VARSTVOSLOVJE,
let. 13
št. 3
str. 261-279

Informacijsko bojevanje v Sloveniji - od tradicionalno lokalnega v globalni kibernetski prostor

Igor Bernik, Kaja Prislan

Namen prispevka:

Opozoriti želimo na tveganja, ki so jim izpostavljeni vsi informacijski sistemi in jih prinaša informacijsko bojevanje. Z razvojem sodobne informacijsko-komunikacijske tehnologije (v nadaljevanju IKT) je vojaško, politično, gospodarsko in ideološko motivirano bojevanje pridobilo popolnoma nove razsežnosti in nevarnosti, čeprav se njene resnosti marsikatera država še vedno ne zaveda. Zaradi anonimnosti, možnosti dostopanja z oddaljene lokacije in zakrivanja izvora napada, storilci svoje cilje dosegajo lažje in hitreje, kot je to bilo mogoče pred razvojem spleta in informacijske tehnologije. To je omogočilo razvoj in prenos informacijskega bojevanja na različna družbena področja. Ker pa so tehnike informacijskega bojevanja postale primerljive z ostalo (klasično) računalniško kriminaliteto, je kompleksnost problematike še toliko širša. Resnost in nevarnost tovrstne grožnje prikazujemo skozi primere. S predstavitvijo trenutne zakonske ureditve v Sloveniji pa želimo prikazati neustrezno normativno podlago za delo organov pregona. Trenutna zakonska ureditev omogoča stanje, v katerih je primere informacijskega bojevanja lažje vršiti kot preganjati.

Metode:

Podan je pregled definicij informacijskega bojevanja v strokovni literaturi. Na podlagi analize definicij je predlagana konkretna in natančnejša opredelitev pojava informacijskega bojevanja. Kratko so predstavljeni nekateri primeri kibernetskih napadov, ki potrjujejo obstoj tovrstne grožnje. Analizirana je aktualna zakonodaja v Republiki Sloveniji. Na podlagi ugotovljenih slabosti so podani utemeljeni predlogi za izboljšave zakonodaje.

Ugotovitve:

Temeljna ugotovitev prispevka je, da se je (informacijsko) bojevanje, kot tradicionalni način doseganja ciljev, z razvojem sodobne IKT razširilo v vse sfere družbenega življenja, skladno s tem pa so se spremenile tudi njegove tehnike delovanja. Kibernetsko okolje je tej grožnji omogočilo neobvladljivo širjenje, kar je povzročilo novo globalno/transnacionalno tveganje za države in organizacije. Gospodarstvo, kritična infrastruktura, politični odnosi in svetovni mir so tista temeljna področja, ki jih informacijsko bojevanje želi kompromitirati. Kot kaže trenutno stanje normativne ureditve informacijskega bojevanja, so na nacionalni

ravni naše države pomanjkanje politične volje, nerazumevanje in ravnodušnost temeljni atributi, ki omogočajo obstoj in razvoj informacijskega bojevanja. Na ravni svetovnih velesil in mednarodnih organizacij pa gre, zaradi zavedanja in uporabe prednosti tovrstnega bojevanja, za poskus ohranjanja neurejenega stanja, saj z informacijskim bojevanjem napadajo normativno ureditev.

Izvirnost/pomembnost prispevka:

Izvirna vrednost prispevka je opredelitev informacijskega bojevanja. Poleg tega pa je pomemben tudi prikaz narave informacijskega bojevanja na primerih in stanje normativne ureditve. Slednje je glavni zaviralec za preprečevanje opisane problematike.

UDK: 343.3/.7:004

Ključne besede: informacijsko bojevanje, informacijsko-komunikacijske tehnologije, pravna ureditev, Slovenija

Information Warfare in Slovenia – from Traditional Local to Global Cyber Space

Purpose:

The purpose of this paper is to draw attention to security risks to information systems which confront every country and organization – the risk in question is information warfare. Development of modern information communication technology has led us to the situation in which politically, economically and ideologically motivated warfare has gained a completely new dimension and constitutes new dangers, but many countries still don't acknowledge its presence. Anonymity, the possibility of accessing information from distant locations, and the possibility of concealing the source of the attack are enabling perpetrators to achieve their vicious goals much easier and faster than before the development of the Internet and information technology in general. Development made it possible for information warfare to spread to different social spheres. The complexity of this modern threat has become much more worrisome, because techniques of information warfare have became comparable with other (classic) computer crimes. We would like to demonstrate the gravity and danger of this threat through practical examples and present the current legal regulation of this issue in Slovenia. The current Slovenian legislation creates conditions in which it is easier to commit information warfare than prosecute it.

Design/Methods/Approach:

In forming a definition of information warfare, we used a comparative method. We carried out a comparison of different written sources published abroad. For better understanding the nature of modern warfare, we presented some practical examples. An understanding of the legislation in the Republic of Slovenia in reference to these issues was acquired through a thorough study and comparison of Slovenian legal acts.

Findings:

The main finding of this paper is that information warfare, which was used in the past for military purposes, has now (with the development of modern technology) spread into every area of society. Simultaneously the techniques of

information warfare have also changed. Cyber space allowed information warfare to extend uncontrollably, and this resulted in the birth of new transnational and global threats to all countries and organizations. Economies, crucial national infrastructure, political relations and world peace are the main areas that information warfare tries to compromise. The current legislation, at the national and global levels, reflects, that a lack of political will, incomprehension and apathy are the major factors which allow information warfare to exist and develop.

Originality/Value:

The originality of this paper is in the suggested definition of information warfare, and further in the presentation of the nature of this specific threat through practical examples and an overview of the relevant legislature, which is the main obstacle in the prevention of this type of criminality.

UDC: 343.3/.7:004

Keywords: information warfare, information communication technology, legal regulations, Slovenia

1 UVOD

Državna ofenzivna dejavnost in z njo povezana kriminaliteta sta se od nekdaj razlikovali od klasične kriminalitete, predvsem z vidika družbeno škodljivih posledic in tehnik, ki sta jih pri tem uporabljali. Njuna združitev v eno izmed družbi najnevarnejšo obliko kriminalitet - računalniško kriminaliteto je zaradi tega še toliko bolj problematična. Razvoj sodobne informacijsko-komunikacijske tehnologije (v nadaljevanju IKT) in svetovnega spleta je omogočil razvoj različnih kriminalnih dejanj, ki se dogajajo v kibernetskem prostoru, med njimi tudi posebne oblike bojevanja, t. i. informacijsko bojevanje (ang. Information Warfare). Sodobna IKT ni bila izkoriščena zgolj za poenostavitev kritičnih družbenih in vitalnih organizacijskih funkcij, temveč tudi za razvoj tehnik bojevanja. Le-to je poglobilo problematiko, povezano z odkrivanjem, preiskovanjem in pregonom tovrstne državne in poslovne kriminalitete. Zaradi splošne dostopnosti orodij in znanj so tehnike doseganja ciljev v kibernetskem prostoru postale izjemno lahke, v večini primerov primerljive z ostalo računalniško kriminaliteto. Tako je glavna težava, s katero se srečujejo pristojni organi, ravno razlikovanje med politično motivirano in klasično računalniško kriminaliteto, ki je možno le na podlagi poznavanja identitete storilca in njegovega motiva. Ugotavljanje motivacije pa je izjemno problematično, saj so anonimnost, splošna razširjenost in dostop v kibernetski prostor z oddaljene lokacije glavni atributi sodobne IKT, ki storilcem omogočajo spretno zakrivanje identitete in izvora napada. Izraz »informacijsko bojevanje« nima ene s konsenzom sprejete definicije. Razlog je v izrazih, iz katerih je sestavljen. Vojaški izraz »bojevanje« je predmet številnih razprav, definicija pa se razlikuje glede na področje, v katerem ga uporabimo (npr. v sociologiji, antropologiji, ekonomiji, zgodovini, politiki ali vojski) (Ventre, 2009). Tudi izraz »informacijsko« na posameznih področjih razumejo različno, zato ni enotne definicije, morda pa tudi sam izraz »informacijsko bojevanje« ni najboljši.

