Informacijsko bojevanje: premik tradicionalnih metod vojskovanja in bojevanja v kibernetični prostor

Igor Bernik, Fakulteta za varnostne vede, Univerza v Mariboru
Kaja Prislan, študentka Fakultete za varnostne vede, Univerza v Mariboru

Namen
Prikazan bo trend razvoja državnega vojskovanja in medorganizacijskega tekmovanja v kibernetskem prostoru. Prispevek želi strokovni javnosti pokazati razsežnosti družbeno škodljivih posledic informacijskega bojevanja in opozoriti na grožnjo, ki se ji, zaradi enostavne in splošne uporabe IKT ne more izogniti noben posameznik, podjetje, korporacija, niti države.

Metodologija
Za proučitev narave in trenutnega stanja informacijskega bojevanja sta uporabljeni deskriptivna in primerjalna metoda. Za pridobitev podatkov in oblikovanje spoznanj o pomembnosti in razsežnosti tovrstne grožnje je analizirana in primerjana strokovna literatura ter internetni viri, ki se nanašajo na področje omenjene problematike. Izvedena je dekompozicija stanja in pogled v dogajanje z vidika groženj in zaščitnih ukrepov v prihodnje.

Ugotovitve
Analiza kaže, da države razvoj IKT niso izkoristile zgolj za poenostavitev delovanja kritičnih družbenih funkcij, temveč tudi za razvoj in nadgradnjo tehnik vojskovanja in doseganja političnih in gospodarskih ciljev. Dodatna analiza primerov informacijskega vojskovanja pa je pokazala, kako resna in nevarna je tovrstna problematika. Ugotavljamo tudi, da je informacijsko bojevanje vse bolj v domeni velikih korporacij oz. tistih poslovnih entitet, ki za svoj obstanek, razvoj in konkuriranje potrebujejo informacije, do katerih nimajo avtoriziranega dostopa, pri tem pa izkoriščajo svojo moč in pozicijo.

Omejitve
Prispevek se omejuje na kibernetični prostor in se ne dotika tradicionalnega kibernetskega bojevanja, ki je bil v praksi že mnogo pred uporabo IT.

Praktična uporabnost
Razumeti pomen kibernetskega bojevanja, tveganja, ki se z rabo ITja pojavljajo pred državami in podjetji v sodobnem konkurenčnem okolju je področje, ki bi ga praktično morali poznati vsi, ki delujejo na področju obravnavanja in odločanja na podlagi informacij.

Izvirnost/pomembnost prispevka
Izvirnost prispevka se kaže v njegovem namenu. Opozoriti želimo na novodobno, predvsem pa neizogibno grožnjo z resnimi družbenimi posledicami. Za učinkovito zoperstavljanje je strokovno javnost nujno potrebno ozavestiti, svetovati in opozoriti na izpostavljene kritične točke. Prevencija je ključ do uspešne obrambe pred zlonamernimi grožnjami, česar pa

organizacije in država ne morejo vzpostaviti brez natančnega razumevanja in poznavanja njene narave ter razsežnosti.

Ključne besede: informacijsko vojskovanje, informacijsko bojevanje, tekmovalnost, kibernetični prostor, informacijska varnost

1 Uvod

Politično, gospodarsko ali ideološko motivirana kibernetska kriminaliteta je ena izmed najbolj perečih tematik sodobne družbe, ki pa ta pojav v veliki meri še vedno podcenjuje. Širša družbena motivacija, ki se uresničuje s pomočjo IT, presega individualne interese, krši družbene norme pa vendar je v večini primerov legalna, neopazna in v določenih kulturnih okoljih celo legitimna. Razvoj sodobne informacijsko komunikacijske tehnologije (v nadaljevanju IKT) pa je takšno stanje še poglobil, saj je omogočil prepletenost različnih oblik kriminalnih dejanj, v enem okolju z enakimi tehnikami. Omogočil je tudi razvoj posebne oblike bojevanja, t.i. informacijsko bojevanje (ang. Information Warfare). Zaradi splošne dostopnosti orodij in znanj so tehnike doseganja ciljev v kibernetskem prostoru postale izjemno lahke, v večini primerov primerljive z ostalo računalniško kriminaliteto. Glavna težava, s katero se srečujejo pristojni organi je ravno razlikovanje med širše družbeno 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, kot so npr. sociologija, antropologija, ekonomija, zgodovina, politika ali vojska (Ventre, 2009). Tudi izraz »informacijsko« na posameznih področjih razumejo različno, zato ni enotne definicije, morda pa tudi izraz sam ni najboljši. Zaradi razsežnosti problematike povezane z informacijskim bojevanjem v prispevku predstavljamo naravo in možne odzive. S primeri predstavljamo nevarnosti, ki pretijo vsaki državi in organizaciji. Na teh primerih oz. tujih izkušnjah se lahko pristojni državni organi in odgovorni v podjetjih naučijo, kako ukrepati v kriznih situacijah.
Ob diskusiji o informacijskem bojevanju tako v slovenskem, kot tudi mednarodnem prostoru se pojavlja vprašanje izbire ustreznega izraza. Tako ang. izraz information warfare, kot slovenski prevod iz ang. jezika v informacijsko bojevanje ne popišeta celovitost problematike, ki jo naslavljata.

2 Informacijsko bojevanje

Informacijsko bojevanje zajema boj z informacijami in nastopa v različnih družbenih sektorjih. Menimo, da je 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. Siroli (2006) informacijsko bojevanje razume kot aktivnosti katerih namen je doseči nadvlado oz. prednost z vplivanjem na nasprotnikove informacije,

informacijske procese, informacijske sisteme in računalniška omrežja, hkrati pa tudi varovanje in zaščito lastne informacijske infrastrukture. Sestavljena je iz aktivnosti, katerih namen je zanikati, okvariti ali uničiti nasprotnikove informacijske vire, vključuje tako napadalno kot obrambno dejavnost, ki se medsebojno velikokrat prekrivata. 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. 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.
Med organi pregona in zasebno sfero je kibernetski kriminal požel veliko pozornosti, medtem ko je bil v vojaško-birokratski sferi potisnjen v okvir informacijskega bojevanja, informacijskih operacij, kibernetskega terorizma in kibernetske vojne. V strokovni IT javnosti pa so grožnje veliko natančneje poimenovane, s poudarkom na napade na računalniška omrežja, okvare, motnje in izkoriščanje informacijskih sistemov (Eriksson in Giacomello, 2006).
Povzamemo torej, da je informacijsko bojevanje posledica združitve državnih in organizacijskih ciljev 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 kibernetske kriminalitete. Vsekakor pa to ni sodoben termin, saj se je razumevanje informacijskega bojevanja v preteklosti nanašalo na vojaško uporabo informacij kot orodje vojne za in zoper informacije drugih držav. Wall (2007) navaja, da se je takšna oblika bojevanja dolgo časa uporabljala za oslabitev obrambe nasprotnika in je bila vojskam poznana že mnogo let pred nastankom informacijskih tehnologij.
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.

2.1 Fenomen sodobnega informacijskega bojevanja

Nelegalni posegi državnih organov in služb v računalnik, računalniško mrežo ali 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. Jeffery Carr v knjigi ''Inside Cyber Warfare'', v intervjuju (Slocum, 2010) za spletno stran O'Reilly, informacijsko bojevanje primerja z izumom revolverja, ki je revolucionaliziral bojevanje. In prav to se ob pojavu IKT sedaj dogaja z informacijskim bojevanjem. Meni, da je z njim mogoče doseči ravnovesje med neenakovrednimi nasprotniki. In to zaradi dveh stvari: trenutne ranljivosti spleta in ker so vojaške sile, kakor tudi druge entitete, vključene v lokalna in mednarodna omrežja.
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 IKT bi povzročil zaostanek. Brez IKT nobena organizacija na svetu ne more biti konkurenčna; nekonkurenčnost

pa pomeni finančno izgubo in neuspeh. Tudi vojska brez IKT 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 prinaša. Fritz (2008) navaja, da je za državo nemogoče vzpostaviti ustrezno obrambo pred informacijskim napadom, če sama ne obvlada tehnik informacijskega bojevanja.
Sklepamo, da prenos bojev z informiranjem v kibernetski prostor ni več vprašanje temveč dejstvo. Poznavanje, razvijanje in uporaba tehnik informacijskega bojevanja je nujno potrebna 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 za ofenzivno/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. 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 onemogočanje dostopa do informacij, ki jih 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). Informacijska »vojna« ima dve temeljne obliki: ena vključuje dezinformiranje oz. zavajanje nasprotnika, druga pa predstavlja napad na računalniško omrežje in aktivno uničenje ali okvaro nasprotnikovih informacij (Jurich, 2008).
Tehnike informacijskega bojevanja tako kot ostale oblike kibernetske kriminalitete izkoriščajo varnostne vrzeli v varnostnih sistemih. Informacijska varnost 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. Velikokrat so za vdore in napade na informacijske sisteme za potrebe vohunjenja izkoriščene tudi brezžične spletne povezave (SANS Institute, 2007). Zanimivo dejstvo je, 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 Cyber Crime Statistics (2006) navaja, da sta splet in z njim povezana nezaželjena elektronska pošta (spam) najpogostejša načina izvajanja kibernetske kriminalitete. Elektronska pošta pogosto 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. Pri učinkih, ki jih takšne tehnike lahko povzročijo pa je vseskozi potrebno imeti v mislih dejstvo, da je kibernetski boj orožje za masovno motenje in ne orožje za masovno uničenje (Berkowitz, 2003).

Tehnike informacijskih bojevnikov so najrazličnejše ter prilagojene zahtevnosti, znanju in vrsti ogroženega okolja. Najvišja stopnja ogroženosti pa se kaže na področju naslednje kritične infrastrukture (Siroli, 2006):

- Informacije in komunikacije: poleg naravnih nesreč so največja grožnja okvare sistemov in njihova nestabilnost zaradi kompleksnosti medmrežij; izključene niso tudi namerne okvare in zlonamerni vdori.
- Energija: ranljivosti v tem sektorju so se povečale predvsem zaradi vse večje odvisnosti od IKT in prepletenosti informacijskih sistemov (npr. sistem SCADA[1], ki nadzira in spremlja energijsko infrastrukturo, kar predstavlja resno nevarnost in tveganje s kibernetičnega vidika).
- Bančništvo in finance: zaradi visoke odvisnosti od IT so posamezne institucije velikokrat podvržene kraji in ponarejanju. Največjo grožnjo predstavljajo zaposleni, ki avtoriziran dostop izkoriščajo za krajo zaupnih informacij. Velik problem predstavlja tudi želja po ohranjanju poslovnega ugleda, zaradi česar velikokrat delujejo netransparentno, kar odkrivanje groženj in zaščito sistemov še bolj zapleta.
- Fizična distribucija: transportni sektor je prav tako zaradi odvisnosti od IT predvsem z vidika komunikacij in managementa podvržen kibernetskim grožnjam. Kot najbolj izpostavljen se omenja predvsem zračni transport, ki je povsem odvisen od elektronskih sistemov.
- Oskrba ljudi z nujnimi življenjskimi potrebščinami: ranljivosti v tem sektorju so prav tako povezane z odvisnostjo od SCADA sistemov v preskrbi z vodo. Velika ranljivost se pojavlja tudi na področju komunikacijskih sistemov služb za nujno odzivanje, vladnih informacijskih sistemov in vojaškega informacijskega premoženja.

Varnostne pomanjkljivosti, ki jih izkoriščajo informacijski bojevniki 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 2011), z namenom ugotoviti ali finančna in gospodarska kriza vplivata na delovni odnos ljudi, njihovo etiko in informacijsko varnost. Rezultati so pokazali, da so 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 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.

[1] Supervisiory Control and Data Acquisition System

2.2 Primeri

Tarča informacijskega bojevanja je lahko vsaka država, organizacija ali posameznik. Na državni ravni je težko govoriti o bolj 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 prave bojne linije, zato je potencialno bojišče katerikoli računalniško krmiljen 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. Tudi v zasebni sferi se 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 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 informacij. Connolly (2009) med področja, ki so najbolj izpostavljena z vidika informacijskega bojevanja, uvršča avtomobilsko industrijo, industrijo z obnovljivimi energijami, komunikacijami, optiko, rentgensko tehnologijo, stroji in raziskavami. SANS Institute (2007) pa navaja, da 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).

Viri pogosto omenjajo (Cyber Warfare, 2011), 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 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. Glavne aktivnosti so bile usmerjene 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 ZDA pa je odmeven primer vohunske programske opreme GhostNet, ki so jo leta 2009 odkrili kanadski raziskovalci iz Univerze v Torontu. Harris (2009) navaja, da 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 se je v računalnike penetriral preko spleta nato pa kradel podatke, nadziral elektronsko pošto in vklapljal mikrofone in kamere na okuženih računalnikih. Sum je padel na Kitajsko vlado, saj je ta redno napadala tibetansko gibanje s podpiranjem separatizma in terorizma na Kitajskem.

2.3 Akterji

Primeri informacijskega bojevanja kažejo, da sta najmočnejši državi na tem področju ZDA in Kitajska. Po mnenju Bratuše (2011) 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.
ZDA so na področju informacijske tehnologije najbolj razvita država na svetu. Hkrati pa so tudi najbolj odvisne od komunikacijske infrastrukture, kar ima za posledico da so z vidika IT tudi najbolj ranljiva država. Ravno zaradi slednjega v ZDA potekajo različni programi in aktivnosti z namenom zmanjševanja te ranljivosti. Najpomembnejši korak pri doseganju tega cilja je bil ustanovitev Izvršnega odbora za informacijsko bojevanje (Information Warfare Executive Board) v letu 1995. Nekaj mesecev zatem je bila sprejeta najpomembnejša direktiva na tem področju Presidental Decision Directive 39 (PDD39), ki ureja politiko s področja terorističnih groženj in vključuje aktivnosti povezane z informacijskim bojevanjem (Siroli, 2006). Že leta 1998 je bila v ameriškem nacionalnem programu za zaščito kritične infrastrukture CIP[2] zapisana potreba 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[3]. 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[4], kot hrbtenico NCW. Vsi pomembnejši sistemi vključeni v NCW bodo v prihodnosti medsebojno povezani preko GIGa. Leta 2003 je pod okriljem ameriškega obrambnega ministrstva na področju NCW nastal dokument z naslovom Smernice informacijskih operacij[5]. 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. Temeljna naloga informacijskih operacij je 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

[2] Critical Infrastructure Protection
[3] Network-centic Warfare
[4] Global Information Grid
[5] Information Operations Roadmap

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 zavarovanju, analiziranju in ogrožanju informacijskega okolja: USCYBERCOM[6], za obrambo vojaških računalniških omrežij ter izvedbe kibernetskih napadov; ARCYBER[7] 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; CYBERFOR[8] je enota namenjena poveljevanju ter zagotavljanju sil in opreme za kriptologijo, analiziranje signalov in elektronsko bojevanje; 24 AF[9] pa enota zračnih sil, katere namen je ravno tako kibernetsko bojevanje (Bratuša, 2011). V ZDA so postali pionirji v postavljanju kibernetske zaščite s tem, ko so ustanovili prvi CERT[10] leta 1988 v Carnegie Mellon University, kot odziv na rastočo število omrežnih napadov (Hughes, 2009). Danes je ameriški CERT del ameriškega ministrstva za domovinsko varnost in koordinira obrambne ukrepe ter odzive na napade po celotnem državnem ozemlju[11]. Po celotnem svetu obstaja več kot 250 CERTov vendar je njihovo medsebojno sodelovanje zelo omejeno. Tudi FBI igra veliko vlogo pri preprečevanju in pregonu kibernetskih napadov. V primeru, da je izvor napada zunanji se v preiskavo vključi obveščevalna agencija CIA, če pa kibernetski incident vključuje tudi finančni napad pa glavna agencija preiskovanja postane Secret Service. Lastne specialiste za kibernetsko varnost pa imajo tudi v ameriškem ministrstvu za obrambo in nacionalni varnostni agenciji (NSA-National Security Agency) (Hughes, 2009). 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.
Po letu 2000 so tudi nekatere evropske države kot, so Nemčija, Nizozemska, Norveška, Švedska, Švica, Velika Britanija, Avstrija, Finska, Francija in Italija pričele z izvajanjem analiz ranljivosti nacionalnih infrastruktur, zgodnjega opozarjanja in sprejemanja zakonskih aktov na tem področju (Siroli, 2006). Poleg ZDA se, kot najmočnejša z vidika informacijskega bojevanja omenja še Kitajska, saj je informacijsko bojevanje zanjo kritičnega in vitalnega pomena. Ameriška vojska je identificirala skupno pet kitajskih baz za informacijsko bojevanje, kjer naj bi kitajska oblast zbirala učenjake in nadarjene za tehnologijo, prav tako pa urila lastne vojaške enote za to področje. S tem je močno povečala znanje, kapacitete in sposobnost vojaških sil, ki naj bi bile povsem sposobne prevzeti mesto svetovne velesile in izvesti uspešne mednarodne vojaške operacije (Wu, 2006). 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

[6] United States Cyber Command
[7] Army Cyber Command
[8] Navy Cyber Forces
[9] 24 Air force
[10] Cyber Emergency Response Team
[11] Več o US-CERT na http://www.us-cert.gov/aboutus.html

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

2.4 Slovenija

Prednosti IKT se zaveda tudi Slovenija, v kateri je mogoče opaziti trend vse 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. Pri tem je v Sloveniji 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. 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).

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. 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.

3 Razprava

Nujno je potrebno sprejeti mednarodno - univerzalno definicijo kibernetske kriminalitete, da se bodo strokovnjaki 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 kibernetske kriminalitete, kakor tudi politično, ideološko ali poslovno motivirane primere informacijskega bojevanja in s tem organom pregona omogoči celovitost preiskave. Opredelitev dovoljene informacijske operacije v primerih ofenzivnega in 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. Nujno je čim hitreje zavarovati lastno informacijsko infrastrukturo in pri tem postaviti dober zgled organizacijski sferi. Stremeti moramo k odgovorni in kvalitetni zaščiti (npr. v letu 2010 je izpolnjevanje točno določenih varnostnih standardov, ki jih je določila organizacija North American Electric Realiability Corporation's Critical Infrastructure Protection, v ameriški električni proizvodnji postalo obligatorno). Posamezne države, tudi Slovenija, 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 onemogoča. Samo sprejetje in prilagajanje zakonodaje 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. Na nacionalni in organizacijski ravni je nujno implementirati priporočila in standarde, s pomočjo katerih se lahko učinkovito izvede natančna analiza informacijskega sistema, identificira 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. Celovita zaščita slovenske informacijske infrastrukture je v določeni meri odvisna tudi od odgovornosti in ozaveščenosti vsakega posameznika, kot uporabnika IKT. Vsi uporabniki povezani v globalno omrežje smo potencialne žrtve, ki z zlonamernim izkoriščanjem našega informacijskega premoženja hitro postanemo »informacijski bojevniki«. Izobraževanje o informacijski varnosti je torej neizogiben korak pri spoznavanju, razumevanju in ponotranjenju odgovornosti v digitalnem okolju. Vsak posameznik je odgovoren za lastna dejanja ne glede na to, v katerem okolju se nahaja, naloga držav in organizacij pa je družbo ozavestiti o tveganjih povezanih z omrežji, ki so del našega vsakdana.

Nadaljnje raziskave informacijskega bojevanja bodo zajemale 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.

4 Literatura

Berkowitz, B. (2003). *The New Face of War: How War Will Be Fought in the 21st Century.* New York: Simon & Schuster Inc.

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

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

Coleman, K. (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. (2009). *Germany accuses China of industrial espionage*. 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

Eriksson, J. in Giacomello, G. (2006). The Information Revolution, Security, and International Relations: (IR)relevant Theory? *International Political Science Review,* 27(3), 221-244.

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. (2011). 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

Hughes, B. (2009). *NATO and Cyber Defence: Mission Accomplished*? Pridobljeno 23.7.2011 na http://www.atlcom.nl/ap_archive/pdf/AP%202009%20nr.%201/Hughes.pdf

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

Jurich, J.P. (2008). Cyberwar and Customary International Law: The Potential of a ‘‘Bottom-up” Approach to an International Law of Information Operation. *Chicago Journal of International Law,* 9(1), 275-295.

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

Siroli, G.P. (2006). Strategic Information Warfar: 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 4. 3. 2011 na http://radar.oreilly.com/2010/02/cyber-warfare-dont-inflate-it.html

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.

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

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

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

Wu, C. (2006). An Overview of the Research and Development of Information warfare in China. V E. Halpin, P. Trevorrow, D. Webb in S. Wright (ur.*), Cyberwar, Netwar and the Revolution in Military Affairs* (str. 173-195). New York: Palgrave Macmillan.