UNIVERZA V LJUBLJANI
FAKULTETA ZA DRUŽBENE VEDE

Peter Strnad

Informacijske operacije kot dejavnik preoblikovanja oboroženih sil

Diplomsko delo

Ljubljana, 2008

UNIVERZA V LJUBLJANI
FAKULTETA ZA DRUŽBENE VEDE

Peter Strnad
Mentor: asist. dr. Uroš Svete

Informacijske operacije kot dejavnik preoblikovanja oboroženih sil

Diplomsko delo

Ljubljana, 2008

Za vso podporo pri nastajanju diplomske naloge se zahvaljujem

moji Barbari, za vso ljubezen in pomoč pri izdelavi diplomske naloge,

mami Nadi, za odlično lektorstvo in spodbudo,

očetu Dragu, za smeh in oporo v trenutkih brezpotij ter

bratu Blažu, za vse trenutke, v katerih mi je izkazoval bratsko ljubezen.

INFORMACIJSKE OPERACIJE KOT DEJAVNIK PREOBLIKOVANJA OBOROŽENIH SIL

Z razvojem integriranih vezij in mikroprocesorjev je bilo omogočeno, da so danes informacijska tehnologija in ostale komunikacije prisotne v vseh aspektih družbenega življenja, s tem pa je povečano tudi varnostno tveganje vsake države, saj je vsak element državne varnosti in s tem tudi nemoteno bivanje ljudi v le-tej povezano z informacijsko tehnologijo. Z medmrežnimi dostopi so informacijska orožja dostopna vsakomur, ne glede na osebno prepričanje in kraj bivanja. V ofenzivne in defenzivne namene je zato v državah prisotno prestrukturiranje oboroženih sil, kjer se razvijajo, posodabljajo in ustanavljajo enote ter centri za delovanje v informacijskih operacijah. V analizo je vključen pregled razširjenosti informacijske tehnologije in ostalih komunikacij, razdelana pa so prav tako informacijska orožja, vojaško informacijsko okolje, hkrati pa tudi digitalno bojišče. V primerjalni analizi so tako zajete oborožene sile, enote in učni centri ter raziskovalni inštituti, namenjeni informacijskim operacijam treh držav, in sicer Združenih držav Amerike, Velike Britanije in Slovenije.

Ključne besede: informacija, informacijsko orožje, informacijske operacije, enote za informacijsko bojevanje

INFORMATION OPERATIONS AS A TRANSFORMATION FACTOR OF MODERN MILITARIES

With the development of integrated circuits and microprocessors the presence of information technology and other communications all across the aspects of social life is enabled. Thereby security risk of each country is increased, because every element of national security is connected to information technology. Internet information weapons are indiscriminate of personal beliefs and place of residence and are accessible to anyone. In a offensive or defensive purposes modern militaries are restructuring their armed forces where they are developing and setting up units and Centers for operating in information operations. The analysis includes a review of distribution of information technology and other communications. Information weapons, military information environment and also the digital battlefield are presented.

In a comparative analysis are thus included armed forces and units and at the same time also research centers and institutes intended for information operations of three countries, namely the United States, Great Britain and Slovenia.

Keywords: Information, information weapons, information operations, information warfare units

KAZALO

KAZALO TABEL

KAZALO ORGANIGRAMOV

1 UVOD

Narava vojskovanja in s tem tudi vodenje in poveljevanje so se od začetka 19. stoletja do danes močno spremenili. Razlog za to je predvsem velik tehnološki razvoj, katerega generacijske faze se vedno bolj zmanjšujejo. Tako je bilo v preteklosti potrebno čakati na naslednjo generacijo tehnologije 50, 60 ali celo 100 let in več, sedaj pa se je ta interval zmanjšal na celih sedem let in se še krči.

Poleg vseh sodobnih izumov je bilo odločilno odkritje integriranih vezij in mikroprocesorja, ki ga številni primerjajo z izumom kolesa. Mikroprocesorje s polprevodniki najdemo že v vseh sodobnih tehničnih napravah, od računalnikov, satelitov, prevoznih sredstev, prek sredstev komunikacije do igrač in celo v pojočih čestitkah. Nižanje cen informacijske opreme in uporaba sodobnih komunikacijsko-informacijskih sistemov sta temeljito pospešila globalizacijo in iz sveta naredila vas (Kočevar 2003, 22).

V celoti gledano pa je uporaba računalnikov, satelitov, vodenih orožij in podobne tehnike pomenila v vojaškem smislu prehod iz industrijske v informacijsko dobo bojevanja, kar je v svojem delu War and Antiwar opisal tudi Alvin Toffler Zgodovino bojevanja je razdelil na tri obdobja, in sicer na agrarno obdobje, za katerega je značilna slabo opremljena in neenotna majhna vojska, zbrana na podlagi sklica, industrijsko obdobje, za katerega so značilne množične, dobro opremljene homogene vojske, ter nenazadnje informacijsko obdobje, v katerem gre za uporabo informacijskih in drugih visoko razvitih tehnologij, s pomočjo katerih se je krčila tako količina vojaške žive sile kot količina opreme, rezultat pa je bila enaka oziroma celo večja efektivnost. Zamisel takšnega informacijskega obdobja oziroma vala išče svoj cilj prav v digitaliziranem bojišču, ki ga povezujemo s pojmom C^4I (povzeto po Toffler 1993), ampak o tem v nadaljevanju.

Bistvo diplomske naloge je s pomočjo analize sodobnega bojišča, ki sem ga že prej omenil kot digitaliziranega, in opreme ter tehnoloških inovacij dokazati vpliv na samo organizacijo vojske, kot tudi njeno prenovljeno dojemanje sodobnega bojišča, ki je postavilo nova pravila, zaradi katerih se morajo sodobne vojske prilagoditi novemu

načinu bojevanja, kar posledično vključuje krčenje količine žive sile, ki bi jo naj zamenjala dovršena tehnološka oprema in seveda orožje.

1.1 Metodološka zgradba diplomske naloge

1.1.1 PREDMET IN CILJ PROUČEVANJA

V svoji nalogi se bom osredotočil na informacijske operacije in na posledično preoblikovanje oboroženih sil nekaterih vojaških velesil, izpostavil bom predvsem Veliko Britanijo (VB) in Združene države Amerike (ZDA) ter nenazadnje tudi Slovenijo in njen proces prilagajanja novim razmeram na svetovnem bojišču.

Informacijska operacija ima v vojaški znanosti relativno svež predznak, zato pričakujem, da bodo imele posamezne države različen pristop v benevolentnosti dejanja in samem procesu preoblikovanja oboroženih sil.

Cilj mojega dela je skozi dokumentacijo določenih držav, predvsem ZDA, VB in Slovenije, opisati, kako le-te pojmujejo oziroma dojemajo pojem informacijske operacije kot sestavnega dela oboroženega boja ter posledično tudi razčlenitev in način priprave ter opremljenosti oboroženih sil. Predstavil bom osnovno vojaško tehniko za izvajanje informacijskega bojevanja, ker pa je vloga informacije in komunikacije v tem aspektu neizmernega pomena, bom v svojo analizo vključil tudi pregled količine informacijskih, komunikacijskih in vojaških inovacij ter lastnega razvoja določene države, pri čemer bom upošteval tudi uvoz tehnologije in razvitost same države (komunikacijska infrastruktura) nasproti razvitosti vojske. Moje delo skorajda ne bi imelo smisla brez same analize osrednjega pojma – informacijske operacije. Ob razčlenitvi sodobnega bojišča bom poskušal kar se da temeljito razvozlati pojem informacijske operacije, hkrati pa tudi opisati njen namen in cilje ter podati osnovne smernice razvoja bojišča v prihodnosti.

1.1.2 HIPOTEZE

V nalogi bom skozi preučevanje različnih virov preveril veljavnost naslednje splošne hipoteze (H_1):

- Pojav informacijskih operacij vpliva na strukturo oboroženih sil, kar se vidi in bo v prihodnosti tudi privedlo do samostojnih zvrti oboroženih sil, katerih namen bo zgolj informacijsko bojevanje.

Skozi analizo določenih držav in vojska le-teh bom preveril veljavnost naslednje posebne hipoteze (H_2):

- Zaradi kompleksnosti ciljev in informacijskih operacij, ki zadevajo vse ravni družbenega življenja, imajo vojaško in gospodarsko razvitejše države jasneje dodelan koncept informacijskega bojevanja kot informacijsko manj razvite države.

1.1.3 METODE PREUČEVANJA

Postopek zbiranja podatkov v diplomski nalogi je temeljil na sistematičnem zbiranju sekundarnih informacij (monografije, članki, publicistični viri), v največji meri pa sem se opiral na internet. Aplikacija metod je bila raznovrstna, glede na širino uporab pa so po vrstnem redu sledeče:

- **Deskriptivna metoda**, ki sem jo uporabljal predvsem v teoretičnem delu diplomske naloge, kjer sem sistematično opisoval sestavne dele naloge, kot so informacija, informacijsko bojevanje, informacijske operacije, informacijska orožja, C^4I sistemi in drugo. S to metodo sem predstavil določene teoretične koncepte znotraj informacijskega vojskovanja in poudaril širino tega pojava in informacijskih operacij ter s tem povezanega preoblikovanja oboroženih sil.
- **Primerjalno raziskovanje**, kjer sem na področju razširjenosti informacijsko-telekomunikacijske tehnologije primerjal izbrane države, kasneje pa sem to metodo uporabil tudi v praktičnem delu naloge, ko sem primerjal količinski obstoj enot, katerih namen je informacijsko bojevanje znotraj oboroženih sil izbranih držav. Izvedel sem tudi longitudinalno raziskavo, saj sem primerjal razširjenost uporabe interneta in računalnikov v letošnjem letu z letom 1999. V primerjalnem raziskovanju sem uporabil tudi metodo analize uradnih statistik, ki sem jo uporabil v praktičnem delu naloge, v katerem sem primerjal sestavo oboroženih sil in razširjenost informacijske tehnologije na področju posameznih držav.

- **Zbiranje virov**, ki je kot metoda razlikovanja služilo predvsem kot nabiranje predhodnega znanja na področju informacijskega vojskovanja in informacijske tehnologije.
- **Analiza in interpretacija sekundarnih virov.** To metodo sem uporabljal skozi celotno delo, največ pa na začetku dela, kjer sem se opiral na razne članke, povezane z definiranjem digitalnega okolja, knjige, s pomočjo katerih sem pojasnil predvsem strukture obrambnih sistemov in enot za informacijsko bojevanje.
- **Analiza in interpretacija primarnih virov** je bila uporabljena v teoretičnem in praktičnem delu diplomske naloge. V teoretičnem delu naloge sem s pomočjo te metode iz različnih dokumentov opredelil dojemanje informacijskega bojevanja s strani določenih držav in s strani različnih vojaških zvrsti. V analizi dokumentov in poročil v praktičnem delu naloge sem se zaradi angleške terminologije bolj ali manj uspešno srečeval z jezikovnim tolmačenjem, kjer sem iskal ustrezne pomene za uporabljene besede v dokumentu, pri čemer ciljam predvsem na poimenovanje raznih enot in drugih institucij, povezanih z informacijskim bojevanjem.

2 INFORMACIJSKA DIMENZIJA SODOBNEGA BOJEVANJA

Od samih začetkov bojevanja je informacija osnovni in najpomembnejši dejavnik odločanja na bojišču. Uporabna informacija mora biti resnična, namenska, natančna, popolna in, kar je po mojem mnenju najpomembnejše, pravočasna. Glede na doktrino ameriške kopenske vojske za informacijske operacije gre pri informaciji za podatek, ki je pridobljen iz okolja in predelan v uporabno obliko ter postane udejanjen šele tedaj, ko je postavljen v situacijski kontekst in pridobi pomen (Internet 1).

Informacija je torej ciljno usmerjen podatek, za katerega je značilno, da zmanjšuje neznano oziroma povečuje znano. Edward Waltz je v svojem delu Information warfare principle and operations (Waltz 1998, 24) podal naslednje značilnosti informacije:

- informacija je abstraktna;
- informacija ima več različnih, pogosto pa tudi enake rabe;
- informacija je neizčrpna, vendar zaradi pomena in vrednosti omejena;
- razmerje informacije do njene vrednosti je kompleksno in nelinearno (vrednost informacije ni odvisna od njenega obsega, pač pa od vsebine).

Na drugi strani je Jeremy Sherman (Internet 36) opredelil informacijo kot znanstveni zvok, ki se s svojo obsežnostjo prilagaja človeški neposredni notranji prepoznavi oziroma intuiciji, z namenom določanja samega pomena le-te. Intuicija ima v prepoznavi informacije zelo veliko vlogo, kajti ne glede na to, kakšen je pravilen pomen informacije, se njeno dojemanje vedno začne kot posledica človekove konstruktivne dejavnosti, za korektno prepoznavo pomena informacije pa se moramo včasih tudi odreči naši lastni intuiciji. Informacija mora biti pravilno sestavljena »od spodaj navzgor«. V tem primeru govorimo o »bottom up« pristopu, kjer je informacija sestavljena iz prvotne nežive sfere čiste kemije in fizike in na tem mestu še ni opazna, nato informacija potuje skozi življenjski doživljaj človeka, zavest, medosebno komunikacijo, vse dokler ne doseže družbenega okolja.

2.1 Kritična in informacijska infrastruktura

Ob navajanju vseh teh podatkov sem prišel do spoznanja, da je v bistvu potrebno opredeliti še neposredni cilj ofenzivnih informacijskih operacij, ki si prizadevajo, da bi si ga podredile, uničile, prekinile pretok informacij, in po drugi strani defenzivnih informacijskih operacij, ki si prizadevajo neprekinjeno delovanje tega sistema in ga želijo ohraniti v homogeni osnovni obliki. Govorim o pojmih kritične in informacijske infrastrukture.

Pojma sicer zvenita podobno, vendar je sam pojem kritične infrastrukture, ki vključuje vse sisteme in imetje, čigar nezmožnost ali uničenje bi lahko oslabilo nacionalno oz. državno varnost ter njeno ekonomsko in socialno blaginjo (promet, energetski sistem, bančne in finančne inštitucije itd.), širši od pojma informacijske infrastrukture, ki vsebuje komponente, kot so telekomunikacije, računalniki, njihovo programsko okolje, internet, sateliti itn. Ta termin se uporablja tudi za sistem med seboj povezanih računalnikov in računalniških mrež ter informacijskih tokov, ki med njimi potekajo, kakor tudi za tisti del globalne oziroma nacionalne infrastrukture, ki je posebej pomembna za neokrnjeno delovanje kritičnih infrastrukturnih služb (Svete 2007, 160).

Prav tako je pri razlikovanju med kritično infrastrukturo in kritično informacijsko infrastrukturo potrebno biti pozoren na različne posebnosti, ki se razlikujejo od tradicionalnih in uveljavljenih zgodnjih infrastruktur, kar se kaže v večji razsežnosti kot v medsebojnem povezovanju in soodvisnosti (Svete 2007, 161).

Kot sem že omenil, znotraj kritične informacijske infrastrukture obstaja informacijsko infrastruktura, ki se deli na tri področje, in sicer na globalno informacijsko infrastrukturo, ki vključuje mednarodni kompleks medijskih komunikacij, telekomunikacij, računalnikov, skratka vso opremo, ki omogoča sleherno znakovno, zvočno in komunikacijo v sliki. (Svete 1999, 42), nacionalno informacijsko infrastrukturo, ki predstavlja podsistem globalne informacijske infrastrukture, omejena je na ozemlje določene države (interne telekomunikacije, računalniki, internet znotraj države ipd.) ter obrambno informacijsko infrastrukturo, ki obsega prenos informacij in obdelavo virov, vključno s shranjevanjem informacij in podatkov, manipulacijo, pridobivanjem in prikazovanjem (Internet 1). Vključuje infrastrukturo, ki jo imajo v

lasti vojaške organizacije, uporabljajo pa jo za namene nacionalne varnosti. Ta infrastruktura inhibira komponente C^4I sistemov in tudi različne administrativne elemente.

2.2 Informacijske operacije

Z namenom postavitve trdnih temeljev pojma informacijske operacije moram najprej pojasniti pojem same operacije in pokazati njene člene oziroma determinante ter nenazadnje tudi razmerje oziroma odnos do pojma informacijskega bojevanja.

Operacija kot element kampanje poteka na bojevališču (v operacijski coni) kot delu vojskovališča, v njej pa praviloma sodelujejo posamezne armade oziroma jo izjemoma lahko izvajajo posamezni samostojni okrepljeni korpusi. Vsaka armadna operacija je praviloma sestavljena iz več bitk, ki jih izvajajo korpusi v sestavi armade. Bitke korpusov so povezane v skladno celoto z zamislijo poveljnika armade, ki jih kombinira, da bi dosegel cilj armadne operacije. Operacije letalskih sil in zračne obrambe izvajajo letalski korpusi in korpusi zračne obrambe, medtem ko pomorske operacije izvajajo bojne flote. V nasprotju s kampanjami, ki trajajo celo poletje, jesen, zimo ali pomlad in potekajo na celotnem kopenskem, pomorskem in zračnem vojskovališču, potekajo operacije na eni do dveh operacijskih smereh in v povprečju trajajo od enega do treh tednov (Žabkar 2003, 164).

Znano je, da rezultati operacije v večji meri vplivajo na celotni ali delni potek določenega obdobja vojne, lahko pa tudi na celotno vojno.

Determinante oziroma kriteriji, ki določajo operacije, so:

- **cilj in način izvedbe** (ofenzivne, defenzivne in kombinirane operacije);
- **okolje in kraj v okviru bojišča in vojskovališča** (okolje deli operacije na kopenske, zračne, pomorske, vesoljske, informacijske operacije, ki lahko stojijo kot samostojno okolje ali kot simbiotično z vsemi drugimi okolji; operacije lahko izvajamo na frontni črti, v lastnem ali nasprotnikovem zaledju ali kombinirano);
- **sile** in del oboroženih sil, ki izvajajo operacije (lastne sile, tuje sile in uporabljene sile);

- **trajanje in potek operacije** (vsaka operacija mora pri svojem načrtovanju in izvedbi preiti etape[1], ki so: priprava, izvedba, zaključek);
- **pomen ciljev in rezultati ciljev**, ki jih načrtujemo.

Zgoraj sem že navedel definicijo operacij in podal osnovne gradnike le-teh, še vedno pa nisem pojasnil, kaj je to informacijska operacija.
Informacijske operacije povezujejo oziroma združujejo vse vidike informacij za podporo in dopolnilo elementom bojne moči z namenom prevlade nad bojiščem ob pravem času in na pravem kraju, pravimi orožji in sredstvi. Informacijske operacije so neprekinjene vojaške operacije znotraj vojaškega informacijskega okolja, ki omogočajo, dopolnjujejo in ščitijo sposobnosti prijateljskih sil po zbiranju, obdelavi in delovanju glede na informacije za doseganje prednosti skozi celoten obseg vojaških operacij. Informacijske operacije vključujejo interakcijo z globalnim informacijskim okoljem in izrabo ali preprečevanje nasprotnikovega dostopa do informacij ter njegovih procesov odločanja (Internet 1).

Po navedbi definicije je potrebno pojasniti, da se informacijsko bojevanje nanaša izključno na vojno in sovražne aktivnosti, medtem ko informacijske operacije obsegajo tudi mirnodobne ter predvojne interakcije. Ožji pomen omejuje informacijske operacije predvsem na vojaško (informacijsko) okolje, hkrati pa predstavljajo sinonim za informacijsko bojevanje na vojaškem področju.

Informacijske operacije imajo izreden pomen v državah z visoko razvitim informacijskim okoljem, ker se izvajajo v vseh obdobjih. Zanje je značilna nizka stopnja nasilja, okolje, v katerem se odvijajo, se zelo hitro spreminja, kar bistveno vpliva na potek in s tem tudi prilagajanjem informacijskih operacij. Ko govorimo o informacijskih operacijah, moramo prav tako poudariti, da je zanje značilen izjemno širok spekter sredstev, ki se uporabljajo za dosego ciljev.

Med prebiranjem literature in drugih virov, ki izvirajo iz zahoda, je možno zaslediti delitev informacijskih operacij na ofenzivne in defenzivne. Za lažjo predstavo

[1] Etapa ima lahko več faz, v operativno-strateških delovanjih pa označuje del operacije (VE 1978, 710).

informacijskih orožij, opreme in predvsem vpliva na preoblikovanje oboroženih bomo v naslednjem koraku le-te tudi našteli in podali njihov bistveni opis.

2.2.1 OFENZIVNE INFORMACIJSKE OPERACIJE

- **Psihološke operacije (ang. PSYOP) –** pomembne so za pošiljanje izbranih informacij tujemu občinstvu. Bistvo teh operacij ni v informiranju, ampak v prepričevanju. Namenjene so vplivanju na emocije, motive, miselne procese in končno na obnašanje tujih vlad, organizacij ter posameznikov. Psihološke operacije lahko uporabimo na strateški, operativni in taktični ravni. Na strateški ravni so lahko oblikovane kot pozicije, note ali komunikeji, na operativni ravni lahko vsebujejo razpečevanje letakov, oznanila po zvočnikih, radijske in televizijske oddaje ter ostala sredstva, ki bi lahko pripomogla, da sovražnik prebegne, dezertira ali se preda. Na taktični ravni pa psihološke operacije vključujejo uporabo zvočnikov in ostalih sredstev za ustvarjanje strahu in nemira v sovražnikovih vrstah. PSYOP sile lahko prav tako oblikujejo razpoloženje in vplivajo na obnašanje skozi komunikacijo iz oči v oči, poleg tega pa so lahko tudi v podporo operacijam vojaških ukan. Psihološke operacije lahko razdelimo v štiri glavne kategorije:
  - ofenzivne notranje psihološke operacije – promocija zaželenih zaznav, predstav, mnenj in vedenja med pripadniki lastne organizacije;
  - defenzivne notranje psihološke operacije – preprečevanje zaželenih zaznav, predstav, mnenj in vedenja med pripadniki lastne organizacije;
  - ofenzivne zunanje psihološke operacije – promocija zaželenih zaznav, predstav, mnenj in vedenja med pripadniki tuje organizacije;
  - ofenzivne zunanje psihološke operacije – preprečevanje zaželenih zaznav, predstav, mnenj in vedenja med pripadniki tuje organizacije (Malešič 1996, 142)

- **Elektronske operacije (okr. EW) –** sestavljajo tri glavne podskupine, in sicer:
  - **elektronski napad (ang. Electronic Attack – EA) – napad na nasprotnika z** namenom degradiranja, nevtraliziranja ali uničenja nasprotnikovih bojnih zmožnosti za preprečevanje oz. zmanjšanje uspešne nasprotnikove uporabe elektromagnetnega spektra;

- **elektronska obramba** – vključuje dejanja, kot je samozaščitno motenje in nadzor dejavnika za zaščito prijateljske uporabe elektronskega spektra z namenom zmanjšanja učinkov prijateljske ali nasprotnikove uporabe elektronskega napada, ki bi lahko degradiralo, nevtraliziralo ali uničilo prijateljsko zmožnost bojevanja;
- **elektronska podpora vojskovanju**, ki prispeva k situacijskemu osveščanju poveljujočih s pomočjo zaznave, identifikacije in lokacije virov namerno ali nenamerno sevanje elektromagnetne energije z namenom takojšnje prepoznave grožnje (Internet 3).

Odločitev o uporabi elektronskega napada mora biti zasnovana na tveganjih, ki jih lahko povzroči nasprotnikov odgovor in ne samo na ciljih združene kampanje ali operacije.

