**UNIVERZA V LJUBLJANI**

**FAKULTETA ZA DRUŽBENE VEDE**

**ERVIN HARTMAN**

# VAROVANJE TAJNIH PODATKOV IN VARNOSTNA KULTURA NA OBRAMBNEM PODROČJU; PROTIOBVEŠČEVALNO – VARNOSTNI VIDIK

**Specialistična delo**

**Mentor: doc. dr. IZTOK PREZELJ**

**LJUBLJANA, 2007**

# KAZALO

# SEZNAM KRATIC

| | |
|---|---|
| CIS | Communication and Information Systems (Informacijski sistem) |
| CBU | Center za bojno usposabljanje |
| CDR | Center za doktrino in razvoj |
| COMINT | Communication Intelligence (obveščevalna dejavnost za nadzor komunikacij) |
| DVSU | Dopolnilno vojaško strokovno usposabljanje |
| DVSIU | Dopolnilno vojaško strokovno izobraževanje in usposabljanje |
| ELINT | Electronic Intelligence (obveščevalna dejavnost za nadzor elektronskih naprav) |
| EU | European Union (Evropska unija) |
| GŠSV | Generalštab Slovenske vojske |
| HUMINT | Human Intelligence (agenturna obveščevalna dejavnost) |
| IMINT | Imaginery Intelligence (slikovna obveščevalna dejavnost) |
| INFOSEC | Information Security (Informacijska varnost) |
| J/G/S-2 | Obveščevalno-varnostni organi Slovenske vojske |
| MO | Ministrstvo za obrambo |
| MORS | Ministrstvo za obrambo Republike Slovenije |
| NATO | North Atlantic Treaty Organisation (Organizacija Severnoatlantske pogodbe) |
| OIzag | Obveščevalno izvidniška zagotovitev |
| OSINT | Open Source Intelligence (obveščevalna dejavnost odprtih virov) |
| OVS | Obveščevalno-varnostna služba |
| OVSIU | Osnovno vojaško strokovno izobraževanje in usposabljanje |
| OVSU | Osnovno vojaško strokovno usposabljanje |
| POZ | Prioritetni obveščevalni zahtevek |
| PSC | Personnel Security Clearance (Varnostno potrdilo) |
| PSSV | Poveljstvo sil Slovenske vojske |
| PŠŠ | Poveljniško štabna šola |
| PV | Protivlomno varovanje |
| ReSNV | Resolucija o strategiji nacionalne varnosti Republike Slovenije |
| RS | Republika Slovenija |

| | |
|---|---|
| SIGINT | Signal Intelligence (signalna obveščevalna dejavnost) |
| SV | Slovenska vojska |
| TECHINT | Technical Intelligence (tehnična obveščevalna dejavnost) |
| TELINT | Telemetric Intelligence (obveščevalna dejavnost za nadzor telemetrijskih dejavnosti) |
| TP | Tajni podatek |
| TV | Taktična vaja |
| TVSU | Temeljno vojaško strokovno usposabljanje |
| UE | Učne enota |
| UVTP | Urad za varovanje tajnih podatkov |
| VIU | Vojaško izobraževanje in usposabljanje |
| VO | Varnostno območje |
| VOD | Vojaška obveščevalna dejavnost |
| VOMO | Varnostni organ Ministrstva za obrambo |
| ZObr | Zakon o obrambi |
| ZTP | Zakon o tajnih podatkih |

# 1. UVOD

Danes živimo v času nenehnih sprememb. Tempo življenja v razvitih družbah je vse hitrejši in vse zahtevnejši. To velja tako za človeka kot za posamezne organizacije. Če hoče organizacija preživeti in se razvijati, morajo vsi zaposleni učinkovito opravljati svoje delo. Vsakdo mora prispevati največ, kar zmore, v skladu s cilji organizacijske enote, ki ji pripada, ter slediti ciljem organizacije. Predpogoj za dobro organizacijo in njeno učinkovitost je aktivnost vseh zaposlenih. Energijo je treba usmerjati v reševanje problemov in ne v odkrivanje in iskanje krivcev zanje. Vse aktivnosti v organizacijski enoti morajo biti usmerjene k jasno začrtani viziji, poslanstvu, strategiji ter doseganju zastavljenih ciljev.

Znanje je v izredno hitro razvijajočem se svetu ključni dejavnik razvoja. Ima veliko razsežnosti, veliko različnih obrazov in oblik. Zapisano je v knjigah, shranjeno je v bazah podatkov sodobnih informacijskih sistemov, v patentih, licencah. V razvojnem smislu pa je potrebno eno samo znanje – tisto, ki ga imajo v glavah ljudje. Razvoj bo tem hitrejši, čim več bo ljudi, ki bodo znali več od svojih prednikov, čim bolje bodo organizirani in razporejeni glede na razvojne cilje. Sedanja in prihodnja tehnološka in tehnična razvitost, razvitost tržnoekonomskih odnosov ter sedanja in prihodnja struktura delovnih procesov opredeljujejo v posamezni organizaciji potrebe in zahteve po določenih kadrih. Kadri so ključni nosilci uresničevanja načrtovanih ciljev, programov dela in razvoja v vsaki organizacije. Vsaka organizacija mora na podlagi ustrezne kadrovsko izobraževalne politike aktivno sodelovati pri razvoju in izobraževanju svojih kadrov.

Javnost dela in pravica dostopa do podatkov in informacij državnih organov je splošno sprejeto načelo v sleherni moderni družbi, obenem pa tudi pogoj in zagotovilo za delovanje teh organov, ki brez zaupanja, sodelovanja in podpore javnosti ne morejo biti učinkoviti. Informacija je zelo širok pojem. Lahko rečemo, da se življenje konča tam, kjer ni več informacij. Prevladuje namreč mnenje, da človeku psihično življenje zelo hitro zamre, če je izoliran od zunanjega sveta.
Organiziranost neke družbe oziroma sistema lahko merimo s stopnjo izmenjave informacij. Nekateri avtorji upravičeno štejejo informacijo kot tretjo prvino univerzuma, poleg materije in energije. Nesporno je, da je informacija danes neločljiva komponenta vsakega

posameznika in družbe in vsaj toliko pomembna kot proizvedene materialne dobrine ali energija.
Človek je od nekdaj ločil zasebno od javnega. Pri zasebnem gre za področja, v katera se drugi naj ne bi vmešavali. Ko gre za javne zadeve, lahko vsak razpravlja o vsem. Prav vmešavanje oziroma nevmešavanje pa je tisto, kar omogoča ohranjanje tajnosti v zasebnosti posameznika, skupine, lahko tudi organizacije ali podjetja. Pojem tajnosti je tesno povezan z obveščevalnimi in varnostnimi službami, ki so namenjene ugotavljanju tajnosti o drugih in varovanju lastnih tajnosti.

Izobraževanje kot družbena dejavnost in dejavnost posameznika je ključnega pomena za razvoj vsake družbe. Danes lahko zaposleni v Slovenski vojski le s stalnim izobraževanjem obvladujejo zahteve, ki so povezane z izpolnjevanjem vsakodnevnih delovnih nalog in nalog v mednarodnem varnostnem okolju. Pomembno je, da si posameznik individualno in organizirano v okviru izobraževalnih oblik, ki jih organizira Ministrstvo za obrambo, pridobiva znanje, spretnosti in navade z zavestjo, da je to zanj posebnega pomena v življenju in pri vsakodnevnemu operativnemu delu, posebej pa je pridobljeno znanje pomembno za varovanje tajnih podatkov in izgrajevanje varnostne kulture.

Slovenija si je z vstopom v zvezo NATO in EU v letu 2004 zagotovila višjo stopnjo kolektivne varnosti in hkrati prevzela nove naloge, ki jih članstvo v omenjenih integracijah zahteva. Sprejem je bil v Sloveniji pogojen s prilagoditvijo zakonodaje na mnogih področjih, med drugim tudi na področju varovanja tajnih podatkov. Zaradi tega je bil sprejet Zakon o varovanju tajnih podatkov, ki opredeljuje dolžnosti organizacij in posameznikov pri varovanju tajnih podatkov.

Na obrambnem področju in v vojaški organizaciji kot nosilcu obrambe države je veliko število zaposlenih. Ti se vsak dan srečujejo z izdelavo, distribucijo in varovanjem tajnih podatkov. Zaradi zahtevnosti normativne zakonodaje je treba zaposlene usposabljati. Pri usposabljanju je treba obnoviti in nadgraditi znanje zaposlenih s področja varovanja tajnih podatkov zaradi spremembe zakonodaje in uveljavljanja standardov, ki jih predpisujeta EU in NATO. Z usposabljanji je treba dvigniti tudi raven varnostne kulture ter na zaposlene vplivati do te mere, da varnost postane del njihove vsakodnevne kulture.

# 2. METODOLOŠKO HIPOTETIČNI OKVIR

## 2.1. Predmet in cilj preučevanja

Predmet preučevanja v specialistični nalogi sta v prvem delu vloga in položaj obveščevalnih služb, katerih temeljna naloga je zagotavljanje informacij in obveščevalnih podatkov organom odločanja posamezne države ter hkrati z izvajanjem protiobveščevalne dejavnosti zaščita tajnih podatkov. Večina avtorjev, ki se ukvarja z omenjeno tematiko, je osredotočena na normativno pravno vlogo obveščevalno-varnostnih služb v sistemih nacionalne varnosti držav, izvaja primerjavo z organiziranostjo služb v sosednjih državah ali se ukvarja z nadzorom nad delovanjem obveščevalno-varnostnih služb. Moje raziskovanje pa bo v prvem delu temeljilo na preučevanju oziroma analizi metod in virov, ki jih obveščevalno-varnostne službe uporabljajo za pridobivanje informacij in obveščevalnih podatkov. Ugotovitve so izhodišča za opredeljevanje možnega vira ogrožanja tajnih podatkov. Pomenijo tudi osnovo ukrepov, ki naj jih izvajajo organi na obrambnem področju v protiobveščevalnem smislu. Metode dela, ki jih uporabljajo obveščevalne službe, morajo poznati zaposleni, ki dostopajo do tajnih podatkov, da se prepreči odtujitev teh podatkov ter onemogočajo vdori obveščevalnih služb v sistem varovanja tajnih podatkov na obrambnem področju in v Slovenski vojski.

Zaradi omenjenega dejstva bo drugi del specialističnega dela poskušal pojasniti vlogo OVS MORS ter obveščevalnega organa Slovenske vojske pri varovanju tajnih podatkov, protiobveščevalni zaščiti ter izgrajevanju varnostne kulture. Pri tem se bom omejil na izvajanje varnostne in protiobveščevalne dejavnosti, ki jo ti organi izvajajo.

V zaključku naloge bom skušal podati ugotovitve ter priporočila, ki v povezavi z izobraževanjem zaposlenih v opisani tematiki na obrambnem področju in v Slovenski vojski lahko bistveno pripomorejo k dvigu varnostne kulture ter ustreznejšemu obravnavanju in zaščiti tajnih podatkov.

Raziskovalna relevantnost predlagane teme v drugem delu izhaja predvsem iz pomanjkanja znanstvenega obravnavanja teme s področja varovanja tajnih podatkov v povezavi z varnostno kulturo. Na področju varovanja tajnih podatkov se je v zadnjih petih letih toliko spremenilo, da praksa stežka sledi tempu dogodkov, znanstvena sfera pa nima dovolj

informacij o dogajanju v zakulisju. Posebno oviro na tem področju predstavlja predvsem pojem tajnosti oziroma določila Zakona o tajnih podatkih, ki preprečujejo vpogled v dejansko stanje.

V specialističnem delu ugotovljena dejstva, ki vplivajo na varnostno kulturo, lahko služijo kot osnova za preoblikovanje programov usposabljanja, ki bi zagotavljali učinkovito varovanje tajnih podatkov ter razvijali in izgrajevali ustrezno varnostno kulturo zaposlenih na obrambnem področju in v SV, ki se z varovanjem podatkov ukvarjajo.

Specialistično delo je zasnovano na javno dostopni literaturi s področja, s katerim se ukvarja. Splošni cilj specialističnega dela je preučiti vlogo protiobveščevalno-varnostne dejavnosti na obrambnem področju in v SV.
Izvedbeni cilji:

- analizirati varnostne standarde varovanja podatkov v Republiki Sloveniji ter izvesti primerjavo z varnostnimi standardi, ki veljajo v zvezi NATO in EU;
- prikazati vpliv varnostne kulture na varovanje tajnih podatkov;
- ugotoviti primernost izobraževanja na področju varovanja tajnih podatkov ter varnostne kulture;
- predlagati model usposabljanja, ki bi zagotavljal učinkovito varovanje tajnih podatkov ter razvijal in izgrajeval ustrezno varnostno kulturo zaposlenih na obrambnem področju.

## 2.2. Hipoteze

Glede na zastavljene cilje bo preizkušena splošna hipoteza, ki se glasi:

**Protiobveščevalno-varnostna dejavnost vpliva na varovanje tajnih podatkov in izgrajevanje varnostne kulture.**

Izvedene hipoteze so:

1. protiobveščevalno-varnostna dejavnost na obrambnem področju se izvaja v skladu z zakonskimi določili;

2. varovanje tajnih podatkov v Republiki Sloveniji je primerljivo z varovanjem tajnih podatkov v Evropski uniji in zvezi NATO;
3. izgrajena varnostna kultura kot del organizacijske kulture poleg tehničnih sredstev varovanja in drugih ukrepov zagotavlja učinkovito varovanje tajnih podatkov;
4. za pravilno ravnanje s tajnimi podatki je treba zaposlene usposabljati, saj se s tem zagotavlja odgovornejše ravnanje z njimi.

## 2.3. Uporabljene metode

Obravnavanje in preučevanje tematike specialističnega dela, varovanje tajnih podatkov in varnostna kultura na obrambnem področju zahtevajo uporabo različnih metod, ki so medsebojno prilagojene in usklajene.

Skozi celotno specialistično delo me je spremljala opisna deskriptivna metoda, ki je uporabljena skupaj s teoretičnimi koncepti (na primer opis dejanskega stanja na podlagi pojmovno teoretičnih izhodišč).

V nalogi je uporabljena tudi analiza virov: primarnih (zakonov, pravilnikov, izvedbenih predpisov), sekundarnih (knjig, člankov, raziskovalnih poročil) in tudi terciarnih (internet, diplomske naloge na podobno tematiko).

Zbiranje podatkov je temeljilo na sistematičnem zbiranju bibliografije (znanstvenih in strokovnih knjig, člankov, publicističnih virov in zakonov, ukazov, direktiv itd.) ter selekciji podatkov in virov na dejansko uporabljeno literaturo v specialističnem delu.

Uporabljene metode:

- uporaba in analiza pisnih in elektronskih virov,
- sekundarna analiza,
- deskriptivna metoda,
- primerjalna metoda, in sicer v delu naloge, kjer je opredeljena zakonodaja varovanja tajnih podatkov,
- lastna praksa, empirični podatki.

## 2.4. Temeljni pojmi

### 2.4.1. Varnost

Varnost v spremenjenem mednarodnem okolju je postala ena izmed temeljnih vrednot posameznika, države in družbe. Vsaka država mora z institucijami, ki se ukvarjajo z zagotavljanjem varnosti, zagotavljati prepoznavo indikatorjev in virov ogrožanja, ki vplivajo na varnost.

Varnost lahko opredelimo kot stanje, v katerem je zagotovljen uravnotežen fizični, duhovni, duševni in gmotni obstoj posameznika in družbene skupnosti v razmerju do drugih posameznikov, družbenih skupnosti in narave (Grizold, 1999: 23). Glede na definicijo, ki jo je opredelil Grizold, je Anžič (2001: 43) varnost opredelil kot imanentno strukturno prvino družbe, ki zajema tako stanje oziroma določeno lastnost stanja kot tudi dejavnost oziroma sistem. Varnost je torej družbena in politična vrednota, ki označuje okvir socialne in politične skupnosti, hkrati pa omogoča obstoj družbene reprodukcije, notranji red in mir, razvoj notranje ureditve ter zagotovitev običajnih procesov diferenciacije in integracije znotraj družbe in države.
Za vzpostavitev ravnovesja varnosti in groženj mora torej država vzpostaviti stanje, v katerem bo s svojimi organi vsem svojim državljanom zagotovila minimalni standard osebne varnosti in varnostne razmere za njihovo delo (Anžič, 1997: 36). Varstvo skupnih in posamičnih vrednot določene države je legalen in legitimen cilj v vseh njegovih pomenih, kot odvračanje nevarnosti, kot prizadevanje za ohranitev vrednot in kot odpravljanje posledic, zagotavljajo pa ga med drugim tudi subjekti varnostnega sistema oziroma varnostnoobveščevalne službe (Anžič, 1999: 5–6).

Varnost lahko na obrambnem področju in v SV opredelimo kot »stanje, ki ga dosežemo, ko so določene informacije, materialna sredstva, osebje, aktivnosti, naprave in oprema zaščiteni pred vohunjenjem, sabotažo, uničenjem in pred terorizmom, kot tudi pred izgubo ali nepooblaščenim razkritjem« (AAP-6, 2002).
Zanimivo definicijo varnosti je opredelil tudi Stajić (2006: 22), ki pravi, da varnost ni samo odsotnost ogrožanja (konflikta), temveč prisotnost pravic, morale in kulture. Mogoče je (teoretično) živeti v sredini brez konfliktov, pravic, ideologije, izobraževanja ter morale, vendar takega stanja ni mogoče opredeliti kot varnega v sodobnem pojmovanju. Da bi lahko rekli, da smo varnejši, ni dovolj odsotnost nekoga ali nečesa, kar nas ogroža, temveč

moramo živeti v družbi, polni pravic, morale in kulture, torej v družbi, ki stalno izboljšuje svoje vrednosti. Varnost moramo torej razumeti kot pogoj obstoja in razvoja (države, družbe, nacije, ljudi in živega sveta na planetu). Pomembna je ugotovitev, da varnost sama po sebi ne ustvarja ničesar (še posebej ne materialnih dobrin), temveč samo omogoča mnogo tega (življenje, svobodo, zdravje itd.) pa tudi ustvarjanje materialnih dobrin.

### 2.4.2. Tajnost

Tajnost se pogosto zmotno razume kot skrivnost. Skrivnost je v njenem prvotnem pomenu nekaj, kar se ne da razumeti, dojeti ali pojasniti. Tajnost torej ni nekaj neznanega, temveč obratno. Pri vsebini tajnosti gre za znane stvari, ki jih njen »posestnik« (ali posameznik, ali institucija ali država) ne sme ali noče narediti dostopne širši javnosti. Tajnost torej pomeni obstoj znanih dejstev o družbenih, varnostnih, obrambnih, gospodarskih in drugih podatkih in informacijah, ki so posamezniku ali instituciji zaupani v uporabo in varovanje. Ti jih zaradi obstoja različnih, velikokrat konfliktnih interesov na zavesten, organiziran in formaliziran način skrivajo pred javnostjo (Anžič v Trbovšek, 2004: 20).

### 2.4.3. Tajni podatek

Tajni podatek je dejstvo ali sredstvo z delovnega področja organa, ki se nanaša na javno varnost, obrambo, zunanje zadeve ali obveščevalno in varnostno dejavnost države, ki ga je treba zaradi razlogov, določenih v zakonu, zavarovati pred nepoklicanimi osebami, in ki je v skladu z zakonom določeno in označeno za tajno (ZTP, 2006: 2. člen).

Tajni podatek tuje države je podatek, ki ga je Republiki Sloveniji oziroma njenim organom posredovala tuja država oziroma njen organ ali mednarodna organizacija oziroma njen organ v pričakovanju, da bo ostal tajen, ter podatek, ki je rezultat sodelovanja Republike Slovenije oziroma njenih organov s tujo državo ali mednarodno organizacijo oziroma njihovimi organi in za katerega se dogovori, da mora ostati tajen (ZTP, 2006: 2. člen).

### 2.4.4. Varnost podatkov

Đorđević (1989: 34) trdi, da so za varnost podatkov odgovorni državni organi, ki imajo nalogo, da jih ščitijo, kajti to so z zakoni in drugimi splošnimi akti določeni podatki posebnega državnega interesa.

### 2.4.5. Obveščevalna dejavnost

Obveščevalna dejavnost je proces, ki zaokroža pridobivanje podatkov, zagotavlja analitično obdelavo surovih podatkov ter uporabniku posreduje celovit obveščevalni

izdelek, ki ga lahko uporabi v procesu oblikovanja politike in sprejemanja odločitev (Anžič, 1999: 6).

Šaponja (1999: 9–10) pojem opredeli kot proces, ki zajema zbiranje in analitično obdelavo surovih podatkov in izdela celovit obveščevalni izdelek, ki ga uporabnik potrebuje pri oblikovanju in sprejemanju odločitev na državniškem, političnem, gospodarskem in varnostnem področju. Dodati pa je treba, da gre za organiziran proces znotraj specializiranih organizacij, ki so bodisi samostojne bodisi del večjih organizacij.

Obveščevalna dejavnost, pri kateri gre torej za razumsko odzivanje na probleme in izzive domačega in tujega okolja z uporabo splošnih, znanstvenih in posebnih metod, naj pripelje do določenih vedenj in spoznanj ter ima zaradi svojega pomena prednost in kot taka uživa status državne zasebnosti oziroma tajnosti (Anžič, 1999: 6).

### 2.4.6. Obveščevalna služba

Pojem obveščevalna služba ni enotno in jasno opredeljen, saj imajo različni avtorji glede definicije in opredelitve pojma različna stališča.

Obveščevalna služba je organizirana dejavnost ali organizacija – ustanova, ki po zahtevi in namenih vodilnih političnih struktur države zbira, ocenjuje, tolmači, ponuja tajne (zaščitene) podatke in druge podatke o nasprotniku ali sovražniku ter ščiti lastne strukture, interese države pred nasprotnikom in se ukvarja z drugimi dejavnostmi, s katerimi se prispeva k uresničitvi določenih političnih ciljev (Đorđević, 1989: 299–300).

Na splošno bi lahko opredelili ta pojem kot posebno organizacijo države, katere prednostni cilji so zbiranje, analiziranje in ocenjevanje obveščevalnih podatkov in spoznanj o drugih državah, njihovem vojaškem in ekonomskem potencialu, političnem stanju in namerah ter znanstvenih dognanjih. Da bi take podatke lahko zagotovila, njeno delo ne more temeljiti samo na tajno zbranih podatkih. Danes je ena od temeljnih značilnosti dela obveščevalnih služb, da poleg posebnih metod in sredstev dela uporabljajo tudi številne legalne možnosti za pridobivanje podatkov (Purg, 2001: 17).

Obveščevalne službe se razlikujejo glede na:

- področje dela in položaj v sistemu,
- stopnjo ofenzivnosti,
- velikost – od manjših enot do velikih obveščevalnih sistemov,

- usmerjenost – po posameznih področjih dela in po geografskih območjih,
- notranjo organiziranost (Purg, 1999: 10).

Obveščevalna služba ni nujno le državni organ, saj jo razvijajo tudi razna gibanja, stranke, večji gospodarski subjekti, nedržavna združenja, večje organizacije kriminalcev ipd. (Anžič, 1996: 61 in Purg, 1999: 10).

Obveščevalna služba je posebna organizacijska oblika, v kateri se izvaja obveščevalna dejavnost v tujini oziroma v zvezi s tujino. Obveščevalne službe delujejo praktično na vseh področjih, po naravi so informativne in ne represivne, njihovi uslužbenci pa praviloma nimajo policijskih pooblastil (Šaponja, 1999: 56).
Iz pregleda opredelitve pojma lahko ugotovimo, da posamezni avtorji, ki se bolj poglobljeno ukvarjajo s problematiko obveščevalnih služb, določen problemski sklop bolj izpostavijo, na primer nastanek, cilje, razvoj, zgodovino, način delovanja in drugo, kar bistveno vpliva na celovitost razumevanja obravnavanega pojma (Purg, 1999: 11).

V Sloveniji obveščevalne službe razumemo kot specializirane državne organe in službe, ki se ukvarjajo z zbiranjem, dokumentiranjem in analiziranjem informacij in podatkov o tujini. Opravljajo lahko tudi protiobveščevalne in varnostne dejavnosti, tako da odkrivajo, preprečujejo in preiskujejo dejavnosti tujih organov, skupin, organizacij in posameznikov, ki so uperjene proti obstoju države, varstvu ustavne ureditve, varnosti in drugim državnim interesom, ki zlorabljajo ozemlje za teroristično dejavnost proti tretji državi, kakor tudi varovanje zaupnih podatkov državnih organov (Anžič 1996: 60–61).

### 2.4.7. Varnostna služba

Purg (1995: 35) opredeljuje varnostno službo kot specializirano organizacijo, ki opravlja naloge, s katerimi se uresničuje varnostna funkcija, ali pa kot celoto dejavnosti in ukrepov, s katerimi se država brani pred nasprotnikom. To je služba, ki uporablja obveščevalno dejavnost za izvajanje varnostnih nalog v državi (boj proti organiziranemu kriminalu, terorizmu, nedovoljeni trgovini in proizvodnji mamil, orožja in sredstev za množično uničevanje itd.). Varnostne službe, ki izvajajo obveščevalno dejavnost, so protiobveščevalna služba, služba za varstvo ustavne ureditve in posebni policijski oddelki ali službe.

Po svoji naravi je varnostna služba represivna, uslužbenci pa imajo policijska pooblastila. Lahko se organizira tudi posebna specializirana varnostna služba – na primer za boj proti terorizmu (Šaponja, 1999: 24–29, 58).

Varnostna dejavnost je dejavnost, ki v glavnem temelji na ukrepanjih na podlagi »policijskih« pooblastil, vključno s pravico do uporabe posebnih operativnih metod in sredstev dela. Te pa se razlikujejo od metod in sredstev dela, ki jih uporabljajo obveščevalne službe. Gre torej za to, da varnostne službe s svojo dejavnostjo odkrivajo, preiskujejo, preprečujejo itd., medtem ko obveščevalne službe zbirajo, dokumentirajo in analizirajo informacije in podatke (Anžič, 1997: 43).

### 2.4.8. Protiobveščevalna služba

Pojem protiobveščevalna služba je po vsebini ožji od pojma varnostne službe in pomeni le del njene dejavnosti. Protiobveščevalna služba je specializirana organizacija gibanja ali države, ki odkriva, spremlja in onemogoča delovanje nasprotnikovih obveščevalnih služb, organizira in izvaja zaščito lastnih tajnosti in sistema ter izvaja dezinformiranje nasprotnika (Đorđević, 1989: 201).

Njen poglavitni namen je »preprečiti tujim vohunom, da prodrejo do izvorov informacij (vlada, oborožene sile, varnostni organi), ter skrbi tudi za zaščito visoke tehnologije« (The New Encyclopedia Britannica 1992: 717, v Purg, 1999: 11).

Protiobveščevalna služba je torej služba, ki izvaja (represivno) protiobveščevalno zvrst obveščevalne dejavnosti. Osnovna funkcija je preprečevanje in odkrivanje vsakovrstnega delovanja tujih obveščevalnih služb v državi (izvaja se v tujini). Običajno so te organizirane kot samostojne službe, lahko pa so tudi del služb za varstvo ustavne ureditve. Lahko imajo tudi preiskovalna pooblastila, podobna varnostnim službam, če tako določa notranji pravni red (Šaponja, 1999: 43–46, 58).

Dejavnosti protiobveščevalne službe v okviru odkrivanja, preiskovanja in onemogočanja delovanja tujih obveščevalnih služb so zelo obsežne, saj protiobveščevalna služba odkriva in onemogoča delovanje obveščevalcev in agentov tujih obveščevalnih služb, zbira ustrezno dokazno gradivo in ga izroča sodnim organom, odkriva interese tujih obveščevalnih služb in izvaja ukrepe za onemogočanje delovanja tujih obveščevalnih

služb. V okviru nalog zaščite lastnih tajnosti med drugim načrtuje in izvaja zaščito varnostno občutljivih delovnih mest.

Protiobveščevalne službe so praviloma ločene (tudi prostorsko) od obveščevalnih, od njih se delno razlikujejo glede uporabe metod in sredstev ter imajo drugačno vlogo v varnostnem sistemu (Purg, 1999: 11).

### 2.4.9. Vojaška obveščevalna služba

Vojaška obveščevalna služba je namenjena za podporo odločanja poveljnikov vojaških enot pri izvajanju vojaških operacij. Posamezne zvrsti oboroženih sil imajo specializirane vojaške obveščevalne službe. Podatke pridobivajo od obrambnostrateške službe, z uporabo posebnih izvidniških vojaških enot in s tehničnimi disciplinami na vojaškostrateški, operativni in taktični ravni poveljevanja. Podatke uporabljajo neposredno za odločitve, zbirajo pa jih s specializiranimi vojaškimi enotami ter tehničnimi disciplinami zbiranja podatkov (Šaponja, 1999: 187).

Obrambna (vojaška) obveščevalna služba spremlja in analizira globalne varnostnopolitične trende ter preprečuje strateška presenečenja. Pri tem spremlja različne indikatorje, kot so nakupi nove oborožitvene tehnologije, številčno povečanje sestave tujih oboroženih sil (TOS), večje vojaške vaje, večanje zalog in vojaške proizvodnje, premiki enot v bližini meje, povečanje bojne pripravljenosti TOS ipd. V sklopu tega jo zanimajo oborožene sile (struktura, oborožitev, doktrina ipd.), biografije pomembnih osebnosti, ekonomija, geografija (predvsem vojaški vidiki terena, kot so prehodnost, kanaliziranost zemljišča, rastlinstvo, sestava tal, naseljenost ipd.), podnebje, zunanja in notranja politika tujih držav, znanstvenotehnično področje, populacijski dejavniki, transportne zmožnosti in zdravstvo (Purg, 2002: 15–16).

Vojaška obveščevalna dejavnost Slovenske vojske je celota funkcij, procesov, postopkov in ukrepov posameznikov, enot in poveljstev, s katerimi neprekinjeno in celovito spremljajo, analizirajo in predvidevajo vojaško, vojaškopolitično in varnostno situacijo ter delovanje sovražnika, potencialnega sovražnika ter druge vojaške in varnostne grožnje, da bi poveljnikom in drugim, ki odločajo o uporabi Slovenske vojske, omogočili sprejeti kvalitetne in pravočasne odločitve na vseh ravneh poveljevanja. Del vojaške obveščevalne

dejavnosti je elektronsko izvidovanje, ki se v Slovenski vojski izvaja centralizirano (Vojaška doktrina, 2006: 33).

Vojaško obveščevalno dejavnost na strateški ravni izvajajo Obveščevalno-varnostna služba Ministrstva za obrambo in obveščevalni organi Generalštaba Slovenske vojske. Na operativni ravni izvajajo vojaško obveščevalno dejavnost obveščevalni organi in enote operativnega poveljstva sil, na taktični ravni pa obveščevalni organi poveljstev brigad in bataljonov ter izvidniške enote. Ravni obveščevalne dejavnosti se medsebojno prepletajo in dopolnjujejo. Posamezni organi, ki izvajajo obveščevalno dejavnost Slovenske vojske, jo lahko izvajajo za več ravni ali celo za vse. Med njimi velja načelo sodelovanja in dopolnjevanja (Vojaška doktrina, 2006: 32).

