

**UNIVERZA V LJUBLJANI
FAKULTETA ZA DRUŽBENE VEDE**

Miloš Kosić

**VLOGA IN POMEN OBVEŠČEVALNIH SLUŽB V BOJU ZOPER
MEDNARODNI TERORIZEM**

Diplomsko delo

Ljubljana, 2006

**UNIVERZA V LJUBLJANI
FAKULTETA ZA DRUŽBENE VEDE**

Miloš Kosić

Mentor: doc. dr. Iztok Prezelj

**VLOGA IN POMEN OBVEŠČEVALNIH SLUŽB V BOJU ZOPER
MEDNARODNI TERORIZEM**

Diplomsko delo

Ljubljana, 2006

ZAHVALA

Zahvaljujem se svojim staršema, za zaupanje, podporo in motivacijo v času mojega študija.

Posebna zahvala gre Polonci, za pomoč in vzpodbudo pri nastajanju mojega diplomskega dela ter vsem prijateljem za nepozabna študentska leta.

KAZALO

SEZNAM KRATIC	III
1 UVOD	1
2 METODOLOŠKI OKVIR	4
2.1 CILJI PREUČEVANJA	4
2.2 HIPOTEZE	4
2.3 UPORABLJENE METODE	5
3 OPREDELITEV TEMELJNIH POJMOV	6
3.1 TERORIZEM	6
3.2 MEDNARODNI TERORIZEM	10
3.3 BOJ PROTI TERORIZMU	11
3.4 OBVEŠČEVALNI CIKLUS	12
3.5 OBVEŠČEVALNA DEJAVNOST	17
3.6 OBVEŠČEVALNA SLUŽBA	19
3.7 NACIONALNOVARNOSTNI SISTEM	20
4 DEJAVNIKI MEDNARODNEGA TERORIZMA	22
4.1 ČLOVEŠKI DEJAVNIK	22
4.2 FINANČNI DEJAVNIK	23
4.3 MATERIALNI DEJAVNIK	26
4.4 KOMUNIKACIJSKI DEJAVNIK	29
4.5 IDEOLOŠKI DEJAVNIK	32
4.5.1 RACIONALNA MOTIVACIJA	32
4.5.2 PSIHOLOŠKA MOTIVACIJA	33
4.5.3 KULTURNA MOTIVACIJA	33
5 VPLIV TERORIZMA NA SPREMEMBE NACIONALNOVARNOSTNIH SISTEMOV	35
5.1 PRIMER ZDRUŽENIH DRŽAV AMERIKE	35
5.2 PRIMER VELIKE BRITANIJE	38
5.3 PRIMER RUSKE FEDERACIJE	42
5.3.1 OBDOBJE PRED NAPADI 11. SEPTEMBRA 2001	43
5.3.2 OBDOBJE MED 11. SEPTEMBROM 2001 IN ZAJETJEM TALCEV V MOSKOVSKEM GLEDALIŠČU (23. DO 26. OKTOBER 2002)	45

5.3.3	<i>OBDOBJE MED 26. OKTOBROM 2002 IN ZAJETJEM TALCEV V BESLANU (1. DO 3. SEPTEMBER 2004)</i>	45
5.3.4	<i>OBDOBJE PO 3. SEPTEMBRU 2004 DO DANES</i>	46
5.4	PRIMER IZRAELA	48
6	VLOGA OBVEŠČEVALNIH SLUŽB V BOJU PROTI MEDNARODNEMU TERORIZMU	53
6.1	PRIMER AMERIŠKE OBVEŠČEVALNE SLUŽBE CIA (Central Intelligence Agency).....	53
6.2	PRIMER BRITANSKE OBVEŠČEVALNE SLUŽBE SIS (Secret Intelligence Service).....	61
6.3	PRIMER RUSKE OBVEŠČEVALNE SLUŽBE SVR (Služba vnešnogo razvedki)	66
6.4	PRIMER IZRAELSKE OBVEŠČEVALNE SLUŽBE MOSSAD (ha-Mossad le-Modiin ule-Tafkidim Meyuhadim)	69
7	MEDNARODNO SODELOVANJE OBVEŠČEVALNIH SLUŽB V BOJU PROTI MEDNARODNEMU TERORIZMU	75
8	ZAKLJUČEK	79
9	LITERATURA	85

SEZNAM KRATIC

ACOUSTINT – Acoustical Intelligence (pridobivanje podatkov s pomočjo zvoka)
ATCSA – Anti-terrorism, crime and security act (Zakon o antiterorizmu, kriminalu in varnosti)
BND - Bundesnachrichtendienst (nemška obveščevalna agencija)
BR – Brigade Rosse (rdeča brigada)
CIA – Central Intelligence Agency (Osrednja obveščevalna agencija)
COMINT – Communications Intelligence (spremljanje komunikacijskih kanalov in naprav)
ELECTRO-OPTINT - Electro-optical intelligence (elektrooptično zbiranje podatkov)
ELINT – Electronic Intelligence (spremljanje drugih elektronskih naprav)
EU – Evropska Unija
FAPSI – Federalnoje agencstvo praviteljstvennoj svjazi i informacii (Zvezna agencija vladnih zvez in informacij)
FBI – Federal Bureau of Investigation (Zvezni preiskovalni organ)
FSB – Federalnaya služba bezopasnosti (Zvezna varnostna služba)
GCHQ – Government communications headquarters (vladni štab za komunikacije)
GIA – Groupe Islamique Armé (oborožena islamska skupina)
GSPC – Groupe Salafiste pour la Prédication et le Combat (Salafistična skupina z pridigo in boj)
HUMINT – Human Intelligence (zbiranje podatkov s pomočjo človeških virov)
IDF – Israel defence force (Izraelske obrambne sile)
IMINT – Imagery Intelligence (zbiranje podatkov, ki so v obliki podob)
IRC – Internet Relay Chat (pogovor s pomočjo medmrežja)
IRA – Irish Republican Army (Irska republikanska armada)
JTAC – Joint terrorism analysis centre (skupni analitični center za terorizem)
KGB – Komitet Gosudarstvennoy Bezopasnosti (Komite za državno varnost)
LASINT – Laser Intelligence (pridobivanje podatkov s pomočjo laserjev)
MC&G – mapping, charting and geodesy intelligence (izdelava zemljevidov in zbiranje geodetskih podatkov)
MI5 – Military Intelligence 5 (vojaška obveščevalna služba 5)
MI6 – Military Intelligence 6 (vojaška obveščevalna služba 6)
MIT - Millî İstihbarat Teşkilâtı (Turška obveščevalna organizacija)

NaCTSO – National counter terrorism and security office (Pisarna za nacionalno protiteroristično dejavnost in varnost)

NATO – North Atlantic Treaty Organisation (Organizacija Severnoatlantske pogodbe)

NIAA – Nationality, immigration and asylum act (Zakon o državljanstvu, imigracijah in azilu)

NIEPA – Northern Ireland Emergency Provisions Act (Zakon o Severni Irski)

NUCINT – Nuclear Intelligence (spremljanje radioaktivnega sevanja)

OSINT – Open source intelligence (zbiranje javno dostopnih podatkov)

OVSE – Organizacija za varnost in sodelovanje v Evropi

OZN – Organizacija združenih narodov

PHOTINT – Photographic Intelligence (fotografsko zbiranje podatkov)

PICTU – Police international counter terrorist unit (policijska mednarodna protiteroristična enota)

PIRA – Provisional Irish Republican Army (provincijska irska republikanska armada)

PLO – Palestine Liberation Organization (palestinska osvobodilna organizacija)

PTA – Prevention of Terrorism Act (Zakon o preprečevanju terorizma)

RADINT – Radar Intelligence (pridobivanje podatkov s pomočjo radarjev)

RAF – Rote Armee Fraktion (frakcije rdeče armade)

RF – Ruska federacija

RINT – Radiation Intelligence (spremljanje drugih virov sevanja)

SAS – Special air service (posebna zračna enota)

SBS – Special boat service (posebna pomorska enota)

SIGINT – Signal Intelligence (zbiranje podatkov, ki obstajajo v obliki signalov)

SIS – Secret Intelligence Service (Tajna obveščevalna služba)

SND – Skupnost neodvisnih držav

SVR – Služba vnešnega razvedke (Zunanja obveščevalna služba)

SZ – Sovjetska Zveza

TECHINT – Technical Intelligence (zbiranje podatkov s pomočjo tehničnih sredstev)

TELINT – Telemetry Intelligence (spremljanje telemetrijskih aktivnosti)

USA – United States of America (Združene države Amerike)

VB – Velika Britanija

WTC – World Trade Center (Svetovni trgovinski center)

ZDA – Združene države Amerike

1 UVOD

Po koncu hladne vojne se razmere v mednarodni skupnosti radikalno spremenijo. Države kot temeljni subjekti mednarodnega prava niso več glavni vir ogrožanja druga drugi. Razpad vzhodnega političnega bloka pripelje do stanja unipolarnosti na političnem in vojaškem področju. V svetu vse bolj prihaja do številnih etničnih, socialnih, ideoloških, religioznih in drugih razlikovanj ter sporov, od katerih številni prerastejo območje lokalnega vpliva in začenjajo ogrožati nacionalno in tudi mednarodno varnost. Ti spori se lahko manifestirajo v obliki mednarodnega terorizma, ki ogroža obstoj mednarodnega sistema varnosti kot celoto in prav tako vsak subjekt znotraj tega sistema. Mednarodni terorizem je bil tako prepoznan kot strateška nevarnost za obstoj in razvoj držav in je kot tak nadomestil oborožen spopad večjih razsežnosti, ki je lebdel v zraku v času hladne vojne.

V tem času, ko oborožene sile ne igrajo več glavne vloge pri zagotavljanju nacionalne varnosti, so na njihovo mesto prišle obveščevalne službe, tako civilne kot vojaške. Njihova vloga je predvsem pomembna zaradi specifičnosti delovanja mednarodnega terorizma, ki temelji na tajnosti, visoki mobilnosti, izurjenosti in drugem. Tako pridejo do izraza metode obveščevalnih služb, katerih glavni nalogi sta zgodnje odkrivanje dejavnikov terorizma in preprečevanje terorističnih dejanj (Podbregar 2004: 30).

Vendar se vpliv in vloga obveščevalnih služb kažeta predvsem v luči celotnega nacionalnovarnostnega sistema. Iz tega razloga je potrebno razumeti dinamiko spreminjanja sistema nacionalne varnosti, predvsem z vidika pojava mednarodnega terorizma. Tako je treba vedeti, da samo tisti nacionalnovarnostni sistem posamezne države, ki je fleksibilen in dovzeten za dogajanje v mednarodnem okolju, lahko omogoči preživetje in trajnostni razvoj države. Vendar nikjer ne obstaja univerzalna enačba, kako organizirati sistem nacionalne varnosti, da bo lahko učinkovito odvrčal nevarnosti, ki jih predstavljajo sodobni viri ogrožanja. Prav tako je nerealno pričakovati, da bodo te grožnje delovale vselej po enakih vzorcih in da se ne bodo prilagodile uveljavljenim varnostnim ukrepom. Zato je danes mednarodno varnostno okolje prežeto z negotovostjo, nezaupljivostjo in posledično z željo akterjev v

mednarodni skupnosti po popolnem nadzoru družbe. Tako lahko že v uvodu ugotovim, da je teroristom do določene mere uspelo, saj so vgradili občutek strahu v slehernega posameznika.

Ker se danes v javnosti vse bolj govori o nevarnostih terorizma in o tem, kako najbolje preprečiti to nevarnost, sem se v diplomskem delu podrobneje lotil ravno te tematike. Zanima me predvsem, kako se posamezne države spopadajo s pojavom terorizma in kakšne ukrepe so pripravljene sprejeti za preprečevanje le-tega. Tako bom analiziral celoten nacionalnovarnostni sistem posameznih držav in znotraj njega še posebej vlogo obveščevalnih služb, saj pogosto slišimo, da ravno obveščevalne službe oblikujejo »prvo bojno črto« v spopadu z mednarodnim terorizmom.

Kot sem že omenil, ni univerzalnega recepta za boj proti terorizmu, zato sem v svojem diplomskem delu izhajal iz študij primerov štirih držav, in sicer Združenih držav Amerike, Velike Britanije, Ruske federacije in Izraela, ki so zaradi svojega položaja v mednarodni skupnosti nekako najbolj izpostavljene terorističnim napadom in v svojih nacionalnovarnostnih sistemih posvečajo največ pozornosti boju proti mednarodnemu terorizmu.

V prvem poglavju se bom lotil opredeljevanja posameznih pojmov, ki so neposredno povezani z nadaljnjim proučevanjem in analiziranjem problematike. Opredelil bom pojme, ki se navezujejo na pojav mednarodnega terorizma. Tako bom skušal analizirati pojme terorizem, mednarodni terorizem in boj proti terorizmu. Nadalje bom razložil pojme, ki se navezujejo na delovanje obveščevalnih služb. Ti so obveščevalni cikel, obveščevalna dejavnost in obveščevalna služba. Opredelil bom tudi nacionalnovarnostni sistem, ki predstavlja sistemski okvir boja proti terorizmu.

Drugo poglavje bo namenjeno pojavu mednarodnega terorizma in njegovim značilnostim. Opredelil in analiziral bom temeljne dejavnike, ki morajo biti prisotni, da lahko govorimo o delujoči teroristični organizaciji. Ti dejavniki so človeški, materialni, finančni, komunikacijski in ideološki. Z njihovo pomočjo bom prikazal kompleksnost pojava terorizma, sposobnost hitrega prilagajanja spremenljivim razmeram in tiste kritične točke, na katerih poskušajo delovati obveščevalne službe in drugi elementi nacionalnovarnostnega sistema.

V naslednjem poglavju bom s študijo primerov nacionalnovarnostnih sistemov štirih držav, skušal prikazati, kako pojav terorizma vpliva na spremembe sistema nacionalne varnosti in kakšne so posledice teh sprememb. V posameznih primerih se bom osredotočil na identifikacijo vseh akterjev, ki izvajajo boj proti terorizmu, in na njihovo vlogo. Posvetil se bom potekanju koordinacije protiterorističnih aktivnosti in njihovemu dojemu ter ukrepanju zoper nevarnost terorizma v nacionalno strateških in pravnih aktih.

Tretje poglavje bo namenjeno analizi štirih najmočnejših obveščevalnih služb (CIA, SIS, SVR in Mossad) prej omenjenih držav. Zanimalo me bo predvsem spreminjanje glavne naloge posamezne obveščevalne službe, in sicer od konca hladne vojne pa vse do danes. Ugotavljal bom, kakšno vlogo imajo te službe, glede na protiteroristično delovanje in kako poteka razmejitev delovnih pristojnosti s sorodnimi službami znotraj nacionalnovarnostnega sistema. Prav tako bom poskušal identificirati posamezne metode dela obveščevalnih služb, vendar domnevam, da mi zaradi narave dela teh služb ne bo na voljo dovolj relevantnih virov.

Zaradi mednarodnega delovanja terorizma sta vsak nacionalnovarnostni sistem in znotraj njega obveščevalna služba zelo omejena v smislu ustreznega protiterorističnega delovanja. Zato mednarodno sodelovanje med obveščevalnimi službami predstavlja vse pomembnejši vidik boja proti terorizmu. Tej tematiki se bom posvetil v četrtem poglavju. Identificiral bom interese posameznih služb za mednarodno sodelovanje in osvetlil sistem sodelovanja glede na vsebino in obliko.

