Damjan Štrucl

Kibernetska varnost v Republiki Sloveniji in Slovenski vojski

Cyber Security in the Republic of Slovenia and the Slovenian Armed Forces

Povzetek

Kibernetska varnost je termin, ki se v današnjem času uporablja vse pogosteje, vendar je v Sloveniji na to temo napisano zelo malo, poleg tega je veliko različnih definicij terminov s tega področja. V sprejeti Strategiji kibernetske varnosti Republike Slovenije in novem Srednjeročnem obrambnem programu Republike Slovenije 2016–2020 so opredeljeni cilji, s katerimi bi vzpostavili celovit sistem kibernetske varnosti, ki bo usklajen s cilji zavezništva in mednarodnimi dokumenti. Celovit sistem kibernetske varnosti mora biti vzpostavljen na več ravneh organiziranosti, imeti mora usposobljen kader (tudi pravno področje) ter ustrezen način izobraževanja in usposabljanja, ustrezno komunikacijsko in informacijsko tehnologijo ter osrednje usklajevalno telo. V Slovenski vojski imamo v strateških dokumentih opredeljenih precej zahtevnih nalog, od ozaveščanja do vzpostavitve premičnih operativnih zmogljivosti za zagotavljanje kibernetske varnosti, nimamo pa ustreznega normativno in kadrovsko urejenega sistema. Prav zato želimo vzpostaviti učinkovit sistem kibernetske varnosti, ki bo primerljiv z Natom in Evropsko unijo.

Ključne besede: *kibernetska varnost, Slovenska vojska, izobraževanje in usposabljanje, kader, zakonodaja.*

Abstract

Cyber security is a term that is increasingly used nowadays, but until 2015 very little had been written on this topic in the Republic of Slovenia, and there are many different definitions of terms in this field. The Cyber Security Strategy of the Republic of Slovenia and the new Medium-Term Defence Programme

of Slovenia 2016-2020 have identified goals with the intention of establishing a comprehensive system of cyber security that is consistent with the objectives of the Alliance and international agreements. This comprehensive system of cyber security must be in place at several levels of organization, which requires adequate staffing (including legal knowledge), an appropriate means of education and training, relevant communication and information technology, and a central coordinating body. The strategic documents of the Slovenian Armed Forces have fairly complex tasks, from raising awareness to the creation of mobile operational capacity to ensure cyber security; however, we do not have the appropriate normative system and human recourses management. Because of this we want to establish an effective system of cyber security, which will be comparable with the NATO Alliance and the EU.

Key words: *cyber security, Slovenian Armed Forces, education and training, personnel, legislation.*

1 Uvod

Globalizacija in razvoj informacijsko-komunikacijskih tehnologij (IKT), ki omogočajo povezovanje ter skoraj neskončno hitro izmenjavo informacij ne glede na kraj in čas, sta sprostila zelo velik človeški ustvarjalni potencial. Posledica ni le razvoj novih tehničnih rešitev in tehnologij, temveč tudi sprememba starih ter pojav povsem novih družbenih odnosov. To prinaša negotovosti in grožnje, pred katerimi ni varna nobena država, ustanova ali vojska.

Z razvojem tehnologije se je proces prenosa in obdelave informacije bistveno spremenil. Če so bili nekoč le svetlobni in zvočni signali, torej vidni in slišni, ter fizični prenos informacij s kurirji, se danes informacije večinoma prenašajo z električnimi signali in elektromagnetnim valovanjem. S prehodom s predvsem analognega zapisa signalov na digitalni zapis in z razvojem zmogljivih računalnikov, spominskih medijev ter komunikacijskih poti z visoko prepustnostjo podatkov, ki omogočajo povezovanje včasih ločenih računalniških tokov v svetovni splet, je postal pomen informacij in povezanih informacijskih sistemov tako velik, da smo ga začeli dojemati kot poseben prostor. Imenujemo ga kibernetski prostor.

Informacije so imele v zgodovini vedno velik pomen, zdi pa se, da še nikoli tako velikega kot danes, ko smo priča nenehni prikriti in tudi odkriti vojni

za obvladovanje informacij in zagotavljanje informacijske prednosti lokalno ter globalno na gospodarskem, političnem in vojaškem področju in tudi na drugih. Pomen obvladovanja informacij je postal na vojaškem področju odločilen, saj je uspeh vojaških sil v vojaških akcijah zelo odvisen od zagotovitve informacijske prednosti (Berkowitz, 2010).

Nove okoliščine, ko se je vojaško delovanje z zemlje, iz vode, zraka in vesolja razširilo v peto dimenzijo, torej kibernetski prostor, postavljajo nove izzive tudi pred Slovensko vojsko. Zaradi narave kibernetskega prostora, v katerem so nacionalne meje zabrisane in geografska lega drugotnega pomena, kjer je pogosto težko ločiti med vojaškim in civilnim okoljem in kjer virtualni kibernetski prostor povezuje fizične prostore, je naloga še posebno zahtevna. Posebno okoliščino pomeni dejstvo, da je kibernetski prostor ustvaril človek in da je to dinamičen prostor, ki se zelo hitro širi ter spreminja.

Za uporabo in prilagajanje tehnično ter družbeno tako kompleksnega in dinamičnega sistema je treba imeti ustrezno tehnologijo, predvsem pa znanje. Znanje je mogoče pridobiti le z načrtnim izobraževanjem in usposabljanjem, namenjenim ozaveščanju posameznikov o nevarnostnih kibernetskega prostora in pravilni uporabi IKT ter izobraževanju tehničnih specialistov in vodij oziroma odločevalcev. Ti morajo prepoznati pasti in zmogljivosti kibernetskega prostora ter jih med pripravo, izvajanjem in ob koncu operacije znati obrniti v korist lastnih sil.

1.1 Metodološki okvir

V članku je predstavljeno stanje kibernetske varnosti v Republiki Sloveniji, s poudarkom na SV, na njegovo urejenost pa vplivata tako politika EU in Nata s področja kibernetske varnosti kot tudi mednarodno vojno pravo. Pri pripravi članka sem izhajal iz dveh omejitev:

- napisan je na podlagi javno dostopne literature in virov;
- analiza zaradi občutljivosti podatkov ne posega v podrobnosti opremljenosti Slovenske vojske in njenega opravljanja nalog s področja kibernetske varnosti.

Cilja članka v teoretičnem delu sta predvsem pregledati trenutne dokumente s področja kibernetske varnosti Slovenske vojske in iz trenutnih dokumentov Nata opredeliti potrebe po oblikovanju zmogljivosti kibernetske varnosti v

SV v njenem najpomembnejšem delu, torej funkcionalnem usposabljanju. Empirični cilj je na taktični, operativni in strateški ravni opredeliti sistem funkcionalnega usposabljanja, da bi ozaveščali uporabnike IKT.

Pri pripravi članka sem izhajal iz dejstva, da je kibernetski prostor umeten prostor, ki ga je ustvaril človek, hkrati pa ga človek tudi vzdržuje in spreminja. Prav zaradi dejstva, da je človek »osnovni« element kibernetskega prostora, ga je treba ustrezno motivirati in namensko izobraževati. Zagotovitev visoke ravni kibernetske varnosti je odvisna od vzpostavitve celovitega sistema izobraževanja in usposabljanja, ki bo imel dvojno vlogo kot pospeševalec ozaveščanja pomena kibernetske varnosti in razvijalec ustreznega kadra, sposobnega za učinkovito opravljanje te dejavnosti.

2 Razvoj področja kibernetske varnosti

Področje, ki ga danes vsesplošno opredeljujemo s predpono kiber- (*cyber*), se je začelo razvijati z začetkom človekovega razumevanja in uporabo električnih ter magnetnih pojavov v začetku 19. stoletja. Svoje trdne temelje je dobilo, ko je škotski matematik in fizik James Clark Maxwell med letoma 1864 in 1873 združil ter dopolnil tedanje eksperimentalno in teoretično znanje v sistem parcialnih diferencialnih enačb prvega reda (Fitzpatrick, 2008), ki so danes splošno znane kot Maxwellove enačbe. Dogodki, ki se navezujejo na kibernetsko varnost, so se začeli dogajati precej pred tem, ko so jih poimenovali kibernetski, zato je prav, da najprej določimo njihov pomen.

2.1 Definiranje pojmov

Pojmi informacijska varnost (INFOSEC), kibernetska varnost (CYBERSEC) in kibernetska obramba (KIBO) se pogosto uporabljajo, ne da bi določili njihov pomen. Tudi če so definirani, v svetu še ni poenotene definicije. V različnih okoljih so definirani različno in definicije se spreminjajo tudi s časom (Klimburg, 2012: 9). Pri definiranju pojmov bom sledil priporočilu, da so natančne definicije manj pomembne kot opis in jasnost pomena (Klimburg, 2012: 196), zato v tem delu ne bom uporabil zahtevne definicije CYBERSEC iz Strategije KVRS ali mnenja Sekcije za terminološke slovarje pri SAZU, ki povzemata definicijo Mednarodne telekomunikacijske zveze.