- **Vojaške ukane in prevare –** bistvo teh je, da poskušajo vplivati na nasprotnikove odločitve skozi učinke, ki jih povzročajo na njihove sisteme za zbiranje obveščevalnih podatkov, analize in razpečevanja[2]. Za dosego prevlade je potrebno dobro poznati nasprotnika in njegov sistem odločanja. Ključnega pomena je predvidevanje in prav tukaj mora poveljujoči določiti, kakšna je njegova želja, da se nasprotnik obnaša v bitki. Na tem mestu pridemo do spoznanja, da je vojaška ukana usmerjena na doseganje določenega obnašanja. Z ukanami želimo povzročiti, da si nasprotnikovi poveljniki ustvarijo napačne vtise o nameri ali sposobnosti prijateljskih sil, s tem pa neoptimalno rabo lastnih sil. Dejavnosti, ki temeljijo na vojaški ukani, so odvisne od obveščevalnih operacij, ki kvalificirajo in predvsem usmerjajo cilje nasprotnih in lastnih sil. Vojaške ukane imajo tudi svojo ceno, saj gre pri sami organizaciji le-teh za recipročnost delovanja sil, kjer je za določeno ukano potrebno uporabiti sile, ki bi drugače bile na razpolago bojni dejavnosti.

[2] Kot primer takšne ukane bi lahko navedel med operacijo »Zavezniška sila«, kjer je leta potekal napad na Zvezno republiko Jugoslavijo (ZRJ) s strani NATA. Obe strani sta se zatekala k uporabi vojaških ukan in prevar, izpostavil pa bi ukane ZRJ, s katerimi je nasprotniku prikrila svoje objekte in namene ter ga mnogokrat prisilila, da je napadal neobstoječe cilje. Z različnimi maketami tankov, oklepnih transporterjev, artilerijskih orožij in vojakov so, kot je zapisal časnik The Times (24. 6. 1999), letala in artilerija zveze NATO odvrgla na tisoče bomb, uspešno pa zadela le 13 od 300 tankov ZRJ, močno vrednost zavajanja pa so imele tudi tako imenovane tlakovane ceste (s črnimi plastičnimi pregrinjali), ki so bile nameščene na poljih in tako zavajale NATO-ve pilote, ki so s hitrostjo več kot 800 kilometrov na uro preletavali območja.

- **Fizični napad** - se kot element v sestavi integriranega boja informacijskih operacij nanaša na uporabo orožij za uničevanje (hard kill weapons) proti določenim ciljem (Internet 3). Med primarnimi cilji so največkrat poveljniška vozlišča in strukture, obalni sistemi za nadziranje, sistemi protizračne obrambe ter ofenzivne informacijsko operacijske zmožnosti nasprotnika.

- **Operacijski napadi ali napadi na računalniška omrežja (CNA – Computer Network Attack)** – za to dejavnost se uporablja tudi besedna zveza informacijski napad, saj pri tem poskušamo manipulirati ali uničiti nasprotnikove informacije ali informacijske sisteme brez vidnih sprememb na fizični celoti, v kateri se ti nahajajo. Informacijske napade in napade na računalniška omrežja bi lahko definirali kot »operacije z namenom motenja, preprečevanja dostopa, degradiranja ali uničenja informacij, ki se nahajajo v računalnikih ali računalniških omrežjih ali računalnikov in omrežij samih (Internet 3).

- **Operacijska varnost (ang. krat. OPSEC) –** upočasnjuje nasprotnikov proces odločanja in ustvarja priložnosti za hitrejšo in lažjo dosego lastnih in prijateljskih ciljev. Operacijska varnost skrbi za nemoteno delovanje celotnega sistema informacijskih tehnologij, kar vključuje programsko in strojno opremo, se pa močno prepleta z defenzivnim informacijskim bojevanjem, kar vključuje informacijsko varnost, informacijsko zagotovitev, elektronsko zaščito, fizično varnost, protizavajanje, protiobveščanje in protipropagando.

2.2.2 DEFENZIVNE INFORMACIJSKE OPERACIJE (Internet 1)

- **Informacijsko zagotavljanje (ang. Information Assurance – IA)** – spada v sklop informacijskih operacij, ki varujejo in ščitijo informacije in informacijske sisteme, pri čemer zagotavljajo njihovo dostopnost, celovitost, avtentičnost, zaupnost in nezavračanje. To vključuje skrb za ponovno vzpostavitev informacijskih sistemov z vključevanjem zmožnosti zaščite, zaznavanja in odgovora, ki bi ublažili učinke sovražnikovih dejanj in vplivov okolice.

- **Informacijska varnost (ang. Information Security - INFOSEC)** – katerega glavna funkcija je zagotoviti kontinuiranost funkcionalnega delovanja informacijskega sistema, kamor spadata programska in strojna oprema, hkrati pa ima nalogo ščitenja pred nepooblaščenim razkrivanjem, prenašanjem, spreminjanjem ali uničenjem informacij, ne glede na dejavnike, ki vplivajo na to aktivnost. Tako bi na tem mestu poudaril, da je naloga informacijske varnosti zoperstavljanje vsem informacijskim orožjem na programski (software) osnovi, kar vključuje tako trojanske konje, računalniške viruse, črve in logične bombe, ki so glede na dostopnost interneta in masivnost uporabe le-tega zelo velik zalogaj za informacijsko varovanje in, kot bo vidno v nadaljevanju, se ta zvrst defenzivnih informacijskih operacij zelo prepleta z drugimi zvrstmi.

- **Operacijska varnost (OPSEC) –** preprečuje nasprotniku dostop do kritičnih informacij o prijateljskih zmožnostih in namerah ter s tem povzroča ranljivost nasprotnika. Ključne naloge operacijske varnosti sem podal že v sklopu ofenzivnih informacijskih informacij.

- **Fizična varnost –** preprečuje neposredni fizični napad in uničenje vozlišč poveljevanja in strukture same.
  Vključuje neposredni in posredni ogenj kopenskih, zračnih in pomorskih sil ter seveda branjenje pred le-temi, vključena pa so tudi dejanja sil za posebne operacije (special operations forces – SOF).

- **Protizavajanje (ang. Counterdeception) –** prispevajo k zavesti o nasprotnikovih namerah in služijo za identifikacijo njegovih poskusov ukan lastnih in prijateljskih sil. Sem spadajo dejavnosti za preprečevanje, nevtralizacijo ali zmanjšanje učinkov ukane oziroma za pridobivanje superiornosti nad nasprotnikovimi ukanami in dezinformacijami.

- **Protipropaganda (and. Antipropaganda) -** sem spadajo vse aktivnosti lastnih in prijateljskih sil, ki preko tiskanih oziroma drugih berljivih sporočil ter preko zvoka in slike vplivajo na sovražnikove sile in na civilno prebivalstvo, cilj tega

pa je podrejanje mnenja le-teh ter nasprotovanje nasprotnikovim psihološkim dejavnostim.

- **Protiobveščevanje (ang. Counterintelligence) –** pridobivanje informacij in izvajanje dejavnosti, ki ščitijo prijateljske informacije in informacijske sisteme pred nasprotnikovimi obveščevalnimi in terorističnimi dejavnostmi ter sabotažami.
- **Elektronsko vojskovanje**
- **Posebne informacijske operacije (Special Information Operations – SIO)**

2.3 Informacijsko bojevanje

Že najstarejši vojaški teoretik Sun Tzu Wu je trdil, da je zmaga na strani tistega, ki ima točnejše in popolnejše informacije subjekta in objekta, v katerem se bojuje, kar zadeva poznavanje samega sebe, nasprotnika, terena, vremena in še bi lahko naštevali. Znani vojaški strateg Carl von Clausewitz je pomanjkanje informacij poimenoval kar »megla vojne«. Toffler je v analizi bojišča klasificiral naslednje dejavnike sodobnega bojevanja:

- materialni dejavnik (oborožitev, oprema);
- energetski dejavnik (energija, naravni in umetni viri, človeške zmogljivosti, izurjenost, morala, skratka vse, kar je potrebno za zagon vojaškega stroja);
- informacijski dejavnik, ki pa je v sedanjem času po mojem mnenju dominantnega pomena ravno zaradi močnega tehnološkega skoka, ki ga doživljamo v zadnjih dveh desetletjih. Ta skok je namreč močno spremenil tako vojaške organizacijske strukture kot sam način uporabe vojaških organizacij in formacij (Toffler 1993, 32).

Množična uporaba računalnikov in druge tehnologije ter nivo povezanosti le-teh v informacijska omrežja, kot je na primer internet, prinaša uporabnikom poleg vseh prednosti tudi negativne posledice, kot so nevarnost zlorab, vdorov in drugih aktivnosti, ki jih obravnava področje računalniške varnosti. Kljub začetku uporabe računalnikov, povezanih v omrežja, v začetku 80-ih let prejšnjega stoletja so zahodni obrambni analitiki začeli posvečati večjo pozornost tej problematiki šele v začetku devetdesetih let. Množica različnih študij in poročil s področja varnosti informacijske tehnologije na

strateškem nivoju so oblikovala nov celovit koncept – informacijsko bojevanje (Information Warfare – IW).

Pomembno je poudariti, da je sam pojem »vojne« v informacijskem vojskovanju politično občutljiv v večini držav in prav zaradi tega se je začel namesto IV uporabljati pojem informacijske operacije (IO). V zelo kratkem času je ta pojem sprejelo mnogo večinoma zahodnih držav, kakor tudi zveza NATO. Informacijske operacije so vojaško definiran koncept in doktrina, ki v veliki meri reagirata z družbo, kajti velika večina tarč, bodisi napadenih ali branjenih z informacijskimi operacijami, je civilnih in nevojaških. Kljub temu da je občutljivost na pojem »vojna« velik, se moramo zavedati, da je pojem IV še vedno v uporabi kot vsesplošna knjižnična oznaka za to področje tehnologije in doktrine. Tako lahko v skupni koš termina IV dodamo še druge pojme in tehnologije, kot so elektronsko vojskovanje, informacijsko zagotavljanje, informacijske operacije, HERF/NNEMP orožja[3], netwar, hekanje, cyber napadi, psihološke operacije in podobno.

Glede na določene terminološke zatike je mejo med informacijskim bojevanjem in informacijskimi operacijami postavil dr. Dan Kuehl, profesor na Nacionalni obrambni univerzi v Virginiji, ki pravi, da je informacijsko bojevanje podzvrst večjega sistema, imenovanega informacijska operacija, saj le-ta ne obravnava zgolj informacijskega vojskovanja v času spopada, temveč tudi vladno dejavnost in prav tako informacijsko varnost, ki obsega tudi dele privatnega sektorja (Internet 2)

Enotne definicije informacijskega vojskovanja v virih ni, najdemo pa lahko podrobnosti elementov, ki so v definicijah navedeni.

Ministrstvo za obrambo Združenih držav Amerike (ZDA) je definiralo informacijsko bojevanje (IV) kot izvajanje aktivnosti za dosego informacijske prevlade z vplivanjem na nasprotnikove informacije, informacijske procese in sisteme ter računalniška omrežja ob sprotnem branjenju svojih informacij, informacijskih procesov, sistemov ter računalniških omrežij (Internet 1). Kasnejša definicija Združenega poveljstva oboroženih sil ZDA pravi, da je IV informacijska operacija, izvajana v času krize ali

[3] HERF – high energy radio frequency (visokoenergetske radijske frekvence), NNEMP – non nuclear electro magnetic pulse (nenuklearni elektromagnetni pulz)

konflikta z namenom doseganja ali podpore določenih ciljev nad določenim nasprotnikom ali nasprotniki (Internet 3). V slednji definiciji IV je opazno, da se je samo pojmovanje tega pojma močno posplošilo, kajti IV je postal v zadnjih letih tako obsežen pojem, da že grozi, da bo vključeval vse, razen najbolj primitivnih oblik vojskovanja.

3 RAZŠIRJENOST INFORMACIJSKE TEHNOLOGIJE IN OSTALIH KOMUNIKACIJ V SODOBNIH OBOROŽENIH SILAH

Za današnjo globalno družbo je značilna informatizacija vseh aspektov družbenega življenja. Tako je informacijska tehnologija postala nosilec ekonomskega, političnega in vojaškega razvoja. Glavni problem v tej opredelitvi se nahaja prav v prepadu med sodobnimi informacijskimi in sodobnimi industrijskimi družbami, kjer je delež uporabnikov informacijske tehnologije relativno majhen v primerjavi z industrijsko razvitimi državami.

V nadaljevanju sledi tabela oziroma preglednica razširjenosti uporabe osebnih računalnikov, kot drugi indikator pa bo predstavljeno število uporabnikov internetnih storitev.

Tabela 3.1: Pregled petnajstih vodilnih držav v svetu glede na skupno število računalnikov in števila uporabnikov interneta (september 2007), skupaj s Slovenijo[4]

DRŽAVA (vrstni red)	Število računal. v mil.	Delež v celotnem številu (%)	Število upor. interneta v mil.	Delež glede na št. prebivalcev (%)	Mesto glede na št. upor. interneta
1. ZDA	240.5	24.15	210.2	71	3.
2. Japonska	77.95	7.83	131.1	61	7.
3. Kitajska	74.11	7.44	90.9	5,6	14.
4. Nemčija	54.48	5.47	67.6	66	5.
5. Velika Britanija	41.53	4.17	50.3	67	4.
6. Francija	35.99	3.61	39.7	56	8.
7. Južna Koreja	30.62	3.07	35.0	63	6.
8. Italija	29.31	2.94	32.0	49	9.
9. Rusija	26.97	2.71	31.6	19	12.
10. Brazilija	25.99	2.61	29.5	14	13.
11. Kanada	25.10	2.52	27.6	73	1.
12. Indija	21.17	2.13	23.3	2	15.

[4] Podatki za Slovenijo so vzeti iz delno primerljivih virov (Internet 5 in Internet 6).

13. Avstralija	15.47	1.55	22.7	72	2.
14. Mehika	14.77	1.48	20.6	14	13.
15. Španija	13.42	1.35	17.8	29	10.
16. Slovenija*	0,535	0,07	1,06	27	11.
Prvih 15 držav	727.4	73.00	829.9		
Skupaj - Svet	996.1	100.0	1,216		

Vir: Internet 4, Internet 5.

Iz tabele je jasno razvidno, da prvih petnajst držav, v katerih je prisotnost osebnih računalnikov v gospodinjstvih največja, zaseda vodilna mesta v razvrstitvi glede na število uporabnikov internetnih storitev. Od samega števila uporabnikov je še bolj presenetljiv podatek, da teh vodilnih petnajst držav v svetu obvladuje tako rekoč slabe tri četrtine računalniških (73 %) in internetnih (68,3 %) uporabnikov celotne svetovne populacije.

Glede na zgornje podatke je vidno, da so informacijski sistemi, ki delujejo v vitalnih ekonomskih, političnih in vojaških sferah, ogroženi bolj kot kadarkoli prej, saj se število računalnikov in dostopov do interneta veča s svetlobno hitrostjo, kjer ideološka usmerjenost sistemov ni nobena ovira, s tem pa tudi ni omejen dostop škodoželjnim akterjem, ki želijo za vsako ceno ovirati oziroma onesposobiti za določeno državo ali sistem benevolentne procese znotraj informacijskega sektorja.

Indikator, ki prav tako kaže tehnološki in s tem tudi informacijsko-komunikacijski razvoj določene države, je definitivno raziskovalno-razvojna dejavnost oziroma inovacije. Inovacija je lahko nova ideja, nov proizvodni ali tehnološki postopek, nov izdelek ali predmet z novimi funkcijami. Vse sodobne družbe z razvitim gospodarstvom si prizadevajo, da imajo čim več inovacij, zato v te namene investirajo velika finančna sredstva. Moč držav se danes meri tudi po številu prijavljenih, še bolj pa uporabljenih inovacij.

Tako so ZDA med leti 2002 in 2006 za raziskovalno in razvojno dejavnost namenile 2,68 % BDP oziroma dobrih 371 milijard dolarjev, Velika Britanija je za isto dejavnost namenila 1,9 % BDP oziroma dobrih 52 milijard dolarjev, Slovenija pa je za to

dejavnost namenila 1,61 % BDP oziroma dobrih 74 milijonov dolarjev (Internet 7). Inovacijsko moč oziroma napredek določa zgoščen inovacijski indeks, določen glede na dvajset inovacijskih kazalnikov. V povprečju gledano med leti 2000 in 2005 imata najvišji inovacijski indeks Japonska ter ZDA, kjer se le-ta giblje med 0,58 ter 0,82, medtem ko se ta indeks za skupek držav v Evropski uniji giblje med 0,39 in 0,42, kar jasno kaže na dejstvo, da je količina vloženega denarja v raziskovalno dejavnost veliko nižja kot pri Japonski in ZDA. Zgoščen inovacijski indeks je februarja 2008 za Slovenijo znašal 0,35, za Veliko Britanijo pa 0,57 (Internet 8)

V naslednji tabeli bom prikazal razširjenost komunikacijskih sredstev v izbranih državah, kjer bom pod drobnogled vzel telefonijo, televizijo, in radio. V sklop izbranih držav spadajo Slovenija, Velika Britanija in Združene države Amerike (ZDA), saj se bom kasneje opiral na reorganizacijo vojske oziroma ustvarjanje novih enot, ki so posledica pojava informacijskih operacij, prav v teh državah.

Tabela 3.2: Primerjava razširjenosti komunikacij v državah

	ZDA		**Velika Britanija**		**Slovenija**	
Št. prebivalcev	301.139.947		60.776.238		2.009.245	
Telefonija- št. stac. telefonov	172 mil	0,6 na prebivalca	33.602 mil	0,55 na prebivalca	837.500	0,41 na preb.
Telefonija- št. mobilnih tel.	233 mil	0,8 na prebivalca	69.657 mil	1,15 na prebivalca	1.82 mil	0,91 na preb.
Telefonski sistem	***splošni:*** velik, tehnološko napreden, večnamenski komunikacijski sistem ***domači:***širok sistem optičnih kablov, mikrovalovni radio-relejni sistem in sateliti za domačo uporabo prenašajo vse oblike telefonskih pogovorov; hitro rastoč sistem		***splošni:*** tehnološko napredni domači in mednarodni sistemi ***domači:*** sorazmerna uporaba vkopanih telefonskih kablov, mikrovalovnih radio-relejnih zvez in optičnih sistemov ***mednarodni:*** klicna številka - 44; število podmorskih napeljav zagotavlja povezavo z Evropo, Azijo, Avstralijo, Bližnjim Vzhodom ter ZDA;		***splošni:*** dobro razvita telekomunikacijska infrastruktura ***domači:*** kombinirana stacionarna povezava in mobilna zagotovitev omrežij dosegata 130 telefonskih aparatov na 100 oseb ***mednarodni:*** klicna številka - 386	

	mobilne telefonije omogoča telefonske pogovore po vsej državi ***mednarodni:*** klicna številka - 1; več oceanskih kabelskih sistemov zagotavlja mednarodno povezavo; zemeljske satelitske postaje - 61 Intelsat (45 Atlantski ocean in 16 Tihi ocean), 5 Intersputnik (Atlantska regija) in 4 Inmarsat (Atlantska in tihomorska regija)		zemeljske satelitske postaje - 10 Intelsat (7 Atlantski ocean in 3 Indijski ocean), 1 Inmarsat (regija atlantskega oceana) in 1 Eutelsat; najmanj 8 velikih mednarodnih preklopnih centrov			
Št. radijskih postaj*[5]	13.769	1 na 21.870 prebiv.	653	1 na 93.072 prebiv.	240	1 na 8.371 prebiv.
Št. televizijskih postaj	2.218	1 na 135.770 prebiv.	228 (+ 3.523 repetitorjev)	1 na 266.562 prebiv.	31	1 na 64.814 prebiv.
Državna domen interneta	.us		.uk		.si	

Vir: Internet 9.

V tabeli je predstavljena razširjenost komunikacijskih sredstev ozirom tehnologije v izbranih državah. Opazimo, da je razširjenost stacionarnih telefonskih linij najmanjša v Sloveniji, sledi ji Velika Britanija, ki pa ne zaostaja veliko za ZDA. Pri razširjenosti mobilnih telefonov se glede na prebivalca ZDA in Slovenija ne razlikujeta veliko. Za obe državi je namreč značilno, da je razmerje stacionarnih telefonov glede na prebivalca manjše od ena. Na tem mestu me je zelo presenetila Velika Britanija, kjer razširjenost mobilnih telefonov obvladuje kar 1,15 mobilnega telefona na prebivalca.

[5] Med radijske postaje so vštete AM, FM in tudi kratko-valovne radijske postaje, in sicer: ZDA (AM 4,789, FM 8,961, kratko-valovne 19), Velika Britanija (AM 219, FM 431, kratko-valovne 3) in Slovenija (FM 230).

Glede razvitosti telekomunikacijskih infrastruktur ni bilo pričakovati večjih presenečenj, saj je jasno, da imajo države z večjo finančno močjo in večjimi globalnimi interesi bolj razvit telekomunikacijski sistem. Kot primerjavo kazalnika razvitosti telekomunikacijskega sistema bi izpostavil zemeljske satelitske postaje. ZDA namreč posedujejo 70 zemeljskih satelitskih postaj za razliko od Velike Britanije, ki ima v uporabi 12 zemeljskih satelitskih postaj, ter nazadnje tudi Slovenija, ki le-teh nima, saj so finančni prilivi za to področje manjši, pa tudi ne obstajajo tako veliki interesi in potrebe, ki bi pogojevale takšne sisteme.

Razlika pri razširjenosti telekomunikacijske tehnologije je vidna šele pri manjši sofisticiranosti sistemov, kjer merim predvsem na razširjenost radijskih in televizijskih postaj. Pri obeh kazalcih ima najboljše razmerje na prebivalca Slovenija, ki ima v povprečju eno radijsko postajo na 8371 prebivalcev, medtem ko se največje razmerje pokaže pri Veliki Britaniji, ki ima eno radijsko postajo na 93072 prebivalcev. Tudi pri razširjenosti televizijskih postaj prednjači Slovenija z eno televizijsko postajo na 64814 prebivalcev, najslabše razmerje pa ponovno najdemo v Veliki Britaniji z eno televizijsko postajo na 266562 prebivalcev, pri čemer je potrebno poudariti, da pri računanju razmerja televizijskih postaj na prebivalca v Veliki Britaniji nisem upošteval 3523 repetitorskih postaj.

Iz navedenih tabel sledi, da je število tarčnih ciljev (radio, televizija, internet) informacijske in komunikacijske tehnologije v Sloveniji glede na prebivalca manjše kot v drugih dveh izbranih državah, kar pomeni, da je tudi ponudnikov informacijsko-komunikacijske tehnologije manjše, s tem pa se tudi zmanjša kompleksnost onesposabljanja teh medijev v primeru želje po motenju ali prekinjanju le-teh. Iz zgornje analize je razvidno, da ima Slovenija v primerjavi z ZDA in Veliko Britanijo boljšo radijsko in televizijsko pokritost, kar pa dejansko kaže na to, da razvitost informacijsko-telekomunikacijskih sredstev, uporabljenih v nevojaške namene, ni odvisna od stopnje vojaške razvitosti določene države, kar bom v naslednjih korakih tudi dokazal.