Zaključek bo posvečen primerjalni analizi obravnavanih nacionalnovarnostnih sistemov in obveščevalnih služb. Tako bom na podlagi primerjalnih analiz vsebinsko ovrednotil postavljene hipoteze in predstavil svoje kritično razmišljanje o obravnavani tematiki.

2 METODOLOŠKI OKVIR

2.1 CILJI PREUČEVANJA

Predmet preučevanja sem opredelil v uvodu, njegovi konkretni cilji pa so:

- ugotovitev in analiza temeljnih dejavnikov mednarodnega terorizma,
- analiza boja proti terorizmu v štirih državah, na nivoju nacionalnovarnostnih sistemov in primerjalna analiza posameznih komponent boja,
- analiza vloge obveščevalnih služb v boju proti mednarodnemu terorizmu v nacionalnem in mednarodnem okviru.

2.2 HIPOTEZE

Glavna hipoteza je:

S pridobivanjem pravočasnih in uporabnih informacij o nameri in delovanju terorističnih organizacij in/ali teroristov posameznikov, so obveščevalne službe najpomembnejši akter nacionalnovarnostnega sistema v uspešnem boju proti mednarodnemu terorizmu.

Delovne hipoteze:

1. Teroristični napadi 11. septembra 2001 so prisilili države, da so prilagodile svoje nacionalnovarnostne sisteme sodobnim virom ogrožanja, še posebej pojavu mednarodnega terorizma.
2. Obveščevalne službe v boju proti terorizmu posvečajo vedno večjo pozornost zbiranju obveščevalnih podatkov s pomočjo človeških virov (HUMINT).
3. Sodelovanje in izmenjava informacij med obveščevalnimi službami omogočata večjo uspešnost boja zoper mednarodni terorizem.

2.3 UPORABLJENE METODE

Temeljna metoda, ki jo uporabljam v diplomski nalogi, je analiza primarnih in sekundarnih virov. S pomočjo primarnih virov bom predstavil konceptualno izhodišče boja proti terorizmu, zapisano v nacionalnih zakonodajah in dokumentih s področja nacionalne varnosti, in sicer za vsako državo posebej. Prav tako bom primarne vire uporabil za analizo delovanja obveščevalnih služb. Nadalje bom z interpretacijo sekundarnih virov predstavil dejavnike terorizma, dinamiko spreminjanja nacionalnovarnostnih sistemov in praktični vidik delovanja ter mednarodnega sodelovanja obveščevalnih služb.

Pri analiziranju posamezne države bom uporabil študije primerov. Na njihovi podlagi pa bom primerjal nacionalnovarnostne sisteme in obveščevalne službe, kjer bom uporabil primerjalno analizo.

3 OPREDELITEV TEMELJNIH POJMOV

3.1 TERORIZEM

Pojem terorizma se v sodobnem političnem besednjaku pojavlja vse od obdobja jakobinske diktature v letih od 1794 do 1796, ko so jakobinci branili revolucijo s fizičnim in psihološkim nasiljem nad množicami (Stopar 2002: 1).

Danes se soočamo s težavo definiranja terorizma, saj večina razlag predstavlja odziv na določene teroristične aktivnosti, vendar so te preveč politično in ideološko opredeljene, da bi lahko predstavljale univerzalno opredelitev terorizma. Tovrstno dilemo opredeli Chomsky (Chomsky v Keet 2003: 6) s trditvijo, da sta za opredelitev terorizma možni dve poti, in sicer dobesedna oziroma znanstvena, ki se naj bi lotila resne raziskave tematike, in propagandna, katere namen je oblikovati takšno pojmovanje terorizma, ki ga lahko določeni sistemi oblasti izkoristijo v svoj prid. Za dodatno težavo pri definiranju terorizma pa poskrbi pogosto citirana misel, da je terorist za nekoga, lahko borec za svobodo za nekoga drugega. Ta misel skriva različne in pogosto nasprotujoče si poglede na politične, družbene, ekonomske, religijske in druge vidike, ki dajejo terorističnim organizacijam motiv, cilj in sredstva za svoje delovanje.

Za razumevanje, kako obsežen in kompleksen je problem postavitve enotne definicije, nam pove raziskava, ki jo leta 1984 izvedel Schmid. Uspel je identificirati 101 definicijo terorizma; vsebovale so 22 različnih dejavnikov, značilnih za terorizem, vendar se niti eden ni pojavil v vseh definicijah (Piper v Keet 2003: 5).

Na problem neenotne definicije naletimo že znotraj ideološko homogenega mednarodnega subjekta, kot je država. Primer so ZDA, kjer imajo razni vladni organi in agencije različne poglede na terorizem. Tako je vlada ZDA oblikovala naslednjo definicijo: »Terorizem je naklepno, politično motivirano nasilje, storjeno nad civilnimi in neoboroženimi tarčami s strani etničnih skupin ali tajnih agentov, v večini primerov namenjeno vplivanju na širšo javnost. Terorizem je tudi dejanje napada na vojaške baze in oboroženo osebje, če tam, kjer se je to zgodilo, ni vojaških spopadov.

Teroristično dejanje postane mednarodni terorizem tedaj, če je vanj vpletena več kot ena država ali pa več državljanov različnih držav« (Malvesti v Anžič 2002: 461-462). Ta definicija, čeprav je precej obsežna, vsebuje nekaj pomanjkljivosti. Preozko namreč določa možne izvajalce terorističnih dejanj, saj jih zožuje na pripadnike drugih etničnih skupin in na države, izvajalke terorizma. S tem izključuje široko paleto motivov, ki temeljijo na političnih, socialnih, svetovnonazorskih in drugih pogledih. Prav tako je problematičen drugi del definicije, ki govori o vojaškem osebju, saj kot terorizem opredeli vsakršni napad na vojaške enote pred dejanskim vojaškim spopadom in s tem odvzame legitimnost tudi odporiškim gibanjem.

Druga definicija znotraj ZDA prihaja z ministrstva za obrambo in se glasi: »Terorizem je preračunana uporaba nasilja ali grožnja z nasiljem z namenom, da bi prisilili oziroma ustražovali vlade ali družbe, da zasledujejo določene cilje, ki so ponavadi politični, verski ali ideološki« (U.S.Army, Field Manual 100-20, Stability and Support operations). Ta definicija sicer ne omejuje izvajalcev, vendar tudi ne razlikuje med neposrednimi žrtvami terorističnega napada in dejansko ciljno skupino, kateri je namenjeno sporočilo napada. Tako ne pride do izraza nekoliko večja oddaljenost med dejanjem in ciljem terorizma, ki zaradi svoje narave posrednega delovanja potrebuje vmesni medij, ki ga predstavljajo neposredne žrtve napada (Fromkin v Keet 2003: 8).

Za svojo definicijo pa se je odločil FBI, ki je terorizem opredelil kot »nelegalno uporabo nasilja ali grožnjo z uporabo nasilja proti osebam in njihovemu imetju za dosego političnih ali družbenih ciljev. Uporablja se za ustraževanje oziroma prisiljevanje vlade, civilne družbe ali kateregakoli njenega dela z določenimi političnimi ali družbenimi cilji« (FBI policy and guidelines, http://www.fbi.gov/publications/terror/terror2000_2001.htm). Ta definicija odreja legitimnost vsakršni obliki upora proti državi in ne dopušča ločitve terorizma od uporniških gibanj.

Na še večja nesoglasja v poskusu definiranja terorizma pa naletimo na nadnacionalni ravni, kjer se vrstijo dokumenti, ki poskušajo opredeliti terorizem, vendar brez splošnega konsenza. Ena tovrstnih deklaracij je Ženevska deklaracija o terorizmu (1987), ki posredno opredeljuje vzroke terorizma in razmejuje teroristična dejanja od

pojma »pravične« vojne (Purg 1997: 35). Za nekoliko večji uspeh lahko štejemo definicijo terorizma v Evropski uniji, saj se države članice zavedajo, da politična motivacija napadov ruši temeljne demokratične vrednote evropske povezave. Iz tega sledi opredelitev »terorističnih dejanj kot tistih, ki jih posameznik ali skupina stori proti eni ali več državam, njihovim ljudem ali institucijam z namenom, da ogrozijo ali uničijo njihove politične, socialne ali gospodarske strukture« (Anžič 2002: 460).

Ob analiziranju definicij terorizma sem ugotovil, da se opredelitve pojma velikokrat ne ujemajo, vendar jih večina zaznava posamezne elemente, ki so prisotni v pojmu terorizma. Ti elementi pa so izvajalec terorizma, uporabljena metoda, neposredne žrtve napada, dejanska ciljna skupina in politična motivacija za napad.

Pri opredelitvi izvajalca terorizma je pomembno, da se ne izloči nobenega izmed možnih subjektov (posameznik, skupina, organizacija in država), čeprav veliko definicij ne identificira izvajalca, kot na primer opredelitev Ganorja, »da je terorizem namerna uporaba ali grožnja z uporabo nasilja proti civilistom ali civilnim tarčam, da se dosežejo politični cilji« (Ganor 1998).

Še najmanj težav je pri uporabljenih metodah, saj praktično vse definicije kot uporabljene metode navajajo fizično in psihološko nasilje, katerega del so tudi grožnje z nasiljem. Pomanjkljivost, ki sem jo zasledil pri tem pojmovanju, je neopredelitev do t. i. »cyber« napadov, ki jih ne moremo uvrščati ne med fizične in ne med psihološke napade.

Veliko problemov nastane pri označevanju neposrednih žrtev napada, saj jih definicije opredeljujejo kot civiliste, nedolžne žrtve, nebojevnike itd. Vsekakor sem spadajo tudi objekti, ki so tarče predvsem zaradi svojega simbolnega pomena (primer je napad na WTC v New Yorku). Pomembno je, da so neposredne žrtve napada samo nosilci sporočila in ne dejanski smisel celotne akcije. Temu primerna je tudi izbira neposrednih žrtev, ki pa je zaradi določene navezave na dejansko ciljno skupino vendarle samo delno naključna. Posredna vloga žrtev je bistvenega pomena pri razmejitvi pojma terorizma od podobnih pojmov, kot so uporniška gibanja in gverila, še posebej urbana gverila, ki uporablja podobne taktike delovanja kot

teroristične skupine, vendar so zanjo neposredne žrtve napada tudi dejanski nosilci in izvrševalci politične moči (Ganor 1998).

V primeru opredelitve dejanske ciljne skupine terorističnega delovanja pa so definicije terorizma precej enotne in kot ciljne skupine navajajo države, državne organe, politična gibanja in celotno družbo oziroma njene dele.

Zadnji element opredelitve terorizma je politična motivacija za napad, ki razlikuje terorizem od kriminalnih združb, ki izvajajo nasilje z namenom, da bi se ekonomsko okoristile. V tem primeru je političnost mišljena v širšem smislu, ki obsega vse možne motive in za svoje uresničenje potrebuje spremembo dosedanjih procesov odločanja.

Za določitev ustrezne definicije terorizma bom uporabil metodo posrednega delovanja, ki jo uporablja v svoji sicer relativno široko opredeljeni definiciji Keetova (2003: 10), ki definira terorizem kot »uporabo fizičnega in psihološkega nasilja kot sredstvo za doseg političnega cilja«.

Primerna definicija, ki vsebuje vse našteje elemente pojma terorizma, je definicija Richardsonove (2000: 209), ki trdi, da je »terorizem politično motivirano nasilje, usmerjeno proti civilistom ali simbolnim tarčam, ki je načrtovano s tem namenom, da prenese sporočilo širšemu občinstvu. Bistvena značilnost terorizma je načrtno napadanje nedolžnih, da bi prenesli sporočilo tretji strani. In to je bistvena razlika, ki ga loči od najbolj sorodne oblike političnega nasilja, in sicer od gverilskega vojskovanja«.

Tako sem s pomočjo že sprejetih definicij terorizma in označitvijo prisotnih elementov oblikoval svojo opredelitev, ki terorizem opisuje kot metodo, s katero izvajalec terorizma (posameznik, skupina, država) s pomočjo nasilja in grožnjami z nasiljem nad osebami in objekti, ki niso neposredno vpleteni v procese političnega odločanja, po komunikacijskih kanalih ustrahuje organe političnega odločanja in družbo ter jih prisiljuje v oblikovanje takšne politike, ki je v prid izvajalcem terorizma.

3.2 MEDNARODNI TERORIZEM

Mednarodni terorizem je ena izmed oblik terorizma, ki zaradi svojega vpliva na celotno mednarodno skupnost in dejstva, da ne pozna nacionalnih meja, pritegne tudi največ pozornosti. Prav tako kot pri opredelitvi pojma terorizem zasledimo tudi pri pojmu mednarodni terorizem različne možne razlage in poglede nanj.

Tako pod pojmom mednarodni terorizem Purg (1997: 33) razume grožnje z uporabo sile ali dejansko uporabo fizičnega nasilja, ki presega meje ene države in ki ga izvajajo nedežavne organizacije, skupine ali posamezniki, da bi dosegli določene politične cilje, tako na nacionalni kot mednarodni ravni.

Nadalje Halilović ugotavlja, da se kompleksnost internacionalizacije terorizma ne kaže samo v delovanju posameznih terorističnih skupin izven njihovega običajnega območja, ampak v vseh fazah priprave, izvedbe in posledic terorističnega napada (Halilović 2004: 158). Podobno razmišlja tudi Dimitrijević, ki med vrstami terorizma kot posebno kategorijo navaja mednarodni terorizem, in sicer v primerih, ko imajo teroristična dejanja kakršnekoli elemente inozemskega (Krunić 1997: 161).

Vendar Dimitrijević ugotavlja, da je v mednarodnih odnosih možnih več zvrsti terorizma, in sicer transnacionalni terorizem, ki pomeni vse oblike terorizma v mednarodnih odnosih, katerih izvajalci so nedežavni subjekti. Druga zvrst je meddržavni terorizem, ki obsega vse tiste »teroristične postopke«, ki so opravljeni na osnovi sklepa nekega državnega organa, ali pa so celo neposredni izvajalci v državni službi (Purg 1997: 30-31). Tudi Farrell uporablja delitev na transnacionalni in mednarodni terorizem, ki pa povzema definicijo Cie, ki se glasi: »Mednarodni terorizem se navezuje na skupine ali posameznike, ki so pod pokroviteljstvom suverene države, medtem pa dejanja transnacionalnega terorizma izvajajo avtonomni nedežavni akterji (Martin 2005). Tukaj naletimo na problem prevajanja, saj se v definiciji Cie uporablja beseda »*international*«, ki jo prevajamo kot mednarodni, vendar je v tem primeru bolj ustrezen pojem meddržavni, »*ki je, poteka med državami*« (SSKJ 2000: 532); predstavlja vsa teroristična delovanja, ki se izvajajo s strani države oziroma njenih organov. Tako ta definicija sovpada z Dimitrijevićevo.

Za lažjo obravnavo in razumevanje bom kljub nadaljnji členitvi pojma mednarodni terorizem ostal pri osnovnem pojmu in teroristično dejanje opredelil kot mednarodni terorizem takrat, kadar vsaj eden izmed elementov terorizma, torej izvajalci terorizma, neposredne žrtve napada, dejanska ciljna skupina ali sami politični cilji napadalcev niso vezani na meje ene same države.