Za definiranje kibernetskega prostora sledim Schmittu (2013, 211).

KIBERNETSKI PROSTOR SESTAVLJAJO FIZIČNE IN NEFIZIČNE KOMPONENTE, ZA KATERE JE ZNAČILNA UPORABA RAČUNALNIKOV TER ELEKTROMAGNETNEGA SPEKTRA ZA SHRANJEVANJE, SPREMINJANJE IN IZMENJAVO PODATKOV Z RAČUNALNIŠKIMI MREŽAMI.

Podobno kibernetski prostor definirata tudi Nacionalni inštitut za standardizacijo in tehnologijo ZDA (Kissel, 2013) in Odbor za sisteme nacionalne varnosti (CNSS, 2015), ki deluje v okviru Nacionalne varnostne agencije (NSA) v ZDA z razširitvijo, da je kibernetski prostor več kot le internet ter ne vključuje le strojne in programske opreme in podatkov, temveč tudi ljudi, ki so v interakciji z informacijskimi sistemi (Klimburg, 2012: 8).

Za definiranje pojma CYBERSEC[50] uporabim že definiran pojem kibernetskega prostora in sledim Slovarju kibernetske varnosti Policijske akademije v Pragi (Jirásek in drugi, 2013).

KIBERNETSKA VARNOST JE:

- ZBIRKA PRAVNIH, ORGANIZACIJSKIH, TEHNOLOŠKIH IN IZOBRAŽEVALNIH SREDSTEV, NAMENJENA VAROVANJU KIBERNETSKEGA PROSTORA (ZAGOTAVLJANJE VARNOSTI);
- STANJE KIBERNETSKEGA PROSTORA Z VIDIKA VARNOSTI.

Opredelimo še odnos med CYBERSEC in KIBO. Izraz KIBO se pogosto uporablja v vojaških sistemih (Klimburg, 2012: 12), primerjava med definicijama CYBERSEC in KIBO (CCDCOE, 2016, in Klimburg, 2012: 13) pa pokaže, da med njima ni bistvenih razlik in da ju lahko uporabljamo kot sopomenki.

2.2 Oblike kibernetskih groženj in kibernetskega bojevanja

Kibernetske grožnje ne izbirajo deležnikov v kibernetskem prostoru, zato so tudi za vse deležnike izzivi v kibernetskem prostoru enaki. V članku CDSE (2016) se oblike kibernetskih groženj na splošno delijo na:

[50] INFOSEC se deloma prekriva s CYBERSEC, nikakor pa ju ne moremo primerjati v smislu vsebovanosti ali podrejenosti druge drugi. INFOSEC se v nasprotju s CYBERSEC, ki se omejuje na kibernetski prostor, ni pa omejena le na varovanje podatkov. Večinoma se omejuje na varovanje podatkov z vidika tajnosti, celovitosti in razpoložljivosti, ni pa omejena glede na obliko podatkov. Ti so lahko v papirni, elektronski ali kakršni koli drugi obliki.

- ribarjenje (angl. Phishing), ki omogoča prevzemanje uporabniških imen in gesel do različnih spletnih storitev, podatkovnih baz in podobnega;
- zlonamerne kode (angl. Malicious Code), ki onemogočijo delovanje informacijskega sistema, samodejno pošiljajo podatke, spremenijo in pobrišejo podatke in podobno;
- gesla, ki nam omogočajo dostop do različne IT-opreme, storitev, podatkovnih baz in podobnega;
- zastarelo, neposodobljeno programsko opremo, prek katere se omogoči dostop do informacijskih sistemov;
- izmenljive nosilce podatkov oziroma odstranljive medije, na katere je mogoče namestiti zlonamerno kodo in odtujiti podatke ali omogočiti dostop do informacijskega sistema.

Glede na vrsto deležnika je morebitna škoda, nastala ob kibernetskem napadu, različna. Ob kibernetskem napadu na posameznika je posledica omejena na osebno škodo objektivne ali subjektivne narave, kibernetski napad na državno ustanovo ali mednarodno organizacijo pa lahko povzroči precej večjo škodo, saj se tak napad dotakne posameznikovih podatkov in hkrati ogroža varnost ter delovanje ustanove, gospodarstva in države.

Treba je ločiti dva termina, ki se pogosto prepletata, in sicer informacijsko ter kibernetsko bojevanje. Informacijsko bojevanje je namenjeno pridobivanju informacijske prednosti in manipulaciji s pomočjo informacijsko-komunikacijske tehnologije z različnimi vrstami delovanj (psihološke operacije (PSYOPS), elektronsko bojevanje, vojaško zavajanje (INFOPS), računalniške in omrežne operacije ter operacije za zaščito informacij), kibernetsko bojevanje pa je namenjeno napadu in obrambi informacij kot tudi računalnikov in omrežij v kibernetskem prostoru (GIAC, 2016).

Kibernetsko bojevanje ločimo na defenzivno in ofenzivno obliko delovanja. Če ne poznamo ofenzivnega bojevanja, se ne moremo dobro pripraviti na defenzivno bojevanje. Med ofenzivno obliko bojevanja vključujemo kibernetsko vojno in kibernetski terorizem, oboje pa ima namen ovirati oziroma onemogočati delovanje KIS ali pridobivati informacijsko prednost za svojo korist oziroma povzročitev materialne škode. Kibernetsko bojevanje v defenzivni obliki delovanja poskuša preprečiti sovražniku »oviranje« delovanja našega KIS ali/in pridobivanje informacijske prednosti v svojo korist.

Na splošno je treba opredeliti, da se defenzivno kibernetsko bojujemo proti vohunjenju in sabotaži, kar velja za vse deležnike. To je posebno pomembno v državnih organih in vojaških organizacijah, saj je sovražnik v kibernetskem prostoru pogosto neviden in nedefiniran, taktika se nenehno spreminja in ni doktrinarne ter pravne podlage za analizo. Kibernetski napadi imajo velike razsežnosti in lahko hitro povzročijo krizo, izredno stanje, uporabo konvencionalnega orožja ter orožja za množično uničevanje. Kot v sodobnem času zaznavamo skozi taktiko, se pripravljalna faza bojnega delovanja začne z informacijsko vojno (kibernetsko vojskovanje), sledi ji hibridna vojna z asimetričnimi oblikami vojskovanja, šele nato v redkih primerih tudi neposredni bojni spopad vojaških sil.

2.3 Kibernetska varnost in Nato

Nato priznava pomembno vlogo komunikacijsko-informacijskih sistemov (KIS) in ugotavlja, da se mora kot obrambno zavezništvo odločno upreti kibernetskim grožnjam, saj pomenijo resen izziv stabilnosti, blaginji in varnosti zavezništva. Čeprav je vedno skrbel za zaščito svojih KIS, je KIBO na najvišji politični ravni obravnaval šele leta 2001 na vrhu v Pragi (Nato, 2016). Spoznanje o pomenu CYBERSEC je v Natu utrdil dolgotrajen in intenziven kibernetski napad na Estonijo med aprilom in majem 2007. Po tem napadu je Nato decembra 2007 sprejel politiko kibernetske obrambe, ki jo je posodobil leta 2011. Skladno s politiko kibernetske obrambe je uvedel Upravni organ kibernetske obrambe (Cyber Defence Management Authority – CDMA) (Nato, 2016).

Na vrhu v Walesu leta 2014 je bila skupaj z akcijskim načrtom sprejeta nova, izboljšana politika kibernetske obrambe. Njeni poudarki so na kolektivni obrambi, učinkovitem upravljanju, pomoči Nata zaveznicam pri razvoju zmogljivosti in na odzivanju ter sodelovanju z industrijo (Nato, 2016).

Na varšavskem vrhu julija 2016 so zaveznice ob ponovni potrditvi obrambne narave Nata priznale kibernetski prostor kot področje oziroma domeno delovanja, v katerem se mora Nato braniti tako, kot se brani na kopnem, v morju in zraku. Vodje držav so se na vrhu tudi zavezali, da bodo izboljšali nacionalne kibernetske zmogljivosti obrambnih nacionalnih sistemov in infrastrukture ter hitrost in učinkovitost odzivanja ob kibernetskih napadih (Nato_1, 2016).

