funkcije, do percepcije tveganj in ogroženosti ter psiholoških procesov, ki se odvijajo pri odločevalcih.

3.1 Strah, negotovost in dvom

Pri analiziranju in pojasnjevanju odločitev o informacijski varnosti v organizacijskem okolju je potrebno upoštevati tri glavne psihološke ovire, ki pogosto vodijo v neustrezna varnostna stanja; to so strah, negotovost in dvom, ki jih je težko ustrezno obvladovati brez trdnih in veljavnih analiz tveganj. Omenjeni psihološki dejavniki predstavljajo problem, kadar se pojavijo pri varnostnem managementu, ki lahko zaradi tega sprejema neracionalne odločitve, tveganja precenjuje ali podcenjuje in implementira nepotrebne varnostne kontrole.

Strah, negotovost in dvom se najpogosteje pojavijo pri tistih posameznikih, ki nimajo na voljo ustreznega znanja in razumevanja o informacijski varnosti ter kadar pri njenem urejanju ne izhajajo iz dejanskega stanja. V kombinaciji z nasi-

čenostjo trga s tehnološkimi in varnostnimi rešitvami pa se negotovost in dvom pri odločevalcih še povečujeta. Takšno situacijo zelo pogosto izkoristijo neetični varnostni strokovnjaki, ki lahko na ta način pospešijo svoj posel (Baddeley, 2011). Gre za poznano marketinško taktiko, ki se jo pogosto poslužujejo vodilna ali monopolna podjetja za ohranjanje konkurenčne prednosti. Kot ugotavlja že Pfaffenberger (2000), je na področju IKT taktika povečevanja strahu med uporabniki informacijskih sistemov zelo pogosta in že uveljavljena praksa. Z eksponentnim povečevanjem kibernetske kriminalitete v zadnjih letih pa je še toliko bolj učinkovita. Države uporabljajo podobno taktiko pri upravičevanju, povečevanju ali izkazovanju vojaške in gospodarske moči, še posebej pa v kriznih časih.

Pri ustvarjanju prepričanja o ogroženosti veliko vlogo odigrajo tudi informacije, ki jih pridobimo iz zunanjega okolja. K ustvarjanju strahu na področju zaznave tveganj v povezavi s tehnologijo močno pripomorejo mediji, ki s svojim poročanjem vplivajo na splošno mnenje v družbi. Zelo pogosto, zaradi potrebe po senzacionalnem poročanju, mediji izpostavljajo bolj dramatične in manj pogoste oblike (tudi kibernetske) kriminalitete, kar pri ljudeh ustvarja neupravičen strah (Levi, 2008). In glede na to, da negativne izkušnje s kriminaliteto in grožnjami praviloma (ne pa nujno) vplivajo na zaznano verjetnost viktimizacije (Meško, Šifrer in Vošnjak, 2012), lahko upravičeno domnevamo, da odmevne informacije o varnostnih incidentih, ki jih ljudje pridobijo od medijev, poosebijo in pretvorijo v osebno izkušnjo, njihova percepcija tveganja pa je zaradi tega večja, kot je v resnici. Informacijska tehnologija že sama po sebi pri neveščih oz. neusposobljenih ljudeh izziva občutke negotovosti in kadar mediji prekoračijo svojo vlogo informatorja in nalogo ozaveščanja (kar je zelo pogosta praksa), se posledica lahko kaže ne samo v strahu pred kriminaliteto, temveč tudi v strahu pred tehnološkimi novostmi. Takšno obliko strahu imenujemo tehnofobija (Gilbert, Lee-Kelley in Barton, 2003). In kadar je družba izpostavljena pretiranemu zastraševanju, lahko pride do neupravičenega zavračanja tehnoloških novosti in nevarnega vedenja ali pa ravno nasprotno, do uporabe pretiranih in nepotrebnih varnostnih kontrol za tveganja, ki sploh ne obstajajo.

Takšna zavajanja in pretiravanja se pojavljajo tudi na področjih zagotavljanja varnosti v organizacijskem okolju, pri čemer ponudniki in izvajalci varnostnih storitev vplivajo na prepričanost ljudi o ogroženosti z lažnimi in popačenimi statistikami (Slagell, 2010). Podjetja, ki se ukvarjajo s proizvodnjo in prodajo tehnoloških rešitev pa poleg zastraševanja, s katerim pospešujejo prodajo lastnih storitev in produktov, uporabljajo tudi različne načine, s katerimi preprečujejo nakup in uporabo konkurenčnih proizvodov, kot npr. svarila in opozorila uporabnikov pred novimi, tveganimi sistemi; izgradnja takšnih sistemov, ki so nezdružljivi s konkurenčnimi proizvodi ali pa otežijo kasnejšo zamenjavo sistemov; višje cene popravil sistemov v primeru njihove kombinacije z drugimi proizvodi ipd. Najbolj problematična metoda, ki lahko ogrozi preživetje ponudnikov tehnoloških rešitev in storitev, pa so naznanila novih produktov s strani vodilnih podjetij, ki sploh še niso v izdelavi, niti jih nimajo namena razvijati. Na takšen način se preusmeri pozornost od tehnoloških novosti tekmecev in prepreči njihova prodaja (Prentice, 1996). Monopolna podjetja z omenjenimi metodami zlorabljajo svojo moč, zavirajo razvoj konkurence in produktov, potrošnike/organizacije pa silijo v

nakup slabših proizvodov, ki so precenjeni (Pfaffenberger, 2000). Vse to ima lahko še hujše posledice kot samo precenjevanje produktov in tveganj; zaradi tega lahko uporabniki postanejo ravnodušni ali neobčutljivi na realna in nevarna tveganja, hitri in učinkoviti odzivi pa niso izvedljivi, ker se pozornost preusmeri na manj pomembna področja. Takšna situacija predstavlja etično dilemo, ko se varnostni management odloča o outsourcingu informacijske varnosti in postopkih certifikacije po varnostnih standardih s pomočjo varnostnih svetovalcev.

3.2 Sprejemanje ustreznih odločitev za informacijsko varnost

Poleg omenjenih psiholoških dejavnikov na sprejemanje odločitev vplivajo tudi kognitivni psihološki procesi, ki se odvijajo znotraj vsakega posameznika. Gre za avtomatizirane miselne procese, na podlagi katerih posameznik presoja in ocenjuje situacije oz. informacije, ki jih ima na voljo. Omenjeni procesi so pri sprejemanju odločitev o varnosti še toliko bolj prisotni, saj varnost pri ljudeh vzbuja močna stališča in občutke. Lahko so zelo uporabni, v primeru popačenih informacij ali zunanjih pritiskov pa lahko vodijo v sprejem tveganih odločitev. Ker se odvijajo na nezavedni ravni, se jih ljudje pogosto ne zavedajo in jih posledično tudi ne upravljajo.

S sociološkega in psihološkega vidika so z občutki in načinom zagotavljanja varnosti povezani trije sklopi teorij; to so ekonomska vedenjska teorija (pojasnjuje, kako psihološki intrapersonalni procesi vplivajo na ekonomske in finančne odločitve ljudi); psihologija sprejemanja odločitev (pojasnjuje vpliv razuma, hevristik in intuicije na sprejemanje odločitev); in psihologija tveganj (pojasnjuje, kako ljudje zaznavamo tveganja, zakaj jih precenjujemo ali podcenjujemo).

Ekonomske vedenjske teorije v ospredje proučevanja postavljajo posameznika kot racionalno bitje, ki je izrazito individualistične in egoistične narave. Pojasnjujejo, da se ljudje za aktivnosti ali določeno vedenje odločamo na podlagi ocene koristi in škode, ki sledi izbranemu vedenju (Baddeley, 2011). Začetna teorija (tj. teorija racionalne izbire) predvideva, da ima posameznik pri sprejemanju odločitev na voljo zadostno količino informacij, je dobro organiziran in ima sposobnosti ter voljo proučiti vse možne alternative. Kasnejša nadgradnja omenjenih teorij pa ugotavlja, da obstaja razlika med tem, kako naj bi se ljudje vedli in kako se v določenih situacijah dejansko odzivamo, saj so v praksi redko izpolnjeni vsi pogoji racionalnega odločanja (Simon, 1955). Po omenjeni teoriji je takšno odločanje v največji meri pogojeno s situacijskimi dejavniki in znanjem, ki ga posameznik poseduje v trenutku dane situacije (Sandri, 2009).

Enako je tudi v organizacijskem okolju, pri čemer je potrebno upoštevati še nekatere druge dejavnike, ki vplivajo na ekonomsko oz. racionalno vedenje poslovnih entitet, kot so npr. težnja po konkurenčnosti, potreba po varčevanju, želja po hitrih in konkretnih rezultatih. Vse to zelo otežuje upravičevanje investicij v varnostno področje. Najpogosteje se organizacije (tiste, ki se odločijo izvajati postopke ocenjevanja) v težnji po učinkovitosti na podlagi analiz cena/zmogljivost (ang. cost/benefit) odločajo, kakšne so koristi in izdatki izbranega varnostnega ukrepa. Z varnostnega vidika pa omenjene analize niso priporočljiv način tehtanja koristi

možnih ukrepov in kontrol, saj je za podajanje točnih ocen potrebno imeti na voljo natančne podatke o ogroženosti, ki pa jih organizacije pogosto nimajo (Stewart, 2012). Ocenjevanje koristi in škode pa je na podlagi tovrstnih analiz nerealno in neučinkovito. Problem dodatno poglablja še poplava informacij v kibernetskem prostoru, kjer je na voljo sicer dovolj informacij, ki pa so neurejene in (pogosto) nezanesljive. Zato je težko identificirati informacije, ki jih potrebujemo in so točne ter zanesljive. V sklopu omenjene teorije teorija omejene racionalnosti vidiku pomanjkanja relevantnih in točnih informacij dodaja še vidik pomanjkanja časovnih virov. Zelo pogosto so organizacije pod časovnim pritiskom, od managementa pa se zahtevajo hitre odločitve. Omenjena teorija navaja, da ljudje v situaciji, ko nimamo na voljo (ustreznih) informacij in časa, poenostavimo odločitvene in miselne procese. V takšni situaciji redko sprejemamo odločitve na podlagi natančne analize možnih alternativ in navadno sprejmemo prvo zadovoljivo odločitev, ki pa ni nujno tudi najbolj optimalna ali racionalna. Po tej teoriji ljudje pod pritiskom težimo k zadovoljitvi in ne k optimizaciji (Simon, 1956). Iz tega sledi, da je sprejem racionalnih in posledično najbolj učinkovitih odločitev izjemno zahtevna naloga. Varnostno področje je kompleksno, zaradi številnih zunanjih, osebnih in organizacijskih omejitev ter konstantnih pritiskov s strani vodstva in zunanjega okolja pa so manj racionalni ukrepi povsem razumljivi. Odločitvene procese in razloge posameznika je treba razlagati in razumeti z organizacijskega vidika, ki upošteva vpliv zunanjega okolja, in skupin, ki jim posameznik pripada, trenutne okoliščine ipd.

Poleg ekonomskih vedenjskih teorij razloge neracionalnih odločitev o varnostnih ukrepih razlaga tudi teorija sprejemanja odločitev, ki pojasnjuje kognitivni proces obdelave informacij. Na splošno se ljudje pri sprejemanju odločitev zanašamo na logiko in statistiko ali hevristike (Gigerenzer in Gaissmaier, 2011). Omenjena teorija pri razlagah odločitev upošteva vpliv intuicije in hevristik, ki predstavljajo alternativo oz. nasprotje logičnim in analitičnim procesom reševanja problemov ter sprejemanja odločitev. Intuicija je najpogostejši način sprejemanja managerskih odločitev, ki temelji na nepreverjenih prepričanjih, mnenju in občutku odločevalca. S pomočjo intuicije sprejete odločitve so lahko uspešne in učinkovite, vendar je dobro razvita intuicija odvisna od preteklih izkušenj, povratnih informacij, znanja in temperamenta odločevalca (Jacobs, 2011). Z intuicijo so povezane še hevristike – avtomatizirani miselni vzorci oz. kognitivni miselni procesi, ki potekajo na zavedni ali nezavedni ravni in ignorirajo določene informacije (Tversky in Kahneman, 1974). So lahko zelo dober način sprejemanja vsakodnevnih in manj pomembnih odločitev, kadar ima odločevalec na voljo veliko količino nepreglednih informacij in dobre pretekle izkušnje, lahko pa vodijo v kognitivne pristranskosti in hude sistematične napake (Gigerenzer in Gaissmaier, 2011). Obstaja več različnih kognitivnih pristranskosti in hevristik, ki so pogost način sprejemanja odločitev v organizacijskem okolju, z varnostnega vidika pa so pomembne predvsem tri vrste:

- Hevristika razpoložljivosti
  Ljudje verjetnost nekega dogodka (lahko npr. varnostne grožnje) ocenjujemo na podlagi tega, kako hitro si lahko podoben dogodek prikličejo v spomin. Pogosto izpostavljanje redkih primerov lahko vzbudi občutek, da so ti pogostejši (Slagell, 2010) (in če so npr. v medijih določene grožnje, ki so relativno nepogoste, v določenem trenutku posebej izpostavljene, ima lah-

ko odločevalec občutek, da je tveganje večje, kot je v resnici). V kombinaciji s podcenjevanjem tveganj in prevelikim optimizmom pa lahko omenjena hevristika vodi v prepričanje, da grožnje sploh ne obstajajo, saj v preteklosti organizacija z njimi še ni imela opravka (oz. jih ni zaznala) (Baddeley, 2011).