3.3 BOJ PROTI TERORIZMU

Purg (1997: 34) pod pojmom boj proti terorizmu razume konstruktiven odnos do problema, ki obsega široko paleto možnih odzivov na nasilje, in sicer od verbalnega obsojanja, kazenskopравnih elementov pa vse do organiziranja posebnih organizacij, specializiranih za boj proti terorizmu. Bolj jasne smernice boja proti terorizmu opredeli Anžič (2002: 465), ki protiteroristično delovanje razširi na strukturno raven, ki preko določenih dejavnosti, kot so diplomatska, politična, gospodarska, zdravstvena, znanstvena in druge dejavnosti, poskuša delovati v smeri odpravljanja vzrokov terorizma. Prav tako boj proti terorizmu omeji z že doseženimi standardi pri varovanju človekovih pravic, in nasprotuje dejstvu, da bi delovanje protiterorističnega boja nosilo verski, rasni ali kakšen drugi ideološki predznak.

Na podoben način tudi Črnčec opredeli tri ključna načela, ki jih je potrebno upoštevati v boju zoper terorizem. V prvi vrsti se je treba izogibati pretiravanju, zlasti v obdobju, ko je prisoten strah, prav tako se ne sme posegati na področje ustavno zagotovljenih pravic, kot so politična svoboda in enakost pred zakonom. Potrebno je tudi ohraniti ravnotežje med svobodo in varnostjo in predvsem zaščito manjšin, ki so lahko zaradi posameznih karakteristik označene kot teroristi in posledično izobčene. Tukaj Črnčec navaja predvsem ljudi arabskega oziroma muslimanskega porekla, vendar je potrebno zajeti tudi preostale skupine ljudi, ki so iz drugih razlogov opredeljene kot manjšina (Cole v Črnčec 2004: 63).

Precej bolj operativna razlaga pojma pa prihaja iz ZDA, kjer boj proti terorizmu vsebuje dve komponenti, in sicer antiterorizem ter protiterorizem¹. Antiterorizem predstavlja skupek pasivnih ukrepov, katerih namen je predvsem zmanjšati ranljivost pred morebitnimi terorističnimi napadi, protiterorizem pa obsega ofenzivne ukrepe, katerih namen je preprečiti, zastraševati in odgovoriti na pojav terorizma (Smith 2004).

Tako lahko na podlagi že obstoječih definicij razumem boj proti terorizmu kot celoto ukrepov, s katerimi se na operativni in sistemski ravni deluje v smeri odvratanja, preprečevanja in zmanjševanja ranljivosti pred terorizmom ter odpravljanja vzrokov zanj, seveda ob upoštevanju temeljnih človekovih pravic in svoboščin.

3.4 OBVEŠČEVALNI CIKLUS

Pojem obveščevalni cikel lahko opredelimo kot zaključeno celoto medsebojno povezanih stopenj oziroma procesov, ki predstavljajo temeljno delovanje vsake obveščevalne organizacije. Richelson definira obveščevalni cikel kot proces, v katerem se pridobivajo surove informacije, ki se nadalje analizirajo in pretvorijo v obveščevalne izdelke ter posredujejo uporabnikom, ki sprejemajo končne odločitve (Richelson 1999: 4). Ta proces pa je zaradi večje preglednosti razdeljen na pet delov, in sicer na načrtovanje in usmerjanje, zbiranje, obdelavo, analiziranje in posredovanje (Purg 2002: 14; Richelson 1999: 4; IMADE 1993: 1280-1283).

Vendar si glede števila faz v obveščevalnem ciklu strokovnjaki niso enotni. Tako Šaponja obveščevalni cikel razdeli na štiri stopnje tako, da obdelavo podatkov pridruži zbiranju in jo označi kot operativno analitiko. Zanimivo definicijo postavi tudi Angelo Codevilla, ki med faze obveščevalnega ciklusa vključuje tudi protiobveščevalno delovanje in tajne operacije (Šaponja 1999: 66, 142).

¹ V angl. se uporabljata izraza *anti-terrorism* in *counter-terrorism*, vendar pri prevodu nastanejo težave, saj se obe predponi *anti-* in *counter-* prevajata kot *proti-*. Da bi se izognil semantičnim težavam, sem za pojem *anti-terrorism* uporabil sponojenko, medtem ko sem *counter-terrorism* prevedel v protiterorizem.

Načrtovanje kot prva faza zajema vodenje in upravljanje celotnega postopka pridobivanja obveščevalnih podatkov. Potrebno je ločiti vsaj med strateškim načrtovanjem, kjer se opredelijo cilji in objekti obveščevalnega delovanja, in operativnim načrtovanjem, kjer se določi, kako, s kakšnimi sredstvi in katere podatke je potrebno zbrati (Purg 2002: 14). Pri načrtovanju moramo upoštevati dejstva, da se načrtovane dejavnosti organizirajo na podlagi razpoložljivih podatkov in potreb institucije. Prav tako je potrebno upoštevati razpoložljive človeške in materialne vire ter čas (Stopar 2002: 3).

Druga faza obveščevalnega ciklusa predstavlja zbiranje podatkov, ki je tradicionalno najpomembnejša funkcija delovanja obveščevalnih organizacij. Zbiranje pomeni uporabo različnih metod in virov, s katerimi pridobimo neobdelane podatke, primerne za nadaljnjo obdelavo (Richelson 1999: 4). Da pa lahko obveščevalne organizacije uspešno izvajajo fazo zbiranja podatkov, jih morajo deliti glede na razložene kriterije. Najpomembnejši kriteriji so dostopnost, oblika podatkov in namen, zaradi katerega jih obveščevalne organizacije zbirajo (Šaponja 1999: 79).

Pri dostopnosti delimo podatke v dve skupini, in sicer na javno dostopne in tajne. Polk ugotavlja, da je skoraj 90 % vseh informacij javno dostopnih, vendar se tudi tukaj pojavljajo številni problemi. Podatki, ki so javni, včasih niso dosegljivi zaradi oddaljenosti tistih, ki bi radi posedovali informacije, pomanjkanja določenega znanja za razumevanje podatkov ali nepoznavanja jezika, v katerem so posredovani podatki. Eden glavnih ciljev pri delovanju obveščevalnih organizacij je premostitev teh treh ovir (Polk 1997: 176-177).

Glede oblike podatkov ločimo med pisnimi, ustnimi, podatki v obliki računalniških zapisov, v obliki slike, elektromagnetnega valovanja, v obliki določenega predmeta itd. Glede na namen pa se podatki delijo na vsebinske in operativne. Vsebinski podatki se uporabljajo za izdelavo končnih obveščevalnih izdelkov, operativni podatki pa so tisti, ki omogočajo obveščevalnim organizacijam normalno opravljanje svojega dela (Šaponja 1999: 79-80).

Da pa lahko obveščevalne organizacije sploh pridejo do ustreznih podatkov, je potrebno analizirati ustrezne načine oziroma metode za njihovo zbiranje. Šaponja te metode opredeli kot discipline zbiranja podatkov in jih deli na (Šaponja 1999: 84):

- operativne discipline,
- tehnične discipline in
- discipline zbiranja javno dostopnih podatkov.

Relativno podobno razdelitev lahko zasledimo v ameriški literaturi, kjer pa za razliko od različnih disciplin govorijo o virih in metodah zbiranja informacij. Tako v *International military and defense encyclopedia* (IMADE 1993: 1276-1283) zasledimo naslednjo delitev:

- Zbiranje podatkov s pomočjo človeških virov (*Human Intelligence – HUMINT*); že ime pove, da osrednjo vlogo igra človek. Podatki s pomočjo človeških virov se lahko pridobijo na tajen način, kjer glavno vlogo prevzamejo agenti obveščevalne službe, ki si pri svojem delu lahko pomagajo z različnimi tehničnimi pripomočki (oprema za sledenje, prisluškovanje, tajno opazovanje itd.), ali pa na javen način, kjer gre za široko paleto raznih metod, in sicer od poročil beguncev, prebežnikov do zasliševanja ujetnikov, intervjujev, opazovanj itd. Ta metoda zbiranja podatkov se uporablja predvsem takrat, ko so želeni podatki kodirani, skriti, se ne prenašajo po elektronskih zvezah ali pa preprosto takrat, ko želijo obveščevalne organizacije razumeti način delovanja posameznikov in proces sprejemanja odločitev pri obravnavanih ciljnih (Richelson 1999: 257-258).
- Zbiranje podatkov s pomočjo tehničnih sredstev (*Technical Intelligence – TECHINT*); pri tej vrsti zbiranja podatkov se uporabljajo razna tehnična sredstva in sodobna tehnologija. Opredelitev Polmarja in Allena (1998: 547) je, da so ti podatki pridobljeni iz tujih virov, povezanih s tehnično opremljenostjo in njihovo sposobnostjo. Nadalje se TECHINT deli na dve veliki podskupini, in sicer na zbiranje podatkov, ki obstajajo v obliki različnih signalov (*Signals Intelligence – SIGINT*), in na zbiranje podatkov, ki so v obliki podob oziroma slik (*Imagery Intelligence – IMINT*). Zaradi velikega obsega razpoložljivih podatkov in zapletenosti sodobne tehnologije imata ti dve podskupini še vsaka svoje specializirane discipline, ki pa so na tem mestu samo naštet.

- SIGINT vsebuje:
 - spremljanje komunikacijskih kanalov in naprav (*Communications Intelligence – COMINT*),
 - spremljanje drugih elektronskih naprav (*Electronic Intelligence – ELINT*),
 - spremljanje telemetrijskih aktivnosti (*Telemetry Intelligence – TELINT*).
- IMINT vsebuje:
 - fotografsko zbiranje podatkov (*Photographic Intelligence – PHOTINT*),
 - elektrooptično zbiranje podatkov (*Electro-optical intelligence – ELECTRO-OPTINT*).

Ne glede na široko razvejanost obeh podskupin TECHINT-a obstajajo še drugi viri pridobivanja podatkov s pomočjo tehničnih sredstev, ki pa jih zaradi lastnih specifik ni moč umestiti v katero od navedenih podskupin. To so: pridobivanje podatkov s pomočjo zvoka (*Acoustical intelligence – ACOUSTINT* ali *ACINT*), izdelava zemljevidov in zbiranje geodetskih podatkov (*mapping, charting and geodesy intelligence – MC&G*), pridobivanje podatkov s pomočjo laserjev (*Laser Intelligence – LASINT*), spremljanje radioaktivnega sevanja (*Nuclear Intelligence – NUCINT*), spremljanje drugih virov sevanja (*Radiation Intelligence – RINT*) in pridobivanje podatkov s pomočjo radarjev (*Radar Intelligence – RADINT*).

- Zbiranje javno dostopnih podatkov (*Open source intelligence – OSINT*) temelji predvsem na spremljanju in zbiranju informacij, ki so javnega značaja. Richelsonova opredelitev tega vira podatkov vsebuje zbiranje legalno dostopnih dokumentov, spremljanje tujih političnih, vojaških in ekonomskih aktivnosti, spremljanje in snemanje javnih televizijskih in radijskih programov. V zadnjem desetletju pa so na voljo dodatni viri podatkov, ki pa izhajajo iz računalniških baz podatkov in medmrežja (Richelson 1999: 274). Šaponja pa disciplino zbiranja javno dostopnih podatkov razdeli na sredstva javnega obveščanja (radio, televizija, časopisi itd.), kjer je spremljanje teh sredstev koristno predvsem za preverjanje napovedi, usmerjanje nadaljnjega zbiranja podatkov in oblikovanje osnovne baze obveščevalnih podatkov. Druga veja so računalniški mediji in baze podatkov, kjer prednjači uporaba medmrežja in

nadzor komunikacij preko njega; tretjo, predstavljajo ostali načini zbiranja javno dostopnih podatkov, kamor spada zbiranje strokovne literature s posameznega področja in fotografski posnetki dostopnih površin (Šaponja 1999: 136-138). Kljub izredni pomembnosti in koristnosti zbiranja javno dostopnih podatkov, Šaponja prav tako opozarja na glavne nevarnosti, in sicer na veliko možnost zavajanja s strani vira informacij in na »hipertrofijo« podatkov, ki lahko prej ovira delo obveščevalnih služb, kot pa ga izboljšuje.

V tretji fazi obveščevalnega ciklusa se pridobljeni podatki preoblikujejo v operativno informacijo, ki je primerna za izdelavo končnega obveščevalnega izdelka. Vsebuje interpretacijo, merjenje in dekodiranje slikovnega materiala ter raznih signalov, prevajanje iz tujega jezika, razvrščanje po vsebinah in odstranjevanje nepomembnih in nezanesljivih podatkov (Richelson 1999: 4). Osebe, ki izvajajo tovrstno obdelavo podatkov, Šaponja jih imenuje operativni analitiki, imajo širši pregled nad celotnim procesom zbiranja podatkov kot operativni delavci in zato je njihova nujna naloga kritična presoja verodostojnosti podatkov in zanesljivosti virov. Kot rezultat njihovega dela se lahko proces pridobivanja podatkov ponovi, da se že dobljeni podatki ponovno preverijo in izločijo tisti, ki so se v postopku obdelave izkazali za pomanjkljive, oziroma da se ustrezno zbrani in obdelani podatki posredujejo analitični službi (IMADE 1993: 1282; Šaponja 1999: 139-146).

V fazi analiziranja se operativne informacije nadgradijo v obveščevalne informacije. Glede na to, da se informacije zbirajo iz večjega števila različnih virov, se pogosto zgodi, da predstavljajo samo majhen del celotne slike oziroma so si celo nasprotujoče. Zato se izvede proces vrednotenja in ocenjevanja, da bi ugotovili, kako pridobljene informacije prispevajo k dokončanju zastavljene naloge. Informacije se pregledajo na podlagi preteklih vzorcev in dogodkov, prav tako pa se uporabijo številne druge metode, s katerimi se poskuša doseči kar najvišjo stopnjo zanesljivosti pri napovedovanju dogodkov, ki jih lahko razberemo s pomočjo zbranih informacij (IMADE 1993: 1282; Richelson 1999: 4).

V zadnji fazi obveščevalnega ciklusa se izoblikujejo končni obveščevalni izdelki, ki so primerni za posredovanje naročnikom oziroma oblikovalcem politike. Končni obveščevalni izdelki vsebujejo analitične ugotovitve o predmetu raziskovanja, po

obliki pa so lahko predstavljeni zelo različno (ustno, pisno, v računalniški obliki itd.). Pogosto se dogaja, da kljub dobrim in kakovostnim obveščevalnim izdelkom naročniki ne reagirajo v skladu s priporočili oziroma poročil obveščevalnih služb sploh ne jemljejo resno. Tako je ena glavnih nalog v tej fazi, kako prepričati uporabnika o resnosti informacije, ki mu je posredovana, in kako vzpodbuditi takojšnje in optimalne odločitve. Tako Šaponja opredeli določene standarde, ki jih je potrebno upoštevati pri oblikovanju in načinu predstavitve obveščevalnega izdelka uporabnikom. Upoštevati je treba naročnika, čas, ki je na voljo, da se prebere obveščevalni izdelek, pomembnost informacije in način njenega posredovanja. Le tako je lahko doseženo osnovno poslanstvo vsakega končnega izdelka, in sicer obveščanje o neposrednih in posrednih posledicah raznih dogodkov v mednarodnem okolju za nacionalno varnost države (Šaponja 1999: 168-176).