Kot vsaka oblika računalniške kriminalitete, se tudi omenjena ni izognila problematiki pravne ureditve. V tem trenutku je področje informacijskega vojskovanja neenotno opredeljeno, normativna podlaga pa je z izjemo Konvencije o kibernetski kriminaliteti (v Sloveniji ratificirana z Zakonom 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), prepuščena vsaki državi posebej in njihovim sporazumom o medsebojni pomoči. Nenadzorovan globalen kibernetski prostor, oddaljenost, neosebnost, odsotnost razumevanja in zakonskih omejitev so temeljne lastnosti sodobnega informacijskega bojevanja, ki ogrožajo vsako državo in organizacijo v njej. Škoda pa se kaže tako v kvaliteti kot kvantiteti človekovega in družbenega življenja.

Ravno zaradi razsežnosti problematike povezane z informacijskim bojevanjem v prispevku predstavljamo njeno naravo in možne odzive. Neurejenost zakonske podlage nakazuje na problematiko odkrivanja in preiskovanja kibernetske kriminalitete, povezane z globalnimi političnimi, vojaškimi in gospodarskimi interesi. S predstavljenimi primeri v tujini in v Sloveniji pa se kaže nevarnost, ki preti vsaki državi in organizaciji. Na teh primerih oz. tujih izkušnjah se lahko pristojni državni organi in odgovorni v podjetjih naučijo, kako ustrezno (ne) odreagirati v kriznih situacijah.

1.1 Problematika definiranja in razumevanja informacijskega bojevanja

Informacijsko bojevanje zajema dva pojma, informacijo in bojevanje. V slovenščini termin še ni dobil univerzalne oznake, saj se uporabljajo različna pojmovanja; informacijsko bojevanje, informacijsko vojskovanje, kibernetsko vojskovanje ipd. Vsekakor pa ta pojem zajema boj z informacijami in nastopa v različnih družbenih sektorjih. Tako bi bilo najbolj smiselno uporabljati pojem bojevanje (in ne vojskovanje), saj ne zajema zgolj vojaške ofenzive, temveč tudi obrambno, vohunsko in psihološko dejavnost držav, poslovnih entitet in civilnih skupin. Problem pa se ne pojavlja zgolj pri samem poimenovanju, temveč tudi pri poskusih razmejevanja, kaj naj bi pojem obsegal in kaj ne.

Taylor, Caeti, Loper, Fritsch in Liederbach (2006) informacijsko bojevanje definirajo kot zaščito, zlorabo, okvaro, uničenje ali onemogočenje informacij ali njihovih virov z namenom doseči prednost ali zmago nad nasprotnikom. Druga definicija (Cyber Warfare, 2011) navaja, da se kibernetsko bojevanje navezuje na koordiniran, digitalen napad na vlado s strani druge vlade, ali s strani velikih skupin civilistov. Joyner in Lotrionte (2001) pa menita, da je informacijsko bojevanje kot informacijska aktivnost uporabljena v času krize ali konflikta, da bi se dosegli zastavljeni cilji.

Iz tega sledi, da je informacijsko bojevanje posledica združitve vojaških ciljev države s sodobno IKT. V osnovi se nanaša na pridobivanje in/ali uporabo informacij s pomočjo te tehnologije. Iz semantičnega vidika gre za kombiniran termin med informacijo in bojevanjem. Informacija je del informacijskega sistema, le-ta pa je tarča

ali orodje informacijskega vojskovanja, ki ga izvedemo s pomočjo informacijskega napada. Napad najpogosteje zajema kršitev zakonodaje, politike ali predpisov znotraj lokalnega ali globalnega okolja, zatorej informacijsko bojevanje (največkrat, ne pa vedno) spada v področje računalniške in/ali kibernetske kriminalitete. Ob tem pa se je potrebno zavedati, da gre za sodobno razumevanje omenjenega pojma. To ni novejši termin, saj se je že pred nastankom Interneta uporabljal v vojaških vrstah za aktivnosti oslabitve obrambe nasprotnika.

Ne glede na to, kako stara oblika bojevanja je to, se je z razvojem informacijsko-komunikacijske tehnologije povečala možnost njene učinkovite izvedbe (v smislu onemogočanja podatkov in informacijskih sistemov) (Wall, 2007).

Na podlagi tega lahko sodobno informacijsko bojevanje definiramo kot ofenzivno in defenzivno delovanje (zasebnih in javnih) institucij oz. skupin za pridobivanje in/ali uporabo informacij s pomočjo IKT za doseganje premoči v boju s konkurenco. Pri tem želijo lastne informacije zaščititi pred zlorabo, okvaro in uničenjem oz. preprečiti nedostopnost hkrati pa zlorabiti, okvariti, uničiti in preprečiti dostop do informacij nasprotnika.

2 NARAVA INFORMACIJSKEGA BOJEVANJA

Največja težava ni povezana zgolj z razumevanjem in definiranjem pojava, temveč z njegovimi implikacijami in razsežnostjo. Nelegalni posegi državnih organov in služb v računalnike ali računalniško mrežo ter komunikacijska sredstva, ki spadajo v področje informacijskega bojevanja, niso nič drugega kot državni računalniški kriminal, ki zajema še večjo nevarnost za državno in gospodarsko stabilnost ter kritično infrastrukturo kot poslovni kriminal, saj poleg le-tega vključuje še teroristične in vojaške aktivnosti.

Razvoj informacijskega bojevanja je potekal na enak način kot klasična kriminaliteta, ki se je v veliki meri preselilo v kibernetsko okolje. Kljub temu pa je informacijsko bojevanje zaradi specifične narave, ki jo definirata 'vojskovanje/bojevanje' in 'država/organizacija', iztrgano iz konteksta klasične računalniške kriminalitete.

Jeffery Carr, avtor knjige ''Inside Cyber Warfare'', je v intervjuju za spletno stran O'Reilly (Slocum, 2010) informacijsko bojevanje primerjal z izumom revolverja, ki je revolucionaliziral bojevanje. In prav to naj bi se ob pojavu IKT sedaj dogajalo z informacijskim bojevanjem. Meni tudi, da je z njim mogoče doseči ravnovesje med neenakovrednimi nasprotniki. In to zaradi dveh stvari: trenutne ranljivosti spleta in ker so vojaške sile vključene tako v lokalno kot svetovno omrežje.

Prednost in premoč sta kvaliteti tistih, ki prvi razvijejo tehnologijo. Informacijska revolucija je skupaj z globalizacijo, transnacionalno ekonomijo, hitrim izmenjavanjem novic in dostopom do komunikacij in informacij vseh tipov posameznikom/državam/podjetjem ponudila veliko novih možnosti za doseganje moči. Vsakršen poskus konkuriranja brez uporabe sodobne IKT bi povzročil veliki finančni in vojaški zaostanek. Brez IKT danes nobena organizacija na svetu ne more biti konkurenčna. Nekonkurenčnost pa pomeni finančno izgubo in neuspeh. Tudi vojska brez IT težko načrtuje in koordinira operativne operacije. Vsekakor gre za

vojaški in finančni zaostanek za tistimi, ki sodobno tehnologijo koristijo. Prednosti, ki jih tehnološka odvisnost ponuja pretehtajo tveganja, ki jih le-ta obenem prinaša s seboj. Poleg tega pa je za državo nemogoče vzpostaviti ustrezno obrambo pred informacijskim napadom, če sama ne obvlada tehnik informacijskega bojevanja (Fritz, 2008).

Iz tega je mogoče sklepati, da prenos bojev z informiranjem v kibernetski prostor ni več vprašanje, temveč dejstvo. Poznavanje in razvijanje tehnik informacijskega bojevanja je nujno potrebno za uspešno delovanje državnih in organizacijskih struktur ter njihovo obrambo pred sovražnimi vdori v informacijske sisteme.

Uporaba tehnik informacijskega bojevanja na državni ravni običajno služi pridobivanju informacij o ekonomskem, političnem, kulturnem in vojaškem stanju v drugi državi (tarči) ali pa za konkretno ofenzivno oz. defenzivno delovanje v kibernetskem prostoru. V prvem primeru države cilje dosegajo s pomočjo vohunjenja, v drugem primeru pa s pomočjo vojaškim aktivnostim podobnimi akcijami v kibernetskem prostoru. Vendar pa informacijsko bojevanje ni zgolj v domeni držav, temveč se le-tega poslužujejo tudi korporacije oz. tiste poslovne entitete, ki za svoj obstanek, razvoj in konkuriranje potrebujejo informacije, do katerih nimajo avtoriziranega dostopa. V obdobju visoko razvite IKT pa se kaže, da ta trend nikakor ne bo poniknil. Agresivna konkurenca in podjetja v razvojnem zaostanku bodo diktirala vedno nove in nove smernice ter potrebe po informacijah in z njimi povezanim znanjem.

