Denis Čaleta,
Gorazd Rolih

Pregledni znanstveni članek

KIBERNETSKA VARNOST V DRUŽBI IN DELOVANJE KRITIČNE INFRASTRUKTURE – ANALIZA STANJA NA OBRAMBNEM PODROČJU V REPUBLIKI SLOVENIJI

CYBER SECURITY IN THE OPERATION OF CRITICAL INFRASTRUCTURE – AN ANALYSIS OF THE SITUATION IN THE FIELD OF SLOVENIAN DEFENCE

Review paper

Povzetek Pojav asimetričnih oblik ogrožanja nacionalne in mednarodne varnosti izhaja iz popolnoma drugih predpostavk in dojemanj temeljnih konceptov zagotavljanja varnosti, ki je še nekaj časa po koncu hladne vojne temeljila na statičnem pristopu do obvladovanja konvencionalno opredeljivih vrst groženj. Spreminjajoče se družbene razmere in napetosti, ki jih je prinašal hiter tehnološki razvoj, so posamezna družbena okolja našle popolnoma nepripravljena na spopadanje z novo globalno varnostno situacijo. Zaradi navedenega bo treba kibernetskim grožnjam nameniti posebno pozornost. Učinkovito obvladovanje teh groženj je pomemben pogoj za nemoteno delovanje informacijsko-komunikacijskih sistemov, ki delujejo v okviru kritične infrastrukture. V Republiki Sloveniji bo treba ukrepe zoperstavljanja kibernetskim grožnjam načrtovati in izvajati s sistemskim pristopom, saj si je zaradi omejenosti finančnih, kadrovskih in tehnoloških potencialov nemogoče zamisliti drugačno pot. Pri tem pa mora imeti obrambno področje, vključno s Slovensko vojsko, pomembno vlogo.

Ključne besede ***Kibernetske grožnje, globalna varnost, obrambni sistem, CERT1, kritična infrastruktura.***

Abstract The emergence of asymmetric forms of threats to national and international security arise from completely different assumptions and perceptions related to the provision of security which, until recently, have been based on a static approach towards the management of conventional threats. As a result, changing social conditions and tensions (brought about by rapid technological development) have found individual social environments and classes completely unprepared for confrontation with this new, global, security situation. As the effective management of such threats is a significant condition for the smooth functioning of information and communication systems that are a part of critical infrastructure, cyber threats require special attention.

[1] *Computer Emergency Response Team.*

In the Republic of Slovenia, it will be necessary to plan measures to counter cyber threats and apply these on the basis of a systemic approach. Due to limited financial, personnel and technological potentials, it is impossible to think of a different course of action. In this context, the defence sector, including the Slovenian Armed Forces, must adopt a more active and significant role.

Key words ***Cyber threats, global security, defence system, CERT2, critical infrastructure***

Uvod

Globalizacija sveta in s tem posredno globalizacija varnosti postavlja moderno družbo pred zahtevna vprašanja, po eni strani, kako še naprej svoj razvoj utemeljevati na glavnih postulatih prostega pretoka blaga, storitev in ljudi, ter po drugi, kako grožnje obvladovati na sprejemljivi ravni tveganja. Pojav asimetričnih oblik ogrožanja nacionalne in mednarodne varnosti izhaja iz popolnoma drugih predpostavk in dojemanja osnovnih konceptov zagotavljanja varnosti, ki je še nekaj časa po koncu hladne vojne temeljila na statičnem pristopu k obvladovanju konvencionalno opredeljivih vrst groženj. Spreminjajoče se družbene razmere in napetosti, ki jih je prinašal hiter tehnološki razvoj, so posamezna družbena okolja našle popolnoma nepripravljena na spopadanje z novo globalno varnostno situacijo. Pojav nedržavnih akterjev, ki so vstopili v interakcijo med tradicionalne subjekte mednarodnih odnosov, je na površje potisnil nove oblike varnostnih groženj, ki so asimetrične in se jim s tradicionalnimi sistemi in vzvodi ni bilo več mogoče učinkovito zoperstaviti. Dinamične spremembe in nesluten tehnološki razvoj so tej dimenziji dodali še kompleksnejšo obliko. Dejstvo, da je moderna družba danes v celoti odvisna od delovanja informacijske in komunikacijske tehnologije, to družbo z varnostnega vidika dela še bolj ranljivo, posamezne grožnje nemotenemu delovanju kritične infrastrukture in tveganja zaradi njih pa še bolj neobvladljive[3]. Nekateri deli te infrastrukture so za delovanje družbe tako pomembni, da bi njihovo nedelovanje ali omejeno delovanje lahko povzročilo hude posledice ali težave. To infrastrukturo imenujemo kritična infrastruktura in jo poskušamo definirati tako na nacionalni kot tudi na mednarodni ravni, seveda odvisno od učinkov, ki bi jih imelo njeno nedelovanje ali uničenje.[4] V tem okviru sta po našem mnenju še posebej izpostavljena dva sektorja, in sicer oskrba z električno energijo ter informacijsko-komunikacijska tehnologija, ki sta neločljivo povezani in soodvisno vplivata na delovanje vseh drugih

---

[2] *Computer Emergency Response Team.*

[3] *62 % ameriške kritične infrastrukture je neposredno priključene na internet ali na IP-omrežje (Secure Computing, 2008).*

[4] *»Kritična infrastruktura državnega pomena v RS obsega tiste zmogljivosti in storitve, ki so ključnega pomena za državo in bi prekinitev njihovega delovanja ali njihovo uničenje pomembno vplivalo ter imelo resne posledice na nacionalno varnost, gospodarstvo, ključne družbene funkcije, zdravje, varnost in zaščito ter družbeno blaginjo.« (Sklep Vlade RS, št. 80000-2//2010/3, z dne 19. 4. 2010). V okviru EU pa so definicije naslednje: »kritična infrastruktura« pomeni infrastrukturno zmogljivost, sistem ali njun del, ki se nahaja v državah članicah in je bistven za vzdrževanje ključnih družbenih funkcij, zdravja, varnosti, zaščite, gospodarske in družbene blaginje ljudi, ter katerih okvara ali uničenje bi imelo v državi članici resne posledice zaradi nezmožnosti vzdrževanja teh funkcij,« in »evropska kritična infrastruktura ali EKI pomeni kritično infrastrukturo, ki se nahaja v državah članicah in katere okvara ali uničenje bi imelo resne posledice v vsaj dveh državah članicah. Kaj so resne posledice se oceni skladno z medsektorskimi merili. To vključuje vplive na druge vrste infrastruktur, ki izhajajo iz medsektorskih odvisnosti« (DIREKTIVA SVETA (ES) št. 114/2008 z dne 8. decembra 2008).*

sektorjev kritične infrastrukture. Zaradi navedenega bomo kibernetskim grožnjam v tem prispevku namenili posebno pozornost. Njihovo učinkovito obvladovanje izpolnjuje pomemben pogoj za nemoteno delovanje informacijsko-komunikacijskih sistemov, ki delujejo znotraj kritične infrastrukture.

1 PREGLED LITERATURE IN TEORETIČNA IZHODIŠČA ZA PROUČEVANO VPRAŠANJE

V današnjem svetu lahko ugotovimo, da sta informacijska in komunikacijska tehnologija zaradi ekonomskih, gospodarskih, sociooloških in kulturnih vplivov postali nepogrešljiv del sodobne informacijske družbe. Nemogoče si je namreč predstavljati delovanje družbe brez ustreznega delovanja informacijsko-komunikacijske tehnologije. V kontekstu razumevanja je treba konkretneje definirati pojem te tehnologije. Evropska unija je v to področje uvrstila medmrežje, zagotavljanje fiksnih in mobilnih telekomunikacij, radijsko in satelitsko komunikacijo in oddajnike. (Svete, 2010)

V okvir mogočih vidikov ogrožanja kritične infrastrukture s področja informacijsko-komunikacijske tehnologije lahko uvrstimo naravne grožnje in grožnje, ki jih povzroča človek. Te pa lahko delimo še v namerno in nenamerno ogrožanje. V svojem prispevku se omejujemo na namerno ogrožanje, pri katerem ima pomembno vlogo teroristično ogrožanje. Zlasti po terorističnih napadih v ZDA leta 2001 se je med varnostnimi strokovnjaki okrepilo mnenje, da bodo informacijski sistemi ena izmed naslednjih tarč teroristov (informacijski terorizem – Cyberterrorism). (Weimann, 2006) Vse večja kompleksnost informacijskih sistemov je varnostni izziv za razvijalce in uporabnike. Analiza trenutnega dogajanja na področju kibernetskih groženj je pokazala, da kibernetski terorizem ni največja grožnja. Protiteroristični koordinator EU meni, da so trenutno na tem področju največja grožnja različna kriminalna omrežja in posamezniki, ki jih podpirajo ali sponzorirajo posamezne države (De Kerchove, 2010).