3.1 Informacijska orožja

Pri opredeljevanju do tega pojma sem naletel na težavo, in sicer gre za postavitev mej, kaj je smiselno opredeliti kot informacijsko orožje in kaj ne. Če na primer izpostavimo navadno letalsko bombo, ki zadane določeni poveljniško-informacijski sistem oziroma njegovo za obstoj benevolento komponento (na sistem električnega napajanja), jo lahko prištevamo med informacijska orožja. Enako se lahko opredelim do navadne pištole, s katero določena oseba ubije programerja, s tem pa jo lahko prištevamo med informacijska orožja. Opisane primere potencialnega informacijskega bojevanja oziroma fakturiranja informacijske oboroženosti bom v diplomskem delu opustil, saj so orožja v teh primerih konvencionalna in ne informacijska in so kot takšna zgolj dosegla informacijski cilj.
Med informacijska orožja sodijo:

- **Računalniški virusi –** so fragmenti (deli) kod, ki se kopirajo v večji program in ga s tem tudi modificirajo ter mu dodajo nove karakteristike oziroma lastnosti. Virus je dejaven le v primeru, ko je program, kot poosebljena verzija gostitelja, v pogonu, nakar se v svojem delovanju »razmnoži« in »okuži« programe, s katerimi je v stiku. Virusi so najbolj razširjeno »orožje« informacijskega bojevanja, saj so sami po sebi tudi najbolj dostopni. Za izdelavo le-tega je potrebno poznavanje programa in informacijskega sistema, kateremu je namenjen, ter par spretnih rok, ki s pomočjo virusa ta sistem modificira v svoj prid[6] (Puš 2000, 18).

- **Črv –** je podrazred virusa in je neodvisen program, ki se brez dejanja uporabnika kopira preko omrežnih povezav in do neskončnosti razmnožuje z enega računalnika na drugi računalnik. Za razliko od virusov ne spreminja drugih programov, zelo hitro pa obremeni podatkovne baze in medsebojne komunikacije do te meje, da postanejo neuporabne. Črv je informacijsko orožje,

[6] Lahko si zamislimo situacijo, v kateri nasprotnik v računalniško vodeno centralo vstavi virus. Posledice so lahko katastrofalne, saj lahko izključi vse možne telefonske povezave, zmede centralo do stanja kaosa in popolnoma onemogoči komuniciranje.

ki se lahko prilagodi temu namenu, da zbriše podatke in druge programe[7] (Internet 11).

- **Trojanski konj –** je del kode, skrite v normalnem programu. Mitološki trojanski konj je bil navidezno darilo, v katerem so se skrivali grški vojaki, ki so zavzeli Trojo, računalniški trojanski konji pa so računalniški programi, ki so videti kot uporabna programska oprema, vendar ogrozijo računalnik in povzročijo precej škode. Nedavni trojanski konj je potoval v obliki elektronske pošte s prilogami, ki so se izdajale za varnostne posodobitve podjetja Microsoft, a so bile v resnici virusi, ki so poskušali onesposobiti požarne zidove in protivirusno programsko opremo. Trojanski konji se širijo, ko uporabniki odprejo program, za katerega verjamejo, da prihaja iz pristnega vira. Microsoft uporabnikom pogosto pošilja varnostna opozorila po elektronski pošti, vendar nikoli ne vsebujejo priloženih datotek (Internet 10).

- **Logična bomba –** podvrsta trojanskega konja, ki se uporabi za sprostitev skritega virusa, črva ali druge oblike orožja. Pojavlja se v obliki neodvisnega programa, vstavljena pa je ob programiranju s strani programerja ali vzdrževalca sistema[8]. Logična bomba se lahko sproži z določenimi besednimi zvezami, kot na primer Krieg – Deutschland (ob predpostavki, na primer, da je izdelovalec določene programske opreme določeno nemško podjetje, ki je vstavilo logično bombo z eskalacijo ob določenem geslu), s tem pa se sproži skriti črv ali trojanski konj, ki je v tem računalniku. Zaradi povezanosti računalnika v mreže se tak napad z logično bombo zelo hitro razširi in zaustavi delovanje celotnega sistem v tistem okolju (Internet 10).

- **Stranska vrata –** termin, ki ga uporabljamo za mehanizem, ki ga v program vgradi njegov tvorec. Naloga rezervnih vrat je omogočanje prikritega vstopa programerja v sistem in obhod vgrajenih varnostnih mehanizmov (gesel,

[7] Pred črvi so močno zaščitena predvsem bančna podjetja in podjetja s primarno socialno dejavnostjo. Največji strah v zadnjih letih je povzročil milenijski črv Y2K (ob prehodu na leto 2000), zaradi katerega so v svetu trepetala prenekatera podjetja, posebno pozornost pa so temu črvu posvetili predvsem v nuklearni dejavnosti, kot so na primer nuklearne elektrarne.

[8] Ob dejstvu, da je velika večina svetovne programske opreme narejena in v lasti ameriških podjetij in posameznikov, je popolnoma možno, da ameriška vlada ali vojska v programsko opremo po vsem svetu vstavlja logične bombe, ki bi ji v primeru spopada dala odločujočo prednost pred nasprotnikom.

programske zaščite in podobno). Z množično uporabo programske opreme določenega proizvajalca je le-temu, v primeru da ta program uporabljajo tudi vladne službe, omogočen dostop do vseh informacij na vseh ravneh varnostno-zaupnega rangiranja podatkov. Tak sistem po eni strani deluje hipokritsko, vendar lahko preko rezervnih vrat razkriješ morebitne nasprotnikove namere (Internet 10).

- **Prirejena integrirana vezja –** navadni računalniški programi lahko vsebujejo nenavadne oziroma nepričakovane funkcije. Prav tako pa je mogoče iste funkcije vključiti v strojno opremo. Čipi, ki so dandanes prisotni v skorajda vseh elektronskih sistemih, vsebujejo nekaj milijonov integriranih vezij, ki jih proizvajalec zlahka prilagodi tako, da opravljajo želeno funkcijo. Možnosti so neskončne. Čipi so lahko narejeni na primer z namenom hitre kvarljivosti, poškodbe ob sprejemu določene radijske frekvence, z namenom pošiljanja specifičnega signala in s tem izdajanja lokacije nahajanja osebe ali sistema, kateremu je bil namenjen, in še bi lahko naštevali (Internet 10).

- **Mikroroboti in genetsko prirejeni mikrobi –** ponujajo možnost zadajanja večjih poškodb računalniške opreme. Za razliko od računalniških virusov jih lahko uporabljamo za napad na strojno in ne le na programsko opremo. Mikroroboti so roboti, ki dosegajo velikost, manjšo od mravelj, in se lahko »dostavijo« v sovražnikovo poveljniško mesto (odmetavanje z letal ali drugače). Njihov učinek je viden, ko fizično dosežejo računalnik in uničijo vezja ter napajanje.

  Drugo vrsto fizične grožnje računalniškim vezjem predstavlja posebna vrsta mikrobov. Mikrobi se uporabljajo pri ekoloških katastrofah, kjer razgrajujejo in vsrkavajo olja, zato je na tem mestu tudi vprašanje pojava mikrobov, katerih naloga je razgradnja silicija, kar pomeni, da bi v trenutku uničili vsa integrirana vezja v laboratoriju, poveljstvu, zgradbi ali mestu (Internet 10).

- **Elektronsko motenje –** v preteklosti se je elektronsko motenje uporabljalo predvsem za preprečevanje sovražnikove komunikacije v radijskem prometu in ostalih vrstah telekomunikacij. Danes se poleg te vrste distrakcije elektronsko

motenje uporablja tudi za preplavljanje sovražnikovih sistemov z obilico podatkov in dezinformacij (Puš 2000, 18).

- **Visokofrekvenčna orožja (ang. High Energy Radio Frequency Gun – HERF Gun) –** takšna orožja oziroma pištole so sposobna imitirati radijski signal izjemno velike moči, katerega namen je poškodovanje ali uničenje elektronskega cilja. Škoda je lahko umirjena, kar pomeni, da je sistem lahko ugasnjen, vendar ga je kasneje možno ponovno vključiti, ali resna, kadar ob imitiranju radijskega signala pride do uničenja elektronskega vezja, ki je zelo občutljivo na preobremenitvene vrednosti signalov. Visokofrekvenčno pištolo bi lahko poenostavljeno opisali kot radijski oddajnik z usmerjenim delovanjem, katerega cilj je lahko računalniški sistem v zgradbi, letalo, vozilo z elektronsko opremo ipd (Internet 10).

- **Bombe z elektromagnetnim pulzom (ang. Electro Magnetic Pulse Bomb – EMP Bomb) –** vir elektromagnetnega pulza je lahko nuklearna ali drugačna eksplozija. Slednjo lahko uporabijo enote, ki se infiltrirajo v bližino nasprotnikovega poveljniško-informacijskega sistema in to eksplozijo sprožijo. Eksplozija uniči elektronsko in komunikacijsko opremo v velikem radiju. Sama velikost EMP bombe je lahko manjša od frekvenčne pištole, vendar povzroči večjo škodo, pri čemer je potrebno poudariti, da se EMP bomba uporablja na masovnih ciljih in ne na posamičnih računalnikih, vozilih in telekomunikacijskih sredstvih, za razliko od visokofrekvenčne pištole (Puš 2000, 18, Internet 10).

3.2 Vojaško informacijsko okolje

Znotraj globalnega okolja oziroma prostora, v katerega so vključeni kopno, voda, zrak in tudi vesolje, najdemo okolje, ki pred tridesetimi leti še ni obstajalo. To vojaško informacijsko okolje je definirano kot okolje, ki je vključeno znotraj globalnega informacijskega okolja in je sestavljeno iz informacijskih sistemov in organizacij (prijateljskih in sovražnih, vojaških in nevojaških), ki podpirajo, omogočajo ali močno vplivajo na določeno vojaško operacijo. Za vojaško informacijsko okolje je značilno, da:

- **sega v prostor od domače postojanke do okolja operacije;**
- **sega od začetka faze alarmiranja do faze povratka;**
- **obsega namene od taktične naloge do ekonomskih ali socialnih namer države;**
- **vključuje ljudi, od vojakov na terenu, njihovih družin doma do lokalne ali regionalne populacije in svetovnega občinstva** (Internet 1).

Z razvojem in širitvijo informacijske tehnologije se je bojevanje in sam pogled odločujočih na to dejavnost zelo spremenil in informacijska tehnologija je že bistveno spremenila vojne oziroma vojskovanje, še posebej sestavo in tehnologijo oborožitvenih sistemov in s tem tudi doktrino in načine bojevanja ter organiziranosti, še več: bojišče je skoraj v celoti, če ne že kar celega, elektronizirala oziroma ga naredila digitalnega.

3.3 Digitalno bojišče

Znano je, da v vsakem človeškem obdobju moderna tehnologija in s tem povezani koncepti zaznamujejo vojno. Tako sta v času rimskega imperija in v času Aleksandra Velikega kot najmodernejši obliki bojevanja prevladovali vojaški formaciji legija in falanga, razvita je bila oblegovalna tehnika, kot so katapulti, baliste in podobno, nakar so do iznajdbe smodnika, kot merilo razvitosti in moči, glavno vlogo v vojski prevzeli konji oziroma težko opremljeni konjeniki. Z iznajdbo smodnika se začne način bojevanja spreminjati, poveča se domet orožja, s tem pa tudi površina samega bojišča. Nekje do prve svetovne vojne je gonilna sila vojske človek, sredstvo za uresničevanje ciljev pa puška, vendar to obdobje pomeni prelomnico v bojevanju in s pojavom tankov, podmornic ter nenazadnje tudi orožja za tretjo dimenzijo bojevanja – letal, postavi mejnik vojskovanja, od koder ni več vrnitve. Od takrat dalje je moč spoznati, da gonilo vojska ni več človeška mišica, temveč stroj, ki za nekajkrat nadomesti to mišico, vendar človek ne počiva. Z izumom vezij, računalnikov, laserjev in druge podobne elektronske opreme se človek v začetku devetdesetih (predvsem v času prve Zalivske vojne), spusti v dimenzijo bojevanja, ki je bila do takrat nepoznana. Govorim o informacijski, digitalni vojni. Nekateri trdijo, da je bila prva Zalivska vojna prva informacijska vojna, drugi, da je bila to zadnja industrijska vojna.

Znan teoretik Alberts digitalno vojno opiše kot »del informacijske vojne, vključuje pa nefizične napade na informacije, informacijske procese in informacijsko infrastrukturo, ki ogrožajo, spreminjajo, uničujejo ali razbijajo informacije in preprečujejo, onemogočajo ali dezinformirajo procesiranje informacij in proces odločanja.« (Alberts 1996, 43)

Digitalna vojna ima vse potrebne lastnosti, ki so dobrodošle pri tradicionalnih vojaških načrtovalcih, saj jo zaznamujejo nizki stroški, nevidnost in delovanje iz daljave. Digitalna vojna ogroža sposobnost vojaške organizacije nacionalnih držav, da se vrinejo med lastnim prebivalstvom in sovražnikom, vojaška organizacija pa na ta način izgublja monopol za vodenje vojne, ki se odraža na številnih družbenih področjih in procesih, med katerimi je izguba legitimnosti vojaške organizacije (Svete 1999, 47).

Dejstvo je, da se z razvojem informacijske tehnologije želi bojišče vizualizirati in ga spremeniti v bojevanje na daljavo. Tako so v sodobnih vojskah v uporabi sistemi[9] za zbiranje satelitske slike, slik in podatkov, ki prihajajo od majhnih letal brez pilota (Unmanned Aerial Vehicle – UAV) nad bojiščem, radarjev in vseh drugih virov, ne nazadnje tudi od opazovalcev na tleh. Računalniki predelajo vse vhodne informacije in v realnem času ustvarjajo sliko bojišča z ažurnimi podatki o položaju sovražnih, pa tudi lastnih enot ter njihovem taktično-logističnem statusu. Na sliki so vidne pozicije tankov, bojnih in drugih vozil ter tehnike nasploh, pa tudi različne dodatne informacije, ki se potem pošiljajo po mreži na zaslone računalnikov v tankih, bojnih vozilih in na drugih platformah. Po mreži se neprestano pretakajo elektronska pošta, informacije o lokacijah in premikih sovražnika, pa tudi predvidevanja o njegovih namerah (Internet 12).

Vizualizacija bojišča omogoča hitrejše zaznavanje nasprotnika in ugotavljanje sovražnikovih koordinat, to pomeni, da je sovražnika mogoče tudi hitreje uničiti. Sočasno se povečujejo bojna učinkovitost in možnosti preživetja. Zelo se skrajša čas od nastanka problema do sprejetja bojnih odločitev in ukrepanja. Vse to pa so ključni elementi, ki zagotavljajo dobljeno bitko.

[9] Primer takšnega sistema v ameriški vojski je informacijski sistem **FBCB2** (Force XXI Battle Command Brigade and Below system), namenjen poveljevanju na ravni brigade in povezavi s komandno-kontrolnim sistemom na višjih ravneh. FBCB2 je podprt z brezžičnim taktičnim komunikacijskim omrežjem, na katerem je natovorjen tako imenovani taktični internet (Internet 12).

Vsako vozlišče sistema, ki integrira radijsko zvezo, računalnik, GPS in po potrebi še druge komponente, kot so laserski namerilnik, sistem za kontrolo ognja, termovizija, videokamera in podobna tehnika, je nameščeno na mehanizirani platformi. Vse skupaj je torej kompleksen sistem na vozilih inštalirane računalniške mreže, ki je povezana še z UAV-ji in drugimi viri inteligence. Pričeli smo govoriti o digitalnem bojišču, ki je zlasti po letu 1997 postalo predmet zelo intenzivnih raziskav in razvoja vojska širom po svetu.

Na začetku diplomske naloge sem po Alfinu Tofflerju razdelil zgodovino bojevanja na tri dele, in sicer na agrarni val, industrijski val ter informacijski val, ki se je začel s pojavom integriranih vezij in računalnikov. Po Tofflerju je zamisel industrijskega vala uresničena v zgoraj opisanem digitaliziranem bojišču oziroma v procesu C^4I, ki ponazarja sodoben način vodenja in poveljevanja, zaradi katerega se v sedanjosti prestrukturira ter ponovno opremlja marsikatera vojska, saj brez tega procesa tako rekoč ni moč doseči superiornosti[10] na bojišču.

3.4 C^4I sistemi

Sodobna tehnologija je nekajkrat povečala gibljivost enot, hitrost in natančnost izvajanja bojnih nalog, domete in natančnost orožij in bojnih sistemov ter povečala njihovo učinkovitost. To je vodilo k hitrejšemu razvoju dogodkov na bojišču. Sistemi C^4I so kakovostno nadgradili procese zbiranja, prenašanja in obdelovanja informacij ter odločanja, vodenja in poveljevanja. Osnovni namen teh sistemov je povečati hitrost in učinkovitost bojevanja.

---

[10] Leta 1997 je ameriška vojska izvajala vajo pod imenom Fleet Battle Experiment Alpha, ki je preigravala scenarij, znan pod imenom Hunter-Warrior. Šlo je za različne možnosti, kako ustaviti iraško invazijo na Kuvajt. Rezultati vaje so bili več kot zadovoljivi. Računalniki za kontrolo ognja na vseh ladjah so bili povezani v lokalno mrežo, ki je povezala vsa orožja v enoten sistem. Komandni center je dobival videoslike in druge informacije iz letala USAF J-Stars, izvidniškega letala U-2 in UAV. Na bojišču je bilo le 56 marincev. V oddaljenem komandnem centru se je ustvarila elektronska slika bojišča v realnem času. Sistem je izbral cilje, najprimernejše orožje in poslal potrebne podatke izbranemu sistemu za kontrolo ognja v mreži. "Napadalec", ki je štel nekaj tisoč vojakov in bil oborožen s težkim oklepnim orožjem, je bil zaustavljen. Tokrat sta se preizkušali nova doktrina in organiziranost. Pretok informacij in ukazov je bil tako hiter, da se je včasih izgubila preglednost nad dogajanjem, čeprav preglednost bojišča nikoli dotlej ni bila boljša (Internet 13).

Oznaka **C^{4}I**[11] stoji za procese vodenja in poveljevanja, značilne za sodobno bojišče, in sicer:

- **Command –** vodenje;
- **Control –** poveljevanje, nadziranje;
- **Communication –** komunikacije oziroma povezanost med enotami;
- **Computers –** računalniki (informacijska komponenta, ki je obogatila oznako C^{3}I šele v osemdesetih letih, prvič pa je bila preizkušena med prvo Zalivsko vojno in je pomenila velik tehnično-tehnološki preskok ter prehod iz industrijskega v informacijsko bojevanje);
- **Intelligence –** podatki o lastnih in nasprotnih enotah, zemljišču in vremenu.

S kratico C^{4}I bi zgoraj navedene termine preprosto povzel v stavek, ki pravi, da je sistem C^{4}I proces vodenja in poveljevanja, podprt s sodobno tehnologijo in z nenehnim pridobivanjem informacij v realnem času.

Sestava C^{4}I Sistemov (Internet 14)

Za jasnejše potrebe preoblikovanja in s tem pogojenim opremljanjem sodobnih vojska moram nakazati delitev C^{4}I sistemov v skupine in podskupine, ki so naslednje:

- **POVELJNIŠKO – INFORMACIJSKI SISTEMI**
    - Integrirano poveljniško – informacijski sistemi
    - Meteorološko – informacijski sistemi
    - Sistemi za upravljanje artilerijskega ognja
    - Sistemi za nadzor in kontrolo zračnega prostora
    - Sistemi za upravljanje sistemov zračne obrambe
    - Sistemi za nadzor in opazovanje bojišča
    - Informacijski sistemi enot za hitro posredovanje
    - Integrirani sistemi za podmorniško bojevanje
    - Mornariški bojni C^{4}I sistemi

[11] Struktura **C^{4}I** je vedno bolj kompleksna. Na to kaže dejstvo, da se v sklopu sistemov C^{4}I pojavljajo novi elementi, tako da ima sistem obliko C^{4}I SR (+ surveillance and reconnaissance – nadzor in izvidovanje) in celo C^{5}I (z dodatkom bojnih sistemov – combat systems).

- **KOMUNIKACIJSKI SISTEMI**
  - Satelitski sistemi
  - Integrirani komunikacijski sistemi
  - Bojni radijski sistemi HF, VHF, UHF
  - GPS sistemi

- **SISTEMI ZA ZBIRANJE PODATKOV**
  - Radarski sistemi za nadzor in lokacijo
  - Sistemi za detifikacijo IFF
  - Senzorski sistemi za izvidovanje in nadzor prostora
  - Sistemi za zgodnje opozarjanje in nadzor AWACS
  - Sistemi za zgodnje opozarjanje in odkrivanje balističnih raket
  - Sistemi za odkrivanje artilerijskih položajev

- **SISTEMI ZA ELEKTRONSKO BOJEVANJE**
  - Sistemi za radio lokacijo DF
  - Sistemi za prisluškovanje
  - Sistemi za analizo signalov
  - Sistemi za motenje
  - COMINT in ELINT sistemi

- **RAČUNALNIŠKI HARDVERSKI SISTEMI IN SOFTVERSKI IZDELKI**

C^4I sistem zagotavlja podatke preko različnih sistemov za zbiranje podatkov, jih analizira in predlaga optimalno rešitev uporabe oborožitvenih sistemov, ki so z njimi povezani. Naloga C^4I sistema je zbiranje, ocena in analiza zbranih podatkov z različnih senzorjev in ostalih podsistemov za zbiranje podatkov, povezanega s podsistemom za elektronsko bojevanje, spremljanje dinamike lastnih sil in odkrivanje ter spremljanje sistemov in enot nasprotnikovih sil, analizo trenutnega stanja in iz tega izhajajoč predvidenega stanja v bližnji prihodnosti ter distribucijo podatkov lastnim enotam in usmerjanja oborožitvenih sistemov na odkrite cilje.

Vsi elementi takšnega sistema so glede na načela uporabe v centrih za izvajanje tehnične analize in upravljanje z vsemi izvori podatkov TCAE (Technical controll all source element), ki so na nivoju bataljona oziroma brigade, na višjem nivoju pa se podatki iz teh centrov združujejo in analizirajo v centru za upravljanje z bojnimi kapacitetami divizije ali korpusa, kamor prihajajo še ostali obveščevalni podatki in kjer se izvaja zaključna obdelava podatkov, iz katere sledi operativno taktična ocena situacije. Tako obdelani podatki se hranijo v bazi korelacijskih podatkov ASCDB (All Source Correlation Data Base). Končna obdelava teh podatkov je zasnovana na obdelavi ciljev (Target Development), kar pomeni identifikacijo ciljev in način nevtralizacije le-teh, ki so posredovani enotam za ognjeno podporo ali enotam za elektronsko bojevanje. Nevtralizacija ciljev se vrši z ognjenim udarom in fizičnim uničenjem ali z elektronskim motenjem oz. zavajanjem ali z drugimi načini uporabe različnih podsistemov.

S spremljanjem razvoja najsodobnejših vojska na svetu se jasno kaže tendenca večine vojaško manj razvitih držav k razvoju sistemov C^4I, ki omogočajo upravljanje in koordinacijo z vsemi ostalimi podsistemi, ki zagotavljajo manever, ognjeno moč in kot končni rezultat tega – nadvlado, premoč in zmago.

Jasno je, da se je s pojavom informacijske tehnologije, glede na bojišče, in s tem tudi C^4I sistemov, ki omogočajo učinkovitost delovanja v informacijskih operacijah, v večini vojska po svetu pojavila potreba po modernizaciji vojske, sploh sistemov vodenja in poveljevanja, posledično pa se je spremenila tudi slika sodobnega bojišča in sestava vojska, ki na tem bojišču participirajo.

