UNIVERZA V LJUBLJANI

FAKULTETA ZA DRUŽBENE VEDE

Maša Pertoci

Kibernetske enote kot nova veja oboroženih sil

Diplomsko delo

Ljubljana, 2015

UNIVERZA V LJUBLJANI

FAKULTETA ZA DRUŽBENE VEDE

Maša Pertoci

Mentor: izr. prof. dr. Uroš Svete

Kibernetske enote kot nova veja oboroženih sil

Diplomsko delo

Ljubljana, 2015

ZAHVALA

Iskreno se zahvaljujem svojemu mentorju izr. prof. dr. Urošu Svetetu za vse strokovne nasvete in pomoč pri izdelavi diplomskega dela.

Zahvaljujem se tudi družini, ki mi je omogočila študij in mi ves čas študija stala ob strani.

KIBERNETSKE ENOTE KOT NOVA VEJA OBOROŽENIH SIL

Tradicionalno poznamo tri dimenzije prostora kot bojišče, in sicer kopno, vodo ter zrak. Z razvojem tehnik bojevanja in novih vrst orožij se je zgodil velik napredek v smeri informatizacije, ki je prinesel še naslednjo dimenzijo - kibernetski prostor. Tega lahko v današnjem času označimo kot zelo pomemben element vplivanja na sovražnika. Bojevanje v kibernetskem prostoru izvajajo za to usposobljeni vojaki, ki pa nimajo neposrednega fizičnega stika s sovražnikom , temveč delujejo preko računalniške oziroma informacijske opreme. Kibernetski vojaki so relativno nov pojav, ki se bo razvijal še intenzivneje v prihodnjih letih, vzporedno z napredovanjem kibernetskega bojevanja oz. vojskovanja. Tako lahko kibernetske vojake opredelimo kot novo generacijo vojaških enot, ki bi lahko v prihodnosti odigrale pomembno vlogo pri nacionalni varnosti same države. Človeštvo vse večjo vlogo posveča tehnologiji, zato vedno več groženj izhaja iz same tehnologije ter interneta. Nekatere države že vključujejo kibernetske enote kot novo vejo oboroženih sil, v ostalih državah pa se bo ta trend pojavil verjetno v naslednjih letih.
Ključne besede: kibernetsko bojevanje, varnost, tehnologija, grožnja.

CYBER UNITS AS A NEW BRANCH OF ARMY

Traditionally we know 3 dimensions of warfare: land, sea and air. With the development of the warfare and new weapons the step was taken into the informatziation, which bring the next dimension – cyberspace. The cyberspace today is known as a important element of the influence on the enemy. Warfare in cyberspace is lead from the experts, which has no physical contact with the enemy. They operate through the IT equipment. Cyber soldiers are relatively new phenomena, which will be developed intensively in next years, parallel with the development of cyber warfare. Cyber soldiers can be defined as a new generation of army units, which may play very important role of the national security in the future. The increasing role of mankind devotes technology, so more and more threats arising from the same technology and the Internet. Some countries already include cyber unit as a new branch of the armed forces in other countries, this trend will likely occur in the next few years.

Key words: cyber warfare, security, tehnology, threat.

KAZALO

1 UVOD 7

2 METODOLOŠKI OKVIR 8

2. 1 Predmet in cilj preučevanja 8

2. 2 Hipoteza 8

2. 3 Metodološki pristop 9

2. 4 Temeljni pojmi 9

2. 4. 1 Kibernetski prostor 9

2. 4. 2 Kibernetsko bojevanje 10

2. 4. 3 Bojišče 10

2. 4. 4 Oborožene sile 10

2. 4. 5 Veja oboroženih sil 11

3 RAZVOJ BOJIŠČ VSE DO KIBERNETSKEGA PROSTORA 12

4 OPREDELITEV KIBERNETSKEGA PROSTORA KOT BOJIŠČA 14

5 OPREDELITEV KIBERNETSKIH ENOT KOT POTENCIALNE NOVE VEJE OBOROŽENIH SIL 15

5. 1 Napad na iranski jedrski program 17

5. 2 »Denial-of-Service« v Estoniji 18

6 PRIMERJAVA IZBRANIH DRŽAV GLEDE REKRUTIRANJA IN DELOVANJA KIBERNETSKIH ENOT 19

6. 1 Slovenija 19

6. 2 Severna Koreja 19

6. 3 Velika Britanija 20

6. 4 Tajska 21

6. 5 Latvija 21

6. 6 Združene države Amerike 22

7 USTANAVLJANJE SPECIALIZIRANIH ENOT ZA SOCIALNA OMREŽJA 23
7. 1 Velika Britanija 23
7. 2 Združene države Amerike 23
8 ZAPLETENOST PROCESA REKRUTACIJE 24
9 ANKETNI VPRAŠALNIK O KIBERNETSKIH ENOTAH 25
10 ZAKLJUČEK 34
11 LITERATURA 36
PRILOGE 40
Priloga A: Anketni vprašalnik 40

KAZALO SLIK

Slika 1. 1: Spol anketirancev v odstotkih. 25
Slika 1. 2: Starostne skupine anketirancev. 26
Slika 1. 3: Trenutni status anketirancev. 26
Slika 1. 4: Prikaz seznanjenosti z novejšimi načini vojskovanja. 27
Slika 1. 5: Število dimenzij vojskovanja po mnenju anketiranih. 27
Slika 1. 6: Seznanjenost s pojmom kibernetski prostor. 28
Slika 1. 7: Poznavanje kibernetskega vojskovanja. 28
Slika 1. 8: Viri, kjer so se anketiranci prvič srečali s pojmom kibernetsko vojskovanje. 29
Slika 1. 9: Seznanjenost z ustanavljanjem kibernetskih enot. 29
Slika 1. 10: Orožje, ki ga po mnenju anketiranih uporabljajo kibernetske enote pri svojih nalogah. 30
Slika 1. 11: Stopnja pomembnosti operacij, povezanih s kibernetsko varnostjo. 31
Slika 1. 12: Možnost omejitve operacij nasprotnika s kibernetskimi enotami in njihovimi operacijami. 31
Slika 1. 13: Obstoj enot, ki delujejo zgolj preko socialnih omrežij. 32
Slika 1. 14: Kibernetska enota v Slovenski vojski. 33

1 UVOD

»Ko je tvoje orožje otopelo, tvoja strast ugasla, tvoja moč izčrpana in tvoje zlato porabljeno, bodo nasprotniki to izkoristili. Takrat tudi najpametnejši človek ne more preprečiti tistega, kar sledi«

~ Sun Tzu

Človek si je vedno želel prevlade. Prav zaradi želje po nečem, česar še ni imel v svoji lasti. Tako lahko beremo o zgodovinskih osvajalnih vojnah, mogočnih vojskah in flotah ter herojih, ki so trdno zapisani v zgodovini. Z razvojem človeštva je prišlo do razvoja novih taktik in tehnik bojevanja in tudi orožja. Sprva so se ljudje bojevali le na kopnem, za hrano ali delček zemlje sosednjega plemena, da bi si olajšali življenje in prikazali svoj boljši status v družbi. Kasneje so se začele bitke zaradi povečanja bogastva in večanja strateške (pre)moči določenih držav. S pojavom novih tehnologij v zadnjem stoletju pa se bojevanje odvija v prostoru, ki je mnogim nepredstavljiv. Govorimo o kibernetskem oz. informacijskem bojevanju, ki predstavlja najnovejšo dimenzijo vojskovanja človeštva. Gre predvsem za hekerske vdore in motenje sistemov, ki so izrednega pomena za nacionalno varnost.

Vse od leta 2007 prihaja do porasta napadov na ključno informacijsko opremo in tako tovrstni napadi postajajo vedno kompleksnejša grožnja. V večini primerov se napadi sprožijo iz opreme, ki se nahaja izven ozemlja napadene države, kar še oteži situacijo za napadeno državo. Napadalci izkoristijo ranljivost določenega dela podatkovne baze ali dela informacijske opreme in ga okužijo z obliko škodljive kode, mnogim poznanim pod imenom »worm« oz. računalniški črv. Tovrstni napadi so večinoma usmerjeni na nacionalne sisteme bank, vlade in drugih vplivnejših organizacij in strani. Ker živimo v t. i. »informacijski dobi«, lahko pričakujemo zgolj porast napadov na informacijsko tehnologijo, zato morajo tudi države primerno (re)organizirati obrambne sisteme. Pehota, ki smo jo poznali v 1. in 2. svetovni vojni v tovrstnih spopadih, ni več učinkovita. Za uspeh so pomembne veščine, znanja in poznavanje informacijske opreme in programov ter izobraževanja raznih strokovnjakov v tovrstne namene. Pripadniki kibernetskih enot operirajo z drugačnim orožjem, ki v primeru napada ni osebna oborožitev posameznika, ampak je računalniška oprema in pridobljeno znanje s tovrstnega področja. Ustanavljanje kibernetskih enot, katerih

namen ni napadanje, ampak predvsem preprečevanje napadov na državo, lahko štejemo kot nov trend, ki se bo z leti pojavljal v vse več državah ter se bo razvijal z razvojem tehnologije ter dejansko ogroženostjo določene države pred tovrstnimi napadi.

2 METODOLOŠKI OKVIR

2. 1 Predmet in cilj preučevanja

Predmet preučevanja v mojem diplomskem delu so kibernetske enote kot potencialna nova veja oboroženih sil. Kibernetski vojaki so relativno nov pojav, ki se bo razvijal še intenzivneje v prihodnjih letih, vzporedno z napredovanjem kibernetskega bojevanja oz. vojskovanja.

Prvi sklop diplomskega dela je sestavljen tako, da je najprej predstavljen razvoj dimenzij bojevanja vse do kibernetskega prostora, nato sledi opredelitev kibernetskega prostora kot bojišča. Sledi opredelitev kibernetskih enot kot potencialne nove veje oboroženih sil, kjer primera iz Estonije in Irana prikažeta potrebo po tovrstnih enotah v primeru napada na ključno informacijsko tehnologijo. Zadnji del prvega sklopa diplomskega dela predstavljata še primerjava izbranih držav, kjer sem zbrala podatke za 6 držav, in pa poglavje o ustanavljanju specializiranih enot za socialna omrežja. Drugi sklop diplomskega dela predstavlja anketni vprašalnik o kibernetskih enotah, katerega namen je bil ugotoviti poznavanje tako področja kibernetskega vojskovanja kot tudi ustanavljanja kibernetskih enot.

Glavni cilj diplomskega dela je prikazati kibernetski prostor kot bojišče in izpostaviti potrebo po oblikovanju nove veje oboroženih sil v ta namen.

2. 2 Hipoteza

H1: Proces rekrutiranja kibernetskih enot je zapleten proces, ki od kandidata zahteva odlično poznavanje tehnologije in sledenje razvoju tehnologije, kot tudi odlične računalniške kompetence, s katerimi operira na podoben način kot vojak na klasičnem bojišču z orožjem.

H2: Skozi proces rekrutacije osebja lahko pride do izbire strokovnjakov, ki predstavljajo potencialno notranjo grožnjo tako sistemu kot enoti zaradi njihovega širokega spektra znanja, ki lahko predstavlja večjo neznanko kot sama grožnja s strani nasprotnika.

2. 3 Metodološki pristop

Za pisanje diplomskega dela sem uporabila naslednje metode: analizo primarnih in sekundarnih virov, metodo komparacije ter metodo kompilacije, ki sem jo uporabila predvsem za teoretični del. Za empirični del pa sem uporabila metodo anketiranja.

2. 4 Temeljni pojmi

2. 4. 1 Kibernetski prostor

Kibernetski prostor je domena, karakterizirana s strani uporabe elektronike in elektromagnetnega spektra z namenom skladiščenja, spreminjanja ali izmenjave podatkov skozi omrežne sisteme in s tem povezanih fizičnih infrastruktur (SearchSOA 2015). Gre tudi za navidezno, neotipljivo, virtualno-realno področje, kjer se preko (na splošno) računalniške komunikacije in simulacije in predvsem internetne aktivnosti izvaja neka dejavnost. Je elektronski ekvivalent človeški oz. fizični dejavnosti. Kibernetski prostor tako predstavlja domeni, kjer objekti niso niti fizični niti ne predstavljajo fizičnega sveta, ampak so sestavljeni iz datotek in informacij (BusinessDictionary.com 2015). Obstaja veliko število definicij kibernetskega prostora, vsem pa je skupno spoznanje. Vse razlike in variacije odražajo raven pozornosti državam in organizacijam, ki se soočajo z izzivi kibernetskega prostora (Mahmoud 2013, 3). Kibernetski prostor je globalna domena znotraj informacijskega okolja, ki sestoji od soodvisnih mrež infrastruktur in podatkov, vključno z internetom, telekomunikacijskimi omrežji, računalniškimi sistemi in vgrajenimi procesniki in krmilniki. Iz te dosledne definicije je razvidno, da je kibernetski prostor kompleksen in se v okviru njega razvija skupek tehnologij, s katerimi mora opravljati za to usposobljeno osebje. Pristojen subjekt mora biti seznanjen s številnimi vidiki kibernetskega prostora, ne glede na njihovo vlogo. Glede na širino in globino domene bodo operaterji postali strokovnjaki samo na enem ali dveh vidikih kibernetskega prostora, saj bi bilo zastrašujoče in nerealno, da bi pričakovali obvladanje vseh vidikov kibernetskega prostora in poslovanja. Del problema digitalnega orožja je koncept odvračanja. Težko je odvrniti sovražno državo od določenih dejanj, če ne obstajajo trdni dokazi o njeni škodoželjni nameri. Tako je večina držav že vključena v ozadje dirke s kibernetskim orožjem, približevanje tega koncepta splošni javnosti pa lahko omogoči, da incidenti več ne bi uhajali izpod nadzora (Arnold in drugi 2015).