Lukman in Bernik (2010, str. 5) ugotavljata, da je popolno klasifikacijo kibernetskih groženj težko izdelati, ker se nenehno porajajo nove oblike napadov, ki jih ni mogoče razvrstiti v znane podskupine. Chakrabarti in Manimaran podajata taksonomijo napadov na infrastrukturo interneta kot odgovor na prejšnje razvrstitve, ki so bile usmerjene predvsem v varovanje in zaščito informacij. Napade sta razdelila v štiri osnovne kategorije: napadi na sisteme, prenosne zmogljivosti in programske pakete ter onemogočanje storitev (Chakrabarti, Manimaran, 2003). Za zagotovitev zaupnosti in integritete elektronskih sporočil so bili razviti številni kriptografski algoritmi, ki pa imajo varnostne vrzeli, ki jih izkoriščajo tako sistemski administratorji kot tudi napadalci, da bi izluščili občutljive informacije iz šifriranega omrežnega prometa (Kjaerland, 2005). Razvoj telekomunikacijske infrastrukture poteka tako, da se tradicionalni telefonski sistem in informacijska tehnologija vse bolj združujeta v enotno platformo. Vse hitrejša širitev brezžičnih komunikacijskih sistemov zelo

povečuje možnosti zlorab. V tem primeru namreč tradicionalni obrambni pristop do tveganj, povezanih s kibernetskim prostorom, virtualnim svetom ter terorizmom, dobi kompleksnejšo dimenzijo. Collin virtualni svet opredeljuje kot »/.../ kraj, kjer računalniški programi delujejo in se podatki premikajo.« (v Politt, 1997) Načrtovanje informacijske zaščite teh sistemov zahteva celovit pristop in natančno izvajanje vseh postopkov. Za lažje prepoznavanje vdorov v sisteme so razvili programsko opremo za njihovo odkrivanje in alarmiranje. Kljub visoki tehnični ravni postane programska oprema resnično učinkovita šele v povezavi z analizo. V tem kontekstu ponovno ugotovimo pomen človeškega potenciala in njegovo vlogo v celovitem sistemu zaznavanja obravnavanih groženj. Tun in Aung sta proučila delo analitikov in predlagala orodje za vizualizacijo vdorov (Tun in Aung, 2008). Sisteme za javljanje vdorov je proučeval tudi Kumar, ki predlaga model za avtomatsko klasifikacijo zaznanih vdorov (Kumar, 1994). Kljub številnim razvrstitvam kibernetskih napadov pa lahko vse napade na sisteme kritične infrastrukture razdelimo v tri glavne skupine: vdori v sisteme, onemogočanje storitev ter napadi prek škodljive programske opreme (malware) (Lukman, Bernik, 2010).

Terorizem je v razmerju do uporabe svetovnega spleta povezan na več načinov, in sicer ga uporabljajo kot medij za prenos svojih sporočil ali kot orodje za napad na posamezne cilje. Svetovni splet je postal forum mednarodnega terorizma za širjenje ideologije in novačenje ter mobilizacijo novih članov, zbiranje finančne in materialne podpore, za širjenje sporočil z vsebino sovraštva in nasilja, iskanje informacij, psihološko bojevanje, načrtovanje in usklajevanje dejavnosti ter za medsebojno komunikacijo. Po drugi strani pa poskušajo posamezniki napasti[5] računalniška omrežja, vključno s tistimi, ki so priključena na svetovni splet. (Weimann, 2006)

2 METODE

Analiza mehanizmov zoperstavljanja kibernetskim grožnjam, ki bo opravljena v prispevku, temelji na predpostavki, da se lahko tako kompleksnim grožnjam na nacionalni in mednarodni ravni učinkovito zoperstavimo samo z načrtnimi in ustrezno usklajenimi ukrepi. Analiza daje tisto podlago, s katero nam je omogočeno stvarno ovrednotiti ukrepe, ki jih za zmanjševanje in preprečevanje kibernetskega ogrožanja izvajamo v Republiki Sloveniji. V tem kontekstu v sklepu prispevka podajava tudi posamezne predloge o nujnosti združevanja virov in mehanizmov na področju preprečevanja te grožnje. Ta pristop ima še posebej pomembno vlogo v manjših državah z omejenimi kadrovskimi, finančnimi, organizacijskimi in drugimi viri.

Raziskovalno vprašanje, ki se nam postavlja pri proučevanju mehanizmov odzivanja na kibernetske grožnje, je predvsem, ali so mehanizmi in vzvodi, ki jih ima Republika Slovenija, sposobni ustreznega odzivanja na tako kompleksno grožnjo.

---

[5] *Resnosti groženj z interneta se zavedajo številne države, ki ustanavljajo središča za kibernetsko obrambo (Malezija je ustanovila prvo mednarodno zavezništvo za zaščito pred kibernetskimi napadi, IMPACT – International Multilateral Partnership Against Cyber Terrorism), (Ko, 2008). Nato je v Estoniji ustanovil center odličnosti za kibernetsko obrambo (Cyber Defence Centre of Excellence) (www.nato.int).*

Pri raziskavi tega raziskovalnega vprašanja bomo uporabili tudi več kazalnikov, ki kažejo na podporo političnih struktur vlogi subjektov nacionalnovarnostnega sistema in jih na splošno lahko omejimo na naslednje: (1) število sprejetih zakonskih predpisov, (2) število pripravljenih zakonskih predpisov, (3) jasnost zakonskih predpisov (število vloženih zahtev za razmejitev pristojnosti), (4) število vloženih pobud za spremembo oziroma dopolnitev veljavnih pravnih aktov, (5) količina proračunskih sredstev, (6) pozitivne izjave podpore vodilnih politikov v državi, (7) prisotnost in pogostost programsko-idejne usmerjenosti ter (8) uveljavitev sprejetih zakonskih rešitev v praksi.

V prispevku bomo zato poskušali priti do ugotovitev na podlagi dosedanjega znanja in izkušenj, predvsem pa z različnimi metodološkimi pristopi. Pri pripravi članka bomo kot glavne metode uporabili metode kvalitativne analize, zgodovinsko primerjalno metodo, opisno metodo in metodo vsebinske analize.

Glavne omejitve prispevka so: (1) široko zasnovana tematika, ki odpira številna vprašanja, na katera kljub uresničitvi naštetih ciljev ni mogoče v celoti odgovoriti; (2) razmere, povezane s kibernetskimi grožnjami, se nenehno spreminjajo. Procesi globalizacije vedno znova odpirajo nove možnosti za pojavljanje različnih oblik ogroženosti ter nas postavljajo v situacijo, da je lahko nekaj, kar smo v prispevku ugotovili danes, jutri že zastarelo; (3) podatki o organizaciji sistemov zoperstavljanja kibernetskim grožnjam so v večini držav označeni s stopnjami tajnosti in njihova raba v raziskovalne namene omejena. Poleg tega se je namreč treba zavedati, da je Republika Slovenija s svojimi viri zelo težko primerljiva z drugimi državami.

3 ANALIZA STANJA

Če želimo oceniti stanje na področju sistemskega pristopa k preprečevanju kibernetskih groženj v Republiki Sloveniji in seveda tudi v obrambnem sistemu, je treba opraviti temeljito analizo pravnih in doktrinarnih dokumentov obravnavanega področja. Glede na ugotovitve, da je informacijsko-komunikacijska tehnologija danes povezana skoraj z vsakim področjem, bo analiza pravne podlage usmerjena tudi na področje varovanja kritične infrastrukture, in sicer v tistem delu, ki je neposredno povezan s kibernetsko varnostjo. Rezultati analize so omejeni predvsem na stanje v Republiki Sloveniji, v povezavi z mednarodnim okoljem, ki ga prikazujemo s sklicevanjem na ukrepe EU in Nata. Sledi pregled nekaterih najpomembnejših dokumentov, povezanih s kibernetskimi grožnjami in zaščito pred njimi, ki so opredeljeni v EU in Natu. V nadaljevanju pa bodo analizirani še dokumenti, sprejeti na nadnacionalni ravni.