### 2.4.10. Varnostna kultura

Ko govorimo o varnostni kulturi, se nam postavi vprašanje, kaj to sploh je. V tuji literaturi lahko zasledimo pojem organizacijsko varnostna kultura, ki obravnava nove postopke zahodne jedrske industrije, po černobilski jedrski katastrofi.

V domači literaturi se avtorji Ambrož, Ovsenik in Mihalič ukvarjajo s pojmom varnostne kulture pri varovanju podjetij. Večinoma pa je pojem uporabljen v povezavi z varnostjo in zdravjem pri delu, o čemer govori Molan. Varnostna kultura temelji na pričakovanju, da bodo ljudje, če bodo seznanjeni z nevarnostmi, ki jih pri delu lahko doletijo, in postopki za njihovo preprečevanje, te dosledno upoštevali pri svojem delu. Tudi Vojnovič, ki analizira nekatere pomembnejše dogodke v jedrskih elektrarnah po svetu, poudarja pomen varnostne kulture. Ob tem je treba poudariti, da so navedeni avtorji enotnega mnenja, da je dobra ali slaba varnostna kultura opredeljena kot skupek odgovornih in sprejetih vrednot, zavedanja, načinov vedenja vseh, ki vstopajo v posamezen sistem. Torej je opredeljena z značilnostmi delovnega okolja ter vpliva na zaznavo in ravnanje zaposlenih glede pomembnosti, ki jo organizacija namenja varnosti.
Varnostna kultura v idealni zasnovi je odprta kultura, ki temelji na poštenju, zaupanju, komunikaciji, sodelovanju, gospodarnosti, profesionalnosti, enakosti ter spoštovanju osebne varnosti in varnosti organizacije.

Sodobna in prodorna podjetja spodbujajo inovativnost, odprtost in kompetentnost zaposlenih. Uresničevanje take vizije prinaša številna tveganja, med katerimi je vse

očitnejše varnostno tveganje. Odgovor ponuja celovit varnostni sistem, ki namenja poseben poudarek zaščiti znanja in poslovnih tajnosti ter temelji na profesionalni notranji kontroli in reviziji. Varnostna kultura se lahko oblikuje le s spodbujanjem varnostnih interesov zaposlenih.

Varnostna zavest zaposlenih je poleg tehničnih rešitev (zlasti na področju informacijske tehnologije in varovanja) nujni pogoj za zagotavljanje čim boljše varnosti in odličnosti organizacije. Sistemski pristop k oblikovanju varnostne kulture in dvigu varnostne zavesti temelji na komunikaciji, varnostnih procedurah in uresničevanju normativnega okvira (spoštovanje poslovne skrivnosti in s tem povezane pravne norme in posledice). Poleg pravnih in postopkovnih dejavnikov so najpomembnejše gibalo varnostne kulture komunikacija in medosebni odnosi.

Pojem varnostne kulture opredeljuje Resolucija o strategiji nacionalne varnosti kot zadnji, toda ne nepomemben temelj sistema nacionalne varnosti. V resoluciji je opredeljeno: »Za zagotavljanje nacionalne varnosti Republike Slovenije se organizira sistem nacionalne varnosti, ki temelji na pravnih, političnih, gospodarskih, materialnih, socialnozdravstvenih, informacijskih, infrastrukturnih, znanstvenih, izobraževalnih in drugih zmogljivostih države. Pri tem se ne zanemarja pomena razvitosti varnostne kulture v družbi.«

Opredeljuje jo kot varnostno kulturo državljanov, posebej tistih na vodilnih in vodstvenih položajih, ter pojasnjuje, da stopnja njene razvitosti vpliva na učinkovitost delovanja sistema nacionalne varnosti in njegov razvoj (ReSNV, 2001).

Varnostno kulturo (bezbednosna kultura) Đorđević (1989: 31–32) opredeljuje kot del splošne kulture posameznika, določenega okolja ali družbe. To so spoznanja s področja varnosti (osnovne vrednote in pridobitve, ki so objekt napada in zaščite, metode in oblike ter tudi nosilci ogrožanja), ki pomagajo posamezniku, okolju in družbi, da prepoznajo metode, oblike ter nosilce takega delovanja, ne glede na to, kje in kako se kažejo. Višanje varnostne kulture se doseže z izpopolnjevanjem in varnostnim usposabljanjem ljudi. Z bogatenjem spoznanj o oblikah, metodah in nosilcih ogrožajočega delovanja se posamezniki, okolje in družba ter najširši sloji države usposobijo za neposredno in konkretno zoperstavljanje.

V širše pojmovanje varnostne kulture bi lahko umestili vprašanja, kot so, v kakšni vlogi se vidijo posamezniki znotraj sistema nacionalne varnosti, kakšen je njihov odnos do vojaškega poklica, Slovenske vojske in mirovnih gibanj, ali so pripravljeni sodelovati z

obveščevalno-varnostnimi službami, kako bi se vedli ob oboroženi agresiji na Slovenijo ipd. (Grizold, 1998: 125–130).

Z varnostno kulturo so tesno povezani tudi vrednote in stališča posameznika do najpomembnejših vprašanj nacionalne varnosti. Varnostna kultura v ožjem pomenu posega na področje organizacijske oziroma politične kulture, je njun del in je tesno povezana z verodostojnostjo, lojalnostjo, pripadnostjo, varovanjem tajnosti ter zanesljivostjo (Črnčec, 2003c: 20).

»Varnostna kultura je aktiven odnos človeka do zaščite in varovanja osebnih in zaupnih podatkov, ki zajema celotno znanje o zaščiti in varovanju in se manifestira z zavestnim vedenjem v konkretni situaciji. Ne gre le za vedenje, ampak za vsebino, globlje motive in vzroke. Osnovni motiv je potreba po zaščiti, katere vzrok je ogroženost vrednot.« (Košmrlj, 1982)

Glede na definicije lahko varnostno kulturo na obrambnem področju in v SV povežemo z varovanjem tajnih podatkov oziroma z doslednim izvajanjem vseh postopkov, ki so namenjeni varovanju podatkov, prostorov in objektov, kjer se tajni podatki hranijo, kakor tudi zaščiti zaposlenih, ki se srečujejo z izdelavo, uporabo ter varovanjem. Torej je zaradi tega lahko logično nadaljevanje tajnosti, ki posameznika sili k spoštovanju vseh pravil in postopkov, ki so namenjeni varovanju tajnosti, hkrati pa mora biti usposobljen zaznati poskuse ogrožanja ter znati izvajati ukrepe za preprečevanje groženj.

Zaposleni na obrambnem področju in v SV se pri vsakodnevnem operativnem delu srečujejo z izdelavo, obravnavanjem, varovanjem, izvajanjem predpisanih ukrepov, torej tudi z varnostno kulturo, ki je temeljni predpogoj, da določeni podatki ostanejo prikriti pred nepooblaščenim dostopom in pred tujimi obveščevalnimi službami.

### 2.4.11. Izobraževanje, usposabljanje, vzgoja

**Izobraževanje** v najožjem pomenu besede pomeni zgolj pridobivanje znanj. Toda izobraževanje vsebuje tudi vzgojno komponento. Vsako usposabljanje pa vključuje tudi izobraževanje (v smislu pridobivanja znanj). V nadaljevanju imamo s pojmom izobraževanje v mislih dolgotrajen in načrten proces razvijanja posameznikovih znanj, spretnosti in navad, ki poteka v šolah, drugih izobraževalnih ustanovah pa tudi zunaj njih (Ferjan, 1999: 10).

**Usposabljanje** je proces razvijanja spretnosti in sposobnosti, ki jih človek potrebuje za opravljanje konkretnega dela (Ferjan, 1999: 11).

**Vzgoja** je celovit in dolgotrajen proces graditve in oblikovanja človekove osebnosti, ki poteka vzporedno s procesom izobraževanja, pri čemer se usmerjeno oblikuje osebnost vsakega posameznika ter se prilagaja zahtevam družbenega okolja, katerega vrednote in norme naj bi posameznik sprejel (Ferjan, 1999: 11).

# 3. OBVEŠČEVALNO-VARNOSTNE SLUŽBE

Obveščevalno-varnostne službe so pomemben del političnega delovanja tako v pozitivnem kot v negativnem smislu. Strokovno in zakonito delo teh služb je izredno pomembno za normalno delovanje države, saj prav te službe zagotavljajo potrebne podatke za nemoteno delo vlade na raznih področjih, na varnostnem, zunanjepolitičnem, gospodarskem, ter hkrati ščitijo pomembne podatke, ki naj bi bili ostali javnosti in drugim državam prikriti. Čeprav rezultati in posledice dela teh služb v javnosti največkrat niso vidni, razen ob odkritjih afer, lahko odsotnost obveščevalnih služb predstavlja za vodenje državne politike velik primanjkljaj v odnosu do drugih držav. Posledice njihovega delovanja so žal lahko velikokrat nepredvidljive, protislovne in tudi neobvladljive.

Obveščevalne in varnostne službe obstajajo že tako dolgo, kot obstajajo države. Pa vendar je bilo njihovo delovanje dolga leta zavito v tančico skrivnosti in mistificirano. Razlogov za to je bilo več, odvisni pa so bili največkrat od političnega položaja v posamezni skupnosti. Nekatere obveščevalne službe so s takim delovanjem zagotavljale obstoj določenih političnih nomenklatur na oblasti, druge so imele drugačne razloge. Večini pa je bilo skupno, da so dolga leta delovale brez jasne zakonske podlage v interesu vodilnih političnih struktur, največkrat znotraj državnih meja. In še ena okoliščina je bila odločilna. Še pred ustanovitvijo evropske skupnosti so bile meje bolj ali manj zaprte. Po združitvi Evrope in po padcu berlinskega zidu pa so formalne meje začele padati, s tem pa je začelo rasti tudi čezmejno sodelovanje. Vendar to ni bilo zgolj pozitivno naravnano. Začele so se namreč pojavljati organizirane kriminalne skupine pa tudi organizirane skupine, ki so želele z nasilnimi akcijami doseči svoje cilje, pa kakršni koli so ti že bili (Žirovnik, 2006: 983).

Zagotovo lahko trdimo, da narava in vsebina dela, predvsem pa velika količina raznih podatkov in informacij v povezavi s tajnostjo, ki je osnova dela obveščevalnih služb, predstavlja potencialno veliko moč. Seveda je ta lahko ob neustreznem nadzoru izrabljena tudi v ozke politične namene. Prav zato je bistven parlamentarni nadzor kot najvišja oblika demokratičnega nadzora nad dejavnostjo oziroma delom obveščevalnih služb.

Meja med tajnim in javnim na obveščevalno-varnostnem področju je dobesedno zabrisana, in to namenoma. Obveščevalno-varnostne službe so izredno previdne ne samo pri tajnosti, ampak tudi na splošno. Manj ko se o posamezni obveščevalno-varnostni službi ve ali govori, bolj je učinkovita.

Transparentnost tovrstnih služb bi avtomatsko pomenila njihovo nepotrebnost, ali kot pravi Črnčec, »pojem tajnosti je prežet skozi bistvo delovanja obveščevalno varnostnih služb in brez tajnosti ni obveščevalno varnostnih služb« (Črnčec, 2005: 3, v Anžič, Brožič, 2006: 823).

Prvi zapisi o tako imenovani obveščevalni službi segajo že v 7. stoletje pred našim štetjem, ko so vladarji močnih azijskih in afriških držav pošiljali sle v sosednje države, njihova naloga pa je bila zbiranje podatkov vojaškega in političnega značaja (Brdajev, 1982).
Stoletja se je obveščevalna dejavnost razvijala predvsem za vojaške potrebe, delno tudi za politične oziroma diplomatske. Vladarji, ki so jim bile obveščevalne službe neposredno podrejene, so uporabljali obveščevalne podatke za potrebe bojnih pohodov, pa tudi v kolonialne namene.
Znanstvenotehnični razvoj, različne metode dela in druge zahteve pripeljejo delo v obveščevalnih službah do potrebe po profesionalizaciji. Obveščevalna dejavnost je postopoma postala množična,[1] pa tudi kompleksnejša. Postala je skoraj umetnost, saj se je zanjo treba posebej izobraževati in usposabljati.
Skozi stoletja obstoja obveščevalne dejavnosti je človek kot razumsko bitje razvil različne metode in načine za zbiranje podatkov, njihovo analiziranje in posredovanje v najprimernejši obliki za odločanje, kakor tudi načine zaščite podatkov pred nepooblaščenim dostopanjem. Obveščevalne službe se na prehodu iz 20. v 21. stoletje prilagajajo intenzivnim spremembam na vseh področjih družbenega in političnega življenja ter temu prilagajajo razvoj in organizacijsko strukturo.

V času hladne vojne je vrhunec doživel tako imenovani »klasični« tip obveščevalne službe, katere osnovna naloga je bila pridobivanje in vrednotenje informacij z namenom, da se ugotovijo namere nasprotnika (države) in se s tem zagotovi prednost naročnika (države). Spremenjene družbenopolitične razmere pa so povzročile, da so se obveščevalne službe začele ukvarjati z zbiranjem široke palete informacij z različnih področij. Tako se danes ukvarjajo z analizo procesov, ki bi lahko ogrozili stabilnost celotnega sistema (Tominc, Koren, Sotlar, 2006: 960).
Skrivnost prilagajanja spremembam je v poznavanju trenutnih razmer, predvsem pa dogodkov, ki se bodo šele zgodili. Zaradi novih informacijskih sistemov so postali podatki

[1] Iz vojaške in politične sfere se širi tudi na ekonomsko, znanstvenotehnično in na druga področja.

splošno in hitro dostopni, kar potrjujejo podatki o številu mednarodnih baz podatkov. Večji problem kot pomanjkanje podatkov je postalo njihovo obvladovanje in nacionalna uporaba.

Pred obveščevalne službe oziroma obveščevalne sisteme se postavljajo obsežnejše in zahtevnejše naloge, saj uporabniki od teh služb ne potrebujejo le tajnih podatkov, temveč celovite informacije, ki jim omogočajo pogled v prihodnost (Šaponja, 1999: 180).

Pravočasna in kvalitetna informacija predstavlja pomemben element, ki omogoča prednosti v pogajanjih in pravočasno sprejemanje optimalnih odločitev, ki prinašajo materialne in finančne koristi. Omogoča psihološke in strateške prednosti.

Zakonito, strokovno in učinkovito delo obveščevalno-varnostnih služb temelji na urejeni in jasni zakonodaji, visoko strokovno usposobljenih uslužbencih in vodilnih delavcih ter na učinkovitem nadzoru zakonitosti in strokovnosti njihovega dela (Šaponja, 1999: 3).

Skupaj z razvojem obveščevalnih služb, ki so glede na vire ogrožanja v državah »zaželene«, se pred nosilce oblasti postavljajo vedno nove zahteve glede nadzorstva in zaščite z ustavo pridobljenih pravic, ki državljanom omogočajo varnost na način, da njihove temeljne pravice in svoboščine niso kršene ali ogrožene.

Obveščevalno-varnostne službe so, kljub veliki količini javno dostopnih informacij, še vedno skrite za tančico skrivnega. O njihovi organiziranosti in delovanju govorijo redki verificiranimi viri, pa še ti so praviloma cenzurirani. Glede na pomen obveščevalno-varnostnih služb za državo ter način pridobivanja zanje pomembnih podatkov in informacij veljajo posebni režimi hranjenja in ravnanja z njimi, s čimer se skuša preprečiti možnost odliva podatkov in informacij ter uporaba informacij v smislu zavajanja itd. (Stopar, 2003).

Za celovito razumevanje vloge obveščevalno-varnostnih služb, predvsem v protiobveščevalno-varnostnem smislu, je treba preučevati tuje obveščevalno-varnostne sisteme, kajti le njihovo poznavanje nam omogoča uspešno in učinkovito zaščito pred njihovim delovanjem.

Ko analiziramo relevantne in dostopne podatke o obstoju in delovanju obveščevalnih služb, lahko o njih ugotovimo splošne karakteristike, ki jih opredeljujejo:

- predstavljajo instrument v funkciji realizacije vitalnih interesov nosilcev oblasti,
- imajo predznak tajnosti,
- preventivnost je njihova osnovna funkcija,
- izvajajo obveščevalno in subverzivno dejavnost,

- uporabljajo specifične metode in sredstva,
- pri delu uporabljajo dosežke znanosti in najsodobnejšo tehnologijo ter so
- specializirane in profesionalne (Stajić, 2006: 202).

Avtorji, ki se ukvarjajo s preučevanjem obveščevalnih služb (Purg, Anžič, Šaponja, Črnčec, Stopar, Stajić, Richelson), opredeljujejo osnovne delitve obveščevalnih služb glede na umeščenost v različne državne organe, glede na funkcijo dejavnosti, po imenu, glede na vrsto, položaj v državi, zgodovinska dejstva itd. Zaradi navedenega bom v nadaljevanju opredelil samo nekatere izmed delitev, za katere menim, da so pomembne za celotno razumevanje namena specialističnega dela.

Obveščevalno-varnostne službe lahko delimo na obveščevalne in varnostne, pri čemer obveščevalne službe zbirajo, vrednotijo, obdelujejo in posredujejo zbrane podatke o tujini z namenom zagotavljanja zunanje varnosti države in njenih interesov. Varnostne službe pa so pristojne za izvajanje dejavnosti s področja varovanja ustavne ureditve, boja proti tujim obveščevalno-varnostnim službam,[2] preprečevanja dejavnosti ekstremnih in terorističnih organizacij, ilegalne trgovine z orožjem, z radioaktivnimi snovmi, jedrsko tehnologijo, drogami in belim blagom, begunske problematike in drugih področij, ki lahko vplivajo na zagotavljanje notranje varnosti države in njenih interesov. Lahko rečemo, da so varnostne službe pristojne za preprečevanje, preiskovanje in odpravljanje določenih oblik ogrožanja države in njenih interesov. Pri tem velja omeniti tudi trditev, da je protiobveščevalna služba ožji pojem varnostne službe in je namenjena predvsem za delovanje proti tujim obveščevalno-varnostnim službam. Protiobveščevalne službe lahko delimo na civilne in obrambne, pri čemer so obrambne protiobveščevalne službe pristojne le za izvajanje dejavnosti znotraj obrambno vojaškega sistema.

Naslednja delitev je lahko na civilne in obrambne obveščevalne službe. Bistvena razlika med njimi je področje delovanja. Civilne obveščevalne službe zbirajo podatke s področja gospodarstva, financ, znanosti in tehnologije, politike ter mednarodnih odnosov. Obrambne obveščevalne službe pa izvajajo dejavnosti na obrambno vojaškem področju. V

[2] Boj proti tujim obveščevalno-varnostnim službam oziroma protiobveščevalno dejavnost izvajajo protiobveščevalne službe (The New Encyclopedia Britannica, 15th Edition, 1989, str. 717–723), ki zbirajo podatke in delujejo z namenom varovanja lastnih podatkov in obveščevalnih operacij pred drugimi. Njihov namen je preprečevanje dostopa do zaupnih podatkov v državni upravi, obrambnem sistemu in obveščevalno-varnostnih službah. Prav tako protiobveščevalne službe varujejo domače dosežke pri razvoju visoke tehnologije, preprečujejo terorizem in mednarodno trgovino z drogami, orožjem, belim blagom in drugim.

to skupino štejemo vse tiste obveščevalne službe, ki zbirajo, vrednotijo, obdelujejo in posredujejo zbrane podatke in informacije za potrebe obrambno vojaškega resorja. Ožji pojem od obrambne obveščevalne službe je vojaška obveščevalna služba,[3] ki na specifičen način zbira podatke in informacije, jih vrednoti, obdeluje in posreduje za potrebe izvajanja vojaških dejavnosti doma in v tujini.

Ne glede na področje dela, lahko obveščevalno-varnostne službe delimo na centralne in resorne. Slednje se nahajajo v okviru posameznega resorja. Praviloma gre za posamezna ministrstva. Centralne obveščevalno-varnostne službe pa so neposredno podrejene eni izmed vej oblasti. Praviloma je to izvršna veja (Stopar, 2003: 54–56).

Obveščevalne službe s svojim delom pripomorejo k uspešnemu delovanju državnega aparata ne samo na zunanjem, temveč tudi na notranjem področju. Z zagotavljanjem relevantnih obveščevalnih podatkov političnega, vojaškega in ekonomskega področja tujih držav državnemu vodstvu omogočajo vodenje zunanje politike z namenom usklajevanja mednarodnih odnosov in zvez. Pravočasni podatki oziroma obvestila o stanju in

[3] Vojaška obveščevalna služba (Đorđević, O.: 1985, str. 40–42) deluje v okviru in za potrebe oboroženih sil. Njena naloga je zbiranje podatkov o nasprotnikovih vojaških silah, zemljišču in virih moči. Nahaja se v sestavi generalštaba ali ministrstva za obrambo. Po namenu, dometu in širini preučevanja vojaške problematike se deli na strateške in operativno-taktične vojaške obveščevalne službe.

Strateška vojaška obveščevalna služba zbira podatke, ki so potrebni za izdelavo vojnih načrtov ter vodenja in poveljevanja v posameznih etapah vojskovanja, za potrebe državnega vodstva in vrhovnega poveljstva. Zbirajo se podatki o:

- vojni doktrini in konceptu uporabe oboroženih sil (vojni in mobilizacijski načrti, cilji, naloge in smeri uporabe glavnih sil, uporaba strateških oborožitvenih sistemov in drugo);
- organiziranosti oboroženih sil v zvrsti, rodove in službe, formacijski organiziranosti, oborožitvi in opremi, izurjenosti vojakov in poveljnikov, njihovih vojnih izkušnjah, sistemu vodenja in poveljevanja in drugem;
- resursih, ki jih imajo oborožene sile na razpolago (kadrovskih, materialnih, tehničnih, finančnih, zdravstvenih in drugih potencialih);
- razvitosti znanstvenih disciplin;
- razvitosti vojaške namenske industrije;
- geografskih in topografskih značilnostih (konfiguraciji zemljišča, podnebju, vegetaciji, komunikacijah, naravnih in umetnih ovirah ter drugem).

Operativno-taktična vojaška obveščevalna služba zbira podatke z uporabo izvidniških in brezpilotnih letal, posebnih enot, s posebnimi tehničnimi sredstvi, z zasliševanjem dezerterjev, vojnih ujetnikov in drugih. Na tak način zbrani podatki so potrebni za operativno vodenje in poveljevanje lastnim enotam proti nasprotniku. Zbirajo pa se podatki o:

- načrtih in namerah nasprotnika;
- formacijski sestavi, opremljenosti, usposobljenosti in koncentraciji nasprotnikov sil;
- območjih koncentracije oklepnih ter artilerijsko raketnih enot in možnih smereh njihove uporabe;
- sistemu zvez ter razporedu osnovnih in rezervnih poveljniških mest;
- obrambnih pasovih;
- razporedu posebnih enot in zaledja;
- letališčih in letalstvu na njih in drugem.

Glede na to, da poveljnik na bojišču ne potrebuje le podatkov o trenutnem dogajanju v njegovi neposredni soseščini, temveč tudi podatke strateškega značaja, vse težje ločujemo med strateško in operativno-taktično obveščevalno dejavnostjo na vojaškem področju.

razpoloženju v lastni državi pa državnemu vodstvu zagotavljajo učinkovitejše angažiranje pri reševanju in odpravljanju notranjih nasprotij (Stajić, 2006: 202).

Glede na navedeno lahko zaključim, da bodo obveščevalne, protiobveščevalne ter varnostne službe tudi v prihodnosti potrebne in zaželene, saj jih lahko uvrščamo med bistvene elemente zagotavljanja varnosti države. Njihova vloga se s koncem hladne vojne ni zmanjšala, nasprotno, njihove naloge so se glede na nove vrste ogrožanja celo razširile. S pojavom novih nevojaških virov ogrožanja bodo te službe najverjetneje nekoliko prilagodile tudi metode dela.
Zavedati se je torej treba, da obveščevalno-varnostne službe poleg zbiranja podatkov in njihovega analiziranja opravljajo tudi povsem konkretne naloge. Vrhunec dejavnosti neke obveščevalno-varnostne službe bo tedaj, ko o nasprotniku ne bo sposobna le zbirati kvalitetne podatke, temveč bo na nasprotnika lahko tudi vplivala oziroma ga usmerjala (Krunić, 1996: 152).

## 3.1. Metode dela protiobveščevalno-varnostnih služb

Da bi lahko opredeljevali metode dela obveščevalnih, protiobveščevalnih ter varnostnih služb, je treba najprej opredeliti tako splošno kakor tudi ožjo definicijo metode dela obveščevalno-varnostnih služb. Temeljna značilnost obveščevalno-varnostnih služb je, da praviloma izvajajo vse tri zvrsti obveščevalnih dejavnosti: obveščevalno, protiobveščevalno in varnostno. Šaponja (1999) posamezne zvrsti opredeljuje takole:

- **obveščevalna zvrst** je obveščevalna dejavnost, katere namen je pridobivanje podatkov v tujini z različnih področij;
- **protiobveščevalna zvrst** je obveščevalna dejavnost, ki je usmerjena na odkrivanje, spremljanje, onemogočanje in v nekaterih primerih tudi preiskovanje kaznivega dejanja vohunstva, ki ga izvajajo tuje obveščevalne službe. Ne gre le za odkrivanje vohunske dejavnosti, ampak tudi za spremljanje dejavnosti tujih obveščevalnih služb, kadar ne izvajajo vohunske dejavnosti;
- **varnostna zvrst** je obveščevalna dejavnost, ki je usmerjena proti organiziranemu kriminalu, terorizmu, nedovoljeni trgovini in proizvodnji mamil, orožja in sredstev za množično uničevanje. Namenjena je tudi za odkrivanje in preprečevanje raznih oblik

političnega ekstremizma oziroma radikalizma, katerega cilj je rušenje ustavne ureditve, ter varovanje pred njimi.

Glede na navedeno je mogoče zaključiti, da je temeljna metoda dela vseh obveščevalnih služb, torej tudi protiobveščevalnih in varnostnih, obveščevalna dejavnost. Ko pa govorimo o zvrsti obveščevalne dejavnosti, se pojavljajo razlike v pooblastilih, ki jih imajo delavci posameznih služb, ter v naravi dela. Pri opredelitvi narave dela lahko za obveščevalne službe trdimo, da so informativne, medtem ko so protiobveščevalne in varnostne tako preventivne kakor tudi represivne. Metode dela, ki jih bom opredelil v nadaljevanju, so torej tiste, ki jih uporabljajo obveščevalno-varnostne službe ne glede na zvrst obveščevalne dejavnosti, ki jo izvajajo, zaradi tega bom tudi v nadaljevanju uporabljal le termin obveščevalno-varnostne službe.

Vse obveščevalne in varnostne službe uporabljajo poleg drugih tudi posebne metode in sredstva pri izvajanju svojih dejavnosti. Če bi jih prenehale uporabljati, bi izgubile tudi specifičen položaj, ki ga imajo (Đorđević, 1980).

Metoda je skupek specifičnih postopkov, s katerimi se zbirajo in varujejo določeni podatki. Obveščevalno-varnostna služba jih pred vsako operacijo posebej odreja. Opredeljuje se za tisto metodo oziroma skupek del in postopkov, ki so najprimernejši za predmet preučevanja. Pri njenem izboru morajo biti prisotna načela racionalnosti, ekonomičnosti itd. Pravilen izbor je najpogosteje odločujoč tudi pri učinkovitosti.

**Tajnost** je pomembno obeležje obveščevalne službe in se nanaša na vse, kar ta izraz vsebuje: obstoj posebne organizacije, zaposlene, posebne dejavnosti (akcije), sredstva in metode delovanja, prostore ipd. Tajnost predstavlja enega glavnih objektivnih razlogov znanstvene neraziskanosti pojma in pomena obveščevalne službe (Purg, 1995: 34).

Izbor načina in metode dela je odvisen od naslednjih kriterijev:

- obveščevalnih zahtev države,
- naloge in cilja, ki ga služba mora izvesti,
- politike, ki jo država vodi proti drugi državi,
- časa izvajanja naloge (mir, vojna, izredno stanje),
- ozemlja, kjer se naloga izvaja (lastno, sovražnikovo, zaveznikovo ozemlje),
- razpoložljivih sil in sredstev službe ter
- realnih zmožnosti službe, da nalogo izvede.

Načini in metode dela obveščevalnih služb predstavljajo največjo tajnost in so kot take zaščitene. Če se načini in metode dela posameznih služb odkrijejo, se s tem največkrat odkriva delovanje celotne službe (Stajić, 2006: 217).

Obveščevalne službe uporabljajo vse metode, ki jih imajo v svojem znanstvenoraziskovalnem inštrumentariju vse družboslovne vede, poleg teh pa še določene »posebne« metode dela in posebna sredstva, kar jim tudi daje pomen specifične organizacije oziroma dejavnosti. Metode dela vseh obveščevalnih služb so načeloma enake, razlika je le v obsegu te dejavnosti ter v tem, kdo jih izvaja in proti komu. V osnovi lahko vse metode dela obveščevalnih služb razdelimo na dve skupini:

- legalne in
- ilegalne, ali kakor se pogosto imenujejo, tajne ali klasične metode dela[4] (Krunić, 1996: 144).

Poleg enake razdelitve, ki jo opredeljuje Krunić, razlikuje Stajić (2006: 217) na podlagi sredstev, s pomočjo katerih se dejavnost izvaja, naslednje metode dela: agenturno metodo, metodo uporabe prislušnih naprav ter metodo elektronskega izvidništva. Če pa izvedemo primerjavo glede vsebine dela obveščevalnih služb, lahko pogojno govorimo o dveh skupinah metod, in sicer o:

- metodi zbiranja podatkov in
- metodi izvajanja prevrata oziroma subverzivnega delovanja (Stajić, 2006: 217).

Obveščevalno-varnostne službe pri zbiranju podatkov le redko uporabljajo eno samo metodo ali en sam vir zbiranja podatkov in informacij. Pri uporabi več metod hkrati govorimo o obliki operativnega dela (Žunec, Domišljanović, 2000: 47). Ob tem Šaponja (1999: 8) dodaja, da operativne discipline sestavljajo skupino različnih metod, načinov, postopkov ter za obveščevalno-varnostne in varnostne službe specifičnih opravil, ki jih opravljajo delavci teh služb. Glede na to, da te discipline zahtevajo praktično, fizično delo na terenu, govorimo o operativnem delu in delovanju.

Zbiranje podatkov in informacij z uporabo metod in sredstev dela je tradicionalno najpomembnejša funkcija obveščevalno-varnostne službe. Zbiranje podatkov je

[4] Đorđević uvaja tudi tretjo vmesno skupino in jo imenuje pollegalna ali prikrita metoda.

neprekinjen in zahteven proces, ki je odvisen od iniciative, izkušenj in veščine organa, ki se na tem delu angažira. Novo prispeli podatki se imenujejo surovi podatki, ker v procesu še niso dodelani in niso dobili kvalifikacije vsebine ter osnove za uporabo. Poleg podatkov, ki jih pridobi obveščevalno-varnostna služba sama, so tukaj še podatki drugih institucij, gibanj ali držav (Stopar, 2003: 37).