2. 4. 2 Kibernetsko bojevanje

Gre za uporabo računalnikov in drugih naprav za napad na sovražnikove informacijske sisteme, z namenom povzročitve škode pri sovražniku (Dictionary.com 2015). Gre za konflikte, ki temeljijo na internetu in vključujejo politično motivirane napade ter informacijske sisteme. Kibernetski napadi lahko izmed mnogih možnosti škodovanja nasprotni strani npr. onemogočijo uradne spletne strani in omrežja, motijo ali onemogočijo osnovne storitve, ukradejo ali spreminjajo podatke in pohabijo finančne sisteme (Techtarget 2015).

Gre za obliko vojskovanja, ki se odvija na računalnikih in internetu ter je rastoča sila v mednarodni skupnosti, kjer veliko držav ustaljeno uporablja veščine in se pripravlja na pristne napade s strani sovražnika. S povečanjem globalnega zaupanja tehnologiji je kibernetsko bojevanje ena izmed metod napada, ki izrablja ranljivost držav na kibernetskem področju (Wise geek 2015). Kibernetsko bojevanje štejemo pod asimetrične načine bojevanja, kjer o zmagi ali ranljivosti nasprotnika ne odloča številčnost vojaške moči (Oxford Dictionaries 2015).

2. 4. 3 Bojišče

Bojišče poznamo kot polje na zemlji, kjer se odvija neka bitka. Lahko ga opredelimo tudi kot območje spora, konflikta ali sovražnega delovanja (Dictionary.com). Gre za območje, na katerem prihaja do posrednega ali neposrednega (kadar govorimo o informacijskem bojevanju) boja med sovražniki. Tradicionalno ga razumemo kot del kopnega, morja ali zraka, na katerem se je odvijala vojna oziroma bitka. V današnjem času pa bojišče presega tradicionalno razumevanje in se pojavlja tudi v kibernetskem prostoru, kjer bojišča ne predstavlja več kopno, temveč računalniška oziroma informacijska oprema. Prav tako ne prihaja več do boja zaradi ozemlja ali naravnih virov, ampak se na tovrstnih bojiščih odvija bitka za določene informacije ali vplivanje na le te.

2. 4. 4 Oborožene sile

Oborožene sile ene izmed strank konflikta sestavljajo vse organizirane oborožene sile, skupine in enote, ki so pod poveljstvom odgovornega za ravnanje svojih podrejenih (International Committee of the Red Cross 2015). Gre za silo države ali več držav, ki vključuje kopensko vojsko, letalstvo, mornarico itd. (TheFreeDictionary 2015). Oborožene

sile so sodobnejši izraz, ki postopoma zamenjuje izraz vojska in obsega skupino vojakov, organiziranih za boj (Merriam-Webster 2015).

V primeru Slovenske Vojske oborožene sile sestavljata aktivna in rezervna komponenta. Aktivna komponenta je sestavljena iz profesionalnih članov in jo imenujemo tudi stalna sestava, medtem ko je rezervna komponenta sestavljena iz članov, ki so podpisali pogodbo in s tem postali pogodbena rezerva. Stalno sestavo obsegajo vojaki, podčastniki, častniki in vojaški uslužbenci ter civilne osebe, ki ne opravljajo vojaške službe (Slovenska vojska 2015).

2. 4. 5 Veja oboroženih sil

Veja oboroženih sil predstavlja specializirano stran oboroženih sil za določene naloge in jo lahko imenujemo tudi zvrst. Tako po svetu poznamo kopensko vojsko, vojaško letalstvo, pomorske sile, obalno stražo itd.

Slovenska vojska nima delitve na zvrsti oz. veje, ampak je razdeljena na 9 rodov:

- pehoto,
- oklepne enote,
- letalstvo,
- pomorstvo,
- artilerijo,
- zračno obrambo,
- inženirstvo,
- jedrsko-radiološko-kemično-biološko obrambo in
- zveze (Slovenska vojska 2015).

Glede na koncept skupnih združenih namenskih sil pa v Slovenski vojski obstaja delitev, podobna zvrstem. Tako je Slovenska vojska glede na koncept združenih namenskih sil razdeljena na:

- kopensko komponento,
- mornariško komponento,
- zračno komponento in
- specialne sile (Slovenska vojska 2015).

3 RAZVOJ BOJIŠČ VSE DO KIBERNETSKEGA PROSTORA

Vse od začetka beleženja zgodovine do stoletja nazaj je človeštvo poznalo le dve fizični domeni, na katerih so operativno delovali, torej kopno in morje, od katerih ima vsako specifične fizične karakteristike. Vojskovanje na kopnem je trajnostni vidik človeških izkušenj in predstavlja najstarejšo in najbolj odločno obliko državništva. 3000 let je organizirana družba bila definirana z vrednotami, ki so izhajale in teritorialne zavesti in zaradi česar je zemlja bila glavni geografski prostor, na katerem so se pojavljali konflikti. Tako je vojskovanje na kopnem predstavljalo najbolj celovito obliko konflikta in je poraz ali zmaga predstavljala sinonim za poraz ali zmago države. Velike kopenske sile, kot so Šparta, Rim, Francija, Nemčija in Rusija, so utrpele svoje najbolj odločilne poraze na kopnem.

Operacije na kopnem so igrale ključno vlogo tudi v vojnah pomorskih sil (Atene, Cathage, Benetke, Velika Britanija, Japonska). Sposobnost zmagati vojno na kopnem je bila ključni del vojaške zmogljivosti neke države. Operacije na kopnem so bile večdimenzionalne v smislu povezovanja manevra vojaških formacij in usklajevanja uporabe bojne moči (Gray 2008). Morje je bilo uporabno za ljudi zgolj s pomočjo tehnologije (ladje, galileje ipd.). Velika sprememba se je zgodila stoletje nazaj, ko se je prejšnjima domenama dodala še tretja – zračni prostor (Kuehl 2009).

Z letalstvom se je odprl nov način vojskovanja. V prvih letih 2. svetovne vojne je primarni instrument za zagotavljanje pomorske bojne moči postala letalonosilka. Razlog za to je bil razpon, saj je letalo lahko podalo usklajen napad na 200 milj in več, kar bi bojne ladje lahko storile le na 20 kilometrov ali manj. Vprašanje, ki se je porajalo v letih med 1920 in 1930, je bilo, ali lahko letalo dovolj učinkovito nadomesti bojno ladjo. Vprašanje, ki se je odprlo, je bilo tudi, ali je možno najti sovražnika na zunanjih mejah razpona letal. Sposobnost napasti fiksne tarče, kot sta bila Panamski kanal in Peral Harbor, in s tem doseči presenečenje, je bila prikazana tako v pomorskih vajah kot tudi v bitkah.

Brez poguma in spretnosti letalcev bi lahko rekli, da je učinkovito izvidništvo bil taktični problem vojskovanja in je imelo izreden vpliv na rezultate ključnih bitk v »pacifiškem gledališču« 1942: Koralno morje (4 - 8. maj), Midway (3 - 6. junij), Santa Cruz Islands (26. oktober). ZDA so zmagale zaradi vrhunskega izvidništva in pregleda, zahvaljujoč tudi zračnemu iskalnemu radarju in razbitju japonske kode. Kljub vsemu pa so bile mornariške

letalonosilke orožje odločitve. Čeprav so dvoboji z velikimi nosilkami dobili več pozornosti, so bili zračni napadi iz morja na kopno ključnega pomena pri zagotavljanju nadzora nad morjem. Napadi Britancev pri Tarantu v Italiji (11. novembra 1940), Japoncev na Pearl Harbor (7. decembra 1940) in Američanov v južnem Tihem oceanu v Rabaulu (5. in 11. novembra 1943) in Truku (17. in 18. februarja 1994) so bili tako pomembni, da se končajo, kot so bile vedno bolj senzacionalne bitke med flotami (Encyclopeadia Britannica 2015). Zračna moč je doživljala stalen razvoj od prvega poleta 1903.

Leta 1957[1] se je dodala še četrta domena – vesolje, ki še ni tako vojaško ali komercialno prodorno kot zračni prostor, ampak ima globoke in pomembne povezave do operacij in aktivnosti v vseh drugih okoljih. Vse te 4 zgoraj omenjene domene imajo različne fizične karakteristike, njihova uporaba pa sloni na uporabi tehnologije, ki ustreza tem specifičnim karakteristikam. K tem domenam se je sedaj dodala 5. domena - kibernetski prostor (Kuehl 2009).

Kibernetska moč se je razvila podobno kot zgodnja letalska moč in bo prispevala k skupnemu vojskovanju zdaj in v bližnji prihodnosti. V 1. svetovni vojni so prednosti zračnega izvidništva pripomogle k začetku bojevanja za zračno premoč. Tovrstno izvidništvo je opozorilo na katerakoli gibanja v sovražnem taboru. Kot rezultat zahtev se je pojavilo vprašanje, kako ohraniti zračno premoč z zagotavljanjem informacijske prednosti, ki je izhajala iz opazovanja iz zraka. Na enak način je potekal razvoj kibernetske moči. Velika spodbuda za razvoj kibernetske moči izhaja iz prednosti, ki nastane na tisti strani, kjer lahko opravijo bolj učinkovito kibernetsko poizvedovalno operacijo. Tako kot zračna moč je tudi kibernetska prevlada zmožna delovati prijazno, vendar ni mogoče neposredno razgraditi ali poraziti sovražnikove operacije, kot je to bilo možno z zračno močjo (Bonner III 2014).

Predpostavlja se, da bo kmalu prišlo še do ene domene, katere vojskovanje bo temeljilo na nadzoru človeških misli. Nekateri celo trdijo, da bo 6. domena sposobna oblikovati tudi čustvene in kognitivne odzive. Nadzor nad 6. domeno bo vsekakor pomenil dominacijo nad nasprotnikovimi mislimi tako zunanje (informacijske operacije) kot notranje (Brain-Computer Interface oz. BCI). S takim nadzorom bo človek postal umsko nadzorovano orožje (Little 2012).

[1] 4. oktobra 1957 je Sovjetska zveza uspešno poslala Sputnika v vesolje. To je bil prvi satelit, ki ga je človeštvo poslalo v vesolje.

4 OPREDELITEV KIBERNETSKEGA PROSTORA KOT BOJIŠČA

Vojskovanje se v današnjem času odvija v 5. dimenzijah: tri-dimenzionalnem prostoru (kopno, morje, zrak) ter vesolju. V zadnjem času pa se kot 5. dimenzija vojskovanja začne uveljavljati tudi kibernetski prostor. Pomemben del modernega vojskovanja je postal menedžment kibernetskega prostora. Kljub vsemu pojavljanje kibernetskih groženj še vedno ni v celoti odstranilo tradicionalnih groženj, kot je grožnja z vojaško silo. Kibernetska orožja lahko opredelimo kot vsestranske metode, saj jih je mogoče uporabljati v vseh mogočih varnostnih razmerah (Palokangas 2013, 146). Kibernetski prostor postaja primarno bojišče globalnih sil v 21. stoletju in je kritičen za ustanavljanje modernega vojskovanja. Leta 1980 je prišlo do vzpona napredne informacijske in komunikacijske tehnologije, kar je omogočilo nastanek interneta in kar sedaj imenujemo kibernetski prostor (Mather 2013, 1).

Pobuda, da se kibernetski prostor obravnava kot bojišče, je prišla s strani informacijsko-varnostnih strokovnjakov. Zagovorniki tako tudi zasebnim organizacijam predlagajo sprejetje vojaško naravnanih strategij za obrambo njihove pristnosti na internetu (TechRepublic 2014).

Da kibernetski prostor postaja vedno pomembnejši člen bojevanja in da ga lahko opredelimo kot bojišče, pričajo tudi ukrepi številnih držav na tem področju. Po svetu se je v zadnjem času ustanovilo več organov ter enot za delovanje v kibernetskem prostoru. Tako je bila ustanovljena posebna pan-Evropska delovna skupina znotraj Europola, ki naj bi usklajevala mednarodne preiskave in ukrepe proti grožnji kibernetske kriminalitete v sodelovanju z evropskimi državami in ZDA. Tudi Velika Britanija je vzpostavila vojaške enote za zaščito kritične državne infrastrukture ter za boj proti kibernetskemu kriminalu. Kibernetska obrambna enota je bila ustanovljena v Latviji, medtem ko je tudi francoska vojska podala informacije, da imajo zmogljivosti za kibernetsko vojskovanje. Priprave za kibernetsko vojskovanje in reševanje težav kibernetskega vojskovanja so začele tudi države na Bližnjem vzhodu. Turška vojska je vzpostavila enoto za boj v primeru kibernetske vojne. Jordanija je ustanovila center za kibernetsko bojevanje, s ciljem boriti se proti grožnjam jordanskega finančnega sektorja ter za obrambo nacionalne varnosti. Tudi Iran je ustanovil regionalno poveljstvo kot znak pripravljenosti za boj v kibernetski vojni. Kot del nacionalne obrambne politike tudi Pakistan pripisuje velik pomen kibernetski varnosti in je za to razvil kibernetsko strategijo, z namenom ukvarjanja z napadi ali vdori iz različnih držav v pakistanske kritične infrastrukture. Savdska Arabija je začela z nacionalnim programom kibernetske obrambe, Egipt pa je potrdil Konvencijo z arabskimi državami za boj proti tehnološkim zločinom.

