VARSTVOSLOVJE,
let. 14
št. 3
str. 331-344

Vpliv informacijskega bojevanja na slovenske organizacije

Igor Bernik, Kaja Prislan

Namen prispevka:

Pridobivanje informacijske prevlade z metodami informacijskega bojevanja je oblika organizirane kibernetske kriminalitete, ki se vse pogosteje pojavlja tudi v organizacijski sferi. Predstavljamo stanje tovrstne kriminalitete in družbene odgovornosti do pojava v Sloveniji. Na podlagi prikazanih rezultatov predlagamo priporočila organizacijam pri vzpostavljanju informacijske varnosti. Namen prispevka je ozaveščanje odgovornih v organizacijah o nevarnosti informacijskega bojevanja.

Metode:

Z deskripcijo je predstavljena narava informacijskega bojevanja, stanje v slovenskem organizacijskem prostoru pa je ugotavljano z anketiranjem in statistično obdelavo zbranih podatkov.

Ugotovitve:

Prave informacije omogočajo prednost in konkurenčnost, zato je informacijsko bojevanje s pomočjo sodobne tehnologije preraslo tradicionalne okvirje. V tekmovalnem organizacijskem okolju namreč le prave informacije omogočajo prednost in konkurenčnost. Tehnike informacijskega bojevanja predstavljajo faktor tveganja za informacijsko varnost in poslovni uspeh, glavne grožnje pa izvirajo iz notranjega organizacijskega okolja. Ker so vključene v globalni kibernetski prostor, so pred organizirano kibernetsko kriminaliteto ogrožene tudi slovenske organizacije.

Omejitve:

Reprezentativnost rezultatov je omejena zaradi nezainteresiranosti za predmet raziskave, nerazumevanja obravnavane tematike in neodzivnosti organizacij.

Praktična uporabnost:

Analiza ogroženosti slovenskih organizacij omogoča razumevanje nevarnosti kibernetske kriminalitete in omogoča identifikacijo kritičnih ranljivosti v organizacijski strukturi, obenem pa organizacijam zagotavlja možnost primerjave stanja informacijske varnosti z drugimi organizacijami.

Izvirnost:

Ugotovitve raziskave opozarjajo na prisotnost in nevarnost organizirane kibernetske kriminalitete v Sloveniji in dajejo podlago za nadaljnja preučevanja.

UDK: 343.3/.7:004

Ključne besede: informacijsko bojevanje, kibernetska kriminaliteta, organizacije, Slovenija

The Effects of Information Warfare on Slovenian Organizations in Business and Public Sectors

Purpose:

The achievement of information superiority with information warfare methods is a form of organized cybercrime which is now becoming more obvious also in business environments. We present the current conditions regarding cybercrime and the awareness of this phenomenon in Slovenia, and give organizations recommendations for establishing better information security. The purpose of this paper is to increase the awareness of these issues amongst executives in Slovenian corporations and organizations from the public sector, including the military and police.

Design/Methods/Approach:

We used the descriptive method to outline the nature of information warfare and determined the present state of information security in Slovenian corporations and public sector organizations through the use of questionnaires and a statistical analysis of the compiled data.

Findings:

Information can be a competitive advantage, which is why information warfare, based on modern technology, is bursting out of its traditional frames. In competitive business environments only the right kind of information can be exploited as an advantage. Information warfare techniques are a risk factor to information security in corporations and in the public sector, as they endanger the business success of the former and threaten the operational stability of the latter. The main threats can usually be found within organizational structures. Businesses and organizations from the public sector nowadays interact in the global cyberspace, and since Slovenian organizations are not exempt from this, they, too, are threatened by organized cybercrime.

Research Limitations/Implication:

Statistical representation in our study was limited because of a lack of interest for our research subject, ignorance of these issues, and uncooperativeness on the part of the analyzed Slovenian organizations.

Practical Implication:

This analysis of the information threats to Slovenian organizations in the business and public sector deepens the understanding of how dangerous cybercrime can be, and helps us identify vulnerable spots in organizational structures, and also enables executives to make comparisons between their own information security status and conditions in other organizations.

Originality/Value:

The findings of our research draw attention to the existence of organized cybercrime in Slovenia and its threats to Slovenian businesses and the state sector, and present a basis for future research.

UDC: 343.3/.7:004

Keywords: information warfare, cybercrime, organizations, corporations, business sector, public sector, Slovenia

1 UVOD

Informacijska doba, v kateri živimo, je bistveno spremenila, predvsem pa poenostavila poslovne procese in organizacijske aktivnosti. Kritična odvisnost organizacijske sfere od informacijsko-komunikacijskih tehnologij je omogočila nastanek globalnega kibernetskega prostora, kjer je dostopanje, izmenjevanje in hranjenje informacij izjemno enostavno. Slednje pa je za poslovanje organizacij tudi slabost, saj se zaradi neurejenosti kibernetskega prostora ustvarjajo nove ranljivosti in možnosti neavtoriziranih vstopov v informacijske sisteme. Kriminaliteti v kibernetskem okolju se danes ne more izogniti nihče, še posebej pa so pred tovrstno grožnjo izpostavljene poslovne entitete, saj se najpomembnejše in vredne informacije nahajajo ravno tam. Pri tem se je potrebno zavedati, da odklonska vedenja v kibernetskem prostoru niso zgolj v domeni posameznikov, temveč tehnologijo izkoriščajo tudi številne skupine, ki lahko povzročajo veliko širše in družbeno škodljive posledice kot klasični storilci (Bernik in Meško, 2011). Politično, poslovno in ideološko motivirana kibernetska kriminaliteta je postala ena izmed najbolj perečih, predvsem pa neznanih, področij sodobne družbe. Pri tem družba ne sme dopustiti, da bi bile »... nekatere vrste kibernetske kriminalitete tako razširjene, da so postale družbeno sprejemljive.« (Dimc in Dobovšek, 2010) Širša družbena motivacija, ki se uresničuje s pomočjo informacijske tehnologije, presega posamične interese, krši družbene norme, je v veliko primerih legalna, neopazna in v nekaterih kulturnih okoljih celo legitimna.

Kriminaliteto, ki spada v področje nedovoljenega dostopa do vitalnih informacij imenujemo »informacijsko bojevanje«, saj ogroža in zlorablja informacijski kapital z namenom pridobivanja informacijske moči nad nasprotnikom. Informacije so temeljni cilj storilcev, medtem ko se za doseganje le-tega uporablja sodobna informacijsko-komunikacijska tehnologija. Ugotavljamo, da boj za informacijsko moč poteka na različnih družbenih ravneh, zato se udejanja tudi v različnih pojavnih oblikah. Le-tem je skupen način delovanja, saj v kibernetskem prostoru prihaja do poenotenja tehnik kriminalitete. Informacijsko bojevanje se od klasičnih oblik deviantnosti razlikuje predvsem po motivaciji oz. namenih storilcev, pri čemer se v organizacijskem okolju informacijsko bojevanje pojavlja predvsem v obliki medorganizacijske tekmovalnosti in nelegalnih aktivnosti, povzetih za doseganje konkurenčne prednosti.

1.1 Informacijsko bojevanje na organizacijski ravni

V času kapitalizma in globalizacije je tekmovalnost med komercialnimi organizacijami postala tako agresivna, da velikokrat presega meje dovoljenega.

Konkurenca sili organizacije v nenehen razvoj in izpopolnjevanje, pri čemer imajo veliko prednost večje organizacije v razvitih državah. Tiste v zaostanku pa zato, da bi dohitevale vodilne, uporabljajo najrazličnejše, tudi nelegalne metode. Neavtorizirano dostopanje do tujih informacij in njihova zloraba je del informacijskega bojevanja, ki spada v organizacijski oz. zasebni sektor. Pri pregledu (Knapp in Boulton, 2006) 16-letnega dela (od 1990 do sredine 2005) in raziskav o informacijskem bojevanju je bilo prepoznanih več pomembnih smernic, ki so pokazale, da je primarna tarča kibernetske kriminalitete postala zasebna industrija, hkrati pa se sodobna tehnologija vse pogosteje izkorišča za potrebe industrijskega vohunjenja in napade na manjša podjetja. Informacijsko bojevanje je preraslo tradicionalni vojaški okvir in se zelo razširilo v komercialno sfero. Kot navaja J. Carr (v Slocum, 2010), je temeljni razlog, da se je informacijsko bojevanje preselilo v zasebno sfero, možnost doseganja ravnovesja med neenakovrednimi nasprotniki. To pomeni, da gre za obliko asimetričnega bojevanja, kjer zmožnosti v fizičnem okolju ne vplivajo na tiste v kibernetskem. Mnogi avtorji (npr. Fritz, 2008; Berkowitz, 2003) navajajo, da je razvijanje lastnih tehnik in sposobnosti informacijskega bojevanja pravzaprav nujno potrebno, če se organizacije želijo tovrstni grožnji uspešno zoperstaviti.

Informacijsko bojevanje v organizacijskem okolju z namenom kraje, okvare in zlorabe zaupnih informacij uporablja enake tehnike in orodja, kot jih uporabljajo do sedaj poznani storilci klasične kibernetske kriminalitete. Razlikovanje med posameznimi vrstami deviantnih ravnanj v kibernetskem prostoru je mogoče zgolj na podlagi identifikacije storilca in njegovega motiva, je pa informacijsko bojevanje vsekakor bolje organizirana in načrtovana oblika kriminalitete, zaradi česar so napadi ter vdori v sisteme sofisticirani in težje dokazljivi.

Temeljna orodja informacijskega bojevanja so pravzaprav (Joyner in Lotrionte, 2001; Darnton, 2006, SANS Institute, 2007) dalj časa znani načini delovanja, pri čemer med najpomembnejše tehnike uvrščamo vohunsko programsko opremo (snifferji, keyloggerji ipd.), DOS napade, spoofing, vdore v informacijske sisteme, krajo informacij in socialni inženiring. Poleg teh pa obstajajo tudi druge bolj pogoste in manj sofisticirane možnosti zlorabe informacijskih sistemov (kot npr. virusi, črvi, trojanski konji, spam ipd.), vendar njihova uporaba največkrat ni del informacijskega bojevanja, saj so navadno v domeni posameznikov z individualnimi interesi. Med storilce na tej ravni uvrščamo najrazličnejše skupine (civilne, državne in poslovne), ki lahko z zlorabo tujih poslovnih informacij pridobijo določeno korist (politično ali gospodarsko) in posameznike (hekerje, zaposlene), ki za potrebe naročnika izkoriščajo znanje in sposobnosti (ne)avtoriziranih vstopov v informacijske sisteme.

Najvišja stopnja ogroženosti oz. ranljivosti organizacijskih struktur se kaže predvsem na področju kritične infrastrukture (Siroli, 2006), kot so informacije in komunikacije, energetika, bančništvo in finance, fizična distribucija (transportni sektor) in oskrba ljudi z nujnimi življenjskimi potrebščinami (preskrba z vodo, službe za nujno odzivanje, vladni informacijski sistemi, vojaško informacijsko premoženje ipd.). Onemogočanje, uničenje ali zloraba informacijskih sistemov tovrstnih organizacij, ki nadzirajo elemente kritične infrastrukture, ima lahko velike implikacije na normalno funkcioniranje družbe. Ogroženost se pojavlja tudi

na drugih poslovnih področjih, predvsem tistih, ki so razvojno in poslovno uspešna ter posedujejo za konkurenco in države vredne informacije, npr. avtomobilska, farmacevtska, računalniška in varnostna industrija. Je pa ugotavljanje prisotnosti tovrstnega pojava zelo težavno, saj organizacije o njem le redko poročajo. Kot navaja Vaknin (2009) priznanje oškodovanosti ogrozi zaupanje strank in poslovnih partnerjev, zaposleni pa lahko zaradi tega izgubijo zaposlitev. Pozornost se lahko vzbudi pri ponarejevalcih, konkurenčna podjetja pa izkoristijo negativno publiciteto tekmice. Organizacije zato molčijo iz istih razlogov, zaradi katerih zaupnih informacij ne razkrivajo javnosti.

Ker je pojav informacijskega bojevanja na organizacijski ravni v primerjavi z državno in civilno pojavno obliko najmanj raziskan in posledično tudi nerazumljen, smo izvedli raziskavo v slovenskem organizacijskem okolju o razumevanju narave informacijskega bojevanja in stališčih izpraševancev o njegovi legitimnosti ter razširjenosti v Sloveniji.

2 METODA

Ker se informacijsko bojevanje vztrajno širi tudi v organizacijsko okolje in ker v Sloveniji še ne poznamo stanja tovrstne grožnje, smo z raziskavo analizirali stališča organizacij do posameznih vidikov informacijskega bojevanja. Raziskava je bila izvedena s končnim namenom opozoriti organizacije na nepredvidljivost stanja informacijske varnosti in na nevarnost politične ter poslovno motivirane kibernetske kriminalitete. Izvedena je bila s kvantitativno metodo – anketiranjem. Ankete smo razdelili različnim slovenskim organizacijam, proces zbiranja podatkov pa je potekal v mesecu novembru in decembru 2011. Ciljna populacija so bili zaposleni v slovenskih organizacijah, ki se ukvarjajo z informacijsko varnostjo. V statistično analizo je bilo vključenih 36 podjetij in državnih institucij, pri čemer je bilo skupaj vrnjenih 45 odstotkov od 80 razdeljenih vprašalnikov. Anketni vprašalnik so v večini izpolnjevali strokovnjaki (75 % z višjo, visoko ali univerzitetno izobrazbo in 19,4 % z magisterijem ali doktoratom) zaposleni v varnostnih in IT oddelkih organizacij (skupaj več kot 66 % vseh izpraševancev). Pri tem je 44,4 % organizacij del javnega, preostalih 55,6 % pa del zasebnega sektorja. V raziskavo udeležene organizacije so pretežno velika in srednje velika podjetja (skupaj 77,8 %).

Izbira vzorca ni bila sistematična, saj ne zajema raznolikosti celotnega organizacijskega okolja in zato ni slučajen. V vzorcu so zajeta podjetja različnih velikosti in dejavnosti, vsa pa so pomembna z vidika informacijskega bojevanja (izobraževalne, finančne, varnostne in gospodarske institucije). Za statistično analizo zbranih podatkov je bila uporabljena programska oprema za statistično analizo SPSS.

3 RAZUMEVANJE IN STANJE INFORMACIJSKEGA BOJEVANJA V SLOVENSKIH ORGANIZACIJAH

Preverjali smo naravo in uporabo kibernetskih groženj, storilce, ki ogrožajo uspeh organizacij in informacijsko varnost, ter kako izpraševanci razumejo posamezne vidike informacijskega bojevanja. Analizirano je stanje informacijske varnosti organizacij in stališča do obstoječega zakonodajnega stanja.

Ker je kibernetski prostor glavna domena kibernetske kriminalitete, nas je najprej zanimalo, kako ga izpraševanci dojemajo. Le manjši odstotek izpraševancev je mnenja, da je kibernetski prostor nov, navidezni svet, kjer bi morala veljati posebna pravila (Tabela 1).

Tabela 1: Razumevanje kibernetskega prostora

Kibernetski prostor je:	N	%
Novo navidezno okolje	5	13,9
Nadgradnja realnega sveta	31	86,1
Skupaj	36	100,0

Velika večina je mnenja, da je to nadgradnja ali podaljšek realnega sveta in ga je kot takega potrebno tudi obravnavati z vidika nadzora aktivnosti in pregona različnih oblik kaznivih dejanj. Le-ta postajajo v kibernetskem prostoru vse bolj agresivna in nevarna, s čimer se strinjajo tudi izpraševanci, ki so mnenja, da je danes za uspeh kritičnega pomena ravno informacijska moč (Tabela 2), medtem ko so ostale oblike moči (ekonomska, vojaška in politična) podrejene informacijski prednosti, ki jo ima subjekt pred nasprotnikom.

Tabela 2: Informacijska moč

Za katero moč se bije glavni boj?	N	%
Vojaško moč	2	5,6
Politično moč	4	11,1
Ekonomsko moč	12	33,3
Informacijsko moč	18	50,0
Skupaj	36	100,0

Kljub temu, da so izpraševanci kibernetskemu prostoru in informacijski moči pripisali velik pomen, smo preverili tudi, kako organizacije razumejo informacijsko bojevanje kot grožnjo. Iz tabele 3 je razvidno, da v vzorec zajete organizacije razumejo pomen tovrstnega pojava, saj več kot dve tretjini le-teh (69,4 %) meni, da so to aktivnosti, katerih namen je onemogočiti delovanje nasprotnika s pomočjo sodobne IKT. Večji odstotek (52,8 %) jih je mnenja, da informacijsko bojevanje zajema politično in gospodarsko motivirane kibernetske grožnje. Na prvo mesto postavljajo napade na vladne institucije in nato na konkurenčne organizacije.

Informacijsko bojevanje razumem kot:	N	%
Onemogočanje delovanja nasprotne interesne skupine s pomočjo IT	25	69,4
Politično ali gospodarsko motivirane kibernetske grožnje	19	52,8
Kibernetski napad na vlado in/ ali njene službe	19	52,8
Zlorabo ali spreminjanje informacij konkurenčne organizacije	14	38,9
Zlorabo medijev in propagando	14	38,9
Podporo tradicionalnemu vojskovanju	14	38,9
Zaščitne mehanizme za varnost informacij in IT	12	33,3
Državno superiornost varovanja informacij	7	19,4

Tabela 3: Razumevanje informacijskega bojevanja

Med glavne storilce informacijskega bojevanja izpraševanci uvrščajo vojsko (52,8 %), politične akterje in zasebna podjetja (50 %) ter ideološke skupine (33,3 %). Vloge in možnosti medijev se z vidika nevarnosti in agresivnosti zaveda tretjina izpraševancev, medtem ko so na zadnje mesto postavili nevladne organizacije, ki po njihovem mnenju ne predstavljajo večje grožnje z vidika manipulacije in zlorabe informacijske moči (Tabela 4).

Agresivnost informacijskih bojevnikov	N	%
Vojska	19	52,8
Politika	18	50,0
Zasebna komercialna podjetja	18	50,0
Ideološke in verske skupine	16	44,4
Mediji	12	33,3
Nevladne organizacije	4	11,1

Tabela 4: Akterji informacijskega bojevanja

Tehnike informacijskega bojevanja se po mnenju izpraševancev pojavljajo v obeh sektorjih (javnem in zasebnem) s politično in poslovno motivacijo (Tabela 5). Pri tem je politična motivacija kibernetske kriminalitete pogostejša v javnem sektorju, medtem ko v zasebnem prevladuje poslovna oz. gospodarska motivacija. Po njihovem mnenju se motivi storilcev informacijskega bojevanja prepletajo, saj je politična motivacija prisotna tudi v zasebnem sektorju, hkrati pa je poslovna prisotna tudi v javnem. Informacijsko bojevanje tako ni vezano na določeno okolje ali določene storilce, saj so mnenja, da politični motivi presegajo politično okolje, enako pa se dogaja z gospodarstvom in komercialnim okoljem.

Sektor	Politična kibernetska kriminaliteta %	Poslovna kibernetska kriminaliteta %
Javni	57,00	43,00
Zasebni	32,14	67,86

Tabela 5: Pogostost politične in poslovne kibernetske kriminalitete

Po oceni ogroženosti javnega in zasebnega sektorja nas je zanimalo še, katera področja znotraj dveh sektorjev so pred politično in poslovno motivirano kibernetsko kriminaliteto najbolj ogrožena, pri čemer so izpraševanci ogroženost ocenjevali na tri stopenjski lestvici. V javnem sektorju so kot najbolj izpostavljene subjekte identificirali obveščevalne službe, vojsko in gospodarske organizacije. Najmanj izpostavljena v tem okolju sta zakonodajna oblast in negospodarske službe. V zasebnem sektorju pa so za najbolj ogrožene označili področje informatike in telekomunikacij, farmacevtsko, elektronsko in avtomobilsko industrijo. Trajnostni razvoj in ekologija ter tekstilno-modna industrija pred tovrstno grožnjo naj ne bi bila tako izpostavljeni področji kot ostala. Pri tem standardni odkloni dokazujejo, da so odgovori izpraševancev zelo homogeni (Tabela 6).

Tabela 6: Ogroženost javnega in zasebnega sektorja pred informacijskim bojevanjem

Javni sektor	Povprečna vrednost	Stand. odklon
Obveščevalne službe	2,67	0,63
Vojska	2,47	0,65
Gospodarske javne službe	2,28	0,70
Policija	2,22	0,68
Sodstvo in tožilstvo	2,19	0,71
Zakonodajna oblast	1,89	0,71
Negospodarske službe	1,86	0,72
Zasebni sektor	Povprečna vrednost	Stand. odklon
Informatika in telekomunikacije	2,69	0,53
Farmacevtska in kemična industrija	2,64	0,59
Elektronska in elektro industrija	2,47	0,65
Avtomobilska industrija	2,36	0,64
Mediji	2,25	0,65
Podjetniško-trgovska industrija	2,00	0,72
Trajnostni razvoj in ekologija	1,75	0,65
Tekstilna-modna industrija	1,44	0,56

Ob upoštevanju ugotovitve, da razumejo, kaj je informacijsko bojevanje, je v raziskavi 58,3 % izpraševancev izrazilo mnenje, da tehnike doseganja konkurenčne ali informacijske prednosti, ki so del informacijskega bojevanja, niso legitimne (Tabela 7).

Tabela 7: Legitimnost informacijskega bojevanja

Ali je informacijsko bojevanje legitimen način za doseganje ciljev?	N	%
Da	15	41,7
Ne	21	58,3
Skupaj	36	100,0

To je skladno z ugotovitvami, da tehnike informacijskega bojevanja predstavljajo resno grožnjo njihovi informacijski varnosti z vidika posledic, ki jih

lahko povzročijo. Kljub temu, pa je preostalih 41,7 % mnenja, da informacijsko bojevanje lahko pripomore k uspehu in razvoju njihove organizacije.

Organizacija še ni uporabila nobene izmed tehnik informacijskega bojevanja:	N	%
Da	23	63,9
Ne	13	36,1
Skupaj	36	100,0

Tabela 8: Prisotnost informacijskega bojevanja v organizacijskih aktivnostih

Tabela 8 kaže visok odstotek sprejemanja informacijskega bojevanja, saj ugotavljamo, da je 36,1 % v vzorec zajetih organizacij že uporabil nekatere tehnike te grožnje, da bi dosegel zastavljene cilje. Med uporabljenimi tehnikami so najpogostejše pošiljanje spama, posedovanje (kraja) nedovoljenih informacij in širjenje neresnic o konkurenci. Ostale organizacije naštetih tehnik še niso uporabile.

Med različnimi storilci kibernetske kriminalitete so izpraševanci izpostavili zaposlene – sedanje in bivše kot največjo grožnjo njihovim informacijam v smislu kraje, okvare ali zlorabe (Tabela 9). Takšna ugotovitev je smiselna, saj imajo zaposleni največ znanja in možnosti z vidika dostopanja do zaupnih informacij.

Kateri storilci predstavljajo največjo grožnjo vašim informacijam?	Povprečna vrednost	Stand. odklon
Bivši zaposleni	3,81	1,35
Zaposleni	3,69	1,14
Hekerji, krekerji	3,67	1,31
Vohuni in konkurenčne organizacije	3,03	1,16
Vandali	2,97	1,20
Domače ali tuje vladne službe	2,22	1,15
Nasprotne interesne skupine	1,94	0,83
Ideološke in verske skupine	1,58	0,73

Tabela 9: Storilci kibernetske kriminalitete

Veliko grožnjo njihovi informacijski varnosti predstavljajo še hekerji, vohuni in konkurenčne organizacije, prav tako glavni akterji informacijskega bojevanja, ki informacije pridobivajo z vdori v informacijske sisteme. Kot najmanj ogrožajoče pa so izpostavili vladne službe, nasprotne interesne skupine – društva in ideološke skupine.

Poleg splošnih stališč do informacijskega bojevanja kot kibernetske grožnje in njenega pojava v različnih okoljih, so nas zanimali tudi dejavniki zaviranja organizacijskega uspeha. Kot glavni zaviralec njihovega razvoja (Tabela 10) so izpraševanci označili domačo zakonodajo in konkurenčne organizacije. Najmanj

jih ogroža tuja vladna regulativa, preostalih oblik groženj, ki zavirajo njihov razvoj, pa v raziskavi nismo podrobneje razdelali in zajeli.

Tabela 10: Zaviralci organizacijskega razvoja

Koliko vaš razvoj zavira:	Povprečna vrednost %
Domača vladna regulativa	41,39
Konkurenčne organizacije	21,67
Tuja vladna regulativa	14,72
Skupaj	77,78

Iz kontingenčne tabele (Tabela 11) je razvidno, da javne institucije najbolj onemogoča domača regulativa, domače zasebne organizacije pa njihova konkurenca. Glede pomena zaviralcev med velikimi in majhnim organizacijami ni večjih razlik, pri čemer lahko vidimo, da manjša podjetja domača zakonodaja bolj ovira kot večja. Organizacije, ki aktivno poslujejo v tujini, so v povprečju izrazile večje ovire s tujo in manj z domačo zakonodajo, medtem ko je pritisk konkurence veliko močnejši v mednarodnem kot domačem prostoru. Domača zakonodaja po mnenju izpraševancev tako bolj onemogoča manjše organizacije v javnem sektorju, medtem ko so pred konkurenco bolj izpostavljena zasebna podjetja, ki poslujejo v tujem okolju.

Tabela 11: Kontingenčna tabela o povezavah med zaviralci in organizacijskim okoljem

		Domača vladna regulativa %	Tuja vladna regulativa %	Konkurenčne organizacije %
Sektor	Javni sektor	61	14	7
	Zasebni sektor	26	16	34
Velikost	Majhno podjetje	47	16	23
	Veliko podjetje	34	13	20
Udeležba	V domačem okolju	51	10	11
	V tujem okolju	37	19	30

Ker ugotavljamo, da sta domača in tuja zakonodaja velik zaviralec poslovnega razvoja organizacij, smo želeli oceniti tudi ustreznost zakonske podlage, ki ureja področje kibernetske kriminalitete. Pred tem smo preverili še seznanjenost izpraševancev z zakonodajo. Ugotavljamo, da je poznavanje zakonodaje med izpraševanci dobro, saj je s pravnim področjem kibernetske kriminalitete seznanjeno kar 77,8 % udeležencev v raziskavi. Pri tem jih je 65,7 % mnenja, da je trenutno zakonodajno stanje slabo in neustrezno (Tabela 12). Le 5,7 % pa jih je zadovoljnih s trenutno pravno podlago.

Ocenite trenutno zakonodajo s področja kibernetske kriminalitete:	N	%
Neustrezna in neučinkovita	5	14,3
Slaba	18	51,4
Zadostna	10	28,6
Dobra	2	5,7
Popolna	0	0
Skupaj	35	100,0

Tabela 12: Ustreznost slovenske zakonodaje s področja kibernetske kriminalitete

Statistična analiza rezultatov je v splošnem pokazala, da je razumevanje informacijskega bojevanja kot grožnje v Sloveniji dobro, medtem ko je nadzorstvena, zakonodajna in politična podlaga trenutno neustrezna, kar onemogoča učinkovito zoperstavljanje najhujšim oblikam kibernetskih groženj.

4 RAZPRAVA

Informacijsko bojevanje, kot oblika organizirane kibernetske kriminalitete, je izjemno nepredvidljiv in za klasifikacijo zahteven pojav. Storilec je lahko vsaka država, organizacija ali posameznik, ki pa je lahko hkrati tudi žrtev drugih subjektov (meddržavno, medorganizacijsko in medosebno informacijsko bojevanje). Takšno fleksibilnost novodobne kibernetske grožnje je omogočil ravno globalen kibernetski prostor, ki je odpravil še zadnje ovire pri doseganju zlonamernih ciljev. Tudi izpraševanci so kibernetski prostor večinsko kategorizirali kot podaljšek vojnega bojišča in ekonomskega trga (Tabela 1). Menijo, da sta nadzor in regulacija tovrstnega prostora potrebna v enaki meri, kot smo jima priča v realnosti. Eden glavnih razlogov tega je izjemno enostavno pridobivanje informacijske moči. Le-ta je temelj vseh ostalih oblik moči (Tabela 2), kar pomeni, da so osnova ekonomske, vojaške in politične nadvlade prav informacije, zaradi česar se zaostruje boj za informacijsko nadvlado. Boj za informacijsko moč po mnenju izpraševancev zajema aktivnosti z namenom onemogočiti delovanje nasprotne interesne skupine s pomočjo IKT (Tabela 3). Pri tem kot najpomembnejšo izpostavljajo državno raven informacijskega bojevanja in šele zatem organizacijsko, hkrati pa večinsko informacijsko bojevanje kategorizirajo kot napadalne in manj kot obrambne aktivnosti. Ugotavljamo, da tako kot v teoriji tudi v praksi organizacije še vedno poudarjajo vojaško in manj poslovno naravo tovrstne kibernetske grožnje. Tudi pri identifikaciji najbolj agresivnih storilcev informacijskega bojevanja (Tabela 4) izpraševanci še vedno izpostavljajo državno podprte storilce. Se je pa potrebno zavedati, da natančna kategorizacija narave informacijskega bojevanja ni tako enostavna, kajti različne pojavne oblike, tehnike in motivi se medsebojno prepletajo in niso vezani na določeno poslovno okolje (Tabela 5). Z vidika ogroženosti kot najbolj izpostavljeno področje določajo zasebni sektor in v okviru tega računalniško, farmacevtsko, elektronsko in avtomobilsko industrijo kot najbolj kritična oz. tvegana področja. Pri tem vladne, vojaške in gospodarske institucije prav tako spadajo na seznam potencialnih tarč (Tabela 6). Izpraševanci so torej mnenja, da je

pred tovrstno grožnjo najbolj izpostavljen zasebni sektor, kjer so shranjene skrajno zaupne in vredne informacije, medtem ko so najbolj agresivni akterji, ki takšne informacije ogrožajo, državne narave. Hkrati ugotavljamo, da je razumevanje obravnavane tematike dobro, med izpraševanci pa obstaja ozaveščenost o tem, da je informacijsko bojevanje problem večjih in ne zgolj vojaških razsežnosti.

Za organizacijski uspeh so z vidika storilcev najbolj ogrožajoči akterji informacijskega kapitala organizacij zaposleni (Tabela 9). To pomeni, da le-ti kot storilci predstavljajo največji faktor tveganja. Tudi mednarodna raziskava (Fullbrook, 2009) ugotavlja, da največje grožnje informacijski varnosti prihajajo iz notranjega organizacijskega okolja, saj imajo največji motiv za zlorabo informacij zaposleni, ki imajo neposreden dostop do sistema, kar za Slovenijo ugotavlja tudi Saksida (2010). Zaposleni znotraj organizacije imajo veliko možnosti za dostop do zaupnih podatkov, kar omogoča zlorabe; tako s strani pooblaščenih za dostop do zaupnih podatkov kot tudi zlorabo podatkov s strani zaposlenih, ki niso pooblaščeni za dostop do tovrstnih podatkov. Poleg zaposlenih so izpraševanci kot zaviralec njihovega uspeha in razvoja identificirali tudi domačo zakonodajo, ki onemogoča delovanje javnega sektorja (Tabela 10), kar pomeni da je ogroženost pred kibernetsko kriminaliteto in poslovni uspeh v veliki meri odvisen tudi od trenutnega zakonodajnega stanja. Hkrati pa normativna podlaga odraža družbeno razumevanje in moralna stališča do neke problematike. Izpraševanci so trenutno zakonodajno stanje s področja kibernetske kriminalitete (Konvencija o kibernetski kriminaliteti [MKKKDP], 2004; Kazenski zakonik RS [KZ-1], 2008; Zakon o kazenskem postopku [ZKP], 2007) označili za neustrezno in neučinkovito (Tabela 12), kar pomeni, da je razumevanje kibernetske kriminalitete v družbi in politični ravni nezadostno.

Slovenske organizacije so torej resno ogrožene pred tehnikami informacijskega bojevanja, prav tako pa se le-teh večkrat poslužujejo tudi same (Tabela 8), zato je problematika organizirane kibernetske kriminalitete v slovenskem prostoru veliko kompleksnejša, kot smo predvidevali, saj se informacijsko bojevanje ne pojavlja samo kot grožnja temveč tudi kot način delovanja. Trendi razvoja nakazujejo na to, da bo ta kibernetska grožnja v prihodnosti še nevarnejša in agresivnejša, poleg tega pa različnost storilcev in njihovih motivov onemogoča natančno identifikacijo kritičnih področij. Ob tem je mogoče zaključiti, da stanje informacijske varnosti pred informacijskim bojevanjem potrebuje spremembe, ki so nujne predvsem na zakonodajnem stanju.

Ob pregledu tuje prakse ugotavljamo, da je nujno sprejeti ustrezno strategijo nacionalne varnosti, ki naj poleg preostalih prostorskih domen, ki so kritične za nacionalno varnost, kot takšno izpostavi tudi kibernetsko domeno. Najbolje bi bilo področje kibernetskega okolja – zaradi njegove specifične problematike – urediti v posebni strategiji nacionalne kibernetske varnosti. Pri tem bi kot priporočilo lahko upoštevali Ameriško nacionalno strategijo za zavarovanje kibernetskega prostora (US-CERT, 2003). Pri sprejemanju in oblikovanju zakonodaje se strinjamo z Jurichem (2008), ki predlaga vključevanje nedržavnih akterjev oz. uporabo procesa »bottom-up law making process«, s katerim se lahko identificira in spoštuje faktorje, ki jih potrebuje zasebni sektor, a jih je država spregledala.

Zaščita sodobne IKT je večplasten postopek, ki vsekakor najprej zahteva ustrezno tehnično zaščito (Markelj in Bernik, 2011), zato morajo na mikroravni za ustrezno varnost in zaščito poskrbeti organizacije same, predvsem tiste, ki operirajo s sistemi kritične infrastrukture. Tudi Meško, Bančič, Eman in Fields (2011) pri odpravljanju deviantnih ravnanj priporočajo situacijsko preprečevanje kriminalitete, s katerim težave rešujemo pragmatično in s konkretnimi fizičnimi ukrepi. Opozarjajo pa, da najbolj učinkovita metoda preprečevanja neželenega vedenja zajema ozaveščanje ljudi o različnih oblikah groženj. Slednje predstavlja preventivno ukrepanje, saj z ozaveščenostjo zaposlenih poskrbimo za njihovo odgovorno vedenje. To lahko organizacije dosežejo z dvigom stopnje etike poslovanja in varnostne ozaveščenosti zaposlenih, uporabnikov, poslovnih partnerjev, strank in predvsem vodstva, od katerega je pravzaprav odvisno stanje morale in varnosti v neki organizaciji, s programi informacijskovarnostnega ozaveščanja.

Poleg naštetih predlogov in ukrepov je za ureditev obstoječe problematike informacijskega bojevanja predvsem potrebno razumeti njegovo naravo. Da bi ugotovili, kateri so tisti elementi, ki zahtevajo nujne odzive, je potrebno izvesti analizo nacionalne infrastrukture in same percepcije kibernetske kriminalitete v družbi. Le z dejstvi je mogoče podpreti in načrtovati potrebne zaščitne in preventivne ukrepe. Raziskave informacijskega bojevanja morajo zajeti njegovo dojemanje v organizacijskem okolju ter tako ugotoviti stopnjo njegove uporabe, legitimnosti in razširjenosti. Z iskanjem odgovorov na dileme, izzive in nejasnosti bomo lahko izvedeli, kateri so res najnujnejši koraki, ki jih je potrebno povzeti najprej.

LITERATURA

Berkowitz, B. (2003). *The new face of war: How war will be fought in the 21st century*. New York: Simon & Schuster.

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.

Darnton, G. (2006). Information warfare and the laws of war. V E. Halpin, P. Trevorrow, D. Webb in S. Wright (ur.), *Cyberwar, netwar and the revolution in military affairs* (str. 139-153). New York: Palgrave Macmillan.

Dimc, M. in Dobovšek, B. (2010). Perception of cybercrime in Slovenia. *Varstvoslovje*, *12*(4), 378-396.

Fritz, J. (2008). How China will use cyber warfare to leapfrog in military competitiveness. *Culture Mandala*, *8*(1), 28-80.

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

Joyner, C. C. in Lotrionte, C. (2001). Information warfare as international coercion: Elements of legal framework. *European Journal of International Law*, *12*(5), 825-865.

Jurich, J. P. (2008). Cyber war and customary international law: The potential of a »bottom up« approach to an international law of information opreations. *Chicago Journal of International Law*, *9*(1), 275-295.

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

Knapp, K. in Boulton, W. R. (2006). Cyber-warfare threatens corporations: Expansion into commercial environments. *Information Systems Management*, *23*(2), 76-87.

Markelj, B. in Bernik, I. (2011). Kombinirane grožnje informacijski varnosti pri rabi mobilnih naprav. V *Nove razmere in priložnosti v informatiki kot posledica družbenih sprememb, 18. konferenca Dnevi slovenske informatike* (7 str.). Ljubljana: Slovensko društvo Informatika.

Meško, G, Bančič, K., Eman, K. in Fields, C. (2011). Situational crime-prevention measures to environmental threats. V Gorazd M., Dejana, D. in Charles, F. (ur.), *Understanding and managing threats to the environment in south eastern Europe* (str. 41-68). Dordrecht : Springer.

Saksida, M. (2010). *Politika varovanja informacij s poudarkom na upravljanju s človeškimi viri* (Magistrsko delo). Ljubljana: Fakulteta za varnostne vede.

SANS Institute. (2007). *Corporate Espionage 201*. Pridobljeno na http://www.sans.org/reading_room/whitepapers/engineering/corporate-espionage-201_512

Siroli, G. P. (2006). Strategic information warfare: An introduction. V E. Halpin, P. Trevorrow, D. Webb in S. Wright (ur.), *Cyberwar, netwar and the revolution in military affairs* (str. 32-48). New York: Palgrave Macmillan.

Slocum, M. (2010). Cyber warfare: Don't inflate it, don't underestimate it. *O'Reilly Radar*. Pridobljeno na http://radar.oreilly.com/2010/02/cyber-warfare-dont-inflate-it.html

US-CERT. (2003). *National strategy to secure cyberspace*. Pridobljeno na http://www.us-cert.gov/reading_room/cyberspace_strategy.pdf

Zakon o kazenskem postopku [ZKP]. (2007). *Uradni list RS*, (32/07).

Zakon o ratifikaciji Konvencije o kibernetski kriminaliteti in dodatnega protokola h Konvenciji o kibernetski kriminaliteti, ki obravnava inkriminacijo rasističnih in ksenofobičnih dejanj, storjenih v informacijskih sistemih [MKKKDP]. (2004). *Uradni list RS*, (17/04).

Vaknin, S. (2009). *The industrious spies: Industrial espionage in the digital age*. Pridobljeno na http://samvak.tripod.com/pp144.html

O avtorjih:

Dr. Igor Bernik, doktor znanosti, predavatelj, predstojnik katedre za informacijsko varnosti in prodekan za izobraževalno dejavnost, Fakulteta za varnostne vede, Univerza v Mariboru.

Kaja Prislan, podiplomska študentka, Fakulteta za varnostne vede, Univerza v Mariboru.