- Hevristika sidranja
  Ljudje vrednost dogodka ali pojava ocenjujemo na podlagi neke srednje izhodiščne vrednosti, ki jim je ponujena, ni pa nujno tudi pravilna (z varnostnega vidika se to pogosto dogaja pri ocenjevanju škode uresničene kibernetske grožnje, ki je zelo pogosto subjektivna in ni podprta z natančnimi analizami) (Epley in Gilovich, 2006).
- Hevristika reprezentativnosti
  Povzroča, da lastnosti določenega dogodka ocenjujemo na podlagi stereotipov in lastnosti celotne skupine, v katero ta dogodek, ukrep ali pojav spada (npr. odločevalci zaradi neutemeljenih prepričanj stalno uporabljajo ali se izogibajo storitvam enega ponudnika) (Tversky in Kahneman, 1974).

Vpliv posameznikove percepcije, občutkov in stališč na odločitvene in miselne procese spada v sklop teorij psihologije tveganj, ki so:

- KAB teorija
  KAB teorija, ki se ukvarja s proučevanjem vpliva ozaveščenosti ljudi na njihovo vedenje in spodbujanjem oz. motiviranjem zaposlenih za varnostno pozitivno vedenje. Glede na KAB teorijo se s povečevanjem znanja spreminja odnos do obravnavane tematike, posledično pa ima sprememba v odnosu vpliv na vedenje posameznika. Vendar pa spremembe v vedenju niso tako enostavne, saj nanje vpliva več spremenljivk, pri čemer znanje odigra največjo vlogo.
- TRA teorija
  Da bi razumeli proces spreminjanja odnosa in vedenja je potrebno razumeti tudi TRA (theory of reasonable action), ki je predhodnica TPB (theory of planned behaviour) teorije. Slednja je ena izmed najbolj uveljavljenih teorij pojasnjevanja povezave med odnosom in vedenjem posameznika ter opisuje posredne in neposredne vplive na omenjeno razmerje (Ajzen, 1991).
- TPB teorija
  Glede na TPB teorijo so spremembe v vedenju posameznika odvisne od njegovih namenov oz. motivacije. Ta je pogojena z dvema faktorjema: odnosom in subjektivnimi normami. Iz tega sledi, da je namen izvršiti neko aktivnost večji, kadar ima do le-tega pozitiven odnos (kaj je posamezniku všeč in kaj ne) in izoblikovane močne subjektivne norme (kaj posameznik meni, da se od njega pričakuje) (Khan, Alghathbar, Nabi in Khurram, 2011). Prepričanjem, odnosu in normam je Bandura (1977) pri pojasnjevanju posameznikovega vedenja in odločitev dodal še spremenljivko »občutek samonadzora«. Z njo pojasnjuje, da se posameznik lažje odloči za neko aktivnost, kadar ima večji občutek nadzora oz. kontrole nad določeno situacijo. In ker so zaposleni kot uporabniki v organizacijskem okolju pogosto neustrezno informirani o pravilih, razlogih sprememb in tehnologiji sami, se počutijo nemočne, zaradi tega pa lahko izoblikujejo

negativne norme in odnose do omenjenega področja. Varnostno negativno vedenje, ignoranca in neupoštevanje varnostnih pravil so v takšnem primeru pogosta praksa zaposlenih.

S spodbujanjem proaktivnega varnostnega vedenja se ukvarjata:

- Varnostnomotivacijska teorija (Protection motivation theory)
  Ukvarja se s proučevanjem vedenja potrošnikov in se uporablja na področju marketinga, managementa in varnostnih storitev (Cismaru in Lavack, 2006). Omenjena teorija (Rogers, 1975) ugotavlja, da se posameznik za neko aktivnost odloči na podlagi subjektivne ocene ranljivosti (občutek ogroženosti), nevarnosti (zaskrbljenost), samoučinkovitosti (prepričanje, da lahko sam izvede določeno dejanje, aktivnost), uspešnosti odziva oz. ukrepa (prepričanje, da bo ukrep odpravil grožnjo) in izdatkov/stroškov (neugodje, ki ga bo ob izvedbi aktivnosti ali ukrepa doživel).
- Teorija tveganj
  Na splošno ugotavlja, da smo ljudje pri ocenjevanju lastne ogroženosti nagnjeni k podcenjevanju, kadar se primerjamo z drugimi subjekti; menimo, da smo manj ogroženi kot drugi (West, 2008). Največje napake pa se pojavljajo pri ocenjevanju nevarnosti in verjetnosti tveganj; posledic groženj; uspešnosti varnostnih ukrepov in primerjanju tveganj s finančnimi izdatki za njihovo upravljanje. Razlog je v tem, da ljudje večino odločitev sprejemamo ob nepopolni informiranosti; v takšnem primeru relevantne informacije iščemo v okolju, z opazovanjem, razlaga situacije pa je odvisna od intrapersonalnih dejavnikov in osebnih izkušenj (Floyd, Prentice-Dunn in Rogers, 2000).

Iz povzetih psiholoških in sociološkihteorij je razvidno, da so z vidika uporabnikov tehnologije subjektivne norme in odnos zelo pomemben dejavnik, ki vpliva na njihovo varnostno pozitivno vedenje. V organizacijskem okolju je zato na splošno neozaveščenost in neinformiranost uporabnikov glavni razlog njihovega odpora do sprememb in tehnologij. Posledično je med takšnimi uporabniki odnos do varnosti negativne narave, njihova pripravljenost zaobiti varnostne kontrole in pravila pa zato večja. Z vidika managementa in odločevalcev pa omenjene kognitivne pristranskosti in hevristike predstavljajo pomemben dejavnik, ki vpliva na ne/racionalnost odločitev in zelo pogosto vodi v napačne ocene vrednosti in verjetnosti dogodkov ter pojavov. Kadar posameznikovi občutki in osebna stališča ne temeljijo na točnih informacijah so pogosto neutemeljena in neupravičena. Takšna situacija je posebej pogosta na področju varnosti in ocenjevanja tveganj, kjer subjektivnost vodi v precenjevanje manj pomembnih groženj in zapostavljanje kritičnih ranljivosti. V kombinaciji s slabo razvito intuicijo oz. neizkušenostjo, strahom, negotovostjo in priporočili neetičnih svetovalcev je neučinkovita informacijska varnost popolnoma logičen končni rezultat.

4 SKLEP

Če zgoraj omenjene in opisane pogoje učinkovitosti informacijske varnosti na kratko povzamemo, lahko ugotovimo, da je informacijska varnost učinkovita,

kadar je vnaprej načrtovana in dodeljena v pristojnost sposobnemu upravljavskemu kadru. Ob upoštevanju ugotovitev analize varnostnih trendov v kombinaciji s splošno neugodnim stanjem v poslovnem okolju in vse večjimi varnostnimi tveganji pa lahko upravičeno sklepamo, da se ustvarja velik pritisk ravno na glavni element učinkovitosti informacijske varnosti – varnostni management, kar povzroča omejitve pri doseganju zastavljenih varnostnih ciljev. Potrebe organizacij po hitrih in cenovno sprejemljivih rešitvah so velike, zaradi česar organizacije pogosto nimajo časa, volje in/ali finančnih zmogljivosti, da bi odločitve snovale na podlagi kakovostnih analiz ogroženosti in splošne učinkovitosti. Ker je informacijska varnost, kljub svojemu pomenu, v organizaciji podporne narave, pa se ji z vidika sprejemanja odločitev za reševanje problemov ne namenja poglobljena pozornost, kar je posledica tradicionalne, tehnično usmerjene mentalitete informacijske varnosti. Zaradi omenjenih pritiskov je tudi vpliv psiholoških dejavnikov in kognitivnih miselnih procesov oz. kognitivnih pristranskosti večji, kar ustvarja situacijo, v kateri so logični in primerni varnostni ukrepi prilagojeni organizacijskim potrebam redka organizacijska praksa. To pa ogroža končno uspešnost in posledično konkurenčnost organizacij.

Opisani problemi in predstavljene varnostne dileme dokazujejo, da je učinkovitost informacijske varnosti najpogosteje ogrožena zato, ker organizacije v poizkusih sledenja hitremu razvoju IKT in tehničnim ukrepom pozabljajo na prispevek človeškega faktorja k varnostnem stanju v organizaciji (Ashraf, 2005). Tveganja, ki so povezana z omenjenimi trendi, se sicer lahko uravnotežijo z različnimi ukrepi, vendar je potreben celovit in ne samo parcialen ter površinski pristop. Veliko je odvisno od varnostnega managementa, ki mora tveganja uravnotežiti z natančnimi pogodbami z zunanjimi izvajalci in partnerji, postopki certificiranja po mednarodnih informacijskovarnostnih standardih in dosledno zunanjo revizijo sistemov (Järveläinen, 2012). Tiste gospodarske družbe, ki se resno lotevajo varovanja poslovnega informacijskega sistema, morajo izdelati politiko varovanja informacij, uvajati standarde varovanja in neprekinjenega poslovanja (Vršec, 2013). Predvsem se je potrebno zavedati, da tehnični ukrepi ne morejo biti učinkoviti, kadar jih uporabniki ne upoštevajo in ne razumejo varnostnih pravil (Herath in Rao, 2009), zaradi česar je potrebno varnostno ozaveščanje in vpletenost uporabnikov v varnostne procese organizacije. Že zgodnje psihološke teorije ugotavljajo, da je znanje najpomembnejši element pozitivnega varnostnega vedenja. Tudi Spears in Barkhi (2010) sta ugotovila, da aktivna udeležba zaposlenih pri vzpostavljanju varnostnih ukrepov skupaj s programi ozaveščanja pomembno vpliva na dvig dejanske stopnje informacijske varnosti v organizaciji. Enakega stališča je tudi NIST (Wilson in Hash, 2003), ki v svojih priporočilih navaja, da stanje ozaveščenosti zaposlenih vpliva na manjšo stopnjo informacijskih incidentov. Medtem so Talib, Clarke in Furnell (2010) s pomočjo raziskave prišli do ugotovitve, da ljudje večino z varno uporabo IKT povezanega znanja pridobimo ravno v delovnem okolju. Programi izobraževanja in usposabljanja so torej še toliko bolj pomembni, saj v delovnem okolju pridobljeno znanje prenašamo na druga okolja izven organizacije. Raziskave ugotavljajo tudi, da je človek najpogostejši vzrok informacijskovarnostnih incidentov, še posebej v težkih ekonomskih časih, saj povečan stres in občutek strahu pred izgubo službe povzroči, da se zaposleni pogosteje obnašajo

deviantno (TMT global security study …, 2011). Bernik in Meško (2011) pa sta ob analizi zavedanja in dojemanja kibernetskih groženj med uporabniki interneta v Sloveniji ugotovila, da na splošno obstaja pomanjkanje ozaveščenosti o kibernetskih grožnjah in zakonodaji na tem področju. Iz tega sledi, da je nujno, da se poleg fizičnega in tehničnega varovanja v varnostni sistem uvedejo tudi sodobna managerska orodja varovanja poslovnih procesov, če se želi zagotoviti ustrezno vodenje v kriznih situacijah (Vršec, 2013).

Da bi omenjene dileme in varnostne izzive čim bolje upravljali, je treba poznati tudi možna kognitivna izkrivljanja, ki se lahko pojavijo pri pojasnjevanju groženj in ocenjevanju varnostnih tveganj. Refleksivni in analitični pristopi so najboljši način minimaliziranja subjektivnosti in napak pri odločanju. In kot ugotavlja Jacobs (2011), se morajo odgovorni pri sprejemanju odločitev vprašati, kakšni so razlogi določene odločitve in kakšne so možnosti preverjanja njihove pravilnosti. Za zagotovitev učinkovitosti informacijske varnosti je treba upravljati tudi čustvene komponente, ki lahko vplivajo na neželeno vedenje ali neracionalne odločitve. Predvsem pa se je potrebno zavedati, da informacijska varnost ni zgolj tehnično področje, temveč je proces, ki zahteva obravnavo različnih psiholoških in sociološkihvidikov (Baddeley, 2011). Takšen proces sicer zahteva sistematični pristop, voljo in čas, vendar so dolgoročni učinki na stanje informacijske varnosti v tem primeru največji.

Ob vseh omenjenih pogojih je izjemno pomembno predvsem to, da se varnostni management, ki je pristojen za določanje odgovornosti, pristojnosti in načrtovanje informacijske varnosti nasploh, zaveda morebitnih napak, ki se lahko pojavijo pri sprejemanju odločitev. V primeru dvoma in negotovosti je treba zagotoviti predvsem dovolj časovnih in strokovnih virov, ki bodo prispevali k logičnim sklepom in izbiri racionalnih ukrepov. Pri sprejemanju odločitev morajo biti vzpostavljeni odprti komunikacijski kanali in konstruktiven konflikt med zaposlenimi, saj se s tem zmanjšuje prostor za enostranske in nepreverjene odločitve. Predvsem pa mora imeti managemet posluh za ideje in pripombe zaposlenih, vodstvo pa mora varnost in kredibilnost vključiti med temeljne vrednote in vizijo organizacije.