3.5 OBVEŠČEVALNA DEJAVNOST

Obveščevalno dejavnost bi lahko označili kot najpomembnejšo dejavnost, s katero države skrbijo za nacionalno varnost v miru in vojni (Šaponja 1999: 20). Vendar samo definiranje pojma ni tako preprosto. Richelson definira obveščevalno dejavnost kot rezultat obveščevalnega ciklusa, ki vsebuje: zbiranje, analizo, združevanje in interpretacijo vseh razpoložljivih podatkov, ki se nekako navezujejo na tujo državo oziroma na posamezna operativna področja, ki so predmet zanimanja obveščevalnih služb, in kot taka neposredno ali potencialno pomembna za načrtovanje političnih odločitev (Richelson 1999: 2; Anžič 1997: 42; Purg 1995: 30).

Drugačno definicijo zasledimo pri Šaponji, ki opredeli obveščevalno dejavnost kot proces, ki zajema elemente obveščevalnega ciklusa, in sicer zbiranje, analitično obdelavo surovih podatkov in izdelavo celovitega obveščevalnega izdelka, ki ga uporabniki potrebujejo pri sprejemanju odločitev na državniškem, političnem, gospodarskem in varnostnem področju (Intelligence-Policy & Process v Šaponja 1999: 9). Da pa bi bilo bolj razumljivo, kdo pravzaprav lahko izvaja obveščevalno dejavnost, Šaponja razširi svojo osnovno definicijo in trdi, da gre za organiziran proces znotraj za to specializiranih organizacij, ki so bodisi samostojne bodisi del večjih organizacij.

Oba pogleda na obveščevalno dejavnost, in sicer dejavnost kot rezultat ali kot proces, govorita o širšem in ožjem smislu obveščevalne dejavnosti, vendar tudi tukaj naletimo na bistvene razlike. Pri prvem pogledu obveščevalna dejavnost v ožjem smislu zajema le tajno zbiranje in analizo podatkov ter njihovo transformacijo v obveščevalno informacijo, v širšem smislu pa zajema še protiobveščevalne in tajne akcije. Pri zbiranju tajnih podatkov je poudarek predvsem na tajnosti dejavnosti, medtem ko je pri tajnih akcijah poudarek na tajnosti naročnika (Purg 2002: 15). Pomembno je izpostaviti, da se tako ožji kot širši smisel uporabe obveščevalne dejavnosti uporabljata samo v obveščevalnih službah v nacionalnih varnostnih sistemih.

Šaponja na takšno delitev ne pristaja, in trdi, da so ti pogledi zastareli. Zato obveščevalno dejavnost v širšem smislu označi kot pridobivanje novega znanja in informacij o dogodkih, pojavih in procesih v bivalnem ali poslovnem okolju, naravi, družbi, skratka o vsem, kar se dogaja okrog nas, in sicer na organiziran in institucionaliziran način. Kadar pa govorimo o obveščevalni dejavnosti, ki jo izvajajo državne institucije, ki imajo zakonska pooblastila, da zbirajo tudi tajne podatke na posebne načine, lahko govorimo o obveščevalni dejavnosti v ožjem smislu (Šaponja 1999: 10-12).

Šaponja trdi, da so lahko naloge, nameni ali cilji obveščevalne dejavnosti informativne, represivne ali varnostnopreventivne narave. Glede na to so nastale znotraj obveščevalne dejavnosti posamezne zvrsti, in sicer obveščevalna, protiobveščevalna, varnostna in vojaška (Šaponja 1999: 19-23):

- obveščevalna zvrst se uporablja predvsem za raziskovanje zunanjega okolja, ki vpliva na delovanje države. Po svoji naravi je informativnega značaja.
- Protiobveščevalna zvrst je v svoji naravi represivna in je namenjena odkrivanju, spremljanju, onemogočanju in občasno tudi preiskovanju aktivnosti, ki jih na državnem ozemlju izvajajo tuje obveščevalne organizacije.
- Varnostna zvrst je prav tako represivne narave, uporablja pa se za boj proti organiziranemu kriminalu, terorizmu, nedovoljeni trgovini in proizvodnji mamil, orožja in sredstev za množično uničevanje. Uporablja se tudi za odkrivanje, preprečevanje in varovanje pred različnimi oblikami političnega ekstremizma,

radikalizma in drugih dejavnosti, katerih glavni cilj je rušenje ustavne ureditve neke države.

- Vojaška zvrst pa se uporablja predvsem kot pomoč pri poveljevanju v oboroženih silah. Pogosto se zanjo uporablja tudi izraz »taktična vojaška obveščevalna dejavnost«.

3.6 OBVEŠČEVALNA SLUŽBA

Kot pri večini pojmov s področja obveščevalne dejavnosti, si tudi pri opredelitvi obveščevalne službe strokovnjaki nikakor niso enotni. Tako Anžič meni, da so pri opredeljevanju obveščevalne službe pomembni trije segmenti:

- vsebina obveščevalne dejavnosti,
- metode delovanja,
- organizacijski model.

Nadalje meni, da obveščevalne službe niso samo aparat za zbiranje tajnih podatkov, ampak zbrane podatke tudi analizirajo, ocenjujejo in dajejo konkretna priporočila za vodenje politike. Ravno zato njihovo delo ne more temeljiti samo na tajno zbranih podatkih, ampak se morajo posluževati številnih legalnih možnosti za pridobitev podatkov (Anžič 1996: 61). Drugi avtorji menijo nasprotno; obveščevalno službo opredeljujejo neposredno glede na pojav tajnosti oziroma zbiranje nasprotnikovih skrivnosti. (Purg 2002: 16). Omenjeni avtor nadalje deli obveščevalne službe glede na:

- področje dela in položaj v sistemu (civilne in vojaške, službe znotraj ministrstev ali posebne vladne službe),
- stopnjo ofenzivnosti (od samo pridobivanja podatkov pa vse do izvajanja akcij),
- velikost (od manjših enot pa do velikih sistemov),
- usmerjenost (glede na področje dela in geografsko območje),
- notranjo organiziranost (štabni, linijski, projektni in drugi modeli organiziranja).

Vendar Purg obstoj obveščevalnih služb ne omejuje samo na državni aparat, ampak dopušča možnost, da se službe razvijejo tudi v raznih gibanjih, gospodarskih subjektih, združenjih, kriminalnih in terorističnih organizacijah itd. (Purg 2002: 17-18).

Z vidika nadaljnjega preučevanja taktike dela obveščevalnih služb, predvsem glede boja proti mednarodnemu terorizmu, pa se mi zdi najprimernejša definicija Šaponje, ki obveščevalno službo opredeli kot posebno organizacijsko obliko, v kateri se izvaja obveščevalna dejavnost v tujini oziroma v zvezi s tujino. Tako obveščevalne službe izvajajo obveščevalno, protiobveščevalno in varnostno zvrst, delujejo pa na vseh področjih. Obveščevalne službe delimo v naslednji dve skupini (Šaponja 1999: 32-42):

- strateške in taktične (specializiranost za določena področja ali za določen način zbiranja podatkov),
- aktivne in pasivne (aktivne obveščevalne službe v okviru svojih delovnih nalog izvajajo tudi tajne akcije ali operacije).

3.7 NACIONALNOVARNOSTNI SISTEM

Grizold razume nacionalnovarnostni sistem kot strukturo, katere cilj je zagotavljanje varnosti na nivoju celotne družbe. Vendar lahko varnost na tem mestu razumemo v ožjem in širšem smislu, oziroma dojemanje varnosti kot negativni (odsotnost nevarnosti) ali kot pozitivni cilj (višja stopnja varnosti od golega obstanka) (Nye v Grizold 1992: 68). V tej dvojnosti dojemanja varnosti se odraža tudi učinkovitost nacionalnovarnostnega sistema, ki mora vsebovati sposobnost države, da zavaruje svoje temeljne družbene vrednote in lasten obstoj pred zunanjim in notranjim sovražnikom ter da zagotavlja možnosti za družbeno-gospodarski razvoj in splošno blaginjo ljudi.

Uspešnost zagotavljanja varnosti s strani nacionalnovarnostnega sistema pa je možna takrat, kadar ta sistem izpolnjuje pričakovanja civilne družbe in politične države, ki odražajo vpliv mednarodnega okolja, družbeno-gospodarskih zmogljivosti, političnih interesov in prevladujočih vrednot v družbi. Tako lahko rečemo, da na

vzpostavitev nacionalnovarnostnega sistema delno vplivajo predpostavljene, delno pa dejanske okoliščine dojemanja ogrožanja varnosti (Grizold 1998: 4).

Za ustrezno razumevanje pojma nacionalnovarnostni sistem pa je potrebo identificirati posamezne elemente oziroma nacionalnovarnostne prvine, ki predstavljajo operativne dejavnosti družbe in naj bi zagotovile njeno varnost. Te prvine so (Grizold 1999: 35-38):

- Varnostna politika – obstajata širši (preventivna priprava na potencialne vire ogrožanja) in ožji pomen (skupek ukrepov, dejavnosti in ravnanj, namenjenih vzpostavitvi in delovanju nacionalnovarnostnega sistema).
- Varnostna struktura, katere namen je zagotavljanje varnosti na ravni celotne družbe. Sicer je za vsako državo specifična, vendar se v večini primerov deli na naslednje podprvine:
 - obrambna – namenjena zagotavljanju varnosti proti zunanjim virom ogrožanja,
 - notranjevarnostna – namenjena vzdrževanju ustavne ureditve in zaščiti družbene infrastrukture,
 - zaščitno-reševalna – namenjena pomoči prebivalstvu in zaščiti materialnih dobrin v primeru naravnih in drugih nesreč ter vojn.
- Varnostno samoorganiziranje družbe – mišljeno je predvsem z vidika zagotavljanja varnosti na individualni in skupinski ravni, na temelju »naravne pravice« do samoobrambe, samozaščite in samopomoči.

4 DEJAVNIKI MEDNARODNEGA TERORIZMA

O obstoju in delovanju mednarodnega terorizma, lahko govorimo ob določenih dejavnikih, ki ga omogočajo. Identificiral sem pet dejavnikov, za katere menim, da so bistvenega pomena, da lahko govorimo o terorizmu in delujoči teroristični organizaciji. Preučevanje dejavnikov pa ni potrebno samo za razumevanje terorizma, ampak tudi za razumevanje obveščevalnih služb, saj le-ti predstavljajo najpomembnejša področja, na katerih delujejo obveščevalne in varnostne službe v protiterorističnem boju. Nekatere službe celo prilagajajo svoj obveščevalni cikel in metode zbiranja podatkov tem dejavnikom, kar kaže na njihovo pomembnost v procesu obveščevalne obdelave. Seveda se v primeru mednarodnega terorizma v teh dejavnikih pojavljajo mednarodne razsežnosti, in sicer tako pri človeškem, finančnem, materialnem, komunikacijskem in ideološkem dejavniku.

4.1 ČLOVEŠKI DEJAVNIK

Vsaka teroristična organizacija mora za izpolnitev svojih ciljev imeti na voljo primerne ljudi. Dejstvo je, da se ideje terorističnih skupin manifestirajo preko dejanj, za katerimi stojijo aktivisti, ki predstavljajo prvo skupino ljudi, povezano s terorizmom. Čeprav ta skupina nikakor ni homogena in jo je moč razdeliti na vodstvo, ki se ukvarja s strateškim vodenjem organizacije, in aktiviste, ki dejansko izvajajo teroristična dejanja (Henderson v Miholič 2004: 19-20), bom prvo skupino ljudi obravnaval enotno. Druga skupina so simpatizerji, ki podpirajo delovanje terorističnih organizacij. Z njimi skupine neposredno sodelujejo, in sicer predvsem pri zagotavljanju financiranja, logistične podpore in širjenja idej. Ta skupina je prav tako najbolj dovzetna za rekrutiranje v teroristične vrste. Tretja skupina ljudi pa so tisti, sicer latentni podporniki idej, za katerimi stojijo teroristične organizacije, ki jih s svojim delovanjem poskušajo pritegniti na svojo stran in vpeti v teroristična dejanja.

Če želimo govoriti o vpetosti ljudi v terorizem, je potrebno izpeljati eno najbolj občutljivih dejavnosti v organizaciji, in sicer rekrutiranje. V želji po zmanjševanju možnosti infiltracije agentov obveščevalnih in varnostnih služb, teroristične skupine uporabljajo različne ukrepe pri novačenju sodelavcev. Opazna sta predvsem dva

trenda, in sicer nabor aktivistov iz vrst mladih, ki praktično slepo sledijo ideji terorizma in omogočajo tajno delovanje skupine, ter rekrutacija na osnovi osebnih in sorodstvenih poznanstev, kar omogoča preverjanje posameznikove preteklosti in vzgibov za članstvo v teroristični organizaciji (Miholič 2004: 29-30). Sicer vsaka oblika nabora prinaša določene slabosti, zato je vse težje najti čisti naborni sistem. Med »novimi« teroristi tako namesto študentov, kot glavne naborne baze v 70. letih, vstopa v ospredje brezposelna mladina iz revnih urbanih predelov, za katere je sodelovanje v terorističnih organizacijah izhod iz socialne stiske.

Pri osebni rekrutaciji pa obstaja nevarnost, da se v primeru razkritja dela organizacije, zaradi prijateljskih in sorodstvenih vezi sproži »verižna reakcija« pri razkrivanju teroristične mreže. Zato tovrstni sistem rekrutiranja uporabljajo tiste teroristične skupine, ki delujejo predvsem lokalno oziroma posamezne celice večjih mednarodnih terorističnih organizacij.

4.2 FINANČNI DEJAVNIK

Za nemoteno poslovanje in delovanje terorističnih organizacij je vsekakor potrebno poiskati zadovoljive vire finančnih sredstev, ki pokrivajo potrebe terorističnih akcij. Glavne značilnosti financiranja mednarodnega terorizma so predvsem transnacionalni finančni viri in finančno transakcijske poti.

Pri finančnih virih oziroma načinih financiranja, mednarodne teroristične združbe uporabljajo različne metode, ki so odvisne od velikosti organizacije, velikosti območja delovanja in metod delovanja. Možni načini financiranja so (Miholič 2004: 36-44):

- Državna podpora, ki pa se zaradi želje po izboljšanju meddržavnih odnosov bistveno zmanjšuje. Številne države, ki so bile opredeljene kot podpornice terorizma, svojo podporo umikajo, ena izmed izjem, ki je še zmeraj aktivna pri vzdrževanju terorističnih organizacij na Bližnjem vzhodu, pa ostaja Iran.
- Zakonito poslovanje, ki zajema širok spekter delovanja terorističnih organizacij. Najznačilnejše oblike financiranja v okviru zakonitega poslovanja so predvsem deleži plač aktivistov, ki jih nakazujejo na račune

organizacij za svoj boj, in prodaja raznovrstnega promocijskega materiala². Pri organizacijsko bolj kompleksnih in homogenih organizacijah pa zasledimo tudi lastništvo raznih podjetij in trgovin oziroma delniške in obvezniške naložbe³.