Izjema ni niti Nato. Zveza Nato je napovedala, da namerava na seznam groženj dodati tudi vprašanje kibernetskih napadov, ki bi lahko sprožilo kolektivni odziv. V Evropi je Nemčija napovedala načrte za razvoj temeljitih zakonov za spopadanje s kibernetsko varnostjo. Kuvajt je izrazil željo, da bi povečali kibernetsko varnost, tudi urili uradnike ta soočanje z varnostnimi grožnjami v državi (Tal 2015).

Zagotovljen dostop do kibernetskega prostora je ključnega pomena za nacionalno varnost. Dve izmed pomembnih značilnosti močnega, modernega, industrijskega naroda sta gospodarska blaginja in verodostojna obramba. Sposobnost uporabe kibernetskega prostora je postala nepogrešljiva za doseganje teh ciljev (Armed Forces Journal 2015). Obseg vplivov kibernetskega bojevanja presega geografske in politične meje ter ima ključen pomen za prihodnost nacionalne varnosti države. Hekerji lahko sedaj poplavijo strežnike z zahtevki različnih sistemov, s čimer se paralizirajo operacije in se ustavijo sistemi (Mahmoud 2013, 24).

5 OPREDELITEV KIBERNETSKIH ENOT KOT POTENCIALNE NOVE VEJE OBOROŽENIH SIL

Vse vojaške veje so medsebojno soodvisne in prav ta medsebojna soodvisnost se razteza še na kibernetski prostor. Vojskovanje in obramba v kibernetski domeni sta ključna za ohranjanje operacij na kopnem, vodi in v zraku. Kot rezultat tega vsaka veja potrebuje strokovno izobražene t. i. »kibernetske vojake«, ki so v podporo v primeru napada. Prav zaradi tega mnogi trdijo, da se naj namesto kibernetske divizije v vsaki veji skoncentrirajo vse kibernetske zmogljivosti, kar bo doprineslo tudi mnogo strokovnjakov za različna področja. Večini držav finančni in tehnološki resorji omogočajo, da je njihova vojska »up-to-date« z računalniško opremo. Prav zaradi tega je lahko vojska kompetitivna tudi iz tehnološkega vidika (Solce 2008, 313-315).

Kopenska vojska, mornarica in zračne sile vsebujejo komponente kibernetskega bojevanja, vendar te organizacije obstajajo kot enote, ki skušajo delovati v neprijaznih kulturah, kjer tehnično znanje ni priznano. Revolucija v kibernetskem vojskovanju postavlja današnje vojske pred dejstvo, ki zahteva oblikovanje posebne veje oboroženih sil, ki bi bila enakopravna s kopensko vojsko, mornarico in zračnimi silami. Ustanovitev takšne veje oboroženih sil je pomembna predvsem v boju proti terorizmu, zagotavljanju zmag v

prihodnjih konfliktih in izogibanju tehnološkim presenečenjem. Kulture današnjih vojaških služb so v osnovi nezdružljive s kulturami, potrebnimi za izvajanje kibernetskega vojskovanja. Kibernetika zahteva globoko razumevanje programske opreme, operacijskih sistemov in mrež tako na tehnični kot politični ravni. Globoko razumevanje in spoštovanje kibernetskega bojevanja je s poveljniki teh treh vej oboroženih sil redka (Conti in Surdu 2009, 15-16). Kljub temu da kibernetska moč podpira kopenske operacije in operacije na morju, so zračne operacije tradicionalno vodilni napor v skupnem vojskovanju. Poleg tega je bila sposobnost sodobnih zračnih sil za izvedbo vzporednega vojskovanja prvič uporabljena v vojni v Perzijskem zalivu leta 1991 in je bila kritično odvisna od izkoriščanja kibernetske moči za situacijsko ozaveščenost, komunikacijo in izvidništvo (Bonner III, 2014).

Potrebo po poklicni kibernetski poti poganja operativna potreba in zahteva po učinkovitosti, saj se soočamo s kritičnimi nacionalnimi grožnjami v kibernetskem prostoru, medtem ko danes različni nosilci interesov na kibernetskem področju podvajajo sredstva, izzivajo trenja in nimajo moči, da bi ustanovili enotno skupino za delovanje proti tovrstnim grožnjam.
Da bi se uspešno soočali s številnimi grožnjami v kibernetskem prostoru, morajo današnje vojske vlagati v razvoj voditeljev s tehnološko in strateško vizijo za izgradnjo in vodenje svojih kibernetskih sil. Današnje obdobje kibernetske dimenzije bojevanja ne predstavlja novosti, saj se je vojska že prej morala soočiti z izzivom vključevanja v revolucionarno tehnologijo, ki je zahtevala spremembe v njeni strukturi sil in doktrinarnih temeljev, kot tudi na področju kadrovskega menedžmenta (Arnold in drugi 2013, 1-2).

Reorganizacija vojske v dodatno vejo bi lahko prinesla številne prednosti, saj danes obstaja velika povezanost celotnega sveta, veliko je kritične infrastrukture, kot sta energija ter večnamenske komunikacije, kot tudi ključne korporacije in finančni marketi, ki so veliko bolj ranljivi za kibernetske napade. Oblikovalci politik po vsem svetu se glede tega strinjajo. Na zasedanju vrha NATA septembra 2014 so sodelujoči voditelji izdali skupno izjavo, da »kibernetski napadi lahko dosežejo prag, ki ogroža nacionalno in evroatlantsko blaginjo, varnost in stabilnost. Njihov napad je lahko zelo škodljiv v sodobnih družbah, in sicer kot konvencionalni napad«.

Prišlo je tudi do strinjanja, da je obramba pred kibernetskimi napadi ena temeljnih točk kolektivne obrambe, tako so hkrati tudi opozorili potencialne sovražnike, da lahko kibernetski

napad sproži Natov 5. člen[2]. Težave, povezane s kibernetsko varnostjo postajajo vedno bolj kompleksne v obeh organizacijah. Leta 2011 je NATO sprejel Policy on Cyber Deence of the Alliance and elaborated a detailed plan of the deveopment of capabilities. Kljub vsemu še vedno obstaja problematika glede pravnih okvirov, saj se težave pojavijo že pri uporabi prava pri kibernetskih napadih. Kazensko civilno pravo in obveščevalne agencije so imele večji del odgovornosti, saj so se morale odzvati na napad in razviti sposobnosti za protinapad, v primeru, da so pozvani v ta namen. Vendar pa imajo v primeru resnih kibernetskih napadov na visoki rani, ki bi lahko sprožili Natov 5. člen, potrebna sredstva samo državni akterji (McCoy 2015).

Vedno večjo potrebo po tovrstnih silah dokazujejo tudi primeri hekerskih napadov, kot sta npr. napad na Iranski jedrski program in «Denial-of-Service« v Estoniji.

5. 1 Napad na iranski jedrski program

Virus, imenovan Stuxnet, je onemogočil delovanje objekta Natanzu in Fordowu, ko je virus računalnike prisilil v ponavljajoče igranje skladbe »Thundrstruck« skupine AC/DC pri največji možni glasnosti (Fritzgerald 2012). Neimenovani iranski znanstvenik je po e-pošti kontaktiral Mikko Hyponena, vodjo urada za raziskovanje finskega varnostnega podjetja F-Secure, z namenom, da ga obvesti o dogajanju. Druga e-pošta se je sklicevala na omenjeno skladbo, ki naj bi se predvajala na več delovnih mestih sredi noči.

Primer tovrstnega napada se ni zgodil prvič, saj je iranski jedrski program bil že v preteklosti tarča zlonamernih programov. Uničujoči Stuxnet črv je do zdaj prizadel okoli 60% računalnikov v Iranu in je odgovoren za uničenje centrifug v jedrskem objektu Nantaz. Iran je potrdil, da se je delo na objektu ustavilo večkrat zaradi tehničnih vprašanj in da je uporaba centrifuge padla za 30% (Dailymail 2012).

---

[2] *Pogodbenice soglašajo, da se oborožen napad na eno ali več pogodbenic v Evropi ali Severni Ameriki šteje za napad na vse pogodbenice, in zaradi tega soglašajo, da bo v primeru takega oboroženega napada vsaka od njih ob uresničevanju pravice do individualne ali kolektivne samoobrambe, ki jo priznava 51. člen Ustanovne listine Združenih narodov, pomagala tako napadeni pogodbenici ali pogodbenicam s takojšnjim individualnim in z drugimi pogodbenicami dogovorjenim ukrepanjem, ki se ji zdi potrebno, vključno z uporabo oborožene sile, da se ponovno vzpostavi in ohranja varnost severnoatlantskega območja.*

Vsak tak oborožen napad in vsi posledično sprejeti ukrepi se takoj sporočijo Varnostnemu svetu. Taki ukrepi prenehajo, ko Varnostni svet ukrene, kar je potrebno za ponovno vzpostavitev in ohranjanje mednarodnega miru in varnosti. (Severnoatlantska pogodba 1949, 5. člen)

5. 2 »Denial-of-Service« v Estoniji

Aprila 2007 je Estonija doživela prve kibernetske napade na svetu, ki so po obliki bili porazdeljeni v tri-tedenske valove t. i. denial of service napada, ki so ohromili državno informacijsko tehnologijo. Poglavitni vzrok za napad naj bi bila odstranitev spomenika bronastega vojaka, obstajali pa so tudi drugi dejavniki, ki so prispevali k ranljivosti socialno-politične sfere Estonije. Ti drugi dejavniki so se navezovali predvsem na zgodovino odnosov med Estonijo in Rusijo.

Kibernetski napadi so se pričeli 26. aprila 2007 ob 22. uri, ko so neznani napadalci začeli obširne napade zoper estonsko vlado. Napadi so prvih 24 ur ostali neopazni, vse do nezmožnosti obrambnega ministra, da se prijavi na spletno stran predsednika vlade. Hekerji so bili najprej usmerjeni prav na to spletno stran, nato so svoje napade začeli širiti na druge spletne strani političnih strank in vlade, vključno z uradno stranjo estonskega parlamenta. Do konca prvega tedna so napadi popolnoma ohromili tovrstne spletne strani.

Naslednji teden se je seznam ciljev razširil na večje publiciste, ki so z večanjem števila napadov postale nedostopne. Ko so odkrili, da se večina sistemov, ki povzročajo napade, nahaja izven Estonije, so se uredniki zatekli k blokadi vsega dohodnega mednarodnega prometa. Mediji tako s svojimi objavami niso mogli obvestiti ostalih držav, kaj se dogaja v njihovi državi. Kibernetski napadi so se nadaljevali vse do 9. maja. Ob polnoči po moskovskem času je Estonija doživela najsilovitejši napad do tedaj – več kot 4 milijone paketov podatkov poslanih na sekundo. V tem napadu so hekerji osredotočili svoja prizadevanja na estonski bančni sistem. 10. maja so napadi prisilili Hansabank[3], da zapre svoje internetne operacije.

Napadi so za seboj pustili obsežno opustošenje. Hekerji so napade organizirali z uporabo spletnih dnevnikov, spletnih revij in rusko govorečih klepetalnic. V treh tednih je število ciljnih strani zraslo v stotine vladnih strani, bančnih sistemov, medijskih hiš in strani uglednih estonskih univerz, ki so bile sistematično napade in posledično tudi zaprte. 19. maja so bili napadi ustavljeni in s tem se je končala tudi prva svetovna kibernetska vojna (Richards 2009).

[3] Državno največjo banko in pionirja razvoja mnoge informacijske tehnologije v 90. letih

6 PRIMERJAVA IZBRANIH DRŽAV GLEDE REKRUTIRANJA IN DELOVANJA KIBERNETSKIH ENOT

6. 1 Slovenija

Slovenska vojska je na svoji spletni strani leta 2014 objavila Vabilo k sodelovanju kot strokovnjak za kibernetsko varnost. V svoje vrste so povabili strokovnjake s področja kibernetske varnosti, ki bi svojo dolžnost opravljali v rezervni sestavi. Ti strokovnjaki bi delovali na področju ukrepov za zaščito in varovanje informacij. Na razpis so se lahko prijavili kandidati, ki:

- imajo državljanstvo Republike Slovenije,

- nimajo dvojnega državljanstva,

- so mlajši od 50 let,

- imajo univerzitetno izobrazbo in ustrezna znanja z določenih področij,

- so nekaznovani in privolijo v varnostno preverjanje,

- niso napoteni na delo, usposabljanje ali šolanje v tujino za več kot tri mesece,

- nimajo priznane pravice do ugovora vesti vojaške dolžnosti (Postanivojak.si 2014).

Prijave na razpis je bilo mogoče oddati do 30. junija 2014, vendar enota še danes ni vzpostavljena.

Slovenska vojska se je odločila za vzpostavljanje kibernetske obrambe skladno s ciljem sil E5308N: Information Assurance and Cyber Defence. Znotraj projekta Nata Smart Defence tako poteka delavnica Multinational Cyber Defence Education and Training Project. Februarja 2015 je bil podpisan prvi dokument NATA glede izobraževanja na tem področju (Center vojaških šol 2015).