LITERATURA

Afonso, A., Schuknecht, L. in Tanzi, V. (2006). *Public sector efficiency: Evidence for new EU member states and emerging markets.* Frankfurt: European Central Bank.

Ajzen, I. (1991). The theory of planned behaviour. *Organizational Behaviour and Human Decision Processes*, *50*, 179–211.

Allen, J. H. in Westby, J. R. (2007). *Governing for enterprise security: Implementation guide US-CERT: Article 1 – Characteristics of effective security governance*. Pittsburg: Carneige Mellon University.

Ashraf, S. (2005). *Organization need and everyone's responsibility: Information security awareness – Global Information Assurance Certification Paper*. Bethesda: SANS Institute. Pridobljeno na http://www.giac.org/paper/gsec/4340/organization--everyones-responsibility-information-security-awareness/107113

Baddeley, M. (2011). *Information security: Lessons from behavioural economics.* Cambridge: Gonville and Caius College.

Bandura, A. (1977). Self-efficacy: Toward a unifying theory of behavioral change. *Psychological Review, 84*(2), 191–215.

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.

Burton, S. in Stewart, S. (2009). *Security implications of the global financial crisis*. Austin: Stratfor Global Intelligence. Pridobljeno na http://www.stratfor.com/weekly/20090304_security_implications_global_financial_crisis

Centre for Internet Security. (2010). *The CIS consensus security metrcis*. Pridobljeno na http://benchmarks.cisecurity.org/en-us/?route=downloads.metrics

Cismaru, M. in Lavack, A. M. (2006). Marketing communications and protection motivation theory: Examining consumer decision-making. *International Review on Public and Non Profit Marketing, 3*(2), 9–24.

ENISA. (2012). *Return on security investment.* Pridobljeno na http://www.enisa.europa.eu/activities/cert/other-work/introduction-to-return-on-security-investment

Epley, N. in Gilovich, C. (2006). The anchoring and adjustment heuristics. *Psychological Science, 17*(4), 311–318.

Floyd, D. L., Prentice-Dunn, S. in Rogers, R. W. (2000). A meta-analysis of research on protection motivation theory. *Journal of Applied Social Psychology, 30*(2), 407–429.

Fullbrook, M. (2009). Tips on stamping out data leakage & industrial espionage during recession. *ICT Review: Computer Hardware and Software Review Journal,* (Mar.). Pridobljeno na http://ictreview.blogspot.com/2009/03/tips-on-stamping-out-data-leakage.html

Gigerenzer, G. in Gaissmaier, W. (2011). Heuristic decision making. *Annual Review of Psychology, 62*, 451–482.

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.

Global state of information security survey: Changing the game. (2013). London: PWC. Pridobljeno na http://www.pwc.com/gx/en/consulting-services/information-security-survey/assets/2013-giss-report.pdf

Global state of information security survey: Eye of the storm. (2012). London: PWC. http://www.pwccn.com/webmedia/doc/634653330562192188_rcs_info_security_2012.pdf

Herath, T. in Rao, H. R. (2009). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems, 47*(2), 154–165

Hriberšek, Z. in Ribič, A. (2013). Korporativna varnost kot konkurenčna prednost podjetja. *Korporativna varnost, 2*(3), 30–33.

Info Security. (2011). *Most enterprises poor at measuring information security effectiveness.* Pridobljeno na http://www.infosecurity-magazine.com/view/16928/most-enterprises-poor-at-measuring-information-security-effectiveness/

Internet security threat report. (2012). Mountain View: Symantec. Pridobljeno na http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_2011_21239364.en-us.pdf?om_ext_cid=biz_socmed_twitter_facebook_marketwire_linkedin_2012Apr_worldwide_ISTR17

Ivanc, B. (2013). Varovanje občutljivih podatkov v informacijskih sistemih. V I. Bernik in B. Markelj (ur.), *Sodobni aspekti informacijske varnosti* (str. 6–11). Ljubljana: Fakulteta za varnostne vede.

Jacobs, J. (2011). A call to arms: It's time to learn like experts. *ISSA Journal,* (Nov.), 31–34. Priobljeno na http://beechplane.files.wordpress.com/2011/11/a-call-to-arms_issa1111.pdf

Järveläinen, J. (2012). Information security and business continuity management in interorganizational IT relationships. *Information Management & Computer Security, 20*(5), 332–349.

Khan, B., Alghathbar, K. S., Nabi, S. I. in Khurram, M. (2011). Effectiveness of information security awareness method based on psychological theories. *African Journal of Business Management, 26*(5), 10862–10868.

Knopik, C. in Zhan, J. (2010). *The effects of financial crises on american financial institutions information security.* Prispevek na 5th Conference on Future Information Technology, 21.–23. 5. 2010. Madison: Dakota state University.

Lamm Weisel, D. (2005). *Analyzing repeat victimization* (Tool Guide No. 5). Center for Problem-Oriented Policing. Pridobljeno na http://www.popcenter.org/tools/repeat_victimization/print/

Levi, M. (2008). White-collar, organised and cyber crimes in the media: Some contrasts and similarities. *Crime, Law and Social Change, 49*(5), 365–377.

Markelj, B. in Bernik, I. (2011). Mobilni dostop z vidika informacijske varnosti do podatkov v oblaku. V T. Pavšič Mrevlje in I. Areh (ur.), *Zbornik prispevkov 12. slovenski dnevi varstvoslovja.* Ljubljana: Fakulteta za varnostne vede. Pridobljeno na http://www.fvv.uni-mb.si/dv2011/zbornik/informacijska_varnost/Markelj-Bernik-Oblak.pdf

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.

Mimoso, M. S. (12. 3. 2009). Number-driven risk metrics fundamentally broken. *SearchSecurity*. Pridobljeno na http://searchsecurity.techtarget.com/news/article/0,289142,sid14_gci1350658,00.html#

Peters, T. J. in Waterman, R. H. (1982). *In search of excellence: Lessons from America's best-run companies.* London: HarperCollins Publishers.

Pfaffenberger, B. (2000). The rhetoric of dread: Fear, uncertainty and doubt in information technology marketing. *Knowledge, Technology & Policy, 13*(3), 78–92.

Pironti, J. P. (2007). Developing metrics for effective information security governance. *ISACA Journal, 7*(2), 1–5.

Prentice, R. (1996). Vaporware: Imaginary high-tech products and real antitrust liability in a post-Chicago world. *Ohio State Law Journal, 57*(4), 1163–1262.

Rogers, R.W. (1975). A protection motivation theory of fear appeals and attitude change. *Journal of Consumer Psychology, 91*(1), 93–114.

Sandri, S. (2009). *Reflexivity in economics: An experimental examination on the self-referentiality of economic theories.* Berlin: Physica-Verlag.

Sethuraman, S. in Adaikkappan, A. (2009). Information security program: Establishing it the right way for continued success. *ISACA Journal, 9*(5), 1–7.

Simon, H. A. (1955). A behavioral model of rational choice. *The Quarterly Journal of Economics, 69*(1), 99–118.

Simon, H. A. (1956). Rational choice and the structure of the environment. *Psychological Review, 63*(2), 129–138.

Sjouwerman, S. (2012). 2013 security prediction. *Cyberheist News, 2*(53). Pridobljeno na http://blog.knowbe4.com/cyberheistnews-vol2-53/

Slagell, A. (2010). Thinking critically about computer security trade-offs. *Skeptical Inquirer, 34*(4). Pridobljeno na http://www.csicop.org/si/show/thinking_critically_about_computer_security_trade-offs/

Spears, J. L. in Barkhi, H. (2010). User participation in information systems security risk management. *MIS Quarterly, 34*(3), 503–522.

Stewart, A. (2012). Can spending on information security be justified? *Information Management & Computer Security, 20*(4), 312–326.

Talib, S., Clarke, N. L. in Furnell, S. M. (2010). *An analysis of information security awareness within home and work environments.* Prispevek na 5th International Conference on Availability, Reliability and Security: ARES 2010, 15.–18. 2. 2010. Cracow: IEEE Computer Soc. Pridobljeno na http://ro.ecu.edu.au/cgi/viewcontent.cgi?article=7348&context=ecuworks

Thomson, K. L. in Solms, R. (2006). Towards an information security competence maturity model. *Computer Fraud & Security, 18*(5), 11–15.

Thomson, L. L. (2011). Cybercrime and escalating risks. V L. Thomson (ur.), *Data breach and encrypton handbook* (str. 3–16). Chicago: American Bar Association Section of Science & Technology Law.

TMT global security study: Raising the bar. (2011). New York: Deloitte. Pridobljeno na http://www.deloitte.com/assets/Dcom-Global/Local%20Assets/Documents/TMT/dttl_TMT%202011%20Global%20Security%20Survey_High%20res_191111.pdf

Trček, D. (2006). *Managing infomation systems security and privacy*. Berlin: Springer.

Tversky, A. in Kahneman, D. (1974). Judgment under uncertainty: Heuristics and biases science. *Science, New Series, 185*(4157), 1124–1131.

Vila, A. (1994). *Organizacija in organiziranje*. Kranj: Moderna založba.

Vršec, M. (2013). Varovanje poslovnega informacijskega sistema na osnovi politike varovanja informacij. *Korporativna varnost, 2*(3), 9–11.

West, R. (2008). The psychology of security. *Communications of the ACM, 51*(4), 34–41.

Whitman, M. E. in Mattord, H. J. (2008). *Management of information security*. Boston: Course Technology Cengage Learning.

Wilson, M. in Hash, J. (2003). *Building an information technology security awareness and training Program – NIST Special Publication 800-50.* Gaithersburg: National Institute for Standards and Technology. Pridobljeno na http://csrc.nist.gov/publications/nistpubs/800-50/NIST-SP800-50.pdf

O avtorjih:

Kaja Prislan, mag. var., asistentka za področje varnostnih sistemov in 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. 16
št. 1
str. 68–84

Nacionalne omejitve pri pravilih delovanja oboroženih sil v mednarodnih operacijah in posledice njihovih kršitev

Sabina Zgaga, Maj Fritz

Namen prispevka:

Oborožene sile, ki delujejo v katerikoli operaciji v spektru vojaških operacij, morajo delovati v skladu z določenimi pravili in normami. Ker skupna pravila delovanja mednarodnih sil niso vedno ustrezna za vse sodelujoče države, lahko posamezna država, ki sodeluje v mednarodni operaciji, določi nacionalna pravila delovanja v mednarodni operaciji in poda nacionalne omejitve. Jasna opredelitev nacionalnih omejitev predstavlja jasno podlago za morebitno kasnejšo odgovornost kršitev teh omejitev v okviru kazenskega, prekrškovnega, disciplinskega ali pravdnega postopka. Prispevek obravnava pravila delovanja in nacionalne omejitve na splošno in v Sloveniji ter izpostavlja glavne problematike odgovornosti za kršitev nacionalnih omejitev pravil delovanja.

Metode:

Avtorja uporabljata metodo analize literature s tega področja in pravnih virov, v zvezi s tem pa tudi metodo opisovanja, metodo analize in sinteze, induktivno-deduktivno metodo ter metodo kompilacije.

Ugotovitve:

Zaradi zagotavljanja pravne varnosti ter večje učinkovitosti postopkov je pomembno, da so nacionalne omejitve vojaške misije vnaprej določene in da se v primeru njihovih kršitev tudi uveljavlja pravno odgovornost v pravnih postopkih. Za to se uporablja splošna slovenska kazenska zakonodaja, pri tem pa se odpirajo tako pravna kakor tudi praktična vprašanja. Za prekrškovno odgovornost pripadnikov slovenske vojaške misije v tujini ni pravne podlage, saj se država gostiteljica svoji jurisdikciji za prekrške običajno odpove, slovenski Zakon o prekrških (2011, 2013) pa vsebuje le teritorialno načelo. Po drugi strani pa slovenska zakonodaja omogoča disciplinsko in odškodninsko odgovornost pripadnikov slovenskih vojaških misij za kršitev nacionalnih omejitev.

Izvirnost/pomembnost prispevka:

Članek na celosten, kritičen in poglobljen način obravnava tematiko, ki je relevantna za Slovensko vojsko in slovensko pravosodje, saj se Slovenija udeležuje mednarodnih vojaških misij. Izsledki bodo relevantni za pripravo vojaških misij, izobraževanje pripadnikov misij ter morebitne izboljšave pravne podlage.

UDK: 343:355/359

Ključne besede: vojaška misija, kazenska odgovornost, pravila delovanja, nacionalne omejitve, disciplinska odgovornost, odgovornost za prekršek

National Caveats for Rules of Military Engagement in International Operations and Consequences of Their Violation

Purpose:

Armed forces units participating in any military operation within a spectrum of military operations must comply with certain rules and norms. Nevertheless, joint rules of engagement applicable to international forces are not always suitable for all participating countries. In such a case, individual countries may determine their own national rules of engagement for given international operations and place specific national caveats on the use of their forces. An unambiguous definition of national caveats serves as a clear basis for potential and subsequent enforcement of responsibility for any acts constituting violation of the caveats in criminal, misdemeanour, disciplinary, or civil proceedings. The article addresses the rules of engagement and national caveats in general as well as in Slovenia, emphasising the main issues regarding responsibility for violations thereof.

Design/Methods/Approach:

The authors use the method of analyzing expert literature and legal sources, as well as the descriptive method, the method of analysis and synthesis, the inductive-deductive method, and the compilation method.