3.1 Evropska unija

Kadar govorimo o kibernetskih grožnjah, je ključnega pomena zaščita kritične infrastrukture oziroma zaščita kritične informacijske infrastrukture kot njenega sestavnega in zelo pomembnega ter ranljivega elementa. Decembra 2004 je Svet EU sprejel

Evropski program za varovanje kritične infrastrukture (European Programme for Critical Infrastructure Protection – EPCIP), pozneje pa so potekali še seminarji, na katerih so sodelovali vse članice in industrijska združenja, skupaj s strokovnjaki za informacijsko varnost. Evropska komisija je zatem pripravila Zeleno knjigo o evropskem programu za varovanje kritične infrastrukture. Opredeljenih je bilo 11 področij kritične infrastrukture, to so: energetika, informacijska in komunikacijska tehnologija, preskrba z vodo, preskrba s hrano, zdravstvo, finance, javni in pravni red ter varnost, javna uprava, transport, kemična in jedrska industrija ter vesolje in raziskave, ki jih je komisija pozneje v Direktivi o evropski kritični infrastrukturi št. 114/2008 omejila le na dve področji, in sicer na promet in energetiko. Zelena knjiga o evropskem programu za varovanje kritične infrastrukture (EPCIP) iz leta 2005 prinaša pogled Komisije EU na način organiziranja za zaščito evropske kritične infrastrukture (EKI). Z njo so opredeljeni splošni cilj EPCIP kot zagotovitev zadostne stopnje zaščitnih ukrepov, povezanih s kritično infrastrukturo, zmanjšanje kritičnih točk in vzpostavitev obnovitvenih mehanizmov v EU. Poudarjeni so bili trije vidiki ogrožanja, in sicer pristop z upoštevanjem vseh groženj, pristop s poudarkom predvsem na terorizmu, in pristop, ki je upošteval predvsem teroristično grožnjo. Komisija se je v svojem sporočilu, ki je bilo objavljeno po Zeleni knjigi, zavzela za pristop, ki celovito upošteva vse grožnje. Med načeli EPCIP je določen tudi pristop, ki je usmerjen na posamezne sektorje. Glede na to, da imajo sektorji posebne izkušnje, strokovno znanje in zahteve, povezane z varovanjem kritične infrastrukture, se bo za vsak posamezen sektor oblikoval EPCIP, ki se bo uresničeval na podlagi dogovora. Pot do sprejema direktive je bila v okviru EU vsekakor zelo naporna.[6] Direktiva predstavlja začetek postopnega ugotavljanja in določanja evropske kritične infrastrukture ter uveljavljanja potrebe po izboljšanju njenega varovanja. Od prvotno načrtovanih 11 sektorjev je direktiva po kompromisni rešitvi omejena le na energetski in prometni sektor. Namen je, da se v prihodnje ovrednotita njen učinek in potreba po vključitvi drugih sektorjev. Prednost pri tem naj bi imel sektor informacijskih in komunikacijskih tehnologij (Žel, 2011). Republika Slovenija mora kot članica prenesti v svoj pravni red[7] Direktivo Sveta Evropske unije, št. 114/2008 z 8. decembra 2008, o ugotavljanju in določanju evropske kritične infrastrukture ter presoji potrebe za izboljšanje njene zaščite (v nadaljevanju direktiva). Direktiva določa postopek za ugotavljanje in določanje evropske kritične infrastrukture ter skupni pristop za presojo potrebe po izboljšanju zaščite takšne infrastrukture, da bi s tem prispevali k zaščiti ljudi. Obsega energetski ter prometni sektor, lahko pa se uporabi tudi za druge sektorje, v katerih se bo direktiva izvajala.

---

[6] *Ministri za notranje zadeve so zato na neuradnem sestanku v Luksemburgu leta 2008 podprli zamisel, da se namesto direktive oblikuje samo dokument predsedstva, ki bo predstavljal minimalni skupni imenovalec na tem področju. Maja 2008 je bila sprejeta odločitev, da se vendarle sprejme direktiva, ki pa ji je še vedno nasprotovala Švedska. Zaradi tako zelo različnih mnenj in pristopov ter ozaveščenosti držav na tem področju je bila leta 2008 oblikovana okrnjena direktiva, ki predstavlja začetek urejanja EKI.*

[7] *V 12. členu direktive je določeno, da države članice direktivo uveljavijo oziroma sprejmejo predpise, potrebne za njeno uveljavitev. Direktiva določa tudi rok, in sicer je bilo treba besedila predpisov držav članic in njihovo korelacijo z direktivo posredovati Komisiji Evropske unije najpozneje do 12. januarja 2011.*

Podobno potekajo dejavnosti na področju zaščite kritične infrastrukture tudi v Republiki Sloveniji. Problematiko te zaščite smo začeli proučevati predvsem po letu 2006, ko je bila ustanovljena posebna Medresorska koordinacijska skupina za usklajevanje priprav za zaščito kritične infrastrukture (v nadaljevanju medresorska koordinacijska skupina). Ta skupina je leta 2010 pripravila poseben program, ki je vključeval dejavnosti za uveljavitev direktive. Sestavni del programa je bila tudi opredelitev kritične infrastrukture državnega pomena, kar je ena izmed redkih usklajenih rešitev na tem področju. V medresorski koordinacijski skupini je bil pripravljen osnutek predpisa, ki naj bi zagotovil uveljavitev direktive, obenem pa urejal tudi zaščito kritične infrastrukture državnega pomena. Zaščita naj bi bila urejena zlasti v področnih predpisih.

Prvotni namen medresorske koordinacijske skupine je bil torej pripraviti in Vladi RS predlagati v sprejem predlog predpisa (zakona ali uredbe), ki bo povzel vsebino direktive v celoti, hkrati pa določil podlago za urejanje nacionalne kritične infrastrukture v področnih predpisih. Oblikovana je bila posebna podskupina za pripravo normativnopravnega akta za uveljavitev te direktive. V skupini so sodelovali predstavniki ministrstev za gospodarstvo, promet, za notranje zadeve, za visoko šolstvo, znanost in tehnologijo ter za obrambo, predstavniki Generalštaba Slovenske vojske ter Uprave Republike Slovenije za zaščito in reševanje. Skupina se je srečevala s podobnimi težavami kot EU. Dosežena je bila le uskladitev opredelitve kritične infrastrukture evropskega pomena, vsa preostala vprašanja, med katerimi je ustrezna opredelitev javno-zasebnega partnerstva, pa so ostala odprta in neusklajena.

Ministrstvo za obrambo[8], ki je odgovorno za uveljavitev direktive, se je zato odločilo, da se glede na to, da je rok za njeno uveljavitev v slovenski pravni red potekel že 12. januarja 2011, pripravi le Uredba o evropski kritični infrastrukturi. Dodatno je k taki odločitvi prispeval tudi uradni opomin Evropske komisije, ker nacionalni predpisi za prenos Direktive 2008/114/ES z dne 17. 3. 2011 niso bili notificirani. Pozneje je bila ustrezna uredba tudi sprejeta in tako prenesena v notranji pravni red Republike Slovenije.[9] Usklajevanje aktivnosti oziroma podlag in predpisa, ki naj bi uredil zaščito nacionalne kritične infrastrukture, pa bo potekalo posebej. Težava je predvsem pri določitvi ustreznih, razumnih in primernih meril kritičnosti, ki so ključna za oblikovanje predpisa o zaščiti nacionalne kritične infrastrukture.

