UNIVERZA V LJUBLJANI
FAKULTETA ZA DRUŽBENE VEDE

LIDIJA HORVAT PETEK

OBVEŠČEVALNA ZVRST SIGINT V NACIONALNO VARNOSTNEM SISTEMU REPUBLIKE SLOVENIJE

MAGISTRSKO DELO

LJUBLJANA, 2010

UNIVERZA V LJUBLJANI
FAKULTETA ZA DRUŽBENE VEDE

LIDIJA HORVAT PETEK

Mentor: doc. dr. Iztok PREZELJ

OBVEŠČEVALNA ZVRST SIGINT V NACIONALNO VARNOSTNEM SISTEMU REPUBLIKE SLOVENIJE

MAGISTRSKO DELO

LJUBLJANA, 2010

Univerza
v Ljubljani
Fakulteta
za družbene vede

Kardeljeva ploščad 5
1000 Ljubljana, Slovenija
telefon 01 58 05 122
01 58 05 120

I Z J A V A O A V T O R S T V U
magistrskega dela

Podpisani/-a LIDIJA HORVAT PETEK z vpisno številko 21090965 sem avtor/-ica magistrskega dela z naslovom: OBVEŠČEVALNA ZVRST SIGINT V NACIONALNO VARNOSTNEM SISTEMU REPUBLIKE SLOVENIJE.

S svojim podpisom zagotavljam, da:

- je predloženo magistrsko delo izključno rezultat mojega lastnega raziskovalnega dela;
- sem poskrbel/-a, da so dela in mnenja drugih avtorjev oz. avtoric, ki jih uporabljam v predloženem delu, navedena oz. citirana v skladu s fakultetnimi navodili;
- sem poskrbel/-a, da so vsa dela in mnenja drugih avtorjev oz. avtoric navedena v seznamu virov, ki je sestavni element predloženega dela in je zapisan v skladu s fakultetnimi navodili;
- sem pridobil/-a vsa dovoljenja za uporabo avtorskih del, ki so v celoti prenesena v predloženo delo in sem to tudi jasno zapisal/-a v predloženem delu;
- se zavedam, da je plagiatorstvo – predstavljanje tujih del, bodisi v obliki citata bodisi v obliki skoraj dobesednega parafraziranja bodisi v grafični obliki, s katerim so tuje misli oz. ideje predstavljene kot moje lastne – kaznivo po zakonu (Zakon o avtorstvu in sorodnih pravicah, Uradni list RS št. 21/95), prekršek pa podleže tudi ukrepom Fakultete za družbene vede v skladu z njenimi pravili;
- se zavedam posledic, ki jih dokazano plagiatorstvo lahko predstavlja za predloženo delo in za moj status na Fakulteti za družbene vede;
- je elektronska oblika identična s tiskano obliko magistrskega dela ter soglašam z objavo magistrskega dela v zbirki »Dela FDV«.

V Ljubljani, dne 18.06.2010 Podpis avtorja/-ice: _____

POVZETEK

Predmet preučevanja je obveščevalna zvrst SIGINT kot ena izmed tehničnih obveščevalnih disciplin znotraj nacionalno varnostnega sistema, ali natančneje znotraj nacionalne obveščevalne dejavnosti. Gre za obveščevalno zvrst, ki se danes v sodobni obveščevalni dejavnosti postavlja v novo perspektivo. Postaja vedno bolj kompleksno področje, ki se globalizira in informatizira, a hkrati odpira tudi mnoga vprašanja v vsaki sodobni družbi.
Preučevanje obveščevalne zvrsti SIGINT znotraj nacionalno varnostnega sistema Republike Slovenije je zelo kompleksno in še dokaj zaprto področje. Deloma lahko razloge iščemo v nepoenoteni terminologiji in prepletanju zakonskih določil, kar otežuje kakovostno raziskovalno delo in znanstveno preučevanje tega področja. Deloma pa razloge najdemo v praksi kulture tajnosti in mistifikacije obveščevalne dejavnosti tako v slovenskem kot mednarodnem prostoru.
Obveščevalne službe v okviru izvajanja svojih nalog zagotovo posegajo v človekove pravice in temeljne svoboščine, večno vprašanje, ki se postavlja pred njih in njihove nadzornike pa je, ali je vsako poseganje legitimno, nujno, ustrezno in po načelu sorazmernosti. Analiza pravnega okvira in normativne urejenosti obveščevalne zvrsti SIGINT pokaže, da imamo v slovenskem pravnem redu preširoke in premalo določne zakonske formulacije. Predvsem zaskrbljujoče je prepletanje zakonskih določil, ki urejajo to področje, kar vodi v izrazito netransparentnost področja, dopušča različne strokovne in pravne interpretacije, omejuje pa tudi učinkovito nadzorno funkcijo. V Republiki Sloveniji imamo danes eno večjih demokratičnih pridobitev vzpostavljene sicer vse oblike nadzora nad obveščevalno zvrstjo SIGINT, pa vendar ugotavljam, da so nekateri nadzorni mehanizmi prešibko razviti, da bi lahko bili na tem področju učinkoviti.
Pred obveščevalno zvrst SIGINT se v sodobnem nacionalnem varnostnem okolju postavljajo nove zahteve, ki se vedno bolj izražajo kot potreba po optimalni izrabi vseh razpoložljivih nacionalnih virov izvajanja obveščevalne dejavnosti in njihovem integriranju v skupni obveščevalni proces. Za razvoj optimalnega prihodnjega modela ureditve področja SIGINT v okviru nacionalno varnostnega sistema bo potreben dobro premišljen sistemski pristop, ki bo imel »na svoji strani« podporo javnih politik, kot tudi dimenzijo časa in prostora, ob čemer pa bo obveščevalna skupnost morala simultano razviti tudi etična načela svojega delovanja.
Obveščevalna zvrst SIGINT bo v okviru obrambnega in vojaškega sistema prispevala pomemben delež v skupni obveščevalni proces, ki bo integriran s procesi bojnega delovanja in bo v prihodnje predstavljala nepogrešljiv element pri zaščiti sil Slovenske vojske v mednarodnih operacijah in misijah.

KLJUČNE BESEDE

Obveščevalna dejavnost, obveščevalna zvrst SIGINT, obveščevalni proces, procesi bojnega delovanja, demistifikacija obveščevalnih služb.

ABSTRACT

Signals Intelligence (SIGINT) is one of the technical intelligence disciplines within national Security System, precisely also within Slovenian national Intelligence and as such a subject of my research paper. Signals Intelligence is nowadays set up in a new perspective within the framework of contemporarily Intelligence. In its intense globalization and informatisation it becomes a very complex expert domain which, at the same time opens many questions in each contemporary society.

Researching Signals Intelligence within Slovenian national Security System is a very complex and reserved field of work. Partly we can find reasons for that in disunity of terminology and in legislation interlacement, which makes quality researching and academic studying consequently much more complex. On the other hand some reasons for this complexity in Slovenia and also broader can be found in the secrecy perception and mystification of Intelligence Services.

For sure Intelligence services are encroaching into human rights sphere and the eternal question which arises here is, if every encroaching is really legit, necessary, appropriate and proportional.

Slovenian Signals Intelligence legislation analysis shows some deficiencies in broad legal formulations. Above all the legislation interlacement of SIGINT stays the biggest concern, which consequently leads into expressive un-transparency of this intelligence discipline. As such allows dissimilarity of expert and legal interpretations and aggravates effectiveness of its supervision functions. One of the biggest democratic achievements in Republic of Slovenia today is the restoration of all supervision functions over Signals Intelligence, however some of its mechanisms are still feeblish developed to be well effective.

Signals Intelligence within contemporarily national security environment is now confronting new challenges, which will have a strong impact on horizontal linkage of all available resources within national Security System and in collaboration of allied Intelligence Services joined in net-sphere activity.

Optimal model development of the future SIGINT disposition within national Security System will require a well deliberated comprehensive and systematic approach, which will be fully supported by public policy and will consider also the dimensions of time and space. Within this context the national Intelligence community will also have to simultaneously set forth and raise their ethics principles. Within Slovenian defense and military organization SIGINT will contribute significantly to the overall intelligence process and will as such also be integrated within the battlefield management process. In addition SIGINT will be an indispensable Force Protection component to deployed Slovenian troops in international peace support operations.

KEY WORDS

Intelligence, intelligence discipline SIGINT (Signals Intelligence), intelligence process, battlefield management process, demystification of Intelligence Service.

KAZALO

SEZNAM PRILOG, TABEL IN GRAFOV

SEZNAM KRATIC

AFMBw	Amt für Fernmeldwesen Bundeswehr
ANBw	Amt für Nachrichtenwesen der Bundeswehr
BfV	Bundesamt für Verfassungsschutz
BND	Bundesnachrichtendienst
BSI	Bundesamt für sicherheit in der informationstechnik
CNE	Computer Network Exploitation
COMINT	Communication Intelligence
CRYPTINT	Cryptology Intelligence
EB	Elektronsko bojevanje
EBPL	Enota brezpilotnih letal
EEB	Enota za elektronsko bojevanje
EI	Elektronsko izvidovanje
ELINT	Electronic Intelligence
ESD	Enota za specialno delovanje
EVSI	Enota za večsenzorsko izvidovanje
FISINT	Foreign Instrumentation Signals Intelligence
GCEB	Glavni center za elektronsko bojevanje
GMA	General Morphological Analysis
HUMINT	Human Intelligence
IMINT	Imagery Intelligence
MAD	Militär Abschirmdienst
MASINT	Measurement Intelligence
MOM	Mednarodne operacije in misije
MORS	Ministrstvo za obrambo Republike Slovenije
NATO	North Atlantic Treaty Organisation
NSA	National Security Agency
NVS	Nacionalno varnostni sistem
OIB	Obveščevalno izvidniški bataljon
OKO	Operacije kriznega odzivanja
OSINT	Open Source Intelligence
OVS	Obveščevalno-varnostna služba
RADINT	Radar Intelligence

TECHINT	Technical Intelligence
TELINT	Telemetry Intelligence
PŠTO	Pokrajinski štab Teritorialne obrambe
ReSNV	Resolucija o strategiji nacionalne varnosti
RS	Republika Slovenija
SDV	Služba državne varnosti
SIGINT	Signals Intelligence
SNAV	Svet za nacionalno varnost
SOVA	Slovenski obveščevalno-varnostna agencija
SV	Slovenska vojska
VOMO	Varnostni organ Ministrstva za obrambo
ZNBw	Zentrum für Nachrichtenwesen der Bundeswehr
ZOBr	Zakon o obrambi
ZPNOVS	Zakon o parlamentarnem nadzoru obveščevalnih in varnostnih služb
ZPol	Zakon o policiji
ZSOVA	Zakon o Slovenski obveščevalno-varnostni agenciji

1 UVOD

V domači in tuji strokovni javnosti smo v zadnjem času priča mnogim razpravam o prihodnosti obveščevalne dejavnosti, kar daje neko vzpodbudo za naprej. Na eni strani vedno bolj odkrito govorimo o transformaciji obveščevalne dejavnosti, vzpodbujamo strokovni in znanstveni krog ljudi k boljši, učinkovitejši, uspešnejši stroki, po drugi strani pa je že sama razprava in pisanje o tem dokaz, da se obveščevalna dejavnost v odnosu do družbe odpira. V preteklosti javnost o obveščevalni dejavnosti ni vedela veliko. Kultura tajnosti je bila vedno eno od ključnih vodil delovanja obveščevalnih služb. Z razvojem družbe in njene demokracije, pa se odstira zavesa, za katero so se skrivale tudi hude napake, krivice in zlorabe. Prav ta zavesa je pokazatelj, da družba demokratično zori in si želi varnega in kakovostnega življenja v državni ureditvi, ki ji zaupa. Ravnanje obveščevalnih služb zato mora zato temeljiti na transparentnosti, odprtosti, politični nevtralnosti, profesionalni etičnosti in skladno z demokratičnimi normami. In ravno pri tem vprašanju trčimo na paradoks in dvoličnost države[1], ki ju želim v okviru svoje naloge še posebej preučiti: po eni strani država s svojim pravnim institutom zagotavlja svojim državljanom varstvo z ustavo dodeljenih najvišjih vrednot – tj. nedotakljivost osebne integritete ter varstvo človekovih pravic in temeljnih svoboščin-, po drugi strani pa z oblikovanjem obveščevalnih služb, katerih primarna dejavnost je tako ali drugače poseganje v zasebnost človeka, deluje proti temu, kar v ustavi razglaša kot najvišjo vrednoto. Zagotavljanje varnosti na eni strani in nedotakljivost posameznika na drugi sta in bosta vedno v nasprotju, ključno pri tem pa je, da država vzpostavi učinkovite mehanizme, ki ohranjajo obe dimenziji v ravnovesju.

[1] Dvoličnost države je dr. France Bučar, v intervjuju leta 2007 v Mladini, št. 13, v članku z naslovom *Največjo nevarnost za zlorabo Sove pomeni vlada* tako komentiral:
»Obstoj obveščevalnih služb kot takih je sam po sebi protiustaven. Gre za kolizijo norm. Država jamči nedotakljivost osebne integritete in ščiti človekove pravice. S posegi v zasebnost človeka, ki jo izvajajo obveščevalne službe, namreč sama deluje proti temu, kar je v ustavi razglasila kot eno največjih vrednot. In tu se pojavi vprašanje, ali je država dvolična. V bistvu je. Država mora, če jamči nedotakljivost osebe, sočasno jamčiti tudi varnost svojih državljanov. Recimo varnost pred akcijami teroristov, zunanjih nasprotnikov države in podobno ter tudi pred kriminalom nasploh. In to dolžnost države izvajajo prek organizacij, ki jim rečemo obveščevalne službe, naj se imenujejo tako ali drugače. S tem država dosega protiustavne cilje, ki pa so hkrati komplementarni z njeno dolžnostjo, da zavaruje svoje državljane.«
Dr. France Bučar je bil predsednik parlamentarne komisije za nadzor nad obveščevalnimi in varnostnimi službami v letih 1992-1996.

Edmonds (1988, 131) obravnava obveščevalno funkcijo kot eno izmed petih funkcij[2] v nacionalno varnostnem sistemu, ki so v neprestani interakciji in kot enega izmed temeljnih pogojev za uspešno delovanje tega sistema. Nedvomno se spremembe v zaznavanju groženj varnosti danes odražajo v vseh petih funkcijah in lahko bi rekli, da se odražajo v okviru širše nacionalne varnostne politike, kot tudi splošne nacionalne obveščevalne politike. Ključna sprememba v zaznavanju groženj varnosti je bil prehod od vojaških k nevojaškim in sub-nacionalnim grožnjam ter njihovo širjenje in disperzija čez meje neke države kot posledica sodobnih procesov, kot sta globalizacija in informatizacija (Williams in Moskos 1997 v Prezelj 2001, 127-141).

Znanost obravnava grožnje področno ali sektorsko v več dimenzijah ogrožanja nacionalne varnosti, in sicer: vojaški, gospodarski, policijsko-kriminalistični, ekološki, zaščitno-reševalni, teroristični, zdravstveni, informacijski, migracijski in obveščevalni (Prezelj 2007 v Črnčec 2009, 30). Zato se ta ključna sprememba v zaznavanju groženj kaže tudi v samem večdimenzionalnem pojmovanju varnosti in identifikaciji ključnih varnostnih problemov v teh dimenzijah. Z vidika te naloge sta zanimivi predvsem dve dimenziji, obveščevalna in vojaška. Obe se soočata z »novimi« oblikami groženj (ne-vojaške entitete, uporništvo, terorizem, asimetrično bojevanje, informacijsko bojevanje, kibernetično vojskovanje ipd), na katere bo odgovor treba poiskati skupaj z drugimi dimenzijami, ki prispevajo svoj delež k mednarodni varnosti.

Sodobna obveščevalna dejavnost se v informacijski dobi postavlja v novo luč; postaja vedno bolj kompleksno področje, ki se globalizira in informatizira. Gre za dejavnost, ki se bolj kot kadarkoli doslej opira na tehnološki, znanstveni, raziskovalni, razvojni in etični potencial, zaradi česar postaja ta dejavnost tudi zahtevnejša, celovitejša in dražja. Vse sodobne države, ki prispevajo svoj delež k mednarodnemu miru, se zavedajo, da same ne morejo ukrepati proti sodobnim grožnjam in pred njimi so novi izzivi sodelovanja in povezovanja. Globalne in večdimenzionalne grožnje postavljajo zdaj tudi sodobne obveščevalne službe pred dejstvo, da se mora obveščevalna dejavnost globalizirati, če želi najti ustrezen odgovor na skupne grožnje mednarodni varnosti. Po drugi strani pa je vsaka država sama zase odgovorna za oblikovanje, delovanje in učinkovitost svojega nacionalno varnostnega sistema.

[2] Po Edmondsu ima nacionalno varnostni sistem naslednjih 5 funkcij: 1. odločevalno funkcijo (vladni resorji), 2. operativno funkcijo (oborožene sile in policija), 3. obveščevalno funkcijo (obveščevalne službe), 4. svetovalno funkcijo (lastne/svetovalne službe) in 5. administrativno funkcijo (javna uprava).

Slovenija je v evropskem prostoru med mlajšimi državami in z mlado demokracijo, a kljub temu je kot enakopravni mednarodni subjekt postavljena pred enake grožnje in izzive. Zato je še kako pomembno, da pri oblikovanju svoje nacionalne varnostne politike ne ponavlja napak, ki so jih v preteklosti naredile in nato popravljale starejše države. Prav je, da gre kot suverena mlada država po svoji lastni poti, je pa tudi pomembno, da se pri tem zgleduje po tistih mednarodnih subjektih, ki so uspeli razviti visoko stopnjo demokracije, ki jo želi v prihodnosti tudi sama doseči. Najbrž bo zato morala preurediti nekatere funkcije v nacionalno varnostnem sistemu, zagotovo pa bo morala preurediti obveščevalno funkcijo tako, da bo kljub kulturi tajnosti, ki tudi v prihodnosti ne bo popolnoma prenehala, transparentnejša in bolj odprta, njeno delovanje pa bo temeljilo na jasnih pravnih normah in demokratičnih načelih. Glavni pogoj za dosego tega je vzpostavitev ustreznih in učinkovitih nadzornih mehanizmov po načelu delitve oblasti, preko katerih bo mogoče doseči neko sorazmerje do transparentnosti delovanja obveščevalnih struktur, še posebej pri posebnih ali tajnih načinih zbiranja obveščevalnih podatkov. Ena izmed obveščevalnih zvrsti, ki temelji na omenjenem tajnem načinu pridobivanja obveščevalnih podatkov, je prav gotovo SIGINT (angl. Signals Intelligence) in je z vidika kulture tajnosti za javnost najbolj zaprta obveščevalna zvrst tako v Republiki Sloveniji kot tudi drugod po svetu.

2 METODOLOŠKI OKVIR

2.1 Cilj in namen naloge

Cilj te naloge je preučiti obveščevalno zvrst SIGINT kot eno izmed tehničnih obveščevalnih disciplin znotraj nacionalno varnostnega sistema ali natančneje znotraj obveščevalne dejavnosti, tako s splošnega družbenega kot tudi z varnostnega in strokovnega vidika, da bi na utemeljen in objektivno kritičen način prepoznali pomanjkljivosti normativne in nadzorne ureditve področja ter tudi argumentirali prihodnjo vlogo te zvrsti znotraj obrambnega sistema Republike Slovenije. Z namenom ugotovitve primernosti obstoječih rešitev in nakazati morebitne boljše, sem z oblikovanjem sistemskih scenarijev SIGINT zmogljivosti znotraj obrambnega sistema Republike Slovenije dosegla tudi cilj proaktivnega pomena same naloge. Sekundarni cilj moje naloge je aktualizacija obveščevalne zvrsti SIGINT v strokovni in znanstveni javnosti, da to področje obveščevalne dejavnosti kljub svoji izraziti kulturi tajnosti ne bo ostajalo še naprej nepotrebna neznanka akademskega in znanstvenega preučevanju. Prepričana sem, da je za nadaljnji razvoj te specifične dejavnosti, ki se danes bolj kot kadarkoli doslej, opira na tehnološki, znanstveni, raziskovalni, razvojni in etični potencial, akademsko in znanstveno preučevanje nujno in potrebno. Naloga lahko s svojimi zaključki predstavlja pomembno izhodišče za nadaljnje preučevanje in raziskovanje, tako v strokovni kot tudi v akademski in znanstveni sferi.

2.2 Hipoteze

HIPOTEZA 1:
Normativna ureditev obveščevalne zvrsti SIGINT je na obrambnem področju preširoka in premalo določna, zato je v prihodnje mogoče pričakovati nekatere normativne posege. Z vidika težnje po optimalni izrabi razpoložljivih virov izvajanja obveščevalne dejavnosti znotraj nacionalno varnostnega sistema, pa je mogoče pričakovati tudi nekatere organizacijske spremembe.

HIPOTEZA 2:
Slovenija ima kot eno večjih demokratičnih pridobitev danes vzpostavljene vse oblike nadzora nad obveščevalno zvrstjo SIGINT, kar je nedvomno jasen kazalec demokratičnosti

naše države. Pa vendar bo za vzpostavitev učinkovitega političnega oziroma parlamentarnega nadzora potrebno nekatere njegove mehanizme še izpopolniti ali nadgraditi.

HIPOTEZA 3:
Čeprav si vsaka sodobna obveščevalna skupnost prizadeva, da z vidika poseganja v človekove pravice in temeljne svoboščine uresničuje načelo sorazmernosti, bo ta prizadevanja lahko utemeljevala šele, ko bo razvila svoja etična načela z uveljavitvijo etičnega kodeksa obveščevalne dejavnosti.

HIPOTEZA 4:
Obveščevalna zvrst SIGINT na obrambnem področju bo v prihodnje prispevala pomemben delež tako v obveščevalni proces, ki bo integriran s procesi bojnega delovanja, kakor tudi pri zaščiti sil Slovenske vojske.

2.3 Uporabljena metodologija

Z analizo domačih in tujih pisnih virov, ki obravnavajo problematiko obveščevalne dejavnosti in zvrsti SIGINT, bom preučila primarne pisne vire (normativne, strateške, konceptualne in doktrinarne dokumente) in sekundarne pisne vire (članke, literaturo). S študijo primera SIGINT subjekta v Slovenski vojski bom s funkcijsko analizo normativnih podlag, vloge in poslanstva, organiziranosti in sedanjih ter prihodnjih mednarodnih obveznostih našla stične točke v odnosu do spreminjajočega in transformirajočega se mednarodnega varnostnega okolja. Pri preučevanju vloge, organiziranosti in delovanja SIGINT subjekta v Slovenski vojski bom uporabila tudi metodo neposrednega opazovanja iz prakse.

Za analizo obveščevalne zvrsti SIGINT kot ene izmed tehničnih obveščevalnih disciplin znotraj nacionalno varnostnega sistema bom uporabila deskriptivno metodo. Z uporabo metode primerjalne analize normativne in parlamentarne nadzorne ureditve v obveščevalni zvrsti SIGINT z dvema izbranima evropskima državama bom v okviru naloge poskušala prepoznati njihove stične točke in tudi njihova razhajanja.

Z metodo strukturiranega intervjuja s priznanimi domačimi in tujimi strokovnjaki na obrambnem in vojaškem področju bom utemeljila in sintetizirala vidike prihodnjega razvoja

obveščevalne zvrsti SIGINT na obrambno-vojaškem področju tako v okviru nacionalno varnostnega sistema kot tudi v okviru NATA. Strukturiran intervju je bil z vidika analize vloge obveščevalne zvrsti SIGINT v preteklem obdobju in odločitve o prepodreditvi teh zmogljivosti pod pristojnost Slovenske vojske iz leta 2000 izveden z bivšim dolgoletnim načelnikom prvih SIGINT zmogljivosti na obrambnem področju, s podpolkovnikom Cirilom Belšakom. Z aktualnim poveljnikom sil Slovenske vojske, generalmajorjem Alanom Geder-jem, sem se v intervjuju pogovarjala o sedanji in prihodnji vlogi teh zmogljivosti v okviru Slovenske vojske, z generalnim direktorjem Obveščevalno-varnostne službe Ministrstva za obrambo, Damirjem Črnčecem pa o strokovnih in družbenih vidikih ter prihodnjih izzivih za obveščevalno dejavnost v okviru nacionalno varnostnega sistema. Z visoko predstavnico za obveščevalno dejavnost iz Mednarodnega vojaškega štaba v NATU, Karen Laino[3], sem se pogovarjala o vlogi SIGINT v NATU ter o prihodnjih izzivih in mehanizmih, ki jih prinaša potreba po intenzivnem in učinkovitem sodelovanju na obveščevalnem področju v okviru Severno-atlantskega zavezništva. Rezultati intervjujev in njihova eksploatacija so uporabljeni deskriptivno pri posameznih preučevanih vsebinah in z metodo sinteze v zaključkih.

Analizo prihodnje vloge zmogljivosti SIGINT na obrambno-vojaškem področju sem zaokrožila z oblikovanjem treh sistemskih scenarijev, s ciljem ugotoviti primernost obstoječe rešitve in s prepoznavanjem ključnih parametrov oziroma spremenljivk ter njihovim vrednotenjem, nakazati morebitne boljše. Za oblikovanje scenarijev sem uporabila splošno uveljavljeno (evropsko) tipologijo in kombinirano metodo; kvantitativno metodo in metodo temelječo na ekspertnih mnenjih, pri čemer sem se opirala predvsem na uveljavljeno metodologijo, t.i. splošno morfološko analizo (General Morphological Analysis GMA), primerno za reševanje kompleksnih, večdimenzionalnih in ne-kvantitativnih primerov. Za modeliranje in vrednotenje sem uporabila tiste ključne parametre oziroma spremenljivke, ki sem jih obdelala v okviru magistrske naloge. Pri izbiri najbolj optimalne sistemske rešitve za zmogljivosti SIGINT na obrambnem področju, pa sem uporabila programsko orodje za podporo v procesu odločanja DEXi. Zaradi preobsežnosti modela za uporabo v DEXi, sem nekatere atribute namenoma izključila, kar ni vplivalo na rezultat in njegovo verodostojnost. Verifikacijo postavljenih hipotez bom izvedla z rezultati metode sinteze.

[3] S Karen Laino sem intervju izvedla 23. 3. 2010, in sicer v okviru njene udeležbe na mednarodni regionalni konferenci, ki je z naslovom *Izzivi zoperstavljanja terorizmu v regiji jugovzhodne Evrope* potekala od 22. do 26. marca 2010 v Mariboru. Karen Laino je pred nastopom funkcije pomočnice direktorja Mednarodnega vojaškega štaba v NATU (Assistant Director IMS NATO, Intelligence Division) 4 leta vodila NATO svetovalni odbor za SIGINT.

3 TERMINOLOŠKA OPREDELITEV

3.1 Nacionalna obveščevalna politika

Preden opredelimo nacionalno obveščevalno politiko, je treba opredeliti njen širši okvir - nacionalno varnost in nacionalno varnostno politiko. Če nacionalno varnost opredelimo kot varnost naroda oziroma nacije v neki državi in kot sposobnost zaščite fizične integritete države, njenega ozemlja, ohranjanja gospodarskih odnosov z drugimi državami pod razumnimi pogoji, zaščite narave države, institucij in vodstva pred zunanjim ogrožanjem ter sposobnost nadzora državnih meja (Grizold 1999, 25), potem lahko opredelimo varnostno politiko kot enega izmed temeljnih elementov sistema nacionalne varnosti. Nacionalna varnostna politika Republike Slovenije je opredeljena v okviru Resolucije o strategiji nacionalne varnosti Republike Slovenije[4], ki določa strategijo zagotavljanja nacionalne varnosti, nacionalne interese in nacionalno varnostne cilje, vire ogrožanja in varnostna tveganja, izhodišča politike odzivanja na posamezne grožnje in tveganja ter osnovne sistemsko-organizacijske rešitve delovanja države pri zagotavljanju nacionalne varnosti. Resolucija o strategiji nacionalne varnosti Republike Slovenije je temeljni razvojno usmerjevalni dokument na področju nacionalne varnosti. Zagotavljanje nacionalne varnosti Republike Slovenije temelji na Ustavi Republike Slovenije, spoštovanju človekovih pravic in temeljnih svoboščin ter demokracije in načel pravne države, na sprejetih nacionalnih razvojnih dokumentih, zakonskih in podzakonskih aktih in na spoštovanju načel mednarodnega prava (s pravicami in obveznostmi Republike Slovenije), prevzetih z mednarodnimi pogodbami.

Nacionalna obveščevalna politika je sestavni del nacionalne varnostne politike. Po Grizoldu je obveščevalna politika ena izmed varnostnih politik nacionalno varnostnega sistema sodobne države, poleg nje pa so na seznamu še: zunanja, obrambna, gospodarska, socialna, ekološka, zdravstvena, energetska, izobraževalna in kulturna politika. Varnostna struktura za zagotavljanje varnosti na ravni celotne družbe pa v okviru notranje varnosti obsega obveščevalne in varnostne službe (Grizold 1999 v Črnčec 2009, 27-29).

[4] Nedavno smo v Republiki Sloveniji dobili novo *Resolucijo o strategiji nacionalne varnosti Republike Slovenije (ReSNV-1),* ki je nadomestila zdaj že 9 let staro istoimensko resolucijo. Državni zbor Republike Slovenije jo je potrdil in sprejel na svoji seji dne 26. marca 2010.

Seveda se takoj pojavi vprašanje oblikovanja ali kreiranja obveščevalne politike znotraj nacionalne varnostne politike: kdo so nosilci oblikovanja te politike in kdo so izvajalci? Obveščevalna politika in tudi ostalih prej naštetih devet politik se podreja splošni nacionalni varnostni politiki in izvršilna veja oblasti je nosilec njenega oblikovanja. Ključno vlogo pri njenem oblikovanju imajo:

- Vlada Republike Slovenije kot nosilka izvršilne veje oblasti, ki skrbi za uresničevanje nacionalno-varnostne politike in delovanje sistema nacionalne varnosti na vseh področjih in ravneh. V ta namen sprejema potrebne politične, pravne, organizacijske in druge ukrepe.
- Svet za nacionalno varnost (SNAV), katerega pristojnosti, sestavo in delovanje je opredelila Vlada Republike Slovenije z odlokom[5]. SNAV je skladno s tem odlokom pristojen za usklajevanje varnostne politike in za usmerjanje in usklajevanje dejavnosti, ki se izvajajo za uresničevanje interesov in ciljev nacionalne varnosti[6]. Izhajajoč iz tega gre za telo vlade, ki mu sicer predseduje predsednik vlade[7], ima pa samo posvetovalno oziroma usklajevalno funkcijo. Nekaj več operativnega usklajevanja aktivnosti za delovanje SNAV zasledimo sicer v okviru nalog Sekretariata SNAV, ki so opredeljene v 5. členu odloka. Le-ta je v praksi zadolžen tudi za usklajevanje aktivnosti v zvezi z izvajanjem splošne obveščevalne politike. Pričakovali bi, da bo na tem mestu njegova vloga eksplicitno opredeljena kot operativna in proaktivna, z vključevanjem na obeh ravneh izvajanja obveščevalne politike, vendar ni tako. Odlok v 5. členu določa, da sekretariat SNAV samo operativno usklajuje aktivnosti za delovanje SNAV, skrbi za usklajeno izvedbo stališč SNAV ter opravlja druge naloge za SNAV. Vlogo bolj proaktivne narave je zaslediti samo pri svetovalcu predsednika vlade za nacionalno varnost v 6. členu odloka, seveda mu mora mandat za to podeliti predsednik SNAV, ki je hkrati predsednik vlade.

Izvršilna veja oblasti si mora (vlada in njeni resorji) skladno s sodobnimi demokratičnimi normami prizadevati, da se o oblikovani splošni obveščevalni politiki posvetuje in pouči tudi pri zakonodajni veji oblasti oziroma s pristojnim parlamentarnim telesom (odborom ali komisijo za nadzor obveščevalnih služb) (Born 2003, 68). V tem okviru je zato pomembno

[5] Odlok o Svetu za nacionalno varnost.
[6] Povzeto po 1. členu Odloka o Svetu za nacionalno varnost.
[7] Skladno s 3. členom Odloka o Svetu za nacionalno varnost.

opredeliti tudi vlogo Državnega zbora Republike Slovenije, ki predstavlja institucionalno oziroma politično raven upravljanja sistema nacionalne varnosti, znotraj njega pa tudi obveščevalne politike. Državni zbor določa zakonske okvire in dolgoročne smernice razvoja nacionalno-varnostne politike[8] ter sprejema in potrjuje državni proračun, ki ga pripravi vlada. Državni zbor določa tudi strateške smeri (zunanje, obrambne, notranje-varnostne, gospodarske, obveščevalne in varnostne politike ter druge politike) in preko pristojnih delovnih teles izvaja nadzor nad zakonitostjo dela obveščevalnih in varnostnih služb. Samo nadzorno funkcijo nad zakonitostjo dela obveščevalnih in varnostnih služb bom podrobneje opredelila v nadaljevanju naloge.

Če poskušamo odgovoriti na vprašanje, kdo so neposredni izvajalci (uresničevalci) obveščevalne politike, je treba opredeliti posamezne subjekte izvajanja obveščevalne dejavnosti znotraj nacionalno varnostnega sistema - obveščevalno varnostne službe. Med te subjekte je zato treba poleg Slovenske obveščevalno-varnostne agencije šteti še Obveščevalno varnostno službo Ministrstva za obrambo, s posameznimi subjekti Slovenske vojske za izvajanje vojaške obveščevalne dejavnosti. V nadaljevanju naloge bom vsak subjekt natančneje preučila predvsem z vidika uresničevanja obveščevalne politike s poudarkom na preučevanju normativnih podlag za izvajanje obveščevalne zvrsti SIGINT kot ene izmed tehničnih obveščevalnih disciplin, s poudarkom na njeni vlogi v obrambni oziroma vojaški obveščevalni dejavnosti.

3.2 Obveščevalna dejavnost

Obveščevalna dejavnost je ena najstarejših dejavnosti človeštva, ki se je najprej razvila za potrebe osebne in kolektivne varnosti, kasneje pa tudi za doseganje ostalih (političnih, vojaških, ekonomskih, ideoloških idr.) ciljev.

Po Lowenthalu (2009, 2-4) so obveščevalne službe poklicane, da preprečujejo kakršnokoli strateško presenečenje, zagotavljajo dolgoročna strokovna mnenja, podpirajo nacionalno politiko in zagotavljajo tajnost informacij, potreb in metod. Obveščevalna dejavnost je v nacionalnem varnostnem sistemu postala nepogrešljiv element, vendar pa ne glede na prednosti, ne zagotavlja vseh odgovorov (Scott in Hughes 2006, 654). Obveščevalna

[8] Smernice so opredeljene s temeljnim razvojno usmerjevalnim dokumentom s področja nacionalne varnosti, ki je *Resolucija o strategiji nacionalne varnosti Republike Slovenije*.

dejavnost, ki jo izvajajo obveščevalne službe, primarno zagotavlja neodvisno analizo informacij, pomembnih za varnost države in družbe ter za zaščito njenih glavnih interesov (Born 2003, 64). Obveščevalna dejavnost zaznava sodobne grožnje nacionalni varnosti in se nanje tudi odziva, lahko bi rekli razvija. Danes, ko te grožnje prehajajo od vojaških k nevojaškim in sub-nacionalnim grožnjam, njihove dimenzije pa preraščajo lokalne in regionalne okvire, postaja obveščevalna dejavnost globalna in zelo kompleksna. V njenem razvoju prihaja tako do določene notranje specializacije (zunanja in notranja politika, gospodarska, obrambna, vojaška, idr.). Razlike v izvajanju obveščevalne dejavnosti se kažejo tudi glede na to, kje se uporablja, znotraj suverene države ali pa na ozemlju drugih držav, torej v tujini (Šaponja 1999, 20). V nadaljevanju naloge se bom sicer terminološko opredelila samo na eno izmed specialnosti obveščevalne dejavnosti, tj. vojaško obveščevalno dejavnost, še prej pa si poglejmo nekaj izbranih definicij obveščevalne dejavnosti (angl. Intelligence). Pri svoji izbiri sem se omejila na eno izmed sodobnejših tujih (Schreier 2009) in na definiciji dveh priznanih slovenskih strokovnjakov, Purga in Šaponje. Zanimivo je, da sem najpreprostejše in najnazornejše opredelitve zasledila pri sodobnih, aktualnih strokovnjakih s tega področja. Starejše definicije so bolj kompleksne in deskriptivne narave.

Definicija sodobnega tujega avtorja (Schreier 2009, 47) pravi: *»Obveščevalna dejavnost = informacije + analiza.«* Ta opredelitev že v svoji formulaciji pojasnjuje razliko med zbranimi informacijami in sproduciranimi obveščevalnimi rezultati, ker brez analize ni obveščevalne dejavnosti. Obveščevalna dejavnost ni tisto, kar je bilo zbrano, ampak je rezultat, ki nastane, ko so bili podatki zbrani, informacije pa ovrednotene in analizirane (Schreier 2009, 47).

Purg (2002, 14) na drugi strani pa navaja, da je obveščevalna dejavnost najširši pojem in bi ga lahko opredelili kot rezultat zbiranja, analiz, združevanja in interpretacije vseh razpoložljivih podatkov, ki zadevajo enega ali več vidikov tuje države oziroma operativnega področja, ki je neposredno ali potencialno pomembno za načrtovanje (Richelson 1989 v Purg 2002). Iz navedene opredelitve sta jasna tako proces izvajanja kot namen obveščevalne dejavnosti. Kot elemente navaja zbiranje, analizo in združevanje vseh razpoložljivih podatkov.

Šaponja (1999, 9) navaja, da je obveščevalna dejavnost 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 (Intelligence-Policy & Process 1985 v Šaponja 1999).

Tudi Šaponja je navedel definicijo, ki nakazuje več za nas pomembnih elementov, in sicer zbiranje in analitično obdelavo surovih podatkov ter potrebe uporabnika po obveščevalnih izdelkih (produktih) in področja uporabe celovitih obveščevalnih izdelkov.

Vse opredelitve obveščevalne dejavnosti imajo skupni imenovalec: bolj ali manj opisujejo obveščevalni proces, imenovan tudi obveščevalni cikel ali obveščevalni krog, ki v sodobni obveščevalni dejavnosti vsebuje naslednjih šest korakov (Schreier 2009, 49):

1. definiranje potreb, načrtovanje in usmerjanje (angl. defining the needs, planning and direction).
2. zbiranje (angl. collection).
3. obdelavo (angl. processing).
4. analizo in produkcijo (angl. analysis and production).
5. diseminacijo[9] (angl. dissemination).
6. povratno informacijo (angl. feedback).

Tudi Lowenthal (2009, 65-66) obveščevalni proces deli na 6 korakov, ki jih samo nekoliko drugače imenuje, in sicer na naslednji način: 1. requirements, 2. collection, 3. processing and exploitation, 4. analysis, 5. dissemination in 6. consumption.

V podrobnosti samega obveščevalnega procesa v nalogi ne bom zahajala, je pa za moje nadaljnje preučevanje pomemben predvsem 2. korak (zbiranje podatkov ali collection), ki opredeljuje različne specifične metode in načine zbiranja podatkov v obveščevalnem procesu (management zbiranja); obveščevalne discipline oziroma obveščevalne zvrsti zbiranja (collection disciplines) ali t.i. INTs (Lowenthal 2009, 69). Sam proces zbiranja podatkov vključuje odprte in tajne vire kot tudi številne tajne tehnične discipline ali zvrsti zbiranja podatkov (Schreier 2009, 47-48). Brez tega bi bila obveščevalna dejavnost bolj ali manj dejavnost, ki bi temeljila le na ugibanju.

Na tem mestu je treba poudariti, da različni viri navajajo različno delitev obveščevalnih disciplin zbiranja podatkov. Schreier (2009, 50-51) in Lowenthal (2009, 82-108) navajata 5 obveščevalnih disciplin (OSINT[10], HUMINT[11], SIGINT[12], IMINT[13], MASINT[14]), medtem ko

[9] Izraz dissemination različni avtorji različno prevajajo, v SSKJ beseda diseminacija pomeni razširjanje, zato sem jo uporabila kot termin v 5. koraku.
[10] Open Source Intelligence
[11] Human Intelligence
[12] Signals Intelligence

nekateri drugi viri navajajo samo tri (OSINT, HUMINT in TECHINT)[15] (DCAF 2006a, 2; Shulsky in Schmitt 2002, 11). V TECHINT zato uvrščajo vse tiste obveščevalne discipline ali zvrsti, ki za zbiranje podatkov uporabljajo specializirano tehnologijo. Sem tako prištevajo SIGINT, IMINT, RADINT, COMINT, ELINT, CNE, CRYPINT idr.

Vendar pa ostaja ne glede na raznovrstnost delitve na posamezne obveščevalne discipline ali zvrsti zbiranja podatkov strokovna javnost enotnega mnenja, da sta za obveščevalno dejavnost ključni sinergija in fuzija zbranih podatkov v posameznih disciplinah in produkcija celovite obveščevalne informacije (angl. all-source intelligence). V okviru nadaljevanja naloge se bom podrobneje ukvarjala le z eno izmed obveščevalnih disciplin oziroma zvrsti zbiranja podatkov, in sicer z obveščevalno zvrstjo SIGINT[16].

3.3 Vojaška obveščevalna dejavnost

Vojaško obveščevalno dejavnost, ki jo lahko razumemo kot eno izmed notranjih specializacij obveščevalne dejavnosti, je opredeljena v aktualni Vojaški doktrini (PDRIU 2006, 32-33) v poglavju *6.3 Vojaška obveščevalna dejavnost* kot:
»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, vojaško-politično in varnostno situacijo ter delovanje sovražnika, potencialnega sovražnika in druge vojaške ter varnostne grožnje, s ciljem 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.« Razdelil jo je na tri ravni:

- vojaško obveščevalno dejavnost na strateški ravni, ki jo izvajajo Obveščevalno varnostna služba Ministrstva za obrambo in obveščevalni organi Generalštaba Slovenske vojske,
- vojaško obveščevalno dejavnost na operativni ravni, ki jo izvajajo obveščevalni organi in enote operativnega poveljstva sil, in

[13] Imagery Intelligence
[14] Measurement Intelligence
[15] Technical Intelligence.
[16] Direktor ameriške nacionalne obveščevalne agencije (NSA) je nekoč nazorno pojasnil pomembno razliko med dvema obveščevalnima disciplinama, SIGINT in IMINT: »IMINT nam pove, kaj se je zgodilo; SIGINT pa, kaj se bo zgodilo« (Lowenthal 2009, 92).

- na vojaško obveščevalno dejavnost na taktični ravni, ki jo izvajajo obveščevalni organi poveljstev brigad in bataljonov ter izvidniške enote.

V vojaški obveščevalni dejavnosti se zaradi trenutno omejenih analitičnih zmogljivosti na taktični in operativni ravni, predvideva integriranje v skupno strateško analitiko, zato izvajanje vojaške obveščevalne dejavnosti na operativni in taktični ravni obravnavam kot omejeno samo na določene zmogljivosti (senzorje) zbiranja podatkov za potrebe vojaške obveščevalne dejavnosti.

Obveščevalno zvrst SIGINT na obrambnem področju v nadaljevanju obravnavam kot eno izmed teh zmogljivosti (senzorjev) zbiranja podatkov iz dveh razlogov: ker tako zahteva nacionalna zakonodaja in ker je trenutno umeščena na taktično raven, iz katere pa izvaja naloge za strateško raven in jo hkrati tudi neposredno podpira.

3.4 Obveščevalna zvrst SIGINT

Obveščevalna zvrst SIGINT (angl. Signals Intelligence) je tehnična obveščevalna disciplina zbiranja podatkov, katerega vir so vse vrste elektromagnetnih emisij. Gre za obveščevalno zvrst, ki zagotavlja obveščevalne podatke za vse ravni: od vladno-politične, do vojaško-poveljniške; od strateške do taktične. Obveščevalni podatki se pridobivajo z metodo odkrivanja, prestrezanja, razpoznavanja in določanja lokacij virov oddajanja elektromagnetnih emisij s ciljem odkrivanja virov ogrožanja in tveganja varnosti.

Priznani ameriški strokovnjak Mark Lowenthal pravi, da je SIGINT fenomen 20. stoletja[17].
Kljub mnogim poskusom prevoda tega pojma priznanih strokovnjakov s področja obveščevalne dejavnosti (Šaponja, Črnčec, idr.) v slovenščini še nismo našli dovolj širokega, a hkrati tudi dovolj enostavnega in poenotenega izraza za uporabo, ki bi zajel celotno vsebino te obveščevalne zvrsti.

Različni strokovni viri v tujini in doma navajajo različno delitev obveščevalne zvrsti SIGINT. Šaponja (1999, 81) deli SIGINT na tri poddiscipline: COMINT (Communication

[17] Prvo prestrezanje tujih (vojaških) komunikacij zasledimo že v rusko-japonski vojni (1904-1905). Z razvojem napredne komunikacijske tehnologije, se je razvijala tudi ta zvrst zbiranja obveščevalnih podatkov in je danes zelo kompleksna disciplina, ki temelji izključno na raziskovalnem in tehnološkem potencialu. V praksi deluje v sodelovanju z ostalimi sorodnimi obveščevalnimi zvrstmi (predvsem z IMINT).

Intelligence), ELINT (Electronic Intelligence) in RADINT (Radar Intelligence). Črnčec (2009, 90) opredeli SIGINT kot zvrst pridobivanja podatkov na obveščevalnem področju in ga deli na tri podzvrsti pridobivanja podatkov na obveščevalnem področju; na COMINT, ELINT in FISINT[18] (Foreign Instrumentation Signals Intelligence).

Ameriški avtorji (Lowenthal 2009, 90-96; Shulsky in Schmitt 2002, 27-31) delijo SIGINT na tri podzvrsti: COMINT, ELINT[19] in TELINT[20], medtem ko Schreier iz Centra za demokratični nadzor nad oboroženimi silami (DCAF) v Ženevi SIGINT razdeli kar na pet poddisciplin: COMINT, ELINT, FISINT, CRYPTINT in CNE. Schreier razume FISINT kot RADINT in TELINT, CRYPTINT[21] pa razume kot kriptološko obveščevalno dejavnost (pridobivanje obveščevalnih podatkov z dekriptiranjem), CNE[22] pa kot podatke in informacije, dobljene iz računalniških omrežij ter analize »informacijskega prometa« (Schreier 2009, 50).

V zadnjem primeru gre za izjemno kompleksno delitev, ki po mojem mnenju izstopa iz nekega preteklega okvira še iz enega razloga. V SIGINT zvrst namreč uvršča CRYPTINT kot podzvrst, kar je sicer na neki način logično, a vendar nevsakdanje. Glede na specializiranost nekaterih obveščevalnih struktur bi lahko zaključili, da je SIGINT ena izmed najbolj razvitih tehničnih obveščevalnih zvrsti z najdaljšim stažem, ki je večkrat tudi organizacijsko izločena in avtonomna od ostale obveščevalne strukture, kot npr. SIGINT agencija, direktorat, ipd. (na primer v Avstriji, Belgiji, Bolgariji, Češki, Franciji, Madžarski, Nemčiji, Švedski, Švici in Veliki Britaniji (DCAF 2006, 6)). Najbrž je zaradi tega tudi »posrkala« CRYPTINT, TELINT in druge, dokaj sorodne in šele razvijajoče se tehnične zvrsti obveščevalne dejavnosti, s katerimi deluje v medsebojnem sodelovanju tudi v praksi.

Iz preučevanja številnih delitev obveščevalne zvrsti SIGINT na posamezne podzvrsti, ki se med posameznimi avtorji razlikujejo, ameriški avtorji posamezne podzvrsti razumejo drugače, kot jih razumejo evropski avtorji, zato vprašanje, ali, če in kje globalno razumejo to delitev vsi enako. Morebiten odgovor na to vprašanje se ponuja v primeru Severno-atlantskega zavezništva (NATO), kjer se regionalni (evropski) vidik sooča z ameriškim. Dejstvo je, da je

[18] Tako delitev poznajo tudi v ZDA in nekateri viri uvrščajo FISINT v ELINT poddisciplino.
[19] Lowenthal v nekaterih primerih ELINT razume tudi kot FISINT
[20] Telemetry Intelligence
[21] Cryptology Intelligence
[22] Computer network exploitation

znotraj NATA ta delitev za vse njene članice standardizirano poenotena, kar bomo natančneje spoznali v nadaljevanju naloge. Vendar pa v praksi prihaja do konfuzije med nespremenjeno nacionalno opredelitvijo in širšo poenoteno regionalno ali celo globalno. Na primer: v Sloveniji smo z vstopom v NATO zaradi povezljivosti (interoperabilnosti) z drugimi članicami prevzeli NATO delitev, ki uveljavlja samo dve podzvrsti SIGINT: COMINT (spremljanje elektronskih komunikacijskih omrežij) in ELINT (spremljanje elektronskih nekomunikacijskih omrežij), ob zavedanju, da nam nacionalna zakonodaja določa drugačne pravno-terminološke okvire za izvajanje te obveščevalne zvrsti:

- *spremljanje mednarodnih sistemov zvez* v okviru 20. in 21. člena obstoječega Zakona o Slovenski obveščevalno-varnostni agenciji, ki je v spreminjanju, in
- *elektronsko spremljanje mednarodnih sistemov zvez* v okviru 32. člena Zakona o obrambi.

Vsi štirje termini bodo natančneje predstavljeni v nadaljevanju naloge: COMINT in ELINT v 5. poglavju (podpoglavje NATO), zadnja dva pa v okviru pravne ureditve področja SIGINT v Republiki Sloveniji (podpoglavje 5.1.).

3.5 Elektronsko izvidovanje - terminologija v vojaški praksi

V Ministrstvu za obrambo in Slovenski vojski se je v splošni dolgoletni strokovni uporabi uveljavil izraz *elektronsko izvidovanje*. Najbrž gre za prevzeto terminologijo iz t. i. rdeče literature bivše Jugoslovanske armade, ki je uporabljala termin *elektronsko izviđanje*.

Čeprav osebno menim, da je ta pojem mnogo ožji od angleškega izvirnika *Signals Intelligence*, ga kot slovenski vojaški terminološki »nadomestek« najdemo tudi v aktualni Vojaški doktrini (PDRIU 2006, 33), kjer je elektronsko izvidovanje v poglavju *6.3. Vojaška obveščevalna dejavnost* opredeljeno kot »del vojaške obveščevalne dejavnosti, ki se v Slovenski vojski izvaja centralizirano.« Posredno se na elektronsko izvidovanje nanaša tudi naslednji stavek iz točke *10.2. Elektronsko bojevanje* iste doktrine, kjer je navedeno, da je »elektronsko bojevanje neposredno povezano z obveščevalno dejavnostjo in je eden od stebrov informacijskega delovanja« (PDRIU 2006, 68).

V praksi je v Slovenski vojski elektronsko izvidovanje marsikdaj enako razumljeno kot elektronsko bojevanje[23], vendar so med njima zelo pomembne razlike: medtem ko je elektronsko izvidovanje obveščevalna zvrst, ki jo za potrebe obveščevalne službe (na obrambnem področju) izvaja Slovenska vojska oziroma za to specializirana enota Slovenske vojske, je elektronsko bojevanje izrazito vojaška aktivnost, ki jo izvajajo vsa poveljstva in enote Slovenske vojske. Pristojnosti odrejanja nalog pri elektronskem izvidovanju so specifično opredeljene z zakonom o obrambi, medtem ko so pa pristojnosti odrejanja nalog pri elektronskem bojevanju pod izključno pristojnostjo vojaškega poveljnika.

Iz navedene terminološke opredelitve lahko zaključim, da na obveščevalnem področju ni terminološke usklajenosti, kar lahko vodi v pravno in strokovno zmedo, na drugi strani pa otežuje kakovostno raziskovalno delo, znanstveno preučevanje in izvajanje nadzorne funkcije. V okviru splošne nacionalne obveščevalne politike bi bilo treba zato vzpostaviti enotne terminološke okvirje za vse subjekte izvajanja obveščevalne dejavnosti v okviru nacionalno varnostnega sistema. Menim, da obstoječa terminološka zmeda lahko dodatno ovira naše napore k večji preglednosti in odprtosti te zvrsti in obveščevalne dejavnosti nasploh; nerazumljivost in nejasnost ponavadi v družbi nehote vzbujata dvom. Uporabljana terminologija na obrambnem in vojaškem področju bi se morala poenotiti s terminologijo, ki velja v nacionalnem pravnem redu. Že nekaj let si predstavniki obveščevalne zvrsti SIGINT na obrambnem področju prizadevajo, da bi dobili temeljni organizacijski akt ministra za obrambo, ki bi med drugim postavil in poenotil tudi te temelje. Vse do takrat pa bo obveščevalna zvrst SIGINT opredeljena neustrezno.

[23] Elektronsko bojevanje je vrsta informacijskega delovanja, ki uporablja elektromagnetno energijo, vključujoč elektromagnetno energijo, za izrabo in prevlado v elektromagnetnem spektru ali za napad na sovražnika. Obsega prestrezanje in razpoznavanje elektromagnetnega oddajanja, uporabo elektromagnetne energije za zmanjšanje ali preprečevanje sovražne uporabe elektromagnetnega spektra ter aktivnosti za zagotovitev učinkovitosti njegove izrabe s strani lastnih sil. Obstajajo tri skupine ukrepov elektronskega bojevanja: podporni ukrepi elektronskega bojevanja, elektronski protiukrepi in elektronski zaščitni ukrepi (PDRIU 2006, 94).

4 OBVEŠČEVALNA DEJAVNOST IN OBVEŠČEVALNA ZVRST SIGINT V SODOBNI DRUŽBI

Z razvojem demokracije družba vedno bolj vpliva na oblikovanje celotne nacionalno varnostne politike z različnimi mehanizmi, torej tudi na nacionalno obveščevalno politiko. In ravno tukaj trčimo na paradoks, omenjen že v uvodu naloge. Na eni strani kultura tajnosti in hkrati pooblastilo obveščevalnim službam, da v točno določenih pogojih lahko posegajo v zasebnost posameznika, torej v človekove pravice in svoboščine, na drugi strani pa je njihov osnovni namen zagotavljanje varnosti države in družbe ter zaščita njunih glavnih interesov. Varnost in nedotakljivost posameznika sta v neposrednem neskladju, ključno pri tem pa je, da so vzpostavljeni učinkoviti mehanizmi, ki ohranjajo obe dimenziji v ravnovesju.

Meja med osebno svobodo in varnostjo obstaja in za demokratično družbo je pomembno, da ima vpliv na to, kje se ta meja postavi.

V nadaljevanju bom opredelila nekaj ključnih mehanizmov v vsaki sodobni družbi, ki so formirani zato, da se tehtnica ne prevesi v napačno stran. A kljub temu, ti mehanizmi dihajo skupaj z družbenim razvojem, zato niso nespremenljivi in univerzalni, še več, marsikje so unikatni, a zato nič manj učinkoviti.

V okviru tega poglavja bo prisotna tudi eksploatacija strukturiranega intervjuja, ki sem ga na tematiko preučevanja družbenih vidikov do obveščevalne dejavnosti izvedla z generalnim direktorjem Obveščevalno varnostne službe Ministrstva za obrambo.

4.1 Nadzor nad obveščevalno dejavnostjo

V naravi obveščevalnih služb je, da zbirajo in analizirajo informacije. Za take dejavnosti je potrebna visoka stopnja tajnosti. Po drugi strani pa obstaja nevarnost, da se takšne informacije zlorabijo za notranje politične namene. Obveščevalne službe lahko ogrozijo družbo in politični sistem, ki bi ga morale ščititi. Zato je poleg nadzora, ki ga opravljajo izvršilni organi, nujen tudi jasen demokratični in parlamentarni nadzor obveščevalnih služb. Samo sistem zavor in ravnovesij vseh vej oblasti lahko prepreči izvršilnim organom ali parlamentu zlorabo obveščevalnih služb za lastne politične namene (Born 2003, 64).

Lowenthal (2009, 199) pa še razlaga, da sposobnost nadziranja informacij v vsaki državi, ne glede na to, ali je demokratična ali ni, pomeni pomembno moč, zato mora biti obveščevalna dejavnost pod neprestanim, stalnim nadzorom.

Kot bomo ugotovili tudi na konkretnem primeru analize mehanizma parlamentarnega ali političnega nadzora nad obveščevalno dejavnostjo v nadaljevanju naloge, gre pri različnih sodobnih demokratičnih državah za različne rešitve sistema zavor in ravnovesij, ki so nastajale v specifičnih, unikatnih družbenih in političnih pogojih, vendar je vsem skupno, da mora demokratični nadzor temeljiti na jasno opredeljenem pravnem okviru, znotraj katerega so obveščevalne organizacije postavljene v državne zakone, ki jih je potrdil parlament. Zakoni bi morali natančno določati omejitve in pristojnosti vsake obveščevalne službe, metode njenega delovanja in načine, s katerimi jo je mogoče pozvati na odgovornost (Born 2003, 64).

Čeprav obveščevalne službe pripadajo izvršilni veji oblasti in so od nje odvisne, ima ključno vlogo pri nadziranju njihovih dejavnosti parlament. V vseh pravnih sistemih imajo parlamenti na voljo različna sredstva za pridobivanje informacij za nadziranje politik in vladajoče administracije, zaščito posameznika ali odkrivanje zlorab in krivic (Born 2003, 80).

In zakaj naj bi parlament sploh moral imeti interes za aktivni nadzor obveščevalne dejavnosti? V Centru za demokratični nadzor nad oboroženimi silami (DCAF 2006b, 1-2) navajajo, da parlament sam po sebi potrebuje visoko kakovostne obveščevalne informacije, da bi lahko pravilno odločal tako o zadevah s področja nacionalne varnosti, kot tudi o številnih drugih vprašanjih. Glede na to, da je parlament tudi sam uporabnik obveščevalnih informacij, pa na drugi strani v okviru nadzorne funkcije prispeva k zagotovitvi:

- demokratične legitimnosti obveščevalnih struktur, v okviru katerega preverja in nadzira uveljavljanje demokratičnih norm v teh strukturah;
- preventivnih ukrepov pred morebitno zlorabo teh struktur v protipravne namene;
- učinkovitosti obveščevalnega sektorja, v okviru katerega nadzira in kot končni arbiter tudi oceni, ali so bila vložena proračunska sredstva upravičeno porabljena.

Iz navedenega se da sklepati, da se potreba po nadzoru obveščevalne dejavnosti pojavi iz dveh osnovnih razlogov: prvi je kultura tajnosti delovanja obveščevalnih struktur in drugi je odnos

med ekspertizo in politiko. To potrjujeta tudi Shulsky in Schmitt (2002, 129) v okviru preučevanja menedžmenta v obveščevalni dejavnosti in nadzora nadzornikov[24].

In če se vrnemo k samim oblikam nadzora, je treba poudariti, da obstajajo v vseh sodobnih družbah poleg najpomembnejšega parlamentarnega nadzora, ki predstavlja nadzor zakonodajne veje oblasti, tudi nadzori v ostalih vejah oblasti (izvršilni in sodni), da pa ob tem ne smemo zanemariti tistih oblik nadzora, ki z vidika njihove neodvisnosti in multipolarnosti niso nič manj pomembni. Gre za različne nadzorne mehanizme, ki jih poznamo skozi nadzor civilne družbe in vnašajo vanjo neko višjo stopnjo demokratičnosti in transparentnosti (ombudsmani, informacijski pooblaščenci, nevladne organizacije, mediji, javnost idr.). Ti mehanizmi so natančneje predstavljeni v nadaljevanju naloge, v 5. poglavju, na primeru Republike Slovenije in še dveh evropskih držav.

Parlamentarno nadzorstvo predstavlja obliko političnega poseganja v delo obveščevalno-varnostnih služb s političnimi sankcijami, ki izhajajo iz razmerja med njim in vlado (Anžič 1996, 59), parlament pa lahko nadzor nad obveščevalno dejavnostjo izvaja z uporabo naslednjih mehanizmov: s parlamentarnimi razpravami, s poslanskimi vprašanji in interpelacijami ter s parlamentarnimi preiskavami. Seveda pa za posamezne mehanizme lahko uporabi svoje proaktivne organe (parlamentarna telesa[25] - odbori in komisije). Vsak izmed njih pokriva določeno področje in ima s tega področja tudi določene pristojnosti nadzora (finance, človekove pravice, zunanja in notranja politika, obveščevalne in varnostne službe, obramba ipd.).

V demokratičnih državah je delovanje obveščevalno-varnostnih služb vedno nadzorovano, še posebej z vidika zakonitosti, učinkovitosti, strokovnosti, varovanja človekovih pravic in temeljnih svoboščin, porabe proračunskih sredstev ter pravilnosti izvajanja strateških usmeritev (Garb 2007, 58).

Na obliko nadzora nad obveščevalnimi službami vplivajo pravna tradicija države, politični sistem in zgodovinski dejavniki. Nekatere države, ki so pod vplivom tradicije britanskega običajnega prava, se nagibajo k poudarjanju sodnega vidika nadzora. Nasprotno dajejo

[24] angl. »Guarding the Guardians«
[25] Na spletni strani Državnega zbora RS imamo v Sloveniji 22 stalnih parlamentarnih delovnih teles, od tega 14 odborov in 8 komisij, tudi nekaj preiskovalnih (www.dz-rs.si).

zakonodajnemu nadzoru prednost evropske kontinentalne države in tiste države, ki so v nekem obdobju moderne zgodovine izkusile represijo policije. Nekatere demokratične države so ustanovile institucijo varuha človekovih pravic, ki ima pooblastila, da lahko preiskuje domnevne kršitve človekovih pravic, ki naj bi jih zakrivile obveščevalne službe. (Born 2003, 66). Večina držav izvaja formalni nadzor na določeni ravni, navadno prek parlamentarnih odborov za nadzor. Področje že obstoječih parlamentarnih odborov, kakor sta odbor za obrambo ali odbor za oborožene sile, je včasih razširjeno še na obveščevalne zadeve. V drugih državah parlament ustanovi parlamentarne odbore ali pododbore, ki se posebej ukvarjajo s tajnimi in obveščevalnimi službami (Born 2003, 65).

Nadzor nad delovanjem obveščevalnih služb v vseh demokratičnih družbah ostaja na splošno manj odprt in razvit, kakor nadzor nad drugimi področji dejavnosti države. Delo parlamentarnih odborov za nadzor obveščevalnih služb navadno ne poteka v povsem odprti javni razpravi in sodelujoči člani parlamenta morajo morda izreči posebno zaprisego, ki jih zavezuje, da spoštujejo zaupnost informacij, ki so jim na razpolago (Born 2003, 66).

V nadaljevanju magistrske naloge si bomo natančneje ogledali, kako je parlamentarni nadzor nad obveščevalno dejavnostjo in zvrstjo SIGINT urejen v Republiki Sloveniji in še v dveh izbranih sodobnih evropskih državah, kateri so njihovi proaktivni organi in na kakšnem pravnem okviru temelji njihovo delovanje. Vendar pa je v intervjuju generalni direktor Obveščevalno-varnostne službe Ministrstva za obrambo[26] poudaril, da je ključno vprašanje, kdo nadzira oziroma kontrolira in zakaj, zato je pomembno tudi vprašanje Garba (2007, 57), ki se sprašuje, kdo je tisti, ki vodi in usmerja ter strokovno nadzira nadzornike in kakšne so njegove strokovne vrednote ter lastnosti.

Delo obveščevalnih služb mora biti ves čas in izključno v službi države.

4.2 Varstvo človekovih pravic in temeljnih svoboščin pri izvajanju obveščevalne dejavnosti in zvrsti SIGINT

Obveščevalne službe imajo (skupaj s policijo) v nasprotju z drugimi državnimi organi dovoljenje in dolžnost, da smejo v natančno določenih pogojih posegati v človekove pravice

[26] Strukturiran intervju z njim, 21. aprila 2010.

in svoboščine, zato parlamentarno nadzorstvo nad obveščevalnimi službami ni pomembno samo zaradi političnih razlogov, temveč je namenjeno tudi zaščiti in varstvu človekovih pravic in svoboščin. Vsekakor je to politična oblika nadzorstva, zato ne more in ne sme biti alternativa sodnemu nadzorstvu, saj parlamentarno nadzorstvo uporablja pri svojem delu pravne norme ter varuje ustavne pravice državljanov. Ključnega pomena pri izvajanju parlamentarnega nadzora je dejstvo, da z njim želi in je pripravljena sodelovati tudi izvršna oblast, saj le tako lahko deluje sistem »checks and balances« (Anžič 1996, 57-58).

Obveščevalne službe so tudi z vidika poseganja v človekove pravice in temeljne svoboščine postavljene v vedno intenzivnejši zakonodajni, sodni in politični nadzor, saj v okviru svojih nalog zagotovo posegajo v človekove pravice in temeljne svoboščine. Omejitve in pristojnosti vsake obveščevalne službe, metode njenega delovanja in načine, s katerimi jo je mogoče pozvati na odgovornost, pa bi morali biti jasno določeni v pravnem okviru oziroma zakonih. Večno vprašanje pa je ali je vsako poseganje nujno, ustrezno in po načelu sorazmernosti. S tega vidika so zato pomembne tudi zakonsko določene sankcije v primeru njihove kršitve zakonitih pristojnosti, ki so lahko civilne in kazenske, politične pa v primeru, ko so državni organi posegli v človekove pravice in temeljne svoboščine z zlorabo položaja in na podlagi odgovornosti nosilcev javnih funkcij. V strokovni literaturi zasledimo mnogo razprav v zvezi s to tematiko, ki izpostavljajo predvsem moralna vprašanja v obveščevalni dejavnosti, njeno lojalnost in harmonijo z voditelji (Shulsky in Schmitt 2002, 167). Herman Michael pa po terorističnih dogodkih v ZDA septembra 2001 le-te poglobljeno dopolnjuje z etičnimi načeli v obveščevalni sferi (Scott in Jackson 2004, 180-194) [27].

Večina demokratičnih držav ima človekove pravice in temeljne svoboščine razglašene v ustavi in jih je mogoče omejevati le z zakonom. Zakoni pa določajo pogoje in način omejevanja pravic. V primeru delovanja obveščevalnih služb se v glavnem omejujejo osebne človekove pravice in svoboščine, zlasti pravica do zasebnosti. Pri tem lahko pravico do zasebnosti, v katero posegajo državni organi pri opravljanju obveščevalne dejavnosti, strnemo v pravico do varstva tajnosti pisem in drugih občil ter na pravico do varstva osebnih podatkov. Pri izvajanju obveščevalne zvrsti SIGINT s strani obveščevalnih služb pa lahko v določenih primerih govorimo o omejevanju ali poseganju v pravice posameznika po komunikacijski zasebnosti. Razlikovati moramo med osredotočenim in neosredotočenim

[27] Gre za članek, objavljen v publikaciji z naslovom *Ethics and Intelligence after September 2001*, istoimenskega avtorja.

spremljanjem elektronskih komunikacijskih omrežij. O t. i. posegu v komunikacijsko zasebnost bi lahko govorili le v primeru osredotočenega prestrezanja komunikacij, ko gre za postopek, pri katerem se v komunikacijskem omrežju zbirajo vsebina, okoliščine in dejstva, povezana s komunikacijami med dvema ali več določljivimi priključki v elektronskih komunikacijskih omrežjih. Gre za zelo prikrit in invaziven poseg v zasebnost, za katerega je vsaka država opredelila svoj sistem odrejanja tovrstnih nalog obveščevalnim službam. V primeru neosredotočenega spremljanja mednarodnih elektronskih komunikacijskih omrežij pa gre predvsem za spremljanje in pridobivanje podatkov o tistih aktivnostih, ki so pomembne za zagotavljanje nacionalne varnosti države, varstvo ustavne ureditve ter zaščito interesov Republike Slovenije in se ne nanaša na določljiv priključek telekomunikacijskega sredstva ali na določenega uporabnika tega priključka, zato v tem primeru ne moremo govoriti o posegu v komunikacijsko zasebnost.

Pri opredeljevanju človekovih pravic in temeljnih svoboščin je treba omeniti tudi Evropsko konvencijo o varstvu človekovih pravic in temeljnih svoboščin[28], ki v 8. členu določa, da ima vsakdo pravico do spoštovanja svojega zasebnega in družinskega življenja, svojega doma in dopisovanja, ter da se javna oblast ne sme vmešavati v izvrševanje te pravice, razen če je to določeno z zakonom in nujno v demokratični družbi zaradi državne varnosti, javne varnosti ali ekonomske blaginje države, zato da se prepreči nered ali zločin, da se zavaruje zdravje ali morala ali da se zavarujejo pravice in svoboščine drugih ljudi.

Prav zaradi narave dela obveščevalnih služb in njihovega poseganja v človekove pravice in temeljne svoboščine, bi si le-te morale v vsaki demokratični družbi brezpogojno prizadevati za učinkovitost, politično nevtralnost, profesionalno etično ravnanje, delovanje v okviru svojih zakonskih pooblastil, v skladu z ustavnopravnimi normami in demokratično prakso države. Pred sodobne obveščevalne službe je zato nedvomno postavljen še zahteven dodaten izziv; poleg potrebe in zahteve po interaktivnem sledenju v različnih trendih opremljenosti, v teoretskih, konceptualnih in metodoloških pristopih, mora delo teh služb temeljiti tudi na znanju, inteligentnosti, politični nevtralnosti in predvsem na profesionalni etiki. Obveščevalna stroka v slovenskem prostoru nima svojega etičnega kodeksa, zato je tudi pred njo dodaten izziv. Čeprav si nedvomno prizadeva, da z vidika poseganja v človekove pravice in temeljne

[28] Evropska konvencija o varstvu človekovih pravic in temeljnih svoboščin; podpisana 4. novembra 1950 v Rimu, veljati je začela 3. septembra 1953. Jugoslavija je ni ratificirala, Slovenija pa se je leta 1991 v deklaraciji o spoštovanju temeljnih konvencij Sveta Evrope enostransko zavezala k spoštovanju te konvencije, 18. maja 1994 jo je ratificirala, objavljena je bila 13. junija 1994, veljati pa je začela 28. junija 1994.

svoboščine vedno uresničuje načelo sorazmernosti, pa prav dejstvo, da imajo obveščevalne službe v nasprotju z drugimi državnimi organi, dovoljenje in dolžnost, da posegajo v človekove pravice in svoboščine, nakaže potrebo po etičnem kodeksu obveščevalne dejavnosti. Seveda se pa takoj zastavlja vprašanje, ali uveljavitev takega kodeksa pomeni tudi višjo raven etičnosti?

Generalni direktor Obveščevalno-varnostne službe Ministrstva za obrambo je o tej temi v intervjuju razmišljal predvsem »o potrebi po odgovornosti posameznika«, ki je na taki dolžnosti, in ob tem razložil, da zakonsko ni mogoče predvideti vseh okoliščin, da pa so se uslužbenci obveščevalnih služb kljub temu »dolžni obnašati zakonito, profesionalno, samoocenjevalno, samoomejevalno, etično in odgovorno«. Glede etičnega kodeksa razmišlja drugače in pravi, da za uslužbence obveščevalnih služb velja kodeks javnih uslužbencev, zato v etičnem kodeksu obveščevalne dejavnosti ne vidi posebne dodane vrednosti.

4.3 Demistifikacija obveščevalnih služb

V sodobni demokratični družbi se obveščevalne organizacije vedno bolj odpirajo javnosti prek različnih mehanizmov, kar je odraz stopnje demokratičnosti nekega družbenega sistema. Vedno več strokovne literature iz obveščevalnega področja smo deležni tudi v slovenskem nacionalnem prostoru, vedno več je predstavitev in objav različnih strokovnih in znanstvenih prispevkov in člankov, na slovenskih univerzah se uvajajo obveščevalne vsebine in predmeti, javni nastopi in predstavitve strokovnjakov in avtoritet[29] z obveščevalnega in širše nacionalno varnostnega področja javnosti in v kot že rečeno, preko nadzorne funkcije z različnimi oblikami institucionalnega in neinstitucionalnega nadzora. Vse to je odraz stopnje demokratičnosti nekega družbenega sistema[30].

Demistifikacija[31] obveščevalnih služb in njihove dejavnosti je področje, ki ga prinašajo družbene spremembe in obratno, demistifikacija prinaša družbene spremembe. Družba je tista,

[29] Dr. Damir Črnčec je konec julija 2009 kot prvi direktor Obveščevalno-varnostne službe v slovenski zgodovini dal intervju za Dnevnik oziroma Dnevnikov objektiv (25. julij 2009).
[30] O tovrstnem odrazu stopnje demokratičnosti je govoril tudi aktualni generalni direktor Obveščevalno varnostne službe Ministrstva za obrambo v strukturiranem intervjuju z dne 21. aprila 2010.
[31] O demistifikaciji obveščevalnih služb je govorila ministrica za obrambo, dr. Ljubica Jelušič, ob predstavitvi knjige dr. Damirja Črnčeca *Obveščevalna dejavnost v informacijski dobi*, 16. julij 2009 na Cekinovem gradu v Ljubljani. Njen govor je bil objavljen v članku z naslovom *Sodobne sisteme nacionalne varnosti opazimo šele, ko ne delujejo*, na www.Dnevnik.si (16. julij 2009).

ki mora kritično ocenjevati vse funkcije in atribute, ki ji zagotavljajo varnost in suverenost. Civilna družba skupaj z organi oblasti je namreč lahko edini legitimni apologet obveščevalnim službam. Kultura tajnosti, ki je bila vedno eno od ključnih vodil delovanja obveščevalnih služb, se bo postopoma menjala, ne bo pa prenehala (Črnčec 2009, 85). Glede same kulture tajnosti obstaja splošen konsenz, da je tajnost pomembna sestavina obveščevalne dejavnosti, ker s tem država pridobi prednost pred subjektom, nad katerim izvaja obveščevalno dejavnost. Seveda se takoj pojavi vprašanje, kakšno je razmerje tajno pridobljenih podatkov in podatkov, pridobljenih iz javnih virov. Po nekaterih ocenah (Britovšek 2008, 3) pridobijo obveščevalne službe okoli 90 odstotkov podatkov iz javno dostopnih virov s tako imenovano obveščevalno zvrstjo OSINT. Ostalih 10 odstotkov pridobijo službe z drugimi disciplinami in tajnimi načini zbiranja (npr. SIGINT).

A kljub temu obveščevalne službe niso same sebi namen. Kot ena izmed temeljnih funkcij nacionalno varnostnega sistema, zagotavljajo neke vrste servis za oskrbo z informacijami širokemu krogu institucij, ki so vpete v sistem nacionalne varnosti. Obveščevalne službe se zato demistificirajo tudi z vidika vedno bolj intenzivnega povezovanja in sodelovanja znotraj, v okviru nacionalno varnostnega sistema in navzven, v mednarodnem okolju. Tudi iz tega vidika se kultura tajnosti obveščevalne dejavnosti postopoma menja in se nadomešča z načelom *»potrebe po delitvi z drugimi«*.

Demistifikacija obveščevalnih služb pa po drugi strani poudarja in aktualizira vprašanje poseganja v človekove pravice in svoboščine v razmerju do zagotavljanja nacionalne varnosti. Meja med osebno svobodo in varnostjo obstaja in zelo pomembno je, kje jo postavimo. Nesprejemljivo za demokratično družbo bi bilo, da bi se ta meja postavljala na podlagi neke osebne zaznave, zato je nujen tudi kritični vidik javnosti, da bi lahko zagotovili ravnovesje med sodobno varnostjo na eni strani za ceno varstva človekovih pravic in osebnih svoboščin na drugi strani. In končno se demistifikacija izvaja s transparentnim, legalnim in profesionalno-etičnim delovanjem obveščevalnih služb in tako s svojo celovito podobo v javnosti.

Demistifikacija obveščevalnih služb je proces, ki ga prinašajo družbene spremembe in širše varnostno okolje. Po drugi strani pa demistifikacija sama vnaša družbene spremembe; glede razumevanja vloge obveščevalnih služb s strani družbe, dojemanja kulture tajnosti teh služb in končno tudi neko kritično in objektivno presojo družbe. Zato bi demistifikacija tem službam

morala predstavljati še dodaten motiv: z možnostjo svojega postopnega odpiranja javnosti te službe lahko utemeljujejo svoje profesionalno in etično ravnanje v odnosu do družbe, upravičijo svoj namen, obstoj in vložena sredstva in si na neki način s tem utrjujejo (ali pa tudi ne) svojo nadaljnjo pot.

5 OBVEŠČEVALNA ZVRST SIGINT V SLOVENIJI, NEMČIJI, NA MADŽARSKEM IN V NATU

Vloga in narava obveščevalnega sodelovanja v povezavi z globalizacijo vodita v dejstvo, da se tudi sama obveščevalna dejavnost globalizira. Nekatere multilateralne in bilateralne obveščevalne povezave v zadnjem času intenzivno poglabljajo svoje odnose in obnavljajo zmogljivosti (Len in Hughes 2009, 6-24).

Republika Slovenija in njena nacionalna obveščevalna skupnost sodeluje v različnih mednarodnih intergracijah, do katerih ima poleg koristi tudi nekatere odgovornosti. Ena bolj proaktivnih mednarodnih integracij na preučevanem področju obveščevalne dejavnosti je prav gotovo NATO. Vsekakor je to organizacija, ki pričakuje enako stopnjo proaktivnosti obveščevalnih struktur vseh držav članic. Za nadaljnje preučevanje sem si zato poleg Republike Slovenije, ki je bila v NATO vključena v predzadnjem krogu širitve, izbrala še dve po stažu v NATU starejši in izkušenejši evropski državi, ki sta po mojem mnenju hkrati tudi sodobni in demokratični in sta v nekaterih pogledih zgledno uredili področje obveščevalne dejavnosti in predvsem njene zvrsti SIGINT.

V nadaljevanju tega poglavja bom v okviru primerjalne analize v teh treh državah namenila posebno pozornost preučevanju pravnega okvira, na katerem temeljita delo in organizacija obveščevalnih služb in tudi analiza parlamentarne nadzorne funkcije, ki predstavlja temeljnega varuha vsake demokracije. Poglavje bom zaključila z analizo organiziranosti in sodelovanja na področju obveščevalne zvrsti SIGINT v okviru zavezništva, ki so brez izjeme v sodobnem globalnem varnostnem okolju primorane k vzpostavitvi intenzivnega in učinkovitega sodelovanja.

5.1 REPUBLIKA SLOVENIJA

5.1.1 Pravni okvir obveščevalnih struktur v Republiki Sloveniji

Obveščevalna zvrst SIGINT se, kot sestavni del obveščevalne dejavnosti v Republiki Sloveniji izvaja na dveh ravneh; na vladni ravni v okviru Slovenske obveščevalno-varnostne

agencije in v obrambno-vojaškem resorju v okviru obveščevalnih zmogljivosti Ministrstva za obrambo oziroma Slovenske vojske. V svojem preučevanju se bom omejila samo na obveščevalno dejavnost in znotraj nje obveščevalno zvrst SIGINT, ki je usmerjena na obveščevalno dejavnost zaznavanja tveganj in groženj od zunaj, zato namenoma ne bom zahajala v področje policijske dejavnosti (angl. police intelligence), ki je v osnovi namenjeno odkrivanju in preprečevanju notranjih groženj in pregonu kaznivih dejanj, res pa je, da za svoje delovanje pogosto uporablja enake metode dela in pri tem uporablja enako operativno tehniko. Ključna razlika je v namenu zbiranja teh podatkov, ki se pri policijski dejavnosti ne nanaša na obveščevalno dejavnost za potrebe nacionalne varnosti.

Obveščevalna zvrst SIGINT je eden izmed načinov zbiranja obveščevalnih podatkov, predvsem za izvajanje zunanje obveščevalne dejavnosti. Iz tega razloga se bom v okviru svojega preučevanja omejila samo na tiste obveščevalne strukture v Republiki Sloveniji, ki se ukvarjajo z zunanjo obveščevalno dejavnostjo in pri tem uporabljajo tudi obveščevalno zvrst SIGINT. V Republiki Sloveniji imamo tako naslednjo strukturo obveščevalnih služb [32]:

- Obveščevalno-varnostna služba Ministrstva za obrambo, ki je služba v sestavi ministrstva za obrambo, z vojaško obveščevalno strukturo Slovenske vojske in
- Slovenska obveščevalno-varnostna agencija, ki je samostojna služba Vlade Republike Slovenije.

Normativna ureditev v Republiki Sloveniji

Pravne temelje delovanja obeh predstavljajo ustava, zakonski in drugi predpisi ob upoštevanju splošno veljavnih načel mednarodnega prava in veljavnih ter ratificiranih mednarodnih pogodb.

Pravno-vsebinski okvir delovanja obeh obveščevalnih služb za izvajanje obveščevalne zvrsti SIGINT pa določata dva ključna zakona in sicer:

- Zakon o Slovenski obveščevalno-varnostni agenciji (ZSOVA) s predlaganimi spremembami in
- Zakon o obrambi (ZOBr).

[32] Ker je moje interesno področje preučevanja obveščevalna zvrst SIGINT, namenoma ne bom zahajala v pristojnosti in področje dela drugih organov znotraj nacionalno varnostnega sistema, kot npr. kriminalistične policije v okviru ministrstva za notranje zadeve in analitične službe ministrstva za zunanje zadeve, ki za svoje delovanje ne uporablja zmogljivosti SIGINT.

Natančnejša opredelitev posameznih zakonskih določil v obeh pravnih aktih si z vidika razumevanja pristojnosti in pooblastil posameznih služb, preglednosti ter aktualizacije vprašanja pravne skladnosti zaslužijo posebno pozornost, zato bom to podrobneje obravnavala v nadaljevanju. V splošnem pa lahko rečemo, da se Slovenska obveščevalno-varnostna agencija (SOVA[33]) kot samostojna vladna služba ukvarja pretežno z obveščevalno dejavnostjo, tako da pridobiva in vrednoti podatke, posreduje informacije iz tujine, ki so pomembne za zagotavljanje varnostnih, političnih in gospodarskih interesov države, ter o organizacijah, skupinah in osebah, ki s svojo dejavnostjo iz tujine ali v povezavi s tujino ogrožajo ali bi lahko ogrozile nacionalno varnost države in njeno ustavno ureditev.

Obveščevalno-varnostna služba Ministrstva za obrambo opravlja tako obveščevalne, protiobveščevalne[34] in tudi varnostne[35] naloge. Pri tem je pa treba poudariti, da zanjo veljajo poleg ZOBr tudi ZSOVA, Zakon o Policiji (ZPol) in Zakon o kazenskem postopku (ZKP), medtem ko ima Slovenska obveščevalno-varnostna agencija za svojo podlago le ZSOVA.

Prav to »prekrivanje« zakonskih določil, pooblastil in pristojnosti med službama, oziroma sklicevanje na drug zakon pri uporabi posebnih oblik pridobivanja podatkov v primeru Obveščevalno varnostne službe ministrstva za obrambo, je zelo nenavadno in z vidika transparentnosti neprimerno, na kar so že pred več leti opozarjali domači strokovnjaki[36]. Zato si bomo v nadaljevanju to natančneje pogledali.

---

[33] Agencija ima svoje korenine v Službi državne varnosti (SDV). V času osamosvajanja Republike Slovenije leta 1991, se je takratna republiška SDV preimenovala v Varnostno informativno službo (VIS) in je bila organizacijsko umeščena pod notranje ministrstvo. To ime je služba nosila le do leta 1993, ko je bil sprejet Zakon o vladi Republike Slovenije, ki je VIS preimenoval in agencijo organizacijsko umestil iz sestave notranjega ministrstva pod Vlado, kot njeno samostojno službo.

[34] Obveščevalne in protiobveščevalne naloge obsegajo zbiranje, dokumentiranje in analiziranje informacij ter podatkov, ki so pomembni za obrambne interese države oziroma varovanje takih podatkov, zlasti pa ugotavljanje in ocenjevanje vojaških in politično varnostnih razmer ter vojaških zmogljivosti zunaj države, ki so posebnega pomena za varnost države; zbiranje in ocenjevanje podatkov o razmerah na območjih, kjer med izvrševanjem obveznosti, prevzetih v mednarodnih organizacijah oziroma pri opravljanju vojaške službe, delujejo tudi pripadniki Slovenske vojske ter odkrivanje in preprečevanje dejavnosti obveščevalnih služb, vojaških organizacij ter drugih organov in organizacij, ki ogrožajo obrambne interese države, Slovensko vojsko ali ministrstvo.

[35] Varnostne naloge na obrambnem področju so odkrivanje, preiskovanje in preprečevanje ogrožanja varnosti določenih oseb, delovnih mest, objektov in okolišev, ki jih uporablja 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 ter usmerjanje dela vojaške policije pri opravljanju določenih varnostnih nalog v skladu z zakonom.

[36] Adam Purg o tem piše v svojem delu *Obveščevalne službe* iz leta 1995 na strani 137. Medtem se je ZOBr že nekajkrat spreminjal, a nikoli ni posegel v te okvire.

Kot že rečeno, določata pravno-vsebinski okvir delovanja obeh obveščevalnih služb za izvajanje nalog SIGINT dva zakona, ZSOVA in ZOBr. V okviru teh dveh zakonov nacionalna zakonodaja uveljavlja na tem področju tudi dva termina in sicer:

- *spremljanje mednarodnih sistemov zvez* v okviru 20. in 21. člena obstoječega Zakona o Slovenski obveščevalno-varnostni agenciji, ki je v spreminjanju, in
- *elektronsko spremljanje mednarodnih sistemov zvez* v okviru 32. člena Zakona o obrambi.

Zakon o Slovenski obveščevalno-varnostni agenciji in Zakon o spremembah in dopolnitvah Zakona o Slovenski obveščevalno-varnostni agenciji

Trenutno aktualni predlog Zakona o spremembah in dopolnitvah Zakona o Slovenski obveščevalno-varnostni agenciji predlaga nekatere spremembe in dopolnitve vsebine določbe 21. člena obstoječega Zakona o Slovenski obveščevalno-varnostni agenciji, ki se nanašajo na spremljanje mednarodnega sistema zvez.

Spremljanje mednarodnih sistemov zvez je po mojem mnenju določba, ki predstavlja podlago 4. odstavku 32. člena Zakona o obrambi (ZOBr). Ta uveljavlja pravno določbo *elektronsko spremljanje mednarodnih sistemov zvez* in hkrati tudi pravno podlago za izvajanje strokovnih nalog Enote za elektronsko bojevanje Slovenske vojske *za potrebe obveščevalno varnostne službe ministrstva za obrambo*. Sedanja določba 21. člena ZSOVA je resda preširoka, premalo določna in tudi izrazoslovno neusklajena s pravno zakonodajo s področja sodobnih elektronskih komunikacij. Zato so predlagane spremembe in dopolnitve smiselne in na neki način utemeljene.

Predlog Zakona o spremembah in dopolnitvah ZSOVA pa predlaga dve vsebinsko in z vidika poseganja v človekove pravice bolj omejeni določbi 20. člena in sicer, z opredelitvijo dveh vrst posebnih oblik pridobivanja podatkov s posegom v t. i. mednarodne sisteme zvez, in sicer:

- strateški (neosredotočen) nadzor mednarodnih elektronskih komunikacijskih omrežij in
- osredotočeno prestrezanje komunikacij v mednarodnih elektronskih komunikacijskih omrežjih.

Gre za strokovno sprejemljiv, vendar invazivni poseg v terminološke določbe 20. in 21. člena zakona, zato bi bilo treba v okviru pravno-strokovne preučitve predvideti njegove morebitne implikacije na 32. člen ZOBr.

Kljub temu da je v interni strokovni javnosti veliko različnih interpretacij o (ne)povezavi določbe 4. odstavka 32. člena ZOBr z določbo 20. člena ZSOVA, je nedvomna povezava tega odstavka z 21. členom ZSOVA očitna v praksi in tudi z vidika izvajanja nadzorne funkcije. Tudi zadnja interpretacija informacijske pooblaščenke z vloženo *Zahtevo za oceno ustavnosti 21. člena ZSOVA ter 4. odstavka 32. člena ZOBr* nedvomno kaže na to, saj v njej navaja, da gre po njenem mnenju za sporno določbo, ki je »v obeh aktih v neskladju z Ustavo Republike Slovenije« in ki »nedopustno širi spremljanje mednarodnih sistemov zvez za vnaprej nedoločene namene« (www.ip-rs.si)[37].

Zakon o obrambi

Pravna podlaga za izvajanje obveščevalne zvrsti SIGINT na obrambnem področju je opredeljena z Zakonom o obrambi (ZOBr, 32. člen, 4. odstavek), ki pravi:
»Elektronsko spremljanje mednarodnih sistemov zvez, pomembnih za obrambne interese države, opravljajo za obveščevalno varnostno službo ministrstva in druge potrebe, enote za elektronsko bojevanje Slovenske vojske.«

Če odstavek tega člena natančneje analiziramo, z vidika navezovanja na druga zakonska in podzakonska določila, dobimo vsaj tri sklope, ki zaslužijo posebno pozornost, in sicer:

- Prvi sklop je formulacija »spremljanje mednarodnih sistemov zvez«, ki je preširoka, premalo določna in izrazoslovno neusklajena s pravno zakonodajo s področja sodobnih elektronskih komunikacij.

[37] Informacijska pooblaščenka je lani na Ustavno sodišče vložila Zahtevo za oceno ustavnosti 21. člena ZSOVA ter 4. odstavka 32. člena ZOBr (zahteva za oceno kršitve 2., 15., 37. in 38. člena Ustave Republike Slovenije). Ustavno sodišče tako že drugič rešuje pobudo za oceno ustavnosti 21. člena ZSOVA in prvič za 4. odstavek 32. člena ZOBr. V prvem primeru pobude je sodišče ocenilo, da se zahteva Vrhovnega sodišča za oceno ustavnosti 21. člena ZSOVA zavrže (Sklep Ustavnega sodišča št.:U-I-216/07-8 z dne 4. 10. 2007), je pa sodišče podalo določena navodila v zvezi s tem vprašanjem. Ustavno sodišče je namreč v Sklepu U-I45/08-21 dne 8. 1. 2009 ponovno zavrglo pobudo za oceno ustavnosti 21. člena ZSOVA s stališčem, da se spremljanje mednarodnih sistemov zvez kot del obveščevalne dejavnosti lahko nanaša le na območje zunaj državnega ozemlja R Slovenije in ko ne gre za konkretnega posameznika, temveč za spremljanje zadeve. Spremljajo se lahko samo komunikacije med dvema ali več tujimi telekomunikacijskimi priključki, pri čemer pa se nadzor ne sme nanašati na določljiv priključek (Črnčec 2009, 98-99).

- Drugi sklop predstavlja formulacija »obrambni interesi države«. Resolucija o strategiji nacionalne varnosti Republike Slovenije (ReSNV-1), ki je temeljni dokument na področju nacionalne varnosti in nacionalnih interesov, opredeljuje samo dva trajna, življenjsko pomembna interesa in strateški interes, ne omenja ali opredeljuje pa obrambnih interesov.

- Tretji sklop je besedna zveza »in druge potrebe«, ki ni dovolj eksplicitna. Morebitna interpretacija tega sklopa v smislu zakonite podlage za »poveljnike Slovenske vojske kot morebitne naročnike za odrejanje SIGINT nalog« lahko vodi v stigmatizacijo vojaške obveščevalne dejavnosti in zvrsti SIGINT na obrambnem področju, zato je treba čim prej odpraviti vse dvome in nejasnosti.

Analiza prvega sklopa 4. odstavka 32. člena ZOBr kaže široko, v drugem sklopu pa premalo določno formulacijo. Zadnji, tretji sklop pa ponuja široko in različno interpretacijo. Lahko ga razumemo tudi kot odprto možnost horizontalnega povezovanja SIGINT subjektov v sistemu nacionalne varnosti, kar je lahko eden od rezultatov prihodnjih transformacijskih procesov na področju obveščevalne dejavnosti nasploh in morebitnega preoblikovanja nacionalnih obveščevalnih struktur. Čeprav v zvezi s tem zaenkrat ne zasledimo nikakršnih konkretnejših indikatorjev, kljub temu lahko ostaja odprta možnost za prihodnje razprave na vladni ravni.

Obveščevalna zvrst SIGINT v Slovenski vojski in Ministrstvu za obrambo

Slovenska vojska do leta 2000 ni razpolagala z zmogljivostmi elektronskega izvidovanja, le-te so bile do tega leta izključno v sestavi Obveščevalno-varnostne službe Ministrstva za obrambo (OVS) kot samostojna izpostava službe.
Danes je Enota za elektronsko bojevanje Slovenske vojske umeščena na taktično raven in je po vojaški doktrini opredeljena kot enota bojne podpore[38] Slovenske vojske. Enota je organizirana, opremljena in usposobljena za izvajanje SIGINT nalog, skladno s cilji sil, ki jih je Slovenska vojska sprejela, pa razvija tudi zmogljivosti elektronskega bojevanja za podporo pri zaščiti sil slovenskega vojaškega kontingenta v mednarodnih operacijah in misijah. Podrobnejša analiza teh zmogljivosti bo sledila v nadaljevanju naloge, v poglavju *6. Obveščevalna zvrst SIGINT na obrambnem področju.*

[38] Po aktualni vojaški doktrini med sile za bojno podporo prištevamo vse sile namenjene zagotavljanju ognjene podpore in operativne podpore silam za bojevanje. Sem uvrščamo inženirske enote, artilerijske enote, obveščevalne in izvidniške enote, enote radiološke, kemične in biološke obrambe, enote za elektronsko bojevanje, mornariške enote, enote vojaške policije in letalske enote (PDRIU 2006, 103).

5.1.2 Politični ali parlamentarni nadzor v Sloveniji

Obveščevalne službe imajo (skupaj s policijo) za razliko od drugih državnih organov, v natančno določenih pogojih pristojnost in dolžnost, da smejo posegati v človekove pravice in svoboščine. Zato je pri tem ključno, da je nadzorna funkcija, ne glede na politično polarizacijo učinkovita in permanentno prisotna še posebej, kadar gre za obveščevalno zvrst SIGINT, ki lahko pomeni tudi poseganje v komunikacijsko zasebnost posameznika.

Kot eno od večjih demokratičnih pridobitev ima demokratična Slovenija danes vzpostavljene vse oblike nadzora nad obveščevalnimi službami (Črnčec 2009, 102).

V Sloveniji nadzirajo delo obveščevalnih služb vse tri veje oblasti v okviru svojih pristojnosti: zakonodajna, izvršilna in sodna. Ob tem pa ne smemo pozabiti, da poleg teh obstaja tudi nadzor civilne družbe. Njihovo nadzorstvo nad obveščevalnimi službami je raznoliko in obsega več ravni:

- politično ali parlamentarno nadzorstvo (prek parlamentarnih odborov in komisij - odbor za obrambo, komisija za nadzor obveščevalnih in varnostnih služb, ipd.);
- strokovno nadzorstvo oziroma nadzorstvo vlade v okviru izvršilne veje oblasti;
- sodno nadzorstvo, preko sodišč, pristojnih za odrejanje posebnih oblik pridobivanja podatkov obveščevalnih služb in človekove pravice (ustavno in vrhovno sodišče, preiskovalni sodniki, tožilstvo);
- nadzorstvo neodvisnih institucij (informacijska pooblaščenka, varuhinja človekovih pravic);
- nadzorstvo javnosti (prek medijev in državljanov z uveljavljanjem pravice do informacij javnega značaja, s pritožbami).

Črnčec (2009, 100-101) deli nadzor obveščevalne dejavnosti na institucionalizirani in neinstitucionalizirani nadzor. V institucionaliziranega uvršča politični/parlamentarni nadzor, strokovni nadzor, sodni nadzor in nadzor neodvisnih institucij, v neinstitucionaliziranega pa poleg nadzora javnosti, uvršča še državljanski nadzor. Kot potrdi Garb (2007, 110), pa različne oblike nadzora nad delovanjem obveščevalno-varnostnih služb povečujejo raven njihove legitimnosti, omejujejo zlorabo moči ter s tem služijo varstvu človekovih pravic in temeljnih svoboščin.

Večina držav izvaja formalni politični nadzor na določeni ravni, navadno prek parlamentarnih odborov za nadzor. V Republiki Sloveniji je bila za področje nadzora nad delovanjem obveščevalnih in varnostnih služb ustanovljena posebna parlamentarna komisija (Komisija za nadzor obveščevalnih in varnostnih služb).

Parlamentarna komisija za nadzor obveščevalnih in varnostnih služb je ustanovljena s posebnim Zakonom o parlamentarnem nadzoru obveščevalnih in varnostnih služb (ZPNOVS), po katerem ima pristojnost in nalogo, da nadzira, ali gre za ustavno in zakonito izvajanje dejavnosti nadziranega subjekta (obveščevalne in varnostne službe v Republiki Sloveniji) (ZPNOVS, 6. člen). Vlada mora komisiji po zakonu predložiti v obravnavo celovito poročilo o delu in finančnem poslovanju posamezne nadzorovane službe v preteklem letu. Komisijo, ki ima po zakonu največ 9 članov, sestavljajo predstavniki opozicijskih strank in strank parlamentarne večine, vodi pa jo opozicijski predstavnik. Tudi na ta način je vzpostavljen sistem zavor in ravnovesij nadzora izvršilne veje oblasti obeh političnih opcij (angl. checks and balances). Zakon (ZPNOVS) med drugim v prvem odstavku 11. člena določa še, da so seje komisije zaprte za javnost, v 8. členu pa zavezuje člane komisije in ostale sodelujoče k varovanju tajnih podatkov, s katerimi so bili seznanjeni ali so jih pri svojem delu pridobili.

Nadzor nad zakonitostjo izvajanja obveščevalne zvrsti SIGINT na obrambnem področju in znotraj Slovenske vojske

Ker imamo v Sloveniji deljeno obveščevalno dejavnost na dve povsem ločeni obveščevalni službi (SOVA in OVS), je s stališča demokratičnega nadzora to zelo ugodno, vendar po drugi strani njuna delitev dela pomeni večjo razpršenost pridobljenih obveščevalnih podatkov in manjšo učinkovitost. Po drugi strani pa sta navzočnost in razpršenost nadzora nad tem subjektom nedvomno jasen kazalec demokratičnosti nekega političnega sistema (Črnčec 2009, 101).

Nadzor nad obveščevalno zvrstjo SIGINT v obrambno-vojaškem resorju poteka na več ravneh, ki si jih bomo natančneje ogledali v nadaljevanju, v poglavju 6.2.

5.1.3 Varstvo človekovih pravic in temeljnih svoboščin ter varstvo komunikacijske zasebnosti

Ustava Republike Slovenije[39] je pri določanju in varovanju človekovih pravic in temeljnih svoboščin nedvoumna. Človekove pravice in temeljne svoboščine natančneje opredeljuje v svojem drugem poglavju in jih lahko v splošnem razdelimo na politične, sodne, ekonomske, kulturne, socialne, zdravstvene in druge. Prav tako ustava določa varovanje človekovih pravic. Vsak poseg v ustavno pravico je strogo vezan na urejanje z zakonom. Členi iz ustave, ki si z vidika poseganja v človekove pravice in temeljne svoboščine zaradi narave dela obveščevalnih služb zaslužijo posebno pozornost so:

- 15. člen, ki govori o uresničevanju in omejevanju pravic,
- 16. člen, ki govori o začasni razveljavitvi in omejitvi pravic,
- 35. člen, ki govori o varstvu zasebnosti in osebnostnih pravic,
- 37. člen, ki govori o varstvu tajnosti pisem in drugih občil,
- 38. člen, ki govori o varstvu osebnih podatkov, in
- 87. člen, ki navaja zakonske pristojnosti državnega zbora v zvezi s pravicami.

Če konkretneje pogledamo najbolj izstopajoče ustavne določbe po tem vprašanju ugotovimo, da drugi odstavek 15. člena ustave govori naslednje: »Z zakonom je mogoče predpisati način uresničevanja človekovih pravic in temeljnih svoboščin, kadar tako določa ustava, ali če je to nujno zaradi same narave posamezne pravice ali svoboščine«, ki se dopolni s 87. členom ustave: »Pravice in obveznosti državljanov ter drugih oseb lahko državni zbor določa samo z zakonom.« Tretji odstavek 15. člena ustave pa »omejuje človekove pravice in svoboščine v primerih, ki jih neposredno določa že sama ustava.«

V Republiki Sloveniji izvajata obveščevalno dejavnost Obveščevalno-varnostna služba Ministrstva za obrambo, ki je služba v sestavi ministrstva za obrambo, in Slovenska obveščevalno-varnostna agencija, ki je samostojna služba Vlade RS. Njuno delovanje je skladno z ustavnimi določili (15. in 87. člen ustave) urejeno z zakoni (ZSOVA in ZOBr), s katerimi so predpisane njihove naloge in pooblastila.

[39] Ustava sprejeta dne 23. decembra 1991 in objavljena dne 28. decembra 1991 skupaj z ustavnimi spremembami (Ustavni zakon o spremembi 68. člena Ustave Republike Slovenije z dne 14. julija 1997 in dopolnitve z dne 25. julija 2000 – Ustavni zakon o dopolnitvi 80. člena Ustave Republike Slovenije).

Po ustavni določbi je človekove pravice in temeljne svoboščine mogoče omejevati le z zakonom. Zakoni določajo pogoje in način omejevanja pravic. Na področju obveščevalne dejavnosti se v glavnem omejujejo osebne človekove pravice in svoboščine, zlasti pravica do zasebnosti. Pri tem lahko pravico do zasebnosti, v katero posegajo državni organi pri opravljanju obveščevalne dejavnosti, strnemo v pravico do varstva tajnosti pisem in drugih občil ter na pravico do varstva osebnih podatkov, saj sta ti pravici opredeljeni še kot posebne človekove pravice v sklopu ustavnega varstva zasebnosti, ki ga določa 35. člen ustave.

Republika Slovenija je tudi podpisnica Evropske konvencije o varstvu človekovih pravic in temeljnih svoboščin in se je pri vprašanju zagotavljanja in poseganja na področje človekovih pravic in temeljnih svoboščin obvezala k njenemu spoštovanju in upoštevanju določil. Po njenem 8. členu mora namreč vsaka država zagotavljati pravico do zasebnosti dopisovanja in na drugi strani omejevati vmešavanje v te pravice, razen v določenih primerih.

Obveščevalna zvrst SIGINT in varstvo komunikacijske zasebnosti

Spremljanje mednarodnih sistemov zvez je v 20. členu ZSOVA opredeljeno kot ena izmed posebnih oblik pridobivanja podatkov. Tudi sprememba tega zakona predvideva namesto ene dve ločeni določbi (strateški nadzor in osredotočeno prestrezanje komunikacij) kot posebni obliki pridobivanja podatkov. Da bi lahko razčlenjevali te določbe z vidika poseganja v zasebnost ali natančneje v komunikacijsko zasebnost posameznika, ki je opredeljena še kot posebna človekova pravica v sklopu ustavnega varstva zasebnosti (po 35. členu ustave), je treba opredeliti njihovo odrejanje glede na samo invazivnost posega in mehanizme nadzora oziroma kontrole uporabe.

Spremljanje mednarodnih sistemov zvez (po novem strateški nadzor) bo odrejal direktor agencije s pisno odredbo. Odredba mora vsebovati določene podatke, opredeljene v zakonu. Strateški nadzor mednarodnih elektronskih komunikacijskih omrežij je postopek, pri katerem se v javnem komunikacijskem omrežju med nedoločljivimi komunikacijskimi priključki v mednarodnih elektronskih komunikacijskih omrežjih spremljajo in pridobivajo podatki o tistih aktivnostih, ki so pomembne za zagotavljanje nacionalne varnosti države, varstvo ustavne ureditve ter zaščito interesov Republike Slovenije. Strateški nadzor mednarodnih elektronskih komunikacijskih omrežij se ne sme nanašati na določljiv priključek telekomunikacijskega sredstva ali na določenega uporabnika tega priključka. Ker gre pri tej

posebni obliki pridobivanja podatkov za neosredotočeno spremljanje elektronskih komunikacijskih omrežij, v tem primeru ne moremo govoriti o posegu v komunikacijsko zasebnost[40].

Drugačna zgodba, pa je v primeru osredotočenega prestrezanja komunikacij v mednarodnih elektronskih komunikacijskih omrežjih, ki pomeni poseg v komunikacijsko zasebnost, saj je prestrezanje komunikacij osredotočeno na vnaprej znan cilj. Prestrezanje komunikacij v mednarodnih elektronskih komunikacijskih omrežjih je postopek, pri katerem se v javnem komunikacijskem omrežju zbirajo vsebina, okoliščine in dejstva, povezana s komunikacijami med dvema ali več določljivimi priključki v mednarodnih elektronskih komunikacijskih omrežjih. Zato je predlog spremembe zakona predvideval, da bo osredotočeno prestrezanje komunikacij v mednarodnih elektronskih komunikacijskih omrežjih odrejal sodnik Vrhovnega sodišča Republike Slovenije kot najvišji predstavnik sodne veje oblasti. S tem se namreč predhodna in naknadna kontrola oziroma nadzor uporabe osredotočenega prestrezanja prilagaja posegu v komunikacijsko zasebnost posameznika, tako da je določena sodna pristojnost odrejanja uporabe invazivnejše posebne oblike pridobivanja podatkov in tudi morebitnega podaljšanja izvajanja te oblike pridobivanja podatkov (podaljševanje trajanja odredbe).

Če se pri analizi poseganja v temeljne človekove pravice in svoboščine z izvajanjem obveščevalne zvrsti SIGINT v obrambnem resorju navežem poleg zgornje še na zadnjo interpretacijo informacijske pooblaščenke z vloženo Zahtevo za oceno ustavnosti 21. člena ZSOVA ter 4. odstavka 32. člena ZOBr, o kateri sem pisala v poglavju 4.1., je moja ugotovitev naslednja:

4. odstavek 32. člena ZOBr opredeljuje spremljanje mednarodnih sistemov zvez, kot strateški nadzor elektronskih mednarodnih komunikacijskih omrežij in je postopek, pri katerem se v javnem komunikacijskem omrežju med nedoločljivimi komunikacijskimi priključki v mednarodnih elektronskih komunikacijskih omrežjih spremljajo in pridobivajo podatki o tistih aktivnostih, ki so pomembne za obrambne interese Republike Slovenije. Strateški nadzor mednarodnih elektronskih komunikacijskih omrežij se ne nanaša na določljiv priključek telekomunikacijskega sredstva ali na določenega uporabnika, zato v tem primeru

[40] Povzeto iz obrazložitve Predloga Zakona o spremembah in dopolnitvah Zakona o Slovenski obveščevalno-varnostni agenciji.

ne moremo govoriti o posegu v komunikacijsko zasebnost oziroma v poseganje človekovih pravic in svoboščin. Da bi se izognili vsem nejasnostim in dvomom v prihodnje, pa je treba s spremembo ZSOVA uskladiti tudi 4. odstavek 32. člena ZOBr.

5.2 ZVEZNA REPUBLIKA NEMČIJA

5.2.1 Pravni okvir obveščevalnih struktur v Zvezni Republiki Nemčiji

Zvezna Republika Nemčija ima naslednjo obveščevalno strukturo[41]:

- Zvezna obveščevalna služba (BND),
- Vojaška varnostna služba (MAD) in
- Zvezni urad za varstvo ustavne ureditve (BfV).

Glavna nemška obveščevalna služba je Zvezna obveščevalna služba[42] (Bundesnachrichtendienst - BND) in je skladno z 2. odstavkom 1. člena Zakona o Zvezni obveščevalni službi (Gesetz über den Bundesnachrichtendienst) edina zunanja obveščevalna služba v Nemčiji. Organizacijsko je umeščena pod Zvezni urad nemškega kanclerja (pod urad nemškega predsednika vlade) z glavno nalogo zbiranja obveščevalnih informacij o tujini in s pristojnostjo civilne in vojaške zunanje obveščevalne dejavnosti. Zbiranje obveščevalnih podatkov o tujini izvaja služba z aktivnostmi zunaj države in tudi z zbiranjem obveščevalnih podatkov o tujini znotraj države. To pa ne pomeni notranje obveščevalne dejavnosti, za kar je zakonsko odgovoren in pooblaščen Zvezni urad za varstvo ustavne ureditve (Bundesamt für Verfassungsschutz BfV), ki je organizacijsko umeščen pod nemško ministrstvo za notranje zadeve. Zakon o Zvezni obveščevalni službi namreč v 1. odstavku 1. člena izrecno prepoveduje uporabo policijskih pooblastil in izvajanje policijskih nalog Zvezni obveščevalni službi in njenim delavcem (Rieger 1986).

Zvezni urad za varnost informacijske tehnologije (Bundesamt für sicherheit in der informationstechnik BSI) spada pod ministrstvo za notranje zadeve, vendar pa njegova primarna dejavnost po zakonu (Gesetz zur Stärkung der Sicherheit in der Informationstechnik

[41] Struktura je objavljena na spletnih straneh BND (www.bnd.de).
[42] BND ima svoj sedež v Pullachu in Berlinu.

des Bundes)[43] ni opredeljena kot obveščevalna oziroma notranja obveščevalna dejavnost, kot je to določeno za BfV. Naloge Zveznega urada za varnost informacijske tehnologije so namreč specializirane na varnost vladnih informacijskih sistemov in državnih bančnih sistemov, je pa BSI pristojen tudi za nadzor interneta in za odkrivanje internetne kriminalitete (Grizold in drugi 2008, 348).

Zvezna obveščevalna služba (BND) med drugim razpolaga tudi z zmogljivostmi nadzora radijskih in drugih elektronskih komunikacij na ozemlju Nemčije (Grizold in drugi 2008, 347), zbira pa predvsem obveščevalne podatke s političnega, gospodarskega in vojaškega področja ter izdeluje ocene za vlado in trenutne politične cilje izvršne oblasti. Za nadzor radijskih in drugih elektronskih komunikacij oziroma elektronsko spremljanje mednarodnih sistemov zvez (obveščevalna zvrst SIGINT) je odgovoren 2. oddelek Zvezne obveščevalne službe (Schmid 2001, 38)[44], ki svoje zmogljivosti prispeva tudi v globalni obveščevalni sistem.

Službo vodi predsednik Zvezne obveščevalne službe, v uradu kanclerja pa je za delovanje službe pristojen šef urada zveznega kanclerja.

Nemške vojaške obveščevalne in varnostne strukture

Vojaška varnostna služba (Militärischer Abschirmdienst - MAD), ki ima svoj sedež v Kölnu, je podrejena ministru za obrambo in organizirana v pet oddelkov in 12 regionalnih podenot (centrov), ki so razporejene po celotnem ozemlju Nemčije. Vodi jo direktor, ki je general nemške vojske.

Pristojnosti in naloge Vojaške varnostne službe določa Zakon o Vojaški varnostni službi (Gesetz über den Militärischen Abschirmdienst (MAD-Gesetz - MADG)), ki je bil v zadnjih letih kar nekajkrat spreminjan, predvsem zaradi ogrožanja varnosti zaradi terorizma. Glavna naloga Vojaške varnostne službe je zaščita nemških oboroženih sil, njihovih institucij, naprav, oborožitve in objektov ter vojaškega osebja pred tujim vohunstvom in sabotažami. MAD je preko obrambnega ministra podrejena zvezni vladi (Purg 1995, 167).

[43] Zadnja sprememba tega zakona z dne 14. avgust 2009.
[44] Poročilo Evropskega parlamenta z dne 11. julija 2001 o obstoju globalnega sistema za spremljanje zasebnih in gospodarskih komunikacij ECHELON (Schmid 2001).

Vojaška varnostna služba je organizirana v naslednjih petih oddelkih: oddelek TA/V, oddelek I, oddelek II, oddelek III, oddelek IV. Na spletnih straneh službe je navedeno, da je oddelek I zadolžen za izvajanje centralnih strokovnih nalog, ki se nanašajo na določilo pa 10. členu nemške ustave (Grundgesetz) (poseganje v ustavne pravice do komunikacijske zasebnosti po posebnem zakonu), iz česar se da sklepati, da je ta oddelek pristojen tudi za sodelovanje z Uradom zveznih oboroženih sil za nadzor radijskih komunikacij (Amt für Fernmeldwesen Bundeswehr AFMBw), ki spremlja mednarodne sisteme zvez oziroma tehnično obveščevalno zvrst SIGINT.

Glavna obveščevalna služba nemških zveznih oboroženih sil je Obveščevalni urad zveznih oboroženih sil (Amt für Nachrichtenwesen der Bundeswehr ANBw). Primarna naloga tega urada je ocena vojaške moči, načina delovanja in zbiranje podatkov o oboroženih silah drugih držav. Za zbiranje elektronskih podatkov na vojaško obveščevalnem področju pa je zadolžen Urad zveznih oboroženih sil za nadzor radijskih komunikacij (Grizold in drugi 2008, 348) [45]. Za izvajanje teh nalog uporablja posebno infrastrukturo, ki se nahaja v okviru centrov SIGINT, ki so razporejeni po celotnem ozemlju Nemčije, kakor tudi zmogljivosti, ki delujejo v okviru mednarodnih operacij in misij nemških vojaških kontingentov. Nemčija je kot članica zveze NATO tudi aktivna članica v NATO obveščevalni skupnosti, v okviru katere so angažirane vse obveščevalne službe Zvezne Republike Nemčije. V mednarodnih operacijah in misijah sodelujejo predvsem z vojaškimi zmogljivostmi za izvajanje SIGINT nalog, medtem ko le-te podpirajo civilne SIGINT zmogljivosti iz domovine preko satelitske komunikacije.

V t. i. Beli knjigi o nemški varnostni politiki in prihodnosti oboroženih sil[46], ki jo je leta 2006 izdalo nemško Zvezno ministrstvo za obrambo, so jasno opredeljena stališča zbiranja obveščevalnih informacij Nemške zvezne vojske, in sicer za potrebe političnega in vojaškega vodstva v procesu sprejemanja odločitve. Interesna območja zbiranja obveščevalnih podatkov so predvsem krizna območja in območja mednarodnih operacij in misij po svetu. V okviru mednarodnega sodelovanja s partnerskimi državami izmenjujejo obveščevalne informacije z namenom zaščite nemških vitalnih interesov v okviru mednarodnih organizacij (White Paper 2006, 82-83).

[45] Na spletnih straneh nemškega zveznega arhiva je objavljen zgodovinski pregled formiranja in preoblikovanja teh služb/uradov. Oktobra 1978 naj bi minister za obrambo oblikoval delovno skupino za formiranje obveščevalnega urada zveznih oboroženih sil pri uradu za nadzor radijskih komunikacij. Skupina je operativno začela delovati 1. 10. 1979, svoj sedež in novo zgrajeni podzemni objekt je pa dobila v Gelsdorfu. Urad se je leta 2002 preimenoval v Center za obveščevalne zadeve zveznih oboroženih sil (Zentrum für Nachrichtenwesen der Bundeswehr - ZNBw). Formiranje naj bi bilo zaključeno leta 2003.

[46] White Paper 2006 on German Security Policy and the Future of the Bundeswehr.

V Beli knjigi je vojaška obveščevalna organizacija skupaj s strateškim izvidovanjem (strategic reconnaisance), geoinformacijskimi in psihološkimi operacijami, umeščena pod združeno podporno dejavnost Nemške zvezne vojske (Joint Support Service) (White Paper 2006, 98), ki je, poleg letalstva, mornarice, kopenskih sil in zdravstvene dejavnosti, ena izmed petih zvrsti nemške vojske.

Poveljevanje s stacionarnimi in mobilnimi SIGINT zmogljivostmi, z zmogljivostmi elektronskega bojevanja in s satelitskimi obveščevalnimi zmogljivostmi[47] je v pristojnosti Strateškega izvidniškega poveljstva (Strategic Reconnaisance Command) (White Paper 2006, 99).

5.2.2 Politični ali parlamentarni nadzor v Nemčiji

V Nemčiji nadzirajo delo obveščevalnih služb poleg posebnih parlamentarnih tudi drugi subjekti v vseh vejah oblasti. Tako kot v slovenskem, ima tudi v nemškem pravnem sistemu parlament na voljo različna sredstva za pridobivanje informacij za nadziranje politik in vladajoče administracije, zaščito posameznika ali odkrivanje zlorab in krivic.

Z vidika preučevane tematike političnega ali parlamentarnega nadzora nad obveščevalnimi službami in natančneje nad obveščevalno zvrstjo SIGINT, se bom omejila na dve parlamentarni telesi, ki sta zadolženi in usposobljeni za tovrstni nadzor v Nemčiji, v okviru varstva človekovih pravic pa še institut parlamentarnega pooblaščenca za oborožene sile oziroma varuha človekovih pravic na obrambnem področju.

Ob ponovni vzpostavitvi oboroženih sil v 50. letih prejšnjega stoletja je Nemčija parlamentarnemu nadzoru posvetila posebno pozornost (Rieger 1986). Da bi zagotovila veljavnost ustavnih vrednot, ki v ospredje postavljajo posameznika tudi v oboroženih silah, je to zapisala v nemški ustavi (člen 45.b).

Parlamentarni pooblaščenec je pomožno telo zveznega parlamenta (Bundestag) in del zakonodajne oblasti. Preiskave opravlja po navodilu zveznega parlamenta, njegovega odbora za obrambo ali na lastno pobudo v primerih, ki so pritegnili njegovo pozornost. Skladno z

[47] Nemci so svoj prvi izvidniški satelit SAR-Lupe izstrelili iz ruskega izstrelišča Plesetsk, 19. decembra 2006. Gre za IMINT satelit. V okviru tega projekta je Nemčija vzpostavila sodelovanje še z drugimi državami Evropske unije, predvsem z Italijo in Francijo, ki imata prav tako svoje lastne satelitske izvidniške sisteme (www.c4isrjournal.com).

načelom delitve oblasti pooblaščenec izvaja nadzor nad ministrstvom za obrambo. Kadarkoli lahko obišče katerokoli enoto, štab, agencijo ali organ oboroženih sil in njegove institucije tudi brez opozorila. Pooblaščenec lahko uvede preiskavo, zlasti kadar prejme pritožbo pripadnikov služb katerekoli ravni ali položaja (Born 2003, 92).

Za področje nadzora nad pošto in telekomunikacijami sta po Zakonu G-10 (Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses) pristojni dve parlamentarni telesi in sicer:

- parlamentarni odbor G-10 (Gremium) in

- parlamentarna komisija G-10 (Kommission).

Za nadzor nad posegi v zasebnost posameznika s spremljanjem pisemskih in poštnih pošiljk ter elektronskih komunikacij je pristojen posebni parlamentarni odbor G–10, ki daje tudi soglasje k določitvi zvez, ki bodo predmet nadzora, in parlamentarna komisija G–10. Obe telesi sta namreč edina parlamentarna proaktivna organa, ki izvajata nadzor nad delom nemških obveščevalnih služb.

Odbor G–10 je poslanska skupina petih poslancev, ki se sestaja vsake pol leta zaradi pregleda oziroma preučitve splošnih predpisov, ki urejajo nadzor pošte, telefonov, faksov in drugih komunikacijskih sredstev in ugotavljanja ali so ti predpisi primerni in ustrezajo dejanskemu stanju.

Komisija G–10, ki jo sestavljajo predsednik, dva člana in trije namestniki, mesečno obravnava individualne primere obveščevalnih in varnostnih služb z vidika spoštovanja zakonitosti. Vsi člani komisije morajo predhodno izpolnjevati pogoje za sodnika. Člani te komisije ne opravljajo funkcije poslanca, temveč so zgolj predstavniki posameznih političnih strank v aktivni sodno-nadzorni funkciji, zaradi česar se ti predstavniki pravno in strokovno zelo poglabljajo v to specifično področje. Glavna naloga komisije G-10 je odločanje o upravičenosti in potrebnosti nadzora nad pisemsko-poštnimi in telekomunikacijskimi sredstvi. Bistveno pri tem je, da obveščevalno varnostne službe lahko nadzor začnejo šele, ko tak ukrep odobri pristojna komisija. Komisija G-10 obravnava tudi pritožbe državljanov nad poseganjem v temeljne pravice komunikacijske zasebnosti obveščevalnih in varnostnih služb.

5.2.3 Varstvo človekovih pravic in temeljnih svoboščin ter varstvo komunikacijske zasebnosti

Ustava Zvezne Republike Nemčije[48] (Grundgesetz für die Bundesrepublik Deutschland GG) določa temeljne pravice v svojem 1. poglavju, v drugem poglavju pa ustava navaja, da je človekove pravice in temeljne svoboščine mogoče omejevati le z zakonom. Zakoni določajo pogoje in način omejevanja pravic. 10. poglavje ustave določa pravico do zasebnosti komuniciranja, s katerim ustava določa, da je zaupnost pisem, pošte in telekomunikacij nedotakljiva. Iz določenih razlogov z vidika nacionalne varnosti pa se te pravice lahko omejijo ali se vanje poseže, vendar le z zakonom (www.bundestag.de).

Zvezna Republika Nemčija ima zato, z vidika poseganja v ustavno pravico do zasebnosti komuniciranja, ki je opredeljena v 10. poglavju ustave, poseben Zakon G-10 (Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses), oziroma zakon za omejevanje pisemske, poštne in telekomunikacijske zasebnosti, ki je bil leta 2001 spremenjen z Zakonom o spremembah omejevanja tajnosti pisemsko-poštnih in komunikacijskih sporočil[49].

V Zvezni Republiki Nemčiji je urejanje posegov v (tele)komunikacijsko zasebnost v primeru mednarodnih sistemov zvez ali obveščevalne zvrsti SIGINT določeno z zakonom, v skladu s katerim lahko v določenih primerih posege v komunikacijsko zasebnost izvajajo civilne in vojaške obveščevalne službe. Tako lahko Zvezna obveščevalna služba (BND) v okviru svoje splošne pristojnosti, ki izhaja iz Zakona o Zvezni obveščevalni službi[50], zbira informacije s prestrezanjem mednarodnih sistemov zvez. Takšno obliko dela predstavlja naključno spremljanje zvez z namenom zbiranja informacij o morebitnih grožnjah za državno varnost. Pri tem mora biti izpolnjen pogoj, da ne gre za določljiv priključek telekomunikacijskega sredstva ali določenega uporabnika tega priključka na območju države. Dovoljenje za poseg izda pristojni minister, vsebovati pa mora nabor iskalnih pojmov in določitev področja. Izda se za obdobje treh mesecev z možnostjo podaljšanja, pridobljeni podatki pa se lahko uporabijo le za namen, zaradi katerega je bil poseg dovoljen.

[48] Ustava Zvezne Republike Nemčije je bila sprejeta 23. maja 1949. Njena zadnja zadnja sprememba je iz 29. julija 2009. Že v ustavi iz leta 1949 je bilo zapisano, da mora biti Nemčija sodobna parlamentarna, demokratična republika, zvezna, socialna in pravna država (20. člen ustave).
[49] Gesetz zur Neuregelung von Beschränkungen des Brief-Post und Fernmeldgeheimnisses.
[50] Gesetz über den Bundesnachrichtdienst.

Poleg strateškega nadzora lahko Zvezna obveščevalna služba poseže v mednarodne komunikacije tudi v primerih preprečevanja nevarnosti za osebo, ki je v tujini in je to v posebnem interesu države, podatkov pa ni mogoče pridobiti na drug način. V teh primerih se dovoljenje za poseg izda za veljavnost dveh mesecev z možnostjo podaljšanja v dvomesečnih intervalih.

Tudi Nemčija kot gonilna sila Evropske unije pri vprašanju zagotavljanja in poseganja na področje človekovih pravic in temeljnih svoboščin upošteva Evropsko konvencijo o varstvu človekovih pravic in temeljnih svoboščin.

5.3 REPUBLIKA MADŽARSKA

5.3.1 Pravni okvir obveščevalnih struktur na Madžarskem

Ko je Madžarska s tranzicijo prešla v demokracijo, je morala v celoti prenoviti svoj politični, ekonomski in obrambni sistem. Znotraj obrambnega sektorja je bila skladno s ciljem, ki si ga je zadala, primorana reformirati tudi obveščevalni sistem, tako da bo le-ta najbolje služil njenim ciljem in potrebam (Babos 2003).

Obveščevalna skupnost Republike Madžarske je bila v zdajšnji obliki ustanovljena in pravno regulirana z Zakonom o nacionalnih varnostnih službah iz leta 1995 (Zakon št. CXXV). Službe so po tem zakonu zadolžene za varovanje nacionalne varnosti z uporabo odkritega in prikritega pridobivanja informacij. Zakon za nacionalno varnost opredeljuje kot obrambo suverenosti države in zavarovanje njene ustavne ureditve (Črnčec 2009, 180).

Zakon o nacionalnih varnostnih službah v prvem členu določa dejavnost petih obveščevalnih služb, treh civilnih in dveh vojaških. Leta 2007 je madžarska sestavila posebno komisijo za preučitev možnosti preoblikovanja madžarske obveščevalne skupnosti, ki je vključevala več predlogov združevanja služb na različnih ravneh, vendar je vlada v končni fazi odločila, da sistema ne bo spreminjala.

Madžarsko obveščevalno skupnost sestavljajo naslednje službe (Črnčec 2009, 181):

- Nacionalni varnostni urad (notranja civilna služba),

- Nacionalna posebna varnostna služba (notranja civilna služba),
- Obveščevalni urad (civilna zunanja obveščevalna služba),
- Vojaški varnostni urad (notranja vojaška služba) in
- Vojaški obveščevalni urad (zunanja vojaška obveščevalna služba).

Obveščevalne in varnostne službe na Madžarskem so po upravni liniji podrejene vladi, medtem ko njihovo usmerjanje v praksi neposredno izvajata dva ministra. Vse tri civilne službe so podrejene ministru, odgovornem za usmerjanje nacionalnih in varnostnih služb, obe vojaški službi pa sta odgovorni ministru za obrambo, medtem ko Nacionalna posebna varnostna služba podpira in zagotavlja opremo in sredstva za tajno pridobivanje podatkov za preostale štiri službe, se tudi sicer njihove naloge medsebojno prepletajo in dopolnjujejo, kar seveda natančno opredeljuje zakonodaja. Minister za pravosodje pa odloča o uporabi posebnih operativnih metod in sredstev za vse obveščevalne in varnostne službe.

Z vidika izvajanja obveščevalne zvrsti SIGINT ima ključno vlogo Vojaški obveščevalni urad (a Katonai Felderítő Hivatal), ki je zadolžen za izvajanje vojaške obveščevalne dejavnosti. Pristojnosti in naloge urada so opredeljene v 6. členu Zakona o nacionalnih varnostnih službah (Zakon št. CXXV)[51]. Naloge Vojaškega obveščevalnega urada so zbiranje obveščevalnih podatkov in informacij, ki so pomembni za obrambne in nacionalno varnostne interese države, kar pomeni zbiranje obveščevalnih informacij o vojaško-političnih, vojaško-industrijskih zadevah in drugih z obrambnega vidika pomembnih informacij. Neposredno je odgovoren ministru za obrambo, ta pa vladi, obveščevalno pa neposredno podpira generalštab Madžarske vojske. Službo vodi direktor, ki je general Madžarske vojske. Urad je pod stalnim parlamentarnim nadzorom, in se je zadnjih letih tehnično opremil in moderniziral, tako da je urad v celoti kompatibilen z drugimi vojaškimi obveščevalnimi službami zveze NATO (www.kfh.hu). Organizacijska struktura Urada za obveščevalne zadeve obsega šest direktoratov in en oddelek[52]:

- Direktorat HUMINT,
- Direktorat SIGINT,
- Direktorat za obveščevalne analize,
- Direktorat za varnostne in administrativne zadeve,
- Direktorat za logistiko, razvoj in finance,

[51] Zakon je dostopen na spletnih straneh Katonai Felderítő Hivatal (www.kfh.hu).
[52] Organizacijska struktura urada je dostopna na spletnih straneh Katonai Felderítő Hivatal (www.kfh.hu).

- Direktorat za upravljanje s človeškimi viri in
- Oddelek za načrtovanje in politiko.

Direktorat SIGINT je tisti organski del Vojaškega obveščevalnega urada, ki zagotavlja zmogljivosti SIGINT tudi za združeno obveščevalno podporo v mednarodnih operacijah in misijah ter zagotavlja osebje za NATO SIGINT obveščevalno strukturo.

5.3.2 Politični ali parlamentarni nadzor na Madžarskem

Madžarska ima zelo strogo ureditev za vzpostavitev nadzorne funkcije nad nacionalnimi obveščevalnimi službami. Vsi nadzorniki (politični, parlamentarni, sodni in strokovni) so pred imenovanjem v nadzorno funkcijo nad obveščevalnimi službami predhodno varnostno preverjeni. Varnostno se tako preverijo ministri, sodniki, člani nacionalnega varnostnega odbora, člani parlamentarnega odbora za obrambo, strokovnjaki, ki sodelujejo s temi organi ter javni tožilci, ki sodelujejo pri posebnih ukrepih.

V Republiki Madžarski je parlament v skladu s svojimi ustavnimi in zakonskimi pooblastili pristojen za organiziranje, vodenje in usmerjanje obveščevalno varnostnih služb ter za izvajanje nadzora nad njihovim delovanjem. Neposredni politični nadzor nad delovanjem služb izvajata parlamentarni Odbor za nacionalno varnost in parlamentarni Odbor za obrambo. Nadzor nad njihovim delovanjem pa se izvaja še preko drugih mehanizmov: državnega računskega sodišča, vladnega nadzornega urada in treh ombudsmanov - za varstvo osebnih podatkov, za državljanske pravice in za nacionalno-etnične pravice.

Parlamentarni odbor za nacionalno varnost ima enajst članov, njegov predsednik je član opozicijske stranke. Pristojni minister je zavezan, da odbor redno obvešča o splošnih nalogah varnostnih služb, najmanj pa dvakrat na leto. Odbor lahko zahteva od pristojnega ministra in generalnih direktorjev služb oceno razmer na področju nacionalne varnosti v državi ter poročilo o operacijah in dejavnostih varnostnih služb. Prav tako lahko odbor zahteva podatke od ministra za pravosodje ter drugih odgovornih ministrov in generalnih direktorjev o uporabi prikritih ukrepov. Preiskuje lahko pritožbe posameznikov v zvezi z nezakonitimi dejanji varnostnih služb. Od pristojnega ministra lahko zahteva izvedbo preiskave in dostavo poročila o kršitvah pravic posameznikov (Črnčec 2009, 182).

Za člana Odbora za nacionalno varnost je lahko izbran le poslanec, ki se pred tem podvrže ustreznemu varnostnemu preverjanju in ima dostop do najvišje stopnje tajnih podatkov. Vsi člani odbora so zavezani k molčečnosti v zvezi s podatki in dokumenti, do katerih so prišli kot člani odbora. Ta njihova zaveza k molčečnosti ne preneha tudi, ko niso več člani tega odbora. Parlamentarni nadzor nad delom Vojaškega obveščevalnega urada in Vojaškega varnostnega urada izvaja parlamentarni Odbor za obrambo. Za člane tega odbora veljajo enaka pravila glede preverjenosti za dostop do tajnih podatkov kot tudi njihova zavezanost k molčečnosti.

5.3.3 Varstvo človekovih pravic in temeljnih svoboščin ter varstvo komunikacijske zasebnosti

Temeljne človekove pravice in dolžnosti madžarskih državljanov so opredeljene v 12. poglavju Ustave Republike Madžarske (Listina št. XX/1949, A Magyar Köztársaság Alkotmánya)[53]. Ustava tako v 55. členu določa, da se posegi v temeljne pravice opredelijo z zakonom in ob zakonsko izpolnjenimi določenimi pogoji. Pravica do komunikacijske zasebnosti v ustavi ni eksplicitno določena, je pa posredno opredeljena v 59. členu ustave. V 2. poglavju, 19. člena opredeljuje tudi pristojnosti madžarskega parlamenta, v 35. členu pa vlogo vlade v sistemu nacionalne varnosti.

Postopki poseganja v komunikacijsko zasebnost in njihovo avtorizacijo na Madžarskem so opredeljeni v Zakonu št. CXXV in v vladni uredbi o sodelovanju telekomunikacijskih organizacij z obveščevalno strukturo za potrebe zbiranja tajnih informacij in podatkov. Vladna uredba je dokument, ki natančneje opredeljuje odnos za izvajanje posegov v komunikacijsko zasebnost med telekomunikacijskimi organizacijami in civilnimi obveščevalnimi in varnostnimi službami.

Skladno z navedenimi akti so za posege v komunikacijsko zasebnost opredeljeni postopki za avtorizacijo, za katero so določeni po Zakonu št. CXXV pristojni sodniki. Avtorizacijski postopki za odobritev posebnih ukrepov za poseganje v komunikacijsko zasebnost so zelo natančno opredeljeni v členih 54 do 60 tega zakona. Po 58. členu o upravičenosti posameznega posebnega ukrepa odloča sodnik ali pa minister za pravosodje, za kar imata 72

[53] Ustavo je Madžarska dobila 20. avgusta 1949 in jo je zadnjič spremenila leta 1989. Ustavo sestavlja 15 poglavij in 79 členov.

ur časa, ukrep pa sam po sebi ne sme trajati več kot 90 dni. V posebnih primerih je tak ukrep moče še podaljšati vendar največ za 90 dni. Prvi pogoj, ki mora biti izpolnjen za postopek avtorizacije, je po 53. členu, da so posebni ukrepi edini možni ukrepi za pridobitev določenih obveščevalnih podatkov s strani obveščevalnih in varnostnih služb.

Madžarska pa se je tudi kot država članica Evropske unije pri vprašanju zagotavljanja in poseganja na področje človekovih pravic in temeljnih svoboščin obvezala k spoštovanju in upoštevanju Evropske konvencije o varstvu človekovih pravic in temeljnih svoboščin.

5.4 NATO

Vse tri države, predstavljene v prejšnjem poglavju, so članice NATA, ki so v sodobnem globalnem varnostnem okolju, predvsem pa v okviru delovanja v mednarodnih operacijah in misijah, primorane k vzpostavitvi intenzivnega in učinkovitega sodelovanja tudi na obveščevalnem področju. NATO pred vse države članice postavlja enake okvire in standarde, ki zaradi same narave te obrambne organizacije zahtevajo proaktivno izvajanje same obveščevalne politike. Vse to vodi v nekakšno globalno obveščevalno dejavnost znotraj te organizacije, seveda pa obstajajo med državami članicami tudi velika odstopanja. Nekatere države se bolj nagibajo k bilateralnim obveščevalnim povezavam, druge k izbranim multilateralnim, zato si NATO že nekaj časa prizadeva, da bi vzpostavil bolj proaktivne in za članice dovolj zanesljive (zaupljive) mehanizme. O tej tematiki, o ureditvi in perspektivah obveščevalne zvrsti SIGINT v okviru NATA sem se pogovarjala v strukturiranem intervjuju, ki sem ga 23. 3. 2010 izvedla z visoko predstavnico za obveščevalno dejavnost v Mednarodnem vojaškem štabu NATA, Karen Laino.

Kot za vse države članice NATA veljajo tudi za Slovenijo enotna terminologija, delitev in drugi poenoteni operativni, varnostni in tehnični standardi za obveščevalno zvrst SIGINT, ki jih je NATO zapisal v okviru svoje splošne politike SIGINT. Moja sogovornica iz NATA je v intervjuju poudarila, da obveščevalna zvrst SIGINT predstavlja za vsako obveščevalno skupnost nenadomestljiv »trigger« ali prožilec za aktiviranje ostalih obveščevalnih disciplin.

Terminološko in konceptualno razdeli NATO obveščevalno zvrst SIGINT na samo dve obveščevalni podzvrsti[54], in sicer:

- COMINT (angl. communications intelligence) bi lahko v slovenščini poimenovali kot spremljanje elektronskih komunikacijskih omrežij. Pomeni pa indikacijo, zajem, spremljanje, identifikacijo in obdelavo komunikacijskih in informacijskih signalov (radijskih, radiorelejnih, satelitskih idr.) za pridobitev informacij iz vsebine signalov. To področje se ukvarja predvsem z govornimi in podatkovnimi komunikacijami. Uporabne informacije se običajno pridobivajo skozi daljše časovno obdobje, saj se posamezni pridobljeni podatki sestavijo v celoten mozaik verodostojne informacije šele v daljšem časovnem obdobju. Spremljanje elektronskih komunikacijskih omrežij ali COMINT je eno izmed nacionalno (in NATO) najobčutljivejših obveščevalnih podzvrsti, z zelo specifičnimi in zahtevnimi varnostnimi normami.
- ELINT (angl. electronic intelligence) bi v slovenščini poimenovali kot spremljanje elektronskih nekomunikacijskih omrežij in pomeni zajemanje, spremljanje in obdelavo radarskih, radionavigacijskih, optoelektronskih in drugih nekomunikacijskih signalov, s ciljem analize in ugotavljanja tehničnih lastnosti sistemov, ki niso namenjeni za komunikacijo (nekomunikacijski sistemi). Pridobljene informacije se uporabljajo za načrtovanje raznih operacij (vojaških, specialnih, idr.) na nasprotnikove sisteme.

Tako delitev je z vstopom v NATO sprejela leta 2004 tudi Slovenska vojska.

Glede samih operativnih zmogljivosti SIGINT, pa je treba poudariti, da zveza NATO nima svojih lastnih zmogljivosti SIGINT, zato se v celoti opira na zmogljivosti držav članic in njihovo neposredno podporo. Pa vendar je realnost takšna, da države z vidika SIGINT podpore zelo samovoljno obravnavajo prevzete obveznosti v okviru zavezništva, saj zmogljivosti SIGINT ostajajo nepreklicno v nacionalni pristojnosti. Seveda je pri tistih državah, ki prispevajo svoje vojaške sile v mednarodnih operacijah in misijah, slika drugačna, ker so le-te zainteresirane za čim boljšo obveščevalno in varnostno podporo svojih enot, za katero pa same ne morejo poskrbeti. Ta soodvisnost jih neposredno sili k sodelovanju in izmenjavi podatkov in Karen Laino meni, da se pojavlja nova perspektiva v okviru obveščevalnega sodelovanja t. i. *odgovornost za delitev z drugimi (angl. responsible to*

[54] O sami delitvi obveščevalne zvrsti SIGINT v okviru NATA sem se pogovarjala v intervjuju 23. marca 2010 s Karen Laino, pomočnico direktorja IMS NATO, ki pravi tudi, da je predvsem COMINT tista podzvrst, do katere so v NATU zelo senzibilni. Zaradi občutljive narave te podzvrsti je NATO postavil veliko najstrožjih varnostnih elementov.

share), ki presega do sedaj uveljavljeno načelo *potrebe po delitvi z drugimi (angl. need to share)*. Posledično te države bolj ali manj podpirajo neko zavezništvo. Če pa države nimajo interesa deliti svojih obveščevalnih podatkov z zavezništvom, jih tudi ne bodo, ne glede na obveze, ki so jih prevzele s članstvom, saj le-to nad nacionalnimi zmogljivostmi nima nobenih pristojnosti. In zakaj NATO do sedaj nikoli ni oblikoval lastnih zmogljivosti SIGINT? Ideje o tem so se že pojavljale v preteklosti, vendar pa se takoj postavi veliko vprašanj in neznank, na katera do zdaj niso uspeli odgovoriti: vprašanje »lastništva« teh zmogljivosti, iz katerega izhajajo normativne omejitve, legalnost uporabe teh zmogljivosti, »lastništvo« pridobljenih obveščevalnih podatkov, v končni fazi pa tudi viri (kadrovski, finančni, tehnični...).

Dejstvo je, da je na tej ravni danes uspešnejša paradigma partnerskega sodelovanja, v katero pa poleg držav članic in drugih subjektov NATA vstopajo tudi nečlanice NATA in drugi pravni subjekti (ne-NATO entitete), ki delujejo na nekem skupnem območju operacije. Partnersko sodelovanje, ki temelji na načelu *odgovornosti za delitev z drugimi (angl. responsible to share)*, je veliko učinkovitejše, saj so odnosi, lastništvo in ravnanje veliko enostavnejši in jasnejši, učinki pa transparentni, kar je ključnega pomena pri dejavnosti, ki je z vidika vsake nacionalne varnostne politike tako zelo občutljivo področje. Karen Laino poudarja, da je za učinkovito sodelovanje med obveščevalnimi strukturami ključno medsebojno zaupanje, »če zgradiš zaupanje, dobiš več sodelovanja,« je dejala[55].

NATO se t. i. problema samovoljnosti držav z vidika nacionalnega obveščevalnega prispevka na način »a la carte« resno zaveda. Odgovor poskuša najti v novih oblikah in učinkovitejših načinih sodelovanja in izmenjave informacij na ravni 27 oziroma 28 držav članic kakor tudi držav nečlanic NATA in drugih entitet, ki so prisotne v operacijah NATA. Po besedah Karen Laino je zato NATO že vzpostavil nekatere prožnejše mehanizme za sodelovanje vseh entitet in držav, ki sodelujejo na nekem območju operacije. Seveda se ti mehanizmi zelo podrejajo strogim varnostnim standardom, ki veljajo v NATU, še posebej na področju obveščevalne discipline SIGINT, natančneje COMINT. Zanimivo je, da na novo vzpostavljeni mehanizmi v praksi NATA resnično temeljijo na zaupanju, ki je seveda tudi administrativno formalizirano!

[55] Te besede je Karen Laino izrekla v svojem nastopu 22. marca 2010 v Mariboru, na konferenci *Izzivi zoperstavljanja terorizmu v regiji jugovzhodne Evrope.*

NATO dosledno ločuje področje elektronskega bojevanja od področja obveščevalne zvrsti SIGINT, čeprav se za izvajanje obeh dejavnosti v marsikateri državi uporabljajo enaki tehnični, operativni in kadrovski viri. Res pa je, da obe področji umešča na strateško raven, odgovornosti zanju pa je dodelil dvema ločenima svetovalnima odboroma: svetovalnemu odboru za SIGINT in svetovalnemu odboru za elektronsko bojevanje. V obeh odborih, ki sta v NATOVI organizacijski strukturi neposredno podrejena najvišjemu vojaškemu telesu NATA (vojaškemu odboru), Slovenija danes aktivno sodeluje s svojimi nacionalnimi predstavniki, ki izhajajo iz obrambnega in vojaškega resorja.

Kljub temu da se področji na eni strani strogo ločujeta, se jima pa priznava skupni imenovalec v nekaterih specifičnih pogojih in pogosto se zgodi, da odbora dorečeta nekatere strokovne zadeve za skupno mizo v okviru skupnih zasedanj, razprav in vaj. Enako se pričakuje tudi od držav članic, da strokovno simbiozo obeh področij prenesejo v nacionalno okolje in da vzpostavijo sodelovanje nosilcev posameznih področij in njihovo medsebojno usklajevanje na vseh ravneh. Vsekakor je pa osnovni pogoj za vzpostavitev takšne simbioze dobro poznavanje obeh področij, njunih stičnih točk in razhajanj ter natančna pooblastila glede upravljanja teh zmogljivosti.

Z vstopom Slovenije v NATO leta 2004 so se nam vrata na področju obveščevalne zvrsti SIGINT in elektronskega bojevanja odprla tudi zunaj meja. V okviru NATA je Slovenija po besedah Karen Laino izgradila uspešne partnerske odnose v okviru sodelovanja in povezovanja njegovih obveščevalnih disciplin.

Slovenija oziroma Slovenska vojska je na območje operacij kriznega odzivanja[56] poslala prvo skupino za elektronsko izvidovanje leta 2007, kar je za celotno vojaško obveščevalno dejavnost pomenilo velik korak naprej[57]. Danes bi rekli, da se je model delovanja skupine za elektronsko izvidovanje v mednarodnem okolju že uspešno potrdil in uveljavil. Kakšna je bila pot do njene tranzicije in kakšne prihodnje izzive prinaša večdimenzionalno varnostno okolje na področje obveščevalne dejavnosti, pa bom predstavila v naslednjem poglavju, kjer se bom

[56] V tem kontekstu namenoma uporabljam ožji pojem »operacije kriznega odzivanja« (krajše OKO) od uveljavljenega širšega – »mednarodne operacije in misije« ali MOM.

[57] Enota za elektronsko bojevanje prispeva svoje specialiste v NATO poveljstva v OKO sicer že od leta 2004, vendar je s svojimi operativnimi zmogljivostmi (kadrovskimi, tehničnimi, analitičnimi, varnostnimi, protiobveščevalnimi, idr.) prisotna od spomladi 2007. Slovenija je predvsem zaradi osebne angažiranosti svojih nacionalnih predstavnikov v NATO SIGINT telesih, kot prva nova članica zveze NATO izpolnila vse zahtevane kriterije – predvsem varnostne in strokovne.

poglobila v urejenost, organiziranost in perspektive obveščevalne zvrsti SIGINT na obrambnem področju z oblikovanjem možnih sistemskih scenarijev.

6 OBVEŠČEVALNA ZVRST SIGINT NA OBRAMBNEM PODROČJU V REPUBLIKI SLOVENIJI

6.1 Normativna ureditev obveščevalne zvrsti SIGINT

Pravni okvir izvajanja obveščevalne dejavnosti in obveščevalne zvrsti SIGINT na obrambnem področju, v osnovi določa Zakon o obrambi, ta pa se neposredno naslanja tudi na Zakon o Slovenski obveščevalno-varnostni agenciji.

Podrobnejša razčlemba zakonskih določil iz obeh zakonov, ki se nanašajo na izvajanje obveščevalne dejavnosti in obveščevalne zvrsti SIGINT, je v prejšnjem poglavju, zato se bom tukaj osredotočila samo na tiste pravne podlage, ki predstavljajo neposredni okvir za oblikovanje, uporabo in delovanje zmogljivosti SIGINT na obrambnem oziroma vojaškem področju.

Pravno podlago za izvajanje obveščevalne zvrsti SIGINT na obrambnem področju tako opredeljuje Zakon o obrambi (ZOBr, 32. člen, 4. odstavek), in sicer:
»Elektronsko spremljanje mednarodnih sistemov zvez, pomembnih za obrambne interese države, opravljajo za obveščevalno varnostno službo ministrstva in druge potrebe enote za elektronsko bojevanje Slovenske vojske.«

Analiza tega odstavka je že v prejšnjem poglavju pokazala preširoko in premalo določno pravno formulacijo, ki lahko ob nepravilni interpretaciji vodi v stigmatizacijo obveščevalne zvrsti SIGINT na obrambnem in vojaškem področju. Zaskrbljujoče je namreč prepletanje zakonskih določil, ki se nanašajo na sklicevanje posameznih zakonskih pooblastil in pristojnosti obveščevalnih subjektov med ZOBr in ZSOVA, kar vodi v izrazito netransparentnost in dopušča različne strokovne in pravne interpretacije. Zato bi bilo treba na tem področju sprejeti ustrezen podzakonski akt (pravilnik), ki bi med drugim zapolnil pravno vrzel, ki je nastala med tem določilom ZOBr in akti poveljevanja in kontrole v Slovenski vojski, s katerimi se zaenkrat v Slovenski vojski podrobneje definirajo postopki in načini za uporabo in delovanje njihovih zmogljivosti SIGINT, t. j. zmogljivosti Enote za elektronsko bojevanje Slovenske vojske.

6.2 Nadzor nad zakonitostjo izvajanja obveščevalne zvrsti SIGINT

S parlamentarnim nadzorom nad obveščevalno zvrstjo SIGINT se je Slovenska vojska soočila šele po letu 2002, ko je zaradi spremenjene zakonodaje na obrambnem področju Komisija Državnega zbora Republike Slovenije za nadzor nad delom varnostnih in obveščevalnih služb dala svoje uradno mnenje marca 2002[58]. Obveščevalna zvrst SIGINT v obrambno-vojaškem resorju je od takrat dalje pod permanentnim parlamentarnim nadzorom. Skladno s 17. členom ZPNOVS mora tudi Obveščevalno varnostna služba vsake štiri mesece, po potrebi pa tudi zunaj tega roka, komisiji poročati o izvrševanju svojih splošnih dejavnosti, tudi glede aktivnosti na področju obveščevalne zvrsti SIGINT.

Pa vendar se na tem mestu odpira vprašanje parlamentarnega nadzora nad drugimi subjekti vojaške obveščevalne dejavnosti v okviru Slovenske vojske, ki se razen obveščevalne zvrsti SIGINT v praksi ne izvaja. Tukaj mislim predvsem na druge obveščevalne zvrsti in subjekte, ki jih Slovenska vojska ima, ni pa v javnosti zaslediti izvajanja nobenih proaktivnih parlamentarnih nadzornih mehanizmov, ki bi bdeli nad njihovim delovanjem, čeprav formalnopravno za to obstajajo vsi pogoji. Vojaška obveščevalna dejavnost se po Vojaški doktrini izvaja na vseh treh ravneh poveljevanja, kjer so formirani obveščevalni organi, na taktični ravni pa deluje Obveščevalno izvidniški bataljon, ki razen parlamentarnega nadzora nad izvajanjem obveščevalne zvrsti SIGINT, ni bil deležen tovrstnega nadzora nad izvajanjem drugih obveščevalnih zvrsti. Seveda pa je potrebno poudariti, da obstajajo formalnopravno vsi pogoji za nadzor nad obveščevalno dejavnostjo in zvrstjo SIGINT v obrambno-vojaškem resorju. Nadzor v splošnem poteka na več ravneh, in sicer na institucionalni ravni in na neinstitucionalni ravni. V praksi to pomeni, da se na institucionalni ravni izvaja:

- politični oziroma parlamentarni nadzor, in sicer preko komisije za nadzor nad obveščevalnimi in varnostnimi službami ter preko odbora za obrambo;
- strokovni nadzor ali bolje rečeno resorni nadzor, ki pomeni nadzor različnih komisij znotraj Ministrstva za obrambo, Slovenske vojske in Inšpektorata RS za obrambo, ki za to nalogo pridobijo predhodno poseben mandat;
- sodni nadzor in
- nadzor s strani neodvisnih institucij (varuhinja človekovih pravic, informacijska pooblaščenka idr.).

[58] Mnenje Komisije Državnega zbora Republike Slovenije za nadzor nad delom varnostnih in obveščevalnih služb in Zakon o parlamentarnem nadzoru obveščevalnih in varnostnih služb.

Na neinstitucionalni ravni pa se nadzor izvaja kot posredni nadzor javnosti (npr. z uporabo instrumenta dostopa do informacij javnega značaja in medijev).

6.3 Obveščevalna zvrst SIGINT v Ministrstvu za obrambo

Za obveščevalno zvrst SIGINT na obrambnem področju je leto 2000 tisti časovni mejnik, ki pomeni veliko spremembo v umestitvi teh zmogljivosti. Do tega leta so bile namreč zmogljivosti SIGINT, oziroma takrat t. i. zmogljivosti elektronskega izvidovanja[59], izključno v sestavi Obveščevalno-varnostne službe Ministrstva za obrambo. Organizirane so bile kot samostojna izpostava službe. Slovenska vojska do tega leta teh zmogljivosti ni imela, niti ni razpolagala z njihovimi zmogljivostmi. Sami začetki zmogljivosti SIGINT na obrambno-vojaškem področju pri nas pa segajo že v leto 1991, v čas osamosvajanja Republike Slovenije. Kako se je to področje razvijalo v preteklem obdobju in kam vodijo njegove poti v prihodnje, sem poskušala skozi svoje preučevanje podpreti tudi s strukturiranimi intervjuji z osebami, ki so bile ali pa so še vedno aktualni odločevalci za to področje v okviru obrambnega oziroma vojaškega resorja. Da bi lahko razumeli prihodnost, moramo poznati preteklost, zato sem, o razvoju področja skozi preteklo obdobje govorila z bivšim dolgoletnim načelnikom prvih zmogljivosti SIGINT na obrambnem področju[60]. O prihodnji vlogi zmogljivosti SIGINT za potrebe Slovenske vojske ter o njihovih stičnih točkah z Obveščevalno-varnostno službo sem se v intervjuju pogovarjala z aktualnim poveljnikom sil Slovenske vojske in generalnim direktorjem Obveščevalno-varnostne službe Ministrstva za obrambo.

[59] Elektronsko izvidovanje je, kot že rečeno, terminologija, ki se je v splošni dolgoletni strokovni uporabi in v vojaški praksi uveljavila in je bila edina terminologija do vstopa Slovenije v NATO.

[60] O začetkih zmogljivosti SIGINT na obrambnem in vojaškem področju (obdobje 1991-2000) je v okviru strukturiranega intervjuja zelo izčrpno spregovoril prvi in dolgoletni načelnik teh zmogljivosti na obrambnem področju, podpolkovnik Ciril Belšak. Intervju je bil izveden 19. marca 2010. Večina navedb je v tem podpoglavju vzetih neposredno iz intervjuja, nekaj je pa smiselno umeščenih v samo vsebino naloge.

6.3.1 Obveščevalna zvrst SIGINT 1991-2000

V obdobju osamosvajanja Slovenije Teritorialna obramba Republike Slovenije v svoji sestavi ni imela enote za elektronsko izvidovanje niti ni razpolagala s tehničnimi sredstvi in z ustrezno usposobljenimi pripadniki. Zaradi potreb po poznavanju namer nasprotnika in njegovih načrtovanih potezah sta bili že v samem času izvajanja bojnih dejstev formirani skupini za elektronsko izvidovanje, ki sta izvajali elektronsko izvidovanje iz neposredne bližine centrov odločanja o uporabi enot Jugoslovanske ljudske armade, razmeščenih na ozemlju Republike Slovenije. Prva skupina za elektronsko izvidovanje je delovala na severo-vzhodnem delu Slovenije, druga pa v njenem centralnem delu. Izvajali sta elektronsko izvidovanje radijskih zvez Jugoslovanske ljudske armade ter nekatere ukrepe elektronskega zavajanja in elektronskega motenja. Nadzorovali sta večino radijskega in telefonskega prometa, ki je potekal med korpusnimi poveljstvi Jugoslovanske ljudske armade v Mariboru in Ljubljani in nadrejenim poveljstvom v Zagrebu, pa tudi radijske in telefonske komunikacije več deset obmejnih stražnic. Skupini sta bili podrejeni Varnostnemu organu Ministrstva za obrambo (VOMO), pridobljene podatke pa sta posredovali tako VOMO kakor tudi poveljnikom pokrajinskih poveljstev Teritorialne obrambe, pri katerih sta delovali (7. PŠTO in 5. PŠTO) . Prvo poročilo, pridobljeno s pomočjo elektronskega izvidovanja, je bilo posredovano že 3. julija 1991[61].

Izredno uspešno izvajanje operacij elektronskega izvidovanja je pomenilo eno največjih strateških in tehnično-organizacijskih presenečenj za napadalca. Po koncu vojne 1991 sta bili skupini združeni v četo za elektronsko izvidovanje, ki je bila formalno podrejena Republiškemu odredu za zveze, vendar je enota delovala izključno za potrebe VOMO, saj je bilo po koncu vojne spremljanje vojaško-političnih razmer predvsem na območju zahodnega Balkana strateškega pomena za državo.

Po treh letih je bila četa za elektronsko izvidovanje preoblikovana v Izpostavo za elektronsko zbiranje podatkov o tujih oboroženih silah ter prepodrejena Obveščevalno-varnostni službi, pod okriljem katere je delovala vse do njene prepodreditve v Slovensko vojsko leta 2000.

[61] 3. julij, je kot »dan elektronskega bojevanja« razglasil bivši direktor VOMO Dušan Mikuž na svečanosti leta 1994. To tradicijo je Slovenska vojska prevzela s prepodreditvijo enote v svojo strukturo leta 2000 in 3. julij ohranila kot »dan elektronskega bojevanja«.

6.3.2 Obveščevalna zvrst SIGINT v tranzicijskem obdobju 2000-2004

Od leta 2000 pa do same včlanitve Republike Slovenije v NATO leta 2004, ko so se za to področje obveščevalne dejavnosti v okviru Slovenske vojske odprle nove zahteve in na novo opredelile potrebe, govorimo o t. i. tranzicijskem obdobju, ki je imelo slabe implikacije predvsem na področju strokovnega in kadrovskega razvoja samih operativnih zmogljivosti SIGINT, Slovenska vojska pa je znotraj sistema iskala njihovo najprimernejšo umestitev.

Odločitev o prepodreditvi Izpostave za elektronsko zbiranje podatkov o tujih oboroženih silah v Slovensko vojsko so narekovale potrebe v procesu vključevanja Slovenije v NATO in nujno preoblikovanje celotnega obrambnega sistema. Leta 2000 je Vlada Republike Slovenije sprejela akt *Obseg in struktura Slovenske vojske 2010*[62], s katerim je opredelila, da bodo v sestavi Slovenske vojske organizirane enote za elektronsko bojevanje, ki bodo izvajale vse aktivnosti elektronskega bojevanja. Ker tovrstnih zmogljivosti Slovenska vojska takrat ni imela, niti virov, da jih na novo oblikuje, je bila sprejeta rešitev prepodreditve obstoječih zmogljivosti iz Obveščevalno-varnostne službe pod pristojnost Slovenske vojske.

Slovenska vojska je avgusta leta 2000 v svojo strukturo sprejela subjekt SIGINT (imenovan Enota za elektronsko bojevanje) na podlagi odredbe ministra za obrambo[63]. Dejstvo je, da takrat Slovenska vojska na sprejem tovrstne enote ni bila dovolj strokovno pripravljena; predhodno bi morale biti izdelane strokovne študije o nadaljnjem poslanstvu enote in razvoju teh zmogljivosti, v planskih aktih Slovenske vojske pa zagotovljeni ustrezni kadrovski in finančni viri. Prav zaradi pomanjkanja strateških usmeritvenih dokumentov je bilo v prvih letih formiranih več strokovnih delovnih skupin za področje elektronskega bojevanja in

---

[62] V poglavju Komunikacijski in informacijski sistemi ter elektronsko bojevanje je bilo zapisano, da bo:
Slovenska vojska formirala enote za elektronsko bojevanje, ki bodo:
- odkrivale elektronska sredstva nasprotnika;
- opravljale tehnične analize in dešifrirale elektronske signale nasprotnika;
- določale lokacije elektronskih sredstev nasprotnika;
- motile elektronska sredstva nasprotnika;
- izvajale vdore v informacijske sisteme nasprotnika;
- zagotavljale zaščito lastnih komunikacijskih in informacijskih sistemov;
- preverjale odpornosti lastnih komunikacijskih in informacijskih sistemov in zagotavljale pogoje za informacijsko nadvlado z vplivanjem na nasprotnikove informacije in procese in s tem na njegove informacijske sisteme.

[63] 12. julija 2000 je minister za obrambo Republike Slovenije izdal odredbo, s katero je prenesel dejavnost elektronskega zbiranja podatkov o tujih oboroženih silah izpostave OVS v pristojnost Slovenske vojske.

elektronskega izvidovanja, ki so začrtali smer nadaljnjega razvoja teh zmogljivosti v okviru Slovenske vojske. Planski in razvojni dokumenti so nastajali postopoma, od leta 2004 dalje. Obdobje okarakterizira tudi odliv strokovnega kadra. Razlogi zanj so večplastni, posledica pa je bil zastoj tehničnega razvoja v enoti, poizkusi njenega preoblikovanja v standardizirano vojaško enoto Slovenske vojske, za strokovne naloge pa je zato ostajalo vedno manj časa.

Na tem mestu pa se mi zdi prav, da opozorim na tisti vidik, ki v intervjuju ni bil neposredno omenjen, in sicer na vidik preobrazbe pripadnostne identitete kadra v tej enoti, s katero se je Slovenska vojska takrat soočila, ni pa ga v celoti dojela. Pred omenjeno prepodreditvijo te enote iz Obveščevalno-varnostne službe v Slovensko vojsko, je njen kader čutil veliko pripadnost svoji dotedanji organizaciji. Iz tega razloga je bilo zato nerazumljivo pričakovati njihovo pripadnostno transformacijo čez noč in najbrž je bil kadrovski odliv po letu 2000 prav zaradi tega tudi izrazitejši kot sicer.

Od leta 2000, ko je Slovenska vojska v svojo strukturo sprejela Enoto za elektronsko bojevanje (bivšo Izpostavo za elektronsko zbiranje podatkov iz OVS MORS), je bilo tudi kar nekaj poizkusov najustreznejše umestitve te enote znotraj vojaške strukture. Enota je bila v 10 letih kar nekaj-krat prepodrejena, od strateške do taktične ravni, kjer tudi trenutno deluje, medtem pa je njeno poslanstvo ostalo v večjem delu nespremenjeno[64]. V intervjuju je poveljnik sil Slovenske vojske[65] na vprašanje v zvezi s tem poudaril, da umestitev enote res ni bila nikoli dorečena ali dokončno določena, ker se je tudi misija enote menjala oziroma dopolnjevala. Enoto so tako uporabljali za naloge najprej na strateški, kasneje pa še na operativni in v zadnjem času taktični ravni (v operacijah kot eden glavnih virov zaščite sil). Poveljnik sil pa naprej razmišlja, da bodo te zmogljivosti po končanem doopremljanju tudi v prihodnje najverjetneje uporabljali na vseh treh ravneh zaradi racionalizacije, a hkrati ugotavlja, da bo treba njihovo sistemsko umestitev dobro pretehtati.

[64] Enota za elektronsko bojevanje trenutno deluje pod okriljem 5. obveščevalno izvidniškega bataljona Slovenske vojske (OIB). OIB je namenjen zagotavljanju vojaške obveščevalne podpore in zbiranju, analiziranju ter posredovanju vojaških obveščevalnih podatkov in informacij uporabnikom.
OIB sestavljajo Enota za elektronsko bojevanje (EEB), Enota za specialno delovanje (ESD), Enota brezpilotnih letal (EBPL), Enota za večsenzorsko izvidovanje (EVSI), Enota za pridobivanje vojaških obveščevalnih podatkov s človeškimi viri in poveljniško logistična enota, ki bo vključevala tudi skupino za psihološka delovanja ter skupino za načrtovanje in analizo podatkov (SOPr 2007-2012).
Po SOPr 2007-2012 naj bi v okviru EEB formirali analitični center elektronskega izvidovanja (EI), na njegovi osnovi pa kasneje tudi glavni center za elektronsko bojevanje (GCEB).
[65] V intervjuju z aktualnim poveljnikom sil Slovenske vojske, generalmajorjem Alanom Gederjem, pogovarjala predvsem o njegovem pogledu na sedanjo in prihodnjo vlogo zmogljivosti SIGINT Slovenske vojske.

6.3.3 Obveščevalna zvrst SIGINT v Slovenski vojski po letu 2004

Danes je Enota za elektronsko bojevanje enota bojne podpore Slovenske vojske, ki je organizirana, opremljena in usposobljena za izvajanje nalog SIGINT in se uvršča v premestljive sile[66]. Skladno s cilji sil, ki jih je Slovenska vojska sprejela, pa razvija tudi zmogljivosti elektronskega bojevanja za podporo pri zaščiti sil[67] slovenskega vojaškega kontingenta v mednarodnih operacijah in misijah.

Slovenska vojska sicer s svojimi zmogljivostmi SIGINT sodeluje v mednarodnih operacijah in misijah že od leta 2007 s skupino za elektronsko izvidovanje, kar je zahtevalo veliko združenih strokovnih naporov v celotnem obrambnem resorju, predvsem pa spremembo v miselnosti in dojemanju nove vloge in poslanstva te enote. Do takrat namreč enota ni delovala v nekem mednarodnem okolju in sama predstava o tem, da deluje zunaj ozemlja Republike Slovenije, je bila sprva nesprejemljiva. Pristop k pripravi prve misije je bil za strokovne nosilce zahteven projekt, prepričati ključne odločevalce o varnostnem pomenu za naše pripadnike, ki delujejo na območju mednarodnih operacij in misij, pa velik izziv. Ta projekt je bil uspešen, danes pa se pred stroko in odločevalce na obrambnem področju postavljajo novi izzivi.

Kot že rečeno enota izvaja dva različna sklopa nalog;

- prvi je izrazito obveščevalne narave (izvajanje nalog SIGINT za potrebe obveščevalne službe (na obrambnem področju)),
- drugi, pa je izrazito vojaška aktivnost in se nanaša na načrtovanje, organiziranje in izvajanje ukrepov elektronskega bojevanja za potrebe Slovenske vojske.

Pristojnosti odrejanja nalog prvega sklopa so eksplicitno zakonsko opredeljene, medtem ko so pristojnosti odrejanja nalog pri elektronskem bojevanju (drugi sklop) pod izključno pristojnostjo vojaškega poveljnika. Pri tem je zelo očitno, da gre za strokovno izredno zahtevno razmerje, ki zahteva fleksibilen organizacijski pristop. Kako to funkcionira v praksi hierarhične vojaške organizacije, sem v intervjuju povprašala poveljnika sil.

[66] Po aktualni vojaški doktrini so premestljive sile organizirane, opremljene in usposobljene za uresničevanje svojega poslanstva samostojno ali v sestavi sil zavezništva na nacionalnem vojskovališču ter na kriznih območjih znotraj in zunaj meja zavezništva (PDRIU 2006, 102).

[67] Po aktualni vojaški doktrini je zaščita sil definirana kot aktivnosti, ki se izvajajo za zmanjšanje ranljivosti moštva, opreme, objektov in delovanj pred vsemi grožnjami v vseh situacijah. Zaščita sil obsega aktivnosti zračne obrambe, nuklearne, radiološke, biološke in kemične obrambe, protiteroristične ukrepe, zaščito komunikacijskega in informacijskega sistema ter taktične ukrepe, kot so premik, maskiranje, utrjevanje in varovanje (PDRIU 2006, 108).

Enota zaradi svojega poslanstva in specifične narave dela ohranja svoje ključne vitalne funkcije in operativne zmogljivosti neodvisne od nadrejene matične enote; ima svojo formacijo, svoje specifično poveljstvo s ključnimi štabnimi funkcijami (kadrovska, operativna in logistična) in svoje razvojno jedro. Ima pa tudi svojega zakonitega odredbodajalca za izvajanje nalog SIGINT, ki pa ni njen poveljnik. Ne glede na to je danes enota pri izvajanju svojih nalog še vedno razpeta med dva uporabnika; med Slovensko vojsko (poveljnika) in Obveščevalno-varnostno službo. Zakoniti odredbodajalec za odrejanje nalog SIGINT ni poveljnik, temveč minister za obrambo[68]. In tu zasledimo še eno kolizije načel in predstav[69], ki so v praksi včasih zelo nerodno razumljene, sploh pa je to stanje lahko zelo neugodno za delovanje v vojaški hierarhični organizaciji.

Slovenska vojska kot sestavni del sistema nacionalne varnosti mora uveljavljati vsa pravna načela, pravil pa ne sme postavljati po svoje, zunaj zakonskih norm. Zato je zelo pomembno, da so odločevalci v Slovenski vojski o teh normah poučeni, da jih dosledno spoštujejo in da razumejo iz njih izhajajoče omejitve. Prav tako je pomembno, da razumejo vlogo, pomen in posebnosti te obveščevalne zvrsti tako na obrambno-vojaškem področju, kot tudi v širšem kontekstu nacionalne in mednarodne varnosti.

Vedno večja prisotnost vojaških zmogljivosti Republike Slovenije v mednarodnih operacijah in misijah je na eni strani zelo pomemben dejavnik naše zunanje politike, na drugi strani pa, kot v intervjuju razmišljata oba, tako poveljnik sil Slovenske vojske, kot tudi generalni direktor Obveščevalno-varnostne službe Ministrstva za obrambo, se z večanjem prisotnosti Slovenske vojske v mednarodnih operacijah in misijah povečuje tudi ogroženost varnosti njenih pripadnikov, zato bodo poveljniki v prihodnje še bolj posegali po zmogljivostih Enote za elektronsko bojevanje, predvsem z vidika njenega ključnega prispevka pri zagotovitvi posameznih ukrepov zaščite sil. Obveščevalna zvrst SIGINT se zato na obrambnem in vojaškem področju postavlja zdaj v novo perspektivo. Njeno dosedanjo primarno vlogo bodo dopolnjevale nove in zahtevnejše naloge v okviru sodelovanja Slovenske vojske v mednarodnih operacijah in misijah. Na eni strani bo enota morala še naprej zagotavljati

[68] Odredbodajalec za izdajanje vsebinskih in strokovnih usmeritev Enote za elektronsko bojevanje za izvajanje nalog SIGINT je ministrica za obrambo, ki izda pisno odredbo za določeno časovno obdobje (izhodišče se nahaja v 21. členu ZSOVA).

[69] O »koliziji načel in predstav« v praksi je govoril tudi poveljnik sil Slovenske vojske v sklopu strukturiranega intervjuja, a je v zvezi s tem še poudaril, da »sta zato dobro sodelovanje in izmenjava strokovnih mnenj med vsemi akterji na tem področju zelo pomembna. Prav iz tega razloga je kadrovanje na tem področju, sploh pa v poveljniški liniji, toliko bolj premišljeno.«

ustrezen SIGINT delež v skupno obveščevalno sliko za neposredno podporo silam v operacijah, na drugi strani pa bo z ukrepi elektronskega bojevanja zagotavljala tudi njihovo neposredno zaščito. Generalni direktor Obveščevalno-varnostne službe Ministrstva za obrambo je v intervjuju razmišljal o potrebi po vzpostavitvi učinkovitih mehanizmov za optimalno izrabo vseh razpoložljivih virov znotraj obrambnega kot tudi nacionalno varnostnega sistema in predvsem po opredelitvi uporabe posameznih obveščevalnih podzvrsti za njihovo t. i. preventivno in ofenzivno delovanje, kot jih sam imenuje. V okviru tega bo obveščevalna zvrst SIGINT v prihodnje prispevala pomemben delež predvsem v obveščevalni proces, ki bo integriran s procesi bojnega delovanja[70] Slovenske vojske v mednarodnih operacijah in misijah. Zmogljivosti elektronskega bojevanja pa bo enota prispevala predvsem za izvajanje ukrepov zaščite sil Slovenske vojske. Da bo to lahko izvedla, bo Slovenska vojska svoje razpoložljive zmogljivosti morala dopolniti, razširiti in nadgraditi, za kar bo potrebovala jasne in pravočasne usmeritve odločevalcev ter ustrezne finančne in kadrovske vire[71].

6.4 Sistemski scenariji možne prihodnje ureditve SIGINT področja

Pred zmogljivosti SIGINT se tako na obrambno-vojaškem področju v prihodnosti postavljajo zahtevnejše in kompleksnejše naloge, zato bom poskušala v tem delu naloge ugotoviti, ali so obstoječe sistemske rešitve primerne glede na izzive, ki se pred nas postavljajo v dolgoročnem obdobju, ali pa lahko z oblikovanjem sistemskega scenarija ponudim boljše in ustreznejše. Scenarij sem časovno umestila v dolgoročni okvir, ker predstavlja dolgoročno obrambno načrtovanje, ki ponavadi zajema obdobje 15-20 let (Barjaktarević 2006, 1), tudi temelj za razvoj izbranih parametrov oziroma spremenljivk v obrambnem sistemu, ki sem jih določila za potrebe modeliranja. Srednjeročno obdobje, ki na obrambnem področju pomeni obdobje 5 let, je za razvoj izbranih parametrov oziroma spremenljivk v obrambnem sistemu in oblikovanje sistemskega scenarija prekratko.

[70] Bojno delovanje definira aktualna vojaška doktrina kot skupni naziv za vse vrste ofenzivnih, defenzivnih in specialnih delovanj, ki jih vojska izvaja, da bi dosegla vojaški ali politični cilj. Vključuje tudi nekatere vrste informacijskega delovanja. Bojno delovanje obsega postopke in ukrepe, ki s svojimi učinki povzročajo spremembe bojne moči in taktičnega položaja sovražnika. Izvaja se za zavzetje prostora ali objekta, uničenje, nevtraliziranje ali onemogočanje sovražnika, zadrževanje njegovega napredovanja, obrambo območja ali objekta in drugo (PDRIU 2006, 93).

[71] Na to je v intervjuju opozoril tudi poveljnik sil Slovenske vojske.

Čeprav sem okvirno idejno izhodišče za oblikovanje scenarijev med drugim dobila tudi iz interpretacije dveh izvedenih intervjujev - z generalnim direktorjem Obveščevalno varnostne službe Ministrstva za obrambo in s poveljnikom sil Slovenske vojske, gre pri oblikovanju scenarijev v celoti za plod lastnega razmišljanja.

6.4.1 Teoretične osnove in metodologija oblikovanja scenarijev

Začetki metode načrtovanja s pomočjo scenarijev segajo v vojaško industrijo, kjer se je med drugo svetovno vojno za potrebe projekta Manhattan (razvoj atomskega orožja) tudi prvič formalno izoblikovala. Od 90. let naprej se metoda vedno pogosteje uporablja tudi za potrebe načrtovanja v javni sferi.

Metoda scenarijev je opisni način za obravnavo različnih možnih prihodnosti. Osredotoča se na vzročne procese in točke odločitev, zato je še posebej uporabna za odločevalce na različnih ravneh. Različni scenariji pomagajo izbrati primerno pot tako, da predstavijo različna možna sosledja dogodkov. Možne prihodnosti opisujejo skozi razvoj vzročno-posledičnih korakov. Kadar se uporabljajo za potrebe načrtovanja politik, so scenariji skice prihodnosti, ki temeljijo na shematskih opisih določenih ključnih spremenljivk.

V nasprotju z drugimi metodami napovedovanja scenariji ne predvidevajo enega samega načina v prihodnosti, temveč predstavijo različne možne variante, ki so odvisne od tega, koliko lahko različne spremenljivke vplivajo druga na drugo. Prednost metode scenarijev je večdimenzionalnost, saj dopušča uporabo poljubnega števila spremenljivk. Metoda se tudi izogne problemu izrecnega napovedovanja prihodnosti, saj zanjo predvideva več možnih opcij. Zavedati pa se je treba, da scenariji niso objektivne narave ter da podlegajo omejitvam uporabljenih metod ali ekspertnih mnenj (Twrdy in ostali 2007).

V grobem ločimo dva osnovna tipa metod:

- kvantitativne metode ter
- metode, temelječe na ekspertnih mnenjih.

Prve uporabljajo statistiko in računalniške modele ter tudi kvantificirane predstavitve kvalitativnih informacij, druge temeljijo izključno na poglobljenem ekspertnem mnenju in

tehnikah izmenjave mnenj. V praksi je večina scenarijev kombinacija obeh osnovnih tipov metod (Twrdy in ostali 2007).

Pri strateškem načrtovanju pa pogosto iščemo odgovor na kompleksna, večdimenzionalna vprašanja, ki jih kvantitativno ni mogoče opredeliti. Prvi, ki je na to poskušal najti odgovor že v prejšnjem stoletju, je bil Fritz Zwicky, ki je razvil t. i. morfološko analizo kot splošno metodo za preučevanje ne-kvantitativnih, kompleksnih primerov, ki danes predstavlja temelj ne-kvantitativnega modeliranja za podporo v procesu odločanja. Danes je ta metoda razširjena in znanstveno izpopolnjena ter podprta z računalniško tehnologijo, uporablja pa se strateško načrtovanje in modeliranje rešitev ne-kvantitativnih primerov. Strokovna literatura tovrstne ne-kvantitativne probleme s področja strateškega načrtovanja opredeljuje s terminom »zlobni problemi« (angl. wicked problems) (Ritchey 2005). Za tovrstne probleme je značilno, da (Twrdy in ostali 2007):

- zanje ne obstaja jasna in dokončna formulacija problema,
- ne moremo jasno opredeliti, kdaj je problem rešen,
- rešitve niso prave ali napačne, temveč so samo boljše in slabše,
- ne obstajajo takojšnji ali dokončni preizkusi rešitev,
- je vsaka rešitev ekskluzivna in je število možnih rešitev neomejeno,
- se vsak »zloben problem« lahko obravnava kot simptom drugega »zlobnega problema«,
- so njegovi vzroki lahko pojasnjeni na več načinov, pri čemer izbira razlage določa tudi naravo rešitve problema.

Iz navedenega je razvidno, da se tudi izbrana problematika preučevanja vloge in umestitve zmogljivosti SIGINT znotraj obrambnega sistema Republike Slovenije lahko uvrsti med t. i. zlobne probleme. Vsekakor to velja tudi za primer načrtovanja prihodnjih zmogljivosti SIGINT in oblikovanje scenarijev njihovega razvoja.

Ena od uveljavljenih metodologij za reševanje tovrstnih kompleksnih in ne-kvantitativnih primerov je splošna morfološka analiza (General Morphological Analysis GMA), ki se je razširila in uveljavila predvsem na področju razvoja strateških študij v zadnjih dveh dekadah. Gre za metodo strukturiranja in raziskovanja večdimenzionalnih in praviloma ne-kvantificiranih problemov, ki razvija logični model za predstavitev celote možnih rešitev danega problemskega sklopa (Ritchey 2008).

Proces splošne morfološke analize je sestavljen iz vrste iterativnih korakov, ki predstavljajo cikle analize in sinteze. Analitična faza se začne z opredelitvijo in izborom najpomembnejših dimenzij (spremenljivk) problemskega sklopa. Vsaki od teh dimenzij določimo razpon relevantnih stanj oz. vrednosti. Skupaj sestavljajo parametre nekega problemskega sklopa (Ritchey 2005).

Glede same tipologije scenarijev bom za preučevanje svojega problemskega sklopa prevzela tipologijo scenarijev, ki je bila predlagana v okviru evropskega projekta ESPON 3.2[72] in je tudi sicer splošno uporabna (Twrdy in ostali 2007):

- Tip 1: scenariji iz sedanjosti v prihodnost

so temeljni ali trendni scenariji in slonijo na predpostavki, da bodo strategije in politike akterjev ostale bolj ali manj nespremenjene;

- Tip 2: pričakovani scenariji

slonijo na predpostavki, da se bodo zgodile pomembne spremembe v obnašanju in aktivnostih vpletenih akterjev, medtem ko do pomembnih sprememb javnih politik ne bo prišlo;

- Tip 3: scenariji pričakovanih politik

slonijo na predpostavki, da se bodo glavne spremembe zgodile v polju javnih politik;

- Tip 4: proaktivni scenariji

izhajajo iz prihodnjih situacij in ugotavljajo, kako bi se lahko razvile iz sedanjega stanja in trendov, kaj bi se lahko doseglo in čemu bi se bilo dobro izogniti v okviru danih omejitev, virov ali tehnologij.

Pri preučevanju nakazanega problemskega sklopa bom ob predpostavki, da se obnašanje in aktivnosti vpletenih akterjev in tudi javnih politik spremenijo, uporabila integrirani scenarij, kot kombinacijo zadnjih treh tipov. Proces oblikovanja scenarijev pa bo združil obe osnovni metodi, to je kvantitativno in na ekspertnih mnenjih temelječo metodo. V grobem se je parametrsko kvantificiranje (vrednotenje izbranih spremenljivk) tematsko navezovalo na hipoteze 1, 2 in 4, kar v tem primeru privzemam kot osnovo za nekakšno ekspertno mnenje.

[72] Spatial Scenarios and Orientations in relation to the ESDP and Cohesion Policy.

6.4.2 Scenariji

Pri oblikovanju treh scenarijev zmogljivosti SIGINT na obrambnem področju sem se oprla na prej predstavljeno tipologijo scenarijev, in sicer konkretno na Tip 2, Tip 3, in Tip 4, v okviru katere sem upoštevala tri ključne predpostavke, in sicer:

- Tip 2: da se zgodi *sprememba v obnašanju in aktivnosti vpletenih akterjev*, ki jih v tem problemskem sklopu definiram kot notranje (SOVA, OVS in SV) in zunanje (mednarodna skupnost, tuja država...);
- Tip 3: da se zgodi *sprememba javnih politik,* kar v tem primeru lahko pomeni spremembo nacionalne varnostne strategije, obrambne strategije ali nacionalne obveščevalne politike;
- Tip 4: da se zgodi *sprememba splošne varnostne situacije* (tveganja in grožnje nacionalni varnosti), kar lahko vodi v neposredne spremembe v organizaciji, vodenju in upravljanju zmogljivosti SIGINT znotraj obrambnega sistema.

Najbrž je takoj jasno, da vse te spremembe vodijo tudi v spremembo izbranih ključnih spremenljivk. Sprememba javnih politik vsekakor dolgoročno vodi v spremembo pravnega okvira, ta vpliva na spremembe pri zagotavljanju virov in zato vseh ostalih spremenljivk, vključno z nadzorom. Sprememba splošne varnostne situacije (tveganja in grožnje nacionalni varnosti) pa neposredno vpliva na izbrano spremenljivko težišče delovanja, strukturno odzivnost, proaktivnost v obveščevalnem procesu, vpliva pa lahko tudi na spremembo pri zagotavljanju virov in posledični razvoj. V okviru izbrane tipologije bom pri vseh treh scenarijih poskušala ugotoviti, kako bi se obstoječe zmogljivosti SIGINT na obrambnem področju, ki so umeščene na taktično raven, kar predstavlja sedanjo (aktualno) rešitev in hkrati izhodišče za vse tri scenarije, lahko razvile v učinkovite zmogljivosti ob spremenjenih treh različnih predpostavkah (akterji, javne politike in varnostna situacija).

V časovni dimenziji je vse izbrane spremenljivke treba umestiti v dolgoročno obdobje, čeprav je jasno, da so nekatere spremembe lahko časovno zelo negotove (predvsem pri tipu 4, ki predpostavlja spremembo v splošni varnostni situaciji ter tveganju in grožnjah nacionalni varnosti). Te parametre in dimenzije sem upoštevala pri oblikovanju scenarijev.

Tip 2 »AKTERSKI SCENARIJ«

Ta scenarij predvideva spremembo v obnašanju in aktivnosti vpletenih akterjev, ki jo časovno sicer lahko omejimo tudi na srednjeročno obdobje, vendar pa njene implikacije zagotovo segajo v dolgoročno obdobje. Akterji so v tem problemskem sklopu lahko različni; lahko gre za kateregakoli akterja znotraj nacionalno varnostnega sistema (SOVA, OVS ali Slovenska vojska), lahko pa gre tudi za zunanjega akterja (mednarodna skupnost, tuja država), ki spremeni svoje aktivnosti ali obnašanje tako, da te spremembe neposredno in nedvomno posežejo v razpoložljivost zmogljivosti SIGINT znotraj Slovenske vojske (aktualno stanje). Na mikroravni to pomeni, da Slovenska vojska te zmogljivosti izgubi iz svoje strukture ali pa jih mora prestrukturirati za izvajanje drugačnih nalog. Slovenska vojska zato preusmeri težišče svojega delovanja samo na zmogljivosti elektronskega bojevanja za podporo pri zaščiti sil Slovenske vojske v mednarodnih operacijah in misijah (MOM). V tem primeru si bo strateški obveščevalni organ na obrambnem področju prizadeval za čimprejšnje formiranje lastnih zmogljivosti SIGINT, kar pa neposredno vpliva tako na spremembo pri zagotavljanju virov (kadri, finance, infrastruktura, operativna tehnika) kot tudi na spremembo pravnega okvira (predvsem ZOBr, ki daje podlago za izvajanje SIGINT nalog zgolj EEB Slovenske vojske). Oboje zahteva dolgoročni časovni okvir. Če javne politike v tem časovnem okviru niso uspele podpreti obnašanja in aktivnosti akterjev, bodo ta prizadevanja strateškega obveščevalnega organa zaman. To pomeni, da zmogljivosti SIGINT na obrambnem področju izginejo, kar ima lahko resne implikacije pri zagotavljanju nacionalne varnosti, sploh pa pri zagotavljanju varnosti naših pripadnikov, ki delujejo v mednarodnih operacijah in misijah. Če pa javne politike uspejo v tem času podpreti obnašanje in aktivnosti akterjev, bi imelo na drugi strani to dolgoročno pozitivne implikacije za strateško obveščevalno dejavnost na obrambnem področju: večja strukturna odzivnost teh zmogljivosti, proaktivnost v obveščevalnem procesu, enostavnejši menedžment in boljši razvojni temelji zaradi razpoložljivih virov. Strateški obveščevalni organ na obrambnem področju bi z lastnimi zmogljivostmi SIGINT, v odvisnosti od varnostnih razmer usmerjal težišče delovanja teh zmogljivosti, kar je ključnega pomena predvsem v primeru spremenjene varnostne situacije, kjer mora biti vzpostavljena učinkovita strukturna odzivnost. Glede na varnostno situacijo, bi strateški organ na obrambnem področju prilagajal težišče delovanja tako potrebam Slovenske vojske v mednarodnih operacijah in misijah kot tudi drugim potrebam nacionalne varnosti. Vse to pa bi strateškemu obveščevalnemu organu nedvomno dalo več avtoritete in več moči, kar posledično pomeni tudi intenzivnejšo nadzorno funkcijo.

Sistemske rešitve, ki jih postavlja ta scenarij v prvem delu, so zaskrbljujoče, ker pomenijo razvoj takšnih okoliščin, ki lahko pripeljejo do resnih implikacij za celoten nacionalno varnostni sistem, sploh pa za Slovensko vojsko in njene pripadnike, ki izvajajo naloge zunaj domovine. V drugem delu pa s predpostavko, da se sicer vključijo javne politike, pa se okoliščine relativno dobro iztečejo. Vendar ne glede na to scenarij nazorno prikaže popolno odvisnost sistemskih rešitev od akterjev, zato je tak scenarij brez podpore javnih politik lahko za obveščevalno zvrst SIGINT in za obveščevalno dejavnost nasploh zelo neugoden.

Tip 3 »POLITIČNI SCENARIJ«

Ta scenarij v nasprotju s prvim, predvideva v prvi fazi spremembo javnih politik, kar v tem primeru lahko pomeni spremembo nacionalne varnostne strategije, obrambne strategije ali nacionalne obveščevalne politike in je opredeljen v dolgoročni časovni okvir. K spremembi javnih politik se praviloma pristopa premišljeno, organizirano in sistemsko. Po mojem mnenju gre za ugoden vzročno-posledični scenarij, ker v nasprotju z »akterskim« predvideva postopno spremembo političnih ciljev, katerim sledijo posamezni akterji. Seveda to zahteva kvalitetno načrtovanje ciljev, sredstev in poti oziroma načinov, kako le-te doseči. Vključeni akterji so v tem scenariju lahko enaki kot pri prvem, sam razvoj problemskega sklopa pa se v vsebini bistveno ne razlikuje od prvega. Na mikroravni to pomeni, da se zmogljivosti SIGINT v Slovenski vojski prestrukturirajo za izvajanje drugih ali dopolnjenih nalog. Slovenska vojska težišče svojega delovanja tako preusmeri samo na zmogljivosti elektronskega bojevanja za podporo pri zaščiti sil v mednarodnih operacijah in misijah, medtem ko strateški obveščevalni organ neposredno usmerja težišče delovanja za zmogljivosti SIGINT, glede na varnostne razmere, kar je ključnega pomena v primeru spremenjene varnostne situacije. Vse to pozitivno vpliva na spremembo pri zagotavljanju virov, na razvoj zmogljivosti SIGINT, pomeni pa tudi njihovo večjo strukturno odzivnost, proaktivnost v obveščevalnem procesu in enostavnejši »obveščevalni menedžment«. Tudi v tem primeru bi strateški obveščevalni organ dobil več avtoritete pri načrtovanju ciljev in sredstev za zmogljivosti SIGINT, s tem pa posledično tudi več moči, kar pa zahteva intenzivnejšo nadzorno funkcijo.

Gre za ugoden scenarij, ki predvideva premišljene in dobro načrtovane vzročno-posledične spremembe. Te umeščajo usmerjanje SIGINT zmogljivosti dolgoročno na strateško raven, kar lahko z vidika morebitne potrebe po optimalni izrabi vseh razpoložljivih virov za izvajanje te

dejavnosti olajša povezovanje posameznih subjektov znotraj nacionalno varnostnega sistema in poveča njegovo učinkovitost.

Tip 4 »KRIZNI SCENARIJ«

Ta scenarij predvideva spremembo splošne varnostne situacije, ki je v časovni okvir umeščena nedefinirano in negotovo (npr. neposredna grožnja terorističnega napada ali pa, da se zgodi teroristični napad). Ta situacija pomeni krizno organiziranje vseh državnih institucij, predvsem pa varnostnega sektorja. Intenzivno in proaktivno izvajanje obveščevalne dejavnosti na nacionalni ravni, pomeni:

- angažiranje vseh razpoložljivih nacionalnih obveščevalnih zmogljivosti, predvsem pa tistih obveščevalnih zvrsti, ki zbirajo podatke s pomočjo tehnologije, torej tudi SIGINT;
- angažiranje s strani obveščevalnih zmogljivosti sosednjih držav in mednarodnih struktur (NATO).

Težišče delovanja razpoložljivih nacionalnih zmogljivosti SIGINT bi se usmerilo predvsem na spremljanje indikatorjev groženj nacionalni varnosti. V ta namen bi razpoložljive zmogljivosti SIGINT na taktični ravni Slovenske vojske (aktualna rešitev) prešle pod neposredno pristojnost obveščevalnega organa na strateški ravni, ki bi v okviru proaktivnega obveščevalnega procesa hkrati definiral zahteve in zagotavljal centralizirani »menedžment zbiranja« z ostalimi obveščevalnimi disciplinami in strukturami (tudi mednarodnimi) ter v sklopu procesa, izvajal celovito analizo, produkcijo in diseminacijo. V tem primeru bi lahko dobili spremenjeno, visoko strukturno odzivnost in proaktivnost razpoložljivih zmogljivosti SIGINT. Posledično bi takšna situacija sicer vplivala na spremembo pri zagotavljanju virov, vendar bi bila njena vzdržljivost kratkotrajno omejena. Negotovost časovne dimenzije v tem scenariju je zelo problematična, predvsem z vidika razvoja zmogljivosti SIGINT, ki sam po sebi zahteva dovolj širok časovni okvir.

Ta scenarij nakaže rešitve, ki bi lahko predstavljale priporočilo za prihodnji model proaktivnih SIGINT zmogljivosti na obrambnem področju. Seveda pa se je ob tem potrebno zavedati, da le-ta temelji na organiziranosti za potrebe obvladovanja krizne situacije in na zelo

omejenih časovnih okvirih, zaradi katere lahko trpi predvsem razvojna dimenzija te obveščevalne zvrsti.

Zanimiv zaključek je pri vseh treh scenarijih naslednji: če želimo doseči visoko strukturno odzivnost in proaktivnost obveščevalne dejavnosti na obrambnem področju, je potrebno spremeniti sistemsko umestitev zmogljivosti SIGINT v Slovenski vojski. Ne glede na to, ali zmogljivosti SIGINT umestimo na taktično, operativno ali strateško raven, je za njihovo visoko odzivnost in proaktivnost treba vzpostaviti ustrezne organizacijske, normativne in strokovne mehanizme, ki bodo zagotavljali neposredno pristojnost obveščevalnega organa na strateški ravni za načrtovanje in upravljanje s temi zmogljivostmi.

6.4.3 Programsko orodje DEXi

Z uporabo programskega orodja DEXi, ki je sicer namenjeno za podporo v procesu odločanja in večparametrsko modeliranje, sem želela še na empirični način podpreti svoje zaključke iz zgornjih scenarijev. Za modeliranje in vrednotenje sem izbrala in uporabila samo tiste ključne spremenljivke oziroma parametre, ki sem jih preučevala v okviru te naloge (pravni okvir, zagotavljanje virov, proaktivnost v obveščevalnem procesu, težišče delovanja, strukturna odzivnost, razvoj in nadzor). Ob tem je treba poudariti, da sem se pri modeliranju zaradi preobsežnega modela morala odpovedati eni spremenljivki (konkretno je bila to spremenljivka *razvoj* z vsemi atributi) in dvema atributoma (*koraka 1* in *6* v obveščevalnem procesu).

Kot izhodišče sem vzela vsa tri možna priporočila oziroma tri variante umestitve SIGINT zmogljivosti na obrambnem področju, in sicer:
1) zmogljivosti SIGINT na taktični ravni Slovenske vojske (aktualna rešitev, ki zmogljivosti SIGINT umešča v Obveščevalno-izvidniški bataljon Slovenske vojske);
2) zmogljivosti SIGINT na operativni ravni Slovenske vojske (kot samostojna zvrst na operativni ravni, medtem ko zmogljivosti elektronskega bojevanja ostajajo na taktični ravni);
3) zmogljivosti SIGINT na strateški ravni (v Slovenski vojski ali v Obveščevalno-varnostni službi, medtem ko zmogljivosti elektronskega bojevanja ostajajo na taktični ravni).

6.4.3.1 Modeliranje in vrednotenje

V okviru problemskega sklopa prihodnje vloge zmogljivosti SIGINT na obrambno-vojaškem področju sem določila naslednje spremenljivke s ključnimi atributi:

1. pravni okvir:
   - ZOBr,
   - ZSOVA,
   - Vojaška doktrina[73];
2. zagotavljanje virov (kadrovski, finančni, tehnološki, infrastrukturni viri);
3. proaktivnost v obveščevalnem procesu:
   - korak 1: definiranje potreb (naknadno izločen iz DEXi)[74] ,
   - korak 2: načrtovanje in usmerjanje,
   - korak 3: menedžment zbiranja in obdelave (fuzija z ostalimi disciplinami),
   - korak 4: celovita analiza in produkcija (nagl. all-source),
   - korak 5: diseminacija in
   - korak 6: povratna informacija (naknadno izločen iz DEXi);
4. težišče delovanja:
   - za nacionalno varnostne potrebe,
   - za mednarodne operacije in misije (zaščita sil);
5. strukturna odzivnost (v okviru nacionalno varnostnega sistema (NVS) in v okviru Ministrstva za obrambo (MORS));
6. razvoj strokovnega področja z atributi - naknadno izločen iz DEXi[75] :
   - izvedba projektov,
   - razvojni programi,
   - dolgoročne investicije operativnih zmogljivosti;
7. nadzor (politični, notranji (resorni), sodni, javnost).

[73] Vojaško doktrino sem namenoma umestila v pravni okvir zato, ker predstavlja za Slovensko vojsko najvišji vojaško strokovni dokument in podlago za njeno organiziranje in delovanje in je hkrati tudi akt Vlade Republike Slovenije, ki definira sprejeta načelna stališča o organiziranju, uporabi in delovanju Slovenske vojske pri obrambi države in izvajanju drugih nalog, s katerimi se uresničuje obrambna strategija Republike Slovenije (PDRIU 2006, 7).

[74] Programsko orodje Dexi.dxi v modelu 6-ih korakov v obveščevalnem procesu javi preobsežnost možnih kombinacij, zato sem iz modeliranja in analize izključila korak 1 in korak 6 obveščevalnega procesa.

[75] Model je bil za programsko orodje DEXi preobsežen, zato sem iz modeliranja s pomočjo programskega orodja izključila celotno spremenljivko *razvoj* z vsemi njenimi atributi, kar pa bistveno ni vplivalo na končni rezultat. Spremenljivka *razvoj* je vključena v interpretacijo rezultatov bolj kot posledica.

Vrednotenje (kvantificiranje) zgoraj opredeljenih spremenljivk in njihovih atributov je potekalo opisno:

- optimalno (+)
- dobro (o) in
- slabo (-)

in številčno s ponderji oziroma »težo«, tako da vsota ponderjev posameznih spremenljivk ali njenih atributov ni presegla 1 (oziroma 100 %). T. i. ponderiranje ali »obtežitev« posameznih spremenljivk in atributov je potekalo v dveh delih. Prvi nivo predstavlja ponderiranje spremenljivk, drugi nivo pa ponderiranje atributov znotraj teh spremenljivk. Med šestimi spremenljivkami sem najbolj obtežila spremenljivke *pravni okvir*, *proaktivnost v obveščevalnem procesu* in *strukturna odzivnost* (vsako po 20 %). Vse tri namreč prepoznavam kot temeljne oziroma esencialne z vidika legitimnosti priporočil, ki bodo iz tega modeliranja izhajala. Spremenljivki *zagotavljanje virov* in *težišče delovanja* pa prepoznavam kot sekundarni spremenljivki zato sem vsako obtežila s 15%. Spremenljivko *nadzor* sem obtežila z 10 %, ker izhaja kot pomembna posledica vseh ostalih spremenljivk. Ponderiranje atributov znotraj posamezne spremenljivke je potekalo veliko bolj kompleksno. Zelo pomembno izhodišče je predstavljalo dejstvo, da sem se pri oblikovanju modela omejila zgolj na obrambno področje. Zato je atribut *ZOBr*, ki predstavlja temeljni pravni akt na obrambnem področju obtežen s kar 50 %, atribut *Vojaška doktrina* pa je, kot pomemben strokovni in najvišji načelni okvir, ovrednoten s 40 %. Najmanj obtežen je atribut *ZSOVA*, ker skladno z ugotovitvami iz naloge tudi v prihodnje ne bi smel predstavljati temeljnega izhodišča za oblikovanje zmogljivosti SIGINT na obrambnem področju. Atributa *finance* in *kadri* znotraj spremenljivke *zagotavljanje virov* sem obtežila najbolj, ker ju ocenjujem kot ključna vira, ki posledično zagotavljata pogoje vsem ostalim virom oziroma atributom. Res pa je, da brez ustreznih finančnih virov tudi kadrovskih ne bo, zato prepoznavam finančne vire med vsemi, kot najpomembnejše. Kar se tiče atributov znotraj *proaktivnosti obveščevalnega procesa*, sem kot najpomembnejši atribut ocenila *korak 4* (celovita analiza in produkcija) s 40 %, ki predstavlja rezultat uspešnosti samega modela, medtem ko je po teži takoj za njim *korak 2* (načrtovanje in usmerjanje). Kot »najlažji atribut« sem ocenila *korak 5* (diseminacija), ki po mojem mnenju predstavlja atribut zgolj tehničnih rešitev. Oba atributa znotraj spremenljivke *težišče delovanja* sta, glede na samo poslanstvo teh zmogljivosti, kot tudi glede na trenutne splošne nacionalne in globalne varnostne razmere, enako ovrednotena (vsak po 50 %). V okviru spremenljivke *strukturna odzivnost* pa sem bolj obtežila atribut *nacionalno varnostni sistem*, ker ocenjujem, da je ključno pri tem oblikovanju dobiti ustrezen model, ki z vidika

odzivnosti ne bo omejen zgolj na obrambno področje (atribut *Ministrstvo za obrambo*), temveč bo razširjen na odzivnost v celotnem nacionalno varnostnem sistemu. Zelo pomembno je namreč, da se predvsem zaradi omejenih virov, vse razpoložljive zmogljivosti SIGINT v nacionalno varnostnem sistemu medsebojno povežejo z ustreznim mehanizmom. Pri ponderiranju spremenljivke *nadzor* prepoznavam *parlamentarni nadzor*, ki je temeljni varuh vsake demokracije, kot najpomembnejši. Najmanj sem pa obtežila *resorni nadzor*, ker je omejen zgolj na nadzor v eni veji oblasti in ne zagotavlja temeljnega načela vzpostavitve sistema zavor in ravnovesij vseh ostalih vej ter nadzora nadzornikov. *Nadzor javnosti* sem ovrednotila s težo 20 %, ker je z vidika zagotavljanja legitimnosti te obveščevalne dejavnosti, njen kritični vidik za vzpostavitev ustreznega ravnovesja med sodobno varnostjo in sfero poseganja v človekove pravice zelo pomembno in nezanemarljivo dejstvo. Skladno z navedenim prikazuje spodnja tabela konkretno vrednotenje izbranih spremenljivk in atributov brez podpore programskega orodja DEXi. Z rdečo barvo so označeni tisti atributi in spremenljivka, ki so zaradi preobsežnosti modela bili izključeni iz kasnejše obdelave v DEXi.

Spremenljivka (teža/ponder v %)	**Atribut (teža/ponder v %)**	**SIGINT v EEB/OIB**	**SIGINT v SV**	**SIGINT v OVS MORS**
pravni okvir (20%)	ZOBr (50%), ZSOVA (10%), Vojaška doktrina (40%)	+ - +	o - +	- + -
zagotavljanje virov (15%)	kadri (30%), finance (40%) tehnika (20%), infrastruktura (10%)	o - - +	o o o +	+ + + o
proaktivnost v obveščevalnem procesu (20%)	korak 1 korak 2 (30%) korak 3 (20%) korak 4 (40%) korak 5 (10%) korak 6	- - o - o -	o o + - o o	+ + o + + -
težišče delovanja (15%)	nacionalna varnost (50%) mednarodne operacije in misije (50%)	o o	o +	+ o
strukturna odzivnost (20%)	nacionalno varnostni sistem (60%) ministrstvo za obrambo (40%)	- o	o o	+ +

razvoj (iz DEXi izključena spremenljivka)	izvedba projektov razvojni programi investicijski programi	o - -	o o o	+ o +
nadzor (10%)	parlamentarni (40%) resorni (10%) sodni (30%) javnost (20%)	o o o -	o + o -	+ o o o

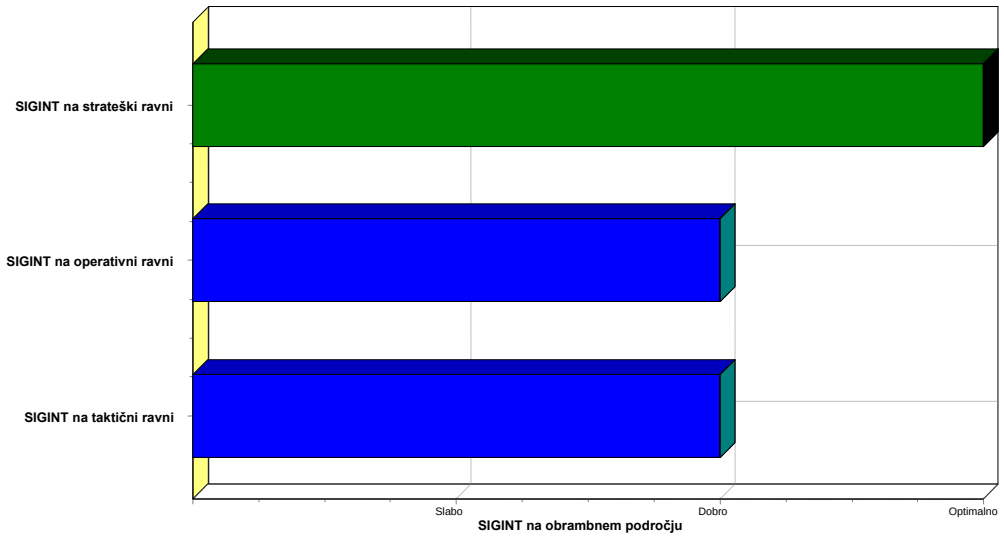
Tabela 6.1: Vrednotenje spremenljivk in atributov.

6.4.3.2 Rezultati

Z vnosom modela v programsko orodje DEXi dobimo za izbrane tri variante umestitve zmogljivosti SIGINT na obrambnem področju rezultate, ki so v naslednji obliki in natančneje predstavljeni v Prilogi - Rezultati modeliranja s programskim orodjem DEXi, in sicer:

- Drevo kriterijev,
- Zaloge vrednosti,
- Rezultati,
- Grafikon.

V splošnem je dobljene rezultate s pomočjo DEXi mogoče interpretirati na naslednji način: Zmogljivosti SIGINT na taktični ravni, ki pomeni trenutno aktualno rešitev znotraj Slovenske vojske, predstavljajo skupaj z varianto zmogljivosti SIGINT na operativni ravni dobro rešitev, vendar slabšo od tiste, ki predvideva umestitev zmogljivosti SIGINT na strateško raven. Ta varianta predstavlja, skladno z rezultati, dobljenimi s pomočjo DEXi, optimalno rešitev (Graf 6.1) in hkrati potrdi splošni zaključek iz scenarijev. Za doseganje visoke odzivnosti in proaktivnosti znotraj obveščevalne dejavnosti na obrambnem področju je kot edina ponujena optimalna rešitev vzpostavitev aktivnega organa SIGINT na strateški ravni.



Graf 6.1: Izbira najustreznejše variante (grafični rezultati iz DEXi).

7 SKLEPNA BESEDA IN VERIFIKACIJA HIPOTEZ

Preučevanje obveščevalne zvrsti SIGINT znotraj nacionalno varnostnega sistema je zelo kompleksno in še dokaj zaprto področje. Deloma lahko razloge iščemo v nepoenoteni terminologiji, ki otežuje kvalitetno raziskovalno delo in akademsko preučevanje tega področja. Deloma pa razloge najdemo v praksi kulture tajnosti in mistifikacije obveščevalne dejavnosti tako v slovenskem kot mednarodnem prostoru.

V vsaki družbeni ureditvi, pa najsi bo demokratična ali ne, pomeni nadzor nad informacijami pomembno moč tistega, ki ta nadzor izvaja, hkrati pa pomeni tudi možnost njene zlorabe, če ni pod neprestanim nadzorom vseh vej oblasti. Obveščevalne službe v okviru izvajanja svojih nalog zagotovo posegajo v človekove pravice in temeljne svoboščine, zato so vedno bolj izpostavljene različnim nadzornim mehanizmom. Po temeljnih demokratičnih in ustavnih načelih delitve oblasti, se tudi nadzor nad delom teh služb izvaja v vseh njenih vejah: zakonodajni, sodni in politični. Poleg najpomembnejšega, političnega ali parlamentarnega nadzora, obstajajo v sodobnih družbah tudi druge oblike nadzora in predvsem z vidika neodvisnosti nič manj pomembni nadzorni mehanizmi, ki vnašajo višjo stopnjo demokratičnosti in transparentnosti (ombudsmani, informacijski pooblaščenci, nevladne organizacije, mediji, javnost idr.). To sem lahko potrdila tudi z analizo treh sodobnih evropskih demokratičnih držav (v Republiki Sloveniji, Zvezni Republiki Nemčiji in na Madžarskem).

Večno vprašanje z vidika upravičenosti poseganja v človekove pravice in temeljne svoboščine, ki se postavlja pred obveščevalne službe in njihove nadzornike, pa je, ali je vsako poseganje legitimno, nujno, ustrezno in po načelu sorazmernosti. Meja med osebno svobodo in varnostjo obstaja in zelo pomembno vprašanje je, kje to mejo postaviti. Nesprejemljivo za demokratično družbo bi bilo, da bi se ta meja postavljala na podlagi enostranske ali celo osebne percepcije, zato je nujen tudi kritični vidik javnosti, da bi lahko zagotovili ravnovesje med sodobno varnostjo na eni strani, za ceno poseganja v sfero človekovih pravic in osebnih svoboščin na drugi. S tega vidika so zato enako pomembne tudi zakonsko določene sankcije v primeru kršitve posameznih pristojnosti, ki so lahko civilne in kazenske, pa tudi politične, če so državni organi posegli v človekove pravice in temeljne svoboščine z zlorabo položaja. Za taka in podobna vprašanja se bodo obveščevalne službe v prihodnje morale še odpreti družbi in kulturo tajnosti ohraniti do meje, ki bo strokovno in družbeno sprejemljiva.

Za njihovo protiutež pa so države vzpostavile različne nadzorne mehanizme, ki bdijo nad legalnostjo in politično nevtralnostjo delovanja obveščevalnih služb, kot tudi nad skladnostjo njihovega delovanja s profesionalno etiko in demokratičnimi normami. Če nekaj teh mehanizmov primerjamo, ugotovimo da ni univerzalnega vzorca, ki bi bil enako učinkovit v vseh državah in vseh demokracijah. Država mora zato razviti svoj lastni, njej in najbolj optimalni model.

Po primerjavi urejenosti nadzorne funkcije v Republiki Sloveniji z nadzornimi funkcijami v Zvezni Republiki Nemčiji in na Madžarskem bi lahko rekli, da ima Slovenija kot eno večjih demokratičnih pridobitev danes vzpostavljene vse oblike nadzora nad obveščevalno zvrstjo SIGINT, kar je nedvomno jasen kazalec demokratičnosti naše države. Pa vendar ima v primerjavi z Nemčijo, ki velja za državo z razvito visoko stopnjo demokracije, še vedno razvite prešibke mehanizme, predvsem parlamentarnega nadzora, ki velja za nosilca in varuha demokracije v državi. Nadzor nad obveščevalno zvrstjo SIGINT je zaradi tehnološke in metodološke kompleksnosti zelo zahteven, zato to področje hkrati zahteva permanentno strokovnost in usposobljenost nadzornih teles, predvsem pa proaktivnost teh organov, ki niso odvisni od politične volje. Kot pri nemškem primeru delovanja komisije G-10 bi tudi v primeru Slovenije potrebovali strokovni proaktivni parlamentarni organ, katerega člani bi bili strokovnjaki ali izvedenci obveščevalne stroke, ki bi bili za vzpostavitev učinkovitejšega parlamentarnega nadzora izvzeti iz poslanske funkcije in bi morali biti tudi politično nevtralni, a z ustreznim predznanjem, bogatimi strokovnimi izkušnjami in mandatom, ki bi bil neodvisen od parlamentarnih volitev. Takšno telo bi lahko na eni strani strokovno podpiralo parlamentarno komisijo pri izvajanju nadzora nad obveščevalnimi in varnostnimi službami, na drugi strani pa bi nudilo tudi pomoč in nasvet izvršilni veji oblasti pri kreiranju splošne obveščevalne politike. Nedvomno bo za ta korak potrebna dodatna politična volja.

V prihodnjem obdobju bo treba vzpostaviti tudi druge učinkovitejše vladne nadzorne mehanizme nad njenimi obveščevalnimi subjekti. Na podlagi opravljene analize ugotavljam, da Vlada Republike Slovenije v tem trenutku nima ustreznega proaktivnega organa, ki bi v praksi izvajal nadzor nad obveščevalnimi službami, le-ta je prepuščen posameznim pristojnim ministrom oziroma njihovim resorjem. Z analizo primera nadzorne funkcije obveščevalne dejavnosti na obrambnem področju pa se odpira vprašanje parlamentarnega nadzora nad

posameznimi subjekti v Slovenski vojski za izvajanje vojaške obveščevalne dejavnosti. Le-ta se namreč, razen v primeru obveščevalne zvrsti SIGINT, v praksi še vedno zanemarja.

Analiza pravnega okvira in normativne urejenosti obveščevalne zvrsti SIGINT v primerjavi z nemškim ali madžarskim sistemom kaže, da imamo v slovenskem pravnem redu preširoke in premalo določne zakonske formulacije, ki urejajo tako občutljivo področje, kot je SIGINT. Predvsem zaskrbljujoče je prepletanje zakonskih določil, ki urejajo to področje v naši nacionalni zakonodaji, in prehajanje oziroma sklicevanje posameznih pristojnosti obveščevalnih služb in njihovih pooblastil, z enega zakona na drugega, kar vodi v izrazito netransparentnost področja, dopušča različne strokovne in pravne interpretacije, omejuje pa tudi učinkovito nadzorno funkcijo. Že samo dejstvo, da na nacionalnem obveščevalnem področju ni terminološke usklajenosti, lahko vodi v dodatno pravno in strokovno zmedo. Obstoječa terminološka neusklajenost lahko dodatno ovira naše napore k večji transparentnosti in odprtosti te zvrsti in obveščevalne dejavnosti nasploh; nerazumljivost in nejasnost pa v družbi upravičeno vzbujata dodaten dvom. V okviru splošne nacionalne obveščevalne politike bi bilo treba po vzoru Madžarske in Nemčije najprej vzpostaviti enotne pravne terminološke okvire za vse subjekte izvajanja obveščevalne dejavnosti v okviru nacionalno varnostnega sistema.

Do takrat pa bo obveščevalna zvrst SIGINT v nacionalnem prostoru definirana s tem, kar ni. Primerjalna analiza je med drugim pokazala, da se obveščevalna zvrst SIGINT v Republiki Sloveniji, v Zvezni Republiki Nemčiji in na Madžarskem izvaja na dveh ravneh: na vladni ravni in na obrambnem (vojaškem) področju. Za razliko od Slovenije, izvajajo obveščevalno zvrst SIGINT v obeh državah samostojne organizacijske strukture SIGINT, ki so del širše obveščevalne skupnosti. Po mojem mnenju so te strukture zelo transparentno in zgledno predstavljene v primeru Madžarske, kjer se direktorat SIGINT Vojaškega obveščevalnega urada predstavlja celo na spletnih straneh. Analiza pokaže tudi, da vse tri države prispevajo svoje obveščevalne zmogljivosti v mednarodnih operacijah in misijah in sodelujejo pri vzpostavljanju mednarodne varnosti pod okriljem NATA. Njihovo vodilo za vzpostavitev učinkovitega večnacionalnega obveščevalnega mehanizma pa mora temeljiti na elementu zaupanja[76]. V praksi NATA ta mehanizem resnično deluje, zakaj ne bi deloval tudi doma?

[76] Zanimivo je, da aktualna vojaška doktrina »zaupanja« ne uvršča med vrednote Slovenske vojske, ki so gonilna sila pri uresničevanju njenega poslanstva in izhajajo iz splošnih civilizacijskih vrednot, vrednot slovenske družbe in posebnosti narave delovanja vojske. (PDRIU 2006, 17 - 18).

Pred obveščevalno zvrst SIGINT v primeru Slovenije se v sodobnem nacionalnem in mednarodnem večdimenzionalnem varnostnem okolju postavljajo nove zahteve, ki se vedno bolj izražajo kot potreba po optimalni izrabi vseh razpoložljivih nacionalnih virov izvajanja obveščevalne dejavnosti in njihovem integriranju v skupni obveščevalni proces. Zelo uspešni vzorec za potrebe obveščevalne podpore v mednarodnih operacijah in misijah je nemški primer integriranja zmogljivosti vseh razpoložljivih obveščevalnih služb, od vladne do vojaških.

Kot ugotavljam na primeru pravnega okvirja in normativne urejenosti obveščevalne zvrsti SIGINT v Republiki Sloveniji, le-ta zaradi svoje nejasnosti in širine dopušča tudi interpretacijo odprte pravne možnosti horizontalnega povezovanja subjektov SIGINT in optimalnejše izrabe razpoložljivih virov v sistemu nacionalne varnosti. Čeprav v zvezi s tem zaenkrat ni zaslediti nobenih konkretnejših kazalnikov ali premikov, pa bodo varnostne razmere iz vedno kompleksnejšega in zahtevnejšega okolja prav gotovo zahtevale nekatere spremembe po preoblikovanju obveščevalne funkcije znotraj nacionalno varnostnega sistema ter posledično nekatere organizacijske spremembe. Z oblikovanjem treh sistemskih scenarijev za zmogljivosti SIGINT na obrambnem področju pride potreba po nekaterih organizacijsko-strukturnih spremembah, kakor tudi po horizontalnem povezovanju zelo do izraza, predvsem pa v t. i. »kriznem scenariju«, ko se spremeni splošna varnostna situacija, ki je v časovni okvir vedno umeščena nedefinirano in negotovo. V primeru kriznega scenarija bi se državne institucije, predvsem pa varnostni sektor, krizno organizirale, kar pomeni intenzivno in proaktivno izvajanje obveščevalne dejavnosti z vsemi razpoložljivimi nacionalnimi obveščevalnimi zmogljivostmi in tudi vključitev obveščevalnih zmogljivosti sosednjih držav in mednarodnih struktur (NATO). Težišče delovanja razpoložljivih struktur SIGINT bi se v primeru kriznega scenarija usmerilo predvsem v spremljanje indikatorjev groženj nacionalni varnosti. V ta namen bi razpoložljive zmogljivosti SIGINT na taktični ravni Slovenske vojske prešle pod neposredno pristojnost obveščevalnega organa na strateški ravni, ki bi v okviru proaktivnega obveščevalnega procesa hkrati definiral zahteve in zagotavljal centralizirani »menedžment zbiranja« in fuzije obveščevalnih podatkov. In tu se postavlja vprašanje, ali lahko model, ki izhaja iz kriznih razmer, katere same po sebi zahtevajo veliko proaktivnost v posameznih rešitvah, predstavlja priporočilo za naprej? Najbrž ne, vsaj dolgoročno ne, in to predvsem zaradi specifičnih okoliščin in razmer, v katerih se tak model oblikuje. Njegova vzdržljivost bi bila namreč časovno omejena na obdobje trajanja krize. Optimalni razvoj

prihodnjega modela zmogljivosti SIGINT zato potrebuje mnogo več kot specifično situacijo, ki bi ključne akterje prisilila v ukrepanje in reorganiziranje. Optimalni razvoj prihodnjega modela zahteva premišljen sistemski pristop, ki ima »na svoji strani« podporo javnih politik, kot tudi dimenzijo časa in prostora. Slednja danes ni omejena samo na nacionalno ozemlje ali na soseščino. Vedno večja prisotnost vojaških zmogljivosti Republike Slovenije v mednarodnih operacijah in misijah na eni strani predstavlja pomemben dejavnik naše zunanje politike, na drugi strani pa se z večanjem prisotnosti Slovenske vojske v teh operacijah povečuje tudi ogroženost varnosti njenih pripadnikov. Obveščevalna zvrst SIGINT se zato predvsem na obrambnem in vojaškem področju postavlja v novo perspektivo. Nedvomno bodo poveljniki v prihodnje za zagotavljanje optimalnih ukrepov zaščite sil lastnih pripadnikov, ki delujejo v mednarodnih operacijah in misijah, še bolj posegali po zmogljivostih SIGINT, kakor tudi po zmogljivostih elektronskega bojevanja. Na področju vojaške obveščevalne dejavnosti se vedno bolj izraža potreba po integriranju vseh obveščevalnih senzorjev (vseh obveščevalnih disciplin) v skupni obveščevalni proces, za zagotavljanje celovitih (angl. »all source«) analiz v realnem oziroma skoraj realnem času, ki bo vključen v proces bojnega delovanja sil Slovenske vojske. Vloga obveščevalne discipline SIGINT postaja skupaj z zmogljivostmi elektronskega bojevanja zato vedno bolj nepogrešljiva in nepredstavljiva pri zaščiti sil Slovenske vojske. Zaradi tega bo ta obveščevalna zvrst na obrambnem področju morala svoje zmogljivosti še izpopolnjevati in razvijati tako na konceptualnem kot tudi na doktrinarnem in izvedbenem področju, na močnih strokovnih temeljih, vendar v novi, spremenjeni paradigmi.

Scenariji, ki sem jih oblikovala, dajejo ravno tak zaključek: če želimo doseči visoko strukturno odzivnost in proaktivnost obveščevalne dejavnosti na obrambnem področju, je treba spremeniti obstoječo sistemsko umestitev zmogljivosti SIGINT v Slovenski vojski. Ne glede na to, ali te zmogljivosti umestimo na taktično, operativno ali strateško raven, je za njihovo visoko odzivnost in proaktivnost treba vzpostaviti ustrezne organizacijske, normativne in strokovne mehanizme, ki bodo zagotavljali neposredno pristojnost obveščevalnega organa na strateški ravni za načrtovanje in upravljanje s temi zmogljivostmi. In ko v okviru modeliranja s pomočjo programskega orodja DEXi, ki je namenjeno predvsem podpori v procesu odločanja, ponudimo vse tri variante, izbere kot najbolj optimalno rešitev zadnjo ponujeno - t. j. umestitev zmogljivosti SIGINT na strateško raven. Ne glede na to, kaj pod tem pojmom razumemo, je jasno, da je vzpostavitev aktivnega organa SIGINT na strateški ravni (z ali brez lastnih zmogljivosti SIGINT) zato nujna.

Vsekakor bo to proces, ki bo trajal še naslednja leta in bo odvisen predvsem od javnih politik in razpoložljivih virov. Zahteval bo pa tudi miselni preskok predvsem v percepciji ključnih odločevalcev v Slovenski vojski in Ministrstvu za obrambo.

Pred sodobne obveščevalne službe se nedvomno postavlja še dodaten izziv. Poleg potrebe in zahteve po interaktivnem sledenju v različnih trendih opremljenosti, globalnega varnostnega okolja v vedno bolj izpopolnjenih teoretskih, konceptualnih in metodoloških pristopih mora delo teh služb temeljiti tudi na znanju, inteligentnosti in predvsem na profesionalni etiki. Temelj vseh obveščevalnih služb je zato primerno izobražen, strokovno usposobljen in ustrezno motiviran kader na obveščevalnem področju, ki mora razumeti, da živi v okolju, ki se je spremenilo in se še spreminja. Razumeti mora, da se bo zato spremenila tudi organizacija, v kateri deluje in s katero naj bi se profesionalno identificiral in da je spoštovanje in varovanje najvišjih vrednot naše družbe temeljno načelo njegovega dela, ne glede na to, ali nosi civilno obleko ali pa vojaško uniformo. Ob tem ugotavljam, da obveščevalna stroka v slovenskem prostoru še nima svojega etičnega kodeksa, pa čeprav si najbrž v praksi prizadeva, da z vidika poseganja v človekove pravice in temeljne svoboščine dosledno uresničuje načelo sorazmernosti. Ne glede na to bo ta prizadevanja nesporno utemeljila šele, ko bo razvila svoja etična načela. Obveščevalna dejavnost je prav z vidika avtorizacije poseganja v človekove pravice in temeljne svoboščine tako specifična in občutljiva, da se s kodeksom javnih uslužbencev ne gre zadovoljiti. Najbrž bo obveščevalna dejavnost v slovenskem prostoru v prihodnosti dobila svoj etični kodeks, kot potrditev demokratične zrelosti in spoštovanja najvišjih ustavnih vrednot - človekovih pravic in temeljnih svoboščin tudi v teh strukturah nacionalno varnostnega sistema, se pa zastavlja vprašanje, ali pridobitev etičnega kodeksa pomeni tudi resnično višjo raven etičnosti?

Sodobne obveščevalne službe imajo zato pred seboj zahtevno okolje, ki se zelo hitro spreminja. V sodobnih demokratičnih sistemih se obveščevalne organizacije vedno bolj odpirajo javnosti tudi preko drugih, ne samo nadzornih mehanizmov. Demistifikacija obveščevalne dejavnosti in obveščevalnih služb je proces, ki je v stalni interakciji z družbenimi spremembami in širšim varnostnim okoljem. Po drugi strani pa demistifikacija vnaša družbene spremembe, tako glede razumevanja vloge obveščevalnih služb s strani družbe kot tudi dojemanja njihove kulture tajnosti in končno tudi neko kritično in objektivno presojo družbe, torej legitimnost. Zato bi demistifikacija morala tem službam predstavljati še

dodaten motiv. Z možnostjo svojega postopnega odpiranja javnosti namreč te službe lahko utemeljujejo svoje profesionalno in etično ravnanje v odnosu do družbe, uveljavljajo transparentnost delovanja, upravičijo svoj namen, obstoj in vložena sredstva in si na neki način s tem utrjujejo (ali pa tudi ne) svojo nadaljnjo pot.

Menim, da sem s tem vse hipoteze v celoti potrdila.

8 LITERATURA

1. ANŽIČ, Andrej. 1996. *Vloga varnostnih služb v sodobnih parlamentarnih sistemih – nadzorstvo*. Ljubljana: ČZP Enotnost.
2. ANŽIČ, Andrej. 1997. *Varnostni sistem Republike Slovenije*. Ljubljana: Uradni list RS.
3. BABOS, Tibor. 2003. *Regulating the Intelligence System and Oversight in the Hungarian Constitutional Democracy.* Master of Arts. ZDA. Monterey: Naval Postgraduate Scool.
4. BARJAKTAREVIĆ, Zoran. 2006. *Dolgoročno in srednjeročno finančno načrtovanje v obrambnem sistemu RS.* Diplomsko delo. Ljubljana: Fakulteta za družbene vede.
5. BELŠAK, Ciril. 2010. Intervju z bivšim dolgoletnim načelnikom prvih zmogljivosti SIGINT na obrambnem področju. Ljubljana, 19. marec.
6. BORN, Hans, uredil; et al. 2003. *Parlamentarni nadzor nad varnostnim sektorjem: načela, mehanizmi in praksa.* Ženeva in Ljubljana: Interparlamentarna unija, Ženevski center za demokratični nadzor nad oboroženimi silami in Državni zbor Republike Slovenije.
7. BRITOVŠEK, Jaroš. 2008. *Možnosti proučevanja obveščevalne dejavnosti*. Članek: Dnevi varstvoslovja 2008.
8. CAVELTY DUNN, Myriam. 2008. *Cyber-Security and Threat Politics. US efforts to secure the information age.* Zurich: Center for Security Studies (CSS).
9. ČRNČEC, Damir. 2009. *Obveščevalna dejavnost v informacijski dobi*. Ljubljana: Defensor d.o.o.
10. ČRNČEC, Damir. 2010. Intervju z generalnim direktorjem Obveščevalno-varnostne službe Ministrstva za obrambo. Maribor, 21. april.
11. DCAF. 2006 a. *Intelligence Services.* DCAF Backgrounder 03/2006. Ženeva: Center za demokratični nadzor nad oboroženimi silami.
12. DCAF. 2006 b. *Parliamentary Oversight of Intelligence Services.* DCAF Backgrounder 03/2006. Ženeva: Center za demokratični nadzor nad oboroženimi silami.
13. DEPARTMENT of DEFENCE. 2004. *Report of the Defense Science Board Task Force on strategic Comunications.* ZDA: Washington.
14. Državni zbor Republike Slovenije. Komisija Državnega zbora Republike Slovenije za nadzor nad delom varnostnih in obveščevalnih služb. 2002. *Mnenje Komisije*

Državnega zbora Republike Slovenije za nadzor nad delom varnostnih in obveščevalnih služb. Številka: 200-01/90-3/50 EPA 439-III, 1. marec.

15. EDMONDS, Martin. 1988. *Armed Services and Society.* United Kingdom: Leicester University Press.
16. *Evropska konvencija o varstvu človekovih pravic in temeljnih svoboščin*. Uradni list RS 33/1994. Dostopno prek: www.mp.gov.si (12. januar 2010).
17. *Federal Ministry of Defence. White Paper 2006 on German Security Policy and the Future of the Bundeswehr.* Dostopno prek: www.bundestag.de (27. januar 2010).
18. GARB, Gregor. 2007. *Oblike tajnega delovanja obveščevalnih in varnostnih služb Republike Slovenije.* Magistrsko delo. Ljubljana: Fakulteta za družbene vede.
19. GEDER, Alan. 2010. Intervju s poveljnikom sil Slovenske vojske. Ljubljana, 19. april.
20. Generalštab Slovenske vojske (GŠSV). 2005. *Skupna obveščevalna, protiobveščevalna in varnostna doktrina (AJP-2.0) (SVS 2190)*. Ljubljana: Ministrstvo za obrambo.
21. GRIZOLD, Anton, TATALOVIĆ Siniša in CVRTILA Vlatko. 2008. *Suvremene sigurnostne politike: države i nacionalna sigurnost početkom 21. stoljeća.* Zagreb: Golden marketing-Tehnička knjiga.
22. GRIZOLD, Anton. 1999. *Obrambni sistem Republike Slovenije.* Ljubljana: Visoka policijsko-varnostna šola.
23. JELUŠIČ, Ljubica. 1997. *Legitimnost sodobnega vojaštva.* Ljubljana: Fakulteta za družbene vede.
24. LAINO, Karen A. 2010. Intervju z visoko predstavnico za obveščevalno dejavnost iz Mednarodnega vojaškega štaba v NATU. Maribor, 23. marec 2010.
25. LIBICKI, Martin C. in JOHNSON, Stuart E. 1996. *Dominant Battlespace Knowledge.* ZDA: Washington DC. National Defence University.
26. LOWENTHAL, Mark M. 2009. *Intelligence. From Secrets to Policy.* ZDA. Washington DC: A Division of SAGE. CQ Press.
27. MALEŠIČ, Marjan (ur.). 2006. *Varnost v postmoderni družbi.* Ljubljana: Fakulteta za družbene vede.
28. NATO Office of Information and Press. 2001 in 2006. *NATO Handbook.* Brussels. Belgium: Public Diplomacy Division.
29. *Odlok o Svetu za nacionalno varnost.* Uradni list RS 111/08. Dostopno prek: www.mp.gov.si (2. oktober 2009).

30. Poveljstvo za doktrino, razvoj, izobraževanje in usposabljanje (PDRIU). 2006. *Vojaška doktrina.* Ljubljana: Defensor d.o.o.
31. *Predlog Zakona o spremembah in dopolnitvah Zakona o Slovenski obveščevalno-varnostni agenciji*. Dostopno prek: www.mp.gov.si/fileadmin/mp.gov.si/pageuploads/2005/PDF/090504 (4. julij 2009).
32. PREZELJ, Iztok. 2000. *Varnost sodobne družbe kot večdimenzionalni pojav (oblikovanje metodološkega modela preučevanja ogrožanja varnosti).* Magistrska naloga. Ljubljana: Fakulteta za družbene vede.
33. PREZELJ, Iztok. 2001. Grožnja varnosti, varnostna tveganja in izzivi v sodobni družbi. *Teorija in praksa.* 38. 1./2001. Ljubljana: Fakulteta za družbene vede.
34. PURG, Adam. 2002. *Primerjalni obveščevalni sistemi.* Ljubljana: Visoka policijsko-varnostna šola.
35. PURG, Adam. 1995. *Obveščevalne službe*. Ljubljana: ČZP Enotnost.
36. *Resolucija o strategiji nacionalne varnosti Republike Slovenije (ReSNV).* Uradni list RS 56/2001. Dostopno prek: www.mp.gov.si (2. oktober 2009).
37. *Resolucija o strategiji nacionalne varnosti Republike Slovenije (ReSNV-1).* Uradni list RS 27/2010 (26. marec 2010).
38. RIEGER, Thomas. 1986. *Die Bundesnachrichtendienst in demokratischen Rechtsstaat*. Ellwangen: Roswitha Wimmer Verlag.
39. RITCHEY, Tom. 2005. *Wicked Problems. Structuring Social Messes with Morphological Analysis. Adapted from a lecture given at the Royal Institute of technology in Stockholm, 2004.* Dostopno prek: www.swemorph.com (10. maj 2010).
40. RITCHEY, Tom. 2008. *General Morphological analysis. A general method for non-quantified modelling.* Dostopno prek: www.swemorph.com (10. maj 2010).
41. SCHMID, Gerhard. 2001. *BERICHT über die Existenz eines globalen Abhörsystems für private und wirtschaftliche Kommunikation (Abhörsystem ECHELON) (2001/2098 (INI)*. Poročilo Evropskega parlamenta z dne 11. julija 2001.
42. SCHREIER, Fred. 2009. *Fighting the Pre-eminent Threats with Intelligence-led operations.* Ženeva: Center za demokratični nadzor nad oboroženimi silami (DCAF).
43. SCOTT, Len V. in JACKSON, Peter. 2004. *Understanding Intelligence in the Twenty-First Century. Journeys in Shadows.* London in New York: Routledge.
44. SCOTT, Len in HUGHES, Gerald R. 2006. Intelligence, Crises and Security: Lessons from History?. *Intelligence and National security.* Vol. 21. No. 5. 2006.

45. SCOTT, Len in HUGHES, Gerald R. 2009. *Intelligence in the Twenty-First Century: Change and Continuity or Crisis and Transformation? Change Crisis and Transformation: Challenges for Western intelligence in the Twenty-First Century. Intelligence and National security.*Vol. 24: No. 1. Februar 2009.
46. SHULSKY, Abram N. in SCHMITT, Gary J. 2002. *Silent Warfare: Understanding the World of Intelligence*. Third Edition. ZDA. Washington, DC: Potomac Books, Inc.
47. *Srednjeročni obrambni program 2007-2012 (SOPr 2007-2012).*Vlada RS, Številka: 803-2/2006-58. Dostopno prek: www.mors.si (2. april 2010).
48. SVETE, Uroš. 2005. *Varnost v informacijski družbi.* Ljubljana: Fakulteta za družbene vede.
49. ŠAPONJA, Vladimir. 1999. *Taktika dela obveščevalnovarnostnih služb.* Ljubljana: Visoka policijsko-varnostna šola.
50. TWRDY, Elen, Marko PETERLIN, Tadej ŽAUCER in Peter JENEÉK. 2007. *Zasnova prostorskega razvoja ob V. koridorju v povezavi z razvojem prometnih povezav med Slovenijo in Italijo.* Končno poročilo. Portorož: Fakulteta za pomorstvo in promet.
51. *Uredba o obveščevalno varnostni službi Ministrstva za obrambo.* Uradni list RS 63/99. Dostopno prek: www.mors.si (16. avgust 2009).
52. *Uredba o sodelovanju telekomunikacijskih organizacij z obveščevalno strukturo za potrebe zbiranja tajnih informacij in podatkov (Uredba št. 180/2004).* Dostopno prek: www.nbh.hu (30. januar 2010).
53. *Ustava Republike Madžarske (Listina št. XX/1949, A Magyar Köztársaság Alkotmánya)*. Dostopno prek: www.kfh.hu (28. januar 2010).
54. *Ustava Republike Slovenije.* Uradni list RS 33/91. Dostopno prek: www.mp.gov.si (2. oktober 2009).
55. *Ustava Zvezne republike Nemčije (Grungesetz GG, 23. Mai 1949 (BGBl. S. 1), 29. Juli 2009 (BGBl. I S. 2248)).* Dostopno prek: www.bundestag.de (27. januar 2010).
56. *Zakon o kazenskem postopku (ZKP).* Uradni list RS 32/2007 - UPB4. Dostopno prek: www.mp.gov.si (2. oktober 2009).
57. *Zakon o krepitvi varnosti informacijske tehnologije (Gesetz zur Stärkung der Sicherheit in der Informationstechnik des Bundes).*Dostopno prek: www.bsi.bund.de (27. januar 2010).
58. *Zakon o nacionalnih varnostnih službah (Zakon št. CXXV 1995).* Dostopno prek: www.faculty.maxwell.syr.edu (29. januar 2010).

59. *Zakon o obrambi (ZOBr).* Uradni list RS 103/04 – UPB1. Dostopno prek: www.mp.gov.si (2. oktober 2009).
60. *Zakon o parlamentarnem nadzoru obveščevalnih in varnostnih služb.* Uradni list RS 93/07. Dostopno prek: www.mp.gov.si (2. oktober 2009).
61. *Zakon o Policiji (ZPol).* Uradni list RS 107/2006 - UPB6. Dostopno prek: www.mp.gov.si (2. oktober 2009).
62. *Zakon o Slovenski obveščevalno-varnostni agenciji (ZSOVA).* Uradni list RS 81/2006 – UPB2. Dostopno prek: www.mp.gov.si (2. oktober 2009).
63. *Zakon o spremembah omejevanja tajnosti pisemsko-poštnih in komunikacijskih sporočil (Gesetz zur Neuregelung von Beschränkungen des Brief-Post und Fernmeldgeheimnisses).* Dostopno prek: www.bundestag.de (27. januar 2010).
64. *Zakon o Vojaški varnostni službi (Gesetz über den Militärischen Abschirmdienst (MAD-Gesetz – MADG).* Dostopno prek: www.mad.bundeswehr.de (27. januar 2010).
65. *Zakon o Zvezni obveščevalni službi (Gesetz über den Bundesnachrichtendienst.* Dostopno prek: www.bundestag.de (27. januar 2010).
66. *Zakon za omejevanje pisemske, poštne in telekomunikacijske zasebnosti (Zakon G-10) (Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses).* Dostopno prek: www.bundestag.de (27. januar 2010).
67. ŽABKAR, Anton. 2003. *Marsova dediščina 1. knjiga.* Ljubljana: Fakulteta za družbene vede.
68. ŽABKAR, Anton. 2004. *Marsova dediščina 2. knjiga.* Ljubljana: Fakulteta za družbene vede.

PRILOGA: Rezultati modeliranja s programskim orodjem DEXi

Drevo kriterijev

Kriterij	Opis
SIGINT na obrambnem področju	Ocena
├**Pravni okvir**	
├Zobr	
├ZSOVA	
└Vojaška doktrina	
├**Zagotavljanje virov**	
├Kadri	
├Finance	
├Tehnika	
└Infrastruktura	
├**Proaktivnost v obv. procesu**	
├Korak 2	
├Korak 3	
├Korak 4	
└Korak 5	
├**Težišče delovanja**	
├Nacionalna varnost	
└Mednarodne operacije in misije	
├**Strukturna odzivnost**	
├NVS	
└MORS	
└**Nadzor**	
├Parlamentarni	
├Resorni	
├Sodni	
└Javnost	

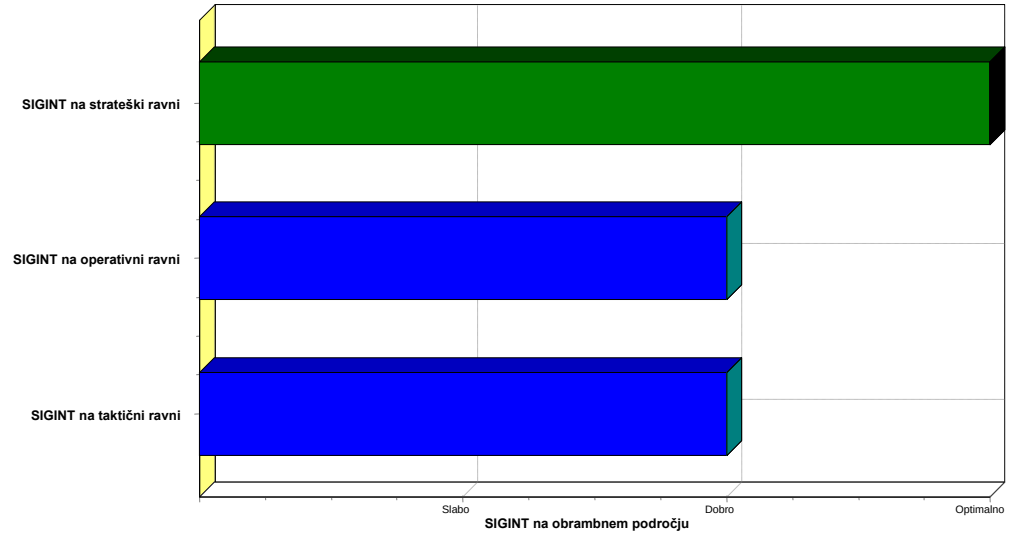
Zaloge vrednosti

Kriterij	Zaloga vrednosti
SIGINT na obrambnem področju	**Slabo**; Dobro; ***Optimalno***
├**Pravni okvir**	**Slabo**; Dobro; ***Optimalno***
├Zobr	**Slabo**; Dobro; ***Optimalno***
├ZSOVA	**Slabo**; Dobro; ***Optimalno***
└Vojaška doktrina	**Slabo**; Dobro; ***Optimalno***
├**Zagotavljanje virov**	**Slabo**; Dobro; ***Optimalno***
├Kadri	**Slabo**; Dobro; ***Optimalno***
├Finance	**Slabo**; Dobro; ***Optimalno***
├Tehnika	**Slabo**; Dobro; ***Optimalno***
└Infrastruktura	**Slabo**; Dobro; ***Optimalno***
├**Proaktivnost v obv. procesu**	**Slabo**; Dobro; ***Optimalno***
├Korak 2	**Slabo**; Dobro; ***Optimalno***
├Korak 3	**Slabo**; Dobro; ***Optimalno***
├Korak 4	**Slabo**; Dobro; ***Optimalno***
└Korak 5	**Slabo**; Dobro; ***Optimalno***
├**Težišče delovanja**	**Slabo**; Dobro; ***Optimalno***
├Nacionalna varnost	**Slabo**; Dobro; ***Optimalno***
└Mednarodne operacije in misije	**Slabo**; Dobro; ***Optimalno***
├**Strukturna odzivnost**	**Slabo**; Dobro; ***Optimalno***
├NVS	**Slabo**; Dobro; ***Optimalno***
└MORS	**Slabo**; Dobro; ***Optimalno***
└**Nadzor**	**Slabo**; Dobro; ***Optimalno***
├Parlamentarni	**Slabo**; Dobro; ***Optimalno***
├Resorni	**Slabo**; Dobro; ***Optimalno***
├Sodni	**Slabo**; Dobro; ***Optimalno***
└Javnost	**Slabo**; Dobro; ***Optimalno***

Rezultati vrednotenja

Kriterij	SIGINT na taktični ravni	SIGINT na operativni ravni	SIGINT na strateški
SIGINT na obrambnem področju	Dobro	Dobro	***Optimalno***
├**Pravni okvir**	***Optimalno***	Dobro	**Slabo**
│├Zobr	***Optimalno***	Dobro	**Slabo**
│├ZSOVA	**Slabo**	**Slabo**	***Optimalno***
│└Vojaška doktrina	***Optimalno***	***Optimalno***	**Slabo**
├**Zagotavljanje virov**	**Slabo**	Dobro	***Optimalno***
│├Kadri	Dobro	Dobro	***Optimalno***
│├Finance	**Slabo**	Dobro	***Optimalno***
│├Tehnika	**Slabo**	Dobro	***Optimalno***
│└Infrastruktura	***Optimalno***	***Optimalno***	Dobro
├**Proaktivnost v obv. procesu**	**Slabo**	Dobro	***Optimalno***
│├Korak 2	**Slabo**	Dobro	***Optimalno***
│├Korak 3	Dobro	***Optimalno***	Dobro
│├Korak 4	**Slabo**	**Slabo**	***Optimalno***
│└Korak 5	Dobro	Dobro	***Optimalno***
├**Težišče delovanja**	Dobro	Dobro	***Optimalno***
│├Nacionalna varnost	Dobro	Dobro	***Optimalno***
│└Mednarodne operacije in misije	Dobro	***Optimalno***	Dobro
├**Strukturna odzivnost**	**Slabo**	Dobro	***Optimalno***
│├NVS	**Slabo**	Dobro	***Optimalno***
│└MORS	Dobro	Dobro	***Optimalno***
└**Nadzor**	Dobro	Dobro	Dobro
├Parlamentarni	Dobro	Dobro	***Optimalno***
├Resorni	Dobro	***Optimalno***	Dobro
├Sodni	Dobro	Dobro	Dobro
└Javnost	**Slabo**	**Slabo**	Dobro

Grafikon


SIGINT na strateški ravni
SIGINT na operativni ravni
SIGINT na taktični ravni
Slabo
Dobro
Optimalno
SIGINT na obrambnem področju