2.4 Kibernetska varnost in EU

Dokumenti Nata so politično zavezujoči za vsako državo članico, dokumenti EU pa pravno zavezujejo države članice. Razvoj kibernetske varnosti v EU je sledil posledicam kibernetskega ogrožanja Nata, saj je večina članic EU tudi članic Nata (EU, 2016).

Za EU je varnost omrežij in informacij (VOI) bistvenega pomena za delovanje spletne ekonomije ter zagotavljanje blaginje državljanov (EU, 2016). Evropska unija je želela leta 2001 v sporočilu Varnost omrežij in informacij: predlog za evropski politični pristop izpostaviti vse večji pomen varnosti omrežij in informacij (EU, 2002). Leta 2004 je bila ustanovljena ENISA (European Network and Information Security Agency), njen namen pa je bil razviti kulturo kibernetske varnosti, hkrati pa izboljšati »dobro prakso« kibernetske varnosti med državami članicami EU, kar je bil tudi cilj Agende EU pod naslovom Informacijska družba (angl. EU's Information Society agenda). Leta 2006 je EU sprejela strategijo za varno informacijsko družbo Dialog, partnerstvo ter povečanje vpliva in moči (EU, 2007). Glavni namen strategije je bil v Evropi razviti varnostno kulturo na področju omrežij in informacij.

Leta 2009 je Evropska komisija sprejela poročilo Kako zaščititi Evropo pred obsežnimi kibernetskimi napadi in prekinitvami: izboljšati pripravljenost, varnost in odpornost, v njem pa izraža zaskrbljenost zaradi ranljivosti Evrope za obsežne kibernetske napade in izredno škodo, ki bi bila povzročena gospodarstvu in blaginji državljanov (McDonogh, 2010).

Leta 2010 je EU izdala poročilo z naslovom Evropska digitalna agenda. Splošni cilj digitalne agende je poskrbeti, da bo enoten digitalni trg, ki se opira na hitre in ultra hitre internetne povezave ter interoperabilne aplikacije, del trajne gospodarske in družbene koristi (EK, 2010). Leta 2012 je bil ustanovljen CERT-EU (CERT-EU, 2016), ki skrbi za odzivanje na incidente v ustanovah EU. Leta 2013 sta Evropska komisija ter Visoko predstavništvo EU za zunanje in varnostne zadeve predstavila Strategijo kibernetske varnosti, ki je opredelila globalno partnerstvo ter povezovanje s civilnim in vojaškim področjem pri kibernetskih izzivih (EU, 2013). 6. julija 2016 je bila sprejeta Direktiva o varovanju omrežij in informacij, veljati je začela 8. avgusta 2016, v nacionalno zakonodajo jo je treba prenesti do maja 2018.

EU je sprejela tudi nekaj drugih pravno zavezujočih dokumentov z naslovom Peta generacija telekomunikacijskih sistemov (angl. 5G), Oblačne storitve,

Elementi (stvari) interneta (angl. Internet of Things) ter Podatkovne tehnologije (angl. Data Technologies), vse pa je povezano s Standardno informacijsko in komunikacijsko tehnologijo (angl. ICT Standards), ki je del Strategije o digitalizaciji evropske industrije (angl. Digitizing European Industry Strategy).

Treba je tudi omeniti, da je od leta 2010 vzpostavljeno sodelovanje med EU in Natom, v ta namen pa sta organizaciji februarja 2016 sklenili tehnični sporazum o sodelovanju med NCIRC in CERT-EU (EPA, 2016).

3 Kibernetska varnost v Republiki Sloveniji in Slovenski vojski

3.1 Kibernetska varnost v Republiki Sloveniji

Republika Slovenija je SI-CERT ustanovila že leta 1995 v okviru javnega zavoda Arnes. S sklepom Vlade RS leta 2010 je ta na SI-CERT prenesla pristojnosti opravljanja nalog vladnega CERT (SI-CERT, 2016). Slovenija je naredila pomemben korak s sprejetjem Strategije o kibernetski varnosti RS, pri pripravi katere so sodelovali državni organi, nista pa sodelovala akademsko okolje in zasebni sektor. S sprejetjem strategije je pokazala, da se zaveda pomena kibernetske varnosti, globalizacije in hitrega razvoja IKT, hkrati pa tudi upošteva Resolucijo o strategiji nacionalne varnosti RS (Uradni list RS, št. 27/10), Strategijo kibernetske varnosti EU (EU, 2013) ter takrat še predloga Direktive o ukrepih za zagotovitev visoke skupne stopnje varnosti omrežij in informacij v Evropski uniji (Republika Slovenija, 2014).

Strategija kibernetske varnosti v analizi takratnega stanja ugotavlja, da je RS več let pripravljala predloge o sistemski ureditvi kibernetske varnosti, vendar do izvedbe ni prišlo. Prav tako ugotavlja, da »*operativne zmogljivosti za odzivanje na kibernetske grožnje predstavljajo: SI-CERT, Sektor za informacijsko varnost v okviru direktoratov za informatiko na Ministrstvu za javno upravo in na Ministrstvu za obrambo (za sisteme na področju obrambe in varstva pred naravnimi in drugimi nesrečami), SOVA na področju protiobveščevalnega delovanja, Policija (Urad za informatiko in telekomunikacije) in Uprava kriminalistične policije s Centrom za računalniško preiskovanje z zmogljivostmi za zatiranje kibernetskega kriminala.*« Strategija hkrati ugotavlja, da razen

Policije nobeden izmed omenjenih organov v zadnjih petih letih ni izboljšal svojih zmogljivosti in da na strateški ravni ni telesa, ki bi skrbelo za usklajevanje med vsemi deležniki. Ta podatek je še posebno zaskrbljujoč ob dejstvu, da se je število incidentov, ki jih obravnava SI-CERT, od leta 2008 do 2014 povečalo za več kot šestkrat.

V Sloveniji je bolje urejeno normativno področje za varovanje informacij in pregon kibernetskega kriminala, na katerem Zakon o elektronskih komunikacijah (VII. poglavje) ureja varnost omrežij in storitev ter delovanje v izjemnih razmerah, Zakon o elektronskem poslovanju na trgu določa splošna pravila odgovornosti ponudnikov storitev ali gostovanja za podatke, Zakon o elektronskem poslovanju in elektronskem podpisu ureja poslovanje v elektronski obliki z uporabo IKT in uporabo elektronskega podpisa, Zakon o varovanju tajnih podatkov, Zakon o varovanju osebnih podatkov ter Kazenski zakonik, ki opredeljuje kot kaznivo dejanje le zlorabo osebnih podatkov (143. člen), napad na informacijski sistem (221. člen) in vdor v poslovni informacijski sistem (237. člen). V izvedbenih podzakonskih aktih niso nikjer uporabljeni termini kibernetski prostor, kibernetska grožnja, kibernetski kriminal ali kibernetski terorizem.

3.2 Kibernetska varnost v Slovenski vojski

3.2.1 Normativne in načrtovalne podlage za razvoj kibernetskih zmogljivosti v Slovenski vojski

Kot je bilo že omenjeno, nobena vojska ni odporna na kibernetske napade, zato je treba graditi kibernetske zmogljivosti, ki zagotavljajo kibernetsko varnost vojske ter posledično države in njenih državljanov. RS mora kot članica Nata in EU izpolnjevati tako politične kot tudi normativne zaveze do obeh organizacij, pri čemer z razvijanjem nacionalne varnosti krepi tudi mednarodno varnost.

Nacionalna normativna podlaga, ki narekuje razvoj CYBERSEC v Slovenski vojski, je Srednjeročni obrambni program (SOPR) 2016–2020 (Vlada RS, 2016), ki je bil pripravljen na podlagi Resolucije o strategiji nacionalne varnosti RS (Uradni list RS, št. 27/10), Resolucije o splošnem dolgoročnem programu razvoja in opremljanja Slovenske vojske do leta 2025 (Uradni list RS, št. 99/10), Obrambne strategije RS (Vlada RS, 2012), Doktrine vojaške strateške rezerve

RS (Vlada RS, št. 80300-2/2012/5, z dne 25. 10. 2012), Političnih usmeritev Nata (št. C-M(2011) 0022, z dne 14. 3. 2011) ter predloga ciljev zmogljivosti Nata leta 2013 za RS. Ena izmed bistvenih usmeritev SOPR 2013–2018 je bila, da se do konca leta 2014 vzpostavijo zmogljivosti zagotavljanja CYBERSEC, hkrati pa je bila izražena potreba po varnostni izboljšavi oziroma nadgradnji omrežnih zmogljivosti, ki bodo izpolnjevale zahtevano stopnjo CYBERSEC pri zagotavljanju zmogljivosti v podporo poveljevanju in kontroli.