- Donacije posameznikov in financiranje preko dobrodelnih dejavnosti prav tako predstavlja pomemben vir dohodka. Tvrstni način financiranja je opazen predvsem pri terorističnih skupinah islamskega porekla, saj po svetu obstaja največ različnih islamskih humanitarnih organizacij, ki del svojega prihodka namenijo za financiranje terorističnih akcij. Shahar ugotavlja, da večina denarja, ki gre preko raznih humanitarnih organizacij, prihaja iz držav na Bližnjem vzhodu. Le-te preko svojih uradnih in neuradnih fundacij namenijo velike vsote denarja različnim islamskim organizacijam, med katerimi je veliko podpornic terorizma. V tem primeru bi lahko govorili o posredni državni podpori terorističnim organizacijam. Glede donacij posameznikov pa nekako prevladujeta dve načeli, in sicer prostovoljne donacije bogatih posameznikov, ki verjamejo v idejo terorizma, in prisilne donacije, ki so povezane z izsiljevanjem in grožnjami (Shahar 2001).
- Kriminalna dejavnost, ki jo lahko izvajajo teroristične organizacije same, kar velja predvsem za manjše skupine in sodelovanje s kriminalnimi združbami. Tvrstno sodelovanje prinaša koristi obema stranema; tako dobijo kriminalne skupine dodatno zaščito, dostop do orožja in usposabljanje za svoje člane, teroristi pa dobijo delež dobička iz nelegalnega poslovanja. Med poglobitve kriminalne dejavnosti spadajo predvsem ugrabitve, izsiljevanja, goljufije in trgovina z orožjem, belim blagom in mamili. Povezava med terorizmom in organiziranim kriminalom je najbolj očitna pri proizvodnji in prodaji mamil, kar se kaže v pojavu narkoterorizma. Shahar (2001) opisuje vlogo Al Kaide in talibanskega režima v Afganistanu pri proizvodnji opija, ki so ga proizvajali izključno za izvoz na zahodno, predvsem ameriško tržišče. Učinki so bili mnogostranski, saj je bila trgovina z mamili eden poglobitvenih virov financiranja, obenem pa se je zahodni svet ubadal s težavami odvisnosti in povečanja kriminala.

² Med propagandni material sodijo avdio in video posnetki vplivnih verskih in političnih voditeljev in so namenjeni predvsem simpatizerjem.

³ Primer takšnega poslovanja je japonski kult Aum Shinrikyo, ki je odgovoren za napad s sarinom na japonski podzemni železnici, in je imel v svoji lasti mrežo internetnih trgovin, fitnes, meditacijske centre itd.

Ob uspešni pridobitvi denarja je potrebno uporabiti primerne mehanizme prenosa finančnih sredstev, ki zagotavljajo varnost, hitrost in anonimnost. To predvsem velja za večje teroristične organizacije, ki svoje delovanje načrtujejo na globalni ravni. Vse mehanizme prenosa financ pa lahko razdelimo na registrirane in neregistrirane finančne transakcije (Miholič 2004: 45). Številne organizacije svoje finančne posle opravljajo s pomočjo legitimnega bančnega poslovanja. Glavna šibka točka pri tovrstnem poslovanju je obstoj fizičnih dokazov o finančnih prenosih, zato se uporabljajo predvsem t. i. *off-shore* banke, v katerih je mogoče odpreti račun in preko njega poslovati brez razkritja identitete lastnika računa. Tako se zakrije izvor denarja. Nadalje se večji finančni zneski razbijejo na več majhnih, ki ne vzbujajo suma pri varnostnih organih in preko osebnih računov simpatizerjev pridejo na končni naslov. Nadalje prav tako Miholič (2004: 46-48) ugotavlja velik pomen uporabe neregistriranih finančnih prenosov, za katerimi ni nikakršnih fizičnih dokazov o izvedbi. Poglavitni načini tovrstnega poslovanja so uporaba kurirjev, tihotapskih poti in tradicionalnih bančnih sistemov.

Kljub temu da ravno pri uporabi kurirjev obstaja velika stopnja tveganja, da se ta sredstva odkrijejo in da je na tovrsten način mogoče prenesti le omejeno količino denarja, se veliko terorističnih organizacij poslužuje prav te vrste transakcij, saj je zelo težko izslediti izvor denarja. Prav tako se večji zneski razbijejo na manjše, kar pomeni manj finančnih izgub v primeru razkritja. Za prenos večjih finančnih sredstev pa se uporabljajo ustaljene tihotapske poti, po katerih se opravljajo tudi ostali kriminalni posli (trgovina z mamili, orožjem, belim blagom itd.).

Med tradicionalnimi bančnimi sistemi pa se v večini primerov uporablja t. i. sistem hawala, ki v bistvu pomeni neposredni prenos denarja preko posrednikov, in sicer brez bančnih transakcij. Deluje na podlagi popolnega zaupanja med vpletenima posrednikoma, ki nastale medsebojne terjatve poravnata z nedenarnimi sredstvi. Tovrstni sistem je praktično nemogoče preprečiti ali odkriti (Podbregar 2004: 34).

4.3 MATERIALNI DEJAVNIK

Če želijo teroristične organizacije manifestirati svoje ideje, morajo imeti na voljo veliko materialnih sredstev. Uporaba le-teh pa je odvisna od načina delovanja organizacije in od cilja, ki bi ga rada dosegla. Sredstva, ki jih teroristične organizacije lahko uporabijo za izvajanje svojih aktivnosti, je mogoče razdeliti na konvencionalna bojna sredstva, sredstva za množično uničevanje in nebojna sredstva, uporabljena v terorističnem boju.

Osrednje mesto v arzenalu tako tradicionalnih kot sodobnih terorističnih skupin zaseda konvencionalno orožje, predvsem lahko pehotno orožje in eksplozivna sredstva, ki jih teroristične skupine pridobivajo preko nelegalnih in legalnih poti oziroma celo same vzpostavijo proizvodnjo določenih vrst orožja (Miholič 2004: 70). Večina skupin za svoje delovanje uporablja raznoliko oborožitev. To pa ima tako pozitivne učinke, saj je težje identificirati posamezno organizacijo, če v svojem boju uporablja različne metode in različna sredstva, kot negativne, saj sta vzdrževanje in shranjevanje različnih vrst orožja velikokrat oteženi.

Velika raznolikost oborožitve pa je posledica načina pridobivanja tovrstnih sredstev. Tradicionalne teroristične skupine so uživale državno podporo, kar je bilo še posebej opazno v času hladne vojne, saj sta tako vzhodni kot zahodni blok igrala pomembno vlogo kot dobavitelja oborožitvenih sistemov za posamezne teroristične skupine, ki so delovale na ozemlju oziroma interesnem območju nasprotnika. Danes državna pomoč ne predstavlja zelo pomembnega vira za nabavo orožja, saj je večina držav umaknila svojo podporo terorizmu, predvsem zaradi strahu pred sankcijami s strani mednarodne skupnosti. Ena redkih držav, ki še javno podpira in tudi oskrbuje teroristične organizacije z različnimi sredstvi, je Iran.

Drugi način pridobivanja oborožitve je nelegalna trgovina z orožjem. Krizne razmere v obdobju razpada Sovjetske zveze, nestabilnost novonastalih držav na tem ozemlju in številni oboroženi konflikti v 90. letih prejšnjega stoletja so omogočili hiter razcvet trgovine z orožjem (Miholič 2004: 73). Posledično imajo teroristične organizacije dostop do praktično neomejenega vira oborožitve. V območje nelegalnega

pridobivanja orožja spadajo prav tako ropi in tatvine, predvsem vojaških skladišč in skladišč gospodarskih družb, ki imajo dostop do gospodarskih eksplozivov⁴.

V državah, kjer je zakonodaja zelo ohlapna glede nabave orožja, predvsem lahkega pehotnega, je pridobivanje tovrstnih sredstev za teroristične skupine lažje. Primer so ZDA, kjer se predvsem skrajne desničarske skupine povsem legalno opremljajo s pehotnim orožjem. Nadalje je do raznih eksplozivnih sredstev in orožja mogoče priti s pomočjo legalnih podjetij, ki so v lastništvu terorističnih skupin, in nabavo orožja za lastne namene prikrijejo s povsem legalnimi posli⁵.

Druga skupina sredstev, ki jih lahko teroristične skupine uporabijo v svojem boju, je orožje za množično uničevanje. Največja nevarnost uporabe tovrstnih sredstev je predvsem izguba političnih ciljev terorističnih organizacij in izvajanje terorja zaradi terorja samega z željo po čim večjem številu žrtev. Orožje za množično uničevanje pa je ravno s tega vidika najbolj primerno sredstvo.

Dejstvo je, da izdelava in vzdrževanje tovrstnega orožja ne predstavljata nepremagljive tehnološko-tehnične ovire, saj je kar nekaj skupin, ki so sposobne izdelati primitivno radiološko bombo in kemično ter biološko orožje (Halilović 2004: 159-160). Še največjo tehnično oviro, kot ugotavlja Miholič (2004: 82), predstavlja izdelava primerne sistema za disperzijo snovi, zaradi česar napadi s sredstvi za množično uničevanje niso tako razširjeni.

Kar zadeva jedrske teroristične napade, obstaja zelo majhna verjetnost, da bi prišlo do njih, saj je za izdelavo sofisticiranega jedrskega orožja že potrebno priskrbeti veliko resursov in znanja, za kar pa v današnjem času teroristične skupine še niso usposobljene. Namesto terorističnih jedrskih udarov je bolj verjetno pričakovati napade z radiološkim orožjem oz. »umazanimi bombami« (t. i. *dirty bombs*), ki so

⁴ Najpomembnejši vir oborožitve za teroristično organizacijo IRA je predstavljala podporna skupina v ZDA, ki jo je z vdori v skladišča ameriške vojske in nakupi orožja na črnem trgu oskrbovala v začetnem obdobju boja (Cralley 2004: III-44-III-45).

⁵ Primer tovrstnega oboroževanja je Al Kaida oziroma preko nje Osama bin Laden, ki je ustanovil gradbeno podjetje v Sudanu, in dobil državno koncesijo za gradnjo cest, kar mu je omogočilo, da je na trgu legalno nabavljal velike količine eksploziva (Shahar 2001).

kombinacija konvencionalnega eksploziva in radioaktivnih materialov, katerih pridobivanje ni tako oteženo, saj se uporabljajo v gospodarske, znanstvene in medicinske namene. S tovrstnimi napadi je mogoče doseči kontaminacijo večjega območja, kar je še posebej nevarno v urbanih naseljih (Leader v Miholič 2004: 82-83). Dodatna nevarnost, v smislu radiološkega napada, so napadi na jedrske objekte (elektrarne, vojaške komplekse, znanstvene laboratorije, skladišča radioaktivnih odpadkov itd.), ki posedujejo radioaktivne materiale. S konvencionalnim napadom na določen objekt je mogoče doseči učinek dolgotrajne kontaminacije širšega območja, na katerem se je nahajal jedrski objekt.

Čeprav je v današnjem času mogoče opaziti trend povečanja žrtev terorističnih napadov, vseeno teroristične skupine, kljub osvojenemu znanju, potrebnemu za izdelavo in uporabo orožja za množično uničevanje, niso »navdušene« nad uporabo le-tega, predvsem zaradi manjše podpore in strahu pred povračilnimi ukrepi napadene države in celotne mednarodne skupnosti. Kljub temu je potrebno posvetiti veliko pozornost oboroževanju s sredstvi za množično uničevanje, predvsem zaradi pojava posameznih skupin, ki delujejo brez političnega cilja oziroma so njihovi cilji zelo radikalni, predvsem v smislu povzročitve materialne škode in človeških žrtev.

V sodobnem svetu, ki temelji na informacijski družbi in na globalni komunikaciji, vse večjo nevarnost predstavljajo morebitni napadi na informacijska središča oziroma vdori v posamezne računalniške sisteme, ki so vitalnega pomena za obstoj družbe. Tovrstno nevarnost imenujemo kibernetični terorizem, ki za svoje cilje ne uporablja konvencionalnega orožja, temveč so njihova glavna sredstva računalnik in računalniška omrežja. Sodobna družba temelji na računalniško vodenih energetskih, transportnih, komunikacijskih sistemih in napad nanje bi ohromil širše geografsko območje. Učinkovitost kibernetičnega terorizma je tako odvisna od stopnje razvitosti informacijske družbe, zato so na tovrstne napade najbolj občutljive zahodnoevropske in severnoameriške države, ki svoje normalno delovanje vse bolj vežejo na pravilno delovanje računalniških sistemov. Najpogostejši napadi preko računalnikov so predvsem uporaba virusov in »trojanskih konj«, ki blokirajo računalniški sistem, vendar dolgoročno ne puščajo posledic. Namen teh napadov je predvsem propaganda in povzročitev ekonomske škode. Večji problem nastane, ko se z uporabo programskih orodij manipulira z večjimi kibernetičnimi sistemi, kar lahko

pripelje do večjega izpada električne energije, pitne vode, komunikacij; lahko se sprožijo trčenja vlakov in letal (Miholič 2004: 80-81).

Kljub vsem sredstvom, ki jih teroristične skupine lahko uporabijo v svojem boju, vselej obstaja možnost improvizacije s strani terorističnih organizacij. Tako so bila v napadih 11. septembra 2001 uporabljena ugrabljena potniška letala, in sicer z namenom, da bi strmoglavili v stavbe velikega simboličnega pomena. Na podoben način se lahko uporabijo tudi druga prevozna sredstva, predvsem sredstva javnega prevoza, kjer je veliko število žrtev in prav tako je velika materialna škoda. Še posebej so ogrožene pomorske poti, kjer obstaja velika nevarnost ugrabitve tankerjev in potniških ladij, s katerimi bi povzročili medsebojno trčenje, oziroma zloraba tankerja, napolnjenega z nafto kot projektil, namenjen v kakšno priobalno mesto ali večje pristanišče (Blanche 2002: 10-11). Takšen napad ne bi imel za posledico samo človeških žrtev in ekonomske škode, temveč bi šlo za ekološko katastrofo večjih razsežnosti, ki bi dolgoročno vplivala na obstoj in razvoj življenja na določenem območju.

4.4 KOMUNIKACIJSKI DEJAVNIK

Če upoštevamo dejstvo, da teroristične skupine delujejo na mednarodni ravni, je bistvenega pomena komunikacija med celicami organizacije in med samimi organizacijami. Dandanes se napadi organizirajo na drugem koncu sveta, kot se dejansko izvedejo. Sredstva za delovanje se pridobivajo na vseh delih sveta in prav tako se tudi tarče nahajajo na praktično celotni zemeljski obli. Ravno zato je sistem komunikacije vitalnega pomena. Prav tako pa je potrebno z idejami in akcijami seznaniti javnost, za kar je ponovno treba vzpostaviti učinkovit sistem komunikacij. Tukaj pride do izraza predvsem povezava med terorističnimi organizacijami in mediji.