6. 2 Severna Koreja

Digitalni razkorak med bogatimi in revnimi je verjetno najbolj izrazit v Severni Koreji. Člani specializirane enote imajo posebne računalniške veščine, medtem ko velika večina prebivalstva Severne Koreje še ni nikoli videla računalnika, kaj se šele prijavila na splet. Nekdanji operativec nacionalne obveščevalne službe pravi, da imajo celo vojsko hekerjev, ki so usposobljeni za kibernetsko vojno proti sovražnikom Severne Koreje. Poudarek, ki ga

Severna Koreja polaga na kibernetsko vojskovanje, je tako dobro prikrit in skrit, da se le redki zavedajo, da obstaja kibernetska enota. Severna Koreja bi naj po besedah Južne Koreje imela 6000 pripadnikov kibernetskih vojakov, katerih naloga je motenje vojske in vlade Severne Koreje (Forbes 2015).

Glavne kibernetske operacije Severne Koreje potekajo pod izvidovalnim generalnim predsedstvom**,** ki samo po sebi spada pod Ministrstvo ljudskih oboroženih sil. RGB že leta deluje v tradicionalnem vohunjenju in tajnih operacijah in ima izoblikovani dve kibernetski diviziji, imenovani Unit 121 in Office 91. Za Office 91 se smatra kot poveljstvo »hekerskih« operacij, čeprav je večina hekerskih operacij bila strojena s strani Unit 121, ki deluje zunaj Severe Koreje (Williams 2015).

6. 3 Velika Britanija

Maja 2013 so skupne sile kibernetske skupine sklenile zagotoviti obrambno kibernetsko kapaciteto, ki vključuje tudi skupno kibernetsko rezervo. Ta rezerva nudi podporo Skupni kibernetski enoti (Corsham), skupnemu kibernetskemu centru (Cheltenham) in tri-storitveni (tri-storitveni) enoti za zavarovanje informacij. Za kibernetsko enoto so primerni kandidati, ki kot redni kadri zapuščajo storitev, sedanji in nekdanji rezervisti ter posamezniki, ki v preteklosti niso služili vojaškega roka. Primarne zahteve, da lahko kandidat postane član kibernetske enote, so:

1. posedovanje preverljivih kibernetskih sposobnosti,
2. starost 18 let ali več,
3. državljanstvo VB
4. življenje v VB zadnjih 5 let,
5. zavezanost k minimalnemu usposabljanju,
6. pripravljenost opravljati in uspešno opraviti postopek varnostnega preverjanja,
7. žrtvovati prosti čas ob koncu tedna, z namenom podpreti poslanstvo obrambe kibernetske varnosti (Joint Forces Command homepage 2015).

Rezervisti se morajo zavezati k vsakoletnemu usposabljanju za obdobje od 19 do 27 dni in je sestavljeno iz:

- številnih nalog, ki se izvajajo za vikende skozi celotno leto;

- obdobja stalnega usposabljanja, običajno ne več kot 2 tedna (Joint Forces Command homepage 2015).

6. 4 Tajska

Tajska vojska je po poročanju medijev 9. februarja 2015 začela z zaposlovanjem strokovnjakov, ki bi delovali v kibernetskih enotah tajske vojske in se bodo ukvarjali s kibernetsko varnostjo. Polkovnik Chatchai Chaikaseam, direktor enote, je na nedavni konferenci z naslovom Meet the Hacker 2015 v Bangkoku pokazal, da vojska rekrutira 7 častnikov, ki bodo vodili njegovo enoto za kombinirane vojaške operacije, ki naj bi začela delovati že 15. februarja 2015. Dejavnosti enote naj bi vključevale prodorna testiranja, forenzične digitalne raziskave ter revizijo kibernetske varnosti (Tal, 2015). Kibernetska enota bo delovala pod Direktoratom za skupne operacije, pod kraljevo tajsko vojsko. Prijave za delovna mesta so se odprle 15. februarja 2015 na spletni strani Direktorata za skupne operacije. Razpisana so bila naslednja delovna mesta:

- uradniki za digitalno forenziko: 1,

- uradniki za testno vdiranje: 3,

- kibernetski varnostni revizijski uradniki: 1,

- podčastnik za testno vdiranje: 1,

- podčastnik za digitalno forenziko: 1.

Tajska vojska sledi ameriškemu modelu v okviru strateškega poveljstva ZDA (Prachatai 2015).

6. 5 Latvija

Februarja 2014 je Latvija najela prvih 13 državnih kibernetskih »varuhov«. Delujejo v sklopu Kibernetske obrambne enote in pomagajo latvijski vladi in vojski pri odzivu na informacijske grožnje v primeru konflikta (Gelzis 2014). Enota je bila ustanovljena z namenom privabiti visoko kvalificirane strokovnjake informacijske tehnologije za izpolnjevanje nalog državne obrambe v svojem prostem času. Za vstop v enoto je potrebno izpolniti naslednje kriterije:

- znanje in spretnosti, potrebne za izpolnjevanje nalog v enoti;

- domoljubje in želja po zagotovitvi prispevka h krepitvi stanja varnosti;
- skladnost delati z državno tajnostjo;
- inovativni način razmišljanja ter sposobnost prilagajanja na spreminjajoče se informacijsko tehnologijo in okolje;
- sposobnost, da namenijo 1,3 dni na mesec za usposabljanje in izpolnjevanje storitev v virtualnem prostoru.

Delo enote je organizirano tako v virtualnem prostoru kot tudi z izvedbo rednih srečanj. Sodelujejo tudi na nacionalnih in mednarodnih usposabljanjih. Glede na operativne potrebe ali specializacije se strokovnjaki razdelijo v skupine, kot so npr.: skupina za hitro odzivanje ali kibernetsko laboratorijsko osebje. Oblikovanje zmogljivosti je planirano za obdobje 5 let:

- z začetkom leta 2015 bo enota dosegla začetne operativne sposobnosti,
- z začetkom leta 2018 bo enota dosegla polne operativne sposobnosti.

Nadaljnje akcije so sestavljene iz:

- zavezanosti izvajanja implementacijskih korakov, zapisanih v dokumentu za formacijo enote;
- študije in uporabe mednarodnih in nacionalnih izkušenj z namenom izoblikovati v podrobnosti ter razvijati idejo o kibernetski obrambni enoti (National armed forces cyber defence unit (CDU) concept 2013).

6. 6 Združene države Amerike

Februarja 2015 so ZDA izbrale 170 kandidatov za kibernetsko vejo oboroženih sil. Vojaško kibernetsko poveljstvo bo uradno premeščeno v Fort Gordon leta 2019, kibernetska šola pa se bo tam odprla že avgusta. Teh 170 izbranih kandidatov je zaposlenih vojakov, ki imajo čin od podporočnika do polkovnika. V kibernetsko enoto so bili premeščeni z drugih področij vojske. Drugi krog selekcije naj bi potekal poleti 2015. Premestitev kibernetskega poveljstva v Fort Gordon, z drugimi spremembami, bo prinesla in vključila nekje 5.000 vojaških in civilnih oseb z njihovimi družinami v roku naslednjih 4 let (Kauffman 2015). Vojaška kibernetska operativna sila je rasla eksponentno od septembra 2013 in je dosegla 25 od 41 (načrtovanih) ekip za operativno zmogljivost (Vergun 2015).

7 USTANAVLJANJE SPECIALIZIRANIH ENOT ZA SOCIALNA OMREŽJA

7. 1 Velika Britanija

Britanska vojska je začela z ustanavljanjem enote vojakov za boj z uporabo socialnih omrežij oz. medijev. Tako so oblikovali enoto »kreativnih« vojakov, ki bodo imeli nalogo, da se vojskujejo z uporabo nekonvencionalnih metod. Člani 77. brigade so bili usposobljeni za uporabo gverilskih taktik in bodo strokovnjaki za operacije psihološkega bojevanja. Britanska vojska upa, da bodo z uporabo nesmrtonosnih tehnik vplivali tudi na tradicionalnem bojišču, vključno z uporabo socialnih omrežij, ki so odraz digitalne dobre. Za enoto se uporablja vzdevek »Twitter troops« (Bunkall 2015). Operativno telo brigade bo sestavljalo 1.500 - 2.000 pripadnikov oboroženih sil. Vsak bo v brigado doprinesel svojo specifičnost drugih vej, kot so kopenska vojska, zračne sile in mornarica. Med njimi bodo tudi strokovnjaki za psihološke operacije, medijske informacijske informacije in podporna skupina. Te skupine pripadnikov se bodo večinoma ukvarjale s tem, kako uporabiti besede in ideje nad nasilnimi sredstvi. Približno 42% brigade naj bi bilo sestavljene iz rezerve oz. »vikend bojevnikov«. Brigada simbolizira priznanje, da trda moč in vojaška sila nista več edini orodji, ki sta potrebni v sodobnem vojskovanju. To je postalo še posebej očitno v vojni v Afganistanu in Iraku. Izkušnje s teh dveh območij govorijo, da je potrebno oblikovati pravo zgodbo, ki bo dosegla pravo občinstvo. Kaj naredi to brigado drugačno od ostalih, je nenasilnost in nesmrtonosnost. Okolje bo oblikovala s pomočjo informacij, pridobljenih na spletu, v nasprotju z orožjem in strelivom. Takšne brigade se lahko uporabljajo za podporo izgradnji miru, za humanitarne intervencije ter za neuspele države (Flint 2015).

7. 2 Združene države Amerike

Specialna enota ZDA, ki je znana po svojih zelo preciznih tajnih operacijah v nevarnih območjih, bo začela vplivati na socialne medije kot del prizadevanj v boju proti terorizmu in z reagiranjem na druge tekoče konflikte.

Te elitne enote načrtujejo uporabo socialnih medijev na 5 praktičnih načinov:

1. zbiranje metapodatkov in drugih vidikov »digitalnih odtisov«, ki se nanašajo na sporočila, objavljena na socialnih medijih s strani sovražnika z namenom izslediti njegovo gibanje;

2. opazovanje spletnih prizadevanj rekrutacije s strani različnih terorističnih skupin, v prizadevanju, da bi bolje ocenili potencialne ravni ogroženosti;
3. izdajanje za morebitne kandidate rekrutiranja, z namenom slediti terorističnim akterjem ali posameznikom do določene mere, v upanju infiltrirati skupino ter zbiranje obveščevalnih podatkov o načrtih, ciljih in notranjem delovanju terorističnih skupin;
4. spremljanje socialnih medijev za dokazovanje načrtovanih srečanj sovražnikovih skupin ali napadov na civiliste ter zaveznike;
5. zbiranje dokazov in njihova predložitev vojaškim nadrejenim, s ciljem prejemati ustrezne smernice ali dovoljenja za ustrezne vojake, odgovore na sedanje ali prihodnje operacije ameriških zaveznikov (Martin 2015).

8 ZAPLETENOST PROCESA REKRUTACIJE

Izbira kadra je ključnega pomena za vsako organizacijo. Vsaka organizacija teži k izbiri najboljših strokovnjakov s svojega področja in si s tem pridobiva prednost pred drugimi organizacijami. Velikokrat pa se organizacije ne zavedajo kolikšno količino znanja nosi v sebi posamezni strokovnjak. Čeprav bi vsak zaposleni moral delati v dobrobit organizacije pa lahko svoje znanje uporabi tudi v drugo skrajnost. Svoje znanje lahko usmeri zoper organizacijo za katero dela ali so ga pa tja poslali drugi z namenom kraje podatkov, škodovanju organizaciji, itd. Programiranje in poznavanje programske opreme so vedno bolj zaželena kompetenca posameznika, pomembna predvsem pri iskanju kadra s področja informacijskega bojevanja. Velikokrat se zgodi da vodilni, ki zaposlujejo tovrstni kader nimajo znanja s področja programiranja in informatike, kar lahko predstavlja idealno priložnost za hekerje, ki s svojo prisotnostjo v timu določene organizacije želijo pridobiti informacije ali zgolj onemogočiti delovanje organizacije.

Primer zapletenosti procesa pridobivanja osebja je Snowden. Snowden je kot analitik bil del uhajanja podatkov o programih nadzora ZDA in Velike Britanije. V ZDA so ga obtožili kraje državne lastnine, nepooblaščenega sporočanja državnih obrambnih informacij in namerne komunikacije glede zaupnih podatkov. Vprašanje ki se pojavlja je, koliko analitikov oz. ostalih strokovnjakov s področja informatike deluje na podoben način kot Snowden in so trenutno zaposleni v organizacijah, ključnih za nacionalno varnost.