Za sodobno bojišče je z vidika vojaške organizacije značilno:

- **nenehno pridobivanje informacij v realnem času;**
- **visoka stopnja gibljivosti enot** (hitri premiki, manevri in hitro spreminjanje razmer);
- **neprekinjeno delovanje –** dnevno-nočne aktivnosti v vseh vremenskih razmerah, ki jih omogočata sodobna oborožitev in oprema;

- **C^4I sistemi –** ki zagotavljajo decentralizirano vodenje in poveljevanje in omrežno 3D povezovanje, sodelovanje in soudejstvovanje (vesolje, zrak, voda, kopno, cyberspace) ter nelinearno bojevanje;
- **natančnost in usmerjenost delovanja –** pametna (»inteligentna«) orožja in optimalna ognjena moč glede na porabo streliva;
- **večplastna in večdimenzionalna zaščita;**
- **usmerjena logistika** (Kočevar 2006, 23)**.**

5 NOVA STRUKTURA SODOBNIH VOJSKA ZARADI POJAVA INFORMACIJSKIH OPERACIJ

S pojavom informacijskih operacij so bile vojske prisiljene reorganizirati sestavo svojih vrst, predvsem ustanavljanje novih enot za informacijsko bojevanje ofenzivne in defenzivne narave. Kot glavno spremembo in odgovor na pojav informacijskih operacij velja omeniti profesionalizacijo vojske, saj zahteva takšna tehnika višjo izobrazbo in daljše služenje roka kot šest ali sedem mesecev. Primere preoblikovanja oboroženih sil bom predstavil na osnovi izbranih držav, ki sem jih primerjal že v razširjenosti telekomunikacijske tehnologije, to so ZDA, Velika Britanija in Slovenija.

5.1 Preoblikovanje sodobnih oboroženih sil

V obrambni politiki večine držav znotraj zveze NATO[12] in zunaj nje je moč opaziti dokaj kontradiktorno situacijo, saj se po eni strani nadaljujejo pritiski za zmanjševanje obsega oboroženih sil in obrambnih proračunov, po drugi strani pa se zahteva prilagodljivost, večstranskost in mnogofunkcionalnost oboroženih sil. Narava vojskovanja se je v zadnjih sto letih spremenila bolj kot v vseh prejšnjih 3500 letih zahodne civilizacije. Hitrost, s katero se pojavljajo nove tehnologije, spreminja naravo sodobnega vojskovanja hitreje kot kadarkoli doslej, tehnološke spremembe pa so privedle do tako temeljnih in obsežnih sprememb v vojskovanju, da se pojavlja veliko vprašanje kontinuiranega zadovoljevanja potreb po ustrezni kadrovski sestavi, saj za takšno vrsto tehnologije, ki je sedaj prisotna v sodobnih oboroženih silah, kjer se vojaki bojujejo v informacijskem okolju, in se še nadgrajuje, niso dovolj le osnovnošolske in srednješolske izobrazbe, temveč strokovna usposobljenost vojakov na višjih ravneh izobrazbe.

5.1.1 KADROVSKE POTREBE

Za sodobno bojišče je značilno, da se sistemi za bojevanje ne nameščajo samo na mehanizirane platforme, pač pa tudi na vojaka, ki se integrira v informacijsko okolje oziroma digitalno bojišče. V sklopu ameriške vojske poteka program Land Warior

[12] North Atlantic Treaty Organisation

(vojak 21. stoletja), ki deluje znotraj projekta Force XXI. Sodobni ameriški vojak je opremljen s tehnologijo, ki povezuje računalnik z zaslonom, vključenim v čelado, radijsko zvezo, GPS in laserski namerilnik ter videokamero, nameščeno na predelani karabin M4, v enoten sistem. Vojak, ki dosega merila sodobnega bojišča, je postal informacijsko vozlišče in vir podatkov, hkrati ima informacije o svojem položaju, pa tudi o položaju nasprotnika. Kamera in laserski namerilnik na M4 omogočata streljanje "okoli vogala" ali pa nad glavo iz zaslona, skratka, opremljen je s tehnologijo, za katero je potrebno imeti precej več nadgrajenega znanja, ki seveda stoji na trdni osnovni podlogi, ki kot samostojnejša enota ne zadovoljuje standardov sodobnega bojišča. Primer vojaka 21. stoletja je samo en primer od neštetih, kjer je jasno vidno, da so potrebe po strokovno usposobljenih kadrih neizmerne (Internet 15).

Dejstvo je, da je človek kljub izrednemu tehnološkemu napredku še vedno najpomembnejši dejavnik oboroženega boja in zato se v sodobnih vojskah predpostavljajo spremembe taktičnih in operativnih postopkov. Poleg sprememb v tehnologiji in vojaški tehniki so predvsem spremembe v človeškem dejavniku, in sicer na kvantitetni in kvalitetni ravni. Tehnološki napredek povečuje taktično in tehnično odgovornost vodij in vodenih pri upravljanju in vzdrževanju vse bolj kompleksnih oborožitvenih sistemov ter spremljajoče infrastrukture, po drugi strani pa začetne spremembe v teh postopkih razkrijejo večino pomanjkljivosti človeškega dejavnika, ki se ponavadi ni sposoben ustrezno odzvati novim zahtevam in jih zadovoljivo izpolniti (Kotnik-Dvojmoč 2002, 249). Zaradi drugačnih zahtev glede sposobnosti in usposobljenosti vojaškega kadra je v procesu urjenja in usposabljanja vse bolj poudarjena zahteva po preoblikovanju fizično in mentalno zelo sposobnih klasičnih herojskih bojevnikov v usposobljene tehnike. Vojaška organizacija ne potrebuje več nerazmišljujočega vojaka, ki je sposoben in pripravljen zgolj slepo izpolnjevati kakršnekoli ukaze, hkrati pa je nesposoben povezati vzrok in posledico ali poiskati različne poti za izvršitev zastavljene naloge.

Uvajanje zmogljivejših oborožitvenih sistemov je neposredno povezano tudi s kakovostjo vojaškega osebja[13]. Višja kot je kakovost vojakov na ravni inteligentnosti,

[13] Kot primer bi navedel nakupe transportnih helikopterjev znamke Cougar v slovenski vojski, kjer je bil seveda pogoj za uporabo le-teh izšolanje vojaških pilotov za pilotiranje teh vrst helikopterjev, poleg tega pa seveda tudi letalskih tehnikov, ki so zadolženi za servisiranje helikopterjev. V tem primeru nam v kadrovski sestavi slovenske vojske osnovnošolska ali srednješolska izobrazba ne pomagata kaj dosti, saj je za takšno sofisticirano vrsto tehnike treba imeti strokovno izobrazbo.

izurjenosti, morale in motiviranosti, lažji je sam proces upravljanja s kompleksnimi oborožitvenimi sistemi na sodobnem bojišču (Kotnik-Dvojmoč 2002, 250). Več istočasno izvedenih operacij zahteva večjo kakovost vojakov, ki upravljajo s takšnimi sistemi, ki se tudi pogosteje kvarijo, zato potrebujejo zelo kakovostno logistično podporo, to pa zahteva dobro izurjene vojake za izvajanje podpornih nalog. To je vidno ravno po pojavu tehnoloških sprememb, ki so v zadnjih dveh desetletjih povsem spremenile značilnosti sodobnih oborožitvenih sistemov in opreme ter posledično tudi metode bojevanja, kar je privedlo do povečanja avtonomije nižjih enot in posameznika ter, skladno s tem, tudi do spuščanja odločanja in delovanja na nižje hierarhične ravni. Na osnovi tega lahko predpostavim, da se bo usposobljenost pri vseh pripadnikih oboroženih sil še nadalje povečevala in da se bo razkorak v izobraženosti in usposobljenosti med vojaškimi in častniškimi dolžnosti vztrajno zmanjševal.

Iz zgoraj navedenih ugotovitev je razvidno, da se potreba po vsej večji specializaciji[14] skozi celotno hierarhijo spušča na nižje in tudi najnižje ravni, kar je ob hkratnem povečevanju obsega nebojnih nalog povzročilo neverjetno ekspanzivnost podčastniških ter nižjih častniških činov, čemur smo priča tudi v Sloveniji, kjer za to vrsto dogajanja oziroma preoblikovanja kadrovske strukture uporabljamo termin profesionalizacija vojske. Ta dejavnost ima nujno posledico zmanjševanja števila navadnih vojakov.

Vse bolj je torej pomembna visoka specializacija vsakega posameznika za opravljanje njegove osnovne naloge, vendar je ob tem po drugi strani vse bolj nujna tudi univerzalnost in zamenljivost, kar v zelo kompleksnem in vse bolj spremenljivem okolju sodobnih vojaških operacij zagotavlja kolikor toliko nemoteno in učinkovito opravljanje drugih nalog v moštvu, skupini in enoti (Adanić in Tatalović 1993, 5). Za učinkovito in optimalno uporabo visoko sofisticiranega orožja in opreme ter dosledno izpolnjevanje zadanih nalog je po eni strani zahtevana vse višja stopnja specializacije, po drugi strani pa se pojavi vprašanje nadomestljivosti človeških izgub na teh področjih, saj je pri izločitvi soborca iz boja potrebna hitra in predvsem učinkovita zamenjava, kar predpostavlja univerzalizacijo znanja, usposobljenosti in izurjenosti.

[14] Specializacija pomeni nadgradnjo splošnega znanja ali strokovno izpopolnjevanje v posebni stroki.

5.2 Slovenija

Pred osemnajstimi leti je bila po dolgih desetletjih od ustanovitve slovenske vojske generala Maistra, partizanskih enot, Teritorialne obrambe leta 1968, kjer je bilo poveljstvo na slovenskem območju skoraj izključno v rokah slovenskih častnikov, po letu 1974 pa je zaradi bojazni pred demokratičnimi gibanji vse več vodilnih položajev v Teritorialni obrambi prešlo v roke srbskih častnikov JLA, kasneje, po osamosvojitveni vojni leta 1991, pa se je leta 1993 Teritorialna obramba Republike Slovenije preimenovala v Slovensko vojsko. Po vojni se je hitro preoblikovala iz rezervne v naborniško vojsko s profesionalnim jedrom, leta 2003 pa v poklicno vojsko. S Splošnim dolgoročnim programom razvoja in opremljanja Slovenske vojske si Slovenska vojska prizadeva doseči mesto verodostojne partnerice drugim vojskam Severnoatlantskega zavezništva in Evropske unije.

5.2.1 ORGANIZACIJA SLOVENSKE VOJSKE

Organizacija slovenske vojske je enotna, saj se ne deli na kopensko vojsko, mornarico in letalske sile kot večina drugih oboroženih sil. Slovenska vojska se je po letu 2003 z vstopom v organizacijo NATO profesionalizirala, njeni pripadniki pa se delijo na dva dela, in sicer:

- **Stalna sestava**, ki so poklicni pripadniki Slovenske vojske: vojaki, podčastniki, častniki, civilne osebe in vojaški uslužbenci, ki so vojaške osebe in opravljajo vojaško službo.
- **Rezervna sestava**, ki jo tvorijo državljani, ki sklenejo pogodbo o službi v rezervni sestavi, in vojaški obvezniki, ki so dolžni služiti v rezervni sestavi.

Omenil sem že, da je slovenska vojska po letu 2003, z vstopom v zvezo NATO, postala poklicna in tako prenehala z obveznišKim sistemom vojaškega služenja. Stalna sestava je marca 2008 merila 7050 pripadnikov, kar predstavlja 48,9 % skupnih sil v slovenski vojski, ostalih 51,1 % sil pa sta pogodbena in obvezna rezerva.

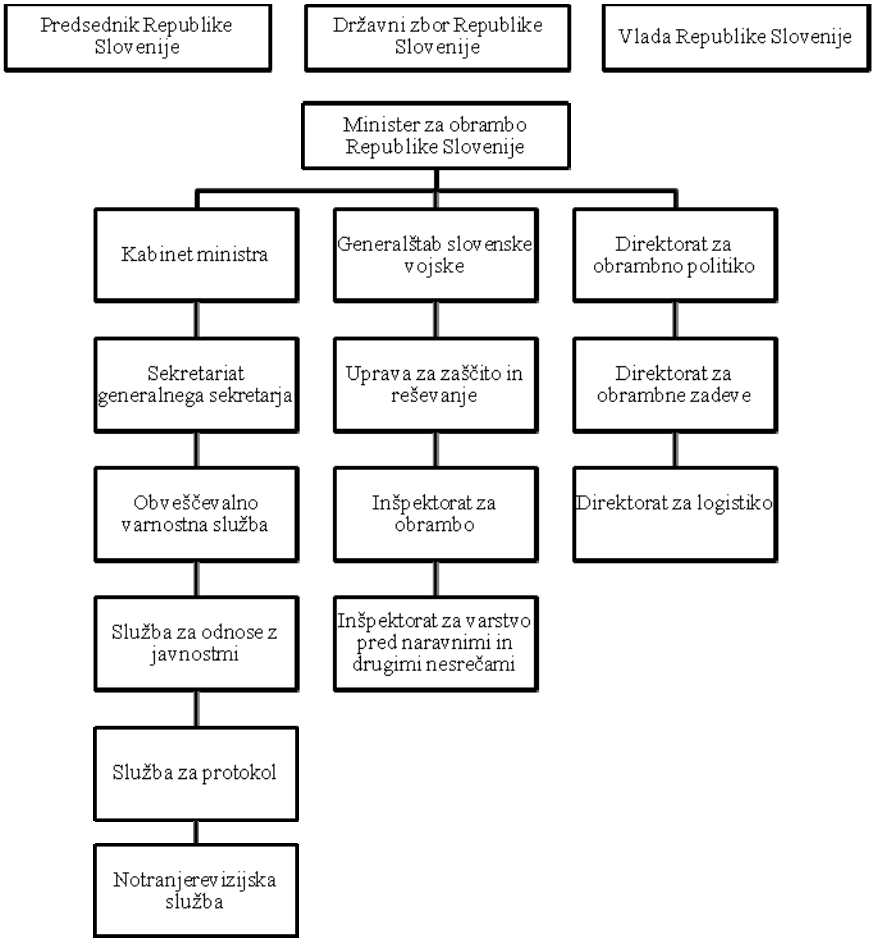
V delu se bomo v vseh državah opirali zgolj na stalno sestavo vojaških sil, saj le-te predstavljajo jedro vojske, iz katerih so sestavljene namenske enote.

Stalna sestava Slovenske vojske je sestavljena iz poklicnih pripadnikov vojske, ti pa so vojaki, podčastniki, častniki in vojaški uslužbenci (vojaške osebe) ter civilne osebe, ki delajo v vojski, vendar ne opravljajo vojaške službe. Indikator profesionaliziranosti slovenske vojske je razmerje med vojaki in podčastniško-častniškimi mesti, kjer na enega vojaka pride 1,16 častnika oziroma podčastnika, kar pomeni, da je nivo strokovnosti in usposobljenosti, ki sta potrebna za sofisticirano opremo in oborožitev, zagotovljen oziroma dosežen. Takšna sestava je značilna tudi za stalno sestavo drugih sodobnih vojska, kar bom v nadaljevanju tudi dokazal.

5.2.2 STRUKTURA OBRAMBNEGA SISTEMA IN SLOVENSKE VOJSKE

Za lažje razumevanje in lažjo predstavo bom, preden bom prišel do ciljnih enot, ustvarjenih kot odgovor na informacijske operacije, predstavil shematični pregled delovanja organov in enot v slovenski vojski.

Organigram 5.1: Organigram obrambnega sistema Republike Slovenije

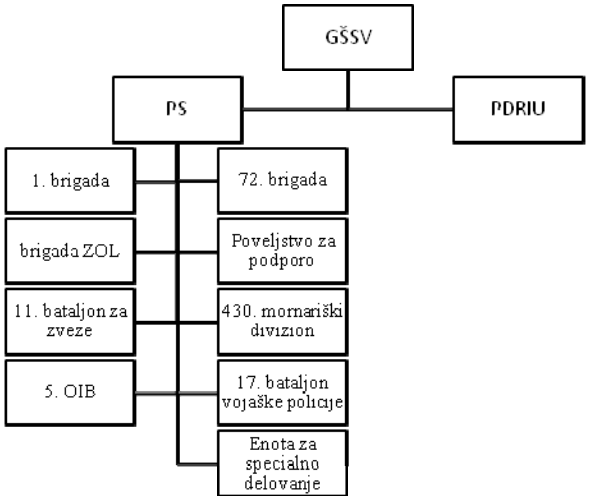


Vir: Kladnik (2006, 32).

Obrambni sistem Slovenske vojske je namenjen odvračanju napada na državo in branjenju neodvisnosti, nedotakljivosti in celovitosti države ter njenih nacionalnih interesov. Ta namen se uresničuje tudi z vključevanjem in dejavnostim države v mednarodnih varnostnih povezavah na podlagi mednarodnih pogodb, iz katerih izhajajo tudi glavna poslanstva in hkrati glavne naloge Slovenske vojske, med katere sodijo preprečevanje katere koli vrste agresije oziroma ustrezen odgovor nanjo, vojaško prispevanje k mednarodnemu miru, varnosti in stabilnosti, podpora sistemu zaščite in reševanja, pomoč drugim državnim organom in javnim institucijam pri zagotavljanju varnosti in blaginje državljanov.

Vrhovni poveljnik Slovenske vojske je predsednik Slovenije. Znotraj vlade Republike Slovenije deluje minister za obrambo, kateremu je poleg drugih, v zgornji tabeli naštetih, oddelkov, podrejen Generalštab Slovenske vojske, načelnik Generalštaba pa skrbi za njeno operativno delovanje. Znotraj Generalštaba velja naslednja shema:

Organigram 5.2: Struktura slovenske vojske



Vir: Internet 16.

Poveljniška struktura v Slovenski vojski je Generalštab Slovenske vojske, organ v sestavi obrambnega ministrstva in najvišji vojaški strokovni organ za poveljevanje vojski. Namenjen je opravljanju vojaško-strokovnih nalog, ki se nanašajo na razvijanje, načrtovanje, organiziranje, usposabljanje in delovanje Slovenske vojske. Operativno sta mu podrejeni Poveljstvo sil Slovenske vojske in Poveljstvo za doktrino, razvoj, izobraževanje in usposabljanje.

Poveljstvo sil je združeno poveljstvo za delovanje na operativni in taktični ravni in je bilo v sedanjo obliko formirano šestega januarja 2003. Poveljuje vsem silam na območju odgovornosti in združuje taktične enote, enote podpore in enote prostorske strukture. Je pristojno za načrtovanje, organiziranje in vodenje obrambnih priprav ter izvajanje vojaških operacij na celotnem ozemlju Republike Slovenije. Organizira in vodi sodelovanje pripadnikov in enot Slovenske vojske znotraj zavezništva ter v operacijah za podporo miru. Izvaja odločitve Generalštaba in neposredno izvaja operativne naloge ter nadzira izvajanje nalog njemu podrejenih enot. Poveljstvu sil so podrejeni:

- **1. brigada:**
  - 10. motorizirani bataljon
  - 20. motorizirani bataljon
  - 74. motorizirani bataljon
  - 670. poveljniško-logistični bataljon
- **72. brigada:**
  - 132. gorski bataljon
  - 45. oklepni bataljon
  - 460. artilerijski bataljon
  - 18. bataljon RKBO
  - 14. inženirski bataljon
- **Brigada zračne obrambe in letalstva:**
  - 15. helikopterski bataljon
  - 16. bataljon za nadzor zračnega prostora
  - 107. letalska baza
  - 9. bataljon zračne obrambe
  - Letalska šola
- **Poveljstvo za podporo**
  - 157. logistični bataljon
  - Vojaška zdravstvena enota
  - Vojaška teritorialna poveljstva (VTP)
    - 23. VTP Kranj
    - 24. VTP Postojna
    - 25. VTP Vrhnika
    - 32. VTP Novo mesto

        - 37. VTP Maribor
        - 38. VTP Celje
    - 11. bataljon za zveze
    - 430. mornariški divizion
    - **5. obveščevalno izvidniški bataljon (+ enote za elektronsko bojevanje)**
    - Enota za specialno delovanje
    - 17. bataljon vojaške policije (Internet 16)

Na drugi strani pa je Poveljstvu sil podrejeno tudi Poveljstvo za doktrino, razvoj, izobraževanje in usposabljanje (PDRIU), katerega naloga je izvajanje selekcije in usposabljanje vojakov ter usposabljanje in izobraževanje vojaškega osebja na vseh ravneh. PDRIU razvija doktrine in pravila, določa standarde bojne usposobljenosti ter sodeluje pri evalvacijah enot in poveljstev.

5.2.3 ENOTE ZA INFORMACIJSKO BOJEVANJE

Slovenija kot celota je lahko tudi cilj takšne agresije, kot je informacijsko bojevanje. Glede na pojav informacijskih operacij konec osemdesetih in v začetku devetdesetih let se je Slovenska vojska na to obliko bojevanja odzvala relativno počasi, po drugi strani pa niti ni bilo take nuje, da bi razvila svoje enote za informacijsko bojevanje, saj v teh letih, dokler ni ustanovila temu primernih enot, ni bila, razen leta 1991 in v času opravljanja mirovnih operacij, nikoli v takšnem položaju, kjer bi lahko le-te enote koristila.

5.2.3.1 11. Bataljon za zveze

Odgovor Slovenske vojske na pojav informacijskega vojskovanja in možnih sodelovanj v informacijskih operacijah smo dobili v sklopu **11. bataljona za zveze** s sedežem v vojašnici 26. oktobra v Vrhniki. Bataljon deluje s sedmih mirnodobnih lokacij, vzdržujemo pa sisteme zvez na več kot 30 lokacijah, razporejenih po celotnem državnem ozemlju, in sodelujejo na vseh večjih vajah, ki jih izvajajo enote Slovenske vojske.

Glavne naloge bataljona za zveze so:

- sodelovanje pri usposabljanju vojakov, podčastnikov in častnikov stalne sestave,
- zagotavljanje in vzdrževanje zvez in informacijskih sistemov,
- nadzor, upravljanje in vzdrževanje komunikacijskih in informacijskih sistemov,
- vzdrževanje materialno-tehničnih sredstev na prvi in drugi stopnji vzdrževanja.

Pripadniki sodelujejo pri preizkušanju nove telekomunikacijske opreme, pomagajo pri montažah nove opreme, ugotavljajo pogoje za vzpostavitev zvez na določenih območjih Republike Slovenije, zagotavljajo zveze na mednarodnih vajah in v mednarodnih operacijah ter za potrebe drugih enot.

Z zgledovanjem po strukturah drugih vojska se je 23. aprila 2001 11. bataljonu za zveze pridružila **enota za elektronsko bojevanje** ki je bila prva enota te vrste v Slovenski vojski. Takrat se je 11. bataljon za zveze preimenoval v **11. bataljon za zveze in elektronsko bojevanje Slovenske vojske.** Bil je nosilec elektronskega bojevanja in vzpostavljanja informacijskih sistemov, zato se je moral razvijati in opremljati z namenom sposobnosti:

- načrtovanja in organiziranja zvez v skladu z doktrino vojaške obrambe;
- zagotavljanja zvez s sistemi, ki so kompatibilni z zvezo NATO;
- zagotavljanja protielektronske zaščite zvez in šifrirne zaščite informacij v združenih taktičnih in višjih poveljstvih.

11. bataljon za zveze in elektronsko bojevanje Slovenske vojske je ostal nespremenjen do 1. julija 2004 s premestitvijo te enote iz tega bataljona v kasneje ustanovljeni 5. obveščevalno izvidniški bataljon, ime bataljona pa je ostalo enako kot pred pridružitvijo enote za elektronsko bojevanje (Internet 17).