### 3.1.1. Metode zbiranja podatkov iz javnih virov

Pod pojmom zbiranja podatkov iz javnih virov lahko razumemo legalne metode, kakor jih opredeljuje Krunić, torej je to dejavnost obveščevalno-varnostnih služb, da za zbiranje informacij izkoriščajo »odprte« vire informacij.

V dobi informacijske tehnologije je na voljo veliko število informacij, ki jih državni organi, podjetja in druge institucije namenoma objavljajo, saj je to eden izmed načinov ponujanja izdelkov, reklamiranja dejavnosti, ustvarjanja dobrega imena oziroma dezinformiranja (Schmid, 2001). V večini evropskih držav obveščevalna skupnost pri svojem delu uporablja metode zbiranja podatkov iz javnih virov, kakor tudi pridobivanje podatkov s posebnimi metodami. Po ocenah pridobijo obveščevalno-varnostne službe z javnimi metodami 60 odstotkov zahtevanih podatkov, s tajnimi metodami 20 odstotkov ter z mednarodnim sodelovanjem in prek drugih državnih organov države 20 odstotkov (Schmid, 2001).

Sredstva množičnega informiranja[5] objavljajo veliko količino informacij. Po nekaterih tujih virih naj bi obveščevalne službe zbrale na tak način tudi do 85 odstotkov vseh podatkov, vendar pa so za njihovo obdelavo potrebni izobraženi kadri, saj je treba izločati dejstva ali posamezne podatke iz informacij ter jih ustrezno obdelati. Osebe, ki se ukvarjajo s takim načinom zbiranja podatkov, so lahko agenti obveščevalci, razni analitiki, zunanji sodelavci in drugi (Hartman, 2006).
Podobno opredeljuje tudi Žirovnik (2001: 74), ko povzema teze mnogih teoretikov, ki skušajo dokazati, da je 80 odstotkov obveščevalnih podatkov pridobljenih iz javnih virov, ter se zaradi tega sprašujejo o smiselnosti obstoja obveščevalnih služb. Vendar pa obveščevalne in varnostne službe pridobijo tudi podatke, ki v javnih virih niso objavljeni in tudi nikoli ne bodo, zato je obstoj obveščevalnih služb smiseln.

[5] Radio, televizija, časopisi, revije, internet …

V sredstvih množičnega informiranja se težje najde popoln podatek, pogosteje gre le za posamezna dejstva ali dele podatkov, ki se lahko uporabijo v dva namena:

- dopolnjujejo se spoznanja, ki jih je obveščevalna služba dobila z drugimi metodami,
- pozornost se lahko usmeri tudi na širši obveščevalni in varnostni problem ter se tako spodbudi uporaba drugih metod in sredstev zaradi potrjevanja že znanega, ali pa podrobnejšega preučevanja določenega problema (Stopar, 2000).

Obveščevalno-varnostne službe sistematično spremljajo delo sredstev javnega obveščanja, kakor tudi tisto založniško dejavnost, ki bi lahko objavila pomembne informacije. Z analitičnim delom prihajajo do spoznanj o splošnem stanju vseh zvrsti življenja določene države.

Nadaljevanje sistematičnega dela služb so naslednji načini zbiranja informacij:

- pošiljanje organov na vojaške parade, vaje, kjer je dovoljena prisotnost javnosti, saj je tako mogoče pridobiti vpogled v bojne zmožnosti določene države (usposobljenost, opremljenost),
- prisotnost na sprejemih, slovesnostih, kjer obveščevalci navezujejo stike s številnimi tujimi predstavniki ter v pogovorih, razpravah in s postavljanjem vprašanj prihajajo do pomembnih informacij, ter
- medsebojni stiki v odnosih med državami (pogodbene obveznosti, obiski delegacij, izobraževanje …), ki obveščevalnim službam omogočajo zbiranje določenih informacij o državi gostiteljici (Stajić, 2006: 218).

Podobno opredeljuje delo obveščevalno-varnostnih služb tudi Krunić (1996: 145), saj med legalne metode prišteva analizo podatkov iz javnih virov, zbiranje podatkov prek diplomatsko-konzularnih in drugih predstavništev, spraševanje/zasliševanje beguncev, vojnih ujetnikov, dezerterjev, prebežnikov ipd. Mnogi avtorji v to kategorijo prištevajo tudi izvidniško dejavnost. Ta se lahko izvaja z vojaškimi enotami, z letali (s piloti ali brez njih), s sateliti, lahko gre za elektronsko izvidništvo (radarsko, optoelektronsko, radioizvidništvo, ki vključuje radioprisluškovanje in radiogonimetriranje). Krunić meni, da nekaterih vrst izvidništva ne moremo šteti med legalne metode (izvidništvo z letali).

Tudi metoda neposrednega opazovanja je na meji med legalnim in ilegalnim. Uporabljajo jo vojaški obveščevalci, ki se pošiljajo v določene države, in »politični prijatelji«. Z

metodo neposrednega opazovanja se opazujejo pomembni objekti in smeri ter se tako zbirajo ali preverjajo zbrani pomembni podatki. Pri tem se običajno uporabljajo sredstva za dokumentiranje (fotoaparat, kamera …). Gibanje v bližini objektov, kjer je gibanje omejeno, običajno ni prepovedano, vendar lahko hitro pride do prekoračitve pooblastil (snemanje, skiciranje, pogovori z zaposlenimi), kar je v vseh državah z zakonom prepovedano (Stajić, 2006: 219).

Z razvojem družbe se širi tudi obseg potrebnih podatkov za vodenje države. Obveščevalno-varnostne službe vse pogosteje sodelujejo z znanstvenimi, raziskovalnimi in drugimi institucijami. Sodelovanje je v informacijski dobi več kot potrebno, zaradi hitrega znanstvenega in tehničnega razvoja na eni strani ter zaradi dejstva, da obveščevalno-varnostne službe ne bodo nikoli razpolagale z neomejenimi kadrovskimi, finančnimi, tehničnimi in drugimi viri, s katerimi bi lahko zagotavljale informacije in podatke za učinkovito vodenje države. Zaradi slednjega lahko znanstvene, raziskovalne in druge institucije za potrebe obveščevalno-varnostnih služb izvajajo določene dejavnosti na področju zbiranja, vrednotenja in obdelave javno dostopnih podatkov.

Pri legalnem zbiranju podatkov velja omeniti še vlogo diplomatsko-konzularnih predstavništev, saj izvajajo tako imenovano »obveščanje«, ki ga je mogoče opredeliti v najširšem smislu kot dejavnost, katere cilj je izvedeti informacije ali zbrati podatke o nečem ali nekom ali posredovati obvestila (podatke, informacije in dokumente) nekomu. Ko govorimo o obveščanju kot diplomatski funkciji, pod tem pojmom razumemo dejavnost, ki je usmerjena na pridobivanje obvestil o pogojih in razvoju dogodkov v državi, kjer je diplomatski predstavnik akreditiran (Stajić, 2006: 298).

Diplomati zbirajo podatke v skladu z Dunajsko konvencijo o diplomatskih odnosih, v kateri je opredeljeno, da je dovoljeno akreditiranim diplomatskim predstavništvom z vsemi legalnimi sredstvi zbirati podatke o državi gostiteljici (Stopar, 2000).
Vojaški atašeji kot člani diplomatsko-konzularnega predstavništva so praviloma uslužbenci vojaških obveščevalnih služb, ki organizirajo vojaški obveščevalni center v državi gostiteljici. Njihov osnovni način pridobivanja podatkov temelji na uporabi legalnih metod. Stajić (2006: 306) opredeljuje, da vojaški atašeji pri izvajanju svoje dejavnosti lahko izjemoma uporabljajo tudi nelegalne metode zbiranja obveščevalnih podatkov, in sicer za zbiranje podatkov, ki jih ni mogoče zbrati z legalnimi metodami. Ti podatki so:

opremljenost in izurjenost, moralno stanje, lokacije pomembnih vojaških objektov, način poveljevanja, mobilizacijska pripravljenost ter podatki, ki so pomembni za obrambo države.
Zaradi navedenega organizirajo agenturno mrežo ter za izvajanje svoje dejavnosti uporabljajo vse kategorije oseb, ne glede na državljanstvo in pobudo sodelovanja.

Podatke lahko z legalnimi metodami zbiramo v lastni državi (na podlagi suverenih pravic) ali v tujini (brez kršenja norm mednarodnega prava). Ti »obveščevalci« ne morejo biti obsojeni za vohunjenje, ker ne počnejo ničesar protipravnega. Tako pridobljeni podatki sami po sebi nimajo obveščevalnega pomena, vendar lahko obveščevalna služba z njihovo obdelavo oziroma analizo naknadno pride do zelo kakovostnih informacij (Krunić, 1996: 145).

### 3.1.2. Metode skrivnega (tajnega) zbiranja podatkov

Te metode so pri delu obveščevalno-varnostnih služb najpomembnejše. Obveščevalno-varnostni službi dajejo poseben pomen in vlogo. Obstoj in uporaba teh metod sta pogojena s pojavom tajnosti, ki jo lahko odkrijemo ali zaščitimo le na ta način (Krunić, 1996: 145).
V to kategorijo bi lahko šteli naslednje metode:

- tajno sodelovanje ali agenturno metodo,
- infiltracijo pripadnika obveščevalne službe v ciljno okolje,
- tajno sledenje in opazovanje,
- tajni odkup predmetov,
- tajno preiskavo,
- tajno uporabo operativno tehničnih sredstev (kontrola telefona in drugih komunikacijskih sredstev, prisluškovanje v prostoru, kontrola pisemskih in drugih pošiljk, slikovno dokumentiranje oseb in stvari, protiprislušni pregled in tehnična zaščita) (Krunić, 1996: 146).

Drugi avtorji, med njimi Brejc (1994: 72–73), med metode skrivnega (tajnega) zbiranja podatkov uvrščajo informativni pogovor, sodelavce, preverjanje oseb, sledenje, dvojne kombinacije, dezinformacije, tajno preiskavo prostora, tajno avdio- in videosnemanje, nadzor komunikacijskih sredstev in podobnega, protiprislušne preglede ter tehnično zaščito objektov.

Zaradi mnenj nekaterih avtorjev, da je mogoče na legalen način in s pomočjo javnih virov zbrati potrebne podatke, bom skušal opredeliti nekatere prednosti agenturne metode oziroma tajnega sodelovanja kot oblike »obrti« obveščevalno-varnostnih služb.
Tajno sodelovanje je ena najstarejših oblik tajnega pridobivanja podatkov. Staro je toliko, kot so stare obveščevalne službe. Način dela se v vseh letih ni spremenil, delo s tajnim sodelavcem pa ostaja še vedno najbolj varovana skrivnost posameznih operativcev. Brezpogojno mora biti zagotovljena tajnost sodelovanja, ki jo obveščevalne in varnostne službe zagotavljajo v različnih obsegih, odvisna pa je tudi od tega, v katero varnostno zanimivo okolje je tajni sodelavec usmerjen (Žirovnik, 2001: 75).

Obveščevalne in varnostne službe menijo, da se najboljša informacija o objektu interesa pridobi s pomočjo zaposlenega, ki v njem dela. Torej je potreben agent, poznavalec situacije, ki lahko to situacijo ustno ali na drugi način prenese operativcu (profesionalnemu pripadniku obveščevalne službe). V prid agenturne metode je naslednje:

- podatkov o volji, nameri in načrtih nasprotnika ni mogoče pridobiti, čeprav uporabljamo najsodobnejša tehnična sredstva. Z uporabo prislušnih naprav je mogoče pridobiti podatke o nameri nasprotnika samo nekaj minut pred začetkom izvajanja določene naloge, vendar protiobveščevalne službe pogosto te podatke posredujejo zaradi oblikovanja napačnih odločitev;
- nemogoče je izvajati tudi najenostavnejše specialne operacije brez pomoči državljanov ogrožene države na njenem ozemlju (Stajić, 2006: 219).

Uporaba agentov obveščevalno-varnostnih in varnostnih služb ima prednost direktnega pristopa do želenih informacij, vendar pa je treba navesti tudi pomanjkljivosti. Schmid (2001: 22) navaja naslednje:

- protiobveščevalna dejavnost je vedno koncentrirana na osebe in vodje,
- pri pridobljenih osebah se lahko slabosti, zaradi katerih so bile pridobljene, izkažejo kot bumerang,
- ljudje običajno delajo napake ter zaradi tega postanejo predmet interesa protiobveščevalnih in varnostnih služb.

Tajno sodelovanje obveščevalno-varnostne službe vzpostavljajo z državljani matične države in tujci zaradi zbiranja podatkov in informacij ter izvajanja drugih dejavnosti. Osebo, s katero se vzpostavi tajno sodelovanje, imenujemo sodelavec[6] (Stopar, 2003: 43).

Vedno znova se postavlja vprašanje, kakšni so motivi ljudi, ki privolijo v sodelovanje z obveščevalno-varnostnimi in varnostnimi službami in se torej ukvarjajo z zbiranjem tajnih podatkov.

Motivi so praviloma različni, velja pravilo, da jih je toliko, kot je ljudi. Kljub vsemu pa poznamo nekaj osnovnih motivov, ki so v praksi najpogostejši. Na prvem mestu je patriotizem, ki je zelo aktualen in učinkovit v obdobjih, ko je nacionalna varnost države očitno ogrožena ali je država v vojni. Pogosto nastopa v kombinaciji z drugimi motivi, kot so avanturizem, ideologija, nasprotovanje določenim sovražnim političnim režimom ali posebnim oblikam kriminalitete, kot so droge ali terorizem. Omeniti velja še: maščevanje, občutek ponižanosti, razočaranja in seveda denar (Šaponja, 1999: 20–21).

Podobno opredeljuje motive tudi Stajić (2006: 220) in pravi, da ljudje zaradi patriotizma začnejo tajno sodelovati z obveščevalnimi službami. Patriotizmu sledijo politična in verska ideologija, denar, želja po karieri, avanturizem, ljubezen, želja po maščevanju, sovraštvo itd. Zaradi tega, ker je agent iz sestave potencialne žrtve najboljša investicija, obveščevalne službe izkoriščajo navedene motive za ustvarjanje številčne, raznovrstne, učinkovite in funkcionalne agenture.

Tudi Schmid (2001: 22) opredeljuje razloge, zaradi katerih pridobljene osebe sodelujejo z obveščevalno-varnostnimi službami. Bistveni razlogi so: izsiljevanje, podkupovanje, grožnje, ideologija, čast, nezadovoljstvo, manjvrednost itd.

Sodelavca lahko obveščevalna služba v ciljno okolje vrine, ali pa je ta že tam. V praksi poznajo obveščevalne službe tri glavne osnove za angažiranje in poznejše sodelovanje:

- prostovoljnost (patriotizem, ideologija itd.),
- materialne koristi,
- prisilo (grožnja z uporabo obremenilnega materiala ipd.) (Krunić, 1996: 146–147).

Da bi se izognili polemiki o tem, ali je tajno sodelovanje pomembno, govori teza, da je treba ločiti med obveščevalno in protiobveščevalno službo. Če je značilnost obveščevalne

[6] Agent ali sodelavec je oseba, ki iz določenih razlogov organizirano, neprofesionalno, tajno in za potrebe obveščevalno-varnostne službe neke države zbira v nasprotnikovih strukturah tajne podatke, ki jih nato na tajen način posreduje obveščevalcu. Agenturna ali sodelavska mreža so vsi tajni viri podatkov – sodelavci, ki delajo po navodilih in usmeritvah obveščevalno-varnostne službe neke države (Đorđević, 1989: 4–5).

službe, da lahko z analizo javnih virov pridobi mnogo podatkov, je nesmiselno govoriti, da lahko z isto metodo dosežemo podobne uspehe pri protiobveščevalnem delu. Agenta tuje službe je mogoče odkriti le z uporabo posebnih oblik pridobivanja podatkov, in ena od njih je nedvomno agenturna metoda (Krunić, 1996).

Izkušnje obveščevalno-varnostnih služb ZDA v zadnjem desetletju so pokazale, da bo človek kot vir informacij eden najpomembnejših načinov pridobivanja podatkov in informacij tudi v prihodnje, predvsem ko govorimo o zbiranju varovanih podatkov, do katerih ni mogoče priti z uporabo tehničnih sredstev. Tak primer so ekstremne in teroristične organizacije, katerih delovanje se lahko le deloma spremlja z uporabo tehničnih sredstev. Glavni vir podatkov in informacij bo tako še vedno predstavljal človek, seveda v kombinaciji s tehničnimi sredstvi (Stopar, 2003: 41).
Podobno razmišljajo tudi Tominc, Sotlar in Koren (2006: 961), saj večina služb ugotavlja, da jim kljub množici informacij primanjkuje tistih, ki bi bile pridobljene iz sredin oziroma iz okolja, od koder grožnje dejansko izhajajo, ali pa jih pogosto ocenijo kot nepomembne in jih zavržejo. Ker gre pri novih vrstah ogrožanja za okolja, v katerih se klasične obveščevalne službe ne znajdejo najbolje, morajo vložiti vedno večji napor, da pridobijo uporaben podatek. Edina rešitev, ki bi jim lahko pomagala premagati ta problem, je vrnitev k bistvu »obrti«, k **tajnemu sodelovanju.** To pa pomeni pridobiti tajne sodelavce, ki bi bili v središču ali v neposredni bližini posameznega vira ogrožanja.

## 3.2. Viri obveščevalno-varnostnih služb

V zadnjem desetletju se od obveščevalno-varnostnih služb pričakuje, da bodo naročnike informirale o dogajanju na več področjih, poleg navedenih tudi na področju migracij, ekstremizma in terorizma, ilegalnih trgovin z orožjem, drogami, človeškimi organi in prepovedanimi snovmi[7] (Stopar, 2003: 41).
Obveščevalno-varnostne službe pridobivajo podatke in informacije iz različnih virov.

- Prvi vir informacij so ljudje. HUMINT (human intelligence) vsebuje zbiranje informacij s človeškimi viri, po navadi agenti (vohuni), lahko pa tudi s pomočjo popotnikov, beguncev, vojnih zapornikov ipd. Najučinkovitejši je tam, kjer se informacija ne prenaša elektronsko ali pa je šifrirana in se je ne da dešifrirati v času, v

[7] Sem štejemo npr. radioaktivne snovi.

katerem je še aktualna. HUMINT je še posebej pomemben tam, kjer obveščevalna informacija zahteva poglobljeno interpretacijo ali pa je dvoumna in zato potrebuje oceno notranjega udeleženca. Zaradi hitrega razvoja dogodkov in potrebe po skupnem nastopanju proti virom ogrožanja obveščevalno-varnostne službe vse pogosteje medsebojno sodelujejo tudi zunaj državnih meja ter si izmenjujejo zbrane podatke, informacije in spoznanja (Military and Defence Encyclopedia, 1993: 1280 v Stopar, 2003: 41).

- Drugi vir so različne tehnične naprave. Z razvojem tehnologije za zbiranje podatkov in informacij ter sposobnostjo njihove uporabe na zemeljskem površju, v zraku in vesolju, na vodni gladini in pod njo je ta vir vse večji in pomembnejši. V to skupino štejemo zbiranje podatkov in informacij s pomočjo elektronskih sredstev TECHINT,[8] ki se deli na zbiranje informacij iz signalov elektronske emisije SIGINT[9] in zbiranje slikovnih informacij IMINT.[10] SIGINT se nadalje deli na nadzor komunikacij COMINT,[11] nadzor drugih elektronskih naprav ELINT,[12] nadzor telemetrijskih dejavnosti TELINT[13] ter programe za zaščito signalov SIGSEC.[14] IMINT je najmlajša in verjetno tudi najsodobnejša disciplina za zbiranje podatkov. Zbiranje slikovnih informacij v izvidniške namene je znano že iz obeh svetovnih vojn. Pri današnjem izvidovanju se podatki zbirajo fotografsko PHOTOINT,[15] informacije pa se prikazujejo digitalno, s pomočjo računalnika. Poleg navedenih načinov pa lahko zberemo slikovne informacije tudi z detektorji, ki so občutljivi za valovne dolžine, ki jih oko ne more zaznati. Tovrstno zbiranje je tako imenovano elektrooptično zbiranje informacij ELECTRO-OPTINT.[16] Obstajajo tudi protiukrepi za zaščito (OPSEC) ter metode maskiranja, prikrivanja in zavajanja CC&D.[17] Med druge, bolj specializirane načine tehničnega zbiranja podatkov sodijo zbiranje informacij s pomočjo naprav za odkrivanje akustičnih valov v vodi ACOUSTINT ali ACINT,[18] ki sta namenjeni odkrivanju ladij in podmornic, izdelava zemljevidov, mornariških kart in zbiranje geodetskih informacij

[8] TECHINT je kratica za Technical Intelligence.
[9] SIGIN je kratica za Signal Intelligence.
[10] IMINT je kratica za Imagery Intelligence.
[11] COMINT je kratica za Communication Intelligence.
[12] ELINT je kratica za Electronic Intelligence.
[13] TELINT je kratica za Telemetry Intelligence.
[14] SIGSEC je kratica za Signals Security.
[15] PHOTOINT je kratica za Photographic Intelligence.
[16] ELECTRO-OPTINT je kratica za Electro Optical Intelligence.
[17] CC&D je kratica za Cover, Concealment & Deception Techniques.
[18] ACOUSTINT ali ACINT sta kratici za Acoustical Intelligence.

MC&G,[19] lasersko izvidništvo LASINT,[20] jedrsko izvidništvo NUCINT,[21] ki odkriva posledice radioaktivnega sevanja, radiacijsko izvidništvo RINT,[22] ki meri elektromagnetno energijo, ter zbiranje informacij s pomočjo radarja RADINT[23] (Stopar, 2003: 42).

Tehnične naprave za zbiranje informacij in podatkov so bile razvite predvsem v vojaške namene. Obveščevalne in varnostne službe so v začetku spremljale predvsem vojaške in diplomatske komunikacije. Z razvojem komunikacijske tehnologije, predvsem interneta, ki je bil razvit v vojaške namene, in spremljanja novosti je sčasoma spremljanje komunikacij prerastlo le vojaško in diplomatsko področje. Zaradi novih oblik ogrožanja se je izkazala potreba po spremljanju tudi civilnih komunikacij, ki uporabljajo enaka frekvenčna območja kot prej omenjene.

- Tretji vir so odprti javno dostopni viri OSINT (open sources intelligence). Največji delež obveščevalnih informacij se pridobi iz odprtih virov. Taki viri so vsa sredstva množičnega obveščanja, vzgojno-izobraževalne institucije, internet, publikacije, seminarji, kongresi, simpoziji ipd. Obveščevalna dejavnost odprtih virov je odsev tako imenovane informacijske revolucije, v okviru katere so informacije vseh vrst, tudi občutljive, javno dostopne.

## 3.3. Opredelitev poslanstva Obveščevalno-varnostne službe Ministrstva za obrambo

Nacionalnovarnostni sistem sestavljajo državni organi in službe skupaj z dejavnostmi, za katere so pristojni in jih izvajajo. Namen delovanja nacionalnovarnostnega sistema je preprečevanje, odkrivanje in preiskovanje vseh tistih pojavov, ki bi grobo posegli v temeljne vrednote in mednarodne standarde. Vsak nacionalnovarnostni sistem in nosilci funkcij sistema morajo upoštevati določene specifičnosti sodobne varnosti (Anžič, 1997: 39):

[19] MC&G je kratica za Mapping, Charting & Geodesy Intelligence.
[20] LASINT je kratica za Laser Intelligence.
[21] NUCINT je kratica za Nuclear Intelligence.
[22] RINT je kratica za Radiation Intelligence.
[23] RADINT je kratica za Radar Intelligence.

- določitev subjektov[24] in objektov varnosti,[25]
- opredelitev varnosti v odnosu do vira ogrožanja iz družbenega[26] in naravnega[27] okolja,
- opredelitev varnosti kot statičnega in razvojnega dejavnika,
- opredelitev stopnje oziroma ravni varnosti,
- postavljanje dilem, ali je mogoče v celoti opredeliti in oceniti stopnjo varnosti.

Nacionalnovarnostni sistem države je ciljno usmerjen sistem, katerega naloga je usmerjanje delovanja njegovih podsistemov zaradi zagotavljanja ustrezne ravni varnosti države kot družbenega sistema (Stopar, 2003: 51).
V sami Resoluciji ni opredeljena vloga Obveščevalno-varnostne službe Ministrstva za obrambo v obrambnem podsistemu (v nadaljnjem besedilu: OVS MORS). Vendar je v Obrambni strategiji Republike Slovenije, št. 820-00/2001-1 z dne 20. 12. 2001, navedeno, da sta za učinkovit obrambni sistem pomembni povezanost in usklajenost s sistemom notranje varnosti zlasti na področju varovanja oblastnih organov, obrambnih ukrepov, varstva osebnih podatkov in varnostnega preverjanja oseb, pri zagotavljanju varnosti določenih varovanih oseb in objektov ter pri preprečevanju kaznivih dejanj v Ministrstvu za obrambo in Slovenski vojski. Zlasti velik poudarek je podan povezavam na področju obveščevalne in protiobveščevalne dejavnosti. Dejavnost teh služb je sestavni del varnostnega podsistema v ožjem smislu, pri tem pa je nedvomno dejavnost OVS MORS tudi predpogoj za uspešno delovanje obrambnega podsistema (Črnčec, 2003b: 4).

Obveščevalno-varnostna služba je samostojna služba Ministrstva za obrambo, ki opravlja obveščevalne, protiobveščevalne in varnostne naloge na obrambnem področju. Službo vodi generalni direktor, ki je za delo OVS MORS neposredno odgovoren ministru za obrambo. OVS MORS je vojaška obveščevalna služba, katere zakonsko podlago opredeljujeta Zakon o obrambi ter Uredba o OVS Ministrstva za obrambo (Uredba o OVS MORS, 1999, dopolnjena 2000). S to uredbo sta podrobneje urejena delovanje in organizacija OVS MORS.

Za začetek OVS MORS štejemo leto 1991, ko je iz Sektorja 9 v okviru MO nastala 6. uprava, ki je delovala proti takratnemu poveljstvu JLA. Šesta uprava se je nato

[24] Subjekti varnosti so posameznik, družbena skupina, politične stranke itd.
[25] V skupino objektov varnosti pa štejemo npr. varnost različnih oblik lastnine.
[26] Npr. notranji in zunanji sovražnik.
[27] Poplave, potresi, suša itd.

preimenovala v VOMO, Varnostni organ MO. Z Zakonom o obrambi, ki je bil sprejet decembra 1994, pa je znotraj MO kot organizacijska enota nastala današnja Obveščevalno-varnostna služba.
OVS MORS opravlja obveščevalne, protiobveščevalne in varnostne naloge, zbiranje, dokumentiranje in analiziranje informacij ter podatkov, ki so pomembni za obrambne interese države oziroma varovanje takih podatkov. V okviru svojih pristojnosti opravlja tudi naloge na obveščevalnem, protiobveščevalnem in varnostnem področju znotraj mednarodnih pogodb, ki jih sklene Republika Slovenija.

Za izvajanje obveščevalnih, protiobveščevalnih in varnostnih nalog Obveščevalno-varnostna služba opravlja za lastne potrebe tudi naloge s področja kadrovskih zadev, izobraževanja in usposabljanja, finančnega in materialnotehničnega poslovanja, naloge, povezane s sprejemom, evidentiranjem, oddajo in hrambo dokumentarnega gradiva, ter naloge, s pomočjo katerih sta omogočena razvoj in vzdrževanje informacijske in telekomunikacijske opreme službe. Za izvajanje teh nalog sodeluje s pristojnimi organizacijskimi enotami Ministrstva za obrambo in Slovenske vojske.
OVS MORS opravlja naloge v okviru sektorjev, oddelkov, centrov in izpostav. Organizirana je tako, da lahko posreduje podatke uporabniku v najkrajšem možnem času.

OVS MORS pri opravljanju svojih nalog sodeluje z ministrstvom, pristojnim za notranje zadeve, policijo in Slovensko obveščevalno-varnostno agencijo ter z njimi izmenjuje obveščevalne in protiobveščevalno-varnostne informacije. OVS ministrstva lahko izmenjuje obveščevalne informacije s tujimi vojaškimi obveščevalnimi in varnostnimi službami po predhodnem soglasju ministra.

V nadaljevanju bom opisal temeljne naloge področja dela OVS MORS, ki so pomembne ter vplivajo na varnost oseb, objektov in varovanje tajnih podatkov.

### 3.3.1. Obveščevalne in protiobveščevalne naloge

V prvem odstavku 32. člena Zakona o obrambi so navedene obveščevalne in protiobveščevalne naloge, ki jih opravlja OVS MORS.
Obveščevalne in protiobveščevalne naloge obsegajo zbiranje, dokumentiranje in analiziranje informacij ter podatkov, ki so pomembni za obrambne interese države, oziroma varovanje takih podatkov, in sicer:

- ugotavljanje in ocenjevanje vojaških in političnih varnostnih razmer ter vojaških zmogljivosti zunaj države, ki so posebnega pomena za varnost države,
- zbiranje in ocenjevanje podatkov o razmerah na območjih, kjer med izvajanjem obveznosti, prevzetih v mednarodnih organizacijah, oziroma pri opravljanju vojaške službe delujejo tudi pripadniki Slovenske vojske,
- odkrivanje in preprečevanje dejavnosti obveščevalnih služb vojaških organizacij ter drugih organov in organizacij, ki ogrožajo obrambne interese države, Slovensko vojsko ali ministrstvo (ZObr., 2004: 32. člen).

### 3.3.2. Varnostne naloge

Na podlagi drugega odstavka 32. člena Zakona o obrambi so varnostne naloge na obrambnem področju, ki jih opravlja OVS MORS:

- odkrivanje, preiskovanje in preprečevanje ogrožanja varnosti določenih oseb, delovnih mest, objektov in okolišev, ki jih uporabljata ministrstvo in Slovenska vojska v državi ali zunaj nje, ter podatkov o razvoju ali proizvodnji določenega vojaškega orožja ali opreme,
- preiskovanje kaznivih dejanj v skladu z zakonom,
- preučevanje in predlaganje rešitev za fizično in tehnično varovanje,
- operativno varovanje določenih oseb, delovnih mest, objektov in okolišev, ki so posebnega pomena za obrambo,
- varnostno preverjanje oseb v skladu s predpisi,
- usmerjanje dela vojaške policije pri opravljanju določenih varnostnih nalog v skladu s tem zakonom (ZObr., 2004: 32. člen).

OVS izvaja tako preventivne kakor tudi represivne ukrepe pri izvajanju protiobveščevalne in varnostne dejavnosti. Pri izvajanju dejavnosti uporablja metode dela, ki so značilne za obveščevalne službe. Delavci, ki izvajajo protiobveščevalno in varnostno dejavnost, so pooblaščene uradne osebe s pooblastili, kot jih določa Zakon za policijo.

Na protiobveščevalnem in varnostnem področju so vse naloge usmerjene v varovanje tajnih podatkov in odkrivanje eventualnih storilcev, torej je to dejavnost, s katero pridobivamo podatke o dejavnostih domačih in tujih državljanov, za katere obstaja sum, da bi bili lahko vpleteni v tako dejavnost oziroma so sodelavci tujih vojaških obveščevalnih služb (Šaponja, Osterman, 1996: 301).