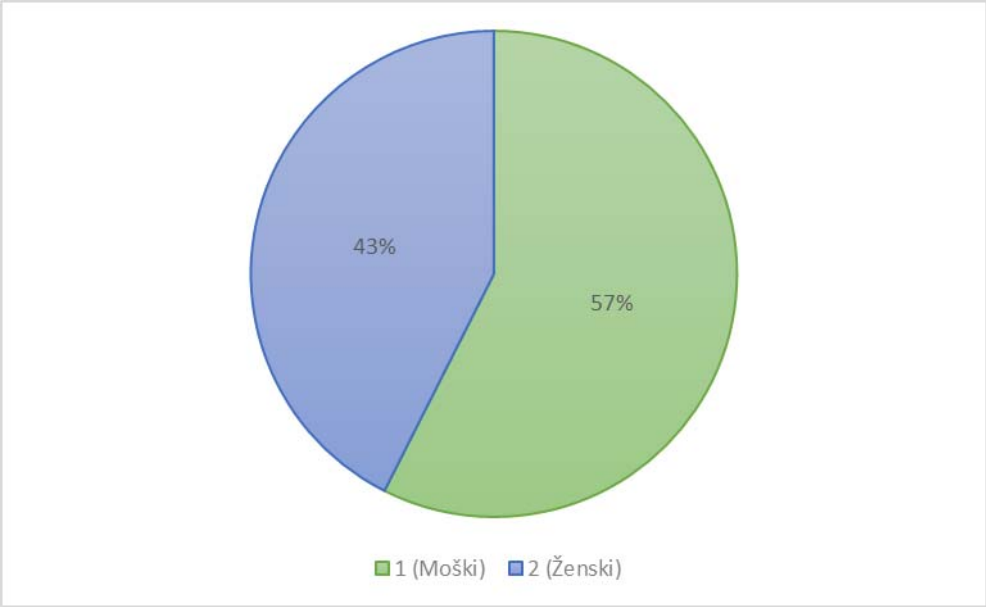
Julija 2015 se je tovrstno uhajanje informacij pripetilo italijanskemu podjetju Hacking Team, ki proizvaja tajno kibernetsko orožje za vladne stranke po vsem svetu. Več kot 400 gigabajtov

internih podatkov je našlo svojo pot na internet. Doslej razkriti dokumenti so razkrili ključne stvari o njihovih strankah in poslih (Defense One 2015).

9 ANKETNI VPRAŠALNIK O KIBERNETSKIH ENOTAH

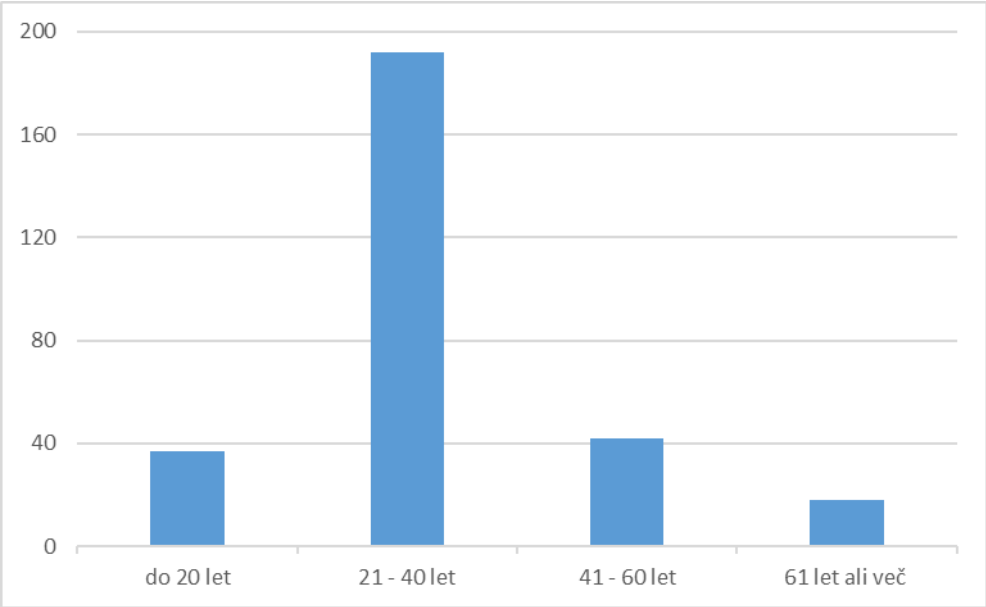
Anketni vprašalnik, ki ga je izpolnilo 289 oseb, je sestavljen iz 12 vprašanj. Vprašalnik se nanaša predvsem na poznavanje tako kibernetskega prostora kot tudi seznanjenosti z ustanavljanjem kibernetskih enot ter orožij, s katerimi operirajo. Prvo vprašanje (slika 1. 1) je demografskega tipa. Tako je na vprašalnik od 289 oseb odgovorilo 166 moških (57%) in 123 žensk (43%).

Slika 1. 1: Spol anketirancev v odstotkih.



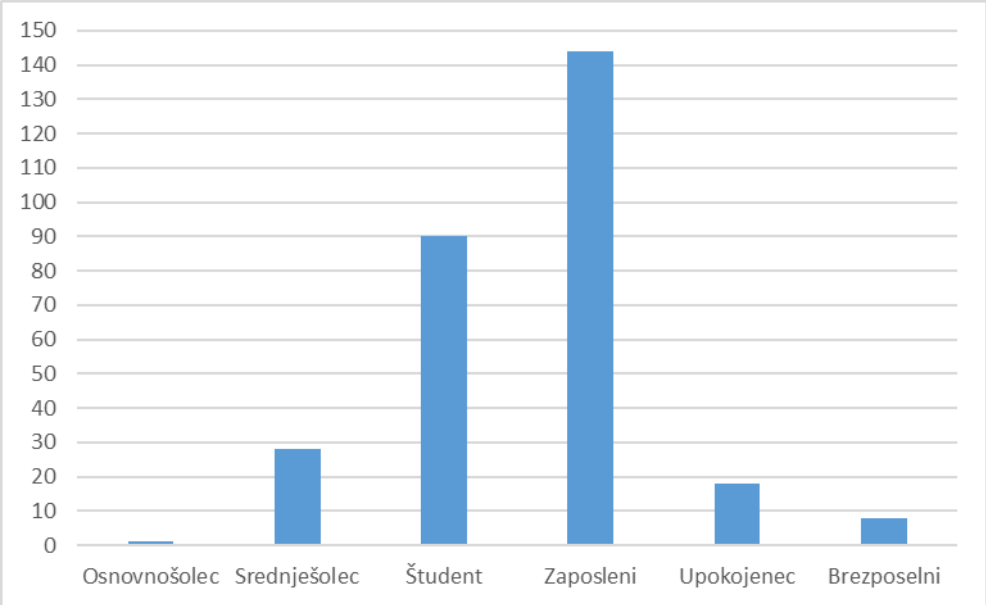
Drugo vprašanje se je nanašalo na starost anketirancev (slika 1. 2). Starostno sem jih razporedila v 4 starostne skupine. V prvo skupino spadajo osebe do 20 let, ki predstavljajo 37 (13%) anketirancev od 289. Naslednja skupina, ki je največja, so osebe med 21 in 40 let. Ta skupina predstavlja 192 (66%) vseh anketirancev. Naslednjo skupino, osebe med 41 in 60 let, predstavlja 42 (15%) anketirancev. Zadnja skupina se nanaša na osebe starosti 61 let ali več in predstavlja 18 oseb (6%) od 289 anketiranih.

Slika 1. 2: Starostne skupine anketirancev.



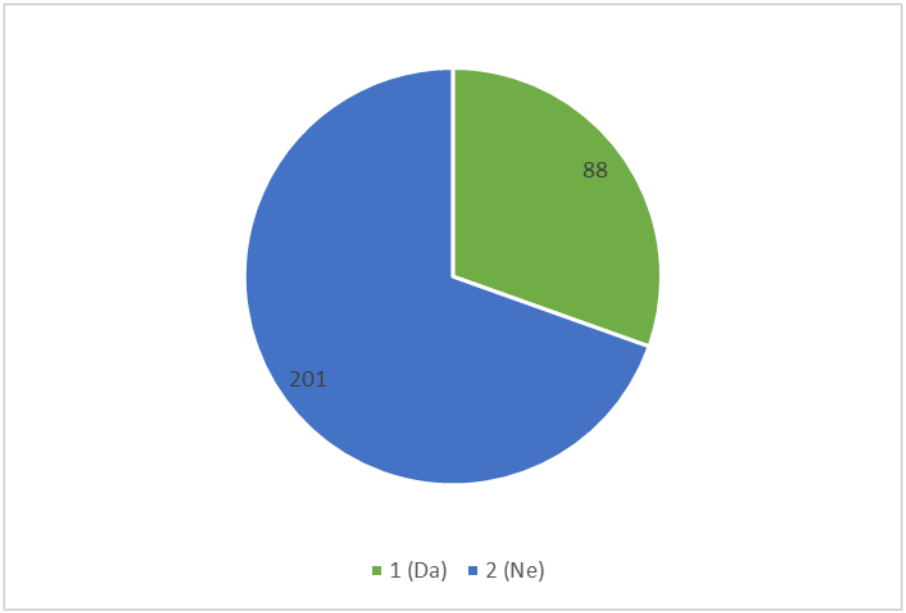
Tretje vprašanje se nanaša na trenutni status anketirancev (slika 1. 3), kjer največjo skupino predstavljajo zaposleni s 141 osebami, sledijo študentje, srednješolci, upokojenci in nazadnje brezposelni.

Slika 1. 3: Trenutni status anketirancev.



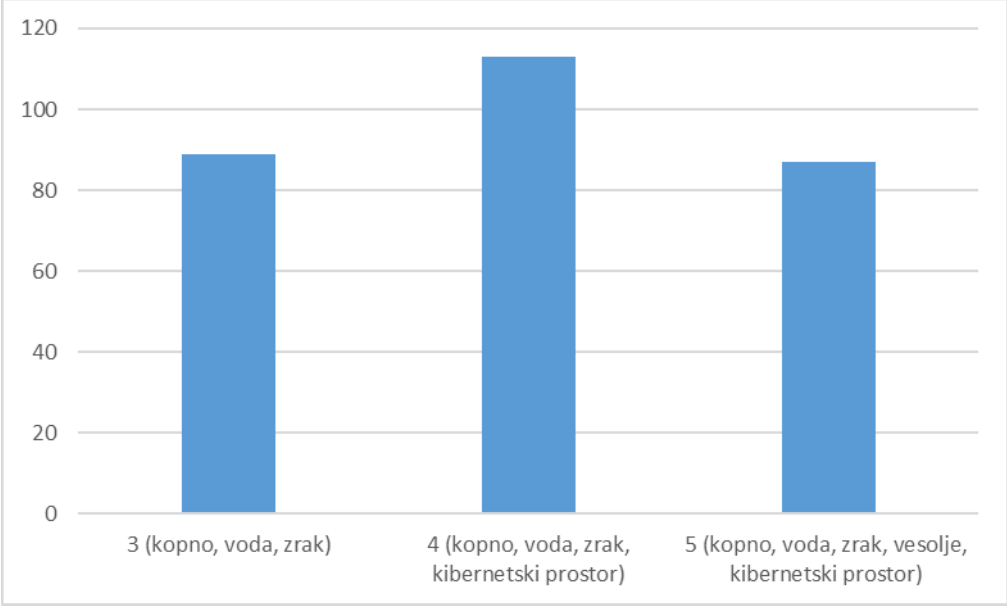
Naslednje vprašanje se je nanašalo na seznanjenost z novimi načini vojskovanja (slika 1. 4). Rezultati so pokazali, da 201 anketiranih (70%) ni seznanjenih z novejšimi načini vojskovanja.

Slika 1. 4: Prikaz seznanjenosti z novejšimi načini vojskovanja.



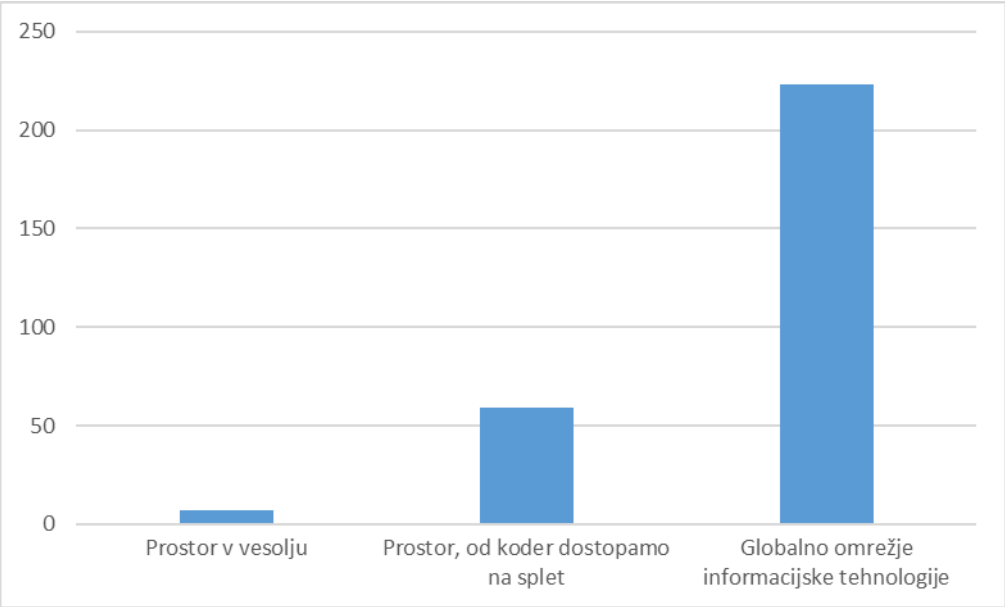
Zanimivo dejstvo, ki se je pojavilo med analizo odgovorov, je, da kar 31% anketiranih med dimenzije vojskovanja danes še vedno prišteva zgolj kopno, vodo in zrak. K prej omenjenim dimenzijam 39% prišteva še kibernetski prostor. Le 87 oseb (30%) meni, da danes obstaja 5 dimenzij vojskovanja (slika 1. 5).