V SOPR 2016–2020 je razvoj zmogljivosti kibernetskega delovanja definiran kot prednostna zmogljivost za bojevanje, hkrati pa je opredeljeno, da bo Ministrstvo za obrambo vzpostavilo ustrezne operativne zmogljivosti za odzivanje na kibernetske grožnje in napade do leta 2020. V SOPR 2016–2020 so opredeljeni ti cilji:

- izboljšati fizične in tehnične zmogljivosti KIS NCKU za ravnanje s podatki ter informacijami višjih stopenj tajnosti;
- izboljšati in prenoviti taktične govorne ter podatkovne povezave;
- povečati ozaveščenost in vzpostaviti zmogljivosti rednega izobraževanja ter funkcionalnega usposabljanja uporabnikov in strokovnega osebja s področja kibernetske varnosti;
- uvesti del temeljnih in funkcionalnih KIS-storitev, ki bodo omogočale varno ter nenehno izmenjavo informacij;
- vzpostaviti operativne zmogljivosti za odzivanje na kibernetske napade in zmogljivosti za kibernetsko obrambo nacionalnih statičnih ter premičnih KIS;
- zagotoviti vojaško zmogljivost za kibernetsko podporo bojevanju;
- zagotoviti visoko razpoložljivost KIS in pomembnih storitev na Ministrstvu za obrambo.

SOPR 2016–2020 poudarja, da je treba zmogljivosti INFOSEC in KIBO vzpostaviti skladno s pravili ter politiko zagotavljanja informacijske in kibernetske varnosti Nata in EU ter na podlagi Nacionalne strategije kibernetske varnosti. Področju CYBERSEC je namenjeno posebno poglavje z naslovom Informacijska varnost in kibernetska obramba, ki ima definirane še posebne cilje:

- Ministrstvo za obrambo bo do leta 2020 vzpostavilo operativne zmogljivosti za odzivanje na grožnje in napade v kibernetskem prostoru, vključno z zmogljivostmi za nadzor KIS, ter za zagotavljanje združene

slike KIBO za premične sile, odkrivanje in blokiranje zlonamernega prometa, alarmiranje, regeneracijo po kibernetskem napadu ter računalniško forenziko;
- na Ministrstvu za obrambo bomo do konca leta 2016 vzpostavili sistem usposabljanja in izobraževanja s področja CYBERSEC, in sicer se bodo sedanjim programom VIU dodale vsebine s področja CYBERSEC ter pripravili programi funkcionalnega usposabljanja za uporabnike IKT na vseh ravneh;
- v nabavne procese in nabavno verigo programske ter računalniške strojne opreme bo vključeno upravljanje tveganj. Skladno z možnostmi bo MO za kritično infrastrukturo KIS nadgradilo zmogljivosti za obnovo po nesreči, v vse sisteme pa vgradilo močno avtentikacijo z možnostjo nadzora dostopa do KIS.

3.2.2 Razvoj kibernetske varnosti v Slovenski vojski

Razvoj CYBERSEC v Slovenski vojski se je začel leta 2003 z uvajanjem častnika za INFOSEC in s tem, ko sta Ministrstvo za obrambo in SV sprejela Natovo direktivo ACO 70-1, ki poudarja, da informacijska varnost ni le varovanje informacij *per se,* temveč pomeni tudi varovanje KIS pred nezakonitim dostopom, uporabo, razkritjem, ločitvijo, spremembo ali uničenjem (Plevnik, 2014: 17).

Ministrstvo za obrambo je na podlagi Natove direktive ACO 70-1 sprejelo in spremenilo različne pravilnike ter navodila, ki obravnavajo varovanje, delovanje in vzdrževanje KIS; varovanje, obdelovanje, hranjenje in prenos podatkov; označevanje gradnikov; posebne podatkovne baze in podobno. Tem normativnim podlagam je sledila tudi SV, ki je za svoje potrebe pripravila akte vodenja in poveljevanja ter direktive v svoji pristojnosti.

Z naraščanjem in odkrivanjem novih oblik groženj ter kriminalitete sta se začela pojavljati tudi nova termina, in sicer kibernetski prostor ter CYBERSEC. Temu terminu sta sledila Nato in EU, zato smo se v SV prilagodili novim »razmeram« na globalni ravni. Generalštab SV je julija 2011 izdal Ukaz za realizacijo strateških transformacijskih imperativov in MO je julija 2013 pripravilo Koncept kibernetske obrambe v obrambnem resorju. GŠSV je v nadaljevanju maja 2014 izdal Ukaz za vzpostavitev zmogljivosti kibernetske varnosti, s katerim je ustanovil delovno skupino za ureditev tega področja.

Delovno skupino sestavljajo pripadniki obveščevalne dejavnosti (J-2), pripadnik sektorja za strateško planiranje (J-5), pripadniki za komunikacije in informatiko (J-6) ter pripadniki iz Enote za komunikacijsko-informacijske sisteme (EKIS). Naloge delovne skupine za kibernetsko delovanje v SV so razvoj kibernetskih zmogljivosti, s poudarkom na sistemu odzivanja na omrežne in računalniške incidente, uvajanje novih IKT, mednarodno sodelovanje ter razvoj izobraževanja in usposabljanja. Ukazu za vzpostavitev zmogljivosti kibernetske varnosti je oktobra 2014 sledil Ukaz za delo v Slovenski vojski za leti 2015 in 2016, hkrati pa je MO že izpolnjevalo cilje zmogljivosti Nata.

Navedenim dokumentom je sledilo oblikovanje novega odseka za kibernetsko varnost v J-6, oblikovan je bil MIL-CERT kot delovna skupina, izvedene so bile številne vaje oziroma usposabljanja, začelo se je ozaveščanje uporabnikov IKT.

3.2.3 Kader s področja kibernetske varnosti v Slovenski vojski

Kader je temelj vsake organizacije, ne glede na tehnologijo, ki jo ima organizacija. Vprašanja CYBERSEC se mora zavedati vsak član organizacije, še posebno pa to velja za pripadnike vojske, saj v kibernetskem prostoru izpostavljajo sebe, tako ogrožajo svojo varnost, varnost svoje družine, sovojakov in enote, kar posledično vpliva na nacionalno varnost.

Za zagotavljanje ustrezne ravni kibernetskega delovanja je treba zagotoviti ustrezen kader, ki mora biti usmerjeno izobražen in usposobljen. Na podlagi potreb dela mora biti narejena ustrezna sistematizacija, ki je poklicno naravnana. V ta namen predlagam:

- vzpostavitev osrednjega usklajevalnega delovnega telesa na MO, ki bi bilo povezovalni člen med civilnim in vojaškim delom (politično-strateška raven);
- kadrovsko okrepitev skupine za KIBV s področja kibernetike na GŠSV (strateška raven);
- oblikovanje enote, ki bi operativno izvajala KIBO (taktična raven), kot jo predvideva omenjeni SOPR.

Trenutno je na politično-strateški ravni vzpostavljena delovna skupina, na strateški ravni je vzpostavljen Odsek za kibernetsko varnost ter na taktični ravni kot oddelek Nadzorni center in kot delovna skupina Center za odzivanje

na računalniške in omrežne incidente. Težave nastanejo pri pridobivanju in ohranjanju primernega kadra, kar posledično povzroča težave pri zagotavljanju ciljev SOPR ter ciljev zmogljivosti Nata. Zaradi pomanjkanja kadra zaposleni v SIK in pripadniki SV opravljajo dela in naloge na več krajih hkrati, kar povzroča veliko težav. Ti pripadniki sodelujejo tudi pri drugih rednih in izrednih nalogah SV, kar še zmanjšuje razpoložljivost kadra za delo na področju kibernetske varnosti. Prav tako je težava v togosti vojaške organizacije in nekonkurenčnosti SV na trgu delovne sile. To se kaže tako, da za posebne poklice SV ni zanimiva, ker ni konkurenčna pri plačah in razmerah za delo.

4 Kibernetska varnost in mednarodno vojno pravo

Če ne bo drugače označeno, so v tem poglavju uporabljeni povzetki po literaturi Tallinn Manual on the International Law Applicable to Cyber Warfare (Schmitt, 2013), ki je rezultat večletnega dela skupine mednarodno priznanih pravnikov v Natovem združenem centru kibernetske varnosti v Talinu.

Mednarodne pravne norme so nastale precej pred časom kibernetskih tehnologij, pravih izkušenj, kako jih uporabiti v tehnološko izpopolnjenih kibernetskih razmerah, pa še ni. Mednarodna pravna skupnost se je za kibernetske operacije začela zanimati proti koncu 90. let prejšnjega stoletja, ko je Mornariška vojaška akademija ZDA organizirala prvo večjo pravno konferenco na to temo. Po napadu na newyorška dvojčka 11. septembra 2001, po kibernetskem napadu na Estonijo leta 2007, po rusko-gruzijski vojni leta 2010, kibernetskem napadu na iranske jedrske zmogljivosti leta 2010 in po drugih dogodkih je bilo vprašanje kibernetske varnosti tudi z vidika vojaških operacij deležno vedno več pozornosti (Schmitt, 2013: 16).