Z ustrezno protiobveščevalno in varnostno dejavnostjo dosežemo:

- zaščito najpomembnejših državnih tajnosti pred ogrožanjem tujih obveščevalnih služb,
- preprečujemo vohunstvo,
- odkrivamo in onemogočamo vse oblike tajne dejavnosti zoper državo, katerih nosilec so obveščevalne službe tujih držav, ter
- odkrivamo in preprečujemo tajno prevratno delovanje zoper ustavno ureditev države.

Neodvisno od tega, da je protiobveščevalna dejavnost defenzivna in obrambna, organi, ki jo izvajajo, večinoma uporabljajo ofenzivne metode dela. Zaradi pravočasnega odkrivanja dejavnosti in načrtov tujih obveščevalnih služb morajo prodreti v njihove obveščevalne sisteme, kajti le na ta način je mogoče predvideti varnostne in druge ukrepe za zaščito države oziroma organizacije (Stajić, 2006: 208–209).

## 3.4. Vojaška obveščevalno-varnostna dejavnost Slovenske vojske

Za celovito razumevanje stanja obveščevalno-varnostne dejavnosti v Slovenski vojski je nujno na kratko pregledati njen razvoj. Obveščevalno-varnostni organi, zadolženi za izvajanje obveščevalnih in štabno varnostnih nalog, so bili v Slovenski vojski ustanovljeni leta 2000, ko je minister za obrambo izdal Uredbo o izvajanju nalog organa, pristojnega za obveščevalno podporo poveljevanju in vodenju ter za izvajanje štabno varnostnih nalog v Slovenski vojski.[28]

Pred tem obdobjem je bila za izvajanje štabno varnostnih nalog v Slovenski vojski zadolžena OVS MORS. Obveščevalna komponenta je bila v Slovenski vojski prisotna od njene ustanovitve. OVS je prek izpostav, ki jih je imela vzpostavljene v Slovenski vojski, in poleg drugih nalog, za katere je bila pristojna, opravljala tudi naloge štabno varnostne podpore v Slovenski vojski. Leta 1991 so bile ustanovljene izpostave pri Republiškem štabu za Teritorialno obrambo in sedmih Pokrajinskih poveljstvih Teritorialne obrambe (Čaleta, 2004).

V kasnejšem obdobju, do leta 2000, so se izpostave spreminjale in združevale skladno z reorganizacijo Teritorialne obrambe in kasneje Slovenske vojske. Struktura izpostav je bila

[28] Uredba o izvajanju nalog organa, pristojnega za obveščevalno podporo poveljevanju in vodenju ter za izvajanje štabno varnostnih nalog v Slovenski vojski (št. 017-06-1/00-2 z dne 19. 9. 2000).

podrejena neposredno OVS MORS, tako da poveljniki poveljstev in enot, kjer so delovale izpostave, niso imeli neposrednega vpliva na delo pripadnikov varnostnega organa, kakor ga je imela vojaška policija. To razmerje je prinašalo tako pozitivne kot tudi negativne posledice. Pozitivne posledice so se kazale predvsem v tem, da poveljniki enot in poveljstev niso imeli vpliva in moči, da bi prikrivali kazniva dejanja in druge deviantne pojave, ki so se dogajali v njihovih enotah ali poveljstvih. Negativne posledice pa so se kazale predvsem v nezaupanju do varnostnega organa; sodelovanje in delo sta bili v veliki meri odvisni od sposobnosti komuniciranja oseb, ki so vodile poveljstva in enote, ter oseb, ki so vodile izpostave varnostnih organov v teh poveljstvih in enotah.

Druga velika pomanjkljivost je bila v tem, da se je vojska počasi in postopoma začela prilagajati zahtevam in normativom zveze NATO. Pripadniki Slovenske vojske so v nasprotju s pripadniki OVS MORS, ki so izvajali naloge v izpostavah, odhajali na različne vrste štabnih usposabljanj doma in v tujino. Zaradi navedenega je na področju štabno varnostnih nalog v Slovenski vojski prihajalo do vedno večjega razkoraka med potrebami in dejavnostmi, ki so jih bili pripravljeni in sposobni na tem področju izvajati pripadniki OVS MORS (Čaleta, 2004).

Zakonska podlaga za izvajanje obveščevalno-varnostne dejavnosti znotraj Slovenske vojske je bila do leta 2002 ozka in nedorečena. Predvsem so na to ves čas opozarjale težave, ki so se pojavljale pri izvajanju protiobveščevalno-varnostnih nalog v Slovenski vojski. Razmejitev pristojnosti na teh področjih med Slovensko vojsko in OVS MORS zakon ni urejal. Zakon o spremembah in dopolnitvah Zakona o obrambi[29] je dokončno opredelil vlogo varnostnega organa za opravljanje štabno varnostnih nalog v Slovenski vojski.
Zakon o obrambi[30] sicer določa, da je za protiobveščevalne in varnostne naloge, ki so navedene v 32. členu, pristojna OVS MORS. Vendar je navedenemu členu dodan nov odstavek, ki natančno opredeli, da štabno varnostni organi Slovenske vojske izvajajo preventivne naloge protiobveščevalne zaščite poveljstev, enot in zavodov vojske in štabno varnostne naloge ter usmerjajo in vodijo delo vojaške policije, razen pri preiskovanju kaznivih dejanj, ki je v pristojnosti OVS ministrstva. Štabni varnostni organ Generalštaba

[29] Zakon o spremembah in dopolnitvah Zakona o obrambi (Uradni list RS, št. 67/2002).
[30] Uradni list RS, št. 82/94.

strokovno vodi in usmerja delovanje podrejenih štabnih varnostnih organov ter sodeluje z Obveščevalno-varnostno službo ministrstva.
Iz drugega odstavka 33. člena ZObr, kjer je opredeljena organizacija OVS MORS, lahko razberemo naslednje: podatki in informacije, zbrani pri opravljanju obveščevalnih in protiobveščevalnih ter varnostnih nalog, so podlaga za analitične in operativne ocene, za opravljanje štabno varnostnih nalog v vojski, za izdelavo načrtov uporabe vojske in drugih obrambnih priprav ter za načrtovanje in izvajanje obrambnih ukrepov, kar opredeljuje medsebojno odvisnost med OVS MORS in obveščevalnimi organi znotraj SV.

Skladno z novim poslanstvom in reorganizacijo zveze NATO v smeri vse pogostejšega izvajanja operacij zunaj 5. člena **Severnoatlantske pogodbe**, nevojaške oblike ogrožanja bolj kot kadar koli prej postavljajo zahtevo po spremljanju in predvidevanju političnih, gospodarskih, diplomatskih, kulturnih, demografskih in informacijskih dejavnikov ter dejavnikov ogrožanja javne varnosti, ki predstavljajo potencialno grožnjo za enote in pripadnike SV v coni obveščevalnega interesa. Zaradi kompleksne narave navedenih dejavnikov ogrožanja ter dejstva, da vpliv in dejavnost teh dejavnikov s področja mednarodne vojaške operacije pogosto segata tudi na ozemlje Republike Slovenije, postaja vse pomembnejša koordinacija delovanja vojaške obveščevalne dejavnosti z dejavnostjo OVS MORS in drugimi subjekti nacionalnovarnostnega sistema ter tujimi obveščevalno-varnostnimi organi. Reševanje teh vprašanj bo v prihodnosti zahtevalo vse več pozornosti ter ustrezne normativne, organizacijske, kadrovske in tehnične ukrepe.

Vojaške operacije NATO in EU zunaj geografskega območja držav članic obeh organizacij (angl.: Out- of- Area Operations) zahtevajo ustrezno obveščevalno podporo v vseh fazah operacije, vključno s fazo odločanja o napotitvi sil SV. V tej fazi je pomembna vloga VOD v podpori odločanju o začetku operacije, njenem načrtovanju ter pri usposabljanju, opremljanju in pripravah sodelujočih enot. Zagotovo najpomembnejša naloga VOD je obveščevalna ter protiobveščevalno-varnostna podpora med izvajanjem operacije, kjer so enote SV izpostavljene kompleksnim varnostnim grožnjam, drugačnim od groženj doma, neugodnim podnebnim razmeram, obveščevalnim dejavnostim različnih tujih obveščevalnih služb ipd. VOD SV mora biti zato podprta tudi z obveščevalno, protiobveščevalno in varnostno dejavnostjo OVS ter obveščevalnimi strukturami operacije in tujih oboroženih sil, saj bo SV le na ta način sposobna pravočasno predvideti, odkriti, oceniti in spremljati navedene grožnje ter odgovoriti nanje (Koncept VOD SV, 2005: 6–7).

Zaradi uspešnega izvajanja vseh nalog vojaško obveščevalno dejavnost na strateški ravni izvajajo OVS MORS in obveščevalni organi Generalštaba Slovenske vojske. Na operativni ravni izvajajo vojaško obveščevalno dejavnost obveščevalni organi in enote operativnega poveljstva sil, na taktični ravni pa obveščevalni organi poveljstev brigad in bataljonov ter izvidniške enote. Ravni obveščevalne dejavnosti se medsebojno prepletajo in dopolnjujejo (Vojaška doktrina, 2006: 32).

Vojaška obveščevalna dejavnost Slovenske vojske je celota funkcij, procesov, postopkov in ukrepov posameznikov, enot in poveljstev, s katerimi neprekinjeno in celovito spremljajo, analizirajo in predvidevajo vojaško, vojaškopolitično in varnostno situacijo ter delovanje sovražnika, potencialnega sovražnika ter druge vojaške in varnostne grožnje, z namenom omogočiti poveljnikom in drugim, ki odločajo o uporabi Slovenske vojske, sprejem kvalitetnih in pravočasnih odločitev na vseh ravneh poveljevanja. Del vojaške obveščevalne dejavnosti je elektronsko izvidovanje, ki se v Slovenski vojski izvaja centralizirano (Vojaška doktrina, 2006: 33).
Vojaška obveščevalna dejavnost Slovenske vojske obsega naslednje temeljne funkcije: zagotavljanje indikatorjev in opozoril, izvajanje obveščevalne priprave bojišča, podporo poznavanju situacije, podporo načrtovanju in delovanju po ciljih, ocenjevanje bojnega delovanja, podporo zaščiti sil in pripravo sil za delovanje (Vojaška doktrina, 2006: 33).

Varnostno delovanje je dejavnost Slovenske vojske, ki s pomočjo aktivnih in pasivnih ukrepov zagotavlja varnost sil tako, da onemogoča sovražniku poznavanje razporeditve, zmogljivosti in namer lastnih sil. Ukrepi so osredotočeni v tiste vsebine, ki odkrivajo ključne dejavnosti ali slabosti oziroma ščitijo bistvene podatke o lastnih silah (Vojaška doktrina, 2006: 68).
Aktivni varnostni ukrepi vključujejo motenje ali uničenje sovražnikovih zmogljivosti za izvidovanje, obveščevalno dejavnost in pridobivanje podatkov o ciljih, napad na poveljniška mesta in druge elemente sistema poveljevanja in kontrole, zavajanje in psihološko delovanje. Pasivni varnostni ukrepi obsegajo varovanje oseb, fizično in tehnično varovanje območij in objektov, varovanje dokumentov, maskiranje ter prikrivanje položajev in dejavnosti, varnost informacij ter varnost komunikacijskega in informacijskega sistema (Vojaška doktrina, 2006: 68).

### 3.4.1. Opredelitev poslanstva obveščevalno-varnostnih organov

Za delovanje vojaške obveščevalne dejavnosti je odgovoren poveljnik, ki izvaja tudi poveljniški nadzor nad vojaško obveščevalno dejavnostjo.
Obveščevalno-varnostna dejavnost v Slovenski vojski je na področju izvajanja nalog obveščevalne podpore poveljevanju in štabno varnostnih nalog organizirana na vseh ravneh poveljevanja do ravni bataljona. Na omenjenih ravneh so vzpostavljeni sektorji, oddelki in odseki (J-2, G-2 in S-2), ki so sestavljeni iz dveh področij, obveščevalnega in protiobveščevalnega ter varnostnega.

**J-2** je glavni nosilec strateške VOD v SV in opravlja razvojno, usmerjevalno in nadzorno funkcijo vojaške obveščevalne dejavnosti v SV na vseh ravneh poveljevanja. Poleg te svoje osnovne funkcije s sodelovanjem z OVS zagotavlja tudi obveščevalno podporo GŠSV in PSSV.
J-2 usmerja delo Oddelka za obveščevalne analize, ki je funkcionalno umeščen v strukturo Analitičnega sektorja OVS. Tako na vojaškostrateški kot tudi na operativni ravni je SV uporabnik obveščevalnih izdelkov, ki jih zagotavlja OVS.

**G-2** PSSV izvaja načrtovanje, organiziranje, usmerjanje in kontrolo vojaške obveščevalne dejavnosti PSSV. PSSV načrtuje in izvaja vse vojaške operacije SV doma in v okviru operacij zavezništva, zato mora tudi G-2 zagotoviti učinkovito obveščevalno podporo za vse navedene operacije. V tem smislu mora G-2 zagotoviti potrebne organizacijsko-formacijske, strokovne, tehnične in druge kapacitete, s katerimi mora opraviti svoje poslanstvo v celotnem spektru operacij. Konkretna vsebina, intenziteta, obseg in zahtevnost obveščevalne podpore se spreminjajo glede na vrsto naloge, kompleksnost groženj, razpoložljivi čas in fazo delovanja.

**S-2** brigade organizira in usmerja VOD v brigadi, na podlagi prioritetnih obveščevalnih zahtev (POZ) in drugih usmeritev poveljnika brigade, zahtevkov za informacijo PSSV in podrejenih poveljstev in enot. S-2 poleg usmeritev zagotavlja podrejenim poveljstvom in enotam tudi vse potrebne informacije v obsegu, ki jih te potrebujejo za vodenje sedanjih in načrtovanje prihodnjih operacij.
Organiziranje in usmerjanje OIZag na bataljonski ravni izvaja S-2, na podlagi prioritetnih obveščevalnih zahtev (POZ) in drugih usmeritev poveljnika bataljona ter potreb

poveljnikov čet. S-2 izdela načrt izvidovanja in nadzora, ki je osnova za izdajanje nalog izvidniškemu vodu.

V nadaljevanju obravnavanja vojaške obveščevalne dejavnosti se bom omejil zgolj na varnostno in protiobveščevalno dejavnost in bom skušal opredeliti temeljne naloge, ki so pomembne za delovanje, zaščito poveljstev in enot ter varovanje tajnih podatkov.

### 3.4.2. Protiobveščevalno-varnostne naloge

Grožnje varnosti so lahko nevtralizirane s protiobveščevalnimi in varnostnimi ukrepi, ki so:

- načrtovanje, usmerjanje, vodenje in nadzor celovitega razvoja varnostne in protiobveščevalne zagotovitve v Slovenski vojski,
- izvajanje protiobveščevalnih in varnostnih priprav pripadnikov pred odhodi v tujino ter opravljanje pogovorov po vrnitvi,
- načrtovanje, usmerjanje, vodenje in nadzor dejavnosti v zvezi z vojaško policijo,
- oblikovanje usmeritev za izdelavo konceptualnih, razvojnih in doktrinarnih dokumentov, programov izobraževanja in usposabljanja s področja varnostne zagotovitve in vojaškopolicijskih nalog,
- usmerjanje pri postopkih ravnanja s kadri na področju varnostne zagotovitve ter vojaške policije,
- preučevanje in uvajanje vojaških standardov na področju varnostne zagotovitve vojaškopolicijskih nalog,
- oblikovanje in razvoj smernic za analiziranje groženj in ranljivosti ter oblikovanje ocen na ravni Slovenske vojske,
- uresničevanje obveznosti do NATA in EU na področju varnostne zagotovitve na strateški ravni,
- načrtovanje ukrepov na področju protiterorizma in protiobveščevalnih zadev ter
- koordinacija s pristojnimi sektorji OVS in izmenjava podatkov.

Z vstopom Slovenije v NATO in izvajanjem varnostnih standardov pa lahko med varnostne in protiobveščevalne naloge, ki jih izvajajo organi znotraj Slovenske vojske, uvrščamo še naslednje:

- svetovanje poveljniku o vseh varnostnih zadevah,
- protiobveščevalno delovanje v mednarodnih operacijah,

- izvajanje zaščite sil,
- preventivna varnost,
- izvajanje zaščitnih ukrepov na bojišču.

Protiobveščevalno delovanje obsega identifikacijo nasprotnikovih obveščevalnih dejavnosti ter vseh vrst subverzivnih in prevratniških organizacij ter protiukrepe nanje. Protiobveščevalna služba deluje po principu zanikanja obstoječih pomembnih informacij ter izvajanja ustreznega varovanja in zaščite lastnih enot (AJP-2, 2001).

Preventivna varnost je definirana kot »organiziran sistem obrambnih ukrepov, uvedenih in zadržanih na vseh ravneh poveljevanja s ciljem doseči in ohranjati varnost«.[31] To je varovanje vseh komponent, vključno z osebjem, pred neželenimi dogodki ter kompromitiranjem (AJP-2, 2001).

Zaposleni, ki se v Slovenski vojski ukvarjajo s protiobveščevalno in varnostno dejavnostjo, niso uradne pooblaščene osebe. Pri svojem delu uporabljajo metode dela, ki jih opredeljuje Zakon o obrambi. Izvajajo protiobveščevalno in varnostno pripravo zaposlenih, spremljajo, analizirajo in predvidevajo vojaško situacijo ter delovanje sovražnika, potencialnega sovražnika, predvsem njegovih obveščevalnih služb in sil za specialno delovanje ter drugih vojaških in varnostnih groženj, z namenom omogočiti poveljnikom in drugim v procesu odločanja sprejem pravočasnih odločitev na vseh ravneh poveljevanja in kontrole SV. Izdelujejo protiobveščevalne in varnostne analize, ocene, poročila in druge izdelke s področja obrambe in varnosti ter s tem omogočajo boljše razumevanje situacije in njeno spremljanje.

Bistvena metoda dela je preventiva, ki je usmerjena k preprečevanju nastajanja neželenih posledic in oblik ogrožanja. Pri sodelovanju z OVS MORS omenjeni organi nudijo podporo pri izvajanju represivnih ukrepov, ki so usmerjeni k izvorom, oblikam ter nosilcem ogrožanja varnosti. Pri izvajanju svojih nalog sodelujejo tudi z drugimi organi v okviru Ministrstva za obrambo pa tudi zunaj njega.

[31] AAP-6.

# 4. VARNOSTNI STANDARDI VAROVANJA TAJNIH PODATKOV

V marcu 2001 je Svet Evropske unije sprejel Varnostna določila Sveta Evropske unije. V juniju 2002 so se spremenili varnostni standardi v zvezi NATO. Glede na to, da je bila Slovenija takrat v postopku vključevanja v Evropsko unijo in zvezo NATO, je bilo treba varnostne standarde in s tem Zakon o tajnih podatkih spremeniti tako, da bi zagotavljali primerljivo in enakovredno možnost sodelovanja slovenskih predstavnikov v postopkih, kjer je za sodelovanje treba imeti dostop do tajnih podatkov in s tem predhodno pridobiti ustrezno dovoljenje za dostop do takih podatkov (Hartman, 2004: 26).

Eden izmed temeljnih pogojev, ki ga je Republika Slovenija morala izpolniti pred vstopom v EU in NATO, je vzpostavitev ustreznega sistema obravnavanja tajnih podatkov. Standardi obeh organizacij predpostavljajo, da je način varovanja tajnih podatkov pri vsaki članici na taki ravni, da omogoča popolno medsebojno zaupanje pri izmenjavi podatkov, brez dodatnega varnostnega dogovarjanja ali ukrepanja. S sprejemom ZTP in njegove novele v letu 2003 je Republika Slovenija področje tajnih podatkov uskladila s standardi omenjenih organizacij, kar sta tudi obe potrdili in ocenili, da je Slovenija na tem področju vredna zaupanja (Predlog Zakona o spremembah in dopolnitvah ZTP, 2005).

Po vstopu v omenjeni organizaciji je Zakon o tajnih podatkih doživel spremembo v letu 2006. Predlagane spremembe in dopolnitve ZTP so bile usmerjene predvsem v večjo učinkovitost sistema in posledično v večjo varnost tajnih podatkov ter osebno varnost oseb, ki imajo zaradi opravljanja funkcije ali delovnih nalog potrebo po dostopu do tajnih podatkov.
Pomembnost varnostnega področja za uspešno delovanje Evropske unije in zveze NATO je razvidna iz dokumentov, ki urejajo varnostno področje. Postopki ravnanja s tajnimi podatki so natančno predpisani, kakor tudi način njihovega označevanja, posredovanja, hranjenja in dostopa. Ključni dejavnik varovanja tajnih podatkov je seveda človek in temu je namenjena posebna pozornost. Pojasniti je treba način dostopa do tajnih podatkov EU in NATO ter pogoje, ki jim morajo zadostiti posamezniki, ki dostopajo ali bi ali bodo dostopali do tajnih podatkov (Brezovšek, Črnčec, 2004: 516).

Ali smo s posameznimi spremembami, ki so bile izvedene, tudi končali uvajanje standardov, ki jih predpisujeta zveza NATO in EU? Osebno menim, da je sama uskladitev standardov (varnostno preverjanje, varnostna območja, tehnično in fizično varovanje, certificirana oprema, informacijska tehnologija …) prvi korak, ki smo ga na obrambnem področju in v Slovenski vojski ponekod popolnoma, drugje pa le deloma uresničili. Standarde smo uvedli, posamezna področja so opredeljena celo strožje, kot jih predpisujeta omenjeni organizaciji.

Ali je to dovolj? Nekateri bi najverjetneje odgovorili pritrdilno, sam pa bom v nadaljevanju poskušal opozoriti na področja, ki se mi zdijo izredno pomembna in smo jih vede ali nevede nekoliko zanemarili. Pri preučevanju zakonodaje, ki področje v EU in NATO normativno ureja, sem skušal povzeti izključno določila, ki opredeljujejo ravnanje s tajnimi podatki in obveznosti, ki jih imajo zaposleni pri njihovem obravnavanju, in za katera menim, da so najpomembnejša.

## 4.1. Varnostni standardi v Evropski uniji

Varnostna določila Sveta Evropske unije[32] (Security Regulations of the Council of the European Union) so bila sprejeta 19. marca 2001 v Bruslju in so začela veljati 1. decembra 2001. Urejajo organizacijo varnosti v Svetu Evropske unije, klasifikacijo in označevanje dokumentov glede na stopnjo tajnosti, fizično varnost v objektih in okoliših, osnovne principe dostopa do tajnih podatkov in varnostno preverjanje, pripravo, distribucijo, pošiljanje, hranjenje in uničevanje tajnih podatkov Evropske unije (Černetič, Brožič, 2003).

Varnostna določila predpisujejo ustanovitev posebnega registra za hranjenje strogo tajnih podatkov Evropske unije. Posebno poglavje obravnava varovanje tajnih podatkov s področja informacijske tehnologije in komunikacijskih sistemov ter postopke za odobritev dostopa do tajnih podatkov tretjim državam, torej nečlanicam Evropske unije. Varnostna določila Sveta Evropske unije veljajo za Svet Evropske unije, Generalni sekretariat Sveta Evropske unije in vse države članice. Definirajo pojem tajnega podatka in oblike

[32] Security Regulations of the Council of the Europoean Union, Official Journal of the European Communities (2001/264/EC), L 101.

potencialnega ogrožanja tajnih podatkov. Določajo, da mora vsaka država članica imeti nacionalni varnostni urad[33] (National Security Organisation) (Černetič, Brožič, 2003).
Varnostna določila Sveta Evropske unije določajo, da imajo dostop do tajnih podatkov Evropske unije samo osebe, ki se morajo s takimi podatki seznaniti zaradi opravljanja funkcije ali delovnih nalog.[34] Navedeno pomeni, da morajo biti v državah članicah varnostno preverjeni vsi tisti zaposleni, ki pri svojem delu potrebujejo tajne podatke Evropske unije v sami državi članici, pa tudi vsi tisti, ki državo članico predstavljajo v institucijah Evropske unije in pri svojem delu potrebujejo njene tajne podatke (Černetič, Brožič, 2003: 578–579).

Vsi posamezniki, ki potrebujejo dostop do tajnih podatkov stopnje ZAUPNO EU ali višje, morajo biti predhodno ustrezno preverjeni. Podobno velja za osebje, ki dela na področju tehničnega delovanja ali vzdrževanja komunikacijskih in informacijskih sistemov, ki vsebujejo tajne podatke. V postopku preverjanja je treba ugotoviti, ali je posameznik:

- nedvomno lojalen,
- takega karakterja in tako diskreten, da ni nobenega dvoma o njegovi integriteti ter s tem o njegovem ravnanju s tajnimi podatki,
- občutljiv za pritiske zunanjih ali drugih virov zaradi svojega prejšnjega prebivališča ali preteklih povezav, ki lahko predstavljajo varnostno tveganje.

Cilj varnostnega preverjanja je ugotoviti, ali obstajajo zadržki za dostop posameznika do tajnih podatkov. Varnostno preverjanje se izvede s sodelovanjem posameznika, izvajajo ga kompetentni organi države članice, katere državljan je posameznik, EU preverjanja ne izvaja (Brezovšek, Črnčec, 2004: 518).

Osebje, ki ima dostop do tajnih podatkov Evropske unije, mora biti usposobljeno in se mora zavedati:

- varnostnih tveganj, ki so lahko posledica nediskretnih pogovorov,
- previdnostnih ukrepov, ki jih je treba upoštevati pri stikih s predstavniki tiska,
- potencialnih aktivnosti obveščevalnih služb, katerih cilj je dostop do tajnih podatkov Evropske unije,

[33] V Sloveniji Urad Vlade Republike Slovenije za varovanje tajnih podatkov, ki je hkrati Nacionalni varnostni organ.
[34] Princip »need to know« pomeni, da oseba, ki je sicer preverjena za dostop do določene stopnje tajnosti in ima ustrezno varnostno potrdilo oziroma dovoljenje, dostopa do podatkov v okviru navedene stopnje tajnosti, vendar samo v okviru svojega dela.

- obveze, da mora nemudoma poročati pristojnim varnostnim organom ob najmanjšem sumu na vohunsko dejavnost ali o neobičajnih okoliščinah, ki bi lahko kakor koli vplivale na varnost,
- potrebe po usposabljanju vseh tistih, ki pri svojem delu redno prihajajo v stik s predstavniki tujih držav, v katerih je eden glavnih ciljev obveščevalnih služb pridobitev tajnih podatkov Evropske unije (Černetič, Brožič, 2003: 580).

Prav tako mora osebje, ki ima dostop do tajnih podatkov Evropske unije, poznati metode, s katerimi obveščevalne in varnostne službe pridobivajo sodelavce.

## 4.2. Varnostni standardi v zvezi NATO

Dne 17. junija 2002 so začeli veljati novi varnostni standardi zveze NATO. Varnost znotraj Severnoatlantske organizacije (Security Within the North Atlantic Treaty Organisation, Document C-M(2002)49) je dokument, ki je sestavljen iz direktiv za vsa področja varovanja tajnih podatkov in je dopolnil ter zamenjal dokument Varnost v okviru organizacije Severnoatlantskega sporazuma C-M(55)15 (FINAL) (Čaleta, 2004a: 62).

Sestavljajo ga naslednje direktive:

- AC/35-D/2000; Direktiva o varnostnem preverjanju. Določa načine in postopke varnostnega preverjanja, stopnje tajnosti, postopke ponovnega varnostnega preverjanja in kriterije za varnostno preverjanje;
- AC/35-D/2001; Direktiva o fizični varnosti. Določa načine in postopke izvajanja fizičnega varovanja objektov in okolišev, ki so posebnega pomena za varovanje tajnih podatkov in objektov;
- AC/35-D/2002; Direktiva o informacijski varnosti. Določa načine in postopke ravnanja na področju informacijske varnosti s poudarkom na tehničnih rešitvah informacijske varnosti;
- AC/35-D/2003; Direktiva o industrijski varnosti. Določa načine in postopke varovanja tajnih podatkov, ki so posredovani drugim organizacijam ali izvajalcem, pri čemer je vključeno tako varnostno preverjanje zaposlenih kot tudi zagotavljanje fizične varnosti objektov in opreme;
- AC/35-D/2004; Osnovna direktiva za INFOSEC. Določa načine in postopke ravnanja na področju informacijske varnosti s poudarkom na informacijskih rešitvah informacijske varnosti;

- AC/35-D/2005; INFOSEC direktiva za organizacijo CIS. Določa načine in postopke ravnanja na področju informacijske varnosti s poudarkom na organizacijskih rešitvah in uvajanju novih tehnologij na področju informacijske varnosti.

K dokumentu C-M(2002)49 sodi tudi dodatek o varnostnih merilih proti terorističnim grožnjam (Protection Measures for Nato Civil and Military Bodies Deployed Nato Forces and Installations against Terrorist Threats) (Černetič, Brožič, 2003: 579).

V dokumentu Varnost v okviru organizacije severnoatlantskega sporazuma, C-M(2002)49, so zajeti in določeni politika varovanja podatkov, sredstev, naprav in objektov, pomembnih za delovanje in uresničevanje ciljev NATA, ter minimalni varnostni ukrepi in postopki, ki jih pri obravnavanju podatkov, opravljanju nekaterih dejavnosti ali pri uporabi določene infrastrukture, na primer objektov, predmetov in naprav, morajo upoštevati organi in članice NATA (Čaleta, 2004a: 63).

Varnostna direktiva zavezniškega poveljstva za Evropo, AD 70-1, podrobneje določa postopke in ukrepe ter minimalne standarde varnosti. To so minimalni standardi, ki so jih sprejele vse članice NATA.
Osnovni varnostni standardi, ki so jih sprejele vse članice NATA, so:

- tajni podatki se lahko posredujejo samo tistim osebam, ki izrazijo potrebo po seznanjanju s temi podatki oziroma so zaradi nalog, ki jih opravljajo, upravičene do seznanitve s temi podatki, pred tem pa so se udeležile varnostnega usposabljanja, na katerem so bile seznanjene z osnovnimi varnostnimi zahtevami za varovanje tajnih podatkov;
- samo posamezniki, za katere je bilo opravljeno ustrezno varnostno preverjanje, bodo imeli dostop do tajnih podatkov stopnje ZAUPNO (confidential) ali višje in se seznanjali z njimi;
- tajni podatki morajo biti varovani z ustreznim sistemom, ki ga sestavljajo ukrepi na področju kadrovske in fizične varnosti, varnosti informacij ter varnosti informacijskih in komunikacijskih sistemov;
- vsak sum ogrožanja varnosti tajnih podatkov mora biti takoj sporočen ustreznemu varnostnemu organu. Poročilo morajo varnostni organi takoj ovrednotiti. Ugotovljena mora biti morebitna škoda, ki bi bila NATU povzročena z ogrožanjem varnosti

podatkov ali njihovo odtujitvijo. Takoj morajo biti sprejeti tudi ustrezni ukrepi (Čaleta, 2004a: 63).

V povezavi z varnostnimi standardi zveze NATO je treba vzpostaviti enotna merila za ugotavljanje lojalnosti, zanesljivosti in vrednosti zaupanja v posameznika, ki bo imel dostop do tajnih podatkov zveze NATO. Da bi navedeno dosegli, mora vsak posameznik, ki pri svojem delu potrebuje dostop do tajnih podatkov, pridobiti ustrezno varnostno potrdilo (Personnel Security Clearance – PSC) z določeno časovno veljavnostjo (Černetič, Brožič, 2003: 579).