Slika 1. 5: Število dimenzij vojskovanja po mnenju anketiranih.



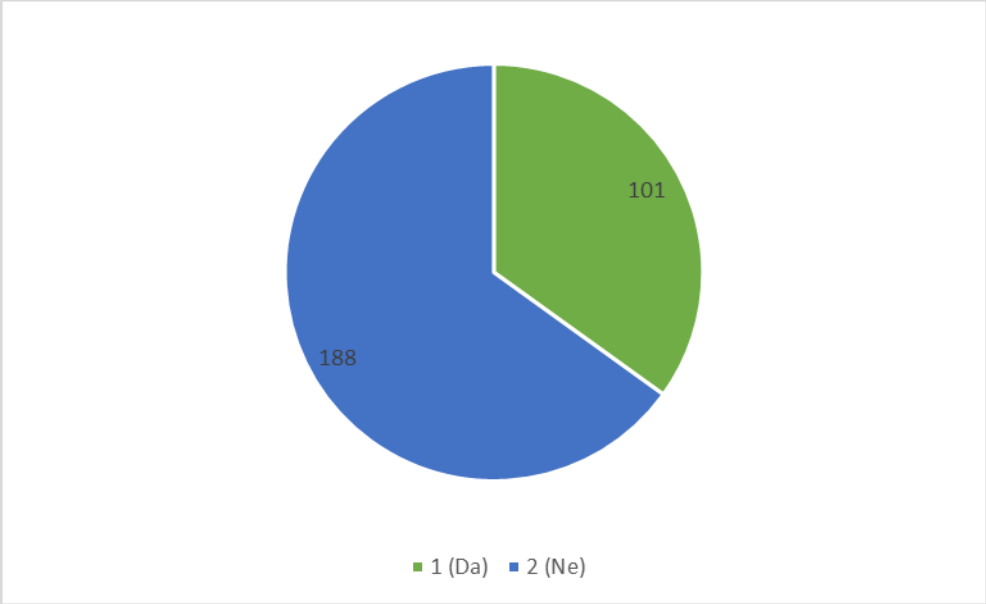
Čeprav ljudje niso toliko seznanjeni z dimenzijami in novejšimi načini vojskovanja, pa večina prepozna pojem kibernetski prostor (slika 1. 6).

Slika 1. 6: Seznanjenost s pojmom kibernetski prostor.



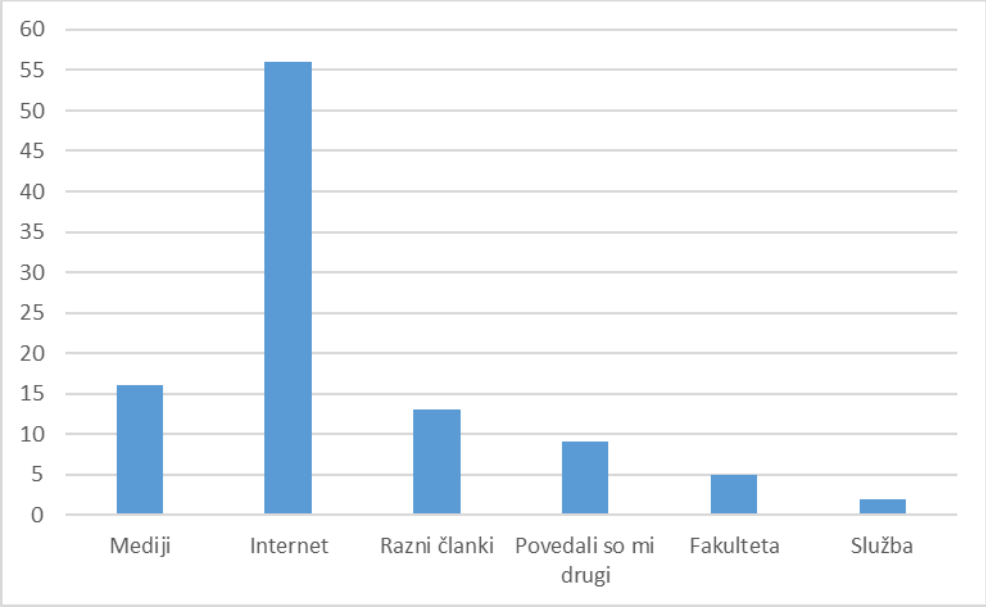
Še večji razkorak se je pokazal pri vprašanju »*Ali ste že slišali za pojem kibernetsko vojskovanje?*«, pri katerem je razvidno, da 65% anketirancev še ni slišalo za omenjeni pojem. Za 35% anketirancev, ki so odgovorili z DA, sem zastavila še 2 dodatni vprašanji, in sicer: najprej sem jih prosila naj mi s svojimi besedami opredelijo pojem, kasneje pa še naj navedejo, kje so ga prvič zasledili. Rezultati so pokazali, da so tisti, ki so s svojimi besedami opredelili kibernetsko vojskovanje, dobro seznanjeni s tematiko (slika 1.7).

Slika 1. 7: Poznavanje kibernetskega vojskovanja.



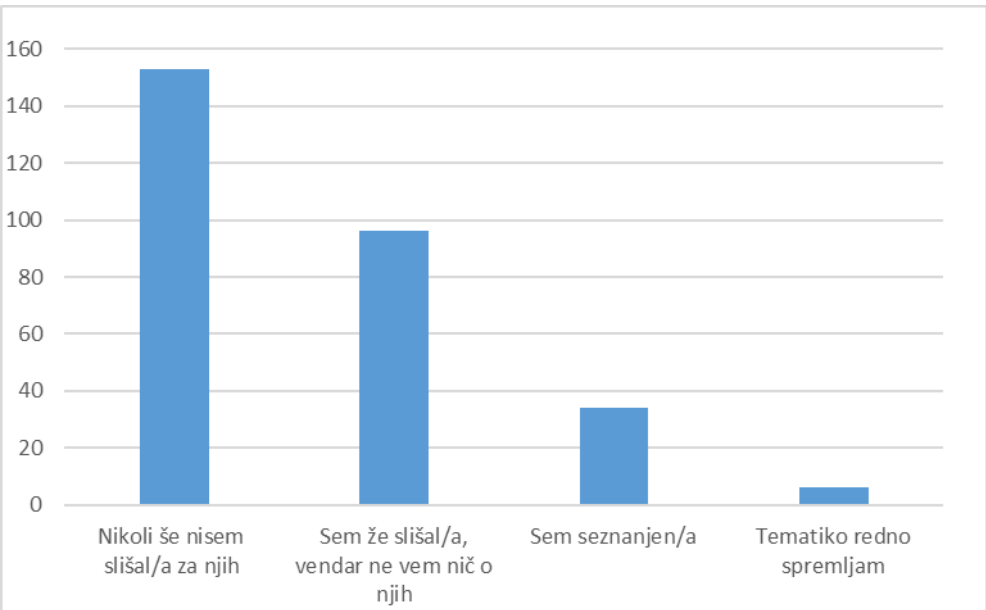
Med viri, kjer so anketirani prvič zasledili pojem kibernetsko vojskovanje, prevladuje internet, sledijo mediji in različni članki. Nekaj jih je pojem prvič zasledilo na fakulteti in v službi (slika 1.8).

Slika 1. 8: Viri, kjer so se anketiranci prvič srečali s pojmom kibernetsko vojskovanje.



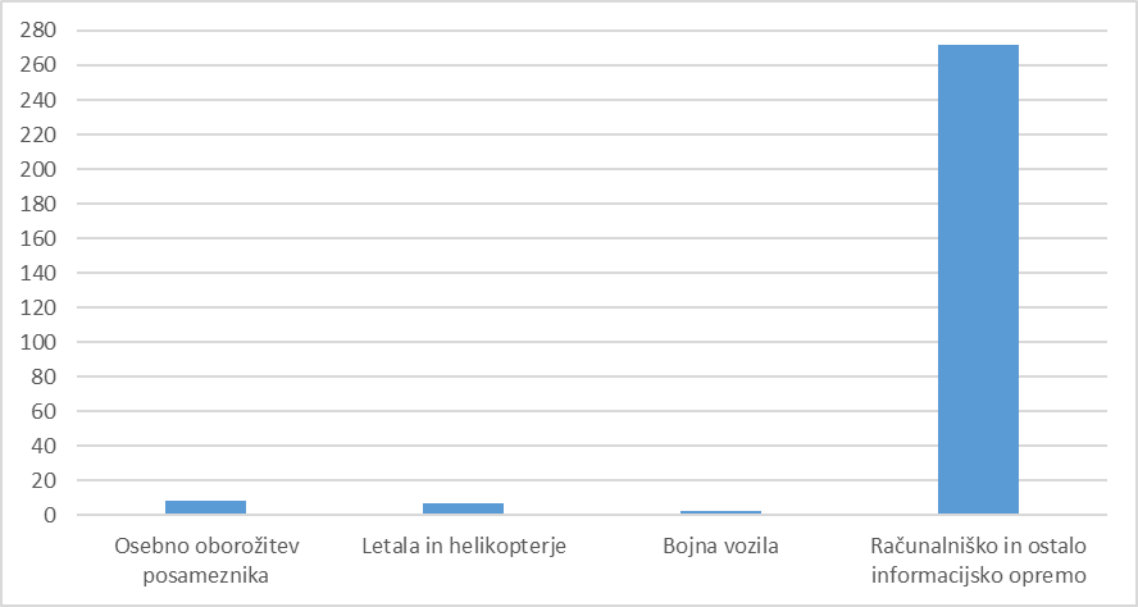
Večina anketirancev še ni slišala za ustanavljanje tovrstnih enot, kar lahko povežemo že z nepoznavanjem pojma kibernetsko vojskovanje in s tem povezane tematike. Velik procent anketirancev je za pojem že slišalo, vendar kaj določenega o njih ne vedo povedati. Zanimivi sta predvsem zadnji dve skupini, iz katerih je razvidno, da tematiko pozna in jo celo redno spremlja kar 14% anketirancev (slika 1.9).

Slika 1. 9: Seznanjenost z ustanavljanjem kibernetskih enot.



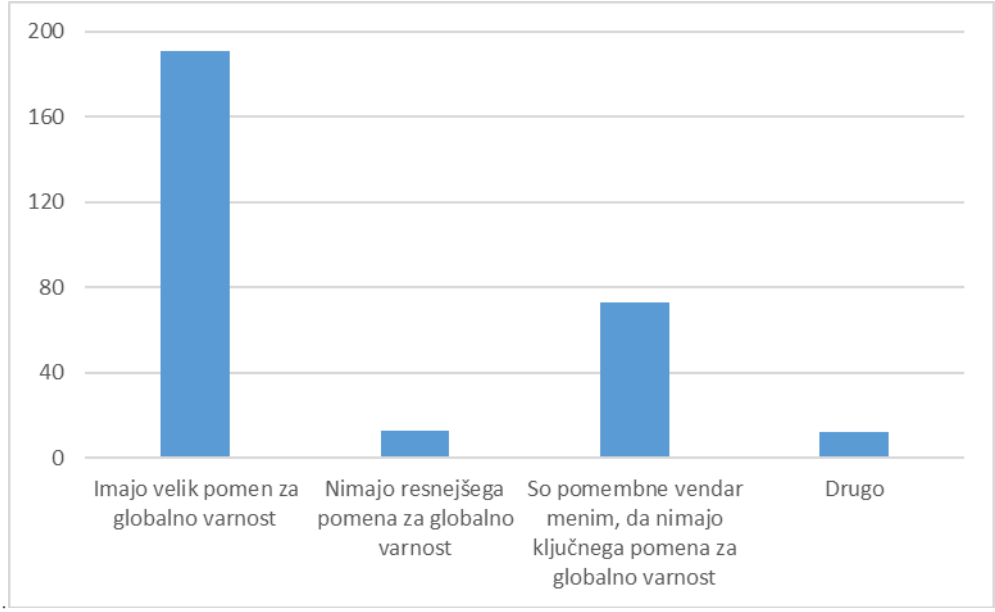
Čeprav prihaja do dileme pri vprašanju, kaj je kibernetski prostor in koliko dimenzij vojskovanja poznamo danes, pa pri vprašanju o orožju, ki ga uporabljajo kibernetske enote, ni dvoma s strani anketirancev (slika 1. 10).

Slika 1. 10: Orožje, ki ga po mnenju anketiranih uporabljajo kibernetske enote pri svojih nalogah.