ZDA so leta 2011 v Mednarodni strategiji kibernetske varnosti zapisale pomembno stališče, da za državno ravnanje v kibernetskem prostoru ni treba spreminjati mednarodnega prava. Menile so, da takratne mednarodne norme s pojavom kibernetskega prostora niso zastarale in da že dolgo priznane mednarodne norme, ki jih države morajo upoštevati v miru in v spopadih, veljajo tudi v kibernetskem prostoru (ZDA, 2011: 9). Za kibernetski prostor torej mednarodnih norm ni treba izumljati na novo, v novi prostor jih je treba le smiselno prenesti oziroma upoštevati.

Pomembno vprašanje je določitev praga v kibernetskem prostoru, ko se je država ob nasilnem dejanju upravičena braniti z vojaško oboroženo silo. Pogledi na to vprašanje še niso povsem oblikovani, pomembno pa je mnenje Stalnega mednarodnega sodišča pri Združenih narodih, da določila praga veljajo za vsako uporabo sile ne glede na uporabljeno orožje.

Za uporabo mednarodnega vojnega prava v kibernetskem prostoru je pomembna definicija kibernetskega napada. Mednarodni pravni strokovnjaki (Schmitt, 2013) so ga definirali kot kibernetsko operacijo bodisi ofenzivno bodisi defenzivno, ki povzroči poškodbe oziroma smrt ljudi ali poškodbe oziroma uničenje objektov. Veljalo bi torej razmisliti o uporabi besedne zveze kibernetski napad, ki jo v vsakdanjem življenju pogosto uporabljamo, saj njena uporaba navadno ne ustreza definiciji, ki se uporablja v mednarodnem pravu.

Zanimivo je vprašanje suverenih pravic in odgovornosti držav v kibernetskem prostoru. Kibernetska infrastruktura, ki je na ozemlju države, torej na zemlji, v notranjih vodah, teritorialnem morju, vodah arhipelagov in nacionalnem zračnem prostoru, je predmet suverenih pravic države. Suverenost pomeni, da država lahko nadzira dostop do svojega ozemlja in ima znotraj omejitev, ki jih določa pogodbeno in običajno mednarodno pravo, ekskluzivno pravico, da izvaja pristojnosti in oblast na svojem ozemlju. Suverenost daje državi pravico in tudi dolžnost varovati kibernetsko infrastrukturo na njenem ozemlju ne glede na to, kdo je njen lastnik. Pri uveljavljanju načela suverenosti je treba upoštevati, da zaradi narave kibernetskega prostora države nimajo monopola moči v kibernetskem prostoru in si ga po vsej verjetnosti tudi v prihodnje ne bodo mogle povsem zagotoviti.

Pogoj za mednarodno nezakonito dejanje države, tudi v kibernetskem prostoru, je dejanje ali opustitev dejanja, ki ga je mogoče skladno z mednarodnim pravom pripisati državi in pomeni kršitev mednarodnih obveznosti. Na nezakonitost po mednarodnem pravu ne vpliva morebitna opredelitev dejanja kot zakonitega po notranjem pravu države.

Odgovornost za dejanje ali opustitev dejanja se lahko predpiše državi, če izvira od:

- organov države;
- posameznikov ali subjekta, ki izkazuje elemente vladnih organov;
- organov, ki jih je država dala na voljo drugi državi.

Odgovornost se pripiše državi tudi, kadar ta izvaja učinkovit nadzor in usmerja dejanja posameznikov ali skupine, kar pa je pogosto težko dokazati. Če država pomaga drugi državi, je soodgovorna za kazniva dejanja druge države. V mednarodnem pravu se lahko uporabi tudi pristop drsečega obsega (sliding scale), torej večji ko je obseg zagrešenih kaznivih dejanj, nižji naj bodo dokazni standardi. Prav tako se uporablja načelo dolžnosti ravnanja (due diligence), ki velja, ko država ni ravnala ustrezno preventivno. Države lahko oporekajo krivdo ob proporcionalni samoobrambi, zakonitih protiukrepih, dejanjih, ki izhajajo iz hude stiske, ob višji sili ali nuji.

Tudi v kibernetskem prostoru je pomembno vprašanje legitimnih vojaških ciljev. Pri določanju vojaških ciljev sta pomembni dve vprašanji, in sicer kdo ali kaj je vojaški cilj ter kdaj in kako napasti. Pri prvem vprašanju je pomembno, ali je potencialni cilj bojevnik ali civilna oseba, ki neposredno izvaja sovražna dejanja ali sodeluje pri njihovem izvrševanju, ali objekt v kibernetskem prostoru prispeva k vojaškim akcijam sovražnika ter ali bo napad na objekt v kibernetskem prostoru zagotovil neposredno in konkretno vojaško prednost. Pri drugem vprašanju procesa določanja ciljev je treba preveriti cilj, izbrati ustrezno orožje, opozoriti civilno prebivalstvo in proučiti alternative. Posebno pozoren je treba biti na izbiro, ki minimizira civilne žrtve.

Pri določanju nekinetičnih in kinetičnih vojaških ciljev v kibernetski vojni naj bi veljala enaka pravila kot za kinetično vojno. Postavlja se vprašanje definicije kibernetskega orožja in metod kibernetskega vojskovanja. Civilni objekti ne smejo biti predmet napada ali povračilnih ukrepov. Definicija civilnih objektov je stroga in izhaja iz negacije vojaških ciljev, saj so civilni objekti vsi objekti, ki niso vojaški cilji. Napad naj bi bil strogo omejen le na vojaške cilje. Vojaški cilji po svoji naravi, lokaciji, namenu ali uporabi učinkovito prispevajo k vojaški akciji in njihovo popolno ali delno uničenje, zajetje ali nevtralizacija v danem času zagotavljajo vojaško prednost. Ob dvomu (cerkveni objekti, šole in civilni bivalni objekt) se šteje, da objekt ni uporabljen v vojaške namene.

5 Izobraževanje in usposabljanje s področja kibernetske varnosti v Slovenski vojski

Izobraženost in usposobljenost uporabnikov IKT sta podlaga za delovanje vsake sodobne in uspešne organizacije, ki potrebuje usposobljen kader z znanjem iz naravoslovja in tehnike, torej informatike, matematike ter računalništva.

Takšno znanje je mogoče pridobiti z individualnim ozaveščanjem, izobraževanjem na civilnih in vojaških ustanovah ter s sodelovanjem na vajah. Na področju CYBERSEC je pomembno izpostaviti uvedbo sodelovanja javnega sektorja z zasebnim in industrijo ter akademskim okoljem, saj so vsi deležniki medsebojno močno povezani. Od medsebojnega sodelovanja so odvisne nacionalna stabilnost in varnost države, pa tudi stabilnost ter varnost Nata in EU.

Razsežnost kibernetskega prostora je nazorno prikazana v Doktrini za usposabljanje in poveljevanje ZDA (angl. The United States Army Training and Doctrine Command – TRADOC), v kateri so kibernetski prostor razdelili na tri sloje, in sicer fizični, logični ter socialni (MCDC, 2013: 12–13):

- fizični sloj sestavljajo fizične lokacije (geografska umeščenost) elementov omrežja, strojne opreme in infrastrukture (komunikacijski vodi, radijske frekvence, delilniki, strežniki, računalniki, sateliti itn.);
- logični sloj sestavljajo logične povezave med napravami (računalniki, mobilni telefonski aparati, IP-naslovi itn.), ki so povezane v računalniška omrežja;
- socialni sloj sestavljajo »kibernetske osebe« (virtualne osebe), osebne identifikacije (kot je elektronski naslov) in resnične osebe, ki uporabljajo omrežja.

Kompleksnosti kibernetskega prostora in prepletenosti vseh deležnikov se zaveda tudi EU, še posebno za potrebe skupne varnostne in obrambne politike. V Predlogu koncepta kibernetske obrambe za vodilne vojaške operacije EU (angl. Draft EU Concept on Cyber Defence for EU-led military Operations and Missions) je navedeno, da so učinki kibernetskih groženj na področju obrambe zelo podobni učinkom v civilnem življenju, razlika so le posledice (EU_1, 2016: 4).