Vsi posamezniki, ki pri svojem delu potrebujejo dostop do tajnih podatkov zveze NATO in pridobijo ustrezno varnostno potrdilo, morajo biti usposobljeni prepoznati:

- potencialno nevarnost za varovanje tajnih podatkov pri pogovorih z osebami, ki pri svojem delu ne potrebujejo določenih podatkov, čeprav imajo dostop do iste stopnje tajnosti kot nekdo drug,
- potencialno nevarnost za varovanje tajnih podatkov pri komuniciranju s predstavniki tiska,
- potencialno nevarnost za varovanje tajnih podatkov, ki jo predstavljajo tuje obveščevalne in varnostne službe, ki se zanimajo za zvezo NATO in države članice.

O zaznavi potencialnih nevarnosti so dolžni nemudoma poročati. Usposabljanja na področju varnosti so obvezna za vse tiste, ki imajo dostop do tajnih podatkov. Pridobljena znanja je treba periodično obnavljati (Černetič, Brožič, 2003: 580).

## 4.3. Varnostni standardi v Republiki Sloveniji

S sprejetjem Zakona o tajnih podatkih smo v Sloveniji zadostili zahtevam pogajalskih izhodišč za vstop v Evropsko unijo v poglavju 24, Pravosodje in notranje zadeve.
Zakon je na ravni države združil nekatera področja varovanja tajnih podatkov, ki so sicer že bila delno urejena v posameznih zakonih oziroma podzakonskih aktih. Zakon o tajnih podatkih je v splošnih določbah opredelil temeljne pojme, kot so tajni podatek, dokument, določanje tajnih podatkov, prenehanje tajnosti podatkov, varnostno preverjanje in varnostni zadržek. Poleg splošnih določb vsebuje še poglavja o določanju tajnih podatkov,

dovoljenju za dostop do tajnih podatkov, dostop do tajnih podatkov in njihovo varovanje ter nadzor nad izvajanjem zakona (Černetič, Brožič, 2003: 579–580).

Urejen sistem varovanja tajnih podatkov je po vključitvi Slovenije v evroatlantske povezave zelo pomemben. Prav tako je vzpostavitev vseh delov sistema v vseh državnih organih pomembna za delovanje sistema. Država, ki ustrezno varuje svoje in tuje tajne podatke, je v mednarodni skupnosti sprejeta kot zaupanja vreden partner. Slovenija je to dosegla s sprejetjem ZTP, kljub vsemu pa je bilo treba v Zakonu in podzakonskih aktih opraviti določene spremembe.

Državni zbor je potrdil njegove spremembe 3. 10. 2003. Bistvene spremembe so bile:

- uvedba četrtega organa, ki izvaja varnostno preverjanje – policije,
- tristopenjsko preverjanje,
- terensko preverjanje je dovoljeno zgolj pri obstoju suma varnostnega zadržka za dostop do TAJNO in STROGO TAJNO,
- razširjen vprašalnik, ki je sestavljen iz dveh delov,
- odvisnost se preverja pri pooblaščenem zdravniku ali zdravstveni organizaciji,
- možnost preverjanja ožjih družinskih članov,
- za ZAUPNO in TAJNO se preverja obdobje zadnjih pet let ter deset let za STROGO TAJNO.

Ker je praksa pri izvajanju ZTP pokazala določene pomanjkljivosti varnostnega preverjanja predvsem v določilih, kjer se odloča o verodostojnosti preverjane osebe za dostop do tajnih podatkov, je v maju 2006 Državni zbor potrdil spremembe in Zakon je začel veljati junija istega leta.

Kot pogoj za začetek varnostnega preverjanja osebe zakon uvaja obvezno usposabljanje s področja obravnavanja in varovanja tajnih podatkov, kar je lahko eden bistvenih pogojev za zagotavljanje večje varnosti tajnih podatkov. Pri preverjanju osebe se organu, pristojnemu za varnostno preverjanje, omogoča, da preveri morebitno kaznovanost preverjane osebe za prekrške, ki bi lahko vzbujali utemeljen dvom o njegovi verodostojnosti, zanesljivosti in/ali lojalnosti za varno obravnavanje tajnih podatkov (na primer prekrški, storjeni pod vplivom alkohola, zloraba drog ipd.).

Zakon nedvoumno opredeljuje tudi varnostne zadržke, zaradi katerih se izdaja dovoljenja zavrne. Dovoljenje se ne izda zaradi lažne navedbe podatkov v vprašalniku, neizbrisane

pravnomočne obsodbe na najmanj tri mesece nepogojne kazni zapora, dokončnega disciplinskega ukrepa zaradi hujše kršitve varnega obravnavanja tajnih podatkov, morebitne odvisnosti preverjane osebe, članstva ali sodelovanja v organizacijah ali skupinah, ki ogrožajo ustavno ureditev, neodvisnost, ozemeljsko celovitost in obrambno sposobnost Republike Slovenije ali držav članic političnih, obrambnih in varnostnih zvez katerih članica je Republika Slovenija (na primer države članice EU in NATO).

Novela ZTP uvaja tudi inšpekcijski nadzor na področju tajnih podatkov. Na obrambnem področju ga izvaja Inšpektorat Republike Slovenije za obrambo. Z vzpostavitvijo inšpekcijskega nadzora je dosežena večja enotnost pri izvajanju predpisov s področja tajnih podatkov. Notranji nadzor, ki ga izvaja predstojnik le znotraj »svojega« organa, ni zagotavljal enotne prakse na tem področju. Prek inšpekcijskega nadzora bo pomembne informacije pridobival tudi nacionalni varnostni organ, ki je pristojen za spremljanje stanja ter razvoj in izvajanja standardov varovanja tajnih podatkov.

Na obrambnem področju in v Slovenski vojski so uvedeni standardi za izvajanje fizično in tehnično podprtega varovanja, ki temeljijo na nacionalnih predpisih (predvsem Zakon o tajnih podatkih, Uredba o varovanju tajnih podatkov in Sklep o določitvi pogojev za varnostno tehnično opremo, ki se sme vgrajevati v varnostna območja). Pri hranjenju TP zveze NATO oziroma EU upoštevamo rešitve, ki jih vsebujejo direktive omenjenih povezav ter niso v nasprotju z našimi predpisi. Varovanje predpisujejo tudi Pravilnik o varovanju tajnih podatkov na Ministrstvu za obrambo (februar 2006) in njegove spremembe in dopolnitve (avgust 2006).

V skladu z določbami Zakona o tajnih podatkih so bili sprejeti še naslednji podzakonski akti:

- Uredba o varovanju tajnih podatkov,
- Uredba o varnostnem preverjanju in izdaji dovoljenj za dostop do tajnih podatkov, ki ureja začetek postopka, definira, kdo so udeleženci v postopku, opredeli varnostni vprašalnik, določa ravnanje z vprašalnikom in varnostno preverjanje,[35] preverjanje podatkov iz vprašalnika, pogovor s kandidatom, oceno o ugotovitvah varnostnega

[35] Varnostno preverjanje kandidata je sestavljeno iz resničnosti navedb v izpolnjenem vprašalniku in pogovora s kandidatom.

preverjanja, izdajo odločbe, vročitev dovoljenja, preklic dovoljenja in odločanje o ugovoru,

- Uredba o izvajanju inšpekcijskega nadzora na področju varovanja tajnih podatkov in vsebini posebnega dela strokovnega izpita za inšpektorja,
- Uredba o notranjem nadzoru nad izvajanjem Zakona o tajnih podatkih in predpisov, izdanih na njegovi podlagi, ki ureja oblike nadzora, splošni nadzor, tematski nadzor, opravljanje nadzora, preverjanje odprave pomanjkljivosti, izvajalce nadzora, vsebino nadzora in poročilo o nadzoru,
- Uredba o ugotavljanju izpolnjevanja pogojev za posredovanje tajnih podatkov drugi organizaciji,
- Sklep o ustanovitvi, nalogah in organizaciji Urada za varovanje tajnih podatkov (UVTP).

Po primerjavi določil, ki jih predpisujeta EU in NATO, je mogoče opredeliti najpomembnejše. Omenjeni organizaciji ne izvajata varnostnega preverjanja, ampak je varnostno preverjanje oseb za dostop do tajnih podatkov obeh v pristojnosti nacionalnih organov. V Sloveniji varnostno preverjanje opravljajo: v Ministrstvu za obrambo OVS MORS, za zaposlene v Ministrstvu za obrambo in Slovenski vojski ter za osebe, ki bodo pri svojem delu ravnale s tajnimi podatki z obrambnega področja, Policija za svoje zaposlene, Slovenska obveščevalno-varnostna agencija za svoje zaposlene ter za vse druge, ki potrebujejo dovoljenje za dostop do tajnih podatkov, Služba za tajne podatke Ministrstva za notranje zadeve.

Pravico do dostopa do tajnih podatkov imajo samo tiste osebe, ki imajo dovoljenje in se morajo s temi podatki seznaniti zaradi opravljanja funkcije ali delovnih nalog. Dostop imajo samo do tajnih podatkov tiste stopnje tajnosti, ki je določena v dovoljenju. V dokumentih je tudi opredeljeno, da za dostopanje do podatkov stopnje INTERNO ni treba opraviti varnostnega preverjanja, temveč je dovolj, da je oseba seznanjena z zakonodajo in podzakonskimi akti ter podpiše izjavo o seznanjenosti po predhodno izvedenem usposabljanju.

Glede na zahteve obeh organizacij je v Republiki Sloveniji ustanovljen UVTP, katerega temeljne naloge so, da:

- spremlja in usklajuje stanje na področju obravnavanja in varovanja TP,
- predlaga ukrepe za izboljšanje varovanja TP,

- skrbi za razvoj in izvajanje fizičnih, organizacijskih in tehničnih standardov varovanja TP v organih in organizacijah,
  koordinira delovanje organov, pristojnih za varnostno preverjanje,
- pripravlja predloge predpisov s področja TP za vlado Republike Slovenije,
- daje mnenja o skladnosti splošnih aktov organov in organizacij z ZTP na področju obravnavanja in varovanja TP,
- skrbi za izvajanje mednarodnih pogodb in sprejetih mednarodnih obveznosti, ki jih je v zvezi z obravnavanjem in varovanjem TP sklenila ali sprejela Republika Slovenija, ter na tem področju sodeluje z ustreznimi organi tujih držav in mednarodnih organizacij, razen če mednarodna pogodba ne določa drugače, ter
- usklajuje dejavnosti za zagotavljanje varnosti nacionalnih TP v tujini in tujih TP na območju Republike Slovenije.

Varovanje in dostop do tajnih podatkov tuje države ali mednarodne organizacije se izvaja v skladu z Zakonom o tajnih podatkih ali s predpisi, izdanimi na njegovi podlagi, oziroma v skladu z mednarodno pogodbo, ki jo je s tujo državo sklenila Republika Slovenija. Po Zakonu o tajnih podatkih se morajo ravnati tudi dobavitelji, izvajalci gradenj ali izvajalci storitev, katerim se tajni podatki posredujejo zaradi izvedbe naročil organa.

# 5. VARNOSTNA KULTURA IN VAROVANJE TAJNIH PODATKOV

## 5.1. Viri ogrožanja tajnih podatkov

Viri ogrožanja tajnih podatkov so sestavni del širokega spektra ogrožanja vsake države, torej tudi Republike Slovenije. Kotnik - Dvojmoč (2000: 144) ugotavlja, da so v sodobni družbi povsem drugačni, kot so bili v preteklosti. Delujejo nekako abstraktno in oddaljeno, saj pogosto ne vemo, koliko je njihovo delovanje (grožnja) res realno in v kolikšni meri je le rezultat percepcije strokovne ali laične dejavnosti. Za percepcijo sta pomembni intenzivnost in časovna opredeljenost določene varnostne grožnje. V razvitih industrijskih družbah se je v zadnjih desetletjih razvijal koncept varnostnih izzivov in varnostnih tveganj, katerega bistvena pozitivna lastnost je v opuščanju tradicionalističnega razmišljanja o neposrednosti in takojšnosti grožnje.
Širše pojem opredeljuje Prezelj (2006: 31), ki pravi, da grožnje nacionalni varnosti po svoji definiciji zajemajo vse družbene ali naravne pojave, ki zmanjšujejo nacionalno varnost oziroma njene definicijske prvine. V tem smislu se grožnje nanašajo na onemogočanje fizičnega obstoja prebivalstva, motenje ali onemogočanje normalnega delovanja temeljnih družbenih in državnih struktur, onemogočanje izvajanja politične suverenosti in preprečevanje relativno nemotenega družbenega razvoja.

Viri ogrožanja so vedno v dvojnem odnosu do oblikovanja varnostne politike države. So del politike države in so dejavnik pritiska ter vplivajo na odločevalce. Hipotetično je mogoče trditi, da je proces odločanja o varnostni politiki determiniran tudi z realnostjo in intenzivnostjo virov ogrožanja (Sotlar, 2000 v Britovšek, 2004: 14). Medtem ko si laična javnost morda še lahko dovoli, da napačno zazna in oceni vire ogrožanja, je veliko bolj nevarno, če se to zgodi subjektom nacionalnovarnostnega sistema (policija, vojska, obveščevalno-varnostne službe), strokovni javnosti (raziskovalni inštituti, univerze in podobno) in tistim, ki odločajo o varnostni politiki, to je vladi in parlamentu (Heywood, 1997: 77–78 v Britovšek, 2004: 14).
Vrste ogrožanja lahko razdelimo v tri skupine:

- vojaška ogrožanja (predvsem v vojnem stanju, ko celotna država predstavlja vojaške cilje, še posebej pa njene oblastne institucije),

- notranjevarnostna ogrožanja (kriminal – vlom, tatvina, rop, fizični napad na varovano osebo, terorizem, zajetje talcev, nastavitev eksplozivnega sredstva, vdor v informacijski sistem, množične kršitve javnega reda, hujše kršitve hišnega reda),
- ogrožanja zaradi naravnih in drugih nesreč (ekološke nesreče, poplava, potres, požar) (Dobovšek, 2004).

Strateško varnostno okolje Republike Slovenije se zaradi procesa globalizacije, razvoja informacijske družbe, hitrega razvoja azijskih trgov, katastrofalnih življenjskih razmer v državah tretjega sveta, okoljskih sprememb in drugih vzrokov vse hitreje spreminja. Nestabilnost, grožnje in tveganja, ki iz tega izhajajo, predstavljajo glavni izziv globalne varnosti, s tem pa tudi varnosti Republike Slovenije. Pomen klasičnih vojaških groženj se sicer zmanjšuje, dolgoročno pa jih tudi ni mogoče povsem izključiti.
Klasične vojaške oblike ogrožanja Republike Slovenije vse bolj nadomeščajo moderne oblike ogrožanja varnosti. Med temi so najpogostejše mednarodni terorizem, ilegalne migracije, organizirani kriminal, trgovina z mamili in belim blagom, ekstremizem, različna etnična gibanja, verski fanatizem, okoljski problemi, nenadzorovana proizvodnja nevarnih bioloških, kemičnih in jedrskih snovi in njihova vse večja dostopnost ter zloraba interneta. Glavne značilnosti naštetih groženj so asimetričnost delovanja, kompleksnost, transnacionalni značaj, raznovrstnost in nedoločljivost struktur, vse večja stopnja organiziranosti nevarnih družbenih skupin ter njihova spretnost v uporabi sodobnih komunikacij. Nekatere hujše oblike navedenih groženj lahko v temeljih zamajejo stabilnost celih držav. Ohranjanje revščine in katastrofalnih življenjskih razmer v precejšnjem delu sveta ostajata glavna vzroka in generatorja večine naštetih groženj (Koncept VOD SV, 2005: 6–7).

Varnostno okolje Republike Slovenije je dinamično in spremenljivo ter je neločljivo povezano z negotovostjo in nestabilnostjo v državah znotraj in zunaj evroatlantskega območja. Nekatere države so soočene z resnimi ekonomskimi, družbenimi in političnimi težavami. Na regionalno nestabilnost lahko vplivajo etnična in verska nasprotja, teritorialni spori, humanitarne katastrofe, neustrezne ali neuspešne ekonomske ali politične reforme, neurejeni odnosi med novimi državami, zlorabe človekovih pravic ter razpad političnega sistema držav. Pojavne oblike organiziranega kriminala so številne in so vzporedna negativna posledica globalizacije. Republika Slovenija je prehodna in ciljna država

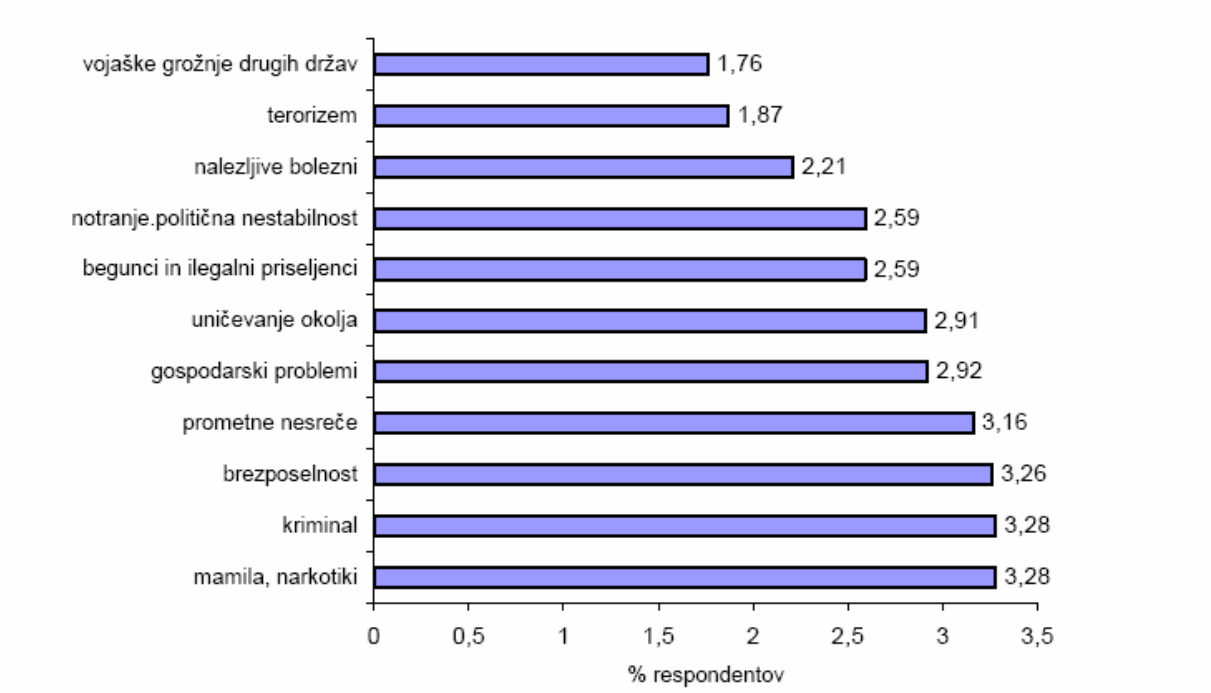
predvsem na tako imenovani balkanski poti ilegalnih migracij, trgovine z mamili, belim blagom in nezakonitim trgovanjem ter oboroževanjem s konvencionalnim orožjem.

Na splošno raven varnosti Republike Slovenije vplivajo vse pojavne oblike kriminalitete, zlasti splošna in gospodarska kriminaliteta, migracije, rasno, etnično in religiozno motivirana dejanja, protiglobalistična in druga ekstremna gibanja in organizacije ter obveščevalno delovanje proti Republiki Sloveniji. Republika Slovenija kot razvita informacijska družba postaja vse bolj ranljiva tudi na komunikacijsko-informacijskem področju. Sooča se z različnimi tveganji, ki ogrožajo varnost kritične infrastrukture na tem področju.

Naravne in druge nesreče ostajajo stalen vir ogrožanja. Intenzivnost in pogostnost nekaterih vrst naravnih nesreč se povečujeta kot posledica verjetnih podnebnih sprememb. Povečujejo se okoljski viri ogrožanja, kar vse vpliva na večjo možnost in pogostnost ekoloških ter drugih nesreč v okolju, ki jih povzroča človek s svojo dejavnostjo (Vojaška doktrina, 2006: 11–12).

V zvezi z viri ogrožanja je bila v Sloveniji izvedena javnomnenjska raziskava z naslovom Nacionalna in mednarodna varnost 2003, ki jo je izvedel Obramboslovni raziskovalni center FDV-IDV).

Slika 5.1: Dejavniki ogrožanja varnosti Slovenije




Vir: (2003) ORC, FDV-IDV (http://nato.gov,si/slo/javnomnenje/nacionalna -varnost.pdf ).

Analiza rezultatov pokaže, da grožnje, ki v svetu prevladujejo, in sicer terorizem, notranjepolitična nestabilnost in vojaško ogrožanje drugih držav, sodijo pri nas med najmanj zaznane dejavnike ogrožanja varnosti. Na prvem mestu so mamila in kriminal.
Čeprav so to podatki pretežno laične javnosti, predstavljajo določen odraz stanja v družbi in lahko služijo kot izhodišče ocenjevanja groženj varovanja podatkov, ki je izvedeno predvsem zaradi poznejšega zoperstavljanja grožnjam in vzpostavljanja varnostnih mehanizmov.

Tabela 5.1: Občutek varnosti prebivalcev Slovenije

| **Če razmišljate o trenutnem družbenem in političnem položaju, ali se na splošno počutite varno ali ogroženo?** | **SJM 2001/3** | **SJM 2003/3** | **SJM 2005/2** |
|---|---|---|---|
| **Varno** | **71,9** | **81,8** | **81,8** |
| **Ogroženo** | **10,9** | **13,8** | **9,4** |
| **Ne vem, ne morem oceniti** | **17,2** | **4,3** | **8,8** |

Vir: Raziskava Stališča o nacionalni in mednarodni varnosti, slovensko javno mnenje 2005/2.
Tabela prikazuje analizo občutka varnosti slovenskega prebivalstva v treh različnih obdobjih od leta 2001 do 2005. Opaziti je, da se je občutek varnosti pri prebivalstvu v zadnjih nekaj letih povečal, saj se je leta 2001 varno počutilo 71,9 odstotka prebivalstva, leta 2003 in 2005 pa kar 81,8 odstotka. Hkrati je tudi vedno manjši delež prebivalstva, ki se počuti ogroženo (13,8 odstotka leta 2003 in 9,4 odstotka leta 2005) (Brezovšek, Haček, 2006: 49).

Ali bi lahko glede na raziskave, ki so bile opravljene v Sloveniji in katerih del rezultatov sem predstavil, trdili, da tajni podatki na obrambnem področju in v Slovenski vojski niso ogroženi? Morda bi lahko odgovorili pritrdilno, če podatki, ki se varujejo, ne bi predstavljali temeljnih dokumentov s področja obrambe in drugih pomembnih področij zagotavljanja nacionalnovarnostnega sistema Republike Slovenije.

Že zaradi same vloge in položaja obveščevalno-varnostnih služb v sistemu državne ureditve, njihovih metod dela ter pričakovanja odločevalcev, da službe pridobijo tajne podatke, lahko trdim, da so tajni podatki na obrambnem področju in v Slovenski vojski zaradi tega ogroženi. Tuje obveščevalne službe ne zanimajo le nacionalni, ampak tudi tajni

podatki organizacij, katerih članica je Republika Slovenija. Poleg obveščevalnih služb lahko med možne vire ogrožanja tajnih podatkov uvrščamo še naslednje:

- zaposlene,
- privatne detektivske oziroma vohunske organizacije,
- hekerje.

Največjo nevarnost izdaje določenih tajnih podatkov predstavljajo razočarani in nezadovoljni zaposleni. Kot zaposleni imajo direkten dostop do informacij in določenih podatkov, ki jih lahko iz nagibov, ki so bili opisani v predhodnih poglavjih, posredujejo naročniku. Veliko nevarnost izdaje podatkov predstavljajo tudi osebe ob zamenjavi zaposlitve, saj v dobi sodobne informacijske tehnologije ni treba prekopirati dokumentov, temveč jih preprosto odnesejo na izmenljivih nosilcih.

Omenjene osebe lahko podatke izdajo namerno ali slučajno. Osebno menim, da je večje število izdaje določenih podatkov slučajno, predvsem zaradi neprevidnosti, neprofesionalnega ravnanja ter neupoštevanja določenih pravil in predpisov. O slučajni izdaji določenih podatkov lahko govorimo tudi takrat, ko nepooblaščene osebe komunicirajo z mediji ter niso predhodno pripravljene. Z izjavo lahko povzročijo negativen vpliv, krnijo ugled organizacije in/ali države ter zaradi tega povzročijo, da se zanje začnejo zanimati organizacije in posamezniki, ki se ukvarjajo z zbiranjem določenih podatkov. Njihovo ravnanje pa ima lahko tudi pozitiven vpliv na organe, ki se ukvarjajo z varnostjo, saj lahko na podlagi povzročene škode predpišejo in izvajajo določene preventivne oziroma represivne ukrepe.

Število detektivskih oziroma privatnih vohunskih organizacij v svetu nenehno narašča. Njihova značilnost je predvsem ta, da so v njih večinoma zaposleni upokojeni delavci obveščevalnih služb. Njihova dejavnost je usmerjena predvsem v svetovanje s področja varnosti in varovanja, vendar pa za posamezne naročnike zbirajo tudi pomembne oziroma skrbno varovane, torej tajne podatke. Za izvajanje svoje dejavnosti praviloma uporabljajo metode zbiranja podatkov iz javnih virov, med njimi pa so tudi organizacije, ki uporabljajo skrivne (tajne) metode zbiranja podatkov (Schmid, 2001).

Hekerji kot računalniški specialisti so pomembna podpora obveščevalno-varnostnih in tudi drugih organizacij, ki se ukvarjajo s pridobivanjem podatkov. Pred desetletjem so se

ukvarjali predvsem z vdori v računalniška omrežja, sedaj pa so nepogrešljiv člen, s pomočjo katerega nekatere obveščevalno-varnostne službe zbirajo določene podatke ali pa jih ščitijo. Hekerji so lahko v omenjenih organizacijah zaposleni ali pa se za izvedbo določene naloge najamejo (Schmid, 2001).

V Nemčiji je bila leta 1995 izvedena analiza o gospodarskem vohunstvu. Njeni rezultati so lahko uporabni tudi danes. Raziskovalci so takrat ugotovili, da se z zbiranjem podatkov ukvarjajo konkurenčne organizacije ter predstavljajo 39-odstotni delež zbranih informacij, sledijo jim stranke, ki zberejo 19 odstotkov želenih informacij, 9 odstotkov informacij zberejo dobavitelji ter 7 odstotkov obveščevalne službe (Schmid, 2001). Menim, da je analiza uporabna tudi za obrambno področje in Slovensko vojsko. V miru smo logistično odvisni od civilnih podjetij, ki izvajajo določene usluge. Čeprav morajo biti vse organizacije in njihovi zaposleni, ki sodelujejo z obrambnim področjem, varnostno preverjeni ter morajo ustrezati določenim kriterijem (imeti morajo pozitivno varnostno mnenje), menim, da je njihove dejavnosti izredno težko nadzirati. Zaradi tega je treba tudi omenjeno kategorijo uvrščati med možne vire ogrožanja varnosti tajnih podatkov.

Tajni podatki na obrambnem področju in v Slovenski vojski so večinoma ogroženi z viri, ki so opisani. Glede na opravljene analize znanih primerov ogrožanja lahko trdim, da so prvi vir ogrožanja tajnih podatkov tuje obveščevalne službe, kar je bilo posebej izrazito v letih 2003 in 2004, ko se je Republika Slovenija intenzivno pripravljala na vključitev v Evropsko skupnost in zvezo NATO. V tem obdobju je bilo njihovo zanimanje usmerjeno predvsem v organizacijo varovanja, angažiranost posameznikov pri varovanju ter načine prenosa tajnih podatkov. Ugotovljen je bil tudi obveščevalni interes tujih državljanov v podjetju s sklenjeno partnersko pogodbo z MORS (na podlagi neutemeljenih zahtev so bili posredovani tajni podatki).
Stalnica ogrožanja tajnih podatkov pa so tudi zaposleni, ki do teh podatkov dostopajo. V enakem obdobju je bilo kar nekaj kršitev, ki jih lahko pripišemo neupoštevanju predpisov oziroma nizki varnostni kulturi. Tako so bili odtujeni tajni podatki stopnje INTERNO, bilo pa je tudi kar nekaj neupravičenih dostopov do tajnih podatkov brez upoštevanja določila »need to know«. Vseskozi pa je prisotno tudi povečano zanimanje pripadnikov tujih oboroženih sil za pripadnike Slovenske vojske, ki so v tujini ali v tujino potujejo in imajo veljavno dovoljenje za dostopanje do tajnih podatkov.

## 5.2. Varnostna kultura pri varovanju tajnih podatkov

Opravljene študije prikazujejo, da sta obnašanje in ravnanje sodelavcev največja ovira za učinkovito zaščito podatkov. Kljub vsemu je še vedno relativno malo organizacij, ki so usmerjene v izobraževanje svojih zaposlenih. Če želimo, da bo varnost podatkov zadovoljiva, mora človek kot uporabnik informacij in informacijske tehnologije postati odgovornejši. Le s celostnim obravnavanjem tehničnih, organizacijskih in človeških vidikov bo določen podatek učinkovito zaščiten pred nepooblaščenim dostopom.
Nekateri trdijo, da kar 80 odstotkov vseh varnostnih dogodkov, ki so povezani z varovanjem podatkov, povzroči človek, le 20 odstotkov pa je takih, ki jih povzroči odpoved tehničnih sredstev. Če si pogledamo preprost primer, lahko s pomočjo požarnega zidu ali antivirusnega programa računalnik zaščitimo pred znanimi napadi, medtem ko lahko človek opazi najmanjšo nedoslednost, ki jo stori nekdo, ki želi odtujiti določene podatke. Njegovo ravnanje je lahko usmerjeno v preprečitev in izvajanje protiukrepov, ki so potrebni za odvrnitev grožnje. Kombinacija tehničnih sredstev in ustreznega ravnanja ljudi lahko potencialno dvigne stopnjo varnosti v organizaciji na zadovoljivo raven.

Pojmovanje varnostne kulture je sorazmerno mlada veda, katere preučevanje se je temeljiteje začelo v zadnjih desetletjih. Velike družbene spremembe, v katerih potekajo varnostni dogodki, povzročajo, da se v družbi in organizaciji pojavlja strah, ki je posledica subjektov ogrožanja. Varnostna kultura kot preventivna dejavnost je usmerjena v odvračanje, preprečevanje določenih oblik ogrožanja, ki lahko povzročijo ter izzovejo manjšo ali večjo škodo posamezniku, organizaciji ali državi.
Znanstveno raziskovanje varnostne kulture je obsežen raziskovalni projekt, ki postaja izziv raziskovalcem. Varnostna kultura je del splošne kulture posameznika, družbene skupine in tudi določene organizacije. Kadar je govor o varnostni kulturi, je mogoče zaslediti pojme, ki so izvedeni iz osnovnega pojma; tako lahko govorimo o jedrski, zdravstveni, prometni, politični, vojaški varnostni kulturi.