3.2 Nato

V zadnjem strateškem konceptu (2010, str. 4), ki je bil sprejet novembra leta 2010 na vrhu v Lizboni, je Nato kibernetske grožnje prepoznal kot zelo resne, vse pogostejše, dobro organizirane in vse bolj uničujoče, ne glede na cilj napada (vladne, poslovne,

[8] *To, da Ministrstvo za obrambo vodi koordinacijsko skupino s področja zaščite kritične infrastrukture, je še ena izmed posebnosti Slovenije. V drugih državah je to naloga resorjev, ki se ukvarjajo z notranjimi zadevami, ali posebnih vladnih služb. To si lahko razložimo z dejstvom, da je bilo Ministrstvo za obrambo že prej zadolženo za usmerjanje civilne obrambe, v katero so zdaj vključili tudi kritično infrastrukturo. Drugo dejstvo pa je vsekakor v tem, da si nekateri resorji po spremenjenih razmerah v družbi iščejo novo mesto v sistemu upravljanja posameznih področij nacionalne varnosti.*

[9] *Uradni list RS, št. 35/11.*

ekonomske ali druge organizacije). Potencialno nevarnost vidi Nato v kritični infrastrukturi, če ne bi delovala, bi to lahko prizadelo nacionalne interese in interese zavezništva, blaginjo, varnost in stabilnost. Kot mogoče vire napadov vidi Nato obveščevalne službe, organizirani kriminal ter teroristične in ekstremistične skupine. Nato bo nove trende, povezane z najnovejšo tehnologijo, vključil v svoje procese načrtovanja in prihodnje operacije.

Skladno s strateškim konceptom (2010, str. 5) bo razvijal in uporabljal svoje zmogljivosti za preprečevanje številnih groženj varnosti svojih prebivalcev in obrambo pred njimi. Naštejmo le tiste, ki so povezane z informacijskimi grožnjami:
– sistemi za preprečevanje in zaznavo kibernetskih napadov ter obrambo pred njimi in okrevanje po njih, vključujoč procese načrtovanja za povečanje in usklajevanje nacionalnih zmogljivosti ter centralizirano zaščito, zavedanje, opozarjanje in odzivanje vseh članic;
– razvoj zmogljivosti za zaščito energetskih virov, vključujoč kritično infrastrukturo.

Nato kot legitimno in legalno pravico za zaščito svojih članic omogoča tudi uporabo 5. člena pogodbe[10]. V tem okviru se pojavljajo še nekatera vprašanja, saj je bil člen napisan in sprejet v času, ko informacijskih groženj še nismo poznali, zato v svojem obsegu definira le oborožen napad. Uporaba tega člena v odgovoru na kibernetski napad bi bila tako pravno vprašljiva, tudi če bi bila motiv in napadalec dokazana. Poleg tega se pojavlja tudi vprašanje, kako se ustrezno odzvati na napad. Pri kibernetskem napadu običajno pride do kraje, poneverbe ali izbrisa podatkov, neposredne fizične škode ali človeških žrtev pa ni. Je torej upravičena uporaba sile?

Uporabo 5. člena Severnoatlantske pogodbe zelo intenzivno zagovarja ameriška zunanja politika. Ta meni, da napadi ne bodo več prihajali iz zraka in topov, temveč po optičnih kablih, in da je na kibernetske napade treba odločno odgovoriti, še posebej, če bo tarča napadov kritična infrastruktura (Amies, 2010).

Bruce Schneier (2010) nasprotno meni, da je kibernetski kriminal postal vsakodnevna praksa in da na primer estonski dogodki[11] niso bili nič drugega kot dejanje etnično vznemirjenih ruskih hekerjev zoper protirusko politiko v Estoniji. Hekersko dejavnost sicer obsoja in razume kot resno grožnjo, a opozarja, da je ta v veliki večini delo otrok in objestnežev. Trdi, da je razvijanje ofenzivnih in defenzivnih kibernetskih zmogljivosti povsem legitimno, vendar pa je treba zelo paziti, da ne pride do zlorab. Pri tem izpostavlja ključna problema, kot sta dokazljiv motiv in identifikacija napadalca, ki ju je zelo težko ali celo nemogoče najti oziroma določiti. Kibernetsko vojno označuje za enako verjetno kot konvencionalno in pričakuje hkratno uporabo obeh oblik, če bi do vojne prišlo. Močno zagovarja stališče, da potrebujemo le

---

[10] 5. člen Severnoatlantske pogodbe v glavnem obsega zamisel, ki pravi, da bo oborožen napad na eno izmed članic razumljen kot napad na vse.

[11] Estonija je bila aprila 2007 tarča napadov, domnevno ruskih hekerjev, ki so z DDoS-napadi (DDoS -– denial-of-service je računalniški napad, izveden z velikim številom lažnih zahtev za dostop, ki onesposobijo ciljne računalnike) onemogočili vitalne strežnike in tako začasno skoraj povsem onesposobili delovanje estonskega bančnega sistema in vlade (Layden, 2007).

'mirnodobno' informacijsko varnost, ki temelji na sinergičnem učinku množice zasebnih in javnih organizacij, ki so nam danes že na voljo.

Prvi korak k postavitvi skupnih zmogljivosti za boj proti kibernetskim grožnjam je Nato naredil z ustanovitvijo centra odličnosti v Estoniji (Cooperative Cyber Defence Centre of Excellence – CCDCOE). Center, ki ni del poveljniške strukture Nata, je bil akreditiran 28. 10. 2008 v Talinu (Estonija) in ga financirajo države ustanoviteljice ter sponzorji. Center se ne ukvarja z informacijskimi incidenti, to je naloga NCIRC. Naloge CCDCOE so:
- krepiti in širiti ozaveščenost o informacijskih grožnjah med članicami Nata in partnericami, in sicer z organizacijo izobraževanj, raziskavami in razvojem ter zagotovitvijo informacij in podpore v procesu učenja iz izkušenj (Lessons Learned);
- podpirati Nato pri iskanju dobrih praks, tokov, konceptov in strategij ter pravne podlage za izvajanje operacij informacijskega bojevanja;
- na taktični ravni zagotavljati tehnične rešitve, varnost sistemov v taktičnih okoljih, prepoznavanje informacijskih groženj in napadov ter sanacijo po vdorih, nadzor sistemov, razvoj interoperabilnosti;
- zaščita kritičnih sistemov;
- razvoj metodologije ocene tveganja in varnosti;
- razvoj tehnik modeliranja in simulacij, povezanih z informacijskimi grožnjami (NATO Cooperative Cyber Defence Centre of Excellence, 2011).

3.3 Nacionalna raven

V nadaljevanju bomo prikazali in analizirali strateške dokumente in organe na nacionalni ravni, ki vsebujejo določila, povezana s prepoznavanjem in preprečevanjem pojava kibernetskih groženj in odzivanjem nanje oziroma so bila ustanovljena za ta namen.

Strategija nacionalne varnosti

Vlade nekaterih držav[12] so se po številnih dogodkih, povezanih z informacijskimi incidenti, začele zavedati naraščanja in resnosti teh pojavov. Republika Slovenija je v svoji Resoluciji o strategiji nacionalne varnosti (ReSNV-1), ki začela veljati marca 2010, med vire tveganja nacionalni varnosti uvrstila terorizem, nedovoljene dejavnosti na področju konvencionalnega orožja in orožja za množično uničevanje ter jedrske tehnologije, organizirani kriminal, nezakonite migracije ter seveda tudi kibernetske grožnje. V dokumentu je zapisano: »Zaradi razvejanosti informacijskih in komunikacijskih sistemov, neomejenosti kibernetskega prostora in težav pri nadzoru nad tem prostorom lahko tudi v Republiki Sloveniji pričakujemo širitev različnih oblik računalniške kriminalitete, zlasti kibernetskih vdorov ter napadov državnih in nedržavnih subjektov, ki jih prostorsko in časovno ne bo mogoče omejiti.« (ReSNV-1, 2010, str. 7) Resolucija prepoznava grožnje asimetrične narave kot vse

[12] *V britanski strategiji nacionalne varnosti (National Security Strategy – NSS), ki je bila izdana oktobra 2010, je britanski Svet za nacionalno varnost postavil kibernetske napade in kibernetski kriminal na visoko drugo mesto v prvi skupini tveganj (NSS, 2010, str. 27).*

bolj verjetne, k bojiščem prihodnosti pa poleg kopnega, morja in zraka prišteva tudi kibernetsko okolje. Kot odziv na kibernetske grožnje in zlorabo informacijskih tehnologij in sistemov je v dokumentu zapisano: »Republika Slovenija bo na področju kibernetske varnosti izdelala nacionalno strategijo za odzivanje na kibernetske grožnje in zlorabo informacijskih tehnologij ter sprejela potrebne ukrepe za zagotovitev učinkovite kibernetske obrambe, v katero bosta v največji možni meri vključena javni in zasebni sektor. Ena od prednostnih nalog na področju zagotavljanja kibernetske varnosti bo tudi ustanovitev nacionalnega koordinacijskega organa za kibernetsko varnost.« (ReSNV-1, 2010, str. 16) V teh strateških dokumentih pa manjkajo odgovori, kako v prihodnosti rešiti bistveno vprašanje javno-zasebnega partnerstva, ki je ključno za učinkovito preprečevanje kibernetskega ogrožanja informacijsko-komunikacijske kritične infrastrukture in odzivanje nanj.