Tako so terorizem in mediji v medsebojni odvisnosti. Sam terorizem je brez pomena, če akcije niso medijsko pokrite in iz tega razloga teroristične organizacije uporabljajo množične medije za pridobivanje publicitete in dosego strateških ciljev (Martin 1985). Zato se teroristične skupine lotevajo različnih načinov promocije svojih akcij, kar vključuje uporabo vseh vrst množičnih medijev. V primeru mednarodnega terorizma,

ko sta cilj napada in ciljna populacija, kateri je namenjeno sporočilo terorističnega napada, geografsko oddaljena od samega območja, na katerem deluje teroristična organizacija, obstaja želja po čim bolj globalni medijski pokritosti. Tako Martin (1985) ugotavlja, da večina terorističnih skupin raje deluje na območju Zahodne Evrope, ZDA in na večjih kriznih območjih, kjer je medijska pokritost tovrstnih akcij na zelo visoki ravni.

Čeprav se najosnovnejši načini promocije, kot so tiskani letaki, razne periodične publikacije in predvsem v primeru skrajnih desničarskih skupin knjige in manifesti, še zmeraj uporabljajo, niso primerni za mednarodno promocijo, predvsem zaradi premajhne koristi in omejenega dometa. Drug način uporabe tiskanih medijev je objavljane propagandnih sporočil v časopisih (Miholič 2004: 56-57).

Vse bolj v ospredje prihajajo elektronski mediji, ki omogočajo realno časovno poročanje o terorističnih aktivnostih in imajo neprimerljivo večji krog občinstva. Preko elektronskih medijev se teroristična propaganda odvija na bolj čustveni ravni, saj je mogoče prikazati neposredne posledice napadov, osebne izpovedi žrtev in aktivistov terorističnih skupin, motivacijske govore političnih in verskih voditeljev itd. Teroristični napadi naj bi dobili čim večjo stopnjo medijske pozornosti, zato na izbor tarče in časa napada vpliva tudi želja po nastopu v »*primetime*« *novicah* (Cralley 2004: III-73).

Nova prelomnica v načinu komuniciranja med terorističnimi skupinami in javnostjo pa je bila širša uveljavitev medmrežja, saj se je s tem zelo poenostavilo objavljane velikega števila informacij; prav tako je dostop do medmrežja praktično globalen in nevarnost odkritja s strani državnih varnostnih organov je veliko manjše. Da je uporaba medmrežja, za komuniciranje z javnostjo, s strani teroristov boljša, je Whine (1999) poudaril pet točk, ki kažejo na koristost uporabe medmrežja.

Prva je, da medmrežje omogoča medsebojno povezanost, in sicer zunanjo in notranjo, ki ima za posledico ažurno objavljane vseh dogodkov in da se pride do hitre povratne informacije. Drugič, medmrežje omogoča prikrito komunikacijo in anonimnost, kar je najbolj opazen trend pri terorističnih dejanjih v zadnjih letih. Tretji razlog za uporabo medmrežja je cenovna ugodnost. Glede na to, da se nekateri tradicionalni finančni viri ukinjajo, so teroristične organizacije prisiljene, uporabljati

finančno ugodnejše načine delovanja in sem nedvomno spada »oglaševanje« akcij. Kot četrto prednost Whine navaja dejstvo, da sodobna informacijsko komunikacijska tehnologija omogoča terorističnim skupinam, da imajo takšen doseg in vpliv, kot so ga včasih imele samo nekatere dobro organizirane in s strani države podprte teroristične organizacije. Zadnji razlog za uporabo medmrežja pa je možnost, da dosežejo tisto ciljno publiko, do katere predhodno, predvsem zaradi nesodelovanja s strani medijev, niso imeli dostopa. To so predvsem mladi in izobraženi ljudje.

Primer teroristične organizacije, ki intenzivno uporablja sredstva sodobne tehnologije, je teroristična organizacija Al Kaida. Uporaba njene spletne strani Alneda.com, je primer, kako se prej navedene prednosti internetne tehnologije uporabljajo v praksi. Internetna stran je profesionalno izdelana baza podatkov, ki omogoča dostop do povzetkov mednarodnih medijskih poročanj o dogajanju v Afganistanu, pogled na dogajanje z vidika Al Kaide; vsebuje povzetke člankov, knjig itd. Iz tega je razvidno, da dandanes teroristične skupine posvečajo zelo veliko pozornost uporabi internetne tehnologije za komunikacijo z mediji in javnostjo ter tudi za morebitno psihološko vojskovanje (Eedle 2002: 25).

Komunikacijska sredstva so pomembna tudi za vzdrževanje notranje komunikacije. Glavni cilji tovrstne komunikacije pa so omogočanje natančnega in učinkovitega načrtovanja, koordinacija in izvedba terorističnih aktivnosti. Rezultati ustreznega vzdrževanja stikov med člani skupine se kažejo predvsem v načinu izvajanja operacij, ki postajajo vse bolj zahtevne, predvsem v smislu logistike in geografske razpršenosti (Miholič 2004: 61).

Kljub temu da se v medsebojni komunikaciji prav tako uveljavlja sodobna tehnologija, z uporabo medmrežja na prvem mestu, so še zmeraj prisotne bolj tradicionalne metode komuniciranja. Tako IRA še zmeraj uporablja na poseben način zvita sporočila, pri katerih je takoj mogoče ugotoviti, ali so bila prebrana s strani nepooblaščenih oseb (Cralley 2004: III-33-III-34). Sodobna tehnologija pa omogoča hitrejšo komunikacijo, ki je nujni pogoj za delovanje v mednarodnem okolju. Tako prihaja do izraza uporaba stacionarne telefonije, vendar zaradi hitre izsledljivosti vodijo predvsem javni telefoni. Nadaljnji korak v medsebojni komunikaciji je bil razvoj mobilne telefonije, kar je omogočilo večjo mobilnost, saj sogovornika nista bila

vezana na specifično lokacijo. Nakup mobilnega telefona omogoča anonimnost kupca, kar pripomore k večji varnosti komunikacije. Vendar se zaradi omejene pokritosti mobilnega omrežja v številnih predelih sveta, za komuniciranje uporablja satelitska telefonija. Sicer omogoča komunikacijo povsod po svetu, a je praktično takoj izsledljiva. V želji, da se omogoči anonimnost delovanja, so vsi prej navedeni elektronski načini komuniciranja postali vmesniki pri dostopu do internetnega omrežja, ki je omogočil lažjo komunikacijo znotraj skupine in ne samo navzven. Preko raznih internetnih komunikacijskih orodij (e-mail, IRC, chat-rooms itd.) komunikacija poteka realno časovno, anonimno in z možnostjo prenosa obsežnejših gradiv, potrebnih za izvedbo akcije (Miholič 2004: 62-65).

4.5 IDEOLOŠKI DEJAVNIK

Ideologija igra odločilno vlogo pri delovanju terorističnih organizacij. Omogoča jim izbiro motiva za svoje delovanje in prav tako poseben pogled na svet okrog njih ter na posamezne dogodke in dejanja ljudi, ki jih s svojim ideološkim vrednostnim sistemom ocenjujejo (Drake 1998). Čeprav se v praksi ideologija razlikuje od skupine do skupine, pa je mogoče poiskati nekatere skupne smernice, ki razvrščajo teroristične skupine v tri pglavitne motivacijske skupine, in sicer racionalno, psihološko in kulturno. Vendar je zaradi kompleksnosti delovanja organizacij čisti motivacijski model v praksi praktično nemogoče zaznati, saj se vsi trije medsebojno prepletajo (U.S.Army, Field Manual 100-20, Stability and Support operations).

4.5.1 RACIONALNA MOTIVACIJA

Tovrstni način motivacije je prisoten predvsem pri skupinah, ki delujejo po načelu vojaške organiziranosti. Teroristična dejanja so samo eno izmed sredstev, ki se lahko uporabijo v boju. Pri teh skupinah prav tako veliko vlogo igra politično gibanje, ki organizaciji poskuša pridobiti legitimnost in legalnost. V primeru izvedbe terorističnih napadov pa se izvede analiza »stroškov in koristi«; pridobijo se ustrezni obveščevalni podatki in analiza posledic dejanja. Če na podlagi predhodnih analiz teroristična akcija ne bi dosegla pričakovanega učinka, se jo preprosto odpove. Ta način razmišljanja je opazen pri terorističnih skupinah s politično ideološko podlago, saj bi z

nepremišljeno uporabo nasilnih akcij izgubile podporo v socialnih skupinah s podobnim mišljenjem, kot se je to zgodilo z organizacijama RAF v Nemčiji in BR v Italiji.

4.5.2 PSIHOLOŠKA MOTIVACIJA

Psihološka motivacija izvira iz posameznikovega osebnega nezadovoljstva z lastnim življenjem in dosežki. Svoj nadaljnji smisel delovanja vidi v terorističnih organizacijah in se dejansko poistoveti z organizacijo. V organizaciji se oblikuje prepričanje v samo eno resnico in ustvari se bipol »mi proti njim«, kar pomeni, da si vsi, ki ne delijo tega prepričanja, zaslužijo kazen in nasilje. To jim omogoči, da svojih žrtev ne vidijo kot ljudi in se s tem otresejo morebitnih dvomov v upravičenost svojih dejanj.

V organizacijah s prevladujočo psihološko motivacijo sta obstoj same skupine in vključenosti posameznika vanjo bolj pomembna kot ideal, za katerega se borijo. Tako večkrat pride do napadov, ki so brez učinka oziroma celo z negativnim učinkom, kljub temu pa se krepijo vezi znotraj organizacije.

Tovrstne skupine so največkrat zelo radikalne in ne dopuščajo kompromisov ter pogajanj, ki so zanje znak slabosti ali celo izdaja. V takšnih primerih pa prihaja do ločitev znotraj organizacij in novo nastala organizacija je v večini primerov bolj radikalna od matične. S tem načinom delovanja so cilji terorističnega delovanja skoraj nedosegljivi, saj bi to lahko pomenilo prenehanje delovanja skupine, kar pa za njene člane ni sprejemljivo. Možnosti za uspeh se izničijo, če se postavijo tako široki in velikokrat utopični cilji, ki jih ni mogoče doseči. Vsak politični korak k izpolnitvi cilja pa je lahko zavrnjen in teroristično delovanje se nadaljuje.

4.5.3 KULTURNA MOTIVACIJA

Dojemanje in oblikovanje življenja posameznika sta posledica kulture na določenem območju. Prav tako kultura oblikuje družbene vrednote in motivira ljudi, da izvajajo dejanja, ki se zunanjim opazovalcem zdijo popolnoma neracionalna. Vendar se v družbah, kjer se posamezniki identificirajo s kulturnimi vrednotami, v primerih, ko

pripadniki družbe začutijo, da so njihove temeljne vrednote ogrožene, lahko sprožijo obrambne reakcije, ki se v skrajnih primerih sprevržejo v teroristične akcije, kjer ogrožena skupina lahko napade in uniči vse »druge«, ki predstavljajo nevarnost določeni kulturi.

Religija in etnična pripadnost sta še posebej »nevarna« identifikatorja, saj vsebujeta vrednote, ki so globoko zakoreninjene v kolektivni zavesti družbe in posameznika, pripadnika te družbe. Ravno zato so teroristični napadi, izvedeni iz religioznih motivov, še posebej nasilni, saj njihovi izvajalci vidijo sebe kot mučenike in svoje akcije kot izpolnjevanje volje višje sile, s čimer se prav tako izloči vsakršen dvom v pravičnost lastnega početja. Ravno zato je med versko motiviranimi teroristi zelo visoka stopnja predanosti in pripravljenosti tudi za samozrtvovanje v boju proti »sovražnikom«, ki ogrožajo njihove kulturne vrednote.

Kot sem že omenil, je čisti model ideološke motivacije praktično nemogoč, saj v vsaki teroristični organizaciji zasledimo elemente vseh treh motivacijskih modelov. Ne glede na poreklo teroristične skupine, se vodstvo le-te vedno racionalno odloča o izvajanju strategije in sledi svojemu cilju, vendar se rekrutiranje novih pripadnikov skupine izvaja predvsem glede na njihovo nezadovoljstvo z lastnim življenjem in občutek, da so ogrožene njegove temeljne vrednote.

Ustrezna identifikacija ideologije in motivacije za izvajanje terorističnih napadov pa je bistvenega pomena tudi pri zaščiti potencialnih žrtev in pri zmanjšanju posledic že izvedenih akcij.

5 VPLIV TERORIZMA NA SPREMEMBE NACIONALNOVARNOSTNIH SISTEMOV

5.1 PRIMER ZDRUŽENIH DRŽAV AMERIKE

Izhodišče za spremembe v nacionalnovarnostnem sistemu v prvem desetletju po koncu hladne vojne je bilo predvsem dejstvo, da ni več nevarnosti globalnega spopada dveh ideoloških blokov in da so se v svetu pojavile nove grožnje in nevarnosti, ki ogrožajo interese ZDA⁶ (Raščan 2005: 40). Temeljni vir ogrožanja nacionalnih interesov sta postala nepredvidljivost in negotovost novega mednarodnega varnostnega okolja. Clintonova administracija v strategiji nacionalne varnosti opredeli tri osnovne kategorije, ki predstavljajo ogrožanje ameriških interesov, in sicer (A National Security Strategy for a New Century, 1997):

1. regionalne krize in grožnje s strani posameznih držav,
2. transnacionalne grožnje, ki zajemajo širok spekter dejavnosti, od terorizma, organiziranega kriminala, ilegalnih migracij do globalnega onesnaževanja,
3. orožje za množično uničevanje, predvsem v rokah »malopridnih« držav, terorističnih in kriminalnih organizacij.

Glede na identificirane grožnje so bili v tej strategiji nacionalne varnosti predstavljeni strateški varnostni cilji in usmeritve:

1. podpiranje miroljubne in demokratične Evrope kot enega osnovnih stebrov varnosti in prosperitete ZDA,
2. širitev stabilnosti in varnosti na azijsko-pacifiškem območju,
3. širitev globalne ekonomije,
4. pozicioniranje ZDA kot globalnega mirovnega posrednika in skrbnika,

⁶ Ameriške nacionalne interese lahko razvrstimo v naslednje kategorije, in sicer po prioritetah:

- Prva kategorija je življenjski interes, ki zajema varovanje domovine. Za zaščito tega interesa se lahko uporabijo vse možnosti, ki so na voljo.
- Druga kategorija je kritični interes, kamor spadajo območja in zadeve, ki se ne nanašajo neposredno na preživetje ZDA in nimajo neposrednega vpliva na domovinsko varnost, vendar lahko v daljšem obdobju postanejo prioriteta prve kategorije in ogrožajo vitalni interes ZDA.
- Tretjo kategorijo predstavlja pomembni interes, čigar določeni kazalci nakazujejo, da lahko njegovi elementi postanejo grožnja nacionalnemu interesu.

Vsi ostali interesi so obrobni in so postavljeni na listo opazovanja ter so s strani ZDA deležni malo, če sploh kaj pozornosti (Raščan 2005: 48-49).

5. preprečevanje transnacionalnih groženj, predvsem omejevanje širjenja orožja za množično uničevanje,
6. vzdrževanje in razvijanje ustreznih mehanizmov za doseg vseh ciljev.

Iz strategije nacionalne varnosti je moč razbrati, da so ZDA v obdobju po koncu hladne vojne naredile največjo napako, ker niso identificirale in s tem preprečile največjega varnostnega problema, ki lahko uničujoče deluje na varovanje nacionalnega interesa in na družbene vrednote, in to je mednarodnega terorizma, kar se je nazorno pokazalo 11. septembra 2001. Ti napadi so naznanili začetek novega obdobja, ki narekuje ponovno razmišljanje in konkretne spremembe v ameriški nacionalni politiki, še posebej z upoštevanjem mednarodnega terorizma in domače varnosti⁷.