Findings:

In order to ensure legal security and a higher level of efficiency of proceedings, it is important that national caveats of military operations be determined in advance and that, in the event of their violation, legal responsibility is enforced in legal proceedings. In the case of Slovenia, the general criminal legislation is applied, which gives rise to both legal and practical issues. There are no legal grounds for misdemeanour liability of Slovenian service members participating in military operations abroad, as the host nation usually renounces its misdemeanour jurisdiction, while the Slovenian Minor Offences Act-1 contains the territorial principle only. On the other hand, Slovenian legislation provides for disciplinary and damage liability for violation of national caveats.

Originality/Value:

The article is a comprehensive, critical, and in-depth analysis of the topic that is important for the Slovenian Armed Forces and Slovenian justice administration, as Slovenia participates in international military missions. The conclusions will be relevant in preparing military missions, education and training of service members to be deployed to missions, and for potential improvements to the legal basis.

UDC: 343:355/359

Keywords: military mission, criminal liability, rules of engagement, national caveats, disciplinary accountability, misdemeanour liability

1 UVOD

Vsaka država ima glede svojih oboroženih sil na voljo vsaj tri možnosti. Lahko jih sploh nima, lahko jih razvija unilateralno, samostojno ali pa multilateralno, torej v sodelovanju z drugimi državami in v okviru večnacionalnih oboroženih sil – v zavezništvu. Opozoriti je treba, da pri sodelovanju oboroženih sil dveh ali več držav ločimo dve vrsti sodelovanja, in sicer zavezništvo in koalicijo. Bistvena razlika med obema vrstama sodelovanja je, da je zavezništvo trajnejše, s širšim namenom in cilji ter tesnim politično-vojaškim sodelovanjem; koalicija pa je navadno ustanovljena *ad hoc* in namenjena sodelovanju oboroženih sil držav v posameznem primeru (Weitsman, 2010). Države, na primer članice zveze NATO, danes razvijajo svoje oborožene sile za lastne potrebe in potrebe zavezništva. Sledijo svojim nacionalnim interesom, hkrati pa se prilagajajo potrebam zavezništva.

Skozi zgodovino so se države pogosto odločale za ustanavljanje in sodelovanje v multilateralnih oboroženih silah. Da so se odločale za to, so vedno morali biti izpolnjeni določeni pogoji. Šibkejše države so navadno sklepale zavezništva za zaščito pred dominantno silo. Na ta način se je ustvarjala bipolarnost in s tem ravnotežje ter *status quo*. Antični Grki so ustanovili zavezništvo za obrambo pred Perzijci, švicarski kantoni so združili sile pred naraščajočo močjo Habsburžanov, Združene države Amerike (ZDA), Kanada in države zahodne Evrope so ustanovile NATO kot odgovor moči Sovjetske zveze in njenih satelitov itd. Zavezništva so bila torej vedno odgovor na neke strukturne pogoje in razmerje moči. Države pa vstopajo v zavezništvo ne samo zaradi ustvarjanja ravnotežja z nasprotno, dominantno silo, ampak tudi zato, da preprečijo drugi državi, da postane premočna in vsiljuje svojo voljo ostalim. Hkrati zavezništvo šibkejšim državam omogoča prikazovanje svoje moči navzven, proti tretjim državam (Jones, 2007).

Šibkejše države so močnejše, kadar združijo svojo vojaško silo, združevanje vojaških zmogljivosti (moštva, orožja in vojaške tehnologije) pomeni prihranek za posamezno državo, hkrati pa povečuje njeno moč navzven. Zavezništvo je vsekakor dobičkonosno! Zavezništvo posamezno državo razbremeni določenih stroškov nakupov in vzdrževanja opreme in tehnologije. Države stroške znižajo s tem, da si med sabo razdelijo breme vojaških operacij in, na primer, postkonfliktne obnove. Ne nazadnje zavezništvo zmanjšuje tudi tako imenovani »krvni davek« posamezne države, saj so druge zaveznice pripravljene žrtvovati življenja svojih vojakov. Toda sodelovanje različnih oboroženih sil vedno ogroža nekompatibilnost med članicami. Neusklajeni strateški cilji držav članic zavezništva, neusklajeno vodenje in poveljevanje, nekompatibilna oprema, težave v komunikaciji in različna pravila delovanja ter različna interpretacija pravnih norm lahko pomenijo nepotrebne civilne in vojaške žrtve, slabo izvedene operacije in celo napetosti med zaveznicami. Zato so za vsako zavezništvo izjemno pomembni procesi načrtovanja skupnih sil, koordinacija strategij in doktrin, integracija sil s skupnim usposabljanjem in skupnimi vajami ter zagotovitev interoperabilnosti in kompatibilnosti sredstev, opreme in tehnologije (Jones, 2007).

Slovenija od leta 1997 sodeluje v mednarodnih operacijah kriznega odzivanja v okviru Organizacije združenih narodov (OZN), zveze NATO in Evropske unije (EU). Slovenska vojska mora pri delovanju v mednarodnih operacijah spoštovati

pravila delovanja oboroženih sil v mednarodni operaciji, hkrati pa delovati tudi v skladu z mednarodnim in slovenskim pravom. Kadar pravila delovanja mednarodnih sil niso v skladu s pravom, ki ureja delovanje Slovenske vojske, mora država na ta pravila delovanja podati nacionalne omejitve, s katerimi prepreči kršenje predpisov, ki veljajo za Slovensko vojsko.[1]

2 PRAVILA DELOVANJA OBOROŽENIH SIL IN NACIONALNE OMEJITVE

Vsaka vojaška sila, ki opravlja zadane naloge, mora poznati cilj svojega delovanja, svoje zmožnosti, sredstva, s katerimi bo dosegla zadani cilj, svoje omejitve in prepovedi. Oborožene sile, ki delujejo v katerikoli operaciji v spektru vojaških operacij (humanitarne misije, operacije ohranjanja miru, operacije vsiljevanja miru, omejena vojna in totalna vojna) morajo delovati v skladu z določenimi pravili in normami (od običajev, do zakonskih določil nacionalnega prava ali določil mednarodnega prava).

Pri delovanju večnacionalnih enot (tudi v zavezništvu) naletimo na določene težave pri poenotenju delovanja oboroženih sil različnih držav, ki delujejo skupaj in imajo isto nalogo in isti cilj v okviru neke operacije. Kljub temu, da države članice zavezništva težijo k poenotenju strategij, doktrin in taktičnih postopkov, poenotenju sredstev, opreme in tehnologije ter celo skušajo poenotiti predpise, ki določajo delovanje oboroženih sil, med državami ostajajo razlike. Oborožene sile različnih držav v zavezništvu nikoli niso enako usposobljene, nimajo popolnoma enake oborožitve, opreme in tehničnih sredstev, nimajo enakih predpisov, ki določajo, kako oborožene sile ali posamezni pripadnik oboroženih sil lahko ravna v različnih situacijah, in končno, države včasih različno tolmačijo določbe mednarodnega prava.

2.1 Pravila delovanja oboroženih sil[2]

Pravila službe v Slovenski vojski (2009) v 314. točki določajo: »Splošna pravila za delovanje Slovenske vojske (v nadaljnjem besedilu: pravila delovanja) določajo splošne postopke posameznikov, skupin, enot ali poveljstev pri opravljanju bojnih in nebojnih nalog. Pravila delovanja določajo tudi okoliščine, pogoje in omejitve ter stopnjo in način, pod katerimi lahko posamezni pripadnik, skupina, enota ali začasna sestava oziroma poveljstvo Slovenske vojske (v nadaljnjem besedilu: pripadnik in enota) v posameznih primerih uporabijo silo«.

Zveza NATO definira pravila delovanja kot »navodila oboroženim silam (in posameznikom), ki definirajo okoliščine, pogoje, stopnjo in način, kdaj se sme uporabiti silo ali druge ukrepe« za izvedbo naloge (NATO legal deskbook, 2010: 254).

1 *To določata 48.a člen Zakona o obrambi (2004) in 25. člen Zakona o službi v Slovenski vojski (2007).*

2 *Ang. Rules of Engagement.*

Pravila delovanja oboroženih sil so torej »navodila« države oziroma mednarodne organizacije svojim oboroženim silam, ki določajo, kdaj, kje, zakaj in kako naj oborožene sile izpolnijo svojo nalogo ter kdaj, kje, kako in pod kakšnimi pogoji lahko uporabijo tudi silo.

Pravila delovanja so izjemno pomembna za delovanje večnacionalnih oboroženih sil. S pravili delovanja, ki naj bi veljala za vse večnacionalne oborožene sile v določeni mednarodni operaciji, se skuša poenotiti delovanje teh sil. Pravila delovanja se predpišejo za vsako mednarodno operacijo posebej. V današnjem svetu mednarodne operacije potekajo v izjemno kompleksnem okolju. Na oblikovanje pravil delovanja vplivajo pravni in politični vidiki ter operativne zahteve mednarodne operacije.

Pravni vidiki postavljajo normativni okvir pravil delovanja oboroženih sil, v katerega se skuša zajeti tudi politične vidike in operativne zahteve za izvedbo mednarodne operacije. Pri določanju pravil delovanja se tako vedno upošteva:

- mednarodno pravo;
- nacionalno pravo sodelujočih držav v mednarodni operaciji;
- pravo države ali držav, kjer se izvaja mednarodna operacija;
- pravo tretjih držav (npr. kadar preko njih poteka transport mednarodnih sil, njihove oborožitve in opreme);
- drugi predpisi, ki lahko vplivajo na izvajanje mednarodne operacije.

Pravila delovanja oboroženih sil v mednarodni operaciji so sestavni del Operativnega načrta (OPLAN[3]) mednarodne operacije.

Pri pripravi pravil delovanja oboroženih sil v mednarodni operaciji se upoštevajo naslednja načela (NATO legal deskbook, 2010: 258):

- načelo (vojaške) nujnosti,
- načelo razlikovanja,
- načelo proporcionalnosti,
- načelo humanosti in
- načelo prepovedi diskriminacije.

Pravila delovanja navadno vsebujejo naslednje (NATO legal deskbook, 2010: 258–259):

- **Mandat operacije.** Opišejo se politične, diplomatske in pravne okoliščine, ki determinirajo naravo mednarodne operacije.
- **Mednarodno pravo/mednarodno vojno in humanitarno pravo.** Navedejo se mednarodnopravne določbe, ki determinirajo mednarodno operacijo. Navedejo se lahko tudi posamezna določila mednarodnega prava s področja človekovih pravic ali celo vojnega in vojaškega prava, kadar to zahteva narava mednarodne operacije.
- **Posebnosti nacionalnih pravnih predpisov držav udeleženk.** Navedene so posamezne države udeleženke mednarodne operacije, ki uveljavljajo nacionalne omejitve in zato nekatere določbe pravil delovanja izvajajo po svojem nacionalnem pravu in torej drugače od večine drugih držav udeleženk v operaciji.

3 *Ang.: OPLAN – Operational Plan.*

- **Silobran.** Zaradi različnih določb in interpretacij silobrana v posameznih državah, udeleženkah mednarodne operacije, je ta del pravil delovanja vedno natančno določen. Države silobran vedno interpretirajo in izvajajo v skladu s svojim nacionalnim pravom, zato je v pravilih delovanja mednarodnih sil to vedno posebej poudarjeno.
- **Varovanje oseb in premoženja s posebnim statusom.** V tem delu pravila delovanja določajo, kdaj in kako smejo ravnati mednarodne sile, kadar varujejo osebe in premoženje s posebnim statusom, kot na primer pripadnike mednarodnih organizacij, humanitarnih organizacij, nevladnih organizacij in drugih, ki opravljajo naloge na območju operacije.
- **Ključne definicije.** Pravila delovanja vsebujejo tudi ključne definicije pojmov, ki so pomembni za enotno razumevanje in izvajanje nalog mednarodne operacije.

Pravila delovanja oboroženih sil v mednarodni operaciji so torej najmanjši skupni imenovalec in konsenz vseh deležnikov mednarodne operacije, na kakšen način se bo izvajala mednarodna operacija, da bodo doseženi cilji operacije.

2.2 Nacionalne omejitve

Pravila delovanja oboroženih sil v mednarodni operaciji se pripravljajo skupaj z Operativnim načrtom mednarodne operacije, pri pripravi pa sodelujejo države, ki bodo v operaciji sodelovale. Kljub temu, da se išče konsenz, se neredko zgodi, da se vse države ne strinjajo oziroma ne morejo izvajati nalog, kot jih določijo skupna pravila delovanja mednarodnih sil. Težava se lahko pojavi tudi, kadar se posamezna država vključi v delovanje mednarodnih sil po začetku operacije in ni sodelovala pri pripravi pravil delovanja ter ima določene zadržke pri izvajanju pravil delovanja.

V takšnih primerih lahko posamezna država, ki sodeluje v mednarodni operaciji določi svoja, nacionalna pravila delovanja v mednarodni operaciji in na skupna pravila delovanja mednarodnih sil poda nacionalne omejitve. Nacionalna pravila delovanja v mednarodnih silah ne smejo širiti pristojnosti skupnih pravil delovanja mednarodnih sil. Nacionalna pravila delovanja so lahko le bolj omejujoča in ne smejo biti v nasprotju s pravili mednarodnih sil (NATO legal deskbook, 2010: 261).