5.2.3.2 5. Obveščevalno izvidniški bataljon

Znotraj sil Slovenske vojske za podporo poveljevanja in kontrole je poleg bataljona za zveze in bataljona za nadzor zračnega prostora tudi obveščevalno-izvidniški bataljon. Sile so namenjene zagotavljanju delovanja komunikacijskih in informacijskih sistemov Slovenske vojske, podpirajo vodstvene poveljniško-štabne procese, izvajajo nadzor in

kontrolo zračnega prostora ter obveščevalno oskrbujejo strateško in operativno-taktično raven poveljevanja.

30. septembra 2005 je bilo vzpostavljeno poveljstvo bataljona, ki se je začelo popolnjevati ter pripravljati na sprejem enote za specialno delovanje ter enote za elektronsko bojevanje. V letu 2007 so bile delno vzpostavljene začetne zmogljivosti bataljona. Nadaljuje se kadrovsko popolnjevanje poveljstva, enote za elektronsko bojevanje, poveljniško logistične čete, enota za specialno delovanje pa je umaknjena in ni več v sestavi 5. izvidniško obveščevalnega bataljona .

Bataljon ima nalogo obveščevalnega oskrbovanja vojaškega poveljstva na strateški in operativni ravni, hkrati pa to pomeni tudi sodelovanje s Sektorjem za obveščevalno-varnostne zadeve (J-2) ter Obveščevalno varnostno službo (OVS), katere namen delovanja je opisan v 32. členu zakona o obrambi. Službi lahko s podatki implementirata ugotavljanje in ocenjevanje vojaških in politično-varnostnih razmer ter vojaških zmogljivosti zunaj države, ki so posebnega pomena za varnost države ter odkrivata in preprečujeta dejavnosti obveščevalnih služb vojaških organizacij ter drugih organov in organizacij, ki ogrožajo obrambne interese države (Internet 18).

Namen bataljona je zbiranje, analiziranje in posredovanje vojaških obveščevalnih podatkov, znotraj njega pa je v stadiju formiranja in popolnjevanja enota za globinsko izvidovanje, enota za pridobivanje in analizo obveščevalnih podatkov, enota za analizo podatkov, enota za psihološke operacije, posodabljajo pa se tudi komunikacijsko-informacijski sistemi, sistem elektronskega izvidovanja, s čimer se zagotavljata večja mobilnost ter možnost bataljona za izvajanje podpore elektronskega bojevanja. Do konca leta 2008 bodo nabavljena sredstva za elektronske odvračilne ukrepe (predvsem elektronsko motenje) (Internet 19).

O končnem opremljanju in postavitvi 5. obveščevalno izvidniškega bataljona v dokončno operativno funkcijo najdemo podatke v Resoluciji o splošnem dolgoročnem programu razvoja in opremljanja Slovenske vojske (ReDPROSV) iz leta 2004, ki pravi sledeče:

»Elektronska in komunikacijska oprema predstavlja ogrodje sodobnih komunikacijskih in informacijskih sistemov, sistemov za upravljanje z ognjem, izvidniških sistemov, sistemov za elektronsko bojevanje in sistemov za izvajanje informacijskih operacij. Kot celota, sistemi za podporo vodenja in poveljevanja (C4) zagotavljajo izmenjavo podatkov znotraj celovitega sistema poveljevanja in kontrole. Slovenska vojska bo s stalnim posodabljanjem elektronske in komunikacijske opreme zagotovila učinkovitost in povezljivost z zavezništvom (Internet 20).«

Tako so se in se še bodo komunikacijski in informacijski sistemi izboljševali z vzpostavitvijo bojiščnega sistema poveljevanja in kontrole, ki združuje taktično telekomunikacijsko hrbtenico, taktični intranet in bojno radijsko omrežje, uporabo senzorjev za pridobivanje podatkov, vojaški sporočilni sistem, sistem poročanja in podpore odločanju, sistem za upravljanje in zaščito omrežja ter uporabo globalnega pozicijskega sistema (GPS). Gibljivo, zaščiteno in redundančno telekomunikacijsko hrbtenico bo možno z uporabo taktičnih satelitskih sistemov razširiti tudi v območja delovanja vojske izven ozemlja Republike Slovenije.

Posebna pozornost je namenjena povezljivosti in združljivosti sistemov z zavezniškimi. Vpeljan je sistem učinkovitega upravljanja in nadzora komunikacijskih in informacijskih sistemov, integrirane sistemske kontrole ter zagotovljene zmogljivosti za odzivanje ob informacijskih incidentih. Tako je zagotovljena zaščitena radijska povezava, uvedene pa bodo tudi taktične podatkovne povezave za zračna plovila in letalske baze ter nacionalni sistem za identifikacijo lastnih in nasprotnikovih sil.

S trenutno nabavo elektronske in komunikacijske opreme je deloma zagotovljeno izvajanje informacijskih operacij in operacij elektronskega bojevanja. Elektronski obrambi je zaradi povečanega vdora v računalniške sisteme posvečena posebna pozornost, vključno z obrambo stacionarnih komunikacijskih in informacijskih sistemov in senzorskim nadzorom. Z njenim neprekinjenim delovanjem bodo v prihodnosti vzpostavljeni pogoji za sodelovanje v zavezniškem sistemu kopenskega nadzora, omogočena pa bo tudi obveščevalna zagotovitev enot, poveljstev in štabov ter upravljanje z obveščevalnimi podatki.

V skladu z ReDPROSV bodo predvidoma do leta 2015 v sestavi bataljona:

- enota brezpilotnih letal,
- enota za elektronsko bojevanje,
- enota globinskih izvidnikov,
- enota za psihološke operacije,
- ter poveljniško-logistična enota.

Bataljon bo končne operativne zmogljivosti dosegel leta 2009, s tem bo uvrščen v kategorijo nepremestljivih sil v visoki stopnji pripravljenosti. Del enote bo uvrščen v kategorijo premestljivih sil v visoki stopnji pripravljenosti in se bo prilagajal namenskim silam, kadar bo v njihovi sestavi (Internet 20).

Trenutno v sklopu 5. izvidniško obveščevalnega bataljona deluje poleg poveljniško-logistične čete le ena enota v Slovenski vojski, namenjena izvajanju informacijskih operacij, to je enota za elektronsko bojevanje. Glede na ReDPROSV bo dol leta 2015 ta bataljon dočakal še vsaj dve sestrski enoti – enota brezpilotnih letal in enota za psihološke operacije, s čimer bodo ravni delovanja Slovenske vojske prešle v dejansko oziroma v uporabno obliko.

5.3 Združene države Amerike

Ameriške oborožene sile so, kar se tiče v vojaške tehnike, razvoja in organiziranosti, trenutno najbolj napredna in sofisticirana vojska na svetu. Že sam podatek, da ZDA v obrambne namene vloži slabih 579 milijard dolarjev (Internet 21), uvršča to državo na prvo mesto svetovnih vojaških porabnikov in zagotavlja ZDA monopolno vojaško moč v svetu, ki recipročno vpliva tudi na njene ostale prvine obstoja, kot je gospodarstvo.

V ameriških oboroženih silah je trenutno 1,449,428 oseb, v rezervni sestavi pa jih je trenutno 1,458,500 (Internet 22). Kadrovska sestava oboroženih sil ZDA je sledeča:

Tabela 5.1: Število pripadnikov oboroženih sil ZDA

ZVRST	ŠTEVILO PRIPADNIKOV	DELEŽ	DELEŽ ŽENSK	ŠTEVILO ČASTNIKOV
Kopenska vojska	519,998	36 %	14 %	84,698
Mornarica	373,830	26 %	14,9 %	51,265
Zračne sile	328,270	23 %	20,1 %	65,410
Marinci	186,209	13 %	6,2 %	19,535
Obalna straža	39,121	3 %	10,7 %	7,835
SKUPAJ	**1,449,428**	**100 %**	**14,9 %**	**228,743**

Vir: Internet 22.

Iz zgornje tabele je razvidno, da je največ osebja stacioniranega znotraj kopenske vojske. Povprečni delež žensk znotraj oboroženih sil je 14,9 %, kar je približno enak procent deležu žensk v Slovenski vojski. Največ žensk je v oboroženih silah ZDA prisotnih znotraj zračnih sil, to je 20,1 %. Gibanje števila častnikov je približno ista kot v Slovenski vojski, le da v zgornji tabeli prihaja do odstopanja v razmerju med številom častnikov in vojakov, ker niso všteti podčastniški čini.

Osebje oboroženih sil je stacionirano po vsem svetu, v glavnem pa se stacioniranost deli na dva dela, in sicer (Internet 23):

- **Stacioniranost znotraj ZDA:**
    - Kontinentalne ZDA: 879,523
    - Havaji: 37,021
    - Aljaska: 19,531
    - Guam 2,890
    - Na ladjevjih 92,337

- **Stacioniranost po svetu[15]:**
    - Irak: 196,600
    - Nemčija: 57,155
    - Japonska (United States Forces Japan): 33,164
    - Južna Koreja (United States Forces Korea): 26,076

[15] Oborožene sile so prisotne v najmanj 39 državah po svetu. Izpostavil sem le največje enote.

- Afganistan: 25,700
- Italija: 9,701
- Velika Britanija: 9,655

5.3.1 STRUKTURA OBOROŽENIH SIL

Oborožene sile ZDA so združene pod enotnim poveljstvom in se delijo na pet zvrsti:

- **Kopenska vojska ZDA (US Army)**
- **Marinci (US Marine Corps)**
- **Mornarica (US Navy)**
- **Zračne sile (US Air Force)**
- **Obalna straža (US Coast Guard)**

Vse zvrsti so pod civilnim nadzorom in vse, razen Obalne straže, spadajo v Obrambni oddelek (Department of defense – DoD).

Organigram 5.3: Struktura poveljevanja oboroženih sil ZDA

Vir: Internet 24.

Ustava Združenih držav določa, da je vrhovni poveljnik oboroženih sil (ang.Commander-in-Chief) predsednik ZDA. Za koordinacijo vojaških akcij oziroma dejanj mu ob strani stojita Svet za nacionalno varnost in Svetovalec za nacionalno varnost. Hierarhično sledi predsedniku Ministrstvo za obrambo ZDA, kjer je minister odgovoren za Obrambni oddelek (ang. Department of defense). Tako predsedniku ZDA kot obrambnemu ministru svetuje Združeno poveljstvo oboroženih sil ZDA (ang. Joint

Chiefs of Staff – JCS), vključno z načelnikom in namestnikom načelnika Združenega poveljstva oboroženih sil ZDA.

5.3.2 ENOTE ZA INFORMACIJSKO BOJEVANJE (INTERNET 25)

Znotraj oboroženih sil ZDA obstaja kompleksen sistem enot znotraj vsakega rodu vojske, namenjen informacijskemu bojevanju. Glede na naslov diplomske naloge ne morem trditi, da so se oborožene sile ZDA začele preoblikovati zaradi informacijskih operacij, saj so tako rekoč izumitelj oziroma pobudnik in narekovalec tempa dogajanja v le-teh. Znotraj oboroženih sil ZDA ne delujejo zgolj enote, namenjene informacijskemu bojevanju, ampak tudi druge združene organizacije in izobraževalne ustanove, namenjene tej obliki bojevanja. Za lažjo predstavo enot in drugih institucij za informacijsko bojevanje bom opisal sistem, namenjen za delovanje v operacijskih operacijah na najvišji ravni poveljevanja.

5.3.2.1 Združeno poveljstvo, namestnik direktorja za globalne operacije (Joint Staff, Deputy Director for Global Operations) – (ang. DDGO)

Namestnik direktorja za globalne operacije (DDGO) je odgovoren Direktorju za operacije (Director for Operations) in načelniku JCS. Zagotavlja strokovne nasvete v zvezi s koordinacijo združenih globalnih operacij, ki vključujejo informacijske operacije. Znotraj DDGO je pomočnik namestnika direktorja za informacijske operacije (DDGO/IO), odgovoren za informacijsko operacijske aktivnosti, kar vključuje razvoj združene informacijske politike in doktrine, zadolžen pa je tudi za koordinacijo z Ministrstvom za obrambo, bojnimi poveljstvi, službami, obrambnimi agencijami, drugimi poveljstvi, obveščevalno skupnostjo, z drugimi besedami, DDGO/IO je osrednja točka za vse specialne tehnične operacije.

5.3.2.1.1 Organizacija

Direktorat za globalne operacije je sestavljen iz štirih divizij, in sicer:

- **Divizija za informacijske operacije (Information Operations Division – IOD) –** je namenjena razvoju in koordinaciji elektronskega bojevanja (EW), računalniških mrežnih operacij (CNO), posebnih dejavnosti in strateških

komunikacij, prav tako pa deluje v podporo vsemi bojnim poveljstvom (Combatant Comands – COCOM), vključno s pisarno ministrstva za obrambo (OSD).

- **Divizija za psihološke operacije (Psychological Operations Division – POD)** – razvija, zagotavlja vodenje in koordinacijo z vsemi COCOM in drugimi službami glede planiranja ter uporabe psiholoških operacij (PSYOP).

- **Divizija za podporo programov (Program Support Division – PSD) –** zagotavlja operativne zmožnosti združenemu poveljstvu in vsem COCOM pri urjenju bojevnikov. PSD je osrednja izhodiščna točka združenega poveljstva za specialno-tehnično operativno programiranje in je odgovorna za združeno informacijsko-operacijsko koordiniranje doktrine in politike ter za združeni informacijsko-operacijski pregled nad potrebami kadrov.

- **Divizija za specialne ukrepe (Special Actions Division – SAD) –** je zadolžena za razvoj in širjenje skupne politike in deluje kot operacijska zveza med COCOM in JCS, skupaj z ministrstvom za obrambo ter izbira medagencijske partnerje za vojaško zavajanje (ang. military deception), operacijsko varnost in občutljive obrambne podporne dejavnosti.

5.3.2.2 Združeni spectrum center (Joint Spectrum Center - Jsc)

Združeni spectrum center zagotavlja učinkovito in zmogljivo uporabo elektromagnetnega spektra in nadzor nad elektromagnetnimi učinki v podporo nacionalni varnosti in vojaškim nalogam. JSC je zveza in neposredna koordinacijska podpora informacijskim operacijam in elektronskemu bojevanju. Zagotavlja neposredno podporo Združenim bojnim poveljstvom (Unified Combatant Commands), Združenim namenskim silam (Joint Task Forces), Združenemu poveljstvu za informacijske operacije in elektronsko bojevanje (IO/EW) ter Združenemu informacijsko-operacijskemu centru (Joint Information Operations Center – JIOC) pri vojaško-operacijskemu IO/EW planiranju.

V začetni shemi strukture poveljevanja oboroženih sil ZDA je omenjeno Združeno bojno poveljstvo, katerega struktura je nujnega pomena za nadaljnji razvoj v definiranju enot za informacijsko bojevanje v oboroženih silah ZDA.

5.3.2.3 Združeno bojno poveljstvo (Unified Combatant Command – Ucc)

UCC je združeno poveljstvo oboroženih sil ZDA in je lahko organizirano na geografski osnovi, poznani kot Območja odgovornosti, ali pa glede na funkcionalno osnovo. UCC je zaradi svoje specifičnosti bojnih delovanj vodena s strani bojnih poveljnikov (Combatant Commanders – CCDRs).

Glede na Območja odgovornosti se UCC deli na:

- Poveljstvo Združenih držav za Afriko - USAFRICOM (Poveljstvo (HQ): Kelley Barracks, Stuttgart, Nemčija)
- Poveljstvo Združenih držav Center - USCENTCOM (HQ: MacDill AFB, Florida)
- Poveljstvo Združenih držav za Evropo - USEUCOM (HQ: Patch Barracks, Stuttgart, Nemčija)
- Poveljstvo Združenih držav za Pacifik - USPACOM (HQ: Camp H. M. Smith, Honolulu, Havaji)
- Severno poveljstvo Združenih držav - USNORTHCOM (HQ: Peterson AFB, Colorado Springs, Kolorado)
- Južno poveljstvo Združenih držav - USSOUTHCOM (HQ: Miami, Florida)

Glede na funkcionalno odgovornost se deli na:

- Združeno poveljstvo sil Združenih držav - USJFCOM (HQ: Norfolk, Virginia)
- **Poveljstvo Združenih držav za posebne operacije - USSOCOM (HQ: MacDill AFB, Florida)**
- **Strateško poveljstvo Združenih držav - USSTRATCOM (HQ: Offutt AFB, in Omaha, Nebraska)**
- Poveljstvo Združenih držav za transport - USTRANSCOM (HQ: Scott AFB, in Illinois)

Za to delo je izrednega pomena razdelitev glede na funkcionalno odgovornost, kjer izstopata v informacijskih operacijah predvsem USSTRATCOM in USSOCOM.

5.3.2.4 Strateško poveljstvo sil ZDA (USSTRATCOM)

Kot naslednik Strateškega zračnega poveljstva (Strategic Air Command) je USSTRATCOM 1. junija 2002 postal eden od desetih združenih bojnih poveljstev. Pod nadzorom ima jedrski arzenal ZDA in je prav tako globalno usmerjeno poveljstvo, ki je zadolženo za izvajanje misij na področju vesoljskih operacij, informacijskih operacij, integriranih protiraketnih obramb, globalnega poveljevanja in nadziranja, obveščevalne dejavnosti, nadzora, izvidovanja, strateškega zastraševanja ter bojevanja z orožji za množično uničenje. Skupaj v tem poveljstvu sodeluje 960 oseb iz vseh rodov vojske.

Znotraj USSTRATCOM-a se nahajata dve pomembni entiteti, in sicer:

- **Združene sile za globalne mrežne operacije (Joint Task Force – Global Network Operations – JTF-GNO) –** je nastanjena v Arlingtonu v Virginiji. Naloga teh sil je vodenje operacij in obrambe globalnega informacijskega omrežja ministrstva za obrambo, z namenom zagotavljanja medmrežnih povezav in drugih, s tem povezanimi, zmožnostmi na strateških, operativnih in taktičnih ravneh v podporo celotnega spektra bojevalne, obveščevalne ter poslovne dejavnosti oddelka za obrambo (DoD).
    - **Global NetOps Center –** znotraj JTF-GNO deluje tudi Globalni mrežnooperacijski center, ki je zadolžen za dnevno delovanje in obrambo globalnega informacijskega omrežja (GIO). Zagotavlja popolno upravljanje, nadzor in tehnično podporo za GIO ter pregled nad koordinacijo procesov, ki zadevajo vsa bojna poveljstva, agencije, ministrstva za obrambo, predsednika ZDA.
- **Združeno poveljstvo za informacijsko operacijsko bojevanje (Joint Information Operations Warfare Command – JIOWC) –** je bilo ustanovljeno septembra 1999 in je odgovorno za integracijo informacijskih operacij v vojaške načrte in operacije vzdolž celotnega spektra konflikta. Znotraj JIOWC deluje 210 oseb, poleg teh pa še trije častniki zveze NATO in 160 pogodbenih oseb, ki so popolnoma integrirani v poveljstvo. JIWC operativnim poveljnikom zagotavlja neposredno tehnično-analitično podporo bojevanja na področju vodenja in poveljevanja (C2W). Podpira integracije operacijske varnosti, psiholoških operacij, vojaškega zavajanja, elektronskega bojevanja in

uničenja skozi izvrševanje različnih faz informacijskih operacij. Neposredna podpora se izvaja Združenemu poveljstvu, Združenim namenskim silam (Joint Task Forces), pisarni ministrstva za obrambo, drugim vladnim agencijam ter podrejenim bojnim poveljstvom, ki so:

- **Združeni center za elektronsko bojevanje** (Joint Electronic Warfare Center - JEWC)
- **Združeni center za podporo operacijski varnosti** (Joint Operations Security Support Center - JOSC)
- **Združeni center za podporo misijam** (Joint Mission Support Center - JMSC)
- **Združena celica za podporo strateškim komunikacijam** (Joint Strategic Communications Support Cell - JSSC)

5.3.2.5 Poveljstvo sil ZDA za specialne operacije (U.S. Special Operations Command - USSOCOM)

USSOCOM je tako kot USSTRATCOM eno od devetih Združenih bojnih poveljstev oboroženih sil ZDA in je podrejeno Oddelku za obrambo (Department of Defense). Naloga USSOCOM-a je organizacija, urjenje in opremljanje sil za specialne operacije, ki so nato dodeljene geografsko porazdeljenim bojnim poveljstvom, ameriškim ambasadorjem in njihovim državnim ekipam. USSOCOM upravlja in ima pregled nad vsemi enotami za specialne operacije, ki so sestavljene iz pripadnikov vseh rodov oboroženih sil ZDA. Naloga tega poveljstva je tudi zagotavljanje, da so enote njegove enote dobro izurjene in skupno pripravljene na bojno delovanje ob morebitnem vpoklicu. Za nas zanimive osnovne jedrne naloge enot za specialno delovanje so naslednje:

- psihološke operacije,
- operacije, ki temeljijo na javnih zadevah (Civil and Public Affairs) – operacije, ki vzpostavijo, vzdržujejo oziroma vplivajo na odnose med oboroženimi silami ZDA in tujimi civilnimi avtoritetami in populacijami z namenom sprejemanja delovanja oboroženih sil ZDA;
- informacijske operacije.

Sestavni deli USSOCOM-a so **štiri podpoveljstva** in eno podrejeno poveljstvo.

- **Poveljstvo kopenske vojske za specialne operacije (U.S. Army Special Operations Command – USASOC) –** stacionirano v Severni Karolini. Naloga tega poveljstva je organizacija, urjenje, opremljanje, izobraževanje, vzdrževanje bojne pripravljenosti in namestitev stalne ter rezervne sestave enot kopenske vojske za specialno delovanje. V to poveljstvo spadajo:
    - **4th PSYOP Polk (Group) – Leteči (Airborne) –** predstavlja edino aktivno enoto kopenske vojske, namenjeno psihološkim operacijam. S 1,300 možmi predstavlja 26 % vseh psihološko operacijskih enot kopenske vojske, do leta 2011 pa naj bi ta enota štela 2,300 mož. Znotraj tega polka deluje šest bataljonov, in sicer 1., 3., 5., 6., 8. in 9. PSYOP bataljon.
    - **95th Civil Affairs Brigade (brigada za civilne zadeve) –** je bila ustanovljena 16. marca 2006 in je edina enota za civilne zadeve, ki deluje v sklopu Oddelka za obrambo. Kljub temu da še ni polno operativna, bodo do konca leta 2008 v njej operativni 95., 97., 98. in nazadnje tudi 91. bataljon za civilne zadeve.
    - **Poveljstvo kopenske vojske za specialne operacije**
    - **Center in šola J. F. Kennedy-a za specialno vojskovanje**
- **Poveljstvo pomorskih sil za specialno bojevanje (Naval Special Warfare Command – NAVSPECWARCOM),** nastanjeno v Coronado, Kalifornija. Naloga tega poveljstva je organizacija, urjenje, opremljanje, izobraževanje, vzdrževanje bojne pripravljenosti in namestitev dodeljenih sil v podporo združenim ter pomorskim operacijam širom po svetu.
- **Poveljstvo letalskih sil za specialne operacije (Air Force Special Operations Command – AFSOC) –** locirano v Hulburt Field-u, Florida. Prispevek AFSOC-a k informacijskim operacijam je viden predvsem v obliki **193th Special Operations Wing (eskadrilje za specialne operacije)** v sklopu zračnih sil nacionalne garde, katere naloga je podpora psihološkim operacijam z letali EC-130E Commando Solo, ki predvajajo temu namenjene programe na standardnih AM/FM radio, televizijskih, kratkovalovnih in raznih vojaških frekvencah.
- **Poveljstvo enot marincev za specialne operacije (Marine Corps Forces Special Operations Command – MARSOC) -** je bilo vzpostavljeno februarja 2006, primarna naloga poveljstva je organizacija, urjenje, opremljanje,

izobraževanje, vzdrževanje bojne pripravljenosti specialnih sil marincev. Podrejeni elementi MARSOC-a zagotavljajo urjenje sil tujih vojska, ki vključuje urjenje na področju specialni operacij, izvidništva in podobno.