Spremembe, ki so po napadih sledile v nacionalnovarnostnem sistemu, lahko kronološko razdelim na dve skupini.

Prvo skupino sprememb označuje predvsem *ad hoc* uvajanje varnostnih ukrepov, s katerimi so poskušali kratkoročno preprečiti ponovitev napadov, sanirati območje napadov, stabilizirati družbeno okolje in dvigniti moralo ter zaupanje v družbene vrednote. Med te ukrepe tako štejemo poostren nadzor meje, pristanišč in letališč, vojaško posredovanje v Afganistanu, priprave za vojaško posredovanje v Iraku, sprejetje zvezne zakonodaje, ki varnostnim in sodnim organom bistveno povečuje pooblastila, velikokrat na račun krčenja človekovih pravic, ustanavljanje civilno-družbenih institucij z namenom zaščite prebivalstva, gospodarstva, energetskih virov, itd., vzpostavljanje in aktiviranje varnostnih mehanizmov na ravni zveznih držav in večjih mest (National Strategy of homeland security, 2002). V prvi skupini ukrepov je potrebno posebej omeniti spremembe v strukturi ameriške vlade, in sicer ustanovitev Urada za domovinsko varnost, Sveta za domovinsko varnost in Ministrstva za domovinsko varnost. Vsi trije organi so nastali z namenom enovite koordinacije varnostnih ukrepov v primeru terorističnih napadov. Tako je Urad za domovinsko varnost koordiniral izvajanje nacionalne strategije ZDA. Svet, katerega ustanovitev je

⁷ Tudi pred tem datumom smo bili priča odmevnim »spopadom« med ZDA in terorističnimi organizacijami, in sicer napadu na Svetovni trgovinski center v New Yorku leta 1993, napadu na ameriško vojašnico v Savdski Arabiji leta 1996, napadu na veleposlaništvi ZDA v Keniji in Tanzaniji leta 1998 in povračilnim napadom na bazo Al-kaide v Afganistanu in Sudanu istega leta, napadu na ladjo Cole leta 2000 itd. (Raščan 2005: 61).

sovpadala z Uradom, pa je zagotavljal koordinacijo vseh institucij, ki so povezane z domovinsko varnostjo. Prav tako je namenjen za pospeševanje razvoja in uresničevanja domovinske varnostne politike. Naslednje leto (2002) pa je bilo na podlagi Zakona o domovinski varnosti ustanovljeno ministrstvo za domovinsko varnost, ki igra osrednjo vlogo pri uresničevanju funkcij domovinske varnosti⁸ (Prezelj 2005: 197-201).

Druga skupina ukrepov pa je bolj strateškega pomena in predstavlja spremembe v vseh varnostnih prvinah nacionalnovarnostnega sistema ZDA. Te spremembe so zapisane v Strategiji nacionalne varnosti, ki je nastala septembra 2002. V nasprotju s predhodnimi uradnimi dokumenti na področju nacionalne varnosti, kjer terorizem ni bil obravnavan kot posebna grožnja ta strategija jasno opisuje mednarodni terorizem kot največjo grožnjo ameriškim interesom.

Na področju varnostne politike so se ZDA odločile za dve večji spremembi, in sicer strategijo preventivnega delovanja in možnost samostojnega delovanja. Glede uporabe preventivnega napada si ZDA, kot edina svetovna velesila, prilaščajo monopol nad takšnim napadom, saj bi po njihovem generalizacija preventivnega delovanja privedla do globalne destabilizacije mednarodnega okolja (Raščan 2005: 54). Samostojno delovanje ZDA v mednarodnem okolju pomeni predvsem zmanjševanje političnih kompetenc zaveznikom in črno-belo delitev sveta pod geslom: »Če niste z nami, ste proti nam«. Posledično se tudi mednarodnim organizacijam podeljuje nova vloga. NATO izvršuje že zastavljene naloge, OZN se večinoma uporablja po koncu dogodkov, mednarodni sporazumi so neobvezujoči, v gospodarstvu prihaja do uporabe protekcionističnih ukrepov itd. (Raščan 2005: 57).

V okviru varnostne strukture so posebej vidne spremembe na obrambnem področju, predvsem na vojaškem, kjer pride do vzpostavitve večjih ekspedicijskih sil, enot, namenjenih za specialno delovanje, in protiterorističnih enot. Prav tako pride do spreminjanja strukture ministrstva za obrambo, kjer se vzpostavi posebno poveljstvo za Ameriko; bistveno se poveča proračun. Izjema pa ni niti civilna obramba, saj se

⁸ Najpomembnejše naloge Ministrstva za domovinsko varnost so zapisane v Zakonu o domovinski varnosti, predstavljajo pa preprečevanje terorističnih napadov v ZDA, zmanjševanje ranljivosti ZDA pred terorizmom, zmanjšanje škode in pomoč pri obnovi itd. (Prezelj 2005: 201).

spremeni koncept dojemanja civilne obrambe, in sicer v smeri »nevojaškega« vrednotenja in dojemanja vprašanj nacionalne varnosti (National Security Strategy, 2002; Raščan 2005: 42-43).

Na področju notranje varnosti pride do povečevanja pristojnosti obveščevalnim in varnostnim službam ter konceptualnih in organizacijskih sprememb na obveščevalnem področju, kar pomeni povečevanje medsebojne komunikacije in izmenjavo obveščevalnih informacij, razvijanje novih sistemov pravočasnega opozarjanja in razvijanje novih metod pridobivanja obveščevalnih informacij (National Security Strategy, 2002).

Takšnega preoblikovanja nacionalnovarnostnega sistema v ZDA, kot smo mu priča v zadnjih petih letih, ni bilo že od konca 2. svetovne vojne, ko se je celotni sistem nacionalne varnosti moral prilagoditi prihajajočemu obdobju hladne vojne. Sodobne spremembe kažejo na to, da so ZDA ponovno nedvomno v vojni, vendar je tokrat sovražnik decentraliziran, neviden in lahko ogrozi življenjske interese in vrednote ameriške države in družbe. Vendar ravno te lastnosti današnjega nasprotnika pričajo o prihajajoči dolgotrajnosti spopadov, še posebej, če upoštevamo mnenje nekaterih skeptikov in kritikov do ameriške politike, »da vsakega ubitega terorista nadomestita dva nova.«.

5.2 PRIMER VELIKE BRITANIJE

Združeno kraljestvo Velike Britanije in Severne Irske (kar je uradni naziv države) je v določenem smislu netipična država, kar zadeva njeno geografsko strukturo in dolgo kolonialno ter vojaško tradicijo. Posledica tega dejstva je vedno aktualno vprašanje nacionalne varnosti, ki predstavlja ogrodje nacionalnega interesa oziroma aktivnosti, namenjenih za preprečevanje vseh vrst groženj VB in njenim zaveznikom (Grizold in drugi 1999: 152).

Oblikovanje politike nacionalne varnosti po koncu hladne vojne izvira predvsem iz ocen, da je nevarnost večjega vojaškega spopada minimalna, vendar so se v

novonastalih razmerah pojavile druge nevarnosti, ki lahko ogrozijo nacionalno varnost VB. Te grožnje so predvsem (Grizold in drugi 1999: 156-157):

- viri nestabilnosti v nekaterih evropskih regijah,
- nevarnost, ki jo predstavljajo nekateri politični režimi v svetu,
- širjenje jedrskega, kemijskega in biološkega orožja ter nenadzorovano oboroževanje s konvencionalnim orožjem,
- pojav nekonvencionalnih oblik ogrožanja (droge, organizirani kriminal, nove oblike terorizma, uničevanje okolja in ogrožanje informacijskih mrež).

Vendar se je v obdobju po koncu hladne vojne kot največji varnostni problem v Veliki Britaniji izkazala nerešena situacija v Severni Irski, kjer je kriza trajala že od konca šestdesetih let prejšnjega stoletja. V tem času so se tako na lojalistični kot na republikanski strani pojavile številne nasilne radikalne skupine, ki so svoje politične cilje poskušale doseči predvsem z raznimi terorističnimi akcijami. Največjo nevarnost pa je predstavljala PIRA, ki je od začetka krize izvajala zelo odmevne in krvave teroristične napade, velikokrat tudi v samem središču Londona.

V britanskem nacionalnovarnostnem sistemu je pred napadi 11. septembra 2001 osrednjo vlogo v boju proti terorizmu (predvsem proti severnoirskemu) igrala varnostna služba – MI5. Vendar MI5 nima policijskih pooblastil, zato je zaradi terorizma razvila tesno sodelovanje s policijo in sicer s Posebnim oddelkom (*Special branch*), ki je prevzel izvršno vlogo MI5. Naslednja institucija, ki se ukvarja z bojem proti terorizmu, je Antiteroristični oddelek (*Anti-terrorist branch*), ki spada pod okrilje metropolitanske policije, namenjen pa je za preiskavo terorističnih aktivnosti in predhodno delovanje. V sistemu obveščevalnih služb pa se s terorizmom ukvarjata še Tajna obveščevalna služba (*Secret intelligence service – SIS ali MI6*) in Vladni štab za komunikacije (*Government communications headquarters – GCHQ*), ki pa se primarno ukvarja z zbiranjem podatkov, ki so v obliki signalov – SIGINT (Krunič 1999: 211 – 216).

Po terorističnih napadih 11. septembra 2001 je boj proti mednarodnemu terorizmu postal eden izmed osrednjih prioritet britanske nacionalne varnosti. VB je na pojav te varnostne grožnje odgovorila z izboljšanjem protiterorističnih struktur in prilagajanjem

posameznih prvin nacionalnovarnostnega sistema za soočanje z mednarodno teroristično grožnjo.

Takoj na začetku je britanska vlada odobrila dodatnih 54 milijonov funtov sredstev za obveščevalne službe, vendar je istočasno tudi ugotovila, da obveščevalna skupnost ni uspela realno oceniti nevarnosti, ki jo predstavlja Al Kaida, kar posledično pomeni izpeljavo reorganizacije obveščevalnih služb za bolj kakovostno delovanje na področju boja proti mednarodnemu terorizmu.

Tako so se prve spremembe pokazale z ustanovitvijo novega Skupnega analitičnega centra za terorizem (*Joint terrorism analysis centre – JTAC*), ki formalno deluje v okviru MI5, vendar vključuje strokovnjake iz vseh pomembnih institucij in združuje vse obveščevalne informacije, ki se navezujejo na terorizem na enem mestu in v eni organizacijski strukturi. Glavna naloga JTAC je prevzem izvajanja analitične faze obveščevalnega procesa celotne obveščevalne skupnosti, da bi zagotovili širši izbor obstoječih obveščevalnih podatkov, kar naj bi pripeljalo do enotnih končnih obveščevalnih izdelkov (National intelligence machinery 2000: 13).

Naslednja organizacijska sprememba je bila vzpostavitev, Mednarodne policijske protiteroristične enote (*Police international counter terrorist unit – PICTU*), ki igra pomembno vlogo pri pravočasnem posredovanju končnih obveščevalnih informacij ustreznim uporabnikom. Prav tako sodeluje pri koordinaciji operacij v boju proti mednarodnemu terorizmu.

Drugi sklop sprememb se je navezoval predvsem na sprejemanje ustrezne protiteroristične zakonodaje. Vendar je zaradi izkušenj s pojavom terorizma, ki jih je VB imela pred zlovesčim 11. septembrom, v svojo zakonodajo že vgradila določene zakone, ki so predvidevali posamezne protiteroristične ukrepe⁹. Leta 2000 pa je bil sprejet en sam zakon, in sicer Zakon o terorizmu (*The Terrorism act*), ki je podrobno opredeljeval ukrepe za zajezitev terorizma in posamezna izredna pooblastila, ki so omogočala varnostnim organom prijetje osumljencev. Problem obstoječe zakonodaje je predstavljajo dejstvo, da so bili ti zakoni namenjeni predvsem zoperstavljanju

⁹ Zakon o Severni Irski (Northern Ireland /emergency provisions/ acts – NIEPA) in Zakon o preprečevanju terorizma (Prevention of terrorism /temporary provisions/ acts – PTA).

notranjemu terorizmu in ne veliko bolj kompleksnemu mednarodnemu terorizmu. Zato je vlada VB sprejela posamezne spremembe obstoječe zakonodaje, ki pa velikokrat posegajo na področje temeljnih človekovih pravic, kar vzbuja dvome v smiselnost sprejetih sprememb. Tako je bil oktobra 2001 kot prvi sprejet Zakon o antiterorizmu, kriminalu in zagotavljanju varnosti (*Anti-terrorism, crime and security act – ATCSA*), ki omogoča neomejen pripor, in sicer brez sojenja, za imigrante, ki jih ni mogoče deportirati, vendar predstavljajo resno grožnjo za nacionalno varnost VB in so osumljeni kot mednarodni teroristi.

Drugi pomembni zakon, Zakon o državljanstvu, imigracijah in azilu (*Nationality, immigration and asylum act – NIAA*), omogoča notranjemu ministrstvu, da državljanu, ki s svojim dejanjem resno ogrozi vitalne interese VB ali britanskih prekomorskih ozemelj, odvzame državljanstvo.

Tretji vidik britanskega odgovora na nastale razmere zajema predvsem povečanje fizičnega varovanja pomembnih zgradb, letališč in transportnih centrov. Za potrebe informiranja vlade in zasebnega sektorja o varnostnih ukrepih je bila ustanovljena Pisarna za nacionalno protiteroristično dejavnost in varnost (*National counter terrorism and security office – NaCTSO*), katere glavni namen je svetovanje pri oteževanju dostopnosti do posameznih potencialnih tarč in oblikovanju kriznih načrtov.

V britanskem protiterorističnem delovanju igra pomembno vlogo tudi vojska, ki s svojim udejstvovanjem v Afganistanu in Iraku sodeluje pri uničevanju infrastrukture terorističnih organizacij in pri preprečevanju terorističnih operacij. Prav tako vojska igra svojo vlogo tudi na domačih tleh, kjer izvaja priobalne patrulje, vzdržuje visoko stopnjo pripravljenosti v letalskih silah in sodeluje s civilnimi institucijami pri izvajanju poostrelega nadzora (Bamford 2004: 742-751).

Če pa želi VB smiselno uporabiti nove ukrepe zagotavljanja protiteroristične varnosti, je potrebno identificirati posamezne akterje mednarodnega terorizma. Bamford jih razdeli v tri kategorije (Bamford 2004: 739-740):

- Največjo teroristično grožnjo predstavlja Al Kaida, ki je uspela vzpostaviti obširno, fleksibilno in tajno mrežo posameznih islamskih terorističnih skupin in

njihove posamične interese združiti v veliko širši ideološki kontekst, ki se predvsem navezuje na boj med islamom in zahodnimi vrednotami.