Države podajo nacionalne omejitve glede delovanja svojih oboroženih sil v določeni mednarodni operaciji zaradi:

- **Nacionalnega prava**. Država lahko omeji izvajanje posameznih določil pravil delovanja mednarodnih sil zaradi neskladnosti pravil z nacionalnim pravnim redom. Tipičen primer razlik med nacionalnimi pravnimi redi je področje silobrana.
- **Mednarodnega prava.** Država lahko omeji izvajanje posameznih določil pravil delovanja mednarodnih sil zaradi različne interpretacije mednarodnega prava ali zaradi obveznosti, ki jih ima država na podlagi mednarodnega prava.[4]

4 *Slovenija je na primer podpisnica Ottawske konvencije o prepovedi protipehotnih min, kar pomeni, da Slovenska vojska pri svojem delovanju v nobenem primeru ne sme uporabljati takšnih min.*

- **Nacionalne interpretacije mandata mednarodnih sil.** Država lahko omeji izvajanje posameznih določil pravil delovanja mednarodnih sil zaradi drugačne interpretacije mandata mednarodnih sil v določeni operaciji.
- **Omejevanja in prepovedi iz objektivnih razlogov.** Država lahko omeji ali prepove izvajanje posameznih določil pravil delovanja mednarodnih sil tudi zaradi »političnih« in drugih razlogov. Država lahko recimo prepove uporabo gumijastih nabojev ali solzivca, lahko omeji delovanje svojih enot na posameznih območjih znotraj območja izvajanja mednarodne operacije ali pa omeji oziroma prepove izvajanje določenih nalog zaradi neustrezne opreme ali usposobljenosti svojih oboroženih sil. Državi pri tovrstnem omejevanju ni potrebno opravičevati razlogov za takšno omejevanje skupnih pravil delovanja mednarodnih sil.

3 POSLEDICE KRŠITEV PRAVIL DELOVANJA MEDNARODIH SIL ALI SLOVENSKIH NACIONALNIH OMEJITEV

Če pride do kršitev skupnih pravil delovanja mednarodnih sil ali nacionalnih omejitev v mednarodni operaciji, lahko sledi pravna odgovornost. Samo dejstvo, da je prišlo do kršitve zunaj ozemlja Republike Slovenije in na vojaški misiji, pa povzroča določene posebnosti. Pripadnik oboroženih sil, ki deluje na tujem ozemlju, lahko potencialno odgovarja kazenskopravno, prekrškovno, odškodninsko in disciplinsko.

3.1 Kazenskopravna odgovornost

3.1.1 Vprašanje kazenskopravne jurisdikcije Republike Slovenije

Za razliko od nekaterih drugih držav (na primer Nemčije)[5] Slovenija ne pozna posebne vojaške kazenske zakonodaje, ampak v skladu s 56. členom Zakona o obrambi (2004) vojaške osebe kazensko odgovarjajo po kazenskem zakoniku Republike Slovenije. Tako v skladu s pravili za časovno in krajevno veljavnost kazenske zakonodaje zanje velja Kazenski zakonik (KZ-1, 2012), pravila postopka pa določa Zakon o kazenskem postopku (ZKP, 2012, 2013).

Posebej za opravljanje vojaške službe izven države Zakon o obrambi (2004) v 48.a členu določa, da je pripadnik Slovenske vojske, zoper katerega se uveljavlja disciplinsko, kazensko ali odškodninsko odgovornost za dejanje, ki je bilo storjeno pri opravljanju nalog vojaške službe izven države ali v zvezi z njo, disciplinsko, kazensko in odškodninsko odgovoren po tem zakonu in v skladu s pravnim redom Republike Slovenije.

V zvezi s kazensko odgovornostjo pripadnikov vojaških misij pa se zastavlja kar nekaj pravnih vprašanj, začenši s kazenskopravno jurisdikcijo Republike

5 *Wehrstrafgesetz. Pridobljeno na http://www.gesetze-im-internet.de/wstrg/*

Slovenije. Tukaj se zastavi vprašanje, ali lahko Slovenija konkretno kaznivo dejanje podredi sojenju svojim sodiščem (Bavcon, Šelih, Korošec, Ambrož in Filipčič, 2013). Potencialno kaznivo dejanje je izvršeno izven ozemlja Republike Slovenije, hkrati pa se država gostiteljica običajno s sporazumom o statusu sil (ang. *Status of Forces Agreement)* odpove svoji jurisdikciji v korist države pošiljateljice vojaških sil. Tako sta na primer Prehodna administracija Afganistana ter ISAF[6] za primer vojaške misije v Afganistanu leta 2001 sklenila Vojaško-tehnični sporazum, ki vsebuje tudi določbe o statusu sil, ki pomagajo pri zagotavljanju varnosti v tej državi (annex A).[7] Če član osebja ISAF-a ali njegovega podpornega osebja izvrši kaznivo dejanje ali disciplinsko kršitev na ozemlju Afganistana, je v vsakem primeru in ne glede na kakršnokoli okoliščino pristojna država storilčevega državljanstva. Država storilčevega državljanstva ima torej izključno jurisdikcijo[8] (aktivno personalitetno načelo), pa čeprav bi na primer Afganistan v skladu s svojo kazensko zakonodajo za to kaznivo dejanje imel jurisdikcijo na podlagi teritorialnega načela (Penal code [Afganistanski kazenski zakonik], 1976). Afganistan se je torej odpovedal jurisdikciji za primere, ko kaznivo dejanje izvršijo člani sil ISAF ali podporno osebje.

Zveza NATO je sprejela tudi svoj sporazum o statusu oboroženih sil, ki podobno ureja situacijo, ko so sile ene države članice poslane na ozemlje druge države članice. V skladu s tem sporazumom ima država pošiljateljica praviloma izključno jurisdikcijo nad kaznivimi dejanji, izvršenimi na ozemlju države gostiteljice s strani pripadnikov sil države pošiljateljice med izvrševanjem vojaške dolžnosti (Agreement between the parties to the North Atlantic Treaty regarding the status of their forces [NATO SOFA], 1951).

Ker se država gostiteljica odpove svoji jurisdikciji, je toliko bolj pomembno, da v državi pošiljateljici veljajo pravila o jurisdikciji, ki omogočajo jurisdikcijo države pošiljateljice tudi v primeru, ko je kaznivo dejanje izvršeno izven njenega ozemlja. V Sloveniji načeloma nimamo problemov z zagotavljanjem pravne podlage za kazenski pregon, saj KZ-1 (2012) pozna kar pet načel, po katerih ima Slovenija kazenskopravno jurisdikcijo.

Teritorialno načelo, v skladu s katerim ima Republika Slovenija jurisdikcijo v primeru, ko je kaznivo dejanje izvršeno na ozemlju Republike Slovenije (KZ-1, 2012), v tem primeru praviloma ne pride v poštev, saj se vojaška misija izvaja izven našega ozemlja. To načelo bi bilo mogoče uporabiti le v primeru, da bi bilo kaznivo dejanje izvršeno na domačem plovilu ali na domačem civilnem zrakoplovu med poletom ali na državnem letalu, ne glede na to, kje sta bila ob izvršitvi dejanja. Bolj relevantna so realno (če je v tujini izvršeno kaznivo dejanje, določeno v 11. členu KZ-1), aktivno personalitetno (državljan Republike Slovenije izvrši v tujini kakšno drugo kaznivo dejanje, kot tisto, našteto v 11. členu, lahko tudi zoper slovenskega državljana ali državo), pasivno personalitetno (tujec izvrši zunaj Republike Slovenije, proti njej ali njenemu državljanu kaznivo dejanje, pa ne gre za kazniva dejanja iz 11. člena KZ-1) in univerzalno načelo (v tujini tujec izvrši kaznivo dejanje zoper tujca ali tujo državo, pa se zaloti na ozemlju Republike

6 *International Security Assistance Force, ki v Afganistanu deluje na podlagi Resolucije VS OZN 1386 iz leta 2001. Več o tem glej Vuk, Vertovšek, Dolenc, Perko in Žokalj, 2010.*

7 *Pridobljeno na http://webarchive.nationalarchives.gov.uk/+/http://www.operations.mod.uk/isafmta.pdf*

8 *3. člen aneksa A sporazuma.*

Slovenije in se ne izroči tuji državi, ali gre za kaznivo dejanje, ki se po mednarodni pogodbi ali po splošnih pravnih načelih, ki jih priznava mednarodna skupnost, preganja v vseh državah, ne glede, kje je izvršeno) (KZ-1, 2012).

Slovenija torej na podlagi splošnih pravil o kazenskopravni jurisdikciji ima jurisdikcijo in s tem potrebno pravno podlago za izvršitev mednarodne obveznosti *aut dedere aut iudicare* (Ambrož et al., 2012).

3.1.2 Ustrezna pravna kvalifikacija kaznivega dejanja

Ker za kazensko odgovornost veljajo pravila KZ-1 (2012), morajo biti za kazensko odgovornost izpolnjeni vsi zakonski znaki relevantnega kaznivega dejanja iz posebnega dela KZ-1, hkrati pa tudi vsi elementi splošnega pojma kaznivega dejanja iz splošnega dela KZ-1 (ravnanje, bit inkriminacije, protipravno in krivda).

Glede relevantnih kaznivih dejanj v prvi vrsti pomislimo na kazniva dejanja iz 14. poglavja KZ-1 (kazniva dejanja zoper človečnost), ker vojaška misija običajno poteka na območju spopadov ali napetosti, in na kazniva dejanja iz 27. poglavja KZ-1 (kazniva dejanja zoper vojaško dolžnost), ker ima večina pripadnikov vojaške misije status vojaške osebe, a je seveda glede na dejansko stanje in okoliščine primera mogoče govoriti o kazenski odgovornosti za katero koli kaznivo dejanje iz posebnega dela KZ-1 (2012).

V zvezi s kaznivimi dejanji zoper človečnost pa se zastavlja dilema. Kazniva dejanja, ki jih slovenski vojaki morebiti izvršijo na vojaški misiji, je namreč lahko bodisi vojno hudodelstvo ali kakšno drugo kaznivo dejanje iz poglavja kaznivih dejanj zoper človečnost bodisi »navadno« kaznivo dejanje iz drugih poglavij KZ-1. Subsumcija vojakovega ravnanja pod ustrezno kazenskopravno določbo je odvisna tudi od tega, ali je bilo ravnanje izvršeno v povezavi ali med (mednarodnim ali notranjim?) oboroženim spopadom. Vojno hudodelstvo je namreč mogoče izvršiti zgolj v povezavi z ali med oboroženim spopadom,[9] za »navadno« kaznivo dejanje pa ni tega predpogoja. Uboj civilista s strani vojaške osebe lahko torej predstavlja vojno hudodelstvo, če je bilo izvršeno v povezavi z oboroženim spopadom (KZ-1, 2012), v nasprotnem primeru pa gre za navadno kaznivo dejanje uboja ali umora po 115. ali 116. členu KZ-1.

Oborožen spopad je zakonski znak, katerega obstoj bo moralo ugotavljati slovensko sodišče, ko bo odločalo o kazenski odgovornosti slovenskega vojaka. Če tega zakonskega znaka ni, potem je kaznivo dejanje vojnega hudodelstva izključeno že na ravni biti inkriminacije. Ostaja pa še vedno možnost, da bo sodišče izdalo obsodilno sodbo in ugotovilo kazensko odgovornost za »navadno« kaznivo dejanje na podlagi istega dejanskega stanja. Sprememba kvalifikacije v nasprotni smeri (torej iz navadnega kaznivega dejanja v vojno hudodelstvo) pa s strani sodišča ni dopustna, ker običajno pomeni spremembo v hujšo

9 *Glej na primer sodbo Mednarodnega kazenskega sodišča za nekdanjo Jugoslavijo Tadić, IT-94-1, odločitev pritožbenega senata o pritožbi obrambe glede pristojnosti, 2. 10. 1995 (Mednarodno kazensko sodišče za nekdanjo Jugoslavijo, 1995) in ustrezne določbe Znakov kaznivih dejanj k vojnim hudodelstvom iz Rimskega statuta (Rome Statute of the International Criminal Court, 2002). Določbe vojnih hudodelstev v KZ-1 (2012) so namreč skoraj dobesedno prepisane iz Rimskega statuta.*

kvalifikacijo,[10] zato bo še toliko bolj pomembna vloga tožilca in njegova presoja, ali gre za oborožen spopad ali ne in posledično, kakšno pravno opredelitev bo določil v obtožnem aktu. Sam tožilec bi si sicer do konca glavne obravnave lahko premislil in spremenil pravno kvalifikacijo (ZKP, 2012, 2013), sodišče pa možnosti spremeniti pravno kvalifikacijo v hujšo nima. Po izdani sodbi je na drugi stopnji mogoča sprememba obtožnega akta s strani upravičenega tožilca le še v korist obdolženca (ZKP, 2012, 2013).