- **Združeno poveljstvo za specialne operacije (Joint Special Operations Command – JSOC) –** je podrejeno poveljstvo USSOCOM-u in zagotavlja združeni delovni štab za študijo potreb specialnih operacij, zagotavlja medoperatibilnost in standardiziranost opreme ter razvija združene načrte in taktike za specialne operacije.

5.3.3 SILE ZNOTRAJ ZVRSTI VOJSKE (Internet 25)

5.3.3.1 Kopenska vojska (U.S. Army)

5.3.3.1.1 1st Information Operations Command (Poveljstvo za informacijske operacije – 1st IO Cmd)

1st IO Cmd zagotavlja podporo informacijskim operacijam kopenski vojski ZDA in drugim silam z razvijanjem podpornih enot informacijskih operacij, informacijsko operacijskim planiranjem in analizo ter sinhronizacijo in upravljanjem računalniško-mrežnih operacij (Computer Network Operations) z ostalimi CNO. Namen tega je operativna integracija informacijskih operacij, ojačanje osrednjih informacijsko-operacijskih zmožnosti ter zaščita kiberprostora z namenom zagotavljanja in omogočanja informacijskih operacij v informacijskem okolju.

1st IO CmD je glavni nadrejeni organ Obveščevalnemu in varnostnemu poveljstvu kopenske vojske (U.S. Army Intelligence and Security Command – INSCOM), vendar je kljub temu podrejeno Operativnemu poveljstvu in specialnim nalogam kopenske vojske (Operational Control and tasking of the Army G-3), z drugimi besedami povedano, Direktoratu za operacije, pripravljenost enot in mobilizacijo.

5.3.3.1.2 Poveljstvo kopenskih rezervnih sil za informacijske operacije (Army Reserve Information Oprations Command – ARIOC)

Poveljstvo kopenskih rezervnih sil za informacijske operacije zagotavlja celoten spekter načrtovalnih zmožnosti informacijskih operacij z namenom podpore misijam Združenih sil (Joint Force) in kopenske vojske. V sklopu rezervnih sil tako delujejo:

- **350., 351., 352. in 353. poveljstvo za civilne zadeve** (Civil Affair Commands)
- **2nd PSYOP Group (polk)**
    - 11. PSYOP bataljon: 303., 305. in 312. enota za psihološke operacije
    - 13. PSYOP bataljon: 339. in 319. enota za psihološke operacije
    - 15. PSYOP bataljon: 321., 346. in 350. enota za psihološke operacije
    - 16. PSYOP bataljon: 310., 345. in 362. enota za psihološke operacije
- **7th PSYOP Group (polk)**
    - 10. PSYOP bataljon: 307., 308. in 318. enota za psihološke operacije
    - 12. PSYOP bataljon. 315., 320. in 361. enota za psihološke operacije
    - 14. PSYOP bataljon: 301., 304., in 324. enota za psihološke operacije
    - 17. PSYOP bataljon: 306., alpha in bravo enota za psihološke operacije

5.3.3.1.3 Ustanova kopenske vojske za predlogo informacijskih operacij (U.S. Army Information Operations Proponent – USAIOP)

USAIOP je zadolžen za institucionaliziranje razvoja informacijskih operacij v sklopu doktrine kopenske vojske, operacij, urjenj, osebja, logistike in drugih ustanov z namenom vzpostavljanja informacijskih operacij kot kompetenčnega jedra v sklopu kopenske vojske.

5.3.3.2 Pomorske sile (Internet 25)

5.3.3.2.1 Pomorsko poveljstvo za mrežno bojevanje (Naval Network Warfare Command – NAVNETWARCOM)

NAVNETWARCOM zagotavlja centralno operativno poveljstvo pomorskih sil za informacijske operacije v podporo pomorskim silam. Poveljstvo je odgovorno za identificiranje, koordiniranje in predvidevanje informacijsko operativnih potreb pomorskih sil in razvoj medmrežne strukture. Kot funkcionalna enota za informacijske operacije, ki je podrejena USSTRATCOM, je NAVNETWARCOM odgovorna za strateško informacijsko operativno planiranje in za operativno podporo.

5.3.3.2.2 Pomorsko poveljstvo za informacijske operacije Norfolk (Navy Information Operations Command Norfolk)

To poveljstvo je zadolženo za zagotavljanje operativno usmerjenega urjenja enot: načrtovanje podpore in porast le-te iz taktične na strateško raven; razvoj doktrine informacijskih operacij, taktike, tehnik in procedur; zagotavljanje in upravljanje z informacijskooperacijskimi podatki za pomorske operacije. NIOC Norfolk deluje pod operativnim in administrativnim vodstvom NAVNETWARCOM in ima dve podrejeni poveljstvi: NIOC San Diego in NIOC Whidbey Island.

5.3.3.2.3 Pomorsko poveljstvo za kibernetske obrambne operacije (Navy Cyber Defense Operations Command - NCDOC)

NCDOC koordinira, nadzira in ima pregled na obrambo s pomorskimi računalniško-mrežnimi sistemi, vključno s telekomunikacijami in je zadolženo za izvrševanje misij na področju računalniško-mrežne obrambe. NCDOC je podrejeno NAVNETWARCOM in Združenim silam za posebne operacije – Globalne mrežne operacije (JTF-GNO).

5.3.3.2.4 Pomorsko poveljstvo za informacijske operacije Suitland (Navy Information Operations Command Suitland – NIOC)

NIOC Suitland služi kot Inovativni center za informacijske operacije pomorskih sil ZDA; ima funkcijo glavnega tehničnega dejavnika za raziskovanje in razvoj prototipnih

informacijsko-operacijskih zmožnosti. NIOC Suitland podpira razvoj zmožnosti za vse vrste informacijsko-operacijskih napadov, zaščite in zlorabe. Je tudi v sodelujočem odnosu z Vesoljskim in pomorskim poveljstvom za bojne sisteme (Space and Naval Warfare Systems Command) in Centrom sistemov (System Center San Diego) za zagotovitev učinkovite in zmogljive tehnične strokovnosti znotraj računalniških, komunikacijskih, obveščevalnih, nadzornih, izvidniških in informacijskih operacij ter operacij na področju vodenja in poveljevanja.

5.3.3.3 Zračne sile (Internet 25)

V oboroženih silah ZDA je letalstvo zagotovo tista zvrst oboroženih sil, ki najbolj entuziastično podpira informacijsko bojevanje. Znotraj zračnih sil obstajajo eskadrilje, namenjene informacijskemu vojskovanju, že od osemdesetih let prejšnjega stoletja, pa tudi uradna naloga zračnih sil Združenih držav je zagotavljanje suverenih zmožnosti za obrambo Združenih držav Amerike in njihovih globalnih interesov. To vključuje letenje in vojskovanje v zraku, vesolju in kiberprostoru, kar dokončno opredeljuje vlogo zračnih sil.

Doktrina zračnih sil ZDA poleg že uveljavljenim in tradicionalnim nalogam v zraku in vesolju, kot so counter-air, counter-space, counter-land, counter-sea in strateški napad, dodaja še novo funkcijo, in sicer proti-informacije (counter-information). Te poskušajo vzpostaviti informacijsko premoč skozi nadzor informacijskega okolja, osredotočajo pa se na preprečevanje nasprotnikove sposobnosti za doseganje informacijske prednosti.

Dejstvo je, da smo pri drugih zvrsteh oboroženih sil našli bore malo enot, ki bi zadovoljevale potrebo oboroženih sil ZDA po tako obsežnih informacijskih operacijah, ki jih v sedanjosti tako množično izvaja. V nadaljevanju bomo videli, da je večina teh sil razporejenih prav znotraj zračnih sil ZDA.

5.3.3.3.1 Agencija zračnih sil za obveščevalno, nadzorno in izvidniško dejavnost (Air Force Intelligence, Surveillance and Reconnaissance Agency – Air Force ISR Agency)

Air Force ISR Agency, s poveljstvom v Texasu, je bilo aktivirano 8. junija 2007. Prej bolj znano kot Air Intelligence Agency, je kot kopensko operativna agencija sedaj

podrejena Namestniku generalštaba zračnih sil za obveščevalno, nadzorno in izvidniško dejavnost (Air Force Deputy Chief of Staff for Intelligence, Surveillance and Reconnaissance – A2).

Naloga agencije je organiziranje, urjenje, opremljanje in predstavljanje dodeljenih sil z namenom vodenja in izvajanja obveščevalne, nadzorne ter izvidniške dejavnosti za bojne poveljnike in cel narod. Naloga agencije je tudi izvrševanje in pregled nad vodstvom ter politiko Poveljstva zračnih sil (HQ USAF) z namenom širjenja Air Force ISR zmožnosti za spopadanje s trenutnimi in bodočimi izzivi. Osebje Air Force ISR trenutno šteje 12 000 ljudi, ki so nastanjeni na 72 lokacijah po vsem svetu.

5.3.3.3.2 Organizacija agencije zračnih sil za obveščevalno, nadzorno in izvidniško dejavnost

- **70th Intelligence Wing (IW)**[16] – je bilo aktivirano 16. avgusta 2000 in integrira zmožnosti zračnih sil v globalne kriptološke operacije, pri čemer neposredno podpira organe odločanja na nacionalni ravni, bojne poveljnike in taktične bojne skupine. 70th IW deluje skupaj z Nacionalno varnostno agencijo (NSA), s čimer drži vzvode vseh omrežnih zmogljivosti. Vpliv delovanja na bojišče je takojšen, z visoko intenzivnostjo in odločilen. 70th IW vsebuje sedem drugih operativno obveščevalnih skupin na ravni polka v sklopu kontinentalnega dela ZDA, pacifiškega in evropskega poveljstva. Te skupine so:
    - 70th Mission Support Group
    - 70th Operations Group
    - 373rd Intelligence Group
    - 543rd Intelligence Group
    - **544th Information Operations Group**
    - 692nd Intelligence Group
    - 693rd Intelligence Group
- **Nacionalni center za zračno in vesoljsko obveščevalno dejavnost** (National Air and Space Intelligence Center – NASIC) - ki ima poveljstvo v Zvezni državi Ohio, je primarni proizvajalec zračne in vesoljske obveščevalne dejavnosti v

[16] Znotraj zračnih sil ZDA pomeni termin wing skupino šestih eskadrilj.

sklopu Oddelka za obrambo (DoD). NASIC razvija podatke z analiziranjem vseh podatkov, ki so na voljo glede tujih zračno-vesoljskih sil in oborožitvenih sistemov, z namenom determiniranja njihovih zmožnosti, značilnosti, ranljivosti in namenov. Ugotovitve tega centra so pogosto pomemben dejavnik pri oblikovanju politike nacionalne in obrambne varnosti. Od leta 1961, odkar je bil ta ustanovljen, je naloga tega centra tudi soočenje z izzivi svetovnih tehnoloških razvojev.

- **Center zračnih sil za informacijske operacije (Air Force Information Operations Center – AFIOC)** - AF ISR Agencija zagotavlja vodenje in podporo misijam specifičnih obveščevalnih operacij znotraj AFIOC-a. Ta zaposluje približno 1000 vojaških in civilnih oseb, izurjenih v inženirskih, raziskovalnih, obveščevalnih, radarsko-tehnoloških ter C2W operacijah.
- **67th Network Warfare Wing** (omrežno bojevanje) – AF ISR Agencija zagotavlja vodenje in podporo misijam specifičnih obveščevalnih operacij znotraj 67th Network Warfare Wing-a, ki ima globalno zadolžitev za organizacijo, urjenje in opremljanje cyberspace sil za izvrševanje mrežne obrambe, napada ter izkoriščanje. V sklopu te enote delujejo naslednje enote na ravni polka:
    - 67th Network Warfare Group (omrežno bojevanje)
    - 26th Network Operations Group (omrežne operacije)
    - 690th Network Support Group (omrežna podpora)
- **55th Wing** – AF ISR Agencija zagotavlja vodenje in podporo misijam specifičnih obveščevalnih operacij znotraj 55th Wing-a, ki ima nalogo izvajanja izvidniške dejavnosti širom po svetu, vodenja, poveljevanja in komunikacijske dejavnosti, izvajanje podpore predsedniku ZDA, Ministrstvu za obrambo, Združenemu generalštabu oboroženih sil ZDA, nacionalnim obveščevalnim agencijam ter poveljnikom velikih poveljstev Zračnih sil ZDA (Commanders of major Air Force Commands). Trenutna sestava te enote je sledeča:
    - 1st Airborne Command & Control Squadron (eskadrilja za vodenje in poveljevanje)
    - 25th Information Operations Squadron (eskadrilja za informacijske operacije)
    - 38th Reconnaissance Squadron (Izvidniška eskadrilja)

- 45th Reconnaissance Squadron (Izvidniška eskadrilja)
- 55th Operations Support Squadron (eskadrilja za operativno podporo)
- 82nd Reconnaissance Squadron (Izvidniška eskadrilja)
- 95th Reconnaissance Squadron (Izvidniška eskadrilja)
- 97th Intelligence Squadron (obveščevalna eskadrilja)
- 338th Combat Training Squadron (eskadrilja za bojno urjenje)
- 343rd Reconnaissance Squadron (Izvidniška eskadrilja)
- 390th Intelligence Squadron (obveščevalna eskadrilja)
- 488th Intelligence Squadron (obveščevalna eskadrilja)

- **480th Intelligence Wing** (obveščevalna dejavnost) - AF ISR Agencija zagotavlja vodenje in podporo misijam specifičnih obveščevalnih operacij znotraj 480th Intelligence Wing, ki pravočasno razvija in zagotavlja primerne obveščevalne podatke in zmožnosti, ki zadovoljujejo potrebe zračnih sil. S tem dostavlja pomembne informacije do ključnega naročnika oziroma do bojnih enot ZDA. 480th IW je bilo aktivirano 1. decembra 2003 in izvaja obveščevalne, kriptološke ter znakovno-obveščevalne ukrepe, katerih cilj so splošne tuje obveščevalne enote, obveščevalno-podatkovni sistemi mrežnih operacij ter raztros podatkov. Trenutna sestava te enote je sledeča:
    - 27th Intelligence Squadron (obveščevalna eskadrilja)
    - 497th Intelligence Group (obveščevalna skupina)
        - 10th Intelligence Squadron (obveščevalna eskadrilja)
        - 30th Intelligence Squadron (obveščevalna eskadrilja)
    - 548th Intelligence Group (obveščevalna skupina)
        - 9th Intelligence Squadron (obveščevalna eskadrilja)
        - 13th Intelligence Squadron (obveščevalna eskadrilja)
        - 48th Intelligence Squadron (obveščevalna eskadrilja)
    - 693rd Intelligence Group (obveščevalna skupina)
        - 24th Intelligence Squadron (obveščevalna eskadrilja)

- 450th Intelligence Squadron (obveščevalna eskadrilja)
- 485th Intelligence Squadron (obveščevalna eskadrilja)

- 117th Intelligence Squadron (obveščevalna eskadrilja)
- 123rd Intelligence Squadron (obveščevalna eskadrilja)

5.3.3.3.3 Center zračnih sil za informacijske operacije (Air Force Information Operations Center – AFIOC)

AFIOC je locirana v Lacklandski letalski bazi v Zvezni državi Teksas. V isti bazi delujeta tudi 67th Network Warfare Wing in AFISRA (Air Force Intelligence, Surveillance, Reconnaisance Agency). AFIOC je namenjen dostavljanju preizkušenih zmožnosti za informacijske operacije, ki so integrirane na vesoljskem, zračnem področju in področju cyberspace-a. 1. maja 2007 je bil AFIOC dodeljen v 8. zračne sile (8th Air Force) kot del Poveljstva zračnih sil za kibernetsko delovanje (Air Force Provisional Cyber Command). Trenutno šteje AFIOC približno 800 vojaških in civilnih oseb, izurjenih v inženirskih, raziskovalnih, obveščevalnih, radarsko-tehnoloških in C2W operacijah. Člani AFIOC-a zagotavljajo bojnim poveljnikom glavnih poveljstev zračnih sil zmožnosti za delovanje v informacijskih operacijah.

Med drugimi so naloge AFIOC-a sledeče:

- vodenje tehnoloških raziskav in inovacij;
- podpora razvoju zmožnosti zračnih sil za delovanje v informacijah kibernetske narave;
- vodenje ocene ranljivosti in dovoljene ravni tveganja;
- povečanje bojnih zmogljivosti na področju elektronskega bojevanja;
- vodenje urjenj, podpornih vaj in razvijanje taktike na področju informacijskih operacij;
- integracijami s ključnimi partnerji, kot so na primer NSA, Raziskovalni center zračnih sil (Air Force Research Laboratory – AFRL), koalicijske sile in osebje šole za oborožitev zračnih sil (USAF Weapons School);
- vodenje testiranj in vrednotenje mrežnih bojnih operacij;
- zagotavljanje operativne podpore.

5.3.3.3.4 Eight Air Force (8th Air Force)

Zračne sile ZDA so sestavljene iz glavnih poveljstev (Major Command – MAJCOM), razdeljena so na oštevilčene zračne sile (Numbered Air Forces), ki jih je 24. Znotraj teh se nahaja tudi 8th Air Force.

8th Air Force zagotavlja integrirane globalne zračne napade, mrežno bojevanje, vodenje bitk, nadzorovanje, izvidovanje, obveščevalno delovanje in taktični zračni nadzor. »Vsemogočna osmica« ima prav tako nalogo vodenja računalniško-mrežnih operacij kot del Združenih sil za posebne naloge – Globalne mrežne operacije (JTF-GNO), hkrati pa vzdržuje Zračno-vesoljni operativni center v podporo USSTRATCOM-ovim misijam na globalni ravni in uri osebje za uporabo širom po svetu.

Enote in centri, ki delujejo znotraj 8th Air Force, so sledeči:

- **2nd Bomb Wing** (bombne eskadrilje, opremljene z bombniki B-52H)
- **917th Wing** (bombne eskadrilje, opremljene z bombniki B-52H, A-10)
- **5th Bomb Wing** – (bombne eskadrilje, opremljene z bombniki B-52H)
- **9th Reconnaissance Wing** – (izvidniške eskadrilje, opremljene z letali U-2S)
- **55th Wing**
- **67th Network Warfare Wing** (omrežno bojevanje)
- **116th Air Control Wing** - (eskadrilje za zračni nadzor, opremljene z letali E-8C)
- **480th Intelligence Wing** – (eskadrilje za obveščevalno dejavnost)
- **509th Bomb Wing** - (bombne eskadrilje, opremljene z bombniki B-2)
- **552nd Air Control Wing** - (eskadrilje za zračni nadzor, opremljene z letali E-3B/C)
- **Center Zračnih sil za informacijske operacije (AFIOC)**
- **Poveljstvo zračnih sil za kibernetsko delovanje (Air Force Cyber Command)**

5.3.3.3.5 Air Force Cyber Command (Provisional) (Poveljstvo zračnih sil za kibernetsko delovanje (začasno) - Afcyber (P))

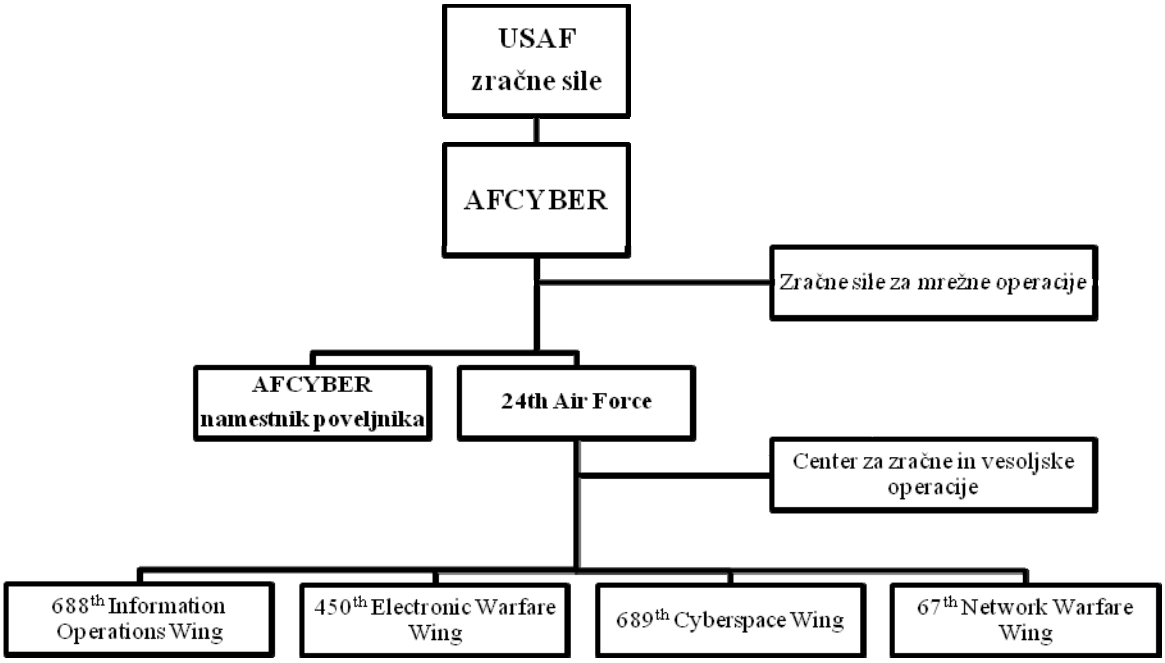
AFCYBER (P) je najnovejše glavno poveljstvo, podrejeno zračnim silam ZDA, katerega razvoj je bil napovedan 2. novembra 2006. V prvotnem načrtu je bilo, da bo AFCYBER (P) pričel delovati poleti 2007, vendar je uradni datum pričetka operativnega delovanja pogojen z razglasitvijo začetne operativne zmožnosti delovanja, ki bo prešlo v dejanje 1. oktobra 2008. AFCYBER (P) ima status začasnega poveljstva, ker je to začasno organizirana enota z namenom izvajanja specifičnih nalog. Sam pomen začasnosti najdemo tudi v dejstvu, da AFCYBER (P) nima dodeljenega stalnega osebja, ker bo osebje sestavljeno iz svojih stacionarnih enot. Naloga poveljstva je zagotovitev, da lahko sile, ki so del operacij po celem svetu, uporabljajo kiberprostor z namenom integracije operacij.

AFCYBER (P) bo imelo vlogo glavno vlogo poveljstva za:

- Mrežno obrambo (Network defense)
- Bojno podporo enotam
- Zadeve, povezane z računalniško varnostjo (informacijska zagotovitev)
- Mrežne napade
- Elektronsko bojevanje in usmerjeno energijo
- Informacijske operacije
- Celotne mrežne operacije
- Globalne integracije vodenja in poveljevanja
- Ekspedicijska komunikacijska omrežja (satelitske komunikacije)
- Podatkovne vezne člene
- Operacije elektromagnetnega spektra
- Integracije podatkov in skupne komunikacijske ter informacijske funkcije
- Inženiring in namestitev komunikacijske podpore
- Elektronsko vzdrževanje in vrednotenje (satelitske komunikacije, vremenski radarji, kriptologija, nadzor zračnega prometa in pristajalni sistemi ter omrežne infrastrukture)

AFCYBER (P) bo črpal osebje iz 67th Network Warfare Wing in iz drugih delov poveljstva Eight Air Force.