Varnostno kulturo lahko definiramo kot skupek stališč, znanj, veščin ter pravil s področja varnosti, ki se odražajo kot obnašanje in proces o potrebi, načinih in sredstvih zaščite osebnih, družbenih in mednarodnih vrednot pred izvori in oblikami ter nosilci ogrožanja, ne glede na mesto ali čas delovanja (Stajić, 2005: 35). Iz definicije je mogoče zaključiti, da

je varnostna kultura del vsakodnevnega dela (obnašanje, proces) kakor tudi metoda, s katero se sistem varnosti s pomočjo raznih sredstev zoperstavlja virom ogrožanja.
Ugotavljam, da varnostna kultura lahko pomeni zavest o nepogrešljivosti neprekinjenega, samoiniciativnega in zavestnega izvajanja varnosti, z namenom zaščite določenih vrednosti na moralen in zakonit način (Stajić, 2005). Da bi lahko izgrajevali varnostno kulturo, moramo upoštevati naslednja njena načela:

- načelo moralnosti,
- načelo zakonitosti,
- načelo doslednosti,
- načelo odgovornosti,
- načelo neprekinjenosti ter
- načelo pravočasnosti.

Opredeliti bom poskušal načela, za katera menim, da so pomembna pri varovanju podatkov tako za organe, ki zagotavljajo varnost, kakor tudi za posameznike, ki do tajnih podatkov dostopajo.

**Načelo zakonitosti**, obveza in pravica posameznikov kakor tudi OVS in J/G/S-2 (v nadaljnjem besedilu: organov), ki se ukvarjajo z zagotavljanjem varnosti, je zagotavljati varnost podatkov ter izvajati ukrepe za njihovo zaščito. Pri tem je bistvenega pomena uporaba pooblastil organov, ki so lahko uporabljena samo v skladu z določili zakonodaje. Pri uporabi pooblastil lahko govorimo o pravici in dolžnosti organov, da uporabijo ukrepe, izvajajo določene postopke ter pri tem uporabljajo zakonita sredstva proti virom ogrožanja. Da lahko govorimo o ustrezni varnostni kulturi teh organov, je bistvenega pomena, da so vsa dejanja, ki jih izvajajo, v skladu z zakonodajo. Z zakoni in drugimi internimi akti so predpisani dolžnosti in pravila posameznikov. Njihovo varnostno kulturo je mogoče ocenjevati predvsem z njihovim ravnanjem in obnašanjem v določeni situaciji. Večina posameznikov ravna v skladu z zakonodajo, torej je njihova varnostna kultura na zadovoljivi ravni, pri nekaterih posameznikih pa je nekoliko nižja. Če ocenjujemo varnostno kulturo, lahko z gotovostjo trdimo, da ni nikogar, ki je brez nje, razlika med posamezniki je v tem, da je pri nekaterih raven varnostne kulture nižja kakor pri drugih. Načelo zakonitosti v povezavi z varnostno kulturo torej pomeni, da je treba izvajati ukrepe, izobraževanja in usposabljanja z namenom vplivati na vse subjekte, ki se ukvarjajo s tajnimi podatki, da bodo vse postopke izvajali na podlagi veljavne zakonodaje. Hkrati pa

morajo organi, ki se ukvarjajo z zagotavljanjem varnosti, preventivno ali represivno delovati zoper kršitelje.

**Načelo odgovornosti** pri izgrajevanju varnostne kulture posameznikov je bistveno predvsem zaradi njihove sposobnosti, da sami prepoznajo grožnje ter nanje samoiniciativno odgovorijo. Zavesten odnos posameznikov do varovanja podatkov ter njihova odgovornost sta indikator razvitosti morale v organizaciji. Visoko razvita morala in samozavest razvijata visoko odgovornost posameznika, kar zagotavlja primeren odnos posameznika do varovanja določenih podatkov. Pri tem je treba omeniti tudi nepisano pravilo, ki velja v večini organizacij, da so starejši izkušeni zaposleni odgovorni za uvajanje novozaposlenih. Njihova vloga je predvsem v usmerjanju, vodenju ter izgrajevanju primernega odnosa do upoštevanja pravil in zakonitosti, ki v organizaciji veljajo. Posledično je njihovo ravnanje usmerjeno v izgrajevanje varnostne kulture in spoštovanja določil varnosti. Ko govorimo o organih, ki zagotavljajo varnost, je njihova odgovornost predvsem zakonska, torej zavestno izvajati poslanstvo. Njihova odgovornost se kaže v strokovnem, kvalitetnem in odgovornem izvajanju vseh predpisanih obveznosti, brez katerih sistem varnosti ne bi zagotavljal določene stopnje varovanja. S svojo prisotnostjo zagotavljajo dvig varnostne kulture, svetujejo ob varnostnih problemih ter skrbijo za spremembe postopkov in predpisov.

**Načelo neprekinjenosti** pomeni, da je treba stalno izvajati določene postopke, z namenom zagotavljati »želeno« varnost. Želeno stanje je mogoče doseči z varnostnimi ukrepi, ki se stalno izvajajo in nenehno dopolnjujejo glede na vire ogrožanja. Vloga zaposlenih je zagotavljati neprekinjeno pripravljenost oziroma izvajati varovanje posebno pomembnih prostorov. To lahko dosežemo s fizičnim ali tehničnim varovanjem ali kombinacijo obeh. Pripadniki organov varnosti funkcijo neprekinjenosti izvajajo na način, da se nenehno izobražujejo in usposabljajo s področja zakonodaje, spremljajo varnostno dogajanje v okolici glede na vire ogrožanja, izdelujejo ocene ogroženosti ter skrbijo, da se postopki varovanja izvajajo v skladu z elaborati. Osnova uspešnega zoperstavljanja ogrožanju je stalno spremljanje stanja varnosti ter varnostne problematike.

**Načelo pravočasnosti**. Lahko rečemo, da so varovani podatki občutljivi za nekatere oblike ogrožanja. Cilj virov ogrožanja je preučiti slabosti sistema varovanja kakor tudi slabosti zaposlenih, ki z njimi ravnajo. Bistvo načela pravočasnosti je v odkrivanju in zmanjševanju

ter izvajanju pravočasnih dejavnosti za zaščito varovanih prostorov, dokumentov ali zaposlenih. Da se izognemo ogrožanju, izvajamo preventivne in represivne ukrepe. Ti ukrepi so pretežno usmerjeni k izvorom, oblikam in virom ogrožanja varnosti. Zaposleni bi morali preventivno, in če je mogoče, tudi represivno odgovoriti na določeno grožnjo. Njihovo varnostno kulturo je mogoče opredeliti kot visoko, če znajo pravočasno odreagirati, tako da sočasno z izvajanjem drugih varnostnih ukrepov obvestijo tudi organ, ki je odgovoren za varnost. Organi varnosti morajo nenehno opravljati svojo funkcijo varnosti, tako da spremljajo in ocenjujejo stanje varnosti. Z zbiranjem varnostnoobveščevalnih podatkov ter njihovo obdelavo in interpretacijo določajo vire ogrožanja in izdelujejo ocene možnega razvoja ogrožanja varnosti (Stajić, 2005: 55–72).

Medtem pa varnostna in obrambna kultura v ožjem pomenu posega na področje organizacijske in politične kulture oziroma je njen sestavni del in obsega vsebine, kot so lojalnost, verodostojnost, pripadnost, zaupanje, varovanje tajnosti, zanesljivost itn. Varnostno in obrambno kulturo merimo na čustveni, spoznavni in vrednostni ravni ter na ravni aktivne udeležbe v obrambnih in varnostnih procesih okolja, pri čemer upoštevamo klasično opredelitev politične kulture (Almond in Verba, 1965 v Brezovšek, Haček, 2006: 44).

Če v organizacijah, ki so bistvene na področju zagotavljanja nacionalne varnosti, ni jasno postavljenega vrednostnega sistema, občutka pripadnosti in ustrezne organizacijske, varnostne ter obrambne kulture, lahko trdimo, da je delovanje nacionalnovarnostnega sistema oziroma opravljanje njegove primarne vloge vprašljivo (Brezovšek, Haček, 2006: 44).

Temelj vsake organizacije je organizacijska kultura, ki se posebej odraža v organizacijah, v katerih so varnost in dejavnosti, povezane z njo, temeljnega pomena. Obrambno področje kot del nacionalnovarnostnega sistema karakterizirata vsebina in način delovanja kar je posebej izrazito v organih, ki se ukvarjajo s protiobveščevalno in varnostno dejavnostjo. Torej lahko govorimo, da je njihova značilnost kompleksnost glede vsebine dela kakor tudi organiziranost.

## 5.3. Varovanje tajnih podatkov in organizacijska kultura na obrambnem področju in v Slovenski vojski

Univerzalna definicija organizacije ne obstaja. Organizacijo lahko definiramo kot združbo ljudi, ki delujejo zaradi uresničevanja skupnega cilja ali več ciljev (več o tem Lipovec, 1987: 15–38), kot tudi kot relativno celoto (več o tem Kavčič, 1991: 13–24), ki je sestavljena iz delov in odnosov med deli ter je jasno razmejena z okoljem.
Kavčič pojasnjuje, da je pojav v menedžerski literaturi in organizacijski teoriji sicer znan že več kot pol stoletja. Nekateri avtorji so že sredi prejšnjega stoletja našteli več kot 160 različnih definicij organizacijske kulture. To dokazuje, da tudi strokovnjaki, ki se ukvarjajo z organizacijsko kulturo, (še) niso soglasni glede pomena tega pojma. To pa seveda ne pomeni, da gre za nepomemben pojav v organizaciji.

Organizacijska kultura je splet miselnih modelov ali skupnih paradigem v organizaciji o tem, kako svet deluje ali naj bi deloval. Govorimo o zaznavah, vrednotah, načelih, prepričanjih, simbolnem vedenju in obredih članov organizacije, ki jim predstavljajo izhodišče za oblikovanje organizirane kompleksnosti (Ovsenik in Ambrož, 2000: 148). Drugi avtorji kot sestavine organizacijske kulture navajajo: vrednote, norme, tipične obrazce vedenja, vzornike, običaje in obrede, komunikacije, proizvode in storitve. Pagon (2004) poudarja, da organizacijsko kulturo določene organizacije krasi zelo širok spekter socialnih pojavov, med katere uvršča tipični način oblačenja, jezik, vedenje, vrednote, statusne simbole in avtoriteto, mite, obrede in slovesnosti, način upoštevanja drugih in razdiralne oblike ravnanja. Večina naštetih pojavov karakterizira tako področje obrambe kakor tudi subjekta, ki se ukvarjata z zagotavljanjem varnosti in določenimi dejavnostmi pri varovanju podatkov.

V teoriji se srečujemo s tremi ravnmi organizacijske kulture, ki so medsebojno povezane in v nenehni interakciji. Te ravni so: fizični svet, vrednote in norme ter temeljne predpostavke in prepričanja. Organizacijsko kulturo lahko opredelimo kot kolektivni fenomen, ki ima v sebi določene subkulture. Subkultura opredeljuje določeno skupino ljudi. Na obrambnem področju in v Slovenski vojski lahko eno izmed subkultur sestavljajo zaposleni, ki dostopajo do tajnih podatkov, drugo pa organi varnosti, ki z izvajanjem določenih ukrepov in postopkov skrbijo, da ti podatki ostanejo prikriti. Menim, da lahko govorimo, da varnostno kulturo obojih opredeljujejo enaka načela, vendar pa se pojavljajo razlike pri

zagotavljanju varnosti in izgrajevanju varnostne kulture. Enoten je tudi cilj obeh omenjenih subjektov, to je ohraniti tajnost podatkov, pravočasno zaznati ogrožanje ter pravilno ravnati. Da bi lahko izgradili ustrezno varnost podatkov, morajo sodelovati vsi subjekti na vseh ravneh, pri čemer ima seveda sleherni od njih svojo vlogo. Varnostno kulturo torej lahko povezujemo z organizacijsko kulturo ter jo opredelimo kot del organizacijske kulture. Zaradi tega varnostna kultura podpira dnevne dejavnosti zaposlenih, da ravnajo v skladu s pravili, s tem pa postaja potreba po zaščiti informacij njihova vsakodnevna obveznost. V nadaljevanju bi želel poudariti pomembne elemente vsake ravni, ki lahko pripomorejo k varovanju tajnih podatkov.

### 5.3.1. Materializirana raven

Temelj vsake organizacije je fizično okolje (stavbe, prostori, oprema ipd.), kjer organizacija deluje. Za fizični svet je značilno, da je dobro viden, vendar ne vedno in nujno dobro in do konca razumljen. Osnovni element organizacijske kulture sestavljajo tako fizični objekti v okolju kot vidni in slušni vedenjski vzorci (Pagon, 2004).

To je vidna raven organizacijske kulture, ki temelji na ponavljajočih se vzorcih vedenja, obredih, standardnih postopkih in navodilih, na zgodbah, izročilih, pisnih dokumentih, simbolih, tehnologiji, zgradbah, arhitekturi, opremi, načinu oblačenja (Ovsenik, Ambrož, 2000: 151).

Področje vidne ravni je zelo pomembno za poslovanje s tajnimi podatki, saj velja mnogo pravil, omejitev ter posebnih standardov, ki ustvarjajo specifičnost omenjenega okolja. V prvi vrsti velja pri tem omeniti zgradbe, opremo in postopke, ki so večinoma standardizirani.

Zgradbe same po sebi v okolju ne izstopajo, posebna pa je njihova notranjost, saj se v teh zgradbah izvajajo določeni varnostni ukrepi ob vstopu in med gibanjem zaposlenih in drugih oseb. Gibanje oseb je večinoma pod nadzorom ter se izvaja s spremstvom. Prostori so opremljeni s tehničnimi sredstvi, ki zagotavljajo nadzor nad gibanjem in nudijo določeno varnost dokumentom in opremi, ki se v njih uporabljajo.

Večina postopkov, ki jih izvajajo zaposleni, je standardiziranih. Posebej natančno so opredeljeni postopki, ki jih zaposleni izvajajo pri ravnanju s tajnimi podatki. Področje je urejeno z določenimi omejitvami, ki izhajajo iz veljavne zakonodaje, urejeno pa je tudi sankcioniranje v primeru kršitev. Pri izdelavi dokumentov in prenosu se uporablja

prilagojena informacijska in komunikacijska oprema, prenos se izvaja po zaščitenih komunikacijah.

Glede na opisano je mogoče dokaj hitro ugotoviti, da je fizični svet, v katerem delujejo zaposleni na obrambnem področju in v SV, drugačen, saj ustvarja občutek drugačnosti in omejuje svobodo. Kljub vsemu pa naj bi zaščita podatkov postala sestavni del dnevnega življenja zaposlenih na obrambnem področju. Sodelavce moramo obravnavati kot partnerje pri zagotavljanju varnosti, čeprav so velikokrat obravnavani le kot varnostno tveganje. Kljub določenim varnostnim ukrepom in izgrajevanju varnostne kulture ni mogoče vsem osebam popolnoma zaupati. Vedno obstaja določeno tveganje, ki ga lahko omejimo z uvajanjem novih tehničnih rešitev oziroma organizacijskih rešitev. Kljub vsemu pa nikoli ni mogoče zagotoviti popolne varnosti, saj večina ljudi ne razume fizičnega sveta enako. Pagon (2004) pravi, da si moramo pri razumevanju fizičnega sveta pomagati z analizo vrednot in norm, ki v konkretnem okolju veljajo.

### 5.3.2. Vrednote in norme

Vrednote, ki jih imajo zaposleni na obrambnem področju, se nekoliko razlikujejo od vrednot, ki karakterizirajo vrednote širše populacije. Z gotovostjo lahko trdim, da obstajajo specifične vrednote, ki v nekaterih drugih organizacijah niso tako pogoste oziroma niso razvite do tolikšne mere kot na obrambnem področju.
Privzete vrednote, ki običajno izražajo pričakovanja organizacije, zlasti vodstva, so osnova za njeno pričakovano skupno podobo. Oblikujejo jo vrednote, prepričanja, načela in drugi miselni modeli, ki so posledica opazovanja okolja. So zlasti podlaga za načine reševanja problemov v organizaciji (Ovsenik, Ambrož, 2000: 151).

Vrednote Slovenske vojske so gonilna sila uresničevanja poslanstva Slovenske vojske. Izhajajo iz splošnih civilizacijskih vrednot, vrednot slovenske družbe in posebnosti narave delovanja vojske. Vrednote Slovenske vojske dajejo okvire za delovanje in vedenje posameznikov samostojno in v skupini. Temeljna skupna vrednota pripadnikov Slovenske vojske je domoljubje. Domoljubje je zavest pripadnosti domovini Sloveniji in nesebično opravljanje dolžnosti pri uresničevanju skupnih ciljev.
Ena izmed vrednot je tudi lojalnost Republiki Sloveniji, Slovenski vojski in enoti ter povezuje pripadnike Slovenske vojske med seboj. Lojalnost Slovenski vojski pripadniku enote narekuje skrb za njeno učinkovitost. Lojalnost slovenski državi mu narekuje skrb za

zaščito njenih interesov in krepitev ugleda v svetu. Lojalnost podrejenih do svojih nadrejenih je sestavni del lojalnosti vojaški organizaciji. Podrejeni so lojalni do nadrejenih tako, da izvajajo povelja, ki uresničujejo poslanstvo Slovenske vojske in podpirajo interese Republike Slovenije. Lojalnost se izraža z medsebojnim zaupanjem in spoštovanjem ter disciplinirani m in odgovornim opravljanjem dolžnosti (Vojaška doktrina, 2006: 17–19).

Vrednote gotovo zasedajo zelo pomembno mesto v organizacijski kulturi vsake organizacije. Kot pravi Pagon (Pleteršek 2006: 29), so vrednote v središču vsake organizacije, še zlasti to velja za nepridobitne organizacije. Sprejete vrednote pomenijo tista načela in vrednote, ki jih organizacija skuša uresničiti.

Lojalnost kot temeljna vrednota na obrambnem področju in v Slovenski vojski je pomembna predvsem z vidika dostopanja do tajnih podatkov in njihovega obravnavanja. Vrednota je pomembna za zaposlene, ki dostopajo do tajnih podatkov ter morajo zaradi tega biti varnostno preverjeni. Ob izvedbi varnostnega preverjanja zaposlenih je prav lojalnost eden izmed najpomembnejših kriterijev, s pomočjo katerega se omogoča, da lahko zaposleni dostopa do tajnih podatkov oziroma posluje z njimi.

Znova se potrjuje, da je najpomembnejši faktor človek, uslužbenec organa javne oziroma državne uprave. Pomembni so odnosi med zaposlenimi, nadrejenim in podrejenimi, stopnja politične, organizacijske in varnostne kulture, občutek pripadnosti organizaciji, lojalnost in ne nazadnje seznanjenost s tem, kako ravnati. To so ključne determinante, ki prispevajo k temu, da bo nedovoljenega sporočanja tajnosti čim manj oziroma nič (Brezovšek, Črnčec, 2004: 516).

Vrednote se udejanjajo s standardi vedenja v Slovenski vojski, za katere se njeni pripadniki zavzemajo in ki jih cenijo, ter se poučujejo na vseh ravneh izobraževanja in usposabljanja. Vrednote niso le seznam kvalitet, ki jih dosega posameznik, temveč skupna odgovornost Slovenske vojske in vsake enote. Uveljavljajo in krepijo se z voditeljstvom in usposabljanjem. Vsi pripadniki Slovenske vojske z osebnim zgledom in ravnanjem uveljavljajo njene vrednote, nadrejeni pa skrbijo, da jih podrejeni upoštevajo pri svojem delu (Vojaška doktrina, 2006: 18).

### 5.3.3. Zavestna raven delovanja organizacijske kulture

Sestavljajo jo temeljne predpostavke o tem, kako svet dejansko deluje. Temeljne predpostavke ali paradigme so nezavedna raven delovanja, ki je podlaga konkretnemu vedenju pod vplivom okoliščin, in so izid stalne interakcije z okoljem (Ovsenik, Ambrož, 2000: 151). Gre za predpostavke, o katerih se posamezniki v organizaciji ne sprašujejo, so nevidne in delujejo na podzavedni ravni. Temeljne predpostavke so za člane organizacije same po sebi umevne in nastanejo na podlagi kulturnih paradigem, ki so v konsistenten vzorec povezane predpostavke o človeštvu, naravi, načinu delovanja. Iz njih izvirajo tudi posameznikova prepričanja oziroma posameznikove ideje o tem, kako svet dejansko deluje. Zasnovane so na osebni izkušnji ter izkušnjah, ki jih ima posameznik s pomembnimi drugimi, saj mnenje pomembnih drugih vpliva na razvoj posameznikovih prepričanj (Pagon, 2004).

Zaradi naštetega je to raven organizacijske kulture, na katero ima organizacija najmanjši vpliv, mogoče je celo trditi, da ga skoraj nima. V organizaciji so zaposleni ljudje, ki imajo svoja prepričanja bolj ali manj izgrajena. Bistvenejše kot izgrajevanje prepričanj je za organizacijo ugotavljanje prepričanj pred vstopom vanjo.

## 5.4. Subjekti zagotavljanja varovanja tajnih podatkov in njihove naloge

V nadaljevanju bom skušal opredeliti subjekte zagotavljanja varovanja podatkov in njihovo vlogo. Med subjekte lahko prištevamo: OVS MORS, organe J/G/S-2, pooblaščene osebe in posameznike oziroma osebe, ki imajo dostop do tajnih podatkov.

### 5.4.1. Obveščevalno-varnostna služba Ministrstva za obrambo

#### 5.4.1.1. Preverjanje oseb po Zakonu o tajnih podatkih

S pomočjo varnostnega preverjanja se ugotavlja primernost posameznika za delo na varnostno občutljivem delovnem mestu ali za ravnanje s tajnimi podatki. Varnostno preverjanje kot splošni preventivni varnostni ukrep se izvaja v Sloveniji od konca leta 2001. Zakon o tajnih podatkih definira varnostno preverjanje oseb kot poizvedbo, ki jo pred izdajo dovoljenja za dostop do tajnih podatkov opravi pristojni organ in katere namen

je zbrati podatke o morebitnih varnostnih zadržkih. Uspešno varnostno preverjanje se zaključi z izdajo dovoljenja za dostop do tajnih podatkov.

Glede na predvideni dostop osebe do podatkov različnih stopenj tajnosti v Ministrstvu za obrambo OVS MORS za zaposlene v Ministrstvu za obrambo in Slovenski vojski ter za osebe, ki bodo pri svojem delu ravnale s tajnimi podatki z obrambnega področja, opravi:

- osnovno varnostno preverjanje (ZAUPNO),
- razširjeno varnostno preverjanje (TAJNO) in
- razširjeno varnostno preverjanje z varnostnim poizvedovanjem (STROGO TAJNO).

Osnovno varnostno preverjanje se opravi tako, da se preverijo posameznikove navedbe v osnovnem vprašalniku ter podatki iz evidenc in drugih zbirk podatkov upravljavcev zbirk osebnih in drugih podatkov, ki se nanašajo na določeno osebo. (Če obstaja sum varnostnega zadržka, se lahko opravi pogovor tudi s tako imenovanimi »referenčnimi osebami«.)

Pri razširjenem varnostnem preverjanju kandidat izpolni še posebni vprašalnik, podatki pa se lahko preverijo pri referenčnih osebah, zgolj ob sumu varnostnega zadržka.

Ob izvajanju razširjenega preverjanja z varnostnim poizvedovanjem po izpolnitvi osnovnega posebnega in prvega dela dodatnega vprašalnika lahko organ samo v primeru suma varnostnega zadržka preveri podatke pri drugih osebah, organih ali organizacijah, ki o preverjani osebi kaj vedo (ZTP-UPB2, 2006, 22.d člen). Ta dikcija omogoča tako imenovano terensko preverjanje.

Zveza NATO in EU ne izvajata varnostnega preverjanja, temveč je to v pristojnosti držav članic. Nacionalno dovoljenje za dostop do tajnih podatkov pa je podlaga za pridobitev potrdila PSC (Personal Security Certificate) za dostop do tajnih podatkov zveze NATO in EU. Nedvomno sta lojalnost (državi, organizaciji) in zanesljivost (na delovnem mestu in zunaj njega) ključna kriterija, na podlagi katerih se ocenjuje, ali je posameznik verodostojen. Dvom o lojalnosti in/ali zanesljivosti predstavlja glavni kriterij pri ocenjevanju varnostnih zadržkov ( Črnčec, 2003b).

#### 5.4.1.2. Dejavnosti na področju fizične in tehnične varnosti

Nacionalni in interni predpisi na področju zagotavljanja varnosti tajnih podatkov na obrambnem področju usmerjajo varnostno dejavnost OVS predvsem na naslednja področja:

- odkrivanje, preiskovanje in preprečevanje ogrožanja varnosti določenih oseb, delovnih mest, objektov in okolišev, ki jih uporabljata MO in SV v državi ali zunaj nje, preučevanje in predlaganje rešitev za sisteme fizičnega in tehničnega varovanja ter po potrebi predlaganje sprememb in dodatnih ukrepov,
- izvajanje rednih in izrednih protiprisluškovalnih pregledov v varnostnih območjih (v nadaljnjem besedilu: VO), naprav in opreme,
- sodelovanje z drugimi organizacijskimi enotami ministrstva pri določanju VO v ministrstvu, v postopkih do izdaje sklepa o določitvi VO (razen za GŠSV),
- vodenje evidenc VO ter ugotavljanje potrebnih finančnih in materialnih sredstev, potrebnih za varovanje TP,
- izdelava usmeritev za izdelavo načrtov varovanja TP v VO v ministrstvu in sodelovanje pri izdelavi predlogov drugih predpisov in splošnih aktov s področja varovanja tajnih podatkov.

Sistemi za varovanje občutljivih informacij (kot so tajni podatki, TP) ali drugih občutljivih materialov slonijo predvsem na naslednjih stebrih:

- varnostna kultura zaposlenih,
- načrtovanje in upravljanje sistema varovanja (načrti varovanja, usposabljanja, vzdrževanje sistema, preverjanja in testiranja, dokumentiranje sprememb …),
- sistem fizičnega varovanja (varnostniki, straža, patrulje, intervencija),
- tehnični podporni sistemi (mehansko varovanje, nadzor in evidentiranje dostopov, protivlomno (PV) varovanje, videonadzor in varnostna osvetlitev, povezave z nadzornimi centri).

Tajni podatki in druga občutljiva oprema ali materiali v MO in SV se s sistemi varovanja varujejo pred nepooblaščenim dostopom, vpogledom, uničenjem, odtujitvijo z namenom vohunstva, sabotaž, vandalizma in podobno. Pri TP se varuje njihovo hranjenje, obdelava in prenašanje v varnostnih območjih (VO), objektih, vozilih in plovilih ….

Primerna kombinacija in izbira metod, tehničnih sredstev in osebja za varovanje objektov in tajnih podatkov v njih mora učinkovito in pravočasno zaznati, ovirati in preprečevati take vdore (povzeto po intranetni strani MORS, 2007).

#### 5.4.1.3. Protiprisluškovalni pregledi

Protiprisluškovalni pregledi se izvajajo kot ena od metod varovanja določenih oseb, delovnih mest in dolžnosti, objektov in okolišev, ki so posebnega pomena za obrambo in varovanja tajnih podatkov.
S protiprisluškovalnimi pregledi se ob uporabi ustreznih metod in pripomočkov v VO (ter napravah in na opremi), v katerih se pogosto zvokovno obdelujejo TP stopnje TAJNO in višje, odkriva prisotnost tehničnih sredstev, načinov ali varnostno šibkih točk, ki bi lahko omogočale pasivni ali aktivni nepooblaščeni odtok ali zajemanje podatkov prek akustičnih, električnih, elektromagnetnih in drugih signalov v območjih, prostorih, vozilih itd., kjer se obdelujejo podatki. Na podlagi ugotovitev se ocenjuje varnostno tveganje in predlagajo potrebni varnostni ukrepi (povzeto po intranetni strani MORS, 2007).

### 5.4.2. Obveščevalno-varnostni organi Slovenske vojske

#### 5.4.2.1 Naloge v zvezi s tajnimi podatki

Najpomembnejše naloge so:

- strokovno usmerjanje ukrepov in dejavnosti na področju varovanja tajnih podatkov,
- oblikovanje in razvoj smernic za uvajanje sistema tehničnega varovanja in strokovno usmerjanje ukrepov na področju postavitve tehničnega varovanja,
- oblikovanje smernic in spremljanje varnosti dokumentov, izvajanje varnostnih postopkov za spremljanje, obdelovanje, prenašanje, določanje stopenj tajnosti, hranjenje in uničevanje tajnih dokumentov,
- izvajanje osnovnega in dopolnilnega usposabljanja za obravnavo in varovanje tajnih podatkov,
- izvajanje notranjega nadzora nad izvajanjem določil ZTP in spoštovanja predpisov internih aktov,
- sodelovanje pri pridobivanju dovoljenj zveze NATO in EU,
- izdelava ocene ogroženosti in načrta varovanja tajnih podatkov,
- posredovanje zahtevkov za izvedbo protiprislušnih pregledov varnostnih območij,

- sodelovanje pri določanju in izvajanju ukrepov s področja zaščite informacijsko telekomunikacijske infrastrukture (INFOSEC).

Pri izvajanju preventivne protiobveščevalne in varnostne zaščite tajnih podatkov je treba vso pozornost usmeriti v naslednja področja: kadrovsko, fizično in organizacijsko varnost ter INFOSEC. Pri tem je treba poveljnikom, ki so odgovorni za protioobveščevalno in varnostno delovanje, zagotavljati protiobveščevalne informacije, ki podpirajo učinkovito izvajanje njihovih nalog ter omogočajo izdelavo dokumentov, ki zaposlenim predpisujejo izvajanje preventivnih ukrepov pred ali med obravnavanjem tajnih podatkov.
Osnovni ukrepi so:

- izbor kadra za občutljiva delovna mesta,
  izvajanje nadzora zanesljivosti oseb, ki imajo dostop do tajnih podatkov (varnostno preverjanje daje le podatek na datum izvedbe preverjanja o tem, ali oseba je oziroma ni zanesljiva za obdelovanje tajnih podatkov),
- določitev in vzpostavitev varnostnih območij,
- nadzor nad vstopom v varnostna območja, kjer se hranijo tajni podatki, in prepovedana območja,
- izdelava načrtov varovanja, ki zajemajo varovanje, izredne dogodke in nadzor,
- varnostna usposabljanja, ki zajemajo varnostno situacijo, vire ogrožanja ter veljavne varnostne postopke,
- izvajanje varnostnih vaj, pri katerih se preverja načrt varovanja, itd.

### 5.4.3. Pooblaščene osebe

Pooblaščena oseba določi stopnjo tajnosti podatka ob njegovem nastanku oziroma ob začetku izvajanja naloge organa, katere rezultat bo tajni podatek. Pri določanju stopnje tajnosti mora pooblaščena oseba oceniti možne škodljive posledice za varnost države ali za njene politične ali gospodarske koristi, če bi bil podatek razkrit nepoklicani osebi. Na podlagi te ocene se podatku določi stopnja tajnosti in način prenehanja, nato pa se podatekoznači z oznakami, predpisanimi z zakonom (ZTP-UPB2, 2006, 11. člen).
Pooblaščene osebe na obrambnem področju in v Slovenski vojski so osebe, ki jih določi minister za obrambo. V Slovenski vojski so pooblaščene osebe, ki lahko določajo stopnje tajnosti, poveljniki enot in poveljstev, njihovi namestniki in načelniki štabov v poveljstvih brigad in višje. Poveljnik enote je tudi neposredno odgovoren za izvajanje varnostnih in

protiobveščevalnih ukrepov v enoti. Poveljniki izdajajo povelja, predpisujejo varnostne ukrepe in zagotavljajo standarde varovanja tajnih podatkov. Odgovorni so tudi za izvajanje in napotitev podrejenih na usposabljanja o varovanju tajnih podatkov. Določajo cilje usposabljanja, usmerjajo načrtovanje, organizacijo in izvedbo, vrednotijo različne oblike usposabljanja in ocenjujejo doseženo stopnjo usposobljenosti poveljstva/enote. Določeni deli sistema VIU poveljnikom zagotavljajo pomoč pri izvajanju temeljne naloge in s tem sprejemajo odgovornost nad stopnjo usposobljenosti.

### 5.4.4. Zaposleni

Pravico dostopa do tajnih podatkov imajo samo tiste osebe, ki imajo dovoljenje in se morajo s temi podatki seznaniti zaradi opravljanja funkcije ali delovnih nalog. Dostop imajo samo do tajnih podatkov stopnje tajnosti, določene v dovoljenju (ZTP-UPB2, 2006, 31. člen).
Vse osebe, ki opravljajo funkcijo ali delajo v organu, imajo dostop do tajnih podatkov stopnje INTERNO. Zaposleni z nastopom funkcije oziroma opravljanja dela podpišejo izjavo, da so seznanjeni s tem zakonom in drugimi predpisi, ki urejajo varovanje tajnih podatkov, ki jih bodo obravnavali v okviru izvajanja funkcije oziroma delovnih nalog, in da se zavezujejo s tajnimi podatki ravnati v skladu predpisi (ZTP-UPB2, 2006, 31.a člen).

Dostop do tajnih podatkov je definiran v sistemizaciji vsake organizacijske enote posebej. Pri vsakem delovnem mestu je med pogoji za zasedbo delovnega mesta določena tudi stopnja tajnosti, do katere mora posameznik pridobiti dovoljenje za dostop do tajnih podatkov. Glede na izjavo o seznanjenosti z določili Zakona o tajnih podatkih in predpisih, izdanih na njegovi podlagi, mora posameznik imeti tudi potrdilo o usposobljenosti za varovanje takih podatkov.
Ne glede na določila zakona, se zaposleni na obrambnem področju in v Slovenski vojski seznanjajo z varnostno pomembnimi in občutljivimi informacijami, ki niso označene s stopnjo tajnosti, kar pa ne pomeni, da so prosto dostopne javnosti. Tudi take informacije je treba varovati pred razkritjem. Zaradi tega se od zaposlenih pričakujeta poleg vsega naštetega še visoka stopnja osebne odgovornosti in sposobnost varovanja vseh vrst informacij.
Moralna dolžnost zaposlenih, s katero kažejo lojalnost organizaciji, je tudi ta, da svojemu nadrejenemu sporočijo vse informacije ali vire ogrožanja, ki lahko ogrozijo organizacijo

in/ali tajne podatke. Poročanje o vseh deviantnih pojavih je eden izmed načinov varovanja organizacije in s tem tudi njenih tajnih podatkov.

# 6. IZOBRAŽEVANJE S PODROČJA VAROVANJA TAJNIH PODATKOV

V procesu vključevanja Republike Slovenije v Evropsko unijo in zvezo NATO je bilo potrebnih veliko organizacijskih naporov za vzpostavitev enotnih meril in standardov v najširšem smislu. Pogajanja in usklajevanja niso potekala zgolj za področje varnosti, temveč tudi za področje ribištva, kmetijstva, gospodarstva … (Hartman, 2004).

Navedeno pomeni, da bo treba za udejanjanje uradno prilagojenih standardov organizirati oblike izobraževanja in usposabljanja na vseh področjih, da bo proces dosegel svoj namen.
Mednarodne in regionalne sile v medsebojni odvisnosti vplivajo na izobraževalni razvoj skupaj z gospodarskimi, družbenimi, političnimi, kulturnimi in demografskimi silami (Černetič, 1999: 72).

Strategija in politika izobraževanja prevzemata vse več neekonomskih oziroma socialnih funkcij, kar se kaže ob povečanem deležu generacij pri prehodu srednješolskih generacij na univerzo (Černetič, 1999: 96).
Kako pomembno je vlaganje v izobraževanje in s tem v znanje, pove ocena Mednarodne banke za obnovo in razvoj, ki pravi, da je struktura svetovnega kapitala sestavljena iz 64 odstotkov znanja, 20 odstotkov naravnih bogastev in 16 odstotkov finančnega kapitala (Černetič, 2002: 478).

Glede na določila Zakona o tajnih podatkih se posamezniki srečujejo s tajnimi podatki predvsem v organih državne uprave in v vseh tistih organizacijah, ki s temi organi sodelujejo.
Namen ugotavljanja in analiziranja potreb po usposabljanju in izpopolnjevanju je oblikovanje ciljev usposabljanja. Temu sledijo določitev ustrezne strategije, priprava programov usposabljanja ter njihovo izvajanje in ovrednotenje.
Usposabljanje je odgovornost vseh organov javne uprave, analiza potreb po usposabljanju pa je odgovornost vodilnih javnih uslužbencev (Miglič, 2002: 7). Za doseganje kakovosti dela javnih uslužbencev mora biti v ta namen v javni upravi omogočena ustrezna raven usposabljanja in izpopolnjevanja.
Za ugotavljanje potreb po usposabljanju v javni upravi je priporočljivo ugotavljanje potreb na treh ravneh:

- »prva je raven **celotne uprave**, kjer je začrtana splošna strategija usposabljanja, usklajena s potrebami reformne strategije javne uprave. Usposabljanje je na tej ravni sredstvo za oblikovanje organizacijske kulture, naklonjene reformnim procesom v upravi,
- druga raven je **organizacijska**, kjer so za usposabljanje odločilne specifične zahteve dela in potrebne kvalifikacije,
- tretja je **individualna raven**, ki se mora v idealnih razmerah skladati s potrebami prve in druge ravni, hkrati pa dopuščati posameznikom individualni razvoj in prihodnjo kariero« (Miglič, 2002: 15).

Za vse osebe, ki dostopajo do tajnih podatkov, mora država zagotoviti ustrezne oblike usposabljanja in izpopolnjevanja v obliki seminarjev, delavnic, predavanj, pogovorov na individualni ravni in drugo.
Vsebine – teme seminarjev, pogovorov naj bi bile zelo pestre, odvisno od ciljne skupine. Posameznik mora biti seznanjen s ključnimi metodami dela »vsiljivcev«,[36] če želimo, da bo pravočasno zaznal okoliščine, ki kažejo na to, da je postal zanimiv. Zanimivo je, da nekatere tuje države na spletnih straneh objavljajo članke, v katerih nekako nalagajo svojim državljanom, kako naj se samozaščitno obnašajo, koga naj obvestijo, če ugotovijo, da so zaradi dela, ki ga opravljajo, tarča tuje obveščevalne službe, in drugo. Gre za zanimiv pristop preventivnega dela, bistveno teže pa je to prenesti v predpis – zakon in to zahtevati od državljanov. Prav iz teh razlogov trdim, da je sistem usposabljanja in izpopolnjevanja ključnega pomena za učinkovito varovanje tajnih podatkov (Rozman, 2005: 4).

Priporočila, po katerih je treba izvajati usposabljanje osebja, ki dostopa do tajnih podatkov v Evropski uniji in v zvezi NATO, pomenijo, da mora tudi Republika Slovenija izvesti podobna usposabljanja, kar pomeni, da je to področje izobraževanja, ki ga je treba urediti in prilagoditi.

[36] Namenoma je uporabljen izraz vsiljivci, ker želim s tem zajeti najširši možni krog oseb, ki želijo priti do tajnih podatkov, do katerih dostopa oseba, pa te pravice nimajo (od radovednega sodelavca, soseda, žene do pripadnika tuje obveščevalne službe) (Rozman, 2005).

## 6.1. Zaznavanje potreb po usposabljanju varovanja tajnih podatkov

Varnostni standardi EU in NATO poleg podpisane izjave o seznanjenosti z določili Zakona o tajnih podatkih predvidevajo tudi izobraževanja in usposabljanja s tega področja. Urad vlade Republike Slovenije za varovanje tajnih podatkov je sicer tovrstna izobraževanja začel izvajati šele konec leta 2005, vendar pa to pomeni, da je Slovenija na pravi poti. Izobraževanje je namreč ključnega pomena pri zaščiti tajnih podatkov, saj nam zagotavlja pravilno in odgovorno ravnanje s tajnimi podatki, obenem pa tudi Slovenija zaradi izobraževanja postaja kredibilnejši partner (Korošec, 2006).

Podrobneje sta način in izvajanje usposabljanja opredeljena v Uredbi o varnostnem preverjanju in izdaji dovoljenja za dostop do tajnih podatkov. Členi 21 do 23 opredeljujejo osnovno in dodatno usposabljanje ter izvajalce usposabljanja. Osnovno usposabljanje se izvede za osebe, preden jih predstojnik predlaga v postopek varnostnega preverjanja ali preden podpišejo izjavo o seznanitvi s predpisi s področja tajnih podatkov.
Dodatnega usposabljanja se morajo enkrat letno udeležiti osebe, ki imajo dovoljenje za dostop do tajnih podatkov ZAUPNO ali višje ter določajo stopnje tajnosti, zaradi opravljanja funkcije ali izvajanja nalog na delovnih mestih v ministrstvih. Usposabljanja so se dolžne udeležiti tudi osebe, ki v civilnih organizacijah skrbijo za varno obravnavanje tajnih podatkov, predstojniki organov ali organizacij, ki izvajajo notranji nadzor, ter osebe, ki jih določi predstojnik organa in organizacije. Dodatno usposabljanje mora obsegati skrajšano obliko osnovnega usposabljanja, vključevati mora morebitne nove predpise in vsebine s posameznih področij obravnavanja in varovanja tajnih podatkov, za katere je bilo z notranjim, inšpekcijskim nadzorom in nadzorom Nacionalnega varnostnega organa ugotovljeno, da se izvajajo pomanjkljivo, oziroma druge vsebine, za katere predstojnik meni, da jih je treba vključiti v program dodatnega usposabljanja. Okvirni program izdela nacionalni varnostni organ v sodelovanju s pristojnima inšpektoratoma (Inšpektorat Republike Slovenije za notranje zadeve in Inšpektorat Republike Slovenije za obrambo) (ZTP-UPB2, 2006, Uredba o varnostnem preverjanju in izdaji dovoljenja za dostop do tajnih podatkov, 2006).

Po pregledu trenutno veljavnega programa usposabljanja, ki je priloga Uredbe o varnostnem preverjanju, sem ugotovil, da v njem ni vsebin, ki jih za osebje, ki dostopa do tajnih podatkov EU in NATO, predlagata omenjeni organizaciji (komuniciranje z mediji,

zaznave delovanja tujih obveščevalno-varnostnih služb, nevarnosti, ki izhajajo iz nediskretnih pogovorov …).

Glede na dejstvo, da smo zaupanja vreden partner, bomo morali tudi na obrambnem področju in v Slovenski vojski prilagoditi način usposabljanja ter uvesti vsebine, ki jih predlagata in jih za svoje zaposlene, ki dostopajo do tajnih podatkov, izvajata EU in NATO. Na obrambnem področju in v Slovenski vojski, glede na določila Uredbe o varnostnem preverjanju, osnovno in dopolnilno usposabljanje izvajajo pooblaščeni delavci OVS in predavatelji Zakona o tajnih podatkih iz organa S/G/J-2, ki bodo morali predlagati tudi spremembo programa, tako kot ga priporoča EU in NATO.

Poleg naštetega bo treba izvajati tudi usposabljanja s področja varnostne kulture, ki je nekoliko zastalo, osebno pa menim, da ni dovolj določene postopke predpisati, nadzirati, ukrepati, temveč je treba zaposlene tudi usposobiti, kako ukrepati ter katere varnostne ukrepe v določeni situaciji uporabiti, da bo dosežena preventivna prvina varnosti, kar visoko izgrajena varnostna kultura nedvomno je.

### 6.1.1. Izvajalci izobraževanja in usposabljanja

- Šola za častnike in podčastnike, ki zagotavlja izvedbo programov OVSIU ter DVSIU;
- Poveljniško štabna šola PŠŠ, ki zagotavlja izvedbo štabnega, višje štabnega in generalštabnega šolanja, kjer se slušatelji usposobijo za delo v poveljstvih ter za najvišje dolžnosti znotraj Slovenske vojske;
- Center za usposabljanje z učnimi enotami (UE) po strukturi in sestavi, ki zagotavlja izvedbo programov TVSU kandidatov za vojaške osebe, programov OVSU in DVSU vojakov in specialističnega dela programov OVSIU in DVSIU podčastnikov in častnikov;
- Center za bojno usposabljanje (CBU) poveljstev in enot, ki zagotavlja strokovno pomoč, deloma tudi izvedbo nalog (zahtevnejše oblike) urjenja in TV poveljstev in enot ter strokovno pomoč in podporo pri ocenjevanju bojne usposobljenosti.

Razvojni, vojaškodoktrinarni in pedagoški deli so oblikovani in organizirani v eni organizacijski enoti, Centru za doktrino in razvoj s podenotami, ki izvajajo temeljno poslanstvo CDR na področju pedagoškega dela, vojaških doktrin ter razvoja vojaške znanosti, teorije in prakse vojne veščine in vojaških sistemov ter razvoja najpomembnejših segmentov podpore VIU. Osnovne organizacijske enote pedagoško razvojnega dela bodo

katedre glede na rodove ali discipline vojaške in drugih znanosti in podobno (Žunkovič, Toš, 2006: 997).

Vsi izvajalci izvajajo predpisane programe, ki so glede na stopnjo izobraževanja različni in prilagojeni udeležencem ter stopnji izobraževanja. Pregled programov po posameznih stopnjah izobraževanja pokaže določene pomanjkljivosti s področja varovanja tajnih podatkov in varnostne kulture. Področje varovanja tajnih podatkov je sicer posebej opredeljeno ter se izvaja kot enodnevni seminar, medtem ko vsebin, ki bi izgrajevale varnostno kulturo in preventivno varnost ter bi slušateljem predstavile delovanje in metode dela obveščevalnih služb, v predpisanih programih ni. Glede na določila in previdnostne ukrepe, ki jih predpisujeta EU in NATO, bi bilo treba vsebine opredeliti v vseh programih, ki se izvajajo v sistemu izobraževanja in usposabljanja na obrambnem področju in v SV.
Vsebine izobraževanja je treba določiti glede na potrebe posameznika in organizacije, ki v njej delujejo. Posameznikove potrebe se pogosto razlikujejo od potreb delovne organizacije. Interesi se v življenju spreminjajo – ne toliko njihov obseg kot vsebina in pripravljenost, da bi jih človek dosegel.

Izobraževanje na individualni ravni je še posebej pomembno zato, ker je v Kazenskem zakoniku Republike Slovenije za izdajo tajnih podatkov predvidena zaporna kazen. Posameznik, ki podpiše izjavo, da je seznanjen z zakonodajo, ki ureja varovanje tajnih podatkov, bi moral dejansko biti usposobljen na tem področju. V primeru kršitve varovanja tajnih podatkov bi lahko prišlo do zelo neugodnih scenarijev, saj sta na prvem mestu za varovanje tajnih podatkov odgovorna posameznik in državni organ, ki izda dovoljenja za dostop.
Posameznik bi moral poznati vse določbe Zakona o tajnih podatkih, podzakonske akte, previdnostne ukrepe, ki so neposredno povezani z nediskretnimi pogovori, previdnostne ukrepe pri stikih s predstavniki tiska in potencialnimi dejavnostmi tujih obveščevalnih in varnostnih služb. Pridobljeno znanje na področju varovanja tajnih podatkov je treba periodično obnavljati. Zaradi navedenega bi morali v vsa organizirana izobraževanja in usposabljanja uvesti navedene vsebine, prilagojene udeležencem izobraževanja. Z izobraževanjem in usposabljanjem bi teoretične osnove s področja varnostne kulture in varovanja podatkov s stopnjami tajnosti dopolnili s praktičnimi izkušnjami in nasveti zaposlenih, ki so izkušnje z obeh obravnavanih področij pridobili v tujini.

Le tako lahko omogočimo trajnejše znanje, ki bo služilo namenu, udeleženci pa ga bodo znali uporabiti v življenju. Zato znova poudarjamo pomen poznavanja posameznikovih izkušenj in ugotavljanja potreb.
Vendar pa izobraževanja ne bi bilo treba izvajati le na najnižji, individualni ravni. Varnostno kulturo bi bilo treba spodbuditi na ravni organov, ki pri svojem delu prihajajo v stik s tajnimi podatki, v ta namen pa bi se morali izobraževati tudi nadrejeni (Korošec, 2006).

Na prehodu iz 20. v 21. stoletje smo bili priča velikemu razvoju znanosti na vseh področjih življenja. Razvoj novih tehnologij omogoča izdelavo novih komunikacijskih sredstev, s katerimi posamezniki komunicirajo med seboj in družbo. Razvoj interneta in mobilne telefonije spreminja način življenja družbe na globalni ravni. Pri tem postaja komuniciranje med ljudmi vedno bolj neosebno. Hkrati z razvojem novih komunikacijskih sredstev se znova pojavlja tudi potreba po varovanju podatkov s stopnjami tajnosti, saj je še vedno treba ločiti zasebno od javnega.
Sodobne obveščevalne službe uspešno izkoriščajo razvoj znanosti in tehnologije. Danes veliki obveščevalni sistemi ne morejo preživeti brez globalnega računalniško podprtega obveščevalno informacijskega okolja (Šaponja, 1999: 13). Z vstopom Slovenije v EU in NATO se je zanimanje tujih obveščevalnih služb okrepilo, hkrati pa sta Slovenija in njen obrambno-varnostni sistem postala predmet nadzorov držav članic EU in NATA. Državni organi bodo tudi v prihodnje morali dokazovati, da so vredni zaupanja in da so z dvigom varnostne kulture zaposlenih poskrbeli za primeren način komuniciranja. Obveščevalne službe kljub sodobnemu načinu zbiranja podatkov še vedno zbirajo določeno število podatkov z direktnim komuniciranjem s pripadniki Slovenske vojske in zaposlenimi na obrambnem področju.

Glavni cilj izobraževanja zaposlenih je, da se usposobijo za varovanje podatkov s stopnjami tajnosti ter tako dvignejo varnostno kulturo na raven, ki jo pričakujeta EU in zveza NATO. Predmet, ki bi ga v programe uvedli, bi se imenoval Varnostna kultura in varovanje podatkov.

Vsebina predmeta je lahko naslednja:

| Št. učne enote | Učna snov | Vsebina | Čas |
|---|---|---|---|
| 1 | Zakon o tajnih podatkih | osnovni pojmi – terminologija, tajnost kot družbeni in varnostni fenomen | 2 |
| 2 | pravna ureditev varovanja tajnosti | primerjava pravne ureditve v Sloveniji s pravno ureditvijo v EU, NATU … | 2 |
| 3 | vrste in stopnje tajnosti, določanje in označevanje tajnosti podatkov in dokumentov | osnovni pojmi, pooblastila in odgovornost, omejitev dostopa do tajnih podatkov, varovanje tajnih podatkov … | 2 |
| 4 | možne zlorabe podatkov s stopnjami tajnosti in protiukrepi | izdaja tajnosti, manipuliranje s tajnimi podatki, kazenska odgovornost … | 1 |
| 5 | viri ogrožanja tajnih podatkov | zunanji, notranji viri ogrožanja … | 2 |
| 6 | sodobne obveščevalne službe | osnovni pojmi, organiziranost, način dela, pridobivanje sodelavcev … | 4 |
| 7 | osnove komuniciranja | sporočila v komunikaciji, poslušanje, vedenje in komunikacijsko ozračje ... | 2 |
| 8 | varnostna kultura | previdnostni ukrepi, ki jih je treba upoštevati pri komunikaciji, zaznavanje vohunske dejavnosti, poročanje varnostnim organom … | 4 |
| 9 | igranje vlog – komuniciranje z različnimi sogovorniki | udeleženci bodo skušali do sedaj osvojeno znanje uporabiti pri igranju vlog komuniciranja z novinarji, pripadniki tujih OS, sodelavci … | 3 |
| 10 | zaključna analiza | | 2 |
| SKUPAJ | | | 24 ur |

Predmet bi se izvajal za zaposlene, ki pri svojem delu izdelujejo dokumente s stopnjami tajnosti ZAUPNO in višje ter dostopajo do njih, v predlagani obliki. Za druge zaposlene, ki dostopajo do dokumentov s stopnjami tajnosti INTERNO, bi predmet zajemal samo izbrane vsebine.

# 7. ZAKLJUČEK

## 7.1 Verifikacija hipotez

*H1 Protiobveščevalno-varnostna dejavnost na obrambnem področju se izvaja v skladu z zakonskimi določili.*

Protiobveščevalno in varnostno dejavnost na obrambnem področju izvajajo OVS MORS in obveščevalni organi Slovenske vojske. Oba subjekta svoje poslanstvo izvajata glede na zakonska določila.

Pri tem je treba poudariti, da vojaški organi izvajajo predvsem preventivno dejavnost na vseh področjih varnostne dejavnosti. Preventivno delujejo predvsem na področju protiobveščevalne zaščite in protiterorističnega delovanja, kar pomeni, da v procesu izvajanja štabno varnostnih nalog izvajajo dejavnosti, ki preprečujejo manifestiranje varnostno deviantnih pojavov v Slovenski vojski. Poleg štabno varnostnih nalog izvajajo varnostna usposabljanja in skrbijo za dvig varnostne kulture pri pripadnikih Slovenske vojske. Skrbijo tudi za uvajanje in izvajanje vseh varnostnih zahtev in standardov, ki jih predvidevajo nacionalna zakonodaja in predpisi zveze NATO (Balant, Čaleta, 2006: 853). Protiobveščevalno-varnostna dejavnost, ki jo izvajajo vojaški organi, je organizirana na vseh ravneh poveljevanja do ravni bataljona. To je torej organ, ki izvaja protiobveščevalno in varnostno dejavnost znotraj enot in poveljstev.

Dostopanje do tajnih podatkov in njihovo varovanje sta zagotovljeni s protiobveščevalno-varnostno dejavnostjo, ki jo izvaja OVS MORS. Bistvena dejavnost v zvezi s tajnimi podatki je varnostno preverjanje. Cilj varnostnega preverjanja je namreč zagotoviti, da se bo nevarnost razkritja tajnih podatkov zmanjšala na sprejemljivo mero. Tajnosti bodo namreč še vedno ogrožale tuje obveščevalne službe, katerih temeljni cilj je pridobivanje tajnih podatkov (Anžič, Trbovšek, 2004: 37). »Nedvomno sta lojalnost (državi, organizaciji) in zanesljivost (na delovnem mestu in zunaj njega) ključna kriterija, na podlagi katerih se ocenjuje, ali je posameznik verodostojen. Dvom o lojalnosti in/ali zanesljivosti predstavlja glavni kriterij pri ocenjevanju varnostnih zadržkov.« (Črnčec, 2003b: 61)

Poleg tega OVS MORS sodeluje tudi v procesu zagotavljanja protiobveščevalne zaščite in notranje varnosti SV z aktivnostmi od zunaj – predvsem s spremljanjem varnostnega okolja in izdelovanjem določenih analiz in predlogov ter z izvajanjem ukrepov, ki jih predvideva Zakonom o obrambi, ter v skladu s svojimi pooblastili in resursi izvaja ustrezne preiskave in operativne ukrepe.

Sodelovanje med obema subjektoma je zelo tesno in poteka na naslednjih področjih:

- izmenjava informacij,
- skupno sodelovanje v okviru svojih pristojnosti na področju kadrovske, fizične, informacijske, industrijske varnosti in varnosti informacijskih sistemov,
- sodelovanje na področju protiobveščevalnega dela,
- sodelovanje na področju protiterorizma,
- sodelovanje na področju usposabljanja in izobraževanja,
- sodelovanje na področju mednarodnih dejavnosti (Balant, Čaleta, 2006).

Z namenom izboljšanja varnostne in protiobveščevalne dejavnosti znotraj Slovenske vojske ter upoštevajoč področja, kjer sta organa že sedaj povezana, omenjena avtorja predlagata določene konceptualne spremembe področja. Osebno se strinjam s predlogi, ki jih navajata, ter povzemam najpomembnejša med njimi:

- v Slovensko vojsko je treba prenesti določene pristojnosti na varnostnem področju, ki jih ima sedaj obveščevalno-varnostna služba, in sicer tisti del, za katerega ni potrebna uporaba posebnih metod in sredstev,
- vse resurse na različnih področjih varnostne dejavnosti je treba povezati v celoten sistem, ki bo sposoben hitrega odzivanja na vse dejavnike, ki bi lahko ogrozili varnost oboroženih sil in njenih pripadnikov.

Omenjeno pomeni, da bi bilo treba spremeniti zakonodajo ter ponovno opredeliti naloge subjektov zagotavljanja varnosti. Spremembe bi pomenile tudi, da bi sistem zagotavljanja varnosti prilagodili strukturi zveze NATO. Poenotiti bi morali tudi sistem izobraževanja na področju varnostne dejavnosti. S tem bo strokovno področje postalo zanimivo tudi za varnostne strokovnjake, ki bodo lahko videli razvoj svoje karierne poti v tem sistemu. Brez ustreznega strokovnega kadra je nemogoče pričakovati napredek in razvoj varnostne dejavnosti v oboroženih silah.

*H2 Varovanje tajnih podatkov v Republiki Sloveniji je primerljivo z varovanjem tajnih podatkov v Evropski uniji in zvezi NATO.*

Varovanje tajnih podatkov ni pomembno samo po sebi, temveč je nujno zaradi varovanja vrednot, ki veljajo v družbi. Varovanje tajnih podatkov vzpostavi ravnovesje med tveganjem (ogrožanjem) in obvladovanjem (nadzorom) tega tveganja. To pa sta bistvena naloga in cilj sistemskega varovanja tajnih podatkov. Prvo fazo sistemskega varovanja predstavlja identifikacija oziroma prepoznava ogrožanj, nato sledi njihova analiza. V tretji fazi se pojavijo dejavnosti, ki so usmerjene v preprečevanje groženj oziroma nevarnosti, ki ogrožajo podatke, ter v odpravljanje morebitnih škodljivih posledic (Čaleta, 2004).

Na področju varovanja tajnih podatkov so se zgodile velike konceptualne spremembe, ki temeljijo predvsem na individualni odgovornosti posameznika, zadolženega za obdelovanje ali varovanje določenega tajnega podatka. Največ sprememb je bil deležen postopek varnostnega preverjanja oseb. Dopolnjeni so bili standardi, ki predpisujejo tehnične in fizične ukrepe varovanja tajnih podatkov.

Spremembe na tem področju je treba pripisati predvsem vzpostavljanju ustreznega razmerja med operativnostjo obdelave tajnih podatkov in stopnjo njihovega varovanja. S spremembami, ki so bile izvedene po sprejemu Zakona o tajnih podatkih, smo zadostili predpisom, ki jih opredeljujeta EU in zveza NATO. Spremembe so bile izvedene v smeri doseganja minimalnih standardov. Minimalni standardi varovanja podatkov so zagotovljeni povsod, kjer so izgrajena in opremljena varnostna območja, nekatera določila pa so celo strožja, kot jih predpisujeta organizaciji, katerih članica je tudi Republika Slovenija.

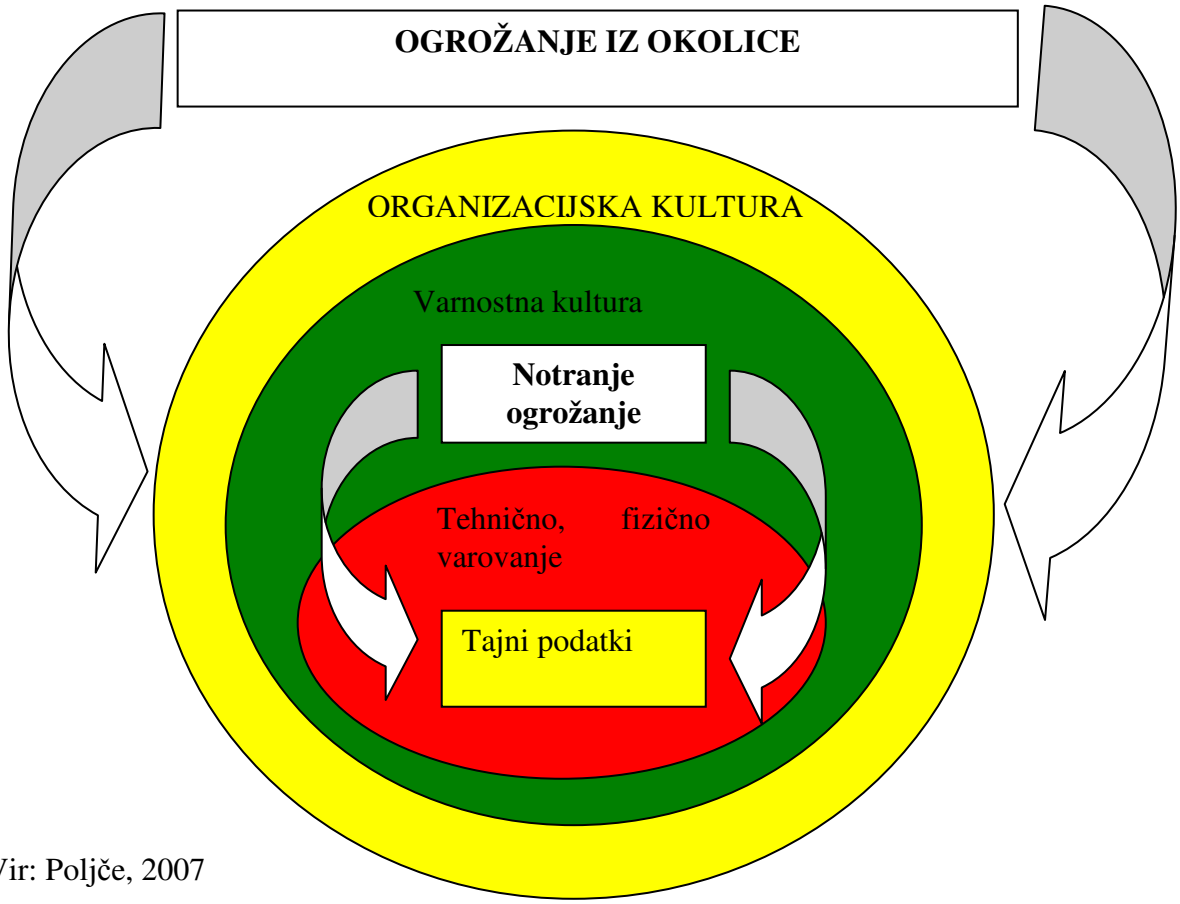
Vse, kar smo na tem področju storili, dokazuje, da je urejen sistem varovanja tajnih podatkov za delovanje Slovenije v evroatlantskih povezavah zelo pomemben. Pomembna je tudi vzpostavitev vseh delov sistema varovanja tajnih podatkov v vseh državnih organih. Država, ki ustrezno varuje svoje tajne podatke, je v mednarodni skupnosti sprejeta kot zaupanja vreden partner, kar sta Sloveniji priznali tako EU kot zveza NATO.

*H3 Izgrajena varnostna kultura kot del organizacijske kulture poleg tehničnih sredstev varovanja in drugih ukrepov zagotavlja učinkovito varovanje tajnih podatkov.*

Vrednote so za posameznika merilo, s katerim presoja svoja dejanja. Vrednote določajo, kaj ljudje mislijo, da je treba narediti. Določajo torej, kaj je prav in kaj narobe, kaj je dobro in kaj slabo. Služijo torej kot imperativi pri presojanju ter kot standardi za vrednotenje in racionalizacijo primernosti individualnih in socialnih odločitev (Kavčič, www. delavska-participacija.com/clanki/IDO30505.doc).

Če poenostavim, bi lahko rekel, da je varnostna kultura lahko ena izmed vrednot posameznika, ki jo je treba izgrajevati ter kot del preventivne varnosti bistveno vpliva na varnost in varovanje tajnih podatkov. Zaradi vse večjih zahtev po varnosti in zaradi spremenjenih viroh ogrožanja se čedalje bolj izraža tudi potreba po znanstvenem preučevanju varnostne kulture. Ker sta bila pojem in pomen varnostne kulture opredeljena, lahko z gotovostjo trdim, da bo z upoštevanjem določil zakonodaje, pravil, postopkov ter predpisanih ravnanj posameznikov tudi varovanje podatkov doseglo višjo raven.

Shema 7.1: Pomen varnostne kulture pri varovanju tajnih podatkov




Vir: Poljče, 2007

Iz sheme je razvidno, da je varnostno kulturo mogoče opredeliti kot del organizacijske kulture, ki povzema in izgrajuje tiste vrednote posameznika, ki so bistvenega pomena za varovanje tajnih podatkov.
Varnostna kultura v ožjem smislu torej posega na področje organizacijske kulture, je njen sestavni del in je v tesni povezavi z verodostojnostjo, lojalnostjo, varovanjem tajnosti, zanesljivostjo itd. (Črnčec, 2003b: 20). Če želi organizacija zagotavljati visoko stopnjo varovanja tajnih podatkov, mora vzpostaviti sistem, v katerem so individualne vrednote posameznikov, ki ravnajo s tajnimi podatki, v čim večji meri usklajene z vrednotami organizacije.

Tajni podatki so vselej ogroženi z različnimi viri ogrožanja, ti pa so lahko zunanji ali pa notranji. Z zagotavljanjem ustrezne protiobveščevalno-varnostne dejavnosti, se ta ogrožanja lahko zmanjšajo na najmanjšo možno mero. Dejavnost, ki jo pri tem izvaja OVS MORS, je usmerjena predvsem na zagotavljanje relevantnih protiobveščevalno-varnostnih podatkov ter izvajanje varnostnega preverjanja. Ob tem pooblaščeni delavci izvajajo tudi osnovno in dopolnilno usposabljanje s področja varovanja tajnih podatkov.
Obveščevalno-varnostni organi Slovenske vojske poleg preventivne protiobveščevalne varnostne dejavnosti, ki jo izvajajo, predlagajo poveljnikom na vseh ravneh poveljevanja ukrepe, ki zagotavljajo ustrezno raven varovanja tajnih podatkov. Posebnega pomena pa je njihova vloga pri izgrajevanju ustrezne varnostne kulture, ki jo na vseh ravneh izgrajujejo z usposabljanji, ki jih izvajajo v poveljstvih in enotah.

Ključnega pomena pri zagotavljanju varovanja tajnih podatkov v organizaciji pa je še vedno posameznik, ki dostopa do tajnih podatkov in jih obravnava. Njegova dolžnost je predvsem, da upošteva predpisane varnostne ukrepe, ki veljajo na obrambnem področju in v Slovenski vojski, ter se zaveda, da je možna »tarča« tuje obveščevalne službe. Sposoben mora biti zaznati take poskuse ter jih sporočiti nadrejenemu oziroma organu, ki se ukvarja z zagotavljanjem varnosti.
Kljub uporabi najsodobnejših tehničnih sredstev pri varovanju tajnih podatkov ni zagotovila, da bodo ti ostali prikriti, zato mora biti vzpostavljen sistem ravnanja s tajnimi podatki, ki poleg izobraževanja vključuje še tehnične, fizične in organizacijske ukrepe. Treba je torej zagotavljati in vzdrževati določeno stopnjo varnostne kulture pri zaposlenih, izgrajevati lojalnost in pripadnost organizaciji ter tako vplivati na zmanjšanje zlorabe tajnih podatkov.

*H4 Za pravilno ravnanje s tajnimi podatki je treba zaposlene usposabljati, saj se s tem zagotavlja odgovornejše ravnanje z njimi.*

Uspešno opravljeno varnostno preverjanje nam še ne zagotavlja pravilnega ravnanja s tajnimi podatki, ljudi je treba tudi izobraziti. Zavedati se namreč moramo, da še tako dober sistem varovanja tajnih podatkov ne pomeni nič, če nimamo dobro usposobljenih ljudi, ki se z njimi ukvarjajo (Korošec, 2006: 57).

Hipotezo potrjuje kontinuirano izobraževanje zaposlenih na obrambnem področju in v Slovenski vojski, ki z različnimi oblikami izobraževanja in usposabljanja sprejemajo novo znanje. Pridobljeno znanje pozneje uporabijo pri svojem strokovnem delu, omogoča pa jim tudi kvalitetnejše opravljanje operativnih nalog, kjer so zaposleni. Izobraževanje in usposabljanje se izvajata skladno s programi, ki predstavljajo poklicno izpolnjevanje. Izobraževanje in usposabljanje omogoča strokovno izpopolnjevanje vojaških oseb za opravljanje višjih in zahtevnejših dolžnosti ter pridobitev višje vojaško strokovne izobrazbe. Usposobljenost omogoča vojaški strokovni razvoj in napredovanje oziroma karierni razvoj.

Primerjava zakonodaje in predpisov, ki opredeljujejo obravnavanje tajnih podatkov v EU, NATO in Republiki Sloveniji, pokaže, da bo poleg osnovnega in dopolnilnega izobraževanja, ki ga predpisuje novela Zakona o tajnih podatkih, treba izvajati izobraževanja in usposabljanja, s katerimi bodo zaposleni pridobili nekatera specialistična znanja.

Predlagam, da bi se v vse izobraževalne programe umestil predmet, ki bi obravnaval področja varnostnih standardov v Republiki Sloveniji, Evropski uniji in zvezi NATO. Posameznik bi moral poznati vse določbe Zakona o tajnih podatkih, podzakonske akte, previdnostne ukrepe, ki so neposredno povezani z nediskretnimi pogovori, previdnostne ukrepe pri stikih s predstavniki tiska in potencialne dejavnosti tujih obveščevalnih in varnostnih služb.

Po zaključku usposabljanja bi posameznik pridobil ustrezno potrdilo o udeležbi na usposabljanju. Pridobljeno znanje na področju varovanja tajnih podatkov pa bi bilo treba periodično obnavljati znotraj enote, kjer je zaposlen.

Menim, da bi predmet Varnostna kultura in varovanje podatkov, če bi ga uvedli v sistem vojaškega izobraževanja v teoretičnem in praktičnem delu, kompleksno predstavil izbrano temo.

Na ta način bi vsi udeleženci usposabljanja med predavanji in praktičnim delom dojeli pomen varnostne kulture in varovanja tajnih podatkov. Izpolnili smo vse zahteve za članstvo v Evropski uniji in NATO, vendar za tvorno in produktivno sodelovanje potrebujemo veliko usposobljenih ljudi, ki bodo s svojim znanjem in izkušnjami prispevali k vsestranskemu razvoju Republike Slovenije, njenih prebivalcev in prebivalcev Evropske unije, ki so v večini primerov tudi člani zveze NATO. Uvedba predmeta je lahko le majhen korak k približevanju predpisanim standardom in omogoča dvig usposobljenosti zaposlenih, ki jih standardi neposredno ali posredno zadevajo.

Na podlagi prebranega je mogoče hipoteze potrditi.

## 7.2. Uporabnost ugotovitev za obrambno področje

V kontekstu zagotavljanja nacionalne varnosti je treba posebej poudariti pomen tajnosti kot družbenega fenomena, po drugi strani pa je vrednota, ki jo želi država oziroma v njenem imenu ali za njene potrebe državna institucija obdržati zase. V ta namen so bila sprejeta določena merila, kriteriji in pravila obnašanja v obliki zakonskih in podzakonskih normativnih aktov (Stopar, 2003).

Čeprav je Republika Slovenija sprejeta v EU in zvezo NATO ter si je s tem zagotovila višjo kolektivno varnost, je še vedno posredno oziroma neposredno ogrožena. Ogroženost opredeljujejo viri ogrožanja, vendar kljub vsem drugim ne smemo izključiti ogrožanja, ki ga predstavljajo obveščevalno-varnostne službe držav, ki niso članice omenjenih institucij. Zaradi tega je treba na obrambnem področju in v Slovenski vojski dejavnosti, ki jih izvajajo varnostni organi, usmerjati v preprečevanje njihove dejavnosti.
Metode in sredstva, ki jih obveščevalno-varnostne službe uporabljajo danes, bodo v prihodnosti doživeli nadaljnji razvoj, predvsem na področju tehnologije. Kljub občutnemu porastu uporabe tehničnih sredstev bodo ta še vedno služila kot pripomoček človeku pri zbiranju podatkov in informacij. Njegove popolne nadomestitve pa ni realno pričakovati v relativno kratkem času (Stopar, 2003).

Zahteve NATA in EU v procesu približevanja Slovenije obema zvezama so bile usmerjene predvsem v postavitev takega nacionalnega sistema varovanja tajnih podatkov, ki bo primerljiv z njihovimi standardi oziroma predpisi. Ni nujno, da je nacionalni sistem varovanja tajnosti države članice enak zahtevam EU ali NATA, mora pa omogočiti spoštovanje njunih standardov in predpisov, kadar v državah članicah obravnavajo tajne podatke ene ali druge zveze (Čaleta, 2004). Zagotovili smo primerljiv sistem varovanja (tehnično, fizično, kadrovsko ...), izvajamo preverjanje posameznikov, ki imajo ali bodo imeli dostop do tajnih podatkov, izvajamo usposabljanje, ki ga predpisujejo ZTP in podzakonski akti. Postorili smo skoraj vse, kar sta zvezi pričakovali od nas, v bližnji prihodnosti moramo zagotoviti le še, da bodo osebe, ki obravnavajo tajne podatke, ustrezno usposobljene, da bodo upoštevale vsa navodila in predpise ter da bodo v skladu z njimi tudi ravnale.

Ko je govor o varnostni kulturi, bi se morali njenega preučevanja lotiti celovito in znanstveno. Zaradi tega bi morali v okviru Poveljstva za doktrino, razvoj in usposabljanje, ali bolje rečeno, v Centru za doktrino in razvoj ustanoviti katedro, ki bi se ukvarjala s preučevanjem varnostne kulture ter bi pripravila ustrezne programe usposabljanja, ki bi bili vključeni kot predmet v programe izobraževanja in usposabljanja, ki se izvajajo v okviru vojaškega šolstva.
Zaradi zagotavljanja večje varnosti posameznikov, enot in poveljstev bi bilo treba ponovno preučiti organiziranost organov varnosti ter njihove naloge ponovno opredeliti. To pomeni, da bi bilo treba spremeniti tudi Zakon o obrambi. Verjetno bi morali tudi na obrambnem področju v enotnem zakonu opredeliti pristojnosti, naloge in pooblastila organov, ki se na obrambnem področju ukvarjajo z zagotavljanjem varnosti. Trenutna rešitev namreč opredeljuje, da organi svojo dejavnost izvajajo po Zakonu o obrambi, Zakonu o policiji in Zakonu o SOVI.

**»Obveščevalna dejavnost ni neka eksaktna znanost. To je bolj mešanica umetnosti in obrti, v kateri pogosto logika nima kaj iskati, obveščevalci pa morajo biti igralci z velikim smislom za igro, biti morajo kreativni in sposobni, da svojo dejavnost prikrijejo pred javnostjo.«**

**Efraim Halevy, nekdanji direktor Mossada**

# 8. LITERATURA IN VIRI

## KNJIGE IN ČLANKI:


1. AMBROŽ, M., MIHALIČ, T., OVSENIK, M. (2000): Varnostna kultura in sistem varovanja v organizaciji, Revija Varstvoslovje, letnik 2.
2. ANŽIČ, A. (1996): Vloga varnostnih služb v sodobnih parlamentarnih sistemih – nadzorstvo, Enotnost, Ljubljana.
3. ANŽIČ, A. (1999): Obveščevalne službe – legalni in legitimni labirinti in izhodi, Revija za teorijo in prakso varstvoslovja, 1, 1, str. 5–12.
4. ANŽIČ, A., BROŽIČ, L. (2006): Obveščevalno varnostni interesi Republike Slovenije po vstopu v zvezo NATO in Evropsko unijo, 7. slovenski dnevi varstvoslovja, Bled, Zbornik prispevkov (elektronski vir), Fakulteta za policijsko-varnostne vede, Ljubljana.
5. ANŽIČ, A., TRBOVŠEK, F. (2004): Varnostno preverjanje oseb v sistemu nacionalne varnosti, 5. slovenski dnevi varstvoslovja, Bled, Zbornik prispevkov (elektronski vir), Fakulteta za policijsko-varnostne vede, Ljubljana.
6. AAP-6, Nato slovar izrazov in definicij (NATO Glossary of Terms and Definitions), 2002.
7. BALANT, M., ČALETA, D. (2006): Varnostna dejavnost v Slovenski vojski – nove dimenzije razvoja. 7. slovenski dnevi varstvoslovja, Bled, Zbornik prispevkov (elektronski vir), Fakulteta za policijsko-varnostne vede, Ljubljana.
8. BRADLEY, C., JOHNSTON and CAMPBELL (2004): The army culture and climate survey, Kinhston, RCM.
9. BRDAJEV, A. (1982): Kaj počne obveščevalna služba, Revija Obramba 2, 3.
10. BREČKO, D. (2002): Andragoška spoznanja, številka 2/2002, Uvodnik, Andragoško društvo Slovenije, Ljubljana.
11. BREZOVŠEK, M., ČRNČEC, D. (2004): Tajnost v demokraciji, izvirni znanstveni članek, Teorija in praksa, letnik 41, 3–4/2004, Ljubljana.
12. BREZOVŠEK, M., HAČEK, M. (2006): Obrambna in varnostna kultura v Sloveniji, Bilten Slovenske vojske 2006 – 8/št. 4, Generalštab Slovenske vojske, Ljubljana.
13. BRITOVŠEK, M. (2004): Ogroženost in varnost parlamenta, diplomska naloga, Ljubljana.

14. BROŽIČ, L. (2004): Ustrezna strokovna usposobljenost kot predpogoj za uspešno izvajanje obveščevalno varnostnih nalog, 5. slovenski dnevi varstvoslovja, Bled, Zbornik prispevkov (elektronski vir), Fakulteta za policijsko-varnostne vede, Ljubljana.
15. ČALETA, D. (2004 a): Varovanje tajnih podatkov v zvezi NATO, Bilten Slovenske vojske 2004 – 6/št. 1, Generalštab Slovenske vojske, Ljubljana.
16. ČALETA, D. (2004): Konceptualne spremembe na področju varovanja tajnih podatkov v Republiki Sloveniji, 5. slovenski dnevi varstvoslovja, Bled, Zbornik prispevkov (elektronski vir), Fakulteta za policijsko-varnostne vede, Ljubljana.
17. ČERNETIČ, M. (1999): Ekonomika izobraževanja in raziskovanja, Založba moderna organizacija, Kranj.
18. ČERNETIČ, M. (2002): Vlaganje v razvoj človeških virov in univerz, Založba moderna organizacija, Organizacija, številka 10.
19. ČERNETIČ, M., BROŽIČ, L. (2003): Potrebe po novih znanjih – varovanje tajnih podatkov v Evropski uniji in zvezi NATO, Založba moderna organizacija, Organizacija, številka 8.
20. ČRNČEC, D. (2003 a): OVS MO kot conditio sine qua non obveščevalno-varnostne skupnosti RS, Visoka policijsko-varnostna šola, Ljubljana.
21. ČRNČEC, D. (2003 b): Tajnost podatkov (varnostno preverjanje in obveščevalno varnostne službe) (magistrsko delo), Fakulteta za družbene vede, Ljubljana.
22. ČRNČEC, D. (2003 c): Varnostna kultura in varnostno preverjanje oseb na obrambnem področju, Revija Slovenska vojska, leto XI/21.
23. DOBOVŠEK, B., FLANDER, B., MEŠKO, G., SOTLAR, A. (2004): Varovanje parlamenta, Uvodni referat k temi Problemi uravnoteženosti/usklajevanja med potrebo po odprtosti parlamentov in zahtevo po varovanju parlamentov, Posvet Varnost v parlamentih, Ljubljana, Državni zbor RS.
24. DOMIŠLJANOVIĆ, D., ŽUNEC, O. (2000): Obavještajno sigurnosne službe Republike Hrvatske, Naklada, Jesenski i Turk, Zagreb.
25. ĐORĐEVIĆ, O. (1985): Osnovi državne bezbednosti (opšti deo), Viša škola unutrašnjih poslova, Beograd.
26. ĐORĐEVIĆ, O. (1989): Leksikon bezbednosti, Založba Privredapublik, Beograd.
27. FERJAN, M. (1999): Organizacija izobraževanja, skripta, Založba moderna organizacija, Kranj.

28. FRANKOVIČ, M., PRESTON, M. (1993): Sodobni obveščevalni sistemi (analiza primerov ZDA, Izraela in Avstrije), diplomska naloga, Ljubljana.
29. FURLAN, B. in ostali (2006): Vojaška doktrina, PDRIU, Defensor, d. o. o., Ljubljana.
30. GRIZOLD, A. (1998): Javnost o organiziranju in upravljanju nacionalne varnosti Slovenije, V: Perspektive sodobne varnosti, FDV, Teorija in praksa, str. 99–134.
31. GRIZOLD, A. (1999): Obrambni sistem Republike Slovenije, MNZ, Ljubljana.
32. GRMEK, M., NOVAK, B. (2000): Modeli racionalnega in empiričnega modela evalvacije kurikula, Zbornik Evalvacija, Pedagoški inštitut.
33. GŠSV (2001): Metodologija načrtovanja izobraževanja in usposabljanja v SV (št. 811-02-1/01-10 z dne 4. 12. 2001), Ljubljana.
34. GŠSV (2003): Koncept sistema vojaškega izobraževanja in usposabljanja v SV (št. 811-01-6/2003-4 z dne 9. 7. 2003), Ljubljana.
35. GŠSV J-2 (2005): Koncept vojaške obveščevalne dejavnosti sv do leta 2010 – Osnutek, Ljubljana.
36. HARTMAN, E. (2004): Usposabljanje kadrov v poveljstvu brigade s področja varnostne kulture in varovanja podatkov s stopnjami tajnosti – študij konkretnega primera, diplomska naloga, Kranj.
37. HARTMAN, E. (2006): Obveščevalne službe Republike Slovenije v sistemu nacionalne varnosti, seminarska naloga, PŠŠ, Poljče.
38. JELENC, S. (1996): ABC izobraževanja odraslih, Andragoški center Republike Slovenije, Ljubljana.
39. JELENC, Z. in skupina avtorjev (1991): Terminologija izobraževanja odraslih, Pedagoški inštitut pri Univerzi v Ljubljani, Ljubljana.
40. JELUŠIČ, L. (1997): Legitimnost sodobnega vojaštva, FDV, Ljubljana.
41. JOHNSON, R. W. (1988): Thwarting enemies at home and abroad: How to be a Counterintelligence officier, Stone Trail Press, DIA Library, USA.
42. KAVČIČ, B. (1991): Sodobna teorija organizacije, Državna založba Slovenije, Ljubljana.
43. KAVČIČ, B. Uspešna organizacijska kultura, dostopno na www. delavska-participacija.com/clanki/IDO30505.doc, oblika HTML (21. 2. 2007).
44. KOROŠEC, S. (2006): Varnostno preverjanje v Republiki Sloveniji, diplomsko delo, Fakulteta za družbene vede, Ljubljana.
45. KOŠMRLJ, R. (1982): Varnostna kultura v sistemu družbene samozaščite, FDV, diplomska naloga, Ljubljana.

46. KOTNIK - DVOJMOČ, I. (2000): Preoblikovanje oboroženih sil sodobnih evropskih držav (študija primera Slovenije), doktorska disertacija, Ljubljana, FDV.
47. KRUNIĆ, Z. (1996): Metode dela obveščevalnih služb – poskus klasifikacije in pomen agenturne metode, Zbornik strokovno-znanstvenih razprav, posvet POMS, Visoka policijsko-varnostna šola, Ljubljana.
48. KUREŽ, B. (2005): Mednarodno obveščevalno sodelovanje, diplomska naloga, Ljubljana.
49. LIPOVEC, F. (1987): Razvita teorija organizacije, Založba Obzorja, Maribor.
50. LUKIĆ, D. (1981): Savremena špijunaža, Šabac.
51. MIGLIČ, G. (2002): Analiza potreb po usposabljanju, Ministrstvo za notranje zadeve Republike Slovenije.
52. MOLLER, C. (1995): Employeeship, Time Manager International A/S, Denmark.
53. MOŽINA, S. in skupina avtorjev (2002): Management, Didakta, Radovljica.
54. OSTERMAN, A., ŠAPONJA, V. (1996): Pomen uporabe posebnih operativnih metod in sredstev na področju vojaške obveščevalne, protiobveščevalne in varnostne dejavnosti, Zbornik strokovno-znanstvenih razprav, posvet POMS, Visoka policijsko-varnostna šola, Ljubljana.
55. OVSENIK, M., AMBROŽ, M. (2000): Ustvarjalno vodenje poslovnih procesov, Turistica, Visoka šola za turizem, Portorož.
56. PAGON, M. (2004): Razvoj organizacijske kulture v javnem sektorju, HRM – strokovna revija za ravnanje z ljudmi pri delu, številka 3, Gospodarski vestnik, Ljubljana.
57. PLETERŠEK, M. (2006): Organizacijska kultura v obveščevalno varnostni dejavnosti, Specialistična naloga, Fakulteta za organizacijske vede, Kranj.
58. PREZELJ, I. (2001): Grožnje varnosti, varnostna tveganja in izzivi v sodobni družbi, razreševanje nekaterih terminoloških dilem, Teorija in praksa, let. 38, št. 1.
59. PURG, A. (1994): Obveščevalne službe, politični sistemi in državna suverenost, doktorska disertacija, Ljubljana.
60. PURG, A. (1995): Obveščevalne službe, Enotnost, Ljubljana.
61. PURG, A. (1999): Varnostno-obveščevalni sistemi, Center za izobraževanje in svetovanje, Ljubljana.
62. PURG, A. (2001): Vloga obveščevalnih in varnostnih služb v političnih sistemih: primer Ruske federacije, Teorija in praksa, 38, 1, str. 103–118.

63. PURG, A. (2002): Primerjalni obveščevalni sistemi, Visoka policijsko-varnostna šola, Ljubljana.
64. ROZMAN, J. (2005): Varovanje oseb, ki imajo dostop do tajnih podatkov, 6. slovenski dnevi varstvoslovja, Bled, Zbornik prispevkov (elektronski vir), Fakulteta za policijsko-varnostne vede, Ljubljana.
65. SCHMID, G. (2001): BERICHT über die Existenz eines globalen Abhörsystems für private und wirtschaftliche Kommunikation (Abhörsystem ECHELON) (2001/2098 (INI)), http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A5-2001-0264+0+DOC+PDF+V0//DE, pdf, (11. 1. 2007).
66. SRĐANOV, I. (1983): Metodika izvođenja obaveštajno – bezbednostne obuke u vojnim školama JNA, Savezni sekretarijat za narodno odbranu, Uprava bezbednosti, Vojna štamparija Beograd.
67. STAJIĆ, L. (2006): Osnovi bezbednosti, Izdavačka kuča Draganić, Beograd.
68. STAJIĆ, L., MIJAKOVIĆ S., STANAREVIĆ, S. (2005): Bezbednosna kultura, Izdavačka kuča Draganić, Beograd.
69. STOPAR, M. (2000): Viri oziroma discipline zbiranja podatkov, seminarska naloga, Fakulteta za organizacijske vede, Kranj.
70. STOPAR, M. (2003): Kibernetski vidik informacije pri organiziranju varnosti družbenih sistemov, magistrsko delo, Fakulteta za organizacijske vede, Kranj.
71. ŠAPONJA, V. (1999): Taktika dela obveščevalno varnostnih služb, Visoka policijsko-varnostna šola, Ljubljana.
72. TOMINC, B., KOREN, B., SOTLAR, A. (2006): Novi časi – nove obveščevalne službe, 7. slovenski dnevi varstvoslovja, Bled, Zbornik prispevkov (elektronski vir), Fakulteta za policijsko-varnostne vede, Ljubljana.
73. TOŠ, D. (2003): Ugotavljanje in vrednotenje izobraževalnih potreb v funkciji razvoja kadrov, seminarsko delo, PŠŠ, Poljče.
74. TOŠ, D. (2006): Obrambno varnostno izobraževanje in usposabljanje v nacionalnem obrambno-varnostnem sistemu, 7. slovenski dnevi varstvoslovja, Bled, Zbornik prispevkov (elektronski vir), Fakulteta za policijsko-varnostne vede, Ljubljana.
75. TRBOVŠEK, F. (2004): Varnostni in pravni vidiki varnostnega preverjanja oseb, magistrsko delo, Fakulteta za podiplomske državne in evropske študije, Ljubljana.
76. ŽIROVNIK, J. (2001): Pridobivanje podatkov kot temeljna naloga slovenske obveščevalno-varnostne agencije, 2. slovenski dnevi varstvoslovja, Zbornik, Visoka policijsko-varnostna šola, Ljubljana.

77. ŽIROVNIK, J. (2006): Sodelovanje obveščevalnih in varnostnih služb pri zagotavljanju vitalnih interesov držav, 7. slovenski dnevi varstvoslovja, Bled, Zbornik prispevkov (elektronski vir), Fakulteta za policijsko-varnostne vede, Ljubljana.
78. ŽUNKOVIČ, J., TOŠ, D. (2006): Poveljstvo za doktrino, razvoj, vojaško izobraževanje in usposabljanje – odgovor na zahtevane nove pristope v vojaškem izobraževanju in usposabljanju v spremenjenem varnostnem okolju, 7. slovenski dnevi varstvoslovja, Bled, Zbornik prispevkov (elektronski vir), Fakulteta za policijsko-varnostne vede, Ljubljana.

**PRAVNI VIRI:**

1. Ustava Republike Slovenije (Uradni list RS/I, št. 33/1991 in 24/2003).
2. Zakon o obrambi (Uradni list RS, št. 49/98 in 66/98).
3. Zakon o obrambi, uradno prečiščeno besedilo (Uradni list RS, št. 103/04).
4. Zakon o Sovi (ZSOVA, Uradni list RS, št. 20/04).
5. Zakon o tajnih podatkih (Uradni list RS, št. 135/2003 in 28/2006).
6. Zakon o ratifikaciji varnostnega sporazuma med R Slovenijo in organizacijo severnoatlantskega pakta (Uradni list RS, št. 23/97).
7. Resolucija o strategiji nacionalne varnosti Republike Slovenije (Uradni list RS, št. 56/01).
8. Resolucija o splošnem dolgoročnem programu razvoja in opremljanja Slovenske vojske ReDPROSV (Uradni list RS, št. 89/04).
9. Uredba o izvajanju nalog organa pristojnega za obveščevalno podporo poveljevanju in vodenju ter za izvajanje štabno varnostnih nalog v Slovenski vojski (št. 017-06-1/2000-2, 19. 9. 2000).
10. Uredba o obveščevalno varnostni službi Ministrstva za obrambo (Uradni list RS, št. 63/99).
11. Uredba o varovanju tajnih podatkov (Uradni list RS, št. 74/2005).
12. Security Regulations of the Council of the European Union (2001/264/EC), L 101.
13. Nato Security Committee, Directive on Personnel Security, Document AC/35-D/2000, North Atlantic Council.
14. Protection Measures for Nato Civil and Military Bodies Deployed Nato Forces and Installations (Assets) Against Terrorist Threats, Document C-M(2002)50, 17. June 2002, North Atlantic Council.

15. Security Within the North Atlantic Threaty organization (NATO), Document C-M(2002)49, 17. June 2002, North Atlantic Council.
16. AJP-2 Skupna zavezniška obveščevalna, protiobveščevalna in varnostna doktrina, NATO, julij 2003.
17. AJP-2.2 Protiobveščevalni in varnostni postopki, NATO, november 2001.
18. ACE varnostna direktiva, NATO, AD 70-1.

**INTERNETNI VIRI:**

1. Australian defence intelligence organisation. http://www.defence.gov.au/dio/ (5. 10. 2006).
2. DIA at a glance. http://www.dia.mil/DIAglance.pdf (12. 3. 2007).
3. Europäisches parlament entwurfe ines berichts. http://www.szeredy.de/geschaeft/EUsonderausschuss.pdf (5. 2. 2007).
4. Factbook on Intelligence. http://www.fas.org/irp/cia/product/fact97/exeover.htm (27. 3. 2007).
5. Hungarian Intelligence Agencies. http://www.fas.org/irp/world/hungary/ (26. 3. 2007).
6. Military Security Service (MAD) Militaerischer Abschirmdienst. http://www.fas.org/irp/world/germany/mad/ (12. 2. 2007).
7. Startseite bundeswehr. http://www.bundeswehr.de/portal/a/bwde (9. 2. 2007).
8. The Defence Intelligence Organisation (DIO). http://www.defence.gov.au/dio/ (12. 3. 2007).
9. UK Security Service. http://www.mi5.gov.uk/ (12. 3. 2007).
10. United States intelligence Community. http://www.intelligence.gov/1who.shtml (8. 2. 2007).
11. Urad za varovanje tajnih podatkov. http://www.uvtp.gov.si/si/zakonodaja_in_dokumenti/veljavni_predpisi/ (6. 3. 2007).
12. Varnostno preverjanje oseb. http://www.uvtp.gov.si/index.php?id=381 (6. 3. 2007).
13. Vlada Republike Slovenije. http://www.gov.si/sova/ (9. 2. 2007).
14. Zakon o spremembah in dopolnitvah zakona o tajnih podatkih (Uradni l. RS, št. 28/2006), temeljni razlogi za spremembo in dopolnitve ZTP. http://www.uvtp.gov.si/fileadmin/uvtp.gov.si/pageuploads/UVTP_usmeritve_ZTP.pdf (22. 3. 2007).