Ločnica med javnim in zasebnim sektorjem v odnosu do odgovornosti na področju zaščite kritične infrastrukture se počasi, a vztrajno briše, tako da odgovornost ni le na posameznem segmentu, temveč je deljena. Nesporno je, da je večina kritične infrastrukture v zasebni lasti. To pomeni, da država sama ni več sposobna zagotavljati celovite varnosti te kritične infrastrukture in je močno odvisna od izmenjave informacij in skupnih ukrepov sodelujočih partnerjev. Dobro opredeljeno javno-zasebno partnerstvo je tisti dejavnik, ki je nujen za zagotovitev uspešne politike varovanja kritične infrastrukture. V tem okviru je nujna celovita vizija, ki bo zagotovila ustrezno strategijo in močno politično zavezanost za dosego želenega stanja. Taka vizija mora biti dosegljiva vsem lastnikom kritične infrastrukture. Vizijo, strategijo in ustrezno stopnjo zavedanja lahko opredelimo kot osnovni temelj za katero koli učinkovito politiko varovanja kritične infrastrukture. (Čaleta, 2011)

CERT[13]

CERT-i so danes osnovno orodje za zaščito kritične infrastrukture. Vse države, ki so priključene na internet, morajo imeti zmogljivosti za učinkovito odzivanje na računalniške incidente. Te zmogljivosti so primaren vir zaščite za državo in njene državljane (Porenta, 2011). V Sloveniji imamo SI-CERT (Slovenian Computer Emergency Response Team), katerega naloge so posredovanje pri internetnih incidentih, usklajevanje dela, obveščanje o varnostnih težavah v računalniških omrežjih v Sloveniji in njihovo reševanje. Je kontaktna točka, ki opravlja posredniško in svetovalno vlogo. Deluje znotraj Arnesa (Akademske in raziskovalne mreže Slovenije), vendar pa, kot nakazuje ime, sprejema le prijave varnostnih incidentov za vsa računalniška omrežja v Sloveniji. Arnes in Ministrstvo za javno upravo (MJU) sta na podlagi sklepa Vlade RS, št. 38600-3/2009/21 z dne 31. 5. 2009, podpisala sporazum o sodelovanju na področju informacijske varnosti. Sporazum določa, da bo Arnesov SI-CERT pomagal pri postavitvi vladnega centra, do takrat pa bo za vse informacijske sisteme javne uprave usklajeval odzive na varnostne incidente. Vladni center

[13] *Prvi CERT je bil ustanovljen leta 1988 v ZDA, ustanovitelj je bil ARPA (Advanced Research Projects Agency), in sicer kot odgovor na prvi večji internetni incident – širjenje prvega črva, pozneje imenovanega kar The Internet Worm. S širitvijo interneta so se začele podobne organizacije pojavljati tudi drugje po svetu (CERT-SI, 2011).*

CERT bo specializiran za omrežje in sisteme v javni upravi, medtem ko bo SI-CERT še naprej nacionalna kontaktna točka (Božič, 2011). CERT je organiziran tudi na MO, podlaga za njegovo delovanje je opredeljena v Navodilu o izvajanju ukrepov ob varnostnih dogodkih in incidentih v KiS MO (št. 007-70/2008-1 z dne 6. 3. 2008). Navodilo predpisuje organizacijske in tehnične ukrepe, s katerimi se zagotavlja odzivanje računalniške odzivne interventne skupine (RIOS – angl. CERT) na varnostne dogodke in incidente v KiS MO.

Zavedati se je namreč treba, da je področje, na katerega vpliva kibernetska varnost, izredno široko, kar se kaže tudi v obsegu zakonskih podlag, ki se posredno ali neposredno dotikajo obravnavanega področja. Tudi Republika Slovenija je zato sprejela zakonske predpise, ki se povezujejo s tem področjem, in sicer zakon o varstvu osebnih podatkov, zakon o dostopu do informacij javnega značaja, zakon o elektronskem poslovanju in elektronskem podpisu, zakon o elektronskih komunikacijah, zakon o tajnih podatkih, uredbo o upravnem poslovanju in druge.

4 ANALIZA STANJA NA OBRAMBNEM PODROČJU

Svet za informacijsko varnost

Svet za informacijsko varnost deluje na Ministrstvu za obrambo. Pomemben del njegovih nalog je trenutno usmerjen k vse večjim naporom Nata, da oblikuje koncept skupne kibernetske obrambe, pri čemer imajo vse članice, vključno z Republiko Slovenijo, enakovredno vlogo. Cilja zavezništva, ki izhajata iz Lizbonske deklaracije, sta nadgradnja komunikacijsko-informacijskih sistemov in doseganje polne zmogljivosti kibernetske obrambe do leta 2012. Vsaka članica mora postaviti aktivno zmogljivost CERT, se zavzemati za izboljšanje varnostne kulture, začeti centralno upravljanje omrežij in sistemov ter opredeliti in postaviti sistem varovanja kritične infrastrukture. Po mnenju večine držav članic je namreč pri oblikovanju koncepta ključni element kritična infrastruktura, ki postaja vse pogostejša tarča napadov z interneta. Nekatere članice so zaradi racionalnejše izkoriščenosti virov izpostavile pomembnost sodelovanja med EU in Natom ter sodelovanje nacionalnih CERT z NCIRC (NATO Computer Incident Response Capability). Članice Nata pri oblikovanju koncepta kibernetske obrambe usklajujejo tri področja, ki naj bi bila vključena v pristojnost usklajene Natove kibernetske obrambe:

1. vsa Natova omrežja, omrežja za podporo operacijam zavezništva in omrežja za podporo delovanju poveljstva in agencij;
2. vsa nacionalna komunikacijska omrežja, ki so ključna za Natove operacije;
3. vsa civilna omrežja članic, ki so ključna za delovanje nacionalne kritične infrastrukture.

Članice so pri obravnavi koncepta dosegle načelno soglasje na prvih dveh področjih, na tretjem pa še ne. Nekatere so namreč zadržane do vključitve tretjega področja v Natov koncept.

Svet za informacijsko varnost je konec aprila 2011 v MO imenoval delovno skupino za uskladitev stališč o kibernetski obrambi pred nacionalno obravnavo. Skupina trenutno, preden gredo predlogi na obravnavo na nacionalni ravni, pripravlja predlog aktivnosti MO pri pripravi in uveljavitvi koncepta kibernetske obrambe. Stališče je usmerjeno k nacionalnim in mednarodnim prizadevanjem, k nadgradnji komunikacijskih in informacijskih sistemov ter postavitvi učinkovite zmogljivosti kibernetske obrambe. Pri tem ministrstvo podpira aktivnosti Nata, EU in posameznih članic za oblikovanje kolektivne in nacionalnih zmogljivosti kibernetske obrambe. Pri oblikovanju koncepta in nacionalne strategije kibernetske obrambe sta medresorsko sodelovanje in sodelovanje v zavezništvu izrednega pomena. Dogovorjeno je bilo, da se smiselno uporabijo rešitve dobrih praks, že uveljavljenih v državah EU in Nata, ki se prilagodijo nacionalnim potrebam Slovenije. Ključno pri tem je varovanje nacionalne kritične infrastrukture, ki pa še ni opredeljena. Ministrstvo za obrambo bo aktivneje sodelovalo z NCIRC, ki zagotavlja zmogljivosti odzivanja na računalniške incidente.