- Drugo veliko nevarnost predstavljajo teroristične organizacije z območij severne Afrike, kjer prednjačita predvsem dve alžirski organizaciji (oborožena islamska skupina – GIA in salafistična skupina – GSPC). Ti dve organizaciji ravno zaradi povezav z Al Kaido predstavljata eno izmed osrednjih nevarnosti za Evropo, kar se kaže v izvedbi terorističnih dejanj v Franciji.
- Tretjo skupino predstavljajo teroristi posamezniki oziroma »amaterji«, ki podpirajo cilje skrajnih islamskih gibanj z Osamo bin Ladnom na čelu, vendar nimajo neposrednih povezav z drugimi terorističnimi organizacijami ali mrežami. Ti teroristi so še posebej nevarni ravno zaradi samostojnosti delovanja, kajti obveščevalni in varnostni organi jih zelo težko odkrijejo.

Britanci se že tri desetletja soočajo z nevarnostjo terorističnih aktivnosti, predvsem tistih, ki izvirajo iz severnoirske krize. Prav tako so bili tudi žrtve več mednarodnih terorističnih napadov, ki pa v večini primerov niso bili uperjeni neposredno proti njim.¹⁰ Vendar dogodki po 11. septembru 2001 in vključenost britanskih sil v vojaške operacije v Afganistanu in Iraku kažejo na to, da bo tudi VB postala stalna tarča mednarodnega terorizma, kar se je pokazalo julija 2005 s serijo bombnih eksplozij v Londonu. Tako prvič v zgodovini mednarodni terorizem predstavlja daleč največjo nevarnost Veliki Britaniji, njenim prebivalcem in njihovim vrednotam.

5.3 PRIMER RUSKE FEDERACIJE

Spremembe, ki jih je povzročil terorizem na nacionalnovarnostnem sistemu Ruske federacije, bi lahko razdelili na štiri posamezna obdobja. Mejnike med obdobji so zmeraj predstavljali odmevni teroristični napadi, ki so prisili oblast, da je sprožila val ukrepov in reform, s katerimi so poskušali popraviti neuspehe in nepripravljenost sistema nacionalne varnosti na soočanje s terorizmom.

¹⁰ Primer je bombni napad na ameriško letalo Pan Am, let 103, ki je eksplodiralo nad škotskim mestecem Lockerbie, v katerem je umrlo 270 ljudi.

5.3.1 OBDOBJE PRED NAPADI 11. SEPTEMBRA 2001

Eden temeljnih pravnih aktov, ki določa delovanje ruskega sistema nacionalne varnosti, je Zakon o varnosti iz leta 1992. V njem je zapisano, da varnostni sistem RF sestavljajo organi zakonodajne, izvršne in sodne veje oblasti. Prav tako so vključene državne, družbene in druge organizacije ter združenja in seveda državljani, ki sodelujejo pri zagotavljanju varnosti. Pomembna je tudi zakonodaja, ki določa odnose na varnostem področju (Purg 2001: 106).

Leta 1997 je ruska vlada objavila »koncept nacionalne varnosti Ruske federacije«, ki opredeljuje temeljne smernice razvoja ruske varnostne politike, in sicer na področju zagotavljanja varnosti oseb, družbe in države ter zaščite države in njenih interesov pred zunanjimi in notranjimi viri ogrožanja.¹¹

Med nacionalnimi interesi, ki so opredeljeni v tem dokumentu, prevladujejo ekonomski, saj je kompleksno reševanje problemov, možno samo v primeru stabilnega gospodarstva. Druga skupina nacionalnih interesov izvira z notranjepolitičnega področja, kjer je glavna naloga države ohranitev stabilnosti ustavne ureditve, oblasti in njenih institucij, vzpostavitve pravne države ter promocija demokratičnih vrednot. Eden pomembnih nacionalnih interesov pa je zaščita oseb, družbe in države pred mednarodnim terorizmom. Tako organi oblasti preganjajo osebe, ki so nekako povezane s terorizmom, tudi v primeru, ko se teroristične akcije pripravljajo in izvajajo izven območja RF, vendar škodijo njenim interesom.

Za uspešno realizacijo nacionalnih interesov, pa je potrebna sposobnost RF, da svoje politične, ekonomske in socialne probleme rešuje samostojno. Prav tako mora zagotoviti takšno stopnjo življenjske ravni lastnega prebivalstva, ki bo zagotavljalo nacionalno soglasje in posledično tudi družbeno-politično stabilnost v državi.

V poglavju, ki navaja vire ogrožanja varnosti RF, se pogosto omenjajo aktivnosti organiziranega kriminala in terorističnih organizacij. Na tej podlagi se oblikuje tudi

¹¹ Koncept nacionalne varnosti RF je bil zaradi spremenljivih razmer spremenjen in dopolnjen leta 2000.

posebna vsedržavna struktura, ki s paleto ukrepov in sodelovanjem posebnih služb RF deluje v smeri zmanjševanja ranljivosti v primeru terorističnega napada in v smeri zmanjševanja verjetnosti napadov.

Za učinkovit boj proti mednarodnemu terorizmu pa je potrebno sodelovanje vseh elementov nacionalnovarnostnega sistema, ki so usmerjeni v zagotavljanje varnosti oseb, družbe in države (Grizold, Ferfila 2000: 100-115).

Dojemanje novih virov ogrožanja ruske nacionalne varnosti, predvsem mednarodnega terorizma, se je zlasti manifestiralo leta 1998, ko je bil sprejet Zakon o boju proti terorizmu. Ta zakon določa osnovna načela, na katerih temelji delovanje nacionalnovarnostnega sistema v boju proti terorizmu. Nadalje navaja tiste elemente sistema nacionalne varnosti, ki so osnovni nosilci protiterorističnega delovanja. To so: Zvezna varnostna služba, Ministrstvo za notranje zadeve, Zunanja obveščevalna služba, Zvezna služba za zaščito, Ministrstvo za obrambo in Zvezna mejna služba (Federalnij zakon Rossijskoj Federaciji o borjebе s terorizmom, 1998).

V zakonu je opredeljena tudi zvezna antiteroristična komisija, ki koordinira delo omenjenih institucij in oblikuje predloge uradnih dokumentov s področja protiterorističnega delovanja. Vendar pa pri svojem delu ta komisija nima nikakršnih pooblastil, s katerimi bi lahko pritiskala na vladne institucije in jih vzpodbudila ali prisilila k sodelovanju.

Tako zakon v primeru terorističnega napada namesto institucionaliziranega osrednjega organa, ki bi prevzel vodenje protiteroristične dejavnosti, opredeljuje vzpostavitev *ad hoc* operativne skupine. Problemi pri delovanju te skupine so se začeli kazati v dejanskih akcijah, ki so se zaradi nekoordinacije, različnih interesov, neusposobljenosti in hitrega menjavanja poveljujočih končale dokaj klavrno in z visokim številom mrtvih civilistov in pripadnikov oboroženih enot.

5.3.2 OBDOBJE MED 11. SEPTEMBROM 2001 IN ZAJETJEM TALCEV V MOSKOVSKEM GLEDALIŠČU (23. DO 26. OKTOBRA 2002)

V tem času pride v Ruski federaciji do okrepitve mednarodnega sodelovanja na področju boja proti mednarodnem terorizmu. RF se vključi v protiteroristično koalicijo in podpre vojaško intervencijo v Afganistanu. Prav tako pride do vzpostavitve bolj kakovostnih odnosov med RF in nadnacionalnimi organizacijami (NATO, EU, Šanghajska zveza) ter posameznimi državami (ZDA). RF začne podpirati boj proti terorizmu na nivoju mednarodnih organizacij, kjer prednjači Skupnost neodvisnih držav (SND). Rusija da pobudo za bolj integriran boj proti terorizmu in v tem duhu predlaga spremembe protiterorističnega centra SND. Prav tako pride do krepitev koordinacije stalnih predstavnikov posebnih služb v državah SND, ki bi koordinirali protiteroristično dejavnost SND in delovali v okviru skupnih protiterorističnih vaj in srečanj (Purg 2004: 167).

Nadalje RF vzpostavi komite za finančni monitoring, ki je kot zvezni organ vgrajen v Ministrstvo za finance. Njegova osrednja naloga je spremljanje finančnih transakcij sumljivega porekla, posredovanje ustreznih informacij pristojnim organom in sodelovanje s podobnimi institucijami v tujini (Purg 2004: 167).

5.3.3 OBDOBJE MED 26. OKTOBROM 2002 IN ZAJETJEM TALCEV V BESLANU (1. DO 3. SEPTEMBRA 2004)

Novejše spremembe v nacionalnovarnostnem sistemu so se zgodile po katastrofi v Moskvi, ko so teroristi zasedli gledališče in v njem zadrževali večje število talcev. Takratno posredovanje ruskih sil za posebno delovanje se je končalo z več kot 160 mrtvimi, ki so bili večinoma talci.

Kmalu po drami v gledališču je ruski predsednik Putin zahteval korenite reforme sistema nacionalne varnosti, še posebej v obveščevalno-varnostnem sistemu. Prvi ukrepi so prinesli spremembe v koordinaciji organov in služb, v pristojnosti katerih je delovanje proti organiziranemu kriminalu in terorizmu. Takrat to funkcijo začasno prevzame Generalštab oboroženih sil RF.

Nadaljnje spremembe so se navezovale predvsem na delovanje obveščevalnih in varnostnih služb. Pride do ukinitve Zvezne mejne službe in Zvezne agencije vladnih zvez in informacij (FAPSI). Na račun ukinitve teh dveh služb največ pridobi Zvezna varnostna služba (FSB), ki prevzame pooblastila in oborožene enote mejne službe. Pooblastila in organi FAPSI pa preidejo tako na FSB kot na SVR.

Zaradi povezav FSB-ja s kabinetom predsednika RF, prevzame FSB glavno vlogo pri protiterorističnem delovanju. Sicer je tudi v preteklosti primarno deloval v boju proti terorizmu, predvsem z antiterorističnim centrom na čelu, ki ima korenine še v antiterorističnem oddelku bivšega KGB.

Istočasno postane Ministrstvo za notranje zadeve drugi najpomembnejši akter v protiterorističnem delovanju. Pridobi pooblastila za delovanje na območju severnega Kavkaza in na zveznem nivoju, kjer ustanovi lasten antiteroristični center, imenovan »T« (Soldatov, Borogan 2005: 3).

V prvi polovici leta 2003 ministrstvo RF za tisk, televizijo in sredstva množičnih komunikacij predstavi Protiteroristično konvencijo¹². Bistvo te konvencije je, da imajo sredstva javnega obveščanja sicer pravico in tudi dolžnost sodelovati pri javnih obravnavah problemov terorizma, obveščati javnost o poteku protiterorističnih akcij itd., vendar morajo pristati na določene omejitve, ki preprečujejo, da bi se teroristi okoriščali s posredovanimi informacijami, da bi izkoriščali javne medije za promocijo lastnih idej, da ne bi prišlo do ogroženosti protiterorističnih akcij in s tem tudi do ogroženosti življenj morebitnih talcev in pripadnikov posebnih enot itd. (Purg 2004: 167-169).

5.3.4 OBDOBJE OD 3. SEPTEMBRA 2004 DO DANES

Predsednik Putin je takoj po krizi v Beslanu podpisal uredbo, v kateri je zahteval reformo tistih institucij, ki so neposredno sodelovale pri izvedbi protiteroristične akcije in se niso izkazale. Vendar se ta sprememba ni pokazala kot učinkovita, saj je prišlo

¹² Pravila ravnanja sredstev množičnega informiranja v primerih terorističnega dejanja in protiteroristične operacije.

samo do lepote popravkov znotraj posameznih institucij¹³ in ne do izboljšanja medsebojne komunikacije in poenostavitve organizacijskih struktur.

Edina pozitivna izjema, ki zadeva vsebinske spremembe, se je pokazala na območju severnega Kavkaza, kjer je prišlo do poenotenja interesov in delovanja posameznih vladnih organov. Vendar je enotnost delovanja v protiterorističnem boju vodila v radikalizacijo posameznih ukrepov. Ustanovljene so bile posebne enote, ki so izvajale neposredne likvidacije prepoznanih teroristov. Prav tako so se posluževale drugih vprašljivih taktik, kot so na primer povratne ugrabitve¹⁴.

Svojo vlogo pri radikalizaciji postopkov vladnih organov pa igra tudi ruska дума, ki po hitrem postopku sprejema nove zakone in amandmaje k obstoječim, s katerimi daje zakonsko podlago za uporabo vprašljivih metod protiterorističnega delovanja. Zakonodaja pa povečuje pooblastila v boju proti terorizmu tudi drugim organom prisile. Tako lahko ruska vojska napade »zavetišča« teroristov tudi izven državnih meja; v primeru ugrabitve potniškega letala ali ladje ima vojska pooblastila, da letalo ali ladjo sestrelji oziroma uniči, in sicer ne glede na civilne žrtve.

Kljub vsem napovedanim spremembam znotraj nacionalnovarnostnega sistema, je bil po krizi v Beslanu le majhen del sprememb dejansko izveden. Ne glede na ugotovitev, da je za uspešno zoperstavljanje terorizmu bistvenega pomena zvezna koordinacija vseh vladnih institucij in medsebojno izmenjavanje informacij, do tovrstnega organa še zmeraj ni prišlo.

Prav tako obveščevalne in varnostne službe niso sposobne strateškega delovanja in analiziranja, kar posledično pomeni, da se celotni sistem namesto s preventivo terorizma ukvarja s kurativo.

V protiterorističnem boju se vse pogostejše uporabljajo vprašljive metode, ki globoko posegajo na področje človekovih pravic, istočasno pa v skrajnost silijo tiste družbene skupine, ki so bile do sedaj bolj zmerne (Soldatov, Borogan 2005: 10-11).

¹³ Tako so se v FSB vsi oddelki preimenovali v službe, na Ministrstvu za notranje zadeve pa so se direktorati preimenovali v oddelke.

¹⁴ Vladne enote ugrabijo družinske člane teroristov in jih s tem poskušajo prisiliti v pogajanja in izpustitev talcev (Soldatov, Borogan 2005: 7-9).

Če bo RF v prihodnosti želela odpraviti terorizem kot osrednjo grožnjo nacionalne varnosti, bo morala odpraviti omenjene napake, kar pa ne bo lahko, saj so v nacionalnovarnostnem sistemu še zelo prisotni elementi sistema SZ, in kar je še večji problem, Rusija v obdobju po koncu hladne vojne ni uspela v celoti spremeniti filozofije delovanja in uporabe organov, ki zagotavljajo nacionalno varnost. Tako vse prepogosto pretirano uporablja konvencionalne oborožene sile v boju proti nekonvencionalnemu nasprotniku, ki vsako potezo ruske oblasti obrne v svojo korist.

5.4 PRIMER IZRAELA

Nacionalnovarnostni sistem Izraela se že od svojega nastanka leta 1948 srečuje z dvema grožnjama nacionalne varnosti, ki ogrožata eksistenco države. Prva grožnja je vojaški spopad s koalicijo arabskih držav, ki se je do sedaj zgodil štirikrat in vsakič je zmagal Izrael, saj bi morebitni drugačen izid vojne pomenil prenehanje obstoja Izraela.

Drugo obliko ogrožanja varnosti pa predstavlja terorizem, ki ga izvajajo skrajne islamske skupine, katerih cilj je prav tako uničenje Izraela in vzpostavitev palestinske države. Kot podporniki terorizma pa so se v zgodovini vse do danes pokazale nekatere države (Iran, Sirija, Irak itd.), pa tudi avtonomna palestinska oblast. Vendar pri nevarnosti terorizma prav tako ne smemo