Je pa zanimivo, da bo končna odločitev o tem, ali v določenem primeru obstaja oborožen spopad in za kakšno vrsto oboroženega spopada sploh gre, prepuščena posameznemu (nacionalnemu) sodišču, čeprav na mednarodni ravni oziroma v poveljstvu oboroženih sil ne bi bilo soglasja o tem oziroma se ne bi priznalo, da oborožen spopad dejansko obstaja, ker bi to potegnilo za seboj posledice iz mednarodnega humanitarnega prava in prava oboroženih spopadov.[11]

Pravilna kvalifikacija kaznivega dejanja je relevantna še z enega vidika. Če je bilo izvršeno mednarodno hudodelstvo, za katero ima jurisdikcijo tudi Mednarodno kazensko sodišče (MKS), ki deluje na podlagi Rimskega statuta (Rome Statute of the International Criminal Court, 2002), je Slovenija dolžna učinkovito preganjati storilca takega kaznivega dejanja. V primeru mednarodnih hudodelstev bi namreč MKS prevzelo kazenski pregon, če jih Slovenija ne bi mogla ali hotela učinkovito preganjati. To predstavlja posredno prisilo k primerni pravni podlagi za pregon in seveda tudi k dejanski izvedbi le-tega v situacijah, za katere bi MKS imelo jurisdikcijo na podlagi teritorialnega ali aktivno personalitetnega načela držav podpisnic, razen če bi situacijo obravnavalo na predlog Varnostnega sveta, v katerem primeru potem ni omejitev (Rome Statute of the International Criminal Court, 2002). Za vojaške misije, ki jih trenutno izvaja Slovenija,[12] bi MKS imelo jurisdikcijo vsaj na podlagi aktivno personalitetnega načela, saj je Slovenija podpisnica statuta, pri določenih pa tudi na podlagi teritorialnega načela, saj so tudi države gostiteljice same podpisnice Rimskega statuta.[13]

3.1.3 Udeležba pri kaznivem dejanju

Odpira se tudi nekaj zanimivih vprašanj glede udeležbe pri kaznivem dejanju. Kazenskopravno odgovarja običajno sicer tisti, ki sam, neposredno in fizično izvrši kaznivo dejanje (KZ-1, 2012), kazenskopravno pa odgovarjajo tudi drugi udeleženci pri kaznivem dejanju (KZ-1, 2012), vendar pa se prav pri kaznivih dejanjih iz 14. poglavja pojavi možnost odgovornosti na podlagi

10 *Na primer sprememba iz uboja (do 15 let zapora) v vojno hudodelstvo (najmanj petnajst let) naklepnega pobijanja. Glej tudi 354. člen ZKP (2012, 2013).*

11 *Na primer statut vojnih ujetnikov, borcev itd. Je pa pri tem treba upoštevati izrecno določbo 319. člena Pravil službe v Slovenski vojski (2009), v skladu s katerim so pripadniki Slovenske vojske med delovanjem dolžni spoštovati Zakon o obrambi (2004) in Zakon o službi v Slovenski vojski (2007), pravila službe, sprejete mednarodne pogodbe ter mednarodno vojno in humanitarno pravo, ne glede na to, kako je v skladu z mednarodnim pravom opredeljen konflikt ali operacija, v kateri so udeleženi, in ne glede na to, ali določila mednarodnega vojnega in humanitarnega prava spoštuje tudi sovražna stran.*

12 *V mesecu februarju 2014 so to Kosovo, Afganistan, Libanon, Sirija, Bosna in Hercegovina, Makedonija, Srbija ter Mali.*

13 *Afganistan, Bosna in Hercegovina, Makedonja, Srbija ter Mali.*

drugih udeležbenih oblik, tipičnih za mednarodno kazensko pravo. V okviru mednarodnega kazenskega prava se tožilski pregon na podlagi strategije pregona običajno usmerja na oblikovalce politik mednarodnih hudodelstev in ne toliko na neposredne storilce kaznivih dejanj (ang. *foot soldiers*). To seveda ne pomeni, da slednji ne izpolnjujejo vseh pogojev za kazensko odgovornost, ampak zgolj to, da se tožilec po navadi pri njih ne odloči za kazenski pregon zoper njih.

V skladu s KZ-1 neposredni storilci kaznivega dejanja odgovarjajo kot storilci, drugi udeleženci pa na podlagi klasičnih udeležbenih oblik (sostorilstvo, posredno storilstvo,[14] napeljevanje[15] in pomoč), v poštev bi prišla tudi odgovornost organizatorjev in članov hudodelskih združb, posebej za mednarodna hudodelstva pa KZ-1 predvideva kot posebno kaznivo dejanje odgovornost vojaških poveljnikov in drugih nadrejenih (ang. *command responsibility*). Tako se kaznuje vojaški poveljnik za kazniva dejanja iz 100. do 103. člena KZ-1, ki so jih storile enote pod njegovim dejanskim poveljstvom in nadzorom, ker ni pravilno opravljal nadzora nad temi enotami in ni izvedel vseh primernih in potrebnih ukrepov v okviru svojih pooblastil za preprečitev ali ustavitev teh kaznivih dejanj ali za predložitev zadeve pristojnim organom v preiskavo in pregon, čeprav je vedel, da so njegove enote storile ali da bi v danih okoliščinah lahko storile taka kazniva dejanja. Enako se kaznuje oseba, ki dejansko nastopa kot vojaški poveljnik, ali oseba, ki v civilni organizaciji ali podjetju dejansko izvaja vodstveno oblast in nadzorstvo, z milejšo kaznijo pa vojaški poveljnik ali oseba, ki dejansko nastopa kot vojaški poveljnik, ali oseba, ki v civilni organizaciji ali podjetju dejansko izvaja vodstveno oblast in nadzorstvo, ki bi moral ali mogel vedeti, da so njegove enote storile ali bi v danih okoliščinah lahko storile kazniva dejanja iz 100. do 103. člena KZ-1 (KZ-1, 2012).

Ta določba pa ima omejen domet, saj je že z jezikovno razlago mogoče ugotoviti, da velja samo v primeru genocida, vojnega hudodelstva, hudodelstva zoper človečnost in agresije, za ostala kazniva dejanja pa je mogoče uporabiti le klasične oblike udeležbe.

3.1.4 Kaznivo dejanje, izvršeno na ukaz nadrejenega

Za presojo kazenske odgovornosti vojaških oseb na vojaških misijah je relevantno tudi dejstvo, da je po vojaški zakonodaji podrejena vojaška oseba *dolžna* izpolniti ukaz in da je le izjemoma ta dolžnost *ne obvezuje*, še manj pa je primerov, ko ukaza *ne sme* izpolniti (Pravila službe v Slovenski vojski, 2009; Zakon o obrambi, 2004; Zakon o službi v Slovenski vojski, 2007).

Ukaza podrejeni ne sme izpolniti, če gre za ukaz, ki je v nasprotju z mednarodnim vojnim ali humanitarnim pravom, ali če je očitno, da bi vojaška oseba z izvršitvijo ukaza izvršila kaznivo dejanje (Deisinger, 2002; Pravila službe v Slovenski vojski, 2009; Sancin, Švarc in Ambrož, 2009; Zakon o obrambi, 2004).

Ta ureditev velja za čas vojne, saj je v naslednji točki Pravil službe v slovenski vojski določeno, da lahko vojaška oseba *a contrario* v času miru odkloni še izvršitev ukaza, ki pomeni neposredno nevarnost za njeno zdravje in življenje, pa ne gre za

14 *Posredni storilec izrablja in vodi ravnanja drugega.*

15 *Ko bi recimo nadrejeni dal ukaz ali kako drugače pri storilcu povzročil odločitev, da izvrši kaznivo dejanje.*

izvajanje pomoči ob naravnih in drugih nesrečah, za sodelovanje v mednarodnih obveznostih ali za opravljanje bojnih nalog v miru (Pravila službe v Slovenski vojski, 2009; Zakon o službi v Slovenski vojski, 2007). V tem primeru podrejena oseba ni dolžna izpolniti ukaza, ni pa tudi dolžna opustiti njegove izvršitve.

Posebej pa je urejeno izvrševanje ukazov v primeru, ko Slovenska vojska in njeni pripadniki delujejo v drugi državi; 320. člen Pravil službe v Slovenski vojski (2009) tako pravi, da Slovenska vojska in njeni pripadniki v drugi državi ne smejo izvršiti ukazov in odločitev, če bi s tem storili kaznivo dejanje po predpisih Republike Slovenije oziroma če so v nasprotju z mednarodnim vojnim in humanitarnim pravom, in s tem skoraj dobesedno ponavlja dikcijo splošnega 43. člena Zakona o obrambi (2004).

To ureditev vojaške zakonodaje pa potem nadgrajuje KZ-1 (2012) v 278. členu, ki ureja izključitev kazenske odgovornosti v primeru izvršitve kaznivega dejanja na ukaz nadrejene vojaške osebe (Zgaga, 2011). Podrejeni se tako ne kaznuje, če stori kaznivo dejanje na ukaz ali povelje nadrejene vojaške osebe in se ta ukaz ali povelje nanaša na vojaško dolžnost, razen če ne gre za vojno hudodelstvo ali kakšno drugo hudo kaznivo dejanje, ali če je vedel, da pomeni izvršitev ukaza ali povelja kaznivo dejanje.

V slovenski literaturi se pojavljajo kritike glede nedoločnosti ureditve v KZ-1 (Kambič, 1996; Korošec, 1994; Korošec in Ambrož, 2007) in že prej v Kazenskem zakoniku RS (1994), saj zakon govori o tem, da se storilec »ne kaznuje«. Ali to pomeni, da gre v tem primeru za odpust kazni, ali za kaznivost kot nov element kaznivega dejanja, za razlog upravičenosti ali opravičenosti (Bačić et al., 1982)? To nam lahko pove šele razlaga določbe.

Storilec se tako ne kaznuje, razen če ne gre za vojno hudodelstvo ali kakšno drugo hudo kaznivo dejanje ali je storilec vedel, da pomeni izvršitev ukaza ali povelja kaznivo dejanje.

V prvi alineji gre za objektivno merilo; kadar gre za vojno hudodelstvo in za drugo hudo kaznivo dejanje, potem kljub ukazu nadrejene vojaške osebe podrejeni ne sme izvršiti ukaza in se v tem primeru ne more sklicevati nanj. Drugo merilo je subjektivno in je oblikovano na podlagi zmote o protipravnosti. Storilec se lahko sklicuje na ukaz nadrejenega, razen če je vedel, da bo z izvršitvijo ukaza izvršil kaznivo dejanje. Pri vseh ostalih kaznivih dejanjih (razen pri vojnih hudodelstvih in drugih hudih kaznivih dejanjih) se zmota o protipravnosti ukaza pri podrejenih domneva, kar je po mnenju mnogih neprimerno za moderno in profesionalno vojsko (Ambrož in Korošec, 2008; Bavcon, Šelih, Korošec, Filipčič in Ambrož, 2009; Bavcon, Šelih, Korošec, Filipčič in Jakulin, 2003; Korošec, 1995).

Ker trenutna ureditev gradi na zmoti o protipravnosti ukaza, splošneje gledano torej na zmoti o protipravnosti, ki vpliva na krivdo storilca, gre lahko pri členu 278 kvečjemu za razlog opravičenosti in ne za razlog upravičenosti (Bavcon et al., 2009; Bavcon et al., 2003).

V slovenski literaturi se pojavlja še dodatna kritika te ureditve, in sicer naj bi bila le-ta nedoločna in v nasprotju z *lex certa* tudi s tega vidika, da ni jasno, katero kaznivo dejanje je hudo kaznivo dejanje (Bavcon et al., 2013). Določeni avtorji predlagajo kot hudo kaznivo dejanje, kaznivo dejanje, za katerega je zagrožena kazen deset let ali več zapora (Deisinger, 2002). Po našem mnenju se je treba

po odgovor zateči k drugemu objektivnemu merilu v tej določbi: k vojnemu hudodelstvu. Za izvršitev vojnega hudodelstva je zagrožena kazen najmanj petnajstih let zapora (KZ-1, 2012). Če želimo, da sta objektivni merili enakomerni in usklajeni, potem menimo, da bi bilo treba na podlagi analogije uporabljati to mejo za opredelitev hudega kaznivega dejanja, saj bi morali imeti obe objektivni merili enako težo.

3.1.5 Kazenskopravni problemi v praksi

Poleg teoretičnih in zakonodajnih vprašanj se je v zvezi s kazensko odgovornostjo pripadnikov vojaške misije pojavilo tudi kar nekaj praktičnih vprašanj, začenši s tem, kdo izvaja pooblastila policije v predkazenskem postopku, kadar so podani razlogi za sum, da je kaznivo dejanje v Slovenski vojski ali v ministrstvu, pristojnem za obrambo, storila vojaška ali civilna oseba, zaposlena v Slovenski vojski oziroma drug delavec, zaposlen na obrambnem področju, oziroma oseba, napotena na misijo v tujini. V skladu z ZKP ima tako z zakonom določen pristojni organ v ministrstvu, pristojnem za obrambo, pooblastila policije v predkazenskem postopku, ki jih določa ta zakon (ZKP, 2012, 2013). Podrobneje potem določa Zakon o obrambi, da imajo delavci obveščevalno-varnostne službe ministrstva, ki opravljajo varnostne naloge in ki jih določi minister, v skladu z zakonom pri preprečevanju, odkrivanju in preiskovanju kaznivih dejanj v ministrstvu in Slovenski vojski pooblastila, kot jih zakon določa za policijo, in še, da vojaška policija lahko preiskuje kazniva dejanja v vojski, za katera je predpisana denarna kazen ali kazen zapora do treh let (Zakon o obrambi, 2004).