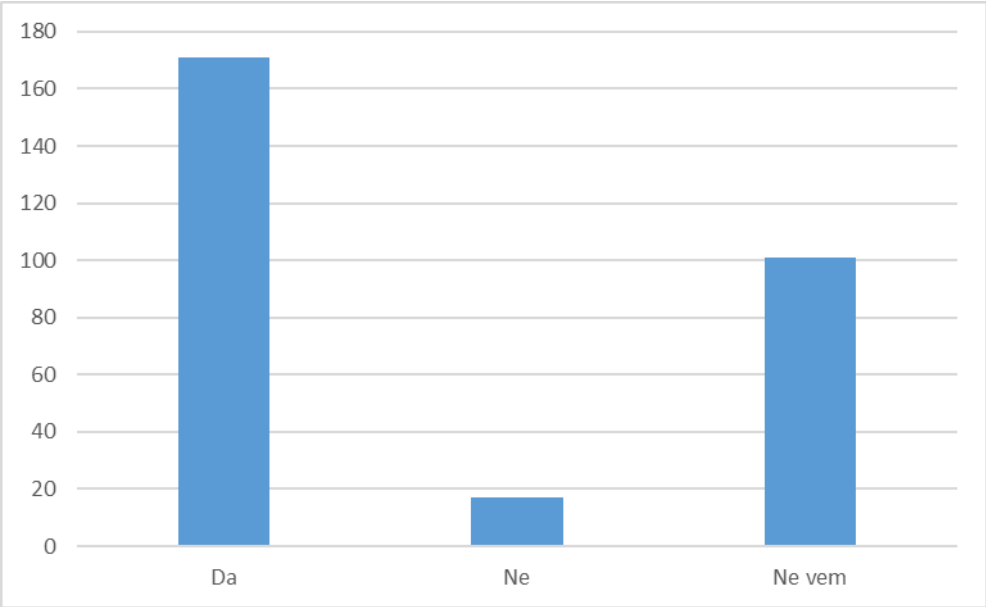
Mnenje o pomembnosti operacij, povezanih z globalno varnostjo, se deli predvsem na osebe, ki menijo, da imajo tovrstne operacije velik pomen za globalno varnost, in med osebe, ki menijo, da operacije sicer so pomembne, vendar ne igrajo ključnega pomena pri globalni varnosti (slika 1. 11).

Slika 1. 11: Stopnja pomembnosti operacij, povezanih s kibernetsko varnostjo



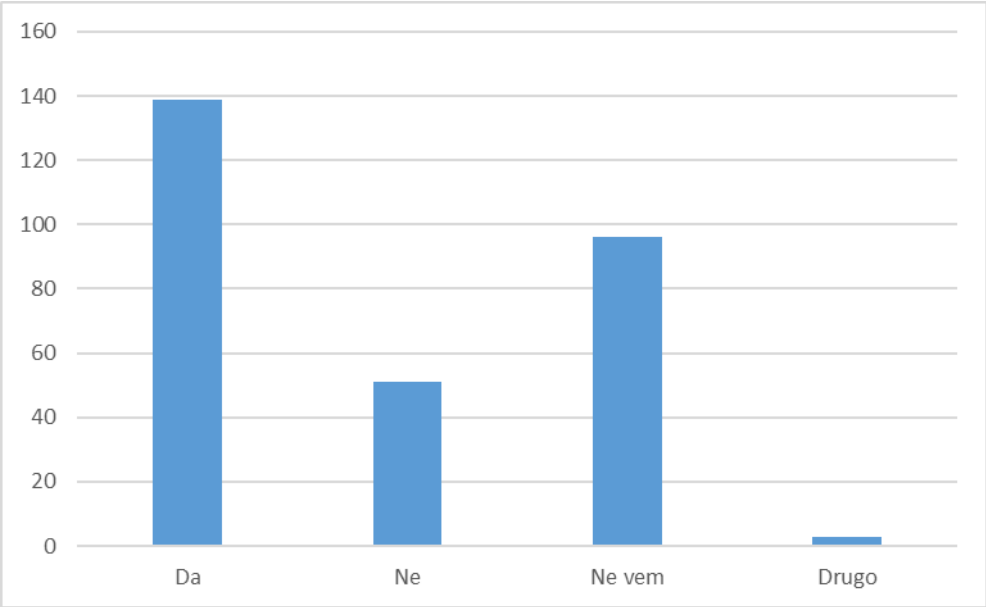
Naslednje vprašanje se je nanašalo na možnost omejitve operacij nasprotnika s kibernetskimi enotami in njihovimi operacijami. Velika večina jih tako misli, da je s tovrstnimi enotami in njim pripadajočimi operacijami možno omejiti operacije nasprotnika, rahlo zaskrbljujoče pa je dejstvo, da jih kar 33% ne ve, ali operacije imajo moč oz. ne znajo izoblikovati mnenja o njih. Zakaj je odstotek oseb, ki se ne znajo opredeliti tako, lahko delno pripišemo nepoznavanju tematike, delno pa lahko vzroke iščemo tudi drugje (slika 1. 12).

Slika 1. 12: Možnost omejitve operacij nasprotnika s kibernetskimi enotami in njihovimi operacijami.



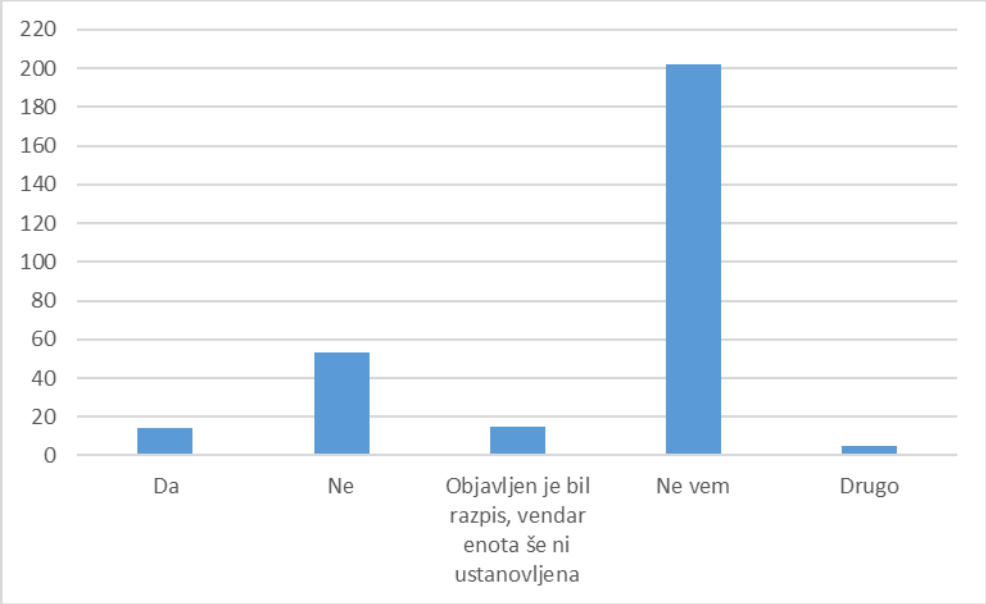
Podobno mnenje obstaja tudi pri vprašanju »Ali obstajajo enote, ki so zmožne vplivati preko Facebooka ali Twitterja?« (slika 1. 13). Mnogim je nepredstavljivo dejstvo, da obstajajo enote, ki so svoje znanje sposobne usmeriti v psihološko bojevanje s pomočjo računalniške opreme. Tovrstne enote z objavami poskrbijo, da ljudje določene stvari vidijo drugače ali pa samo, da ljudje sploh slišijo za določene stvari. Socialna omrežja kot vir vplivanja s pridom uporabljajo za boj proti terorizmu ter kriminalu.

Slika 1. 13: Obstoj enot, ki delujejo zgolj preko socialnih omrežij.



Še večjo neznanko pa predstavlja predvsem stanje v Slovenski vojski glede kibernetske enote. Pri vprašanju »Ali ima Slovenska vojska kibernetsko enoto?« je prevladujoči odgovor »ne vem«. Mišljenje nekaterih je tudi, da je Slovenija premajhna država za tovrstno enoto ali pa da nimamo strokovnjakov, potrebnih za uspešno delovanje tovrstne enote pri nas (slika 1. 14).

Slika 1. 14: Kibernetska enota v Slovenski vojski.



Anketni vprašalnik je pokazal slabše poznavanje kibernetike in z njo povezanih operacij ter enot. Ljudje v večini ne sledijo razvoju, ker jih bodisi ta tematika ne zanima, še niso slišali, da kaj takega sploh obstaja ali pa enostavno dvomijo v uspešnost operacij, ki so povezane s kibernetsko varnostjo. Verjetno tistim, ki jim je tehnologija in njen razvoj tuja, kibernetski prostor predstavlja nekaj nepredstavljivega in s tem tudi nekaj nedostopnega. Veliko večje je poznavanje tematike v starostni skupini med 20 in 40 letom, kar lahko pripišemo tudi seznanjenosti in uporabljanju računalniške opreme in spleta. Glede na spol je s tematiko bolj seznanjena moška populacija, kar je bilo pričakovano. Ne smemo pa zanemariti odlično poznavanje tematike posameznih oseb iz starostne skupine 61 let in več.

Poznavanje tematike bi bilo verjetno večje, če bi ljudje bili seznanjeni s strani organizacij, ki sodelujejo pri izobraževanju strokovnjakov ter izkoriščanju socialnih omrežij, kot to delajo v tujini.

10 ZAKLJUČEK

Vzpostavljanje kibernetske obrambe in kibernetskih enot s strokovnjaki z informacijskim znanjem postaja ključen element nacionalne obrambe. Odsotnost same fizične neposredne ogroženosti nadomešča virtualen skupek groženj, katerih cilj niso življenja ljudi, temveč dostop do ključne informacijske tehnologije neke države ter s tem povezan dostop do pomembnih podatkov. Trend kibernetskega vojskovanja se zadnja leta zgolj še stopnjuje, kar prikazujejo vse bolj kompleksnejši in uničujoči hekerski napadi. Vse večji poudarek se daje (pre)oblikovanju obrambe v tovrstne namene, ustreznemu izobraževanju kadra in ustanavljanju posebnih enot, ki so s svojim znanjem zmožne odvrniti napade. V večini držav se je trend ustanavljanja kibernetskih enot pojavil zgolj nekaj let nazaj, kar lahko pripišemo relativno majhni ogroženosti države ter novejšemu pojavu tovrstnega načina vojskovanja. Prav zaradi novejše tematike tako na spletu še ni mnogo podatkov o določenih enotah, skopi pa so tudi podatki na uradnih spletnih straneh vojska in držav.

Obe hipotezi lahko potrdim, saj ima vsaka država drugačne postopke, drugačne potrebe po strokovnjakih, vendar imajo vse enak cilj – ustanovitev kibernetske enote. Gre za zelo kompleksen proces, ki ga vsaka država prilagodi svojim potrebam po kibernetski obrambi in kadru za zagotavljanje kibernetske varnosti. Prav tako se država mora nenehno ozirati na nacionalne dokumente, saj morajo biti vsi postopki in dokumenti v skladu z nacionalno ustavo oz. najvišjimi akti v državi. Vojaka iz tradicionalnih pehot oz. drugih vej oboroženih sil ne moremo primerjati s specialistom iz kibernetske enote glede na osebno oborožitev in ostalo opremo, saj se le ta nanaša na okolje, v katerem vojak deluje. Primerjamo ju lahko na način uporabe orožja, saj oba delujeta v smeri preprečevanja napada in odvračanja nasprotnika. Prav tako morata biti oba ustrezno usposobljena za uporabo orožja, ključno vlogo pri tem pa imajo pridobljena tehnična znanja. Razlika med njima je zgolj področje delovanja oz. izpolnjevanja nalog. Strokovnjak kibernetske enote svoje operacije večinoma izvaja preko računalniške in ostale informacijske opreme, medtem ko vojak svoje naloge izpolnjuje na terenu in s tem tudi izpostavi svoje življenje oz. tvega poškodbe bolj kot pa vojak iz kibernetske enote.
Izbiranje med primernimi kandidati za opravljanje določenih nalog pa izpostavi problem zapletenosti procesa rekrutacije, saj s sprejetjem nekega strokovnjaka v enoto sprejmejo tudi njegovo zelo obširno znanje z določenega področja. Znanje tako lahko v trenutku postane tudi orožje, ki ga mnogi znajo uporabiti sebi v prid. Tako lahko pride do uhajanja informacij,

katerih število se v zadnjih letih samo še povečuje. Večinoma se ljudje na vodilnih položajih organizacij, ki zaposlujejo takšne strokovnjake tega problema še ne zavedajo v celoti in ne realizirajo potencialnih groženj, ki prihajajo iz same organizacije saj se večinoma osredotočajo zgolj na zunanje grožnje. Večina jih verjame, da bodo zaposleni delovali v prid organizaciji, kar bi naj veljalo v večini primerov, zato tudi ne polagajo posebne pozornosti na zaposlene in njihovo izvajanje danih nalog.

Kadar govorimo o kibernetski varnosti, lahko povemo, da govorimo o varnosti v globalnem pogledu, saj vse države težijo k enakemu cilju, čeprav na različne načine. Vse več je povezovanja v razne programe izobraževanja in tvorjenja zavezništev na nekem področju in s tem tudi izmenjevanje izkušenj. Tendence razvoja težijo k nenehnemu sledenju novejši tehnologiji, prav tako pa tudi sledenju novejšim načinom nezakonitega pridobivanja podatkov ter motenja informacijske opreme.
Socialna omrežja danes pomenijo poglavitni vir informacij, ki se ga poslužujejo večinoma vsi. Predvsem mladi nenehno sledijo novostim, povezanih s tehnologijo. Twitter in Facebook predstavljata socialno omrežje z visoko stopnjo zmožnosti vplivanja na sledilce. Socialnih omrežij se kljub tradicionalni »tajnosti« začnejo posluževati oborožene sile, saj so postala zelo močan vir vplivanja na zaznavo ljudi o dogajanju po svetu. Tako oborožene sile na socialnih omrežjih izvajajo operacije s psihološkim učinkom na ljudi, pri čemer se pripadniki za to usposobljene enote zanašajo na svojo zmožnost vplivanja, zavajanja, prikrivanja itd.