Organigram 5.4: Struktura AFCYBER (P)



Vir: Internet 26.

Znotraj AFCYBER (P) je poleg novoustanovljene entitete oštevilčenih sil – 24th Air Force tudi Center za zračne in vesoljske operacije, ki je element vodenja in poveljevanja ter samostojno poveljstvo zračnih sil za omrežne operacije. Znotraj 24th Air Force se nahajajo enote, namenjene elektronskim napadom, elektronski zaščiti in informacijskim operacijam. Te enote so naslednje:

- **688th Information Operations Wing** (Formalno Center za informacijske operacije)
    - **38th Information Operations Group** (Skupina za informacijske operacije)
        - 273rd Information Operations Squadron (eskadrilja za informacijske operacije)
    - **39th Information Operations Group** (Skupina za informacijske operacije)
        - 229th Information Operation Squadron (eskadrilja za informacijske operacije)

- **346th Test Squadron** (eskadrilja za testiranje)
- **453rd Electronic Warfare Squadron** (eskadrilja za elektronsko bojevanje)
- **92nd Information Operations Squadron** (eskadrilja za informacijske operacije)
    - 262nd Information Warfare Aggressor Squadron (IW agresorska eskadrilja)
- **Direktorat za informacijske operacije**
- **Direktorat za podporo misijam**

- **67th Network Warfare Wing (Omrežni napadi, obramba, varovanje)**
    - **26th Network Operations Group** (Skupina za omrežne operacije)
        - 26th Operations Support Squadron (eskadrilja za podporo operacijam)
        - 561st Network Operations Squadron (eskadrilja za omrežne operacije)
        - 83rd Network Operations Squadron (eskadrilja za omrežne operacije)
        - 299th Network Operations Support Squadron (eskadrilja za podporo omrežnim operacijam)
        - 690th Network Security Squadron (eskadrilja za omrežno varnost)
        - 310th Communications Flight (eskadrilja za zračne komunikacije)
        - 622nd Communications Flight (eskadrilja za zračne komunikacije)
        - 917th Communications Flight (eskadrilja za zračne komunikacije)
        - 33rd Network Warfare Squadron (eskadrilja za omrežno bojevanje)
        - 102nd Information Warfare Squadron (eskadrilja za informacijsko bojevanje)
    - **67th Network Group** (Skupina za omrežne operacije)
        - 67th Operations Support Squadron (eskadrilja za podporo operacijam)
        - 352nd Network Warfare Squadron (eskadrilja za omrežno bojevanje)
        - 68th Network Warfare Squadron (eskadrilja za omrežno bojevanje)

        - 426th Network Warfare Squadron (eskadrilja za omrežno bojevanje)
        - 610th Information Operations Flight (eskadrilja za informacijsko bojevanje)
        - 710th Information Operations Flight (eskadrilja za informacijsko bojevanje)
        - 91st Network Warfare Squadron (eskadrilja za omrežno bojevanje)
        - 315th Network Warfare Squadron (eskadrilja za omrežno bojevanje)
        - 6th Intelligence Squadron (eskadrilja za obveščevalno dejavnost)
        - 166th Network Warfare Squadron (eskadrilja za omrežno bojevanje)
        - 175th Network Warfare Squadron (eskadrilja za omrežno bojevanje)
- **689th Cyberspace Wing** (namestitev in razvoj poveljstva, poveljniško informacijske funkcije)
        - 689th Operations Support Squadron (eskadrilja za podporo operacijam)
    - **38th Engineering and Installation Group** (skupina za inženiring in namestitve
        - 85th Engineering and Installation Squadron (eskadrilja za inženiring in namestitve)
    - **5th Combat Communications Group** (skupina za bojne komunikacije)
    - **3rd Combat Communications Group** (skupina za bojne komunikacije)
        - 84th Radar Evaluation Squadron (eskadrilja za oceno radarjev)
    - **254th Combat Communications Group** (skupina za bojne komunikacije)
    - **252nd Combat Communications Group** (skupina za bojne komunikacije)
    - **251st Combat Communications Group** (skupina za bojne komunikacije)
    - **162nd Combat Communications Group** (skupina za bojne komunikacije)

- **201st Combat Communications Group** (skupina za bojne komunikacije)
- **226th Communications Group** (skupina za komunikacije)
- **281st Combat Communications Group** (skupina za bojne komunikacije)
- **253rd Combat Communications Group** (skupina za bojne komunikacije)
  - 35th Combat Communications Squadron (eskadrilja za bojne komunikacije)
  - 55th Combat Communications Squadron (eskadrilja za bojne komunikacije)
  - 224th Joint Communications Support Squadron (združena eskadrilja za podporo komunikacijam)
  - 290th Joint Communications Support Squadron (združena eskadrilja za podporo komunikacijam)
- **Vrhovne poveljniške funkcije** z Agencijo zračnih sil za komunikacije (Air Force Communications Agency) in Centrom za globalno kiberprostorno integracijo (Global Cyberspace Integration Center)

- **450th Electronic Warfare Wing** (elektronski napad in zaščita)
  - **55th Electronic Combat Group** (bojna skupina za elektronsko bojevanje)
    - 755th Operations Support Squadron (eskadrilja za podporo operacijam)
    - 754th Aircraft Maintenance Squadron (ekadrilja za vzdrževanje letal)
    - 41st Electronic Combat Squadron (bojna ekadrilja za elektronsko bojevanje)
    - 43rd Electronic Combat Squadron (eskadrilja za podporo operacijam)
    - 42nd Electronic Combat Squadron (eskadrilja za podporo operacijam)
    - 388th Electronic Combat Squadron (eskadrilja za podporo operacijam)
    - 18th Intelligence Squadron (ekadrilja za obveščevalno dejavnost)

- **53rd Electronic Warfare Group** (skupina za elektronsko bojevanje)
  - 16th Electronic Warfare Squadron (ekadrilja za elektronsko bojevanje)
  - 453th Electronic Warfare Squadron (ekadrilja za elektronsko bojevanje)
  - 36th Electronic Warfare Squadron (ekadrilja za elektronsko bojevanje)
  - 68th Electronic Warfare Squadron (ekadrilja za elektronsko bojevanje)
- **450th Space Group** (Vesoljska skupina)
  - 76th Space Control Squadron (eskadrilja za nadzor vesolja)
  - 4th Space Control Squadron (eskadrilja za nadzor vesolja)
  - 16th Space Control Squadron (eskadrilja za nadzor vesolja)

Poleg zgoraj naštetih enot bodo v AFCYBER (P) tudi enote iz drugih glavnih poveljstev, in sicer Poveljstva zračnih sil za opremo (AF Materiel Command), Zračnega poveljstva za prevoz (Air Mobility Command), Zračnega poveljstva za izobraževanje in urjenje (Air Education and Training Command), Zračnega bojnega poveljstva (Air Combt Command), Zračnega poveljstva za vesolje (Air Space Command), AF ISR agencije, Zračne Nacionalne Garde (Air National Guard – v primeru mobilizacije) ter Zračnih rezervnih sil (AF Reserve – v primeru mobilizacije) (Internet 25).

Struktura oboroženih sil ZDA, namenjenim informacijskim operacijam, je zelo zapletena. Opredeljevanje in naštevanje teh enot smo opravil na najbolj jedrnat način, saj bi v primeru, da bi se iz operativnega nivoja spustili na taktični nivo opredeljevanja strukture in enot oboroženih sil ZDA za informacijsko bojevanje, zapletli v nedogled in analizo strukture končali na nekaj sto straneh.

5.4 Velika Britanija

Oborožene sile Združenega kraljestva, bolje poznane kot Britanske oborožene sile oziroma Oborožene sile Njenega Veličanstva, so obkrožene z delovanjem vseh treh zvrsti oboroženih sil. S slabimi pol milijona vojaki jih prištevamo med največje vojske v Evropi, čeprav so po številu vojakov v svetovnem merilu »le« na 26. mestu, glede na

višino izdatkov v obrambne namene[17] trdno sledijo vojskama ZDA in Francije, kar pomeni, da so v svetovnem merilu na tretjem mestu (Internet 21).

Vrhovni poveljnik Britanskih oboroženih sil je britanski monarh (kraljica Elizabeta II). Vodene so s strani Obrambnega sveta Ministrstva za obrambo (Defence Council). Skladno s tradicionalno ustavno konvencijo ima dejansko avtoriteto nad oboroženimi silami britanski premier.

V britanski vojski je bilo aprila 2006 195.900 pripadnikov oboroženih sil stalne sestave, v rezervni sestavi pa 191.300 pripadnikov redne rezerve in 42.300 pripadnikov prostovoljne rezerve. Porazdelitev osebja med zvrsti oboroženih sil je prikazana v sledeči tabeli.

Tabela 3: Sestava oboroženih sil Velike Britanije

	Stalna sestava	**Redna rezerva**	**Prostovoljna rezerva**
Mornarica	39.400	23.200	3.600
Kopenska vojska	107.700	160.200	37.300
Zračne sile	48.700	35.000	1.400
SKUPAJ	**195.900**	**222.300**	**42.300**

Vir: Internet 27.

Večina osebja je znotraj kopenske vojske oboroženih sil, v odstotkih bi to pomenilo slabih 55 % vseh oseb, medtem ko je v mornarici dobrih 20 %, v zračnih silah pa slabih 25 % ljudi.

5.4.1 STRUKTURA OBOROŽENIH SIL VELIKE BRITANIJE

Oborožene sile Velike Britanije so združene pod enotnim poveljstvom in se delijo na tri dele:

- **Kraljeva mornarica,**
- **Kraljeva kopenska vojska,**
- **Kraljeve zračne (letalske) sile.**

[17] V fiskalnem letu 2008/2009 bo za obrambno dejavnost namenjeno 33,6 milijard britanskih funtov, kar glede na celoten proračun Velike Britanije znaša 2,2 % bruto domačega proizvoda.

Oborožene sile Velike Britanije se v svojem delovanju povezujejo oziroma imajo značilnosti modularnih sil, kar pomeni, da so namensko oblikovane bojne skupine (Task Forces), sestavljene iz različnih virov, tako v nacionalnem (v primeru podpore silam zveze NATO) kot tudi v strukturno-funkcionalnem vidiku.

V zdajšnjih strukturnih spremembah sil in programski spremembi bistva obrambne dejavnosti se cilja predvsem na zmanjševanje osebja znotraj oboroženih sil Velike Britanije. Do konca leta 2008 naj bi se število ljudi znotraj Kraljeve mornarice zmanjšalo na okoli 36.000, Kraljeve kopenske vojske na okoli 102.000, Kraljevih zračnih sil iz 48.700 na okoli 41.000 ljudi ter znotraj sektorja civilnega osebja za okoli 10.000 ljudi. Zaradi teh procesov bo v skupnem številu oborožene sile moralo zapustiti več kot 15.000 ljudi (Internet 27).

5.4.2 ENOTE ZA ELEKTRONSKO BOJEVANJE

Znotraj oboroženih sil Velike Britanije obstaja sistem enot za informacijsko bojevanje, ki je podvržen sistemu modularnosti. V kopenski vojski tako obstaja del enot znotraj enega samega rodu, ki je namenjen elektronskemu bojevanju in je zadolžen za to delovanje tudi v drugih zvrsteh oboroženih sil. Glede na analizo teh oboroženih sil sem prišel do spoznanja, da so, kljub temu da veljajo za evropsko velesilo in namenjajo v obrambne namene izdaten kup denarja, na področju informacijskega vojskovanja in s tem povezanih enot v primerjavi z oboroženimi silami ZDA še v povojih. Poleg enot, namenjenih informacijskemu bojevanju, znotraj oboroženih sil Velike Britanije delujejo tudi druge organizacije[18] in izobraževalne ustanove, namenjene tej obliki bojevanja.

[18] Ena takšnih organizacij oziroma struktur je Obrambna Informacijska Struktura (Defence Information Infrastructure), ki je v lasti Ministrstva za obrambo. Gre za varno omrežje znotraj ministrstva, ki pokriva tudi druge zvrsti vojske, vključno s kopensko vojsko, mornarico in zračnimi silami. V njeno strukturo so vključene tudi vse letalske baze doma in po svetu ter ladjevje na morju, ne pa tudi letala med samim letenjem. Namen tega omrežja je preprečevanje kopiranja in shranjevanja podatkov končnih uporabnikov znotraj Ministrstva za obrambo. Ta struktura podpira 2.000 spletnih strani znotraj Ministrstva za obrambo z nekaj več kot 150.000 terminali (računalniki) ter 300.000 uporabniških računov. Ta sistem prav tako omogoča dostop uporabnikov do njihovega dovoljenega nivoja informacij, kar pomeni, da lahko vidijo informacije, za katere so avtorizirani.

5.4.2.1 Kopenska vojska (Internet 27)

Struktura britanske kopenske vojske je v glavnem podobna kot pri Kraljevi mornarici in Kraljevih zračnih silah, kar pomeni, da je razdeljena na dva dela, in sicer na Kopensko poveljstvo (Land Command) in Pomožno poveljstvo (Adjutant-General). Ti dve enoti sta zadolženi za zagotovitev operativno pripravljenih sil za uporabo s strani Stalnega združenega poveljstva (Permanent Joint Headquarters). Pomožno poveljstvo je zadolženo za trening tako novincev kot tudi lastnih in profesionalnih sil, medtem ko je vrhovni poveljnik Kopenskega poveljstva zadolžen za planiranje in zagotavljanje popolnjenih in primerno kolektivno izurjenih operativnih formacij.

Kopenska vojska se deli na tri dele, in sicer:

- **BOJNE SILE:**
    - Kraljevi oklepni bataljoni (Royal Armoured Corps),
    - Pehota (znotraj teh sil je tudi SAS[19]),
    - Zračne sile kopenskih sil (sestavljene iz osmih polkov).

- **BOJNE PODPORNE SILE:**
    - Kraljevi artilerijski regiment,
    - Bataljoni kraljevih inženirjev,
    - **Kraljevi bataljoni za zveze,**
    - **Obveščevalni bataljoni.**

- **BOJNE SLUŽBE**
    - Kraljevi oddelek vojaških duhovnikov kopenske vojske,
    - Kraljevi logistični bataljoni,
    - Zdravstvene službe kopenske vojske,
    - Bataljoni kraljevih inženirjev za električno in mehanično dejavnost,
    - Bataljoni pomožnega poveljstva,
    - Bataljon šole za osebno oborožitev,
    - Bataljoni za fizično urjenje kopenske vojske,

[19] Special Air Service regiment, znan po svojih specialnih akcijah.

- Bataljoni splošnih služb,
- Bataljon vojaške godbe.

Od enot, ki zagotavljajo zmožnosti za delovanje v informacijskih operacijah, sta za nas pomembni predvsem dve entiteti znotraj bojnih podpornih sil. Ti enoti sta sestavna dela Kraljevih bataljonov za zveze in obveščevalnih bataljonov.

5.4.2.1.1 Kraljevi bataljoni za zveze (Royal Corps of Signals)

Bataljoni so zadolženi za nameščanje, vzdrževanje in uporabo vseh vrst telekomunikacij in telekomunikacijske opreme ter informacijskih sistemov. Bataljoni za zveze so razdeljeni v tri brigade za zveze, in sicer:

- **1. brigada za zveze,** ki je stacionirana v Nemčiji, v njeni sestavi pa sta 7. in 16. regiment[20] za zveze ter bataljon za podporo zavezniškim hitro odzivnim silam.
- **2. brigada za zveze**, ki je zadolžena predvsem za nacionalne komunikacije na območjih, kjer deluje, v njeni sestavi pa delujejo 10., 31., 32., 36., 37., 38., 40. in 71. regiment za zveze ter 1., 2., in 18. eskadrilja za zveze.
- **11. brigada za zveze,** v kateri delujejo 2., **14.** in 30. regiment za zveze (Internet 29)

5.4.2.1.2 14. regiment za zveze (Internet30)

Organigram 5.5: Struktura 14. regimenta za zveze

Vir: Internet 30.

14. regiment za zveze je edina enota znotraj kopenske vojske, katere namen je elektronsko bojevanje. Naloga regimenta je zagotavljanje učinkovitih in vzdržljivih

[20] Regiment v britanski vojski pomeni enoto na ravni bataljona v oboroženih silah ZDA.

zmožnosti za elektronsko bojevanje, s katerimi odgovarjajo potrebam na boj pripravljenih enot in obveščevalno-zvezni dejavnosti. Omenjene naloge postavljajo 14. regiment za zveze na dominanten položaj v elektronskem bojnem okolju. Za uspešnega doseganje ciljev znotraj 14. regimenta za zveze delujejo trije eskadroni za elektronsko bojevanje, ki so med seboj zmožni delovati kot mešane enote z namenom podpore različnim vrstam operacij.

Poveljstvo regimenta je sestavljeno iz štaba regimenta, celice za koordinacijo elektronskega bojevanja (Electronic Warfare Coordination Cell - EWCC) in logistične podpore.

5.4.2.1.3 226. eskadron za zveze (Internet 30)

226. eskadron za zveze zagotavlja podporo za elektronsko bojevanje Zavezniškemu poveljstvu za hitro odzivne enote v Evropi, ki je sestavljeno iz enot različnih držav. 640. četa za zveze, ki je del eskadrona, zagotavlja podporo za elektronsko bojevanje Skupnim hitro odzivnim silam (Joint Rapid Deployment Force – JRDF). To zagotavlja celotnemu eskadronu edinstveno nalogo delovanja v problematičnih delih sveta, kjer ima vlogo podpore obstoječim operacijam.

5.4.2.1.4 237. eskadron za zveze (Internet 30)

237. eskadron za zveze je dodeljen 3. pehotni diviziji oboroženih sil Velike Britanije in ima nalogo podpore enotam v boju z elektronskim bojevanjem. V času miru eskadron, z namenom urjenja lastnih primarnih vlog, zagotavlja opremo in osebje za podporo operacijam po svetu, a pogosto le z kratek čas. Del eskadrona je tudi novoustanovljena Lahka skupina za elektronsko bojevanje (Light Electronic Warfare Team – LEWT), ki zagotavlja podporo elektronskega bojevanja 16. zračni jurišni brigadi. Ustanovljena je z namenom prikritega in predvsem hitrega[21] apliciranja elektronskega bojevanja na bojnih linijah v vseh situacijah operacije.

[21] Dospetje na bojišče s pomočjo padal.

5.4.2.1.5 245. eskadron za zveze (Internet 30)

245. eskadron za zveze je dodeljen 1. oklepni diviziji oboroženih sil Velike Britanije in zagotavlja elektronsko delovanje v podporo bojnemu mlinu angleških oboroženih sil. Eskadron se prav tako udeležuje vaj po Evropi skupaj s 1. divizijo. Kot drugi eskadroni znotraj 14. regimenta za zveze tudi 245. eskadron za zveze zagotavlja opremo in osebje za podporo operacijam po svetu.

5.4.2.1.6 Obveščevalni bataljon

Obveščevalne enote so v britanski vojski zadolžene za zbiranje in analiziranje vojaških obveščevalnih podatkov, naloga teh enot pa je prav tako protiobveščevalna in podatkovno varnostna dejavnost. Glavna formacija znotraj teh enot je 1. vojaško-obveščevalna brigada, kateri so podrejene sledeče enote:

- 1. vojaško-obveščevalni bataljon,
- 2. vojaško-obveščevalni bataljon,
- 3. vojaško-obveščevalni bataljon,
- 4. vojaško-obveščevalni bataljon (teritorialne enote – v primeru mobilizacije),
- 5. vojaško-obveščevalni bataljon (teritorialne enote – v primeru mobilizacije),
- **15. skupina za psihološke operacije** (15th Psychological Operations Group).

5.4.2.1.7 15. skupina za psihološke operacije (Internet 31)

15. skupina za psihološke operacije je namenjena delovanju v sklopu vseh zvrsti oboroženih sil Velike Britanije, kar pomeni, da so njene enote po potrebi prisotne tako v kopenski vojski kot tudi v mornarici in zračnih silah. Nastanjena je v Bedfordskire-u v sklopu Obrambnega obveščevalnega in varnostnega centra (Defense Intelligence and Security Centre).

Trenutno 15. skupino za psihološke operacije sestavlja 37 pripadnikov stalne sestave oboroženih sil in 28 rezervistov, ki prihajajo iz enot Kraljeve mornarice, Kraljevih marincev, bojnih in podpornih enot kopenske vojske ter Kraljevih zračnih sil. Opremljena z najnaprednejšo elektronsko opremo, je skupina sposobna brez cenzure in

drugih motenj načrtovati, proizvajati in zakodirati PSYOP sporočila. Skupina zagotavlja urjenje praktikantov psiholoških operacij in ima v odnosu do operacij status visoke pripravljenosti. Skupina je prav tako prisotna v Poveljstvu združenih sil in v drugih delih poveljstva z namenom podpore pri načrtovanju ob izvajanju velikih vaj, je pa tudi zelo pomemben element pri urjenju raznih enot pred uporabo le-teh na bojišču.

5.4.2.2 Kraljeve zračne sile

Znotraj zračnih sil Velike Britanije ni visoke sofisticiranosti sistemov za izvajanje informacijskih operacij kot v primeru ZDA. V strukturi samega poveljstva Kraljevih zračnih sil (Royal Air Force Air Command – RAF Command) velja omeniti prisotnost Centra za bojevanje v zraku (Air Warfare Centre – AWC), ki je zadolžen za formuliranje taktične doktrine ter upravljanje poskusov v zvezi z različnimi operacijami. V sklopu AWC so prisotni sledeči sektorji:

- Poveljstvo AWC,
- Sektor za operativno doktrino,
- Sektor za taktiko,
- **Sektor za elektronsko bojevanje,**
- Sektor za operativno analizo,
- Sektor za operativno testiranje in vrednotenje (Internet 32).

V Centru za bojevanje v zraku, ki je stacioniran v Waddington-u, deluje več kot 3.000 ljudi in je glavno operativno oporišče zračnih obveščevalnih sistemov. Opremljen je z letali za pridobivanje obveščevalnih podatkov, kot so Sentinel R1, Nimrod R1, E-3D Sentry (sistem AWACS).

Center sestavlja sedem eskadrilj Kraljevih zračnih sil, od tega so operativne le tri, in sicer:

- **5. eskadrilja** (sodelujoča s kopensko vojsko), ki je bila ustanovljena leta 2004 in je označila začetek vojaškega obveščevalnega, nadzornega in izvidniškega delovanja znotraj zračnih sil. Nova naloga eskadrilje je operiranje z radarskim

sistemom ASTOR[22] R-1, kjer R pomeni izvidniško (reconnaissance) dejavnost. V 5. eskadrilji, ki je največja znotraj Centra za zračno bojevanje, deluje nekaj več kot 300 pripadnikov Kraljevih zračnih sil, kopenske vojske ter civilistov.

- **23. eskadrilja** je prav tako opremljena z letali, ki imajo montiran radarski sistem ASTOR R-1. Namenjena je izvidništvu in obrambi zračnega prostora na področju Velike Britanije in na področju evropskih zavezniških držav v sklopu zveze NATO.
- **51. eskadrilja** je opremljena z letali NIMROD R-1, ki so znotraj angleške vojske že tako prepoznaven sistem, da se ob strukturiranju obveščevalnih, nadzornih in izvidniških misij poveljniki najpogosteje odločijo za letala NIMROD R-1 (Internet 32).

V sklopu Kraljevih zračnih sil na področju zračne obrambe in zgodnjega opozarjanja delujeta še dve eskadrilji, ki pa nista vključeni v Center za zračno bojevanje. To sta 8. in 23. eskadrilja, opremljeni s sedmimi letali tipa E-3D Sentry[23].

5.4.2.3 Kraljeva mornarica

Glede Kraljeve mornarice je zelo malo podatkov o enotah za informacijsko bojevanje, pa vendar imajo na Ministrstvu za obrambo razvit sistem Integriranih skupin za elektronsko delovanje znotraj mornarice (Naval Electronic Warfare Integrated Project Teams - NEWIPT).

Naloga NEWIPT je podpora ladjevju Kraljeve mornarice z zagotavljanjem odkrivanja najnovejših pojavov protiladijskih, letalskih in asimetričnih groženj in ukrepov proti njim. S tem namenom z NEWIPT pokrivajo širok spekter mornariških aktivnosti za elektronsko bojevanje. NEWIPT sestavljajo civilne osebe ter pripadniki Kraljeve mornarice iz različnih disciplin, vključno z inženirji (Internet 34).

[22] Radarski sistem ASTOR je nadgradnja Raytheon-ovega radarskega sistema ASARS-2, ki ga uporablja ameriška vojska v svojih letalih tipa U-2. ASTARS deluje na velikih višinah v vseh vremenskih pogojih z namenom zagotavljanja fotografij z visoko resolucijo (Internet 33).
[23] Letalo E-3D Sentry ima nadzorno vlogo in vlogo vodenja in poveljevanja, posadka pa šteje 18 ljudi.

5.4.3 OMOGOČENA ZMOŽNOST OMREŽNEGA VOJSKOVANJA (NETWORK ENABLED CAPABILITY - NEC)

NEC pomeni ekvivalentni koncept omrežnega vojskovanja znotraj ameriške vojske (Network Centric Warfare – NCW). V daljnoročnem načrtu[24] Ministrstva za obrambo se razvoj NEC-a deli na tri faze, in sicer:

- Začetna faza v letu 2007 večinoma vključuje izboljšanje komunikacijskih povezav med novo nabavljeno in obstoječo opremo.
- Tranzicijska faza do leta 2015 vključuje integracijo komunikacijskih sistemov na ravni države.
- Zrela faza med leti 2020 in 2030 pa bo vključevala komunikacijsko sinhronizacijo z vsakim možnim kosom vojaške opreme (Internet 35).

V obdobju petih let se bodo izvajali številni veliki projekti opremljanja oboroženih sil, s čimer bo podprta sama filozofija NEC-a:

- Skynet 5 med vsemi predstavlja najpomembnejši projekt. V okviru tega projekta bodo prišli v uporabo najsodobnejši vojaški komunikacijski sateliti, ki bodo v podporo delovanju vseh vrst operacij britanske vojske.
- Projekt Cormorant[25] bo imel nalogo povezovanja strateških satelitskih komunikacij z operativnimi poveljstvi in enotami.
- Projekt Falcon bo zagotovil varnost komunikacijskih sistemov na operativni ravni bojišča.
- Obrambna informacijska infrastruktura pa bo omogočala prenos podatkov iz poveljstva neposredno do končnih uporabnikov (komunikacijskih sistemov taktičnih enot) (Internet 36).

Ministrstvo za obrambo prav tako v sklopu NEC[26]-a vlaga denarna sredstva v Program razvoja radarskih sistemov ASTOR, Program brezpilotnih letal, imenovan Watchkeeper, ter v izboljšanje zmožnosti za elektronsko bojevanje.

[24] Ministry of Defence, Future Capabilities: Factsheet 4; Network Enabled Capability; 2007

[25] Cormorant – modularni, zračnotransportni komunikacijski sistem, ki zagotavlja direktno podporo vojaškim uporabnikom in v sami komunikacijski strukturi predstavlja hrbtenico omrežnih povezav med vojaškimi sistemi, kot so na primer BOWMAN, DLAN, RTTS (Transportni telekomunikacijski sistem Kraljevih zračnih sil).

5.4.4 ZDRUŽENI EKSPERIMENTALNI LABORATORIJ ZA ELEKTRONSKO BOJEVANJE (Joint Electronic Warfare Experimentation Laboratory – JEWEL)

Nadzor nad zračnimi potmi je v današnjih bojnih in mirovniških operacijah postal tako kritičen, da se je angleško podjetje Thales UK Ltd. odločilo odpreti novo ustanovo, v kateri lahko britanska vojska in v prihodnosti tudi zavezniške sile urijo svoje spretnosti na področju elektronskega bojevanja in odpravijo pomanjkljivosti, še preden jih odkrije nasprotnik.

V JEWEL-u, ki je bil odprt februarja 2008, se nahaja popolnoma operativna kopija centra za operacije elektronskega bojevanja s številno poskusno opremo. Ustanovitev JEWEL-a je bil Thalesov spontani odgovor na spreminjajoče se razmere na bojišču, saj je informacijska tehnika, ki je lahko uporabljena kot informacijsko orožje (ure, telefoni, računalniki in podobno), dostopna takorekoč na vsakem koraku. Z JEWEL-om želijo v oboroženih silah Velike Britanije razviti inovativne postopke za zoperstavljanje tem nevarnostim.

V prihodnosti se bo JEWEL pridružil ostalim centrom in laboratorijem v Veliki Britaniji in Evropi, znanim pod skupnim imenom Center za transformacijo vojskovanja (Battle Transformation Centre).

[26] Koncept programa NEC je v surovi obliki že bil uporabljen s strani Britanske vojske. Med operacijo Telic (s strani Britanske vojske poimenovana invazija na Irak leta 2003) je bil 42. diverzantski oddelek Kraljevih marincev močno obstreljevan s strani iraškega topništva. Sovražnikovo strelsko pozicijo je odkril radar za lokacijo strelskega orožja ARTHUR, podatke o le-tej pa je posredoval helikopterju za zgodnje opozarjanje, Sea King, ki je deloval v okviru Kraljeve mornarice. Podatki so bili nato posredovani enoti, ki je upravljala brezpilotno letalo, ta pa je odkrila natančno pozicijo iraškega topništva blizu Basre. S temi podatki so Kraljeve letalske sile uspešno onemogočile enoto, ki je obstreljevala 42. diverzantski oddelek Kraljevih marincev (Internet 36).

6 ZAKLJUČEK

V zadnjem delu naloge bom preveril točnost postavljenih hipotez in jih v nadaljnjem koraku tudi potrdil ali zavrgel. V naslednjem koraku bom v sklepnem delu opredelil svoje stališče do preoblikovanja sodobnih vojska, ki se spreminjajo ravno zaradi pojava informacijskih operacij, ter izpostavil probleme pri soočanju z opredeljevanjem enot, namenjenih informacijskemu bojevanju, izbranih držav.

6.1 Preverjanje hipotez

6.1.1 PREVERJANJE SPLOŠNE HIPOTEZE

Splošna hipoteza, ki sem jo postavil na začetku pisanja naloge, se je nanašala na pojav informacijskih operacij in vpliv le-teh na strukturo oboroženih sil. V svojem delu sem dokazal, da ima vsaka izbrana država, ki sem jo podrobneje predstavil, posebne sile oziroma enote, katerih namen je prav delovanje znotraj informacijskih operacij. To ne pomeni, da vsaka enota izvaja vse oblike informacijskega vojskovanja, ampak da obstaja več enot, specializiranih za določeno obliko informacijskega vojskovanja, kot je na primer elektronsko bojevanje. Dejstvo je, in to sem tudi dokazal, da se sodobne vojske precej zavedajo pojava digitalizacije sodobnega bojišča, kar je posledično vplivalo na ustvarjanje novih enot znotraj oboroženih sil, katerih dejavnost je informacijsko bojevanje. Tako lahko na tem mestu mojo splošno hipotezo potrdim.

6.1.2 PREVERJANJE POSEBNE HIPOTEZE

Glede potrjevanja posebne hipoteze sem nekoliko težje prišel do odločitve, da lahko to hipotezo potrdim, kot pri potrjevanju splošne hipoteze. Posebna hipoteza trdi, da imajo zaradi same kompleksnosti ciljev in informacijskih operacij, ki zadevajo vse ravni družbenega življenja, vojaško in gospodarsko bolj razvite države jasneje dodelan koncept informacijskega bojevanja kot informacijsko manj razvite države. Če se na tem mestu opredelim do koncepta informacijskega bojevanja zgolj na podlagi vsebnosti enot za informacijsko bojevanje izbranih oboroženih sil, lahko, s sicer manjšo gotovostjo kot pri osnovni hipotezi, posebno hipotezo potrdim. Glede na število enot in kompleksnost sistema in organizacij, ki zadevajo informacijsko bojevanje, imajo vojaško bolj razvite

države bolj dodelan koncept kot vojaško šibkejše oziroma manj razvite države. Tako imajo ZDA in Velika Britanija v okviru ministrstev za obrambo in v okviru oboroženih sil določene razvojne programe, agencije ali druge institucije, ki se posvečajo delovanju oziroma razvoju lastnih enot v informacijskih operacijah. Na drugi strani pa so tukaj šibkejše, strukturno manj razvite vojske, ki na primer teh institucij nimajo, in sem zlahka prištevam tudi Slovenijo. Torej lahko tudi posebno hipotezo, kakor sem že prej napovedal, potrdim.

6.2 Sklep

Kljub temu, da sem v svojem delu izpolnil in dokazal pričakovanja obeh hipotez, lahko povem, da sem pri doseganju tega cilja naletel na nemalo težav. Problem v analiziranju sistemov in enot za informacijsko bojevanje je v tem, da v vseh državah, in to brez izjem, obstaja velika mera zaupnosti in nedostopnosti virov. Tako sem ob poskušanju podrobnejšega definiranja enot za elektronsko bojevanje v Slovenski vojski naletel na zaprta vrata, saj o podrobnejšem opisu enote za elektronsko bojevanje v Slovenski vojski ni nobene dodatne možne literature, razen na Poveljniško štabni šoli in Šoli za častnike, pri čemer moramo upoštevati, da je dostop do virov omejen. Podobna situacija je veljala tudi za oborožene sile Velike Britanije in ZDA, kjer se je sicer ob jasnejši strukturi enot za elektronsko bojevanje, tipiziranje oziroma razčlenjevanje le-teh najpogosteje končalo na ravni bataljona, kar tudi kaže na dodatno mero zaupnosti glede teh enot. Problem razčlenjevanja enot pa ni bil osamljen problem, saj se je težavnost zbiranja primarnih virov kazala tudi na področju analiziranja opreme, namenjene informacijskemu vojskovanju. Tako sem od pripadnika enote za zveze v Slovenski vojski ob vprašanju glede opremljenosti enote dobil odgovor, da več kot o obstoju enote in njenega nahajanja znotraj 5. obveščevalno izvidniškega bataljona ne morem izvedeti. Znotraj oboroženih sil ZDA in Velike Britanije je sicer bil postopek zbiranja podatkov drugačen, vendar o opremi, razen v grobem opisu, podatkov ni bilo moč najti.

Na koncu pa še beseda ali dve o preoblikovanju oboroženih sil oziroma o pojavu namenskih enot za informacijske operacije. Čeprav so se priprave oboroženih sil na informacijsko bojevanje in digitalno bojišče začele zelo zgodaj (na primer v ameriški vojski, v kateri je artilerija, opremljena s sistemi za vodenje ognja, od leta 1980, oklepne enote od leta 1986 in letalstvo od leta 1989), so informacijski način bojevanja v

praksi prvič predstavili med prvo zalivsko vojno. Ta vojna je znana po tem, da so v njej prvič množično uporabili informacijsko in satelitsko tehnologijo ter digitalne komunikacije, kar pomeni, da imajo ZDA na tem področju vse do danes izkušnje in skoraj dveletno tradicijo, medtem ko je v Sloveniji ta dejavnost še mlada. Dejavnost je relativno mlada tudi v Veliki Britaniji, saj se enote za informacijske operacije, razen nekaterih že obstoječih izjem, šele formirajo. Za sedanjost in prihodnost bojevanja je in bo značilna modularnost oboroženih sil, kjer bodo namenske enote sestavljene iz več različnih podenot, kar pomeni, da bodo enote postale samozadostne in multifunkcionalne. Prav tako bo po mojem mnenju v tej smeri potekal razvoj enot za informacijsko bojevanje, kjer bodo, tako kot v Britanski vojski, te enote razdeljene v modularne celice po 5 ali deset mož, ki se bodo nato priključile večjim enotam. V prihodnosti je možno pričakovati tudi večji razcvet na področju informacijske tehnologije. Države, ki danes veljajo za šibkejše in manj razvite, bodo najbrž že v naslednjem letu ali dveh zaradi konstantnega nižanja cen tehnologije postale njen uporabnik, s čimer se bo informacijsko bojevanje v primeru napada močnejših in informacijsko-tehnološko bolj razvitih držav prevesilo iz unilateralnega v multilateralno informacijsko bojevanje.

7 LITERATURA

1. Adanić, Stjepan in Siniša Tatalović. 1993. *Oružane snage: Novačenje i mobilizacija*. Zagreb: Otvoreno sveučilište.
2. Dokl, Jure. 2006. *Internet in koncept človekove varnosti.* Diplomsko delo. Ljubljana: FDV.
3. International Institute for Strategic Studies. 2006. *The military balance: 2006*. Oxford: Oxford University Press.
4. INTERNET 1: Department of Army. 2003. *FM 3-13: Information operations*. Dostopno prek: http://www.iwar.org.uk/iwar/resources/doctrine/fm-3-13.pdf (12. maj 2008).
5. INTERNET 2: Naef, Wanja Eric. 2003. *Information operations interview with Dan Kuehl.* Dostopno prek: http://www.iwar.org.uk/infocon/io-kuehl.htm (16. maj 2008).
6. INTERNET 3: Joint Chiefs of Staff. 2006. *JP 3-13: Joint doctrine for information operations*. Dostopno prek: http://www.iwar.org.uk/iwar/resources/us/jp3_13.pdf (12. maj 2008).
7. INTERNET 4: *Computer Industry Almanac Inc.* 2007. Dostopno prek: http://www.c-i-a.com/pr0907.htm (29. april 2008).
8. INTERNET 5: Statistični urad Republike Slovenije. 2007. *Uporaba IKT v gospodinjstvih*. Dostopno prek: http://www.stat.si/novica_prikazi.aspx?id=1283 (2. maj 2008).
9. INTERNET 6: Raba interneta v Sloveniji. 2007. *Uporabniki interneta*. Dostopno prek: http://www.ris.org/index.php?fl=0&p1=276&p2=621&p4=1184&id=1184 (29. maj 2008).
10. INTERNET 7: Human development report. 2008. *Technology: diffusion and creation*. Dostopno prek: http://hdrstats.undp.org/indicators/128.html (25. september 2008).
11. INTERNET 8: European innovation scoreboard. 2007. *Comparative analysis of innovation performance*. Dostopno prek: http://www.proinnoeurope.eu/admin/uploaded_documents/European_Innovation_Scoreboard_2007.pdf (27. september 2008).

12. INTERNET 9: Central Inteligence Agency. 2007. *The World Factbook*. Dostopno prek: https://www.cia.gov/library/publications/the-world-factbook/geos/us.html (12. junij 2008).
13. INTERNET 10: Cyberspace Policy Institute. 2003. *Information Warfare – an introduction*. Dostopno prek: http://www.trinity.edu/rjensen/infowar.pdf (22. september 2008).
14. INTERNET 11: Center vlade RS za informatiko. 2006. *Delovanje virusa*. Dostopno prek: http://www.gov.si/cvi/slo/virus/delovanjevirusa.htm (5. maj 2008).
15. INTERNET 12: Federation of american scientist. 2006. *Force XXI Battle Command, Brigade-and-Below (FBCB2)*. Dostopno prek: http://www.fas.org/man/dod-101/sys/land/fbcb2.htm (26. maj 2008).
16. INTERNET 13: Global Security. 2006. *Fleet Battle Experiment*. Dostopno prek: http://www.globalsecurity.org/military/ops/fbe.htm (12. maj 2008).
17. INTERNET 14: Janes Information Group. 2007. *Jane's C4I Systems*. Dostopno prek: http://jc4i.janes.com/client/jc4i/index.shtml (23. maj 2008).
18. INTERNET 15: Turnšek, Tit. 2003. *Digitalno bojišče*. Dostopno prek: http://www.mladina.si/tednik/200036/clanek/vojak-21/index.print.html-l2 (24. maj 2008).
19. INTERNET 16: Slovenska vojska. 2008. *Poklicna struktura*. Dostopno prek: http://slovenskavojska.si/poklicna/struktura/index.htm (9. junij 2008).
20. INTERNET 17: Slovenska vojska. 2008. *Bataljon za zveze*. Dostopno prek: http://slovenskavojska.si/poklicna/enote/pssv/11bzv.htm (9. junij 2008).
21. INTERNET 18: Centralni katalog informacij javnega značaja. 2007. *OVS*. Dostopno prek: http://www.ckijz.gov.si/index.php?id=98&no_cache=1&tx_katalogijzpregled_pi1%5Buid_katalog%5D=190&tx_katalogijzpregled_pi1%5Benota%5D=156&cHash=e1cf1fbe81 (28. september 2008).
22. INTERNET 19: Slovenska vojska. 2008. *5. obveščevalno izvidniški bataljon*. Dostopno prek: http://slovenskavojska.si/poklicna/enote/pssv/oib.htm (4. junij 2008).
23. INTERNET 20: Državni zbor Republike Slovenije. 2004. *Resolucija o splošnem dolgoročnem programu razvoja in opremljanja Slovenske vojske*. Dostopno

prek: http://www.uradnilist.si/1/objava.jsp?urlid=200489&stevilka=4023 (6. junij 2008).

24. INTERNET 21: Stockholm International Peace Research Institute. 2007. *The SIPRI military expenditure database*. Dostopno prek: http://milexdata.sipri.org/result.php4 (13. junij 2008).
25. INTERNET 22: US Military. 2008. *Armed forces strenght figures for August 31 2008*. Dostopno prek: http://siadapp.dmdc.osd.mil/personnel/MILITARY/ms0.pdf (25. maj 2008).
26. INTERNET 23: US Military. 2008. *Stations and bases*. Dostopno prek: http://www.globalsecurity.org/military/ops/global-deployments.htm (5. junij 2008).
27. INTERNET 24: US Military. 2008 *Military organisation*. Dostopno prek: http://www.army.mil/institution/organization/ (5. junij 2008).
28. INTERNET 25: U.S. Army War College. 2007. *Information operations Primer*. Dostopno prek: http://www.iwar.org.uk/iwar/resources/primer/info-ops-primer.pdf (2. junij 2008).
29. INTERNET 26: Air Force Cyber Command. 2008. *Organisation Chart*. Dostopno prek: http://www.afcyber.af.mil/units/ (23. maj 2008).
30. INTERNET 27: Ministry of Defence. 2007. *About Defence*. Dostopno prek: http://www.mod.uk/DefenceInternet/AboutDefence/ (3. junij 2008).
31. INTERNET 28: British Army. 2008. *British Army Structure*. Dostopno prek: http://www.army.mod.uk/unitsandorgs/index.htm (3. junij 2008).
32. INTERNET 29: British Army. 2008. *Royal Signals Website*. Dostopno prek: http://www2.army.mod.uk/royalsignals/index.htm (3. junij 2008).
33. INTERNET 30: British Army. 2008.*11. Signal Regiment*. Dostopno prek: http://www2.army.mod.uk/royalsignals/14sigregt/index.htm (3. junij 2008).
34. INTERNET 31: Ministry of Defence. 2007. *15. (United Kingdom) Psychological Operations Group, Annual report 2007*. Dostopno prek: http://www.psywar.org/psywar/reproductions/15POG_Annual_Report_2008.pdf (3. junij 2008).
35. INTERNET 32: Royal Air Force. 2008. *Air Warfare Center*. Dostopno prek: http://www.raf.mod.uk/rafwaddington/aboutus/airwarfarecentre.cfm (4. junij 2008).

36. INTERNET 33: Raytheon. 2008. *Airbourne Standoff Radar*. Dostopno prek: http://www.raytheon.com/capabilities/products/astor/ (4. junij 2008).
37. INTERNET 34: R & F Defence Publications. 2007. *Defence projects: Naval Electronic Warfare*. Dostopno prek: http://www.armedforces.co.uk/projects/raq40ffa115bc0b6 (7. junij 2008).
38. INTERNET 35: Network Enabled Capability. 2007. *The UK's programme to enhance military capability by better exploitation of information*. Dostopno prek: http://www.iwar.org.uk/rma/resources/uk-mod/nec.htm (8. junij 2008).
39. INTERNET 36: Ministry of Defence. 2008. *Network Enabled Capability*. Dostopno prek: http://www.mod.uk/NR/rdonlyres/E1403E7F-96FA-4550-AE14-4C7FF610FE3E/0/nec_jsp777.pdf (21. junij 2008).
40. INTERNET 36: Sherman, Jeremy. 2007. *SCIBIT: Building a Scientifically Coherent Integrated Bottom-Up Information Theory*. Dostopno prek: http://www.metanexus.net/magazine/ArticleDetail/tabid/68/id/10592/Default.aspx (19. september 2008).
41. INTERNET 37: Thales. 2008. *Thales unveils dedicated electronic warfare laboratory*. Dostopno prek: http://www.thalesgroup.com/uk/Press-Room/Press-Release-search-all/Press-Release-search-result/Press-Release-Article.html?link=0e694e77-0647-4666-0b18-260a6c36442a:central&locale=EN-gb&Title=Thales+unveils+dedicated+electronic+warfare+laboratory&dis=1 (21. junij 2008).
42. Jankovič, Zoran. 1998. *C^4I Sistemi*. Poljče: Poveljniško štabna šola.
43. Kladnik, Tomaž. 2006. Majhna, profesionalna in sodobna: 15 let Slovenske vojske. *Revija Obramba* 38/5: 32 – 43.
44. Kočevar, Iztok. 2003. Irak – digitalizirano vojskovališče?. *Revija Obramba* 35/7: 50 – 55.
45. --- 2004. Digitalizirano bojišče. *Bilten Slovenske vojske* 6/1: 42.
46. --- 2006. Izziv informacijske dobe: digitalizacija vojske in digitalno bojišče. *Revija Obramba* 38/10: 22 – 25.
47. Kotnik-Dvojmoč, Igor. 2002. *Preoblikovanje oboroženih sil sodobnih evropskih držav*. Ljubljana: FDV.
48. Malešič, Marjan. 1996. *Civilna obramba sodobnih držav.* Doktorska disertacija. Ljubljana: FDV.

49. Pajk, Josip. 1996. Informacijsko ratovanje i digitalizirano bojište. *Hrvatski vojnik* 11/VI: 30 – 33.
50. Svete, Uroš. 2007. Varnostne implikacije uporabe informacijsko-komunikacijske tehnologije. *Elektronsko upravljanje in poslovanje v službi uporabnika*, ur. Uroš Pinterič in Uroš Svete, 160 – 161. Ljubljana: FDV.
51. Puš, Robert. 2000. *Informacijsko vojskovanje*. Poljče: Poveljniško štabna šola.
52. Svete, Uroš. 1999. *Informacijsko vojskovanje – opredelitev in koncept.* Diplomsko delo. Ljubljana: FDV.
53. Toffler, Alvin in Heidi Toffler. 1993. *War and Anti War, making sense of today's global chaos*. Boston: Little Brown and Company.
54. Turk, Slavko. 2001. *Vpliv uporabe omrežnega vojskovanja na učinkovitost bojnega delovanja enot in poveljstev*. Poljče: Poveljniško štabna šola.
55. Waltz, Edward. 1998. *Information Warfare – Principles and Operations*. Norwood: Artech House.
56. Žabkar, Anton. 2003. *Marsova dediščina: Temelji vojaških ved*. Ljubljana: FDV.