Tukaj ni problematična pravna podlaga ali ureditev pooblastil, ampak njihovo izvrševanje v praksi. Problem namreč nastane s prisotnostjo oziroma odsotnostjo organov na sami vojaški misiji. Vojaška policija, če je prisotna, lahko preiskuje samo lažja kazniva dejanja, obratno obveščevalno-varnostna služba ministrstva, in če katera ni prisotna na misiji, ni pristojnega organa za opravljanje opravil v predkazenskem postopku.

Podobno nastaja problem s prisotnostjo oziroma bolje, odsotnostjo drugih državnih organov in udeležencev (pred)kazenskega postopka: državnega tožilca, preiskovalnega sodnika in zagovornika. To seveda vpliva tudi na sam potek predkazenskega postopka, saj je onemogočeno marsikatero procesno dejanje po ZKP. Zaslišanje osumljenca je na primer mogoče samo, če je prisoten zagovornik, prikrite preiskovalne ukrepe odredita preiskovalni sodnik ali državni tožilec, tukaj je še vprašanje nujnih preiskovalnih dejanj, pa vprašanje zavarovanja dokazov itd. (ZKP, 2012, 2013). Zaradi praktičnih problemov se je zato že spremenila ureditev policijskega pridržanja v predkazenskem postopku. To lahko traja maksimalno 48 ur, po 48 urah pa je treba osumljenca ali izpustiti ali pa privesti pred preiskovalnega sodnika, če želi državni tožilec predlagati pripor in kasneje izvajati kazenski pregon, kar je v primeru vojaške misije v (oddaljeni) tuji državi praktično nemogoče. To bi namreč pomenilo, da je v 48 urah treba izvesti vsa opravila, zaradi katerih je bilo pridržanje sploh odrejeno,[16] in osumljenca tudi

16 Na primer za preverjanje identitete, alibija osumljenega ali zbiranje obvestil in dokazov.

privesti pred preiskovalnega sodnika. Zato sedaj velja, da v primeru, če pridržane osebe, ki je na misiji v tujini, zaradi oddaljenosti ali drugih izjemnih objektivnih razlogov ni mogoče brez odlašanja privesti k preiskovalnemu sodniku, ki je pristojen, se o tem takoj obvesti osebo, ki ji je vzeta prostost in državnega tožilca, ob privedbi pa je potrebno pisno obrazložiti zamudo (ZKP, 2012, 2013).

Pravno nerešeno pa ostaja vprašanje nujnih preiskovalnih dejanj in drugih dejanj po ZKP na kraju kaznivega dejanja, kadar v slovenski vojaški misiji niso prisotni organi, ki so po slovenski zakonodaji pristojni opravljati dejanje po ZKP (2012, 2013) in Zakonu o obrambi (2004). Ali lahko prepustimo ta opravila organom tujih držav? Kako bo z veljavnostjo tako pridobljenih dokazov? Dokler to vprašanje ni urejeno na splošni oziroma zakonodajni ravni, bi bilo treba po našem mnenju to dejstvo upoštevati in sprejeti dogovor s konkretnimi državami vsaj v fazi priprav na odhod konkretne vojaške misije.

3.2 Druge oblike pravne odgovornosti

Za razliko od kazenske odgovornosti, za katero Zakon o obrambi (2004) jasno določa, da vojaške osebe kazensko odgovarjajo po kazenskem zakoniku Republike Slovenije, take jasne pravne podlage za prekrškovno odgovornost članov vojaških misij ni mogoče najti.

Hkrati Zakon o prekrških (ZP-1, 2011, 2013) kot temeljni predpis prekrškovnega prava glede slovenske jurisdikcije za prekrške pravi, da predpisi o prekrških, ki jih določi državni zbor ali vlada, veljajo na območju Republike Slovenije; predpisi o prekrških, določenih s strani lokalne samoupravne skupnosti pa le na območju samoupravne lokalne skupnosti, ki jih je izdala. Predpisi o prekrških, ki veljajo na območju Republike Slovenije, se uporabijo tudi proti vsakomur, kdor stori prekršek na ladji, ki je vpisana v pristanišču na območju Republike Slovenije, ali na zrakoplovu, ki je vpisan v register oziroma evidenco zrakoplovov v Republiki Sloveniji, medtem ko sta izven njenega območja. ZP-1 torej določa le teritorialno načelo, tako da pripadniki vojaških misij ne bodo odgovarjali za prekrške, izvršene izven ozemlja Republike Slovenije, razen če ti prekrški ne bodo izvršeni na ladji, ki je vpisana v pristanišču na območju Republike Slovenije, ali na zrakoplovu, ki je vpisan v register oziroma evidenco zrakoplovov v Republiki Sloveniji (ZP-1, 2011, 2013).

Hkrati pa se tudi država gostiteljica odpove svoji jurisdikciji za prekrške s SOFA sporazumom, tako da gre v tem primeru za *de facto* imuniteto pred prekrškovno odgovornostjo na vojaških misijah.

Tudi za odškodninsko odgovornost pripadnikov vojaške misije lahko najdemo pravno podlago v Zakonu o obrambi (2004), v skladu s katerim vojaške osebe odškodninsko odgovarjajo po predpisih, ki urejajo odškodninsko odgovornost javnih uslužbencev. V skladu s Pravili službe v Slovenski vojski je pripadnik Slovenske vojske odškodninsko odgovoren v skladu z Zakonom o obrambi in Zakonom o službi v Slovenski vojski za škodo, ki jo je protipravno povzročil pri ali v zvezi z opravljanjem vojaške službe (Pravila službe v Slovenski vojski, 2009).

Pravna podlaga za odškodninsko odgovornost torej obstaja, vprašanje pa je, ali in kdaj bi Republika Slovenija imela jurisdikcijo za vodenje pravdnega postopka na podlagi tožbe, vložene zoper pripadnika slovenske vojaške misije. To določa Zakon o mednarodnem zasebnem pravu in postopku (1999, 2008), v skladu s katerim to velja zlasti v primeru stalnega prebivališča toženca v Republiki Sloveniji.

V skladu z Zakonom o obrambi (2004) pa so vojaške osebe tudi disciplinsko odgovorne za kršitev vojaške discipline, kar velja tudi za vojaško misijo v tuji državi. Disciplinska odgovornost je natančneje urejena v vojaški zakonodaji (Pravila službe v Slovenski vojski, 2009; Zakon o obrambi, 2004; Zakon o službi v Slovenski vojski, 2007).

4 ZAKLJUČEK

Dosledna in jasna določitev nacionalnih omejitev slovenske vojaške misije je pomembna z več vidikov, tudi z vidika uveljavljanje pravne odgovornosti za njihove kršitve. Jasna opredelitev nacionalnih omejitev najprej predstavlja jasno podlago za morebitno kasnejšo odgovornost kršitev teh omejitev. Jasna podlaga onemogoča ali zelo zmanjšuje kasnejše možnosti za sklicevanje na nepoznavanje pravil oziroma nacionalnih omejitev (t. i. pravna zmota), s tem omogoča lažje uveljavljanje pravne odgovornosti in olajša izvedbo (kazenskega, prekrškovnega, disciplinskega ali pravdnega) postopka. Poleg tega jasne in vnaprej določene nacionalne omejitve zagotavljajo pravno varnost vsem pripadnikom vojaške misije, saj so »pravila igre« določena vnaprej in so z njimi seznanjeni. S tega vidika so pripadniki misije zaščiteni, saj vedo, kaj se od njih pričakuje in kaj je prepovedano oziroma zagotovljena je pravna varnost in gotovost. In nenazadnje, jasno opredeljene nacionalne omejitve omogočajo tudi usklajeno delovanje vojaških misij iz različnih držav z različnimi ureditvami v skupnih vojaških operacijah. Zato je po našem mnenju pomembno, da so nacionalne omejitve vojaške misije vnaprej določene in da se v primeru njihovih kršitev tudi uveljavlja pravno odgovornost v pravnih postopkih. Trenutno pa še vedno obstajajo določene pravne praznine ali pa pomanjkljivosti v praksi, zato si posledično pred morebitnimi kršitvami zatiskamo oči, saj postopek oziroma odziv na kršitve ni urejen in predviden v vseh primerih.

Če pustimo ob strani načelo pravne države in varovanje bistvenih pravnih vrednot, ki terjata uveljavljanje pravne odgovornosti tudi v primeru njihovega ogrožanja oziroma poškodovanja na vojaških misijah, zahteva ustrezen odziv na določene hujše pravne kršitve tudi Rimski statut (Rome Statute of the International Criminal Court, 2002) Mednarodnega kazenskega sodišča (MKS), ki ga je Slovenija podpisala in ratificirala.

Z vidika materialnega kazenskega prava je večino vprašanj mogoče rešiti z uporabo KZ-1 (2012), enako velja za odškodninsko in disciplinsko odgovornost, medtem ko je pri kazenskem postopku več problemov, predvsem zaradi oddaljenosti misije in nenavzočnosti določenih subjektov. To terja ali vnaprejšnjo ureditev določenih vprašanj v sporazumu z drugimi navzočimi državami ali prisotnost pristojnih državnih organov in drugih subjektov kazenskega postopka na kraju, kjer se vodi predkazenski postopek.

Po drugi strani sploh ni podlage za prekrškovno odgovornost pripadnikov slovenske vojaške misije v tujini, saj se država gostiteljica temu običajno odpove, slovenski ZP-1 (2011, 2013) pa vsebuje le teritorialno načelo, kar je z vidika številčnosti in včasih tudi bagatelnosti prekrškov smiselno in tudi praktično, vsaj v primeru težjih prekrškov s tudi zagroženo hudo sankcijo pa je po našem mnenju imuniteta za prekrške vprašljiva, zato bi to vprašanje terjalo zakonsko ureditev. Vsa ta številčna dejanska in pravna vprašanja odpirajo vprašanje, ali ne bi bilo vseeno smiselno razmisliti o vojaškem kazenskem pravu.

LITERATURA

Agreement between the parties to the North Atlantic Treaty regarding the status of their forces [NATO SOFA]. (1951). Pridobljeno na http://www.nato.int/cps/en/natolive/official_texts_17265.htm?selectedLocale=en

Ambrož, M. in Korošec, D. (2008). Der Allgemeine Teil des neuen slowenischen Strafgesetzbuchs. *Jahrbuch für Ostrecht*, *52*(49), 351–362.

Ambrož, M., Bavcon, L., Fišer, Z., Korošec, D., Sancin, V., Selinšek, L. et al. (2012). *Mednarodno kazensko pravo.* Ljubljana: Uradni list Republike Slovenije.

Bačić, F., Bavcon, L., Đorđević, M., Kraus, B., Srzentić, N. in Stajić, A. (1982). *Komentar krivičnog zakona Socijalističke Federativne Republike Jugoslavije*. Beograd: Savremena administracija.

Bavcon, L., Šelih, A., Korošec, D., Ambož, M. in Filipčič, K. (2013). *Kazensko pravo, splošni del.* Ljubljana: Uradni list RS.

Bavcon, L., Šelih, A., Korošec, D., Filipčič, K. in Ambrož, M. (2009). *Kazensko pravo, splošni del*. Ljubljana: Uradni list Republike Slovenije.

Bavcon, L., Šelih, A., Korošec, D., Filipčič, K. in Jakulin, V. (2003). *Kazensko pravo, splošni del*. Ljubljana: Uradni list Republike Slovenije.

Deisinger, M. (2002). *Kazenski zakonik s komentarjem, posebni del*. Ljubljana: GV založba.

Jones, G. S. (2007). *The rise of European security cooperation*. Cambridge: Cambridge Universty Press.

Kambič, M. (1996). Izključitev protipravnosti in krivde pri deliktu damnum iniuria datum kot podlaga današnjemu pravu. *Zbornik znanstvenih razprav Pravne fakultete v Ljubljani*, *66*, 121–151.

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

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

Korošec, D. (1994). Ravnanje po pravno zavezujočem navodilu nadrejenega – izključenost protipravnosti ali krivde? *Zbornik znanstvenih razprav Pravne fakultete v Ljubljani*, *54*, 215–230.

Korošec, D. (1995). O nekaterih vojaških določbah nove slovenske kazenske zakonodaje. *Pravna praksa*, *14*(5), 28–29.

Korošec, D. in Ambrož, M. (2007). Splošni pojem, skrajna sila in odgovornost podrejenih. V A. Šelih (ur.), *Sodobne usmeritve kazenskega materialnega prava* (str. 165–181). Ljubljana: Inštitut za kriminologijo pri Pravni fakulteti v Ljubljani.

Mednarodno kazensko sodišče za nekdanjo Jugoslavijo. (1995). Tožilec proti Dušanu Tadiću, IT-94-1, odločitev pritožbenega senata o pritožbi obrambe glede pristojnosti, 2. 10. 1995.

NATO legal deskbook (2nd ed.). (2010). Pridobljeno na http://publicintelligence.net/nato-legal-deskbook/

Penal code [Afganistanski kazenski zakonik]. (7. 10 1976). *Official Publication of the Government of the Republic of Afganistan*, (13). Pridobljeno na http://aceproject.org/ero-en/regions/asia/AF/Penal%20Code%20Eng.pdf/view

Pravila službe v Slovenski vojski. (2009). *Uradni list RS*, (84/09).