Prav zato je v že omenjenem predlogu koncepta kibernetske obrambe EU poudarjeno, da je za 95 odstotkov incidentov na področju kibernetske varnosti vzrok človeška napaka, zato je še toliko bolj pomembna ozaveščenost, ki jo imenujejo kibernetska higiena (angl. cyber hygiene) za vse uporabnike IKT, hkrati pa je treba imeti ozko specialistično usposobljen kader (operativno odzivanje na kibernetske napade) in ta kader na vajah nenehno uriti (EU_1, 2016: 38).

5.1 Izobraževanje in usposabljanje s področja kibernetske varnosti v SV

Kot je bilo že v uvodu omenjeno, se izobraževanje začne z lastnim interesom, torej individualnim izobraževanjem, z viri, ki so na voljo, pogovori, udeležbo na delavnicah, seminarjih in podobnim. Za to še ni treba imeti posebne izobrazbe za posamezno področje, temveč le željo po večji širini znanja in zavedanje, da so za veliko večino neljubih dogodkov v sodobnem svetu krivi neznanje, površnost, neodgovornost in naša nedoslednost.

Stotnik Dejan Šimat (Intervju, 28. april 2016) poudarja, da mora vsaka država oziroma članica Nata samostojno poskrbeti za CDSAC (Cyber Defence Situational Awareness Capabilities), v katerega morajo biti vključene funkcije za omrežni nadzor, obveščanje in alarmiranje ob incidentih, saj se le tako zaščiti večja skupnost, na primer Nato ali EU. Iz tega sledi, da mora vsaka država samostojno vzpostaviti zmogljiv sistem kibernetske varnosti, ki se začne z izobraževanjem in usposabljanjem. VIU se pripadniki SV udeležujemo v domovini in tujini. Pripadniki Nadzornega centra SV ter Centra za odzivanje na računalniške in omrežne incidente SV pridobivajo znanje:

- na individualnem izobraževanju;
- v SI-CERT, v katerem je treba imeti predhodno znanje s področja informatike (osnove html, java script, poznavanje operacijskih sistemov, omrežij itn.);
- s sodelovanjem na konferencah in seminarjih v RS, ki jih organizirajo akademsko okolje in ponudniki komunikacijsko-informacijskih storitev;
- na Natovih šolanjih na US Nato Postgraduate School, v Latini in Oberammergauu;
- s sodelovanjem na mednarodnih vajah, ki so pomemben vir praktičnega znanja;
- v okviru štirih seminarjev Cyber Endeavor, ki jih vodi Nacionalna garda Kolorada iz ZDA, pri čemer se pripadniki SV seznanijo z orodji za ocenjevanje, odkrivanje in zmanjšanje kibernetskih groženj;
- z internim usposabljanjem na Ministrstvu za obrambo v SIK, ki ima strokovnjaka s področja forenzike, to znanje pa je pridobil v SANS Institute (pilotno šolanje za forenzike);
- na vsakoletni Natovi vaji Cyber Coalition (nosilec vaje v RS je Ministrstvo za obrambo) in Immediate Response (nosilec vaje je SV);

– z izobraževanjem in usposabljanjem v sodelovanju s Policijo na področju informacijske forenzike, ki je v fazi načrtovanja.

5.2 Izobraževanje in usposabljanje s področja kibernetske varnosti v Natu

Vse praktično znanje je neprecenljivo, saj je pridobljeno na podlagi realnih scenarijev, zato je to znanje treba deliti, česar se zavezniki tudi zavedajo. Prav zaradi nujnosti povezanosti vseh deležnikov v kibernetskem prostoru je bil na pobudo Portugalske v okviru Natovih projektov pametne obrambe vzpostavljen projekt izobraževanja in usposabljanja s področja kibernetske obrambe (NATO Multi National Smart Defence Project on Cyber Defence Education & Training – MN CD E&T).

Leta 2010 so se članice Nata v Lizboni dogovorile, da je treba povečati zmogljivosti kibernetske obrambe zavezništva in vzpostaviti učinkovit sistem izobraževanja. Ta načrt ni bil uresničen do konca leta 2013, ko je Združeno poveljstvo za Evropo sprejelo Natov načrt za izobraževanje in usposabljanje s področja kibernetske obrambe (angl. NATO Cyber Defence Education and Training Plan). Načrt je vseboval ravni: politično-vojaško, strateško in taktično-specialistično.

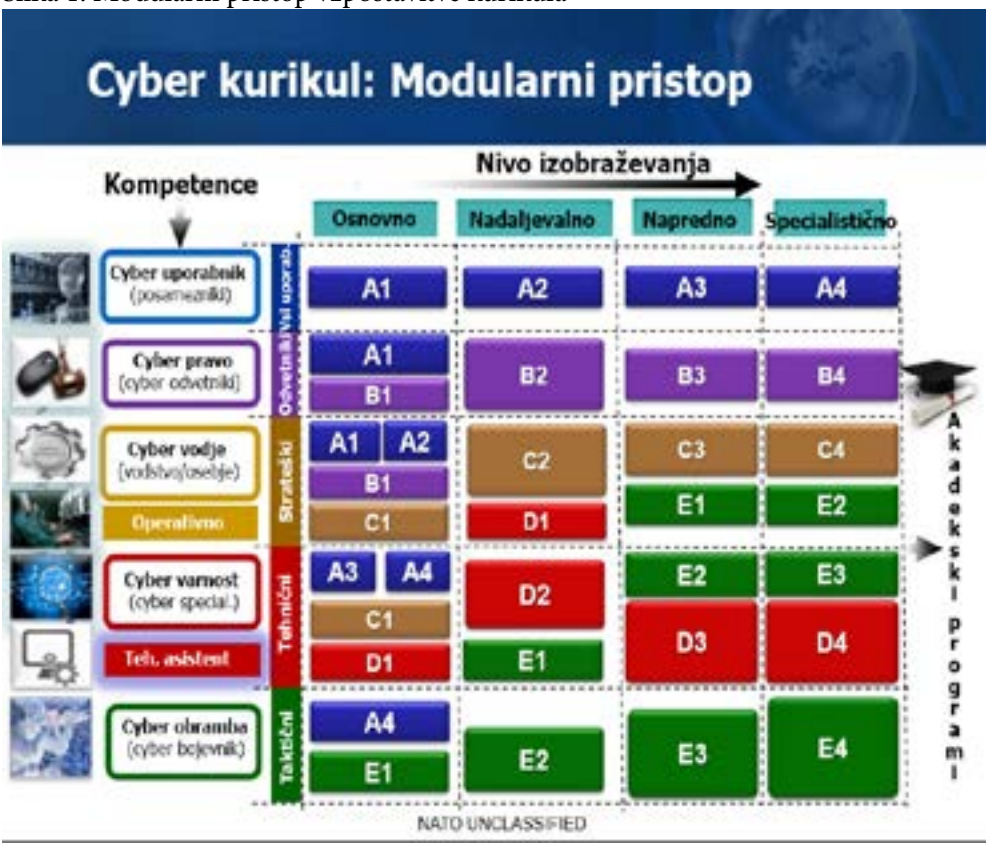
Sledil je Načrt izobraževanja in usposabljanja s področja kibernetske varnosti (C 0616 NATO Cyber Defence Education and Training Plan), ki ga je sprejel Vojaški odbor Nata februarja 2015. Organiziranih je bilo devet delavnic v okviru pametne obrambe (angl. smart defence), na katerih se je razvijal in usklajeval sistem izobraževanja in usposabljanja znotraj zavezništva (Nato in EU). Natov načrt za izobraževanje in usposabljanje s področja KIBO, različica 2.05, določa tri stopnje funkcionalnih usposabljanj:

– osnovno usposabljanje (basic-awareness) za opravljanje omejenih, rutinskih nalog in procedur KIBO; organizacija, predstavitev razumevanja podatkov in razmere KIBO; identifikacije vzroka in učinka razmer KIBO, pri čemer ta ciljna skupina potrebuje dodatna navodila in nadzor;
– nadaljevalno usposabljanje (intermediate) za opravljanje nerutinskih nalog s področja kibernetske obrambe v različnih razmerah; uresničevanje konceptov KIBO, sprejemanje sklepov in mogočih

ukrepov, pri čemer ta ciljna skupina potrebuje krajša navodila, pretežno pa delo opravlja samostojno;
– napredno in specialistično usposabljanje (advanced) za opravljanje ocenjevanja kompleksnih razmer KIBO, združevanje različnih tehnik za izvajanje ukrepov ob »novih« razmerah, izvajanje pomoči in izdajanje navodil, hkrati pa tudi za pripravo novih standardov.

Delovna skupina CD E&T je pripravila modularni pristop izobraževanja glede na različne akterje v kibernetskem prostoru (slika 1). K sodelovanju je povabila industrijo in akademijo ter v okviru socialnega mreženja pripravila razmere za praktično vsebinsko izvedbo na vseh šolah in tečajih Nata in EU, na katerih se bo izvajalo VIU.