4.1 Mednarodna primerjava na obrambnem področju

Pokazalo se je, da so mehanizmi tako mednarodne kot tudi nacionalne zakonodaje v boju proti globalni informacijski grožnji pogosto neučinkoviti. Razlogi za to bi lahko bili:
- ni celovitega in centraliziranega nadzora nad internetom ter komunikacijskimi in informacijskimi sistemi;
- vse države informacijskih groženj ne obravnavajo enako;
- identifikacija napadalcev je izredno zahtevna ali celo nemogoča;
- napadalčev motiv je težko dokazljiv ali celo nemogoč;
- nove tehnologije so vedno korak pred zakonodajo;
- zakonodaja posameznih držav zunaj njihovih meja nima vedno ustreznega učinka.

Zaenkrat še ni dosežen skupen dogovor o tem, kaj kibernetsko ogrožanje sploh je, kako ga prepoznati, dokazati in sankcionirati. V večini primerov se mednarodna skupnost zaveda resnosti problematike, a univerzalne in skupne rešitve še ni (Bosworth, Kabay, 2002, str. 7). Sledi pregled zmogljivosti za zoperstavljanje kibernetskim grožnjam izbranih držav, ki bo v nadaljevanju omogočil lažje razumevanje stanja in umeščenosti tega področja na obrambnem področju v Republiki Sloveniji. Podatki so pridobljeni iz javno dostopnih virov, ki pa se pri Rusiji in Kitajski med seboj razlikujejo in jih je zato treba upoštevati nekoliko z rezervo.

Ameriška vojska verjetno namenja največ virov, tako človeških kot tudi finančnih, za razvoj zmogljivosti na področju kibernetskega bojevanja. Spomladi leta 2010 je ameriški sekretar za obrambo Robert Gates oznanil začetek delovanja poveljstva posebne enote za računalniško bojevanje v sklopu zračnih sil (U. S. Cyber Command – CYBERCOM). Enota je postala polno operativna pol leta pozneje, poveljuje ji general s tremi zvezdicami Rhett A. Hernandez, kar zgovorno priča o njenem pomenu, štela pa bo kar 21.000 pripadnikov. Pripadnike rekrutirajo iz vrst računalniških strokovnjakov in hekerjev, za morebitne operacije pa se bodo, kot

zatrjujejo, pripravljali le najboljši. Američani veliko pozornosti namenjajo forenzičnim zmogljivostim, saj so mnenja, da je zelo pomemben predvsem pravni vidik. Napadalci bodo zelo verjetno na najrazličnejše načine poskušali zabrisati svoje sledi, zaradi česar jih je treba izslediti in identificirati. Prepričani so tudi, da kibernetska obramba sama po sebi ne deluje in da je treba poleg nje graditi tudi ofenzivne metode kot ključni element verodostojne obrambe. (Miles, 2011)

Nemška zvezna vojska je ustanovila posebno enoto, v kateri bodo delovali tako imenovani *hekerji v uniformah*. Trenutno se enota imenuje Oddelek za operacije na področju informatike in računalniških mrež (Abteilung Informations- und Computernetzwerkoperationen), njihova naloga je uriti se v obrambi in protinapadu proti kibernetskim grožnjam. Zvezna vlada je hkrati nemški Zvezni urad za varnost informacijske tehnologije (Bundesamtes für Sicherheit in der Informationstechnik – BSI) dvignila v agencijo za *kiberobrambo*, s čimer je agenciji na voljo več finančnih in kadrovskih virov ter pooblastil (Mann, 2009).

Rusija je v svojem konceptu nacionalne varnosti iz leta 2000 zaradi povečanega razvoja konceptov kibernetskega vojskovanja drugih držav prepoznala kibernetske grožnje kot grožnje svoji nacionalni varnosti. V dokumentu navaja, da bo kibernetski napad ZDA razumela kot vojaško grožnjo in bo nanj odločno odgovorila, pri čemer si jemlje pravico uporabe jedrskega orožja. Znana ruska univerza Tomsk slovi po tem, da izobražuje vrhunske strokovnjake za kibernetsko bojevanje, žal pa nekateri med njimi svoje znanje ponujajo tudi na hekerskem trgu. Iz Rusije izhaja znano *botnet omrežje Storm*, ki ga je sestavljalo ogromno število računalnikov nič hudega slutečih uporabnikov interneta po vsem svetu. Zlonamerna programska koda, s katero so bili okuženi ti računalniki, sama po sebi ni škodljiva, a na računalnikih čaka na ukaze tistih, ki to mrežo upravljajo (CDCOE, 2010).

Tudi Kitajska uspešno sledi težnjam v svetu in domneva se, da tako kot druge velike sile sama razvija zmogljivosti, podprte z informacijsko tehnologijo. V proces modernizacije in informatizacije kitajske vojske je vključeno tudi usposabljanje vojakov za kibernetsko bojevanje, ki poteka v sodobnih računalniških laboratorijih. Temu razvoju se pridružujejo tudi univerze s proučevanjem kibernetske obrambe in napadov, hekerskih metod ter zlonamerne kode. Posebno pozornost Kitajska namenja *kibernetskemu izvidovanju* ali prisluškovanju internetnemu prometu. Znan je primer, kako je Kitajska uspešno izrabila ranljivost internetnega protokola BGP in za 15 minut preusmerila 18 odstotkov svetovnega internetnega prometa na svoje usmerjevalnike. Kitajci so pred tem objavili, da so uspeli izdelati najbolj zmogljiv računalnik na svetu. S takim strojem bi teoretično lahko analizirali tudi internetni promet, a povezava teh dveh dogodkov ni dokazana (Fritz, 2008). Kitajska doktrina namenja asimetrični obliki delovanja veliko pozornosti. Kitajska je država z največjim številom prebivalstva in ogromnim ozemljem, postopoma pa postaja svetovna velesila tudi v ekonomskem smislu. Pri tem si pomaga z razvojem zmogljivosti ofenzivnega kibernetskega delovanja in izvidovanja, s katerim pridobiva različne obveščevalne podatke in tako krepi ekonomsko in vojaško moč. Številne sledi kibernetskih napadov, med

zadnjimi izredno odmeven napad na strežnike Googla, vodijo na Kitajsko, kar je dober dokaz za to, kako tehnološko razvita je ta dežela danes in kako uspešno sledi razvoju v svetu (Fritz, 2008). Kitajske oblasti medtem priznavajo le, da so izurile enoto, imenovano Modra armada, ki jo sestavlja 30 najboljših računalniških strokovnjakov iz vojaških vrst, z univerz in iz drugega civilnega okolja. Usposobljeni naj bi bili izključno za defenzivno delovanje, za mnoge vlade po svetu pa je novica le potrditev njihovega strahu, da so računalniški sistemi resnično lahko kadar koli tarča kitajskih napadov (McConor, 2011).

4.2 Obrambni sistem Republike Slovenije

V svojih strateških dokumentih (ReSNV-1) je Republika Slovenija med viri tveganja za nacionalno varnost prepoznala tudi kibernetske grožnje in se obvezala, da bo pripravila nacionalno strategijo za odzivanje na te grožnje. V ukrepe za zagotovitev učinkovite kibernetske obrambe bo čim več vključila tudi javni in zasebni sektor, ena izmed prednostnih nalog na področju zagotavljanja kibernetske varnosti pa bo ustanovitev nacionalnega koordinacijskega organa za kibernetsko varnost. Slovenija je v svojem strateškem dokumentu Resolucija o splošnem dolgoročnem programu opremljanja in razvoja Slovenske vojske do leta 2025 (ReSDPRO 2025), ki je bil sprejet novembra 2010, spoznala, da bo bojišče prihodnosti poleg kopnega, morja in zraka obsegalo tudi kibernetski prostor in vesolje. Posebno pozornost bo Slovenska vojska namenila razvoju (med drugimi zmogljivostmi) zmogljivosti računalniških in komunikacijskih sistemov za zaščito pred kibernetskimi napadi. Kot multiplikatorje bojne moči bo med drugimi razvila tudi zmogljivosti kibernetskega bojevanja. Uvedena bo varna in prilagodljiva komunikacijska in informacijska omrežna infrastruktura, skladna z zahtevami Natovih zmogljivosti omrežnega delovanja. Uvedeni bodo ukrepi in zmogljivosti za informacijsko varnost, namenjeni preprečevanju nenadzorovanega dostopa in vključevanja v omrežje (povzeto po ReSDPRO, 2010).

Slovenska vojska se je v dokumentu (ReSDPRO 2025) obvezala, da bo v prihodnje posebno pozornost namenila razvoju zmogljivosti računalniških in komunikacijskih sistemov za zaščito pred kibernetskimi napadi ter kot multiplikatorje bojne moči med drugimi razvila tudi zmogljivosti kibernetskega bojevanja. V osnutku srednjeročnega obrambnega programa (SOPR 2011–2016), ki je trenutno še v vladni obravnavi, pa je zapisano le, da se bodo ukrepi kibernetske obrambe v Slovenski vojski izvajali skladno z zavezniki in nacionalno strategijo (SOPR, 2011, str. 9), ki pa je Republika Slovenija še nima.

Skladno z dokumenti Evropske unije, evropskega programa za zaščito kritične infrastrukture, je bilo na nacionalni ravni in tudi na MO sprejetih kar nekaj pravnih aktov. MO je ustanovil svoj RIOS (angl. CERT), ki pa še ni zaživel. Delovna skupina s člani z MO, iz SV ter še z nekaterih drugih ministrstev, v sodelovanju s SI-CERT, ki trenutno sicer predstavlja nacionalno kontaktno točko, a ima le posredniško in svetovalno vlogo, sodeluje pri postavitvi vladnega CERT.

Po estonskih napadih se je na informacijske grožnje začel resneje odzivati tudi Nato. Ustanovil je center odličnosti v Estoniji, v katerem razvija zmogljivosti, ki so in bodo v podporo skupnim naporom za boj proti kibernetskim grožnjam. V zadnjem času zavezništvo intenzivno oblikuje skupen koncept kibernetske obrambe. Članice so pri obravnavi dokumenta dosegle načelno soglasje na prvih dveh področjih, na tretjem pa še ne, saj so nekatere zadržane do vključitve svoje kritične infrastrukture v pristojnost usklajene Natove kibernetske obrambe. Slovenija je ustanovila delovno skupino za pripravo nacionalne strategije kibernetske obrambe, pri čemer bo kot izhodišče uporabila primere dobre prakse. Slovenska vojska je v pripravi nacionalne strategije in koncepta kibernetske obrambe z dvema posameznikoma zgolj prisotna v delovni skupini. Virov za razvoj svojih zmogljivosti pa zaenkrat nima.

Zaradi pomembnih novosti, kot so vključevanje nacionalne kritične infrastrukture v Natov koncept ter izdelava nacionalne strategije kibernetske obrambe in koncepta, bi bilo nujno čim prej ustanoviti nacionalni koordinacijski organ za kibernetsko varnost, k čemur se je Slovenija v Resoluciji o strategiji nacionalne varnosti tudi obvezala. Poleg dejstva, da mora Slovenija prispevati svoj delež k zavezništvu, moramo namreč zaščititi predvsem nacionalni interes, to je zavarovati suverenost in avtonomnost svoje kritične infrastrukture. Ker gre v tem primeru tako za politične kot za strokovne odločitve, bi moral biti po najinem mnenju nacionalni koordinacijski organ sestavljen iz skupine strokovnjakov javnega in zasebnega sektorja ter univerz. Usklajeval bi nacionalne aktivnosti in aktivnosti zavezništva ter EU. Uresničeval bi jih lahko po načelih dobre prakse na estonskem primeru in po zgledu agencij iz drugih večjih držav, na primer Nemčije (Bundesamtes für Sicherheit in der Informationstechnik – BSI). Ključna pri tem bi bila dovolj visoka pooblastila, saj je kritična infrastruktura v domeni več različnih ministrstev. Nacionalni koordinacijski organ za kibernetsko varnost bi zato lahko bil umeščen v organizacijsko strukturo Sveta za nacionalno varnost (SNAV), katerega glavne aktivnosti so povezane z zagotavljanjem nacionalne varnosti.

Slovenska vojska bi v procesih za zagotavljanje kibernetske varnosti morala aktivneje sodelovati, in sicer s predstavniki v nacionalnem koordinacijskem organu in z razvojem svojih zmogljivosti ter znanja, upoštevaje kadrovske razmere, v katerih se je znašla. K uvedbi svojih zmogljivosti kibernetskega bojevanja se je obvezala v ReSDPRO 2025. Razvoj teh zmogljivosti je nujen zaradi tajnih podatkov, ki jih je treba zaščititi, posebne narave dela in množice komunikacijsko-informacijskih sistemov, ki jih ima. Vojska bi po zgledu nekaterih razvitejših vojsk morala sama čim bolj zagotoviti suverenost nad svojimi KiS tudi zato, da bi uveljavila neprekinjen proces poveljevanja in kontrole (PINK). Svoje znanje in veščine bi preverjala z udeležbo na mednarodnih kibernetskih vajah, ki so v zadnjem času vse pogostejše. Omenimo le vsakoletno Natovo vajo kibernetske obrambe in vajo, ki jo letos prvič organizira tudi Evropska agencija za informacijsko in omrežno varnost (European Network and Information Security Agency – ENISA). Pomemben kazalnik intenzivnega odzivanja na kibernetske grožnje je tudi dejstvo, da je Slovenska vojska na vaji Pomlad 2011 v scenarij prvič vključila tudi incidente, povezane s kibernetskimi grožnjami.

Sklep

Morebitni napad iz kibernetskega prostora ni več vprašanje, zanima nas samo, kdaj in kako se bo zgodil, kako smo nanj pripravljeni in kako poguben bo. Da je res tako, pričajo številni zaznani primeri iz bližnje preteklosti, nihče ne ve, koliko jih je ostalo tudi skritih. Dejstvo je, da so ti pojavi vedno pogostejši, bolje organizirani in bolj uničujoči. Že na prvi pogled lahko ugotovimo, da bi uresničitev kibernetskih groženj lahko imela hude posledice, paralizirano bi bilo delovanje ključnih sistemov za normalno delovanje družbe, v najslabšem primeru pa bi povzročila tudi negativne ekonomske učinke ali celo smrtne žrtve.

Sredstva, s katerimi bi morebitni napadalci uresničili svoje grožnje, so nam dobro poznana, pa tudi tehnike in metode uporabe. Vseeno pa dovolj zanesljivega sistema obrambe in zaščite še nimamo. Trenutno vsaka država to rešuje po svoje, v večini primerov so organizirani centri CERT, ki se poskušajo spopadati z izzivi kibernetskih napadov, združujejo se tudi med seboj. Nekatere države, kot so ZDA, Velika Britanija, Nemčija in druge, so kibernetske grožnje v svoje strategije nacionalne varnosti postavile na visoko mesto. Imajo tudi nacionalne centre in agencije, ki usklajujejo dejavnosti na nacionalni ravni, vojske teh držav pa intenzivno uvajajo zmogljivosti, s katerimi se bodo poskušale čim bolj učinkovito spopadati s kibernetskimi izzivi. Zaznati je tudi močno zavedanje pomena povezovanja tako različnih nacionalnih ustanov kot tudi pomena povezovanja in sodelovanja med državami, predvsem na ravni EU in Nata. Slovenska vojska zaradi majhnega števila pripadnikov zmogljivosti za zoperstavljanje kibernetskim grožnjam, kakršne imajo velike države, nima, kljub temu pa poskuša slediti tokovom v svetu. To dosega z izobraževanjem strokovnjakov doma in v tujini ter s povezovanjem s civilnimi ustanovami in univerzami pri razvoju in izobraževanju. Slovenija kot članica Nata aktivno sodeluje pri oblikovanju skupne zavezniške strategije kibernetske obrambe. Pravna podlaga za razvoj zmogljivosti za boj proti kibernetskim grožnjam je v RS opredeljena v doktrinarnih dokumentih na nacionalni ravni (ReSNV-1) in na ravni MO (ReSDPRO 2025). Trenutno potekajo aktivnosti za oblikovanje koncepta kibernetske obrambe in nacionalne strategije, pri katerih ima ključno vlogo zaščita nacionalne kritične infrastrukture, ki pa še ni v celoti opredeljena niti medresorsko usklajena. Sklenjeno je bilo, naj se pri oblikovanju uporabijo načela dobre prakse in podpirajo aktivnosti Nata, EU in posameznih članic. Pomembno je tudi sodelovanje z javnim in zasebnim sektorjem ter izobraževalnimi ustanovami.

Slovenska vojska trenutno nima kadrovskih virov niti koncepta za postavitev zmogljivosti kibernetskega vojskovanja, za kar se je v svojih dokumentih obvezala. Z večino aktivnosti se trenutno ukvarja upravni del MO, Slovenska vojska pa pri tem le delno sodeluje. Zoperstavljanje kibernetskim grožnjam tako trenutno poteka le z ukrepi zaščite in varovanja KiS. Vojskovanje v kibernetskem prostoru je danes dejstvo, ki je z nacionalnovarnostnega vidika za prihodnost bistveno večjega pomena, kot se nam morda v tem trenutku zdi. Slovenska vojska bi morala kibernetsko vojskovanje razumeti kot sestavni del svojega vojskovanja in temu primerno tudi pravočasno načrtovati svoje vire.

Literatura

1. *Amies, F., 2010. NATO includes threat of cyber attack in new strategic concept document, http://www.dw-world.de/dw/article/0,,6072197,00.html (6. 6. 2011).*
2. *Bosworth, Seymour; Kabay, M. E., 2002. Computer Security Handbook. New York: John Wiley & sons, INC.*
3. *Božič, G., 2011. How strong is your cloud?. Zbornik mednarodne konference »Kaj nam prinaša računalništvo v oblaku?«, Armes, Kranjska gora, str.10–12.*
4. *Schneier, B., 2010. It Will Soon Be Too Late to Stop the Cyberwars, http://www.schneier.com/essay-334.html (12. 12. 2010).*
5. *Chakrabarti, A., in Manimaran, G., 2003. A Case for Tree Migration and Integrated Tree Maintenance in QoS Multicasting. Dostopno na http://www.arnetminer.org/dev.do?m=downloadpdf&url=http://arnetminer.org/pdf/PDFFiles2/--d---d-1253857098812/A Case for Tree Migration and Integrated Tree Maintenance in QoS Multicasting1253872172718.pdf (22. 4. 2011).*
6. *Cooperative Cyber Defence Centre of Excellence Tallinn, Estonia, http://www.ccdcoe.org/11.html (14. 12. 2010).*
7. *Čaleta, D., 2011. A comprehensive approach to the management of risks related to the protection of critical infrastructure: public-private partnership. Caleta, D., Shemella, P. (Ed.) Counter-Terrorism Challenges Regarding the Processes of Critical Infrastructure Protection. Institute for Corporative Security Studies and Centre for Civil Military Relations, Ljubljana.*
8. *De Kerchove, G., 2010. Eu Counter terrorism strategy – Discussion paper. Counil of the European Union, number 158941/10 (rev. 1) z dne 29. 11. 2010.*
9. *Direktiva sveta (ES) o ugotavljanju in določanju evropske kritične infrastrukture ter o oceni potrebe za izboljšanje njene zaščite, št. 114/2008 z dne 8. decembra 2008.*
10. *Dunn, M., Wigert, I, A., 2006. International Critical Information Infrastructure Protection (CIIP) Handbook.*
11. *Frtiz, J., 2008. How China will use cyber warfare to leapfrog in military competitiveness. Culture Mandala, Vol. 8, No. 1, October 2008, pp.28-80, http://www.international-relations.com/CM8-1/Cyberwar.pdf (12. 5. 2011).*
12. *Kjaerland, M., 2005. A classification of computer security incidents based on reported attack data, Journal of Investigative Psychology and Offender Profiling, Volume 2, Issue 2, str. 105–120.*
13. *Ko., C., 2008. Network World Canada, 4. jul. 2008, Vol. 24, Issue 13.*
14. *Kumar, S., in Spafford, E., 1994. An application of Pattern Matching in Intrusion Detection, Tecnical Report. West Lafayette: Purdue University.*
15. *Leyden, J., 2007. Estonia has faced down Russian rioters, http://www.economist.com/node/9163598 (dne 30. 08. 2011).*
16. *Lukman, M., Bernik, I., 2009. Ogrožanja kritične infrastrukture iz kibernetskega prostora. 10. Slovenski dnevi Varstvoslovja, Zbornik prispevkov, FVV, Ljubljana, 4–5. junij 2011.*
17. *Mann, U., 2009. Spionage - und Hackerabwehr Bundeswehr baut geheime Cyberwar-Truppe, http://www.spiegel.de/netzwelt/tech/0,1518,606096,00.html (12. 6. 2011).*
18. *Miles, J., 2011. Army Cyber Command Focuses on Protecting Vital Networks. http://www.defense.gov/news/newsarticle.aspx?id=65031 (dne 30. 8. 2011).*
19. *McConor, J., 2011. China's Blue Army of 30 computer experts could deploy cyber warfare on foreign powers, http://www.theaustralian.com.au/australian-it/chinas-blue-army-could-conduct-cyber-warfare-on-foreign-powers/story-e6frgakx-1226064132826 (30. 8. 2011).*
20. *Politt, M. M., 1997. Cyberterrorism – Fact or Fancy? FBI Laboratory, Washington D. C., dostopno: http://www.cs.georgetown.edu/~denning/infosec/pollitt.html (9. 10. 2006).*
21. *Panagiotis, T. (Ed.), 2011. Inter X: Resilience of the Internet Interconnection Ecosystem Summary Report – April 2011 http://www.enisa.europa.eu/act/cert (30. 8. 2011).*

22. *Porenta, J., 2011. Cloud computing at Arnes. Zbornik mednarodne konference »Kaj nam prinaša računalništvo v oblaku?«, Armes, Kranjska Gora, str. 7–9.*
23. *Resolucija o splošnem dolgoročnem programu opremljanja in razvoja slovenske vojske do leta 2025 (ReSDPRO 2025), 23. 11. 2010, številka 200-03/10-29/15.*
24. *Resolucija o strategiji nacionalne varnosti Republike Slovenije, št. 200-01/10-5/22, Ljubljana 2010.*
25. *SI CERT, http://www.cert.si/varnostne-groznje.html (3. 11. 2010).*
26. *Srednjeročni obrambni program 2011–2016 (osnutek), Generalštab Slovenske vojske 2011.*
27. *Strategic Concept For the Defence and Security of The Members of the North Atlantic Treaty Organisation, 2010. Konferenca NATA v Lizboni.*
28. *Svete, U., 2006. Nacionalnovarnostni vidiki ogrožanja informacijske infrastrukture. V: PREZELJ, Iztok (ur.). Ogrožanje nacionalne varnosti, Varstvoslovje, Letn. 8, št. 1. Ljubljana: Univerza v Mariboru, Fakulteta za policijsko-varnostne vede, 2006, str. 31–44, graf. prikazi.*
29. *Svete, U., 2007. Informacijske razsežnosti sodobnega terorizma-teoretična vprašanja in praktični vidiki. UJMA, št. 21/2007, str. 124–129.*
30. *Svete, U., 2010. Informacijska in komunikacijska kritična infrastruktura. V: PREZELJ, Iztok (ur.). Kritična infrastruktura v Sloveniji, Knjižna zbirka Varnostne študije. Ljubljana: Fakulteta za družbene vede, 2010, str. 43–63.*
31. *Tun, Z., Aung, H., M., 2008. Wormhole Attack Detection in Wireless Sensor Networks, Proceedings of world academy of science, engineering and technology, Volume 36, december 2008, http://www.waset.org/pwaset/v36/v36-94.pdf, (21. 2. 2011).*
32. *Uredba o evropski kritični infrastrukturi, Uradni list RS, št. 35/01 z dne 13. maja 2011.*
33. *Weimann, G., 2006. Terror on the Internet - The New Arena, The New Challenges. Washington D.C.: United States Institute of Peace Press.*
34. *Žel, R., 2011. Obrazložitev k predlogu za sprejem Uredbe o evropski kritični infrastrukturi. DOZ, MO RS, 10. 2. 2011.*