Rome Statute of the International Criminal Court. (2002). Pridobljeno na http://www.icc-cpi.int/nr/rdonlyres/ea9aeff7-5752-4f84-be94-0a655eb30e16/0/rome_statute_english.pdf

Sancin, V., Švarc, D. in Ambrož, M. (2009). *Mednarodno pravo oboroženih spopadov*. Ljubljana: Poveljstvo za doktrino, razvoj, izobraževanje.

Vuk, P., Vertovšek, R., Dolenc, G., Perko, S. in Žokalj, J. (2010). Pravni vidiki sodelovanja Republike Slovenije v Afganistanu. *Bilten Slovenske vojske*, *12*(3), 51–70.

Weitsman, P. (2010). Wartime alliances versus coalition warfare. *Strategic Studies Quarterly*, (Summer), 113–136. Pridobljeno na http://www.au.af.mil/au/ssq/2010/summer/weitsman.pdf

Zakon o kazenskem postopku. (2012, 2013). *Uradni list RS*, (32/12-ZKP-UPB8, 47/13-ZKP-L).

Zakon o mednarodnem zasebnem pravu in postopku. (1999, 2008). *Uradni list RS*, (56/99-ZMZPP, 45/08-ZArbit).

Zakon o obrambi [ZObr-UPB1]. (2004). *Uradni list RS*, (103/04).

Zakon o prekrških [ZP-1]. (2011, 2013). *Uradni list RS*, (29/11-ZP-1-UPB8, 21/13–1H, 111/13-ZP-1I).

Zakon o službi v Slovenski vojski. (2007). *Uradni list RS*, (68/07).

Zgaga, S. (2011). Odgovornost za mednarodno hudodelstvo, izvršeno na ukaz nadrejenega. *Zbornik znanstvenih razprav Pravne fakultete v Ljubljani*, *70*, 259–291.

O avtorjih:

Dr. Sabina Zgaga, doktorica kazenskega prava, je docentka za kazensko pravo na Fakulteti za varnostne vede Univerze v Mariboru. Raziskovalno se ukvarja s kazenskim materialnim in procesnim pravom ter mednarodnim kazenskim pravom. E-mail: sabina.zgaga@fvv.uni-mb.si

Mag. Maj Fritz, magister evropskih in državnih študij, je študent doktorskega študija na Fakulteti za varnostne vede Univerze v Mariboru. Njegovo področje raziskovanja in študija je povezano z obveščevalno-varnostno dejavnostjo, mednarodnimi vojaškimi operacijami in zasebnimi varnostnimi ter vojaškimi podjetji. Zaposlen je na Ministrstvu za obrambo.

Igor Bernik: Cybercrime and Cyberwarfare, (Focus Series). London: ISTE; Hoboken: Wiley, 2014

V Sloveniji smo v zadnjem obdobju priča katastrofalnim naravnim nesrečam in zdi se, da se te vrstijo čedalje pogosteje, skorajda vsako leto. Posebne razmere, ki nastopijo zaradi naravnih pojavov, vplivajo na kritično infrastrukturo družbe in brez dvoma tudi na delovanje informacijskih tehnologij. Šele ko je večje število prebivalcev Slovenije nekaj dni ostalo brez elektrike, smo se začeli resneje spraševati o pomenu vsakdanje tehnologije in naši odvisnosti od nje.

Kakšen pomen ima za človeka današnja tehnologija in kaj se zgodi, ko nam jo je onemogočeno uporabljati? Takoj se pokažejo ranljivosti sistemov, priložnosti uresničitve groženj informacijskim sistemom, možnosti za delovanje kibernetskih kriminalcev in celo za kibernetsko vojskovanje. Zato je knjiga doc. dr. Igorja Bernika (v nadaljevanju avtor) *Cybercrime and Cyberwarfare* še posebej aktualna. Knjiga je januarja 2014 izšla pri ugledni mednarodni založbi Willey. Pomembnost in aktualnost tematike dela se kažeta tudi v dostopnosti knjige na svetovnih knjižnih portalih.

Avtor v omenjenem delu opisuje področji, ki združujeta človeške oz. družbene dejavnike z dogajanjem v kibernetskem prostoru: kibernetsko kriminaliteto in kibernetsko bojevanje. Tako kibernetska kriminaliteta kot kibernetsko bojevanje postajata pereč problem številnih posameznikov, podjetij, vladnih in nevladnih organizacij v svetu in Sloveniji. Zato je to delo še toliko bolj pomembno, saj celovito in na razumljiv način obravnava posamezna področja obeh omenjenih pojavov ter poudari glavne pomanjkljivosti na tem področju: šibko mednarodno sodelovanje in posledično počasno skupno odzivanje in preprečevanje.

Avtor omogoča bralcu vpogled v svet kibernetske kriminalitete in kibernetskega bojevanja. To je svet, ki ga, kot vemo, ne omejujejo državne meje. Omenjena pojava ne opisuje s tehničnega vidika, ampak tako, da razširi bralčevo razumevanje vplivov kibernetske kriminalitete in kibernetskega bojevanja na zagotavljanje celovite informacijske varnosti v organizacijah. Opisani so tako splošni kot konceptualni vidiki zlorab kibernetskega prostora, ki so logično in smiselno (po)razdeljeni v področje kibernetske kriminalitete in kibernetskega bojevanja. Prikazane so razlike med kibernetsko kriminaliteto in kibernetskim bojevanjem, delovanje storilcev ter način preiskovanja in zoperstavljanja napadom kibernetskih storilcev, odzivanje na incidente ter ne nazadnje tudi potrebni ukrepi za izboljšanje stanja. Vse posamezne tematike avtor v nadaljevanju podrobno razdela.

V prvem delu knjige avtor obravnava kibernetsko kriminaliteto, ki jo odlično opiše z vidika storilcev, preiskovalcev in žrtev tovrstne kriminalitete. Omenjena so tudi orodja za izvajanje kibernetskih napadov, vendar delo ne obravnava tehničnih vidikov, saj avtor zapiše, da je del o tehnologiji omenjenega področja dovolj, njegov namen pa je poučiti bralca z družbenega in organizacijskega vidika kibernetske kriminalitete. V nadaljevanju avtor predstavi oblike zaščite pred kibernetskimi napadi, strah uporabnikov pred kibernetskim napadom, metode preiskovanja in stroške odpravljanja posledic kibernetske kriminalitete. Na koncu poglavja omeni tudi mednarodne vidike kibernetske kriminalitete in mednarodno usklajene pravne akte za pregon globalne kibernetske kriminalitete, ki ne pozna in ne priznava državnih meja.

Drugi del knjige je namenjen obravnavi kibernetskega bojevanja. Za začetek avtor pojasni razliko med klasično kibernetsko kriminaliteto in dejanji, ki potekajo v sodobnem kibernetskem prostoru in jih uvrščamo v področje kibernetskega bojevanja. Zatem odgovarja na vprašanja, kdo je vpleten v kibernetsko bojevanje, kakšni so motivi storilcev, kdo so njihove žrtve. Avtor podrobno opiše tudi vlogo nekaterih držav, ki so tako ali drugače vpletene v kibernetsko bojevanje. Kot najmočnejši na tem področju izpostavi ZDA in Kitajsko, sledijo Severna Koreja, Rusija in Indija, ki konkurirajo najmočnejšim ter mali Izrael, ki ima nesorazmerno velik vpliv, tudi zaradi pomoči ZDA in Evrope. Omenjene so tudi države, ki imajo pomembno vlogo v omejevanju kibernetskega bojevanja, tako na nacionalni kot nadnacionalni oz. svetovni ravni, saj kot zapiše avtor, se je potrebno pri zoperstavljanju opreti na lastne sile, če pa želi posamezna država omejiti vplive napadov, mora biti sposobna tudi napasti nasprotne države. Tega, kot je zaradi s Snowdnom povezanimi dogodki zdaj znano tudi nepoznavalcem, se poslužujeta v največji meri ZDA in Kitajska, pa tudi Rusija bistveno ne zaostaja.

Ob koncu avtor izpostavi skupne točke kibernetske kriminalitete in kibernetskega bojevanja. Na podlagi skrbnih analiz obravnavanih področij avtor navede metode, ki se uporabljajo za zaščito pred kibernetsko kriminaliteto in kibernetskim bojevanjem, tako na ravni posameznika kot na ravni organizacij in držav. Predlaga smernice razvoja na obravnavanih področjih; mednarodno sprejete pravne akte, izboljšanje mednarodnega sodelovanja, premik v glavah odgovornih od nacionalnega v globalno in splošno zaščito informacijskih sistemov na višjem nivoju. Predstavitev tematike zaokroži z metodami zaščite, ki jih moramo upoštevati vsi uporabniki, tako posamezniki, organizacije kot tudi države s svojimi institucijami, da se zavarujemo pred kibernetskimi napadi. Glede tega avtor posebej izpostavlja pomembnost človeškega dejavnika, predvsem pomen izobraževanja ljudi o nevarnostih kibernetskega prostora, možnostih zaščite v njem, pametnem načinu uporabe informacijske tehnologije ter varnem delovanju uporabnikov v kibernetskem prostoru.

Fakulteta za varnostne vede doslej še ni imela knjige s poglobljeno obravnavo kibernetske varnosti, kibernetske kriminalitete in kibernetskega bojevanja v angleškem jeziku, zato je delo doc. dr. Igorja Bernika pomemben prispevek k širši prepoznavnosti fakultete pri njenem delovanju na različnih področjih informacijske varnosti. Knjiga predstavlja pomemben mejnik v razumevanju in celovitosti pogleda na obravnavano tematiko in je pomembno gradivo pri

načrtovanju smernic razvoja informacijske varnosti ter nadaljnjega raziskovanja te tematike. Izid knjige pri svetovno priznani založbi Willey pa ne pomeni samo veliko priznanje avtorju, ampak krepi tudi ugled Fakultete za varnostne vede in Univerze v Mariboru na področju proučevanja kibernetske varnosti.

Blaž Markelj

Kazalo člankov ter vsebinsko in avtorsko kazalo revije Varstvoslovje za leto 2013

Barbara Erjavec, Nataša Knap

Varstvoslovje je znanstvena revija, ki spodbuja interdisciplinarno razpravo in izmenjavo ugotovitev s področja proučevanja varnosti. Prizadeva si osvetliti pravne, organizacijske, kriminološke, kriminalitetnopolitične, politološke, sociološke, psihološke in druge vidike varnostno relevantnih pojavov in konceptov. Revija prispeva h globljemu razumevanju vloge in delovanja skupnosti, organizacij in posameznikov, ki sodelujejo pri zagotavljanju varnosti.
Članki, objavljeni v reviji Varstvoslovje, so indeksirani v CSA Worldwide Political Science Abstracts, CSA Sociological Abstracts and Criminal Justice Abstracts. Revija Varstvoslovje izhaja štirikrat letno (in sicer marca, junija, septembra in decembra).

Naslov uredništva:
Univerza v Mariboru
Fakulteta za varnostne vede
Kotnikova ulica 8
1000 Ljubljana
Tel: +386 1 300 83 00
Fax: +386 1 230 26 87

Internet: http://www.fvv.uni-mb.si/rV

Glavna in odgovorna urednika:
Bojan Dobovšek, Univerza v Mariboru, Maribor, Slovenija;
Andrej Sotlar, Univerza v Mariboru, Maribor, Slovenija.

Odgovorna urednika angleških številk:
Gorazd Meško, Univerza v Mariboru, Maribor, Slovenija;
Charles B. Fields, Eastern Kentucky University, Kentucky, USA.

Gostujoči uredniki tematskih številk:
Thomas Görgen, German Police University, Muenster, Germany;
Jack R. Greene, Northeastern University, Boston, USA;
Gorazd Meško, Univerza v Mariboru, Maribor, Slovenija.

Tehnično urejanje:
Nataša Knap, Univerza v Mariboru, Maribor, Slovenija;
Jerneja Šifrer, Univerza v Mariboru, Maribor, Slovenija.

ISSN 1580-0253 (print)
ISSN 2232-2981 (online)

Kazalo člankov 2013

leto/številka/stran

Izvirni znanstveni članki

Pregledni znanstveni članki

Predmetno kazalo 2013

Legenda okrajšav – tipologija članka:
1.01 – izvirni znanstveni članek
1.02 – pregledni znanstveni članek
1.03 – kratki znanstveni prispevek
1.04 – strokovni članek
1.19 – prikaz
1.25 – drugo

letnik/številka/stran

Avtorsko kazalo 2013

Legenda okrajšav – tipologija članka:
1.01 – izvirni znanstveni članek
1.02 – pregledni znanstveni članek
1.03 – kratki znanstveni prispevek
1.04 – strokovni članek
1.19 – prikaz
1.25 – drugo

letnik/številka/stran

Navodila avtorjem prispevkov

Splošno	Varstvoslovje je znanstvena revija, ki spodbuja interdisciplinarno razpravo in izmenjavo ugotovitev s področja proučevanja varnosti. Prizadeva si osvetliti pravne, organizacijske, kriminološke, kriminalitetnopolitične, politološke, sociološke, psihološke in druge vidike varnostno relevantnih pojavov in konceptov. Revija prispeva h globljemu razumevanju vloge in 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** Za empirične znanstvene članke priporočamo strukturo **IMRAD**.
Navajanje literature	Seznam literature naj vsebuje le v besedilu navedene vire, urejene po abecednem redu. Celotno navajanje literature mora biti v skladu s sistemom APA.