Slika 1: Modularni pristop vzpostavitve kurikula



Vir: Nato, 2016.

Kurikul na sliki 1 predstavlja različne module VIU za posamezne uporabnike na različnih ravneh. Da se v celoti vzpostavijo kompetence posameznikov na področju KIBO, sta skozi štiri ravni VIU začrtani karierna pot posameznika in vrsta tečajev, ki jih bo moral opraviti za pridobitev ustreznega dodatnega znanja (to bo vpisano v sistemizaciji dela nacionalnih vojaških organizacij).

5.3 Izobraževanje in usposabljanje s področja kibernetske varnosti v EU

Kot vse mednarodne organizacije se tudi EU ukvarja s problematiko kibernetske varnosti in obrambe. Evropska obrambna agencija (EDA) je 19. oktobra 2011 izdala Strateški okvir kibernetske obrambe (angl. Strategic Context Case Cyber Defence, v nadaljevanju SOKIBO), katerega glavni cilj je bila zagotovitev skupne varnostne in obrambne politike EU kot tudi operacij kriznega upravljanja. V 22. točki SOKIBO je opredeljeno usposabljanje, ki vključuje več vaj, izobraževanje in izboljšanje ozaveščanja za vse ravni odločevalcev, da se zagotovijo minimalni standardi osnovnega kibernetskega ozaveščanja (cyber hygiene). Taka zaveza je bila že v Strategiji evropske varnosti leta 2008 za izvajanje učinkovite politike kibernetske varnosti v sodelovanju z drugimi članicami EU in mednarodnimi akterji (ENISA, CERT-EU, Nato itn.). V SOKIBO je ugotovljeno, da je človeški dejavnik bistveni element varnosti, zato se mora zagotoviti izobraževalni program, ki bo izboljšal ozaveščenost s področja kibernetske varnosti vseh uporabnikov IKT v EU, hkrati pa se morajo zagotoviti enotni standardi usposabljanja za vojaške ustanove in civilno-vojaško osebje (EU, 2011, 1–13). V ta namen je EDA ob pomoči inštituta SANS izvedla »pilotni« tečaj digitalne forenzike leta 2014 (EU, 2016), leta 2016 pa je v okviru projekta Hrana za misli izvedla ad hoc projekt *Zahtevano združevanje za usposabljanje in vaje kibernetske obrambe,* ki ga podpira zasebni sektor. Cilj tega projekta je izboljšati usposabljanje EU s področja KIBO ob podpori zasebnega sektorja. Iz tega je jasno razvidno, da je nujno povezovanje z zasebnim sektorjem, ki je »motor« razvoja IKT, hkrati pa tudi razvoja znanja, ki ga vojaške organizacije zaradi podhranjenosti kadra ne razvijajo samostojno.

5.4 Predlog izobraževanja in usposabljanja s področja kibernetske varnosti v SV

V SV imamo dobro razvit sistem vojaškega izobraževanja in usposabljanja (OVIU, OVSIU, DVIU ipd.), zato je treba področje KIBO uvrstiti skladno s sistemizacijo VIU Nata ter vsebine vključiti v sedanje programe rednega VIU (CVŠ) ter pripraviti programe funkcionalnega vojaškega usposabljanja (GŠSV) za usposabljanje drugih pripadnikov, ki niso napoteni na šolanje. V ta namen lahko za osnovno VIU prevzamemo že pripravljeno taksonomijo MN CD E&T (Natov načrt za izobraževanje in usposabljanje s področja kibernetske obrambe, različica 2.05):

- osnovno usposabljanje se izvaja za vse uporabnike IKT kot tudi uporabnike taktičnih in oborožitvenih sistemov. Treba je poudariti, da bo to potekalo za vse ravni vodenja in poveljevanja, dokler se ne vzpostavi določena raven zavedanja. Pozneje bo treba smiselno razdeliti osnovno usposabljanje na ravni vodenja in poveljevanja kot tudi na uporabo različnih sistemov. Za usposabljanje se poskrbi na ravni delovne organizacije, kar za nas v SV pomeni na CVŠ v okviru rednih programov, in za druge uporabnike IKT v matični enoti v okviru letnih obvez ob podpori strokovnih organov J-6 in S-6. Najbolj primerna oblika usposabljanja so predavanja v kombinaciji z e-učilnico;
- nadaljevalno usposabljanje uporabnikov KIS se izvaja zaradi prepoznave nevarnosti, da ni napaka uporabnika, da se uvrsti oziroma definira kot incident ter obvestijo pristojne službe oziroma CERT na nacionalni ravni. Udeležili se jih bodo pripadniki rodu zvez in službe informatike, ki so odgovorni za podporo uporabnikom organizacijske enote. Za izobraževanje in usposabljanje se poskrbi na ravni nacionalnih centrov za kibernetsko obrambo oziroma v Nato CIS&CD Schools (NCISCDS) na tečajih J-6. Najbolj primerna oblika usposabljanja so predavanja v kombinaciji z e-učilnico;
- napredno in specialistično usposabljanje se izvaja zaradi odprave, evidentiranja in analize incidentov. Treba je vnašati incidente v skupno bazo in obveščati druge, ki so povezani v skupno bazo z incidenti. Udeležili se ga bodo vsi, ki operativno načrtujejo in delujejo oziroma odpravljajo incidente v centrih za kibernetsko obrambo. Izobraževanje in usposabljanje se izvajata v Natovih CIS&CD Schools (NCISCDS),

na tečajih J-6. Najbolj primerna oblika usposabljanja so predavanja, e-učilnica, delavnice in vaje.

6 Sklep

Na podlagi sinteze informacij in analize virov lahko potrdim, da je najpomembnejši element varnosti človek, kar je navedeno v dokumentih EU in Nata. Pomembnosti človeškega dejavnika se zaveda tudi mednarodna skupnost. EU in Nato sta ugotovila, da največje tveganje v organizaciji pomenijo uporabniki IKT. Tudi v Strategiji kibernetske varnosti RS je temu namenjeno posebno podpoglavje, hkrati pa v vsej strategiji lahko spoznamo, da je treba izvajati programe ozaveščanja sprotno, celovito in po ravneh prilagojeno uporabnikom.

Za SV velja, da se je z razvojem IKT povečalo povpraševanje po funkcionalnem kadru oziroma specialistih, ki pa jih zaradi enotnega plačnega sistema težko pridobimo in še teže obdržimo, saj MO v plačah ni konkurenčno gospodarskemu sektorju. Težava nastopi zaradi enotnega plačnega sistema in kadrovske strukture SV, ki se v splošnem deli na vojake, podčastnike in častnike, pri katerih se pristojnosti prepletajo, saj struktura ni oblikovana poklicno. Tako bi bilo treba za vojake na področju KIS določiti poleg vojaške tudi poklicne kvalifikacije, ki bi bile konkurenčne zasebnemu sektorju. Dodati je treba, da so delovne razmere in zahteve v SV precej posebne v primerjavi z drugim delom javnega sektorja ali z zasebnim sektorjem. V SV je vojak lahko zaposlen le do 45. leta, vsako leto opravlja obvezno individualno in skupinsko usposabljanje, vsako leto mora opraviti preverjanje gibalnih in strelskih sposobnosti, zaradi deficita kadra pa opravlja dela in naloge, ki niso v opisu njegovih del in nalog. V drugem delu javnega in zasebnega sektorja ni tako. Delo je ovrednoteno drugače, zagotovljena je boljša socialna varnost, kar povzroča »beg« kadra iz SV in ga bo tudi v prihodnje. Kot primerjavo bi želel izpostaviti, da je hrvaški vojski uspelo ustaviti ta beg šele pri 40-odstotnem povečanju plač deficitarnemu kadru (USEUCO – Regionalna delavnica o kibernetski obrambi v Sloveniji, Bled, 25.–29. februar 2016). Tega v Sloveniji trenutno ni mogoče pričakovati, čeprav tudi trenutna delovnopravna zakonodaja omogoča povečanje plač za deficitarne poklice, kot je to na primer urejeno za pilote. Vsekakor se bo RS morala odločiti, ali se bodo kibernetske zmogljivosti vzpostavile ali bodo ostale le prazne črke na papirju.

Urediti je treba še celovit sistem izobraževanja in usposabljanja, k čemur nas usmerjajo tudi dokumenti EU ter Nata. V Strategiji kibernetske varnosti RS je sicer navedeno, da je informacijska oziroma kibernetska varnost vključena v več študijskih programov na različnih fakultetah, ne pa na osnovnih ali srednjih šolah, na katerih se uporabnik začne srečevati z IKT.

Za kakovostno izvajanje kibernetske obrambe in Strategije kibernetske varnosti RS potrebujemo tri ravni znanja, od ozaveščanja do specialističnega znanja. Trenutno to znanje pridobivamo v tujini, SI-CERT-u in Policiji. Slovenska vojska ima malo usposobljenega kadra, zato je treba že pridobljeno znanje širiti v organizaciji. V obliki funkcionalnega vojaškega izobraževanja in usposabljanja je treba pripraviti programe, po katerih se bodo vsebine po ravneh sistemsko prenašale na pripadnike v SV ter na zaposlene na MO in tudi drugih ministrstvih, ki nimajo možnosti razvijati vedno bolj pomembnih vsebin.

Za konec bi želel dodati, da v kibernetskem prostoru ni pomemben le ustrezen in usposobljen kader s področja kibernetske varnosti, temveč tudi zmogljiva in varna informacijsko-komunikacijska tehnologija. Ta je v SV posebna, saj se uporabljata splošna oprema, ki je dostopna vsakomur, in vojaška oprema, ki je posebna zaradi strojne in programske opreme.

7 Literatura in viri

1. Berkowitz, B. D., 2010. *The New Face of War: How War Will Be Fought in the 21st Century.* s.l.: Free Press.
2. CCDCOE, 2016. *Cyber Definitions.* https://ccdcoe.org/cyber-definitions.html (4. avgust 2016).
3. CDSE, 2016. *Common Cyber Threats: Indicators and Countermeasures.* http://cdsetrain.dtic.mil/cybersecurity/data/pdf/Common_Cyber_Threats_Indicators_and_Countermeasures.pdf (10. avgust 2016).
4. CERT-EU, 2016. *About Us.* https://cert.europa.eu/cert/plainedition/en/cert_about.html (8. avgust 2016).
5. CNSS, 2015. *CNSS Glossary.* s.l.: Committee on National Security Systems.
6. Comodo Antivirus, 2014. *A Short History of Viruses.* http://antivirus.comodo.com/blog/computer-history-computer-viruses/ (4. avgust 2016).

7. EK, 2010. *Evropska digitalna agenda.* http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=URISERV:si0016&from=EN (8. avgust 2016).
8. EPA, 2016. *EPA*. http://www.europeanpublicaffairs.eu/time-to-catch-up-the-eus-cyber-security-strategy/ (11. avgust 2016).
9. EU_1, 2016. *Draft EU Concept on Cyber Defence For EU-led military Operations and Missions, 2016.* Bruselj: 2016.
10. EU, 2002. Network and Information Security: Proposla for a Europena policy approach. *Officila Journal of the European Union*, 22. oktober, 113–116.
11. EU, 2007. Strategija za varno informacijsko družbo – Dialog, partnerstvo ter povečanje vpliva in moči. *Uradni list Evropske unije*, 28 4, 21–26.
12. EU, 2011. *Strategic Context Case Cyber Defence.* Bruselj: EDA: 2011.
13. EU, 2013. *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace,* Bruselj: EU.
14. EU, 2016. *Digital Single Market.* https://ec.europa.eu/digital-single-market/en/cybersecurity (8. avgust 2016).
15. EU, 2016. *Direktiva Evropskega parlamenta in sveta o ukrepih za zagotavljanje visoke skupne ravni varnosti omrežij in informacij v Uniji.* s.l.:EU.
16. EU, 2016. *EDA Digital Forensics Pilot Course (SANS FOR408) Students SURVEY.* Bruselj: EDA: 2016.
17. Fitzpatrick, R., 2008. *Maxwell's Equations and the Principles of Electromagnetism.* s.l.: Infinity Science Press.
18. Gascuena, D., 2016. *OpenMind.* https://www.bbvaopenmind.com/en/nevil-maskelyne-vsmarconi-a-hacker-in-1903 (4. avgust 2016).
19. GIAC, 2016. *GIAC.*https://www.giac.org/paper/gsec/3873/information-warfare-cyber-warfare-future-warfare/106165 (16. julij 2016).
20. http://www.wired.com, 2009. *Kim Zetter.* http://www.wired.com/2009/11/1110fred-cohen-first-computer-virus/ (24. maj 2016).
21. ITU-T, 2009. *Overview of cybersecurity.* s.l.:ITU.
22. Jirásek, P., Novák, L.,& Požár, J., 2013. *Cyber Security Glossary.* Druga ured. Praha: National Cyber Security Centre of the Czech Republic.
23. Kissel (Ed.), R., 2013. *Glossary of Key Information Security Terms.* Drugi ured. Gaithersburg: National Institute of Standards and Technology.

24. Klimburg (Ed.), A., 2012. *National Cyber Security Framework Manual.* Tallinn: NATO CCD COE Publication.
25. Lee, T. B., 2013. *How a grad student trying to build first botnet brought the Internet to its knees.*https://www.washingtonpost.com/news/the-switch/wp/2013/11/01/how-a-grad-student-trying-to-build-the-first-botnet-brought-the-internet-to-its-knees/ (5. avgust 2016).
26. MCDC, 2013. *Handbook for Integrating Cyber Defense into the Operational Planning Process, V 1.0, MCDC, 2013-14.*Bruselj: 2013.
27. McDonogh, 2010. Kako zaščititi Evropo pred obsežnimi kibernetskimi napadi in prekinitvami: izboljšati pripravljenost, varnost in odpornost. *Uradni list Evropske unije*, 22 9, 98–102.
28. Monitorpro, 2015. *Monitopro.* http://www.monitorpro.si/168076/praksa/varnost-na-prvem-mestu/ (13. avgust 2016).
29. NATO_1, 2016. *Warsaw Summit Communiqué.* http://www.nato.int/cps/en/natohq/official_texts_133169.htm (5. avgust 2016).
30. NATO, 2011. *Nove grožnje: kibernetska razsežnost.* http://www.nato.int/docu/review/2011/11-september/Cyber-Threads/SL/index.htm (30. april 2016).
31. NATO, 2016. *Cyber defence, More background information, Evolution.* http://www.nato.int/cps/en/natohq/topics_78170.htm (5. avgust 2016).
32. NATO, 2016. *Predstavitev MN CD E&T Project Workshop #8, Lisbona, 27. april 2016.* Lizbona: 2016.
33. NATO, 2016. *Predstavitev MN CD E&T Project Workshop #9, Lisbona, 19.–20. julij 2016.* Lizbona: 2016.
34. Plevnik, M., 2014. *Podatkovne komunikacije* s.l.: s.n.
35. Republika Slovenija, 2014. *Strategija kibernetske varnosti.* s.l.: s.n.
36. Schmitt (Ed.), M. N., 2013. *Tallinn Manual on the International Law Applicable to Cyber Warfare.* s.l.: Cambridge University Press.
37. SI-CERT, 2016. *Kaj je CERT?* https://www.cert.si/si/o-certu/ (5. avgust 2016.
38. SI-CERT, 2016. *Kaj je CERT?* https://www.cert.si/si/o-certu/ (5. avgust 2016).
39. Štrucl, D. (2016). Izgradnja zmogljivosti kibernetske varnosti v Slovenski vojski. Zaključna naloga višještabnega tečaja, Center vojaških šol, Maribor.

40. Uradni list RS, št. 27/10. *Resolucija o strategiji nacionalne varnosti Republike Slovenije.* s.l.: Uradni list RS, št. 27/10.
41. Uradni list RS, št. 99/10. Resolucije o splošnem dolgoročnem programu razvoja in opremljanja Slovenske vojske do leta 2025.
42. Vlada RS, 2012. *Obrambna strategija Republike Slovenije, dok. št. 80000-1/2012/4 z dne 7.12.2012.* s.l.: Vlada R Slovenije.
43. Vlada RS, 2012. *SOPR za leta 2013–2018, dok. št. 803-4/2012-46,* s.l.: Vlada RS.
44. Vlada RS, 2016. *Srednjeročni obrambni plan (SOPR), dok. št. 80300-2/2016/3, z dne 17. 2. 2016.* s.l.: Vlada RS.
45. Wikidot, 2016. *The Virus Encyclopedia.* http://virus.wikidot.com/crepeer (4. avgust 2016).
46. Wikipedia, 2016. *Morris worm.* http://en.wikipedia.org//wiki/Moris_worm (4. avgust 2016).
47. ZDA, 2011. *International Strategy for cyberspace.* s.l.:ZDA, Bela hiša.
48. ZRC SAZU, 2014. *Terminologišče.* isfr.zrc-sazu.si/sl/terminologisce/svetovanje/kibernetska-varnost#v (3. avgust 2016).

Ustni viri:

1. Šimat, Dejan (28. 4. 2016). Intervju. Maribor.