11 LITERATURA

1. Armed Forces Journal. 2015. *Cyberspace what is it, where is it and who cares.* Dostopno prek: http://www.armedforcesjournal.com/cyberspace-what-is-it-where-is-it-and-who-cares/ (29. april 2015).
2. Arnold, Todd, Rob Harrison in Greg Conti. 2015. *Shaping the Army's Cyber Operations orce: the Human Dimension*. Dostopno prek: http://www.cyberdefensereview.org/2015/02/12/human-dimension/ (10. junij 2015).
3. Arnold, Todd, Rob Harrison in Gregory Conti. 2015. *Professionalizing the Army's Cyber Officer Force.* Dostopno prek: http://www.usma.edu/acc/SiteAssets /SitePages/Reports/PACOF.pdf (24. maj 2015).
4. Bonner III, E. Lincon. 2014. *JFQ 74 | Cyber Power in 21st-Century Joint Warfare.* Dostopno prek: http://ndupress.ndu.edu/Media/News/NewsArticleView/ tabid/7849/Article/577536/jfq-74-cyber-power-in-21st-century-joint-warfare.aspx (14. junij 2015).
5. Bunkall, Alistair 2015. *Cyber Warfare: Army Creates 'Twitter Troops'.* Dostopno prek: http://news.sky.com/story/1418376/cyber-warfare-army-creates-twitter-troops
6. BusinessDictionary. *Cyberspace.* 2015. Dostopno prek: http:// www.businessdictionary.com/definition/cyberspace.html (31. marec 2015).
7. Center vojaških šol. 2015. *Prošnja za vpogled v podatke*. Maribor: Interno gradivo.
8. Conti, Gregory in John »Buck« Surdu. 2009. Army, Navy, Air Force, and Cyber – Is it Time for a Cyberwarfare Branch of Military? *Anewsletter 12(1):* 14 – 18.
9. Dailymail. 2012. *Iran nuclear facilities hit by cyber attack that plays AC/DC's Thunderstruck at full volume.* Dostopno prek: http://www.dailymail.co.uk /news/article-2178781/Iran-nuclear-facilities-hit-cyber-attack-plays-AC-DCs-Thunderstruck-volume.html (26. julij 2015).
10. *Defense One.* 2015. Dostopno prek: http://www.defenseone.com/ technology/2015/07/someone-just-leaked-price-list-cyberwar/117043/(26. julij 2016).
11. Dictionary.com. 2015. *Cyberwarfare*. Dostopno prek: http://dictionary.reference.com/browse/cyberwarfare (31. marec 2015).
12. Encyclopeadia Britannica. 2015. *Naval Warfare.* Dostopno prek: http:// www.britannica.com/EBchecked/topic/406883/naval-warfare/53036/Historical-development (31. marec 2015).

13. Flint, James. 2015. *Army joins the social media war with psy-ops brigade.* Dostopno prek: http://theconversation.com/army-joins-the-social-media-war-with-psy-ops-brigade-37125 (26. julij 2015).
14. Forbes. 2015. *North Koreas cyber Warriors a privileged elite in an isolated society.* Dostopno prek: http://www.forbes.com/sites/donaldkirk/2014/12/18/north-koreas-cyber-warriors-a-privileged-elite-in-an-isolated-society/ (17. marec 2015).
15. Fritzgerald, Britney. 2012. *AC/DC Worm: Bizarre Cyberattack Reportedly 'Rocks' Iran's Nuclear Facility Computers, Makes Them Blast 'Thunderstruck' Full Blast*. Dostopno prek: http://www.huffingtonpost.com/2012/07/25/acdc-worm-iran_n_1702179.html (26. julij 2015).
16. Gelzis, Gederts. 2014. *Latvia launches Cyber Defence Unit to beef up online security. Deutsche Welle*. Dostopno prek: http://www.dw.de/latvia-launches-cyber-defence-unit-to-beef-up-online-security/a-17471936 (17. marec 2015).
17. Gray, Colin. S. 2008. *The nature of land warfare*. Dostopno prek: http://www.defence.org.cn/aspnet/vip-usa/uploadfiles/2008-05/chapter1.pdf (31. marec 2015).
18. International Committee of the Red Cross. *Customary International Humanitarian Law*. 2015. Dostopno prek: https://www.icrc.org/customary-ihl/eng/docs/home (26. april 2015).
19. Joint Forces Command homepage. *Recruitment.* 2015. Dostopno prek: https://www.gov.uk/government/organisations/joint-forces-command/about/recruitment (17. julij 2015).
20. Kuehl, Daniel.T. 2009. *From Cyberspace to Cyberpower: Defining the Problem.* Dostopno prek: http://ctnsp.dodlive.mil/files/2014/03/Cyberpower-I-Chap-02.pdf (17. marec 2015).
21. Kuffman, Gary. 2015. *First 170 Officers Picked for Cyber Branch of Army.* Dostopno prek: http://buzzon.biz/2015/02/first-170-officers-picked-for-cyber-branch-of-army/ (29. april 2015).
22. Little, John. 2012. *Is War in the Sixth Domain the End of Clausewitz?* Dostopno prek: http://www.blogsofwar.com/2012/12/13/guest-post-war-in-the-sixth-domain/ (10. junij 2015).
23. Mahmoud, Khalid Walid. 2013. *Cyber Attacks: The Eletronic Battleield*. Qatar: Arab Center for Research and Policy Studies. Dostopno prek:

http://english.dohainstitute.org/file/get/d79c12ba-544b-46ad-9d61-c48c5a041eb9.pdf (29. april 2015).

24. Martin, Chris. 2015. *'Social' Forces? Elite U.S. Military Units Adopting Social Media as Newest Weapon Against Enemies.* Dostopno prek: http://www.ijreview.com/2015/03/275089-social-forces-elite-u-s-military-units-adopting-social-media-newest-weapon-enemies/ (29. april 2015).
25. Mather, Mathew. 2013. *How Space and Cyberspace are Merging to Become the Primary Battlefield of the 21st Century*. Dostopno prek http://matthewmather.com/wp-content/uploads/2013/03/Space-and-Cyberspace-Merging-into-21st-Century-Battlefield.pdf (17. marec 2015).
26. McCoy, Alexander. 2015. *We need a cyber corps as a 5th service*. Dostopno prek: http://foreignpolicy.com/2015/03/18/we-need-a-cyber-corps-as-a-5th-service/(23. junij 2015).
27. *National armed forces cyber defence unit (CDU) concept 2013.* Dostopno prek: http://www.mod.gov.lv/~/media/AM/Par_aizsardzibas_nozari/Plani,%20koncepcijas/cyberzs_April_2013_EN_final.ashx (23. junij 2015).
28. Oxford Dictionaries. 2015. *Cyberwar.* Dostopno prek: http://www.oxforddictionaries.com/definition/english/cyberwar (31. marec 2015).
29. Palokangas, Tero. 2013. 2013. Cyberwar: Another Revolution in Military Affairs? V *The fog of Cyber Defence*, ur. Jari Rantapekonen in Mirva Salminen, 146-153. Helsinki: National Defence University. Dostopno prek: http://www.doria.fi/bitstream/handle/10024/88689/The%20Fog%20of%20Cyber%20Defence%20NDU%202013.pdf#page=147 (31. marec 2015).
30. Postanivojak.si. 2015. *Vabilo k sodelovanju kot strokovnjak za kibernetsko varnost.* Dostopno prek: http://www.postanivojak.si/index.php?id=155 (23. junij 2015).
31. *Prachatai.* 2015. Dostopno prek: http://www.prachatai.com/english/node/4767 (26. april 2015).
32. Richards, J. 2009. Denial-of-Service: The Estonian Cyberwar and Its Implications for U.S. National Security. *International Affairs Review*, 18(2). Dostopno prek: http://www.iar-gwu.org/node/65 (3. avgust 2015).
33. *SearchSOA.* 2015. Dostopno prek: http://searchsoa.techtarget.com/definition/cyberspace (31. marec 2015).

34. NATO. 1949. *Atlantic Charter* - Severoatlantska pogodba, sprejeta 4.aprila 1949. Dostopno prek: http://nato.gov.si/slo/dokumenti/severnoatlantska-pogodba/ (10. junij 2015).
35. Slovenska Vojska. 2015. *Struktura.* Dostopno prek: http://www.slovenskavojska.si /struktura/ (26. april 2015).
36. Solce, Natasha. 2008. *The Battlefield of Cyberspace: The Inevitable New Military Branch — The Cyber Force.* Dostopno prek: http://www.albanylawjournal.org /archives/pages/article-information.aspx?volume=18&issue=1&page=293 (23. junij 2015).
37. Tal, Pavel. 2015. *Thailand's military cyber-warfare unit part of a growing trend*. Dostopno prek: http://blogs.timesofisrael.com/thailands-military-cyber-warfare-unit-part-of-a-growing-trend/ (29. april 2015).
38. TechRepublic. 2014. Dostopno prek: http://www.techrepublic.com/article/treat-cyberspace-like-a-battlefield/ (17. marec 2015).
39. Techtarget. 2015. *Cyberwarfare.* Dostopno prek: http://searchsecurity.techtarget.com/ definition/cyberwarfare (31. marec 2015).
40. TheFreeDictionary. 2015. *Armed forces.* Dostopno prek: http://www.thefreedictionary.com/armed+forces (26. april 2015).
41. Vergun, David. 2015. *Cyber chief: Army cyber force growing »exponentially«.* Dostopno prek: http://www.army.mil/article/143948/Cyber_chief__Army_ cyber_force_growing__exponentially (31. marec 2015).
42. Williams, Martyn. 2014. *What we know about North Korea's cyberarmy.* Dostopno prek:http://www.pcworld.com/article/2861692/what-we-know-about-north-koreas-cyberarmy.html (4. februar 2015).
43. Wise GEEK. 2015. *What is cyberwar.* Dostopno prek: http://www.wisegeek.com/ what-is-cyberwar.htm (31. marec 2015).
44. Merriam-Webster. 2015. *Army.* Dostopno prek: http://www.merriam-webster.com/ dictionary/army (15. julij 2015).

PRILOGE

Priloga A: Anketni vprašalnik

Pozdravljeni!

Moje ime je Maša Pertoci in vas prosim, da odgovorite na spodaj zastavljena vprašanja. Vaši odgovori mi bodo zelo pomagali pri izdelavi diplomske naloge z naslovom Kibernetske enote kot nova veja oboroženih sil.

Za vaš čas se vam iskreno zahvaljujem, hkrati pa vam zagotavljam anonimnost odgovorov in varovanje osebnih podatkov.

1.spol:

M Ž

2. Starost: _____

3. Status

a) osnovnošolec/-ka
b) srednješolec/-ka
c) študent/-ka
d) zaposleni/-a
e) brezposleni/-a
f) upokojenec/-ka
g) drugo _____

4. Ali ste seznanjeni z novejšimi načini vojskovanja?

a) da

b) ne

5. Koliko dimenzij vojskovanja po vašem mnenju obstaja danes?

a) 3 (kopno, voda, zrak)
b) 4 (kopno, voda , zrak, kibernetski prostor)
c) 5 (kopno, voda, zrak, vesolje, kibernetski prostor)

6**. Kaj je kibernetski prostor?**

a) prostor v vesolju

b) prostor, od koder dostopamo na splet

c) globalno omrežje informacijske tehnologije

7. Ali ste že slišali za pojem kibernetsko (informacijsko) vojskovanje?

a) da
b) ne

8. Če ste na prejšnje vprašanje odgovorili z DA, prosim da odgovorite še na spodaj zastavljeni vprašanji (8. 1 in 8. 2):

8. 1 S svojimi besedami opišete pojem kibernetsko vojskovanje.

8. 2 Kje ste prvič zasledili pojem kibernetsko vojskovanje?

a) mediji
b) internet
c) razni članki
d) povedali so mi drugi
e) drugo: _____

9. Ste seznanjeni z ustanavljanjem nove veje oboroženih sil, torej z ustanavljanjem kibernetskih enot?

a) nikoli še nisem slišal/-a za njih.

b) sem že slišal/-a, vendar ne vem nič o njih.

c) sem seznanjen/-a.

d) tematiko redno spremljam.

10. Katero orožje uporabljajo kibernetske enote pri svojih nalogah?

a) osebna oborožitev posameznika

b) letala in helikopterji

c) bojna vozila

d) računalniška in ostala informacijska oprema

11. Kolikšno stopnjo pomembnosti po vašem mnenju v svetu predstavljajo operacije, povezane s kibernetsko varnostjo?

a) imajo velik pomen za globalno varnost.

b) nimajo resnejšega pomena za globalno varnost.

c) so pomembne, vendar menim, da nimajo ključnega pomena za globalno varnost.

d) drugo: _____

12. Ali menite, da je s kibernetskimi enotami možno omejiti operacije nasprotnika?

a) da

b) ne

c) ne vem

d) drugo:_____

14. Ali menite, da obstajajo vojaške enote, ki delujejo preko spletnih omrežij - torej le z vplivanjem preko facebooka ali twitterja?

a) da

b) ne

c) ne vem

d) drugo:_____

15. Ali ima Slovenska vojska kibernetsko enoto?

a) da

b) ne

c) objavljen je bil razpis, vendar še ni ustanovljena

d) ne vem

e) drugo:_____