Informacijsko bojevanje kot ofenzivna dejavnost sestoji iz šestih komponent (Taylor et al., 2006):

- Psiholoških operacij, ki vplivajo na duševno stanje nasprotnika (propaganda ali širjenje informacij, s katerimi želimo vplivati na odločitev ljudi, pri čemer je Internet odlično orodje).
- Elektronskega bojevanja, ki zajema onemogočenje dostopa do informacije, ki jo nasprotnik potrebuje (najpogosteje se le-tega poslužujejo teroristi, hektivisti in države).
- Vojaškega zavajanja kot tradicionalne oblike vojskovanja, s katero nasprotnika zavedemo o dejanski vojaški sposobnosti.
- Fizičnega informacijskega bojevanja, ki zajema fizičen napad na informacijski sistem.
- Zaščitnih ukrepov namenjenih varovanju informacijskega sistema, ki ga nasprotnik ne more onesposobiti.
- Informacijskega napada, ki zajema zlorabo, uporabo, uničenje informacije.

Napadalna informacijska operacija obsega zbiranje zaupnih informacij, nedovoljen vstop v informacijske sisteme, ustvarjanje varnostnih vrzeli v njem, spremembo ali uničenje podatkov in onemogočanje ali uničenje informacijskega sistema (Joyner in Lotrionte, 2001).

Tehnike informacijskega bojevanja tako kot ostale oblike kibernetske kriminalitete izkoriščajo varnostne vrzeli v varnostnih sistemih. Informacijska

varnost pa se ne nanaša zgolj na varnost kibernetskega prostora, temveč tudi na fizično varnost kritičnega okolja in ljudi, ki s takšnim okoljem operirajo.

Za izvedbo informacijskih napadov in vdorov se najpogosteje izkorišča spletne povezave, ki storilcem omogočajo dostavo zlonamerne programske opreme in neavtorizirane dostope do njihovih sistemov. Med to opremo najpogosteje štejemo keyloggerse, aplikacije, ki lahko vohunijo za aktivnostmi uporabnika in zbrane podatke pošiljajo na oddaljeno lokacijo. Velikokrat so za vdore in napade na informacijske sisteme za potrebe vohunjenja izkoriščene tudi brezžične spletne povezave (SANS Institute, 2007).

Pri tem je zanimivo dejstvo, da Internet uporablja več kot 26 % svetovne populacije (Internet usage statistics, 2010), vsekakor pa od tega več milijonov ljudi njegove zmožnosti izkorišča za zlonamerna dejanja. Tudi Computer Forensics (Cyber Crime Statistics, 2006) navaja, da sta splet in z njim povezana nezaželena elektronska pošta (spam) najpogostejša načina izvajanja računalniške in kibernetske kriminalitete.

Ameriška organizacija za obdelovanje in zaščito elektronske pošte IronPortAntispam System je aprila 2011 obdelala skupno kar 9,182,715 elektronskih sporočil, od tega je bilo skupno zaznanih kar 7,5333,707 (82 %) SPAM-a (Spam Statistics, 2011). Kot je znano, se večina orodij računalniške opreme širi s pomočjo le-tega. Najpogosteje elektronska pošta zajema različne oblike računalniških prevar (kot npr. phishing) in vohunske programske opreme (npr. keyloggerse, trojanski konji, virusi, črvi ipd.), ki od uporabnika zbirajo zaupne informacije. Glede na to, da tako velik odstotek elektronske pošte zajema SPAM, so možnosti informacijskih bojevnikov neomejene, njihova žrtev pa lahko postane vsakdo.

To dokazuje tudi primer zlonamerne programske opreme ustvarjene v letu 2009, ki je za svoj obstoj in doseganje ciljev izkoriščala prav splet in elektronsko pošto. Trojanski konj imenovan ZEUS je v računalniški sistem penetriral preko spleta s pomočjo različnih računalniških prevar, pri tem sta bila najpogostejša SPAM in phishing. Program je vseboval vohunsko opremo keylogger, ki je z računalnika uporabnika zbirala informacije o geslih in uporabniških imenih, predvsem s področja bančništva ter jih storilcu pošiljala na oddaljeno lokacijo. Program je bil na voljo tudi za plačilo, okvirno 3000-4000 dolarjev (Stevens in Jackson, 2010). ZEUS je okužil več kot 10.000 računalnikov po celem svetu, dnevno pa je zbral več kot 200.000 vrstic podatkov o kreditnih karticah, geslih spletnega bančništva in socialnih omrežjih na okuženih računalnikih (Topping, 2009).

Podobno se je leta 2009 dogodilo tudi pri nas, ko so slovenski študenti izdelali virus imenovan Mariposa in ga prodali španski spletni združbi. Le-ta je z njim okužila skoraj 13 milijonov računalnikov po celotnem svetu. Virus Mariposa je z enakimi tehnikami, kot ZEUS, zbiral podatke o uporabnikovih računih, geslih o spletnem bančništvu ipd., širil pa se je s pomočjo spamov in drugih spletnih prevar (Botnet hacker caught in Slovenia, 2010).

Slednje dokazuje, da je računalniška tehnologija vsekakor nadgradila tudi vohunsko dejavnost, saj storilcem omogoča lažje in hitrejše doseganje zastavljenih ciljev. Ob ustreznem znanju je kraja poslovnih/zaupnih podatkov s pomočjo informacijske tehnologije veliko lažja in hitrejša kot vohunska dejavnost v fizični obliki. Poleg tega pa je IKT tako razširjena in vpletena v vse poslovne sfere, da

je znanje o njenem delovanju univerzalnega pomena, saj je uporabno na vseh področjih, ne glede na katerem poslovnem področju nek vohun deluje. Za razliko od klasičnih vohunov, heker, ki vdira v informacijske sisteme, ne potrebuje posebnega znanja o posamezni organizaciji, od katere želi pridobiti informacije.

Varnostne pomanjkljivosti, ki jih izkoriščajo informacijski bojevniki, pa so v veliki meri odvisne tudi od trenutnih družbenih razmer v državi, ki pogojujejo tudi organizacijsko klimo in strukturo. Cyber-Ark, podjetje za zagotavljanje informacijske varnosti, je nedavno tega izpeljalo raziskavo med 600 zaposlenimi v Veliki Britaniji, ZDA in Nizozemskem (Fullbrook, 2009), z namenom ugotoviti, ali finančna in gospodarska kriza vplivata na delovni odnos ljudi, njihovo etiko in informacijsko varnost. Rezultati so pokazali, da sta ravno industrijsko vohunstvo in kraja podatkov močno narastla, vendar ne toliko v hekerskih vrstah, temveč predvsem med zaposlenimi, ki se bojijo izgube službe. Tudi hekerska skupnost je mnenja, da jim ekonomija odpira nove priložnosti. Zmanjševanje delovne sile je pripeljalo do outsourcinga (prenos izven organizacijskega okolja) določenih funkcij v organizacijah, kar še posebej ogroža varnost kibernetskega prostora in z njim povezanih informacij. Manjše število ljudi zaposlenih na področju zagotavljanja tovrstne varnosti pa vsekakor pomeni večjo ranljivost podjetja, predvsem pa več prostora za napake.

2.1 Storilci in žrtve - primeri informacijskega bojevanja

Tarča informacijskih bojev je lahko vsaka država, organizacija ali posameznik. Na državni ravni je težko govoriti o najbolj izpostavljenih točkah, vsekakor pa je kritična infrastruktura vitalnega pomena tako za tistega, ki jo poseduje in potrebuje, kot tistega, ki želi škodovati nasprotniku. Bratuša (2011) navaja, da kibernetska vojna nima prve bojne linije, zato je potencialno bojišče katerikoli računalniško krmiljeni sistem od naftovodov, plinovodov, elektrarn pa vse do stacionarnega telefonskega omrežja, GSM mobilnega telefonskega omrežja, bančnih sistemov, sistemov zavarovalnic, vodnih zajetij, vladnih služb, javne uprave, letališč in vse do individualnega uporabnika, ki računalnik uporablja doma. Tako se tudi v zasebni sferi kraji poslovnih podatkov ne more izogniti nobena organizacija, vendar pa so nekatere tovrstni kriminaliteti bolj izpostavljene. Tarče vohunjenja so največkrat večje organizacije, korporacije oz. multinacionalke, ki prodirajo na tuje trge in s tem ogrožajo nacionalne ali druge konkurenčne korporacije. Poleg velikosti pa na privlačnost vohunjenju vpliva tudi vrsta industrije oz. gospodarske panoge. Kjer je več kapitala, zaslužka in poslovnega uspeha, tam je tudi večja želja nasprotnika po pridobitvi le-tega. Connolly (2009) med področja, ki so najbolj izpostavljena pojavu vohunstva, uvršča avtomobilsko industrijo, industrijo z obnovljivimi energijami, komunikacijami, optiko, rentgensko tehnologijo, stroji in raziskavami. Kot navaja SANS Institute (2007), so najpogostejša tarča industrijskega in korporacijskega vohunstva farmacevtska, modna, kozmetična, računalniška in celotna informacijsko-komunikacijska industrija. Napadi so izjemno sofisticirani, vse več pa je tudi ljudi, ki so se jih pripravljeni posluževati. Kitajska zaposluje kar milijon agentov na tem področju, zato so sposobni resno škodovati globalni

infrastrukturi. Med močnejšimi državami je tudi Rusija, ki kljub manjšemu številu agentov v primerjavi s Kitajsko, vse bolj izkorišča zmožnosti spleta za pridobivanje vitalnih informacij, ki rešujejo njen ekonomski razvoj (Connolly, 2009).

V literaturi (kot npr. Cyber Warfare, 2011) se pogosto omenja, da je bil napad na Estonijo prvi primer kibernetskega napada na specifično oblast. Napad na estonske sisteme se je začel aprila 2006, s poplavami podatkov na ključne vladne internetne strani, še posebej na strani predsednika države, predsednika vlade in parlamenta. Ena izmed teh poplav podatkov je ustavila sistem parlamentarne spletne pošte. V napadu je sodelovalo okoli milijon 'botnet' računalnikov iz ZDA in Azije, ki so z ogromnimi količinami podatkov preplavili estonske spletne strani. Napadi so bili domnevno načrtovani na spletu, napadalci pa so se koordinirali preko rusko govorečih klepetalnic in forumov.

Vsekakor pa to ni osamljen primer, saj se je v preteklosti zvrstilo že nepredstavljivo število napadov in vdorov v vladne in gospodarske sisteme. Pri tem se kot žrtev teh napadov in ciljev informacijskih bojevnikov najpogosteje omenjajo ameriške informacijske točke, ki zaradi tehnološke odvisnosti, prednosti v razvoju in inovativnosti ter vojaške premoči pogosto postanejo tarča zlonamernih državno ali korporacijsko sponzoriranih vohunov in napadalcev.

Med letom 1995 in 2008 so bili odkriti številni primeri vohunjenja Kitajske na območju ZDA. Aktivnosti so bile usmerjene predvsem v letalske, vesoljske in morske konstrukcije, izvzeta pa ni bila niti računalniška industrija, izdelava nuklearnega orožja, zavezniške akcije ipd. Uporabili so vse podatke, ki so jih pridobili, tudi tiste zbrane s pomočjo OSINT (zbiranje informacij iz javno dostopnih virov), pri čemer so uporabili decentralizirano mrežo študentov, poslovnežev, znanstvenikov, diplomatov in drugih državljanov Kitajske, ki so večinoma legitimno prebivali v ciljni državi (Fritz, 2008).

Poleg Estonije in večkrat omenjene ZDA pa je v medijih in literaturi nedavno tega močno odmeval primer vohunske programske opreme GhostNet, ki so jo leta 2009 odkrili kanadski raziskovalci iz Univerze v Torontu. Kot navaja Harris (2009) je program kradel zaupne informacije tako, da se je infiltriral v številne računalnike po svetu. GhostNet naj bi bil narejen in odposlan iz Kitajske, njegova tarča pa so bile predvsem ambasade, medijske družbe, nevladne organizacije, mednarodne organizacije, ministrstva in vladne službe, poleg tega pa tudi pisarne Dalai Lame, vodje tibetanskega gibanja. Po desetih mesecih preiskovanja so ugotovili, da je GhostNet vdrl v kar 1,296 računalnikov v 103 državah, kot se je izkazalo pa je bil osredotočen predvsem na države v južni in južno-vzhodni Aziji ter pisarne Dalai Lame v Indiji, Bruslju, Londonu in New Yorku. Program je v računalnike penetriral preko spleta nato pa kradel podatke, nadziral elektronsko pošto in vklapljal mikrofone in kamere na okuženih računalnikih, tako, da je bilo omogočeno spremljanje dogajanja v sobi, v kateri se je nahajal računalnik. Sum je padel na kitajsko vlado, saj je ta redno napadala tibetansko gibanje s podpiranjem separatizma in terorizma na Kitajskem.

O posledicah, ki jih kibernetska kriminaliteta in z njo povezano informacijsko bojevanje lahko povzročita, priča primer virusa imenovanega Tusk.M. Virus, ki je v letu 2007 okužil več milijonov računalnikov in telefonov po svetu, je povzročil za kar 248 milijard dolarjev finančne škode, 150.000 ljudi je zaradi tega izgubilo

svoje službe, poleg tega pa je zaradi prekinitve delovanja kritičnih državnih funkcij življenje izgubilo 58 ljudi (Terrorist hacker gets life, 2008). Omenjenim posledicam se ne more izogniti nobena država, niti organizacija. Tudi Slovenija pri tem ni izjema, o čemer priča pilotska študija izvedena lani v različnih slovenskih organizacijah, ki dokazuje ranljivosti organizacijske in državne infrastrukture. Pri tem je le 35 % organizacij lasten sistem informacijske varnosti ocenilo kot dobrega, ostala večina pa kot nezadostnega ali slabega. Zaskrbljujoče je dejstvo, da se med nekvalitetnimi pojavljajo tudi organizacije, katerih informacijski sistemi so povezani z življenjsko pomembnimi komponentami (Bernik in Prislan, 2010), saj so bile v študijo vključene tudi državne in gospodarske organizacije.

2.2 Vodilni ZDA in Kitajska

Navedeni primeri in številni drugi, ki se omenjajo kot primeri informacijskega bojevanja nakazujejo, da sta najmočnejši državi na tem področju ravno ZDA in Kitajska, po mnenju Bratuše (2011) pa se jima ob bok enakovredno postavlja tudi Severna Koreja. ZDA so vsekakor vodilna svetovna politična, gospodarska in vojaška velesila, zaradi česar so tudi najpogosteje tarča zlonamernih vdorov in napadov na informacijske sisteme. Lahko bi rekli, da ameriške vladne in gospodarske službe niso imele druge izbire, kot da so v poskusih konkuriranja in zoperstavljanja razvile močan ofenziven in defenziven sistem informacijskega bojevanja.

ZDA je leta 1998 v nacionalnem programu za zaščito kritične infrastrukture CIP[1] zapisala potrebo po sodelovanju zasebnega in državnega sektorja na nacionalni in mednarodni ravni. S tem je bil ustanovljen tudi Nacionalni center za zaščito kritične infrastrukture pod okriljem FBI, katerega naloga je zbiranje informacij o grožnjah infrastrukturi in opozarjanje na možne napade, analize stanja, kriminalistično preiskovanje in odzivanje (Joyner in Lotrionte, 2001). Po letu 1990 so ZDA začele namenjati veliko pozornosti tudi razvijanju omrežno usmerjenega vojskovanja - NCW[2]. Slednje pomeni prenos prednosti informacijskih sistemov in tehnologije na vojaško področje z omrežnim povezovanjem dobro obveščenih, geografsko razpršenih vojaških sil. Na podlagi takšnega sistema pa je leta 2002 ameriško obrambno ministrstvo začelo z izgradnjo Globalnega informacijskega omrežja GIG[3], kot hrbtenico NCW. Vsi pomembnejši sistemi vključeni v NCW bodo v prihodnosti medsebojno povezani preko GIG-a. Leta 2003 je pod okriljem ameriškega obrambnega ministrstva na področju NCW nastal dokument z naslovom Zemljevid informacijskih operacij[4]. Tovrsten dokument je dober primer, kako se ZDA trudijo transformirati vojaške kapacitete, da bi ostali v koraku s časom z naraščajočimi grožnjami in z izkoriščanjem novih priložnosti, ki jih ponujajo inovacije na področju informacijske tehnologije. Glede na dokument

1 *Critical Infrastructure Protection*
2 *Network-centic Warfare*
3 *Global Information Grid*
4 *Information Operations Roadmap*

je temeljna naloga informacijskih operacij vladati elektromagnetnemu okolju z onemogočanjem, uničenjem in spreminjanjem nasprotnikovih groženj, nadzornih in kontrolnih sistemov in sistemov kritične infrastrukture (Tolle, 2002).

Za varnost lastne informacijske tehnologije in z njo povezanih sistemov pa ZDA niso poskrbele zgolj na tehnični ravni, temveč so temu priključili tudi posebne specializirane vojaške enote, katerih temeljna naloga je obramba ameriške kritične in vojaške infrastrukture.

Od leta 2010 dalje v ameriškem kibernetskem in fizičnem okolju deluje pet vojaških enot namenjenih ravno zavarovanju, analiziranju in ogrožanju okolja odvisnega in prepletenega z informacijsko tehnologijo. USCYBERCOM[5] je zadolžen izključno za obrambo vojaških računalniških omrežij ter izvedbe kibernetskih napadov na vojaške cilje sovražnih držav. Naslednja enota za kibernetsko vojskovanje je ARCYBER[6] namenjena planiranju, koordinaciji, mrežnim operacijam in obrambi vseh omrežij oboroženih sil. US Marine Corps Forces Cyberspace Command je enota marincev zadolžena za varovanje kritične infrastrukture pred kibernetskimi napadi in vključuje tudi enoto kriptologov. CYBERFOR[7] je enota namenjena poveljevanju ter zagotavljanju sil in opreme za kriptologijo, analiziranje signalov in elektronsko bojevanje. 24 AF[8] pa enota zračnih sil, katere namen je ravno tako kibernetsko bojevanje (Bratuša, 2011).

Kot kaže se ZDA dobro zavedajo nevarnosti in prednosti informacijske vojne, v kateri so udeležene vsakodnevno. Zaradi visoke stopnje odvisnosti kritične infrastrukture od informacijske tehnologije je bila ustanovitev nacionalne politike, načrtov in specializiranih enot za zaščito in odkrivanje groženj na tej ravni nujna, predvsem pa pametna odločitev. To potrjujejo tudi navedbe Colemana (2008), da poleg ZDA tehnike in orodja za potrebe informacijske vojne razvija še približno 120 držav, temu pa se pridružujejo še teroristične skupine, kar grožnjo in nevarnost še zaostruje. Poleg ZDA se kot najmočnejša postavlja še Kitajska, saj je informacijsko bojevanje zanjo kritičnega in vitalnega pomena. Tehnike in načini tovrstne informacijske vojne sovpadajo s cilji Kitajske po vojaškem preseganju sposobnosti, moči in tehnologije drugih držav. S pridobivanjem tujega vojaškega znanja na takšen način bo hitro dohitela sposobnosti svetovnih velesil, kar ji bo omogočilo konkuriranje, medtem ko bi ji neodvisno razvijanje lastne tehnologije vzelo preveč časovnih, kadrovskih in finančnih virov (Fritz, 2008).

Vendar pa visoka usposobljenost pri uporabi tehnologije za potrebe informacijskega bojevanja in njena implementacija v vse družbene sektorje še ne predstavlja ključa do uspeha. Bratuša (2011) je mnenja, da je ravno odsotnost odvisnosti od informacijske tehnologije ključnega pomena pri doseganju prednosti. Navaja, da je trenutno najmočnejša država na področju kibernetske vojne Severna Koreja, ki ima povprečno razvite napadalne sposobnosti, medtem ko ima na drugi strani zelo nizko odvisnost od tehnologije in dobro zasnovano obrambo, ki vključuje filtriranje celotnega internetnega prometa in možnost selektivnega izklopa internetnih povezav tako, da države ne morejo odgovoriti na njihov napad.

5 *United States Cyber Command*

6 *Army Cyber Command*

7 *Navy Cyber Forces*

8 *24 Air force*

Iz tega sledi, da učinkovita obramba zajema tudi sposobnost upiranja poplavi sodobne tehnologije in tehtanje med njenimi prednostmi in slabostmi.

2.3 Slovenija

Dobrih lastnosti IKT se vse bolj zaveda tudi Slovenija, v kateri je mogoče opaziti trend večje odvisnosti državnih, vladnih in poslovnih entitet od sodobne informacijske tehnologije, kar jo avtomatsko uvršča med akterje informacijskega bojevanja. Kljub temu, da se tega ne zaveda, je kritične funkcije, ki jih je želela poenostaviti, še bolj izpostavila nameram sovražnika. Zavedno ali ne je s prepletenostjo informacijskih sistemov in tehnologijo konkurenco in sovražnike opozorila nase in svojo informacijsko ranljivost.

Da pred grožnjo, ki jo predstavlja informacijsko bojevanje, ni varna prav nobena država niti organizacija, še posebej pa ne Slovenija, dokazuje primer okužbe slovenskih informacijskih sistemov Ministrstva za finance v letu 2009. Kot navaja C. R. (2009), je bilo zaradi okužbe s črvom imenovanim Conficker onemogočeno delovanje elektronske pošte ministrstva. Ker se je širil s pomočjo ugibanja uporabniških imen na različnih uporabniških računih, je bilo onemogočeno tudi prijavljanje v omrežje ministrstva. Po trditvah Adamsa (2009) je zlonamerni program Conficker okužil petnajst milijonov računalnikov po svetu, njegov namen pa je bil kopiranje in brisanje podatkov na informacijskih sistemih. Škoda, ki jo je pri tem slovensko ministrstvo utrpelo ni bila velika, vendar pa je bil to dokaz, da pred kibernetskimi grožnjami ni varen nihče, tudi tisti ne, ki pravzaprav ni tarča napada. Seveda pa pri tovrstnih nevarnostih ocenjevanje natančne škode, v primerih izgube in kraje podatkov niti ni mogoče, kadar so napadi sofisticirani in dobro zakrivajo svoje sledi in aktivnosti v žrtvinem sistemu.

Primerov ogrožanja slovenskih informacijskih sistemov je bilo v praksi veliko (vdor v Merkurjeve POS-terminale leta 2007, hekerski vdor v sistem državnega izpitnega centra eRic leta 2007, vdor v spletni sistem RTVS leta 2010), vendar pa menimo, da jih večina, tistih bolj načrtovanih in organiziranih, ni bila zaznana in odkrita. Nerazumevanje in zanemarjanje te agresivne grožnje onemogoča njeno identifikacijo, saj so primeri političnih ali poslovno načrtovanih informacijskih napadov sestavljeni iz posameznih vdorov in se ob nepoznavanju in odsotnosti natančne preiskave kažejo kot nedolžni poskusi neavtoriziranih dostopov. V resnici pa gre za skrbno načrtovane, koordinirane napade s ciljem onemogočiti delovanje sistema in povzročitev čim večje gospodarske škode.

V Sloveniji smo v zelo slabem položaju, saj ameriška programska oprema, nameščena na najbolj izpostavljenih in kritičnih funkcijah državnih in gospodarskih služb, ne omogoča vpogleda v način njenega delovanja. Zato sploh ne moremo vedeti, kaj imamo pravzaprav nameščeno in kaj ta oprema v resnici počne. Poleg tega pa naše državne organe fizično in tehnično varujejo varnostne službe, ki nimajo varnostno preverjenih računalniških sistemov, niti delavcev in delovnih procesov. Slovenija v tem trenutku ni pripravljena na obrambo kritične informacijske strukture pred sodobnimi orožji kibernetske vojne (Bratuša, 2011).

Slabo pripravljenost poslovne in državne sfere na grožnjo informacijske vojne pa potrjuje vdor v informacijski sistem največje slovenske banke, ki je pravzaprav eden izmed glavnih stebrov slovenskega gospodarstva. Pred nekaj leti je v spletno povezavo NLB vdrl slovenski državljan, ki je odkril varnostno pomanjkljivost programa spletnega bančništva te iste banke. Zaradi te pomanjkljivosti bi lahko storilec v nekaj sekundah izpraznil celoten račun uporabnika. Gospodarska škoda in padec poslovnega ugleda te ustanove bi bil v takšnem primeru nepopravljiv, zato so tovrstne ranljivosti in pomanjkljivosti, kot posledica nerazumevanja in malomarnosti vodilnih, nedopustne. Od takrat dalje je v medijih mogoče zaslediti poročanja o vse večjih izkoriščanjih spletnega bančništva. In ravno spletne ranljivosti finančnih ustanov so največkrat tarča zlonamernih uporabnikov. Policija ugotavlja (Felc, 2010), da se je v lanskem letu število kaznivih dejanj povezanih s kibernetsko kriminaliteto v Sloveniji podvojilo. To pomeni, da so nevarnosti, ki pretijo slovenski gospodarski stabilnosti vsak dan večje.

3 ZAKONSKA UREDITEV V SLOVENIJI

Trenutno se Slovenija ne srečuje zgolj s problematiko neustrezne tehnične zaščite in nerazumevanja problematike, temveč jo tako kot ostale države po svetu pesti težava neustrezne pravne ureditve. Stanje zakonske ureditve, ki jo imamo danes, onemogoča odkrivanje in preiskovanje primerov informacijskega bojevanja.

Slovenska podjetja nimajo nobenih možnosti, da bi na zakonit način odkrivala varnostne incidente povezane z industrijskim vohunstvom. Za preiskovalce, ki morajo upoštevati omejitve slovenske zakonodaje s področja varovanja osebnih podatkov, pa je odkritje storilca skoraj nemogoče opravilo. Zakonodajalec je podjetjem in preiskovalcem praktično zvezal roke, s čimer se zaradi nezmožnosti odkrivanja in preprečevanja incidentov povzroča velika škoda gospodarstvu (Bratuša, 2011).

Pravna ureditev računalniške kriminalitete in zakonske omejitve, povezane z njenim odkrivanjem, preiskovanjem in dokazovanjem, so najpomembnejši temelj učinkovite obrambe pred zlonamernimi napadi informacijskih bojevnikov. Brez ustrezne normativne podlage se pristojni organi ne morejo boriti zoper tovrstno grožnjo. Trenutno stanje zakonodaje pri nas in po svetu dokazuje, da se informacijskemu bojevanju še vedno ne posveča dovolj pozornosti. Na ravni Slovenije zakonodajalec nima ustreznega razumevanja o njeni resnosti in nevarnosti. To ustvarja situacijo, v kateri je lažje izvesti informacijski napad in kraje podatkov kot odkrivati in preganjati storilce.

V Sloveniji sicer imamo nekaj normativnih aktov, ki se parcialno nanašajo na področje informacijskega bojevanja. Državni zbor RS je leta 2004 z zakonom ratificiral Konvencijo o kibernetski kriminaliteti (MKKKDP, 2004; v nadaljevanju Konvencija). Na nacionalni ravni pa je z vidika našega prispevka pomembna še naslednja zakonodaja: Zakon o kazenskem postopku [ZKP] (1994, 2003, 2004, 2006, 2007), Zakon o spremembah in dopolnitvah Zakona o kazenskem postopku [ZKP-J] (2009), Kazenski zakonik RS [KZ-1] (2008), Zakon o varstvu osebnih podatkov [ZVOP-1] (2004, 2007) in Zakon o elektronskem poslovanju in elektronskem podpisu

[ZEPEP] (2000, 2004), vendar se kljub temu pojavljajo štirje temeljni problemi, ki kljub obstoječim aktom (ali pa ravno zaradi njih) onemogočajo ustrezno postopanje državnih organov in organizacij v primerih informacijskega bojevanja in so opisani v nadaljevanju.

Prvi problem se nanaša na področje definiranja pristojnosti organov v kibernetskem okolju. Kibernetska kriminaliteta, s pomočjo katere informacijski bojevniki dosegajo zastavljene cilje, deluje v mednarodnem kibernetskem okolju, v katerem nacionalne meje niso začrtane, storilci pa največkrat izvirajo iz tujih držav. V kibernetskem prostoru mora vsak posameznik, služba ali organizacija poskrbeti za lastno zaščito in definiranje meje (ne)dovoljenega dostopa, vendar je zaradi pomanjkanja volje to večkrat izjema kot pravilo. Kdaj je torej mogoče trditi, da se posameznik nahaja v slovenskem in kdaj npr. v italijanskem kibernetskem okolju, če ta okolja niso definirana, strežniki in omrežja so medsebojno prepleteni, vstop vanje pa je prost.

Mednarodna zakonodaja sicer daje vsaki državi pravico do svobode na nacionalnem območju. Ta princip nakazuje na to, da ima vsaka država pravico do avtonomnosti, varnosti pred nasiljem in suverenosti na državnem območju. Nobena država tako ne sme uporabiti oboroženih sil za invazijo na območje druge države preko morja, zraka ali kopnega. Vprašljiv je torej princip državne suverenosti v kibernetskem prostoru (Joyner in Lotrionte, 2001). Najboljšo rešitev na področju oblikovanja zakonodajnih okvirov za informacijsko bojevanje so ponudili Združeni narodi, katerih članica je postala leta 1992 tudi Slovenija. Ustanovna listina Združenih narodov (ang. Chather of the United Nations; v nadaljevanju Ustanovna listina ZN) (United Nations, 1945) preprosto določa, da se morajo vse članice v mednarodnih odnosih vzdržati grožnje ali uporabe sile zoper teritorialno integriteto ali politično neodvisnost druge države, vendar kljub temu problematika razmejevanja kibernetskega okolja še vedno ni rešena. Medtem, ko organi pregona fizično varujejo naše ozemlje, se lahko vprašamo, kdo pravzaprav varuje državno kibernetsko okolje? Glede na pomanjkanje volje ureditve te težave na državni ravni, lahko upravičeno trdimo, da nihče.

Drugi problem, povezan z informacijskim bojevanjem in njegovo pravno podlago, se nanaša na odkrivanje oz. identificiranje posameznih primerov kibernetske kriminalitete, kot politično, ideološko ali poslovno skrbno načrtovanega primera informacijske vojne. Slovenija je leta 2004 ratificirala Konvencijo, ki je na našem ozemlju pričela veljati leta 2005. To je tudi pravzaprav edini mednarodni dokument, ki ureja problematiko računalniške in kibernetske kriminalitete, vendar se srečuje z enako pomanjkljivostjo kot ostala slovenska zakonodaja. Konvencija (MKKKDP, 2004) in KZ-1 (2008) zgolj opredeljujeta posamezne oblike računalniške kriminalitete,[9] medtem ko pojava informacijskega bojevanja, kot v celoto povezanih posameznih informacijskih napadov, ne predvidevata.

9 *Financiranje terorizma (čl. 109), novačenje in usposabljanje za terorizem (čl. 111), neupravičeno prisluškovanje in zvočno snemanje (čl. 137), zloraba osebnih podatkov (čl. 143), kršitev moralnih avtorskih pravic (čl. 147), kršitev materialnih avtorskih pravic (čl. 148), kršitev avtorski sorodnih pravic (čl. 149), prikazovanje, izdelava, posest in posredovanje pornografskega gradiva (čl. 176), goljufija (čl. 211), izsiljevanje (čl. 213), napad na informacijski sistem (čl. 221), poslovna goljufija (čl. 228), vdor v poslovni informacijski sistem (čl. 237), pranje denarja (čl. 245), ipd.*

Po navedbah Joynerja in Lotrionta (2001) je zaradi tehnik in narave vdorov težko dokazati motiv in namen neke države, Bratuša (2011) pa je mnenja, da takšna situacija državam podpisnicam odvzema možnost za aktivni odgovor na kibernetske napade druge države, saj ne more ugotoviti, da gre v nekem primeru za sistematično rušenje njenih informacijskih sistemov. Zato ne moremo razlikovati med okvaro, kaznivim dejanjem vdora v informacijski sistem in vojno napovedjo neke države.

Tretja težava, povezana z neustrezno normativno ureditvijo, pa se nanaša na zajemanje dokazov in vodenja preiskave tako na državni kot organizacijski ravni. Državni organi imajo sicer na področju preiskovanja računalniške kriminalitete večje pristojnosti in s sprejetjem 219. a člena ZKP-J (2009)[10] tudi boljše pogoje pri zajemanju dokazov. Dokazno vrednost elektronskih podatkov določa tudi ZEPEP (2002, 2004: čl. 4). Temeljna težava se na državni ravni kaže v dveh točkah. Kljub temu, da zakoni opredeljujejo pomen dokazov v elektronski obliki, pa se v praksi organi pregona še vedno srečujejo s problemom nerazumevanja postopkov računalniške forenzike, kar povečuje dvom v zanesljivost dokazov in možnost izpodbijanja njihove verodostojnosti. V fazi preiskave so organi pregona v veliki meri, zaradi transnacionalne narave tovrstne kriminalitete, močno odvisni od pomoči tujih držav. Tudi Konvencija opredeljuje potrebo po medsebojnem sodelovanju na podlagi zaprosil ali bilateralnih pogodb in sporazumov o medsebojni pomoči. Trenutno je situacija takšna, da so možnosti prenašanja odgovornosti in igranje na karto nevednosti še vedno pogoste. Poleg tega pa trenutna zakonodaja s področja varstva osebnih podatkov, državnim organom preprečuje pregledovanje internetnega prometa na vstopnih točkah v državo, tako da tudi normativna ureditev trenutno predstavlja veliko omejitev. Tudi na organizacijski ravni se srečujemo s podobno problematiko. Podjetja v primeru suma industrijskega vohunjenja od zaposlenih, po ZVOP-1 (2004, 2007),[11] ne morejo zahtevati predaje osebnih stvari (kot npr. USB ključkov in drugih pomnilniških naprav) ali pridobiti vpogleda v njihovo vsebino na službenem računalniku (npr. elektronsko pošto in druge možnosti shranjevanja podatkov na spletu oz. omrežju). To lahko stori zgolj pristojni organ, v primeru preiskovanja suma kaznivega dejanja na podlagi pisne odredbe, izjemoma, kot določa 15. člen ZVOP-1 (2004, 2007),[12] pa lahko stori

10 *5. člen ZKP-J: Za 219. členom se doda nov 219. a člen, ki se glasi: Preiskava elektronskih in z njo povezanih naprav ter nosilcev elektronskih podatkov (elektronska naprava), kot so telefon, telefaks, računalnik, disketa, optični mediji in spominske kartice, se zaradi pridobitve podatkov v elektronski obliki lahko opravi, če so podani utemeljeni razlogi za sum, da je bilo storjeno kaznivo dejanje in je podana verjetnost, da elektronska naprava vsebuje elektronske podatke. Imetnik oziroma uporabnik elektronske naprave mora omogočiti dostop do naprave, predložiti šifrirne ključe oziroma šifrirna gesla in pojasnila o uporabi naprave, ki so potrebna, da se doseže namen preiskave.*

11 *8. člen ZVOP-1: Osebni podatki se lahko obdelujejo le, če obdelavo osebnih podatkov in osebne podatke, ki se obdelujejo, določa zakon ali če je za obdelavo določenih osebnih podatkov podana osebna privolitev posameznika.*

12 *15. člen ZVOP-1: Avtomatizirana obdelava osebnih podatkov, pri kateri se o posamezniku lahko sprejme odločitev, ki ima za posledico pravne učinke v zvezi z njim ali na njega znatno vpliva in ki temelji zgolj na avtomatizirani obdelavi podatkov, ki je namenjena ovrednotenju nekaterih osebnih vidikov v zvezi z njim, kakršni so zlasti njegova uspešnost pri delu, kreditna sposobnost, zanesljivost, ravnanje ali izpolnjevanje zahtevanih pogojev, je dovoljena le, če je odločitev: sprejeta med sklepanjem ali izvajanjem pogodbe, pod pogojem, da je pobuda za sklenitev ali izvajanje pogodbe, ki jo je vložil*

to organizacija sama, če v pogodbo o zaposlitvi vključi člen, ki določa, da je npr. elektronska pošta last podjetja in da delojemalec s podpisom dovoljuje vpogled organizacije v njegovo delo. Slednje pa je z vidika nadzorstva delavcev in njihove zasebnosti na delovnem mestu občutljiva in pereča tematika. Zanimivo je, da se s tovrstnimi omejitvami srečujemo večinoma v širšem evropskem prostoru, medtem ko v državah, kjer je informacijsko bojevanje izjemno razširjeno (npr. ZDA in Kitajska) koncept zasebnosti delojemalcev močno podrejen interesom in potrebam delodajalcev. Vpogled v njihove delovne navade in aktivnosti (tudi na področju računalniške tehnologije) je nekaj povsem normalnega.

S tem pa je povezana tudi zadnja težava, ki se nanaša na možnost reakcije oz. odgovora države na sovražni napad. Konvencija bi morala opredeljevati tudi možnost odzivanja napadene države v samoobrambi, s čimer bi lahko onemogočila napade na svoje sisteme. Ustanovna listina ZN sicer vsaki državi pripisuje pravico do obrambe, ki se nanaša tudi na kibernetski napad. Vendar se možnost protinapada nanaša samo na primer samoobrambe, v primeru, ko napad še vedno poteka. Pravico do uporabe sile v primeru obrambe se državam po metodi pravne logike odreka in se tovrstni napad na informacijski sistem razume podobno kot vohunjenje. Uporaba sile za povračilne ukrepe torej ni dovoljena. Glavna dilema, ki se pri oblikovanju ustrezne zakonodaje na tem področju pojavlja, je vprašanje ali in v kolikšni meri lahko neka država uporabi informacijsko operacijo in ali jo druga država v samoobrambi sploh lahko uporabi. Poleg tega je potrebno definirati, v katerih primerih jo lahko uporabi in v katerih ne (Joyner in Lotrionte, 2001).

Problematika, povezana z odkrivanjem, preiskovanjem in dokazovanjem primerov informacijske vojne, je izjemno razsežna in še kako prisotna. Trenutna situacija kaže, da mednarodne skupnosti in posamezne države tej grožnji ne posvečajo potrebne pozornosti, kar je največkrat posledica nerazumevanja in lažnega občutka varnosti. Države – informacijske bojevnice, ki ta trenutek narekujejo smernice informacijske vojne pa se tega dobro zavedajo, vendar jim ureditev problematike lahko povzroči več škode kot koristi. Kaj torej organizacije in države ob takšni trenutni situaciji sploh lahko še storijo?

4 PREDLOGI IN REŠITVE

Nujno je potrebno sprejeti mednarodno - univerzalno definicijo (državne) računalniške in kibernetske kriminalitete, da se bodo strokovnjaki in organi pregona sploh zavedali obsega problematike, proti kateri se borijo. Pri tem je potrebno natančno definirati tudi ne/dovoljene metode uporabe informacijsko-komunikacijske tehnologije v primeru ofenzivnega in defenzivnega delovanja držav in organizacij. Le-ta naj omeji in opredeli posamezne oblike računalniške kriminalitete, kakor tudi politično, ideološko ali poslovno motivirane primere informacijskega boja in s tem organom pregona omogoči celovitost preiskave. Opredelitev dovoljene informacijske operacije v primerih ofenzivnega in

posameznik, na katerega se osebni podatki nanašajo, izpolnjena ali da obstajajo primerni ukrepi za varstvo njegovih zakonitih interesov, kakršni so zlasti dogovori, ki mu omogočajo ugovarjati takšni odločitvi ali izraziti njegovo stališče.

defenzivnega delovanja držav je nujno potrebno, prav tako pa tudi zbiranje podatkov v kibernetskem prostoru za učinkovito obrambo. Hkrati je potrebno mednarodne smernice vpeljati v državno zakonodajo in s tem prispevati k mednarodni harmonizaciji dovoljene uporabe tehnologije. Posamezne države, tudi Slovenija, pa morajo, če želijo preprečiti napade na lastno kritično informacijsko strukturo, odpraviti določene zakonske omejitve, ki jim trenutno v želji po varovanju posameznikove zasebnosti in osebnih podatkov v kibernetskem prostoru to onemogočajo. Samo sprejetje in prilagajanje zakonodaje pa seveda ne zadošča: družbo je potrebno ozavestiti o razširjenosti in resnosti problematike, organe pregona ustrezno usposobiti in spodbuditi njihovo sodelovanje na lokalni in globalni ravni. Pristojni organi morajo v fazi preiskovanja in odkrivanja primerov računalniške kriminalitete upoštevati tudi možnost informacijskega napada s strani druge države ali skupine ter pozornost usmeriti na ugotavljanje motivacije napada. Pri tem je medsebojno sodelovanje držav in državnih služb neizogibno, zato je pri zasledovanju tega cilja potrebno krepiti mednarodne odnose v obliki sklepanja bilateralnih in multilateralnih pogodb o medsebojni pomoči.

Na mikro ravni morajo za ustrezno varnost poskrbeti tudi organizacije, predvsem tiste, ki operirajo s sistemi kritičnega pomena za normalno funkcioniranje družbe, 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. Ustrezna varnostna klasifikacija podatkov in omejevanje števila ljudi, ki z njimi operirajo, je nujen korak, ki skupaj z ustreznim varnostnim preverjanjem vstopajočih v fizični ali kibernetski prostor organizacije, prepreči marsikatero tveganje in uresničeno grožnjo. Predvsem pa je nujno na nacionalni in organizacijski ravni implementirati priporočila in standarde, s pomočjo katerih se lahko učinkovito izvede natančna analiza informacijskega sistema, identificirajo ključne ranljivosti in izpostavljene točke ter uvede potrebne varnostne mehanizme. Le tako se lahko zagotovi učinkovita politika neprekinjenega poslovanja, kot primarnega cilja vsake države in organizacije.

Nadaljnje raziskave informacijskega bojevanja bodo zajemale dojemanje in percepcijo bojevanja, odziv organizacij in posameznikov na razraščajočo se grožnjo in na praktično nezmožnost obrambe pred tovrstnimi pojavi/napadi, saj se tako tehnologija, kot znanje in število uporabnikov dnevno hitro povečuje.

Ob diskusiji o informacijskem bojevanju tako v slovenskem kot tudi mednarodnem prostoru se pojavlja vprašanje izbire ustreznega izraza. Angleški izraz information warfare in njegov slovenski prevod informacijsko bojevanje namreč ne popišeta celovitosti problematike, ki jo naslavljata.

LITERATURA

Adams, S. (25. 1. 2009). Conficker Windows virus infects 15 million PCs. *The Telegraph*. Pridobljeno 22. 5. 2011 na http://www.telegraph.co.uk/technology/4338625/Conficker-Windows-virus-infects-15-million-PCs.html

Bernik, I. in Prislan, K. (2010). Proces upravljanja s tveganji v informacijski varnosti. V T. Pavšič Mrevlje (ur.), *Smernice sodobnega varstvoslovja, 11. slovenski dnevi varstvoslovja.* Ljubljana: Fakulteta za varnostne vede. Pridobljeno 22. 5. 2011 na http://www.fvv.uni-mb.si/DV2010/zbornik/informacijska_varnost/Bernik_Prislan%20proces%20upravljanja.pdf

Botnet hacker caught in Slovenia. (28. 7. 2010). *BBC News Technology*. Pridobljeno 22. 5. 2011 na http://www.bbc.co.uk/news/technology-10786701

Bratuša, T. (2011). *Asimetrično bojevanje in strategija posrednega nastopanja v kibernetski vojni* (Magistrsko delo). Ljubljana: Fakulteta za varnostne vede.

C. R. (22. 1. 2009). Conficker nad finančno ministrstvo. *MMC RTV SLO*. Pridobljeno 20.5.2011 na http://www.rtvslo.si/znanost-in-tehnologija/conficker-nad-financno-ministrstvo/96368

Coleman, K. (25. 4. 2008). Cyber-attacks and cyber-disasters: Are You Prepared? *TechNewsWorld.* Pridobljeno 23. 5. 2011 na http://www.technewsworld.com/story/62725.html?wlc=1317055553

Connolly, K. (22..6. 2009). Germany accuses China of industrial espionage. *The Guardian*. Pridobljeno 15. 3. 2011 na http://www.guardian.co.uk/world/2009/jul/22/germany-china-industrial-espionage

Cyber Crime Statistics. (2006). *Computer Forensics*. Pridobljeno 22. 5. 2011 na http://www.computer-forensics-recruiter.com/home/cyber_crime_statistics.html

Cyber Warfare. (2011). *Tech-FAQ*. Pridobljeno 3.3.2011 na http://www.tech-faq.com/cyber-warfare.html

Felc, M. (31. 7. 2010). Računalniški kriminal se širi. *Delo.* Pridobljeno 22. 5. 2011 na http://www.delo.si/clanek/115666

Fritz, J. (2008). How China will use cyber warfare to leapfrog in military competitiveness. *Culture Mandala, 8*(1), 28-80. Pridobljeno 5. 3. 2011 na http://www.international-relations.com/CM8-1/Cyberwar.pdf

Fullbrook, M. (2009). Tips on stamping out data leakage & industrial espionage during recession. *ICT Review: Computer Hardware and Software Review Journal*. Pridobljeno 30. 4. 2011 na http://ictreview.blogspot.com/2009/03/tips-on-stamping-out-data-leakage.html

Harris, P. (29. 3. 2009). Massive Chinese computer espionage network uncovered. *The Observer*. Pridobljeno 30. 4. 2011 na http://www.guardian.co.uk/world/2009/mar/29/china-computing

Internet usage statistics. (2010). *Internet World Stats.* Pridobljeno 22. 7. 2011 na http://www.internetworldstats.com/stats.htm

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. Pridobljeno 3. 3. 2011 na http://ejil.oxfordjournals.org/content/12/5/825.full.pdf

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

SANS Institute. (2007). *Corporate espionage 201.* Pridobljeno 30. 4. 2011 na http://www.sans.org/reading_room/whitepapers/engineering/corporate-espionage-201_512

Slocum, M. (2010). Cyber warfare: don't inflate it, don't underestimate it. *O'Reilly Radar.* Pridobljeno 4. 3. 2011 na http://radar.oreilly.com/2010/02/cyber-warfare-dont-inflate-it.html

Spam statistics. (2011). El Paso: University of Texas, Information Security Office. Pridobljeno 22. 5. 2011, http://admin.utep.edu/Default.aspx?tabid=64462

Stevens, K. in Jackson, D. (11. 3. 2010). ZeuS banking trojan report. *DELL SecureWorks*. Pridobljeno 22. 5. 2011 na http://www.secureworks.com/research/threats/zeus/?threat=zeus

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

Terrorist hacker gets life. (2008). *MindBullets.* Pridobljeno 22. 5. 2011 na http://www.mindbullets.net/Subscription/MindBulletsIssueView.aspx?MindBulletID=170

Tolle, G. A. (2002). Shaping the information environment. *Military Review,* (3), 47-49. Pridobljeno 4. 3. 2011 na http://cdm15040.contentdm.oclc.org/cdm4/item_viewer.php?CISOROOT=/p124201coll1&CISOPTR=233&CISOBOX=1&REC=9

Topping, A. (18. 11. 2009). Two held over ZeuS trojan virus that steals personal data. *The Guardian*. Pridobljeno 22. 5. 2011 na http://www.guardian.co.uk/technology/2009/nov/18/zeus-zbot-trojan-virus

United Nations. (1945). *Chrather of the United Nations.* Pridobljeno 22. 5. 2011 na http://www.un.org/en/documents/charter/intro.shtml

Ventre, D. (2009). *Information warfare*. London: ISTE, Hoboken: Wiley.

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

Zakon o elektronskem poslovanju in elektronskem podpisu [ZEPEP]. (2000, 2004). *Uradni list RS*, (57/00, 98/04).

Zakon o kazenskem postopku [ZKP]. (1994, 2003, 2004, 2006, 2007). *Uradni list RS*, (63/94, 116/03, 96/04, 8/06, 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).

Zakon o spremembah in dopolnitvah Zakona o kazenskem postopku [ZKP-J]. (2009). *Uradni list RS*, (77/09).

Zakon o varstvu osebnih podatkov [ZVOP-1]. (2004, 2007). *Uradni list RS*, (86/ 04, 94/07).

O avtorjih:

Igor Bernik, doktor znanosti, predavatelj in prodekan za izobraževalno dejavnost, Fakulteta za varnostne vede, Univerza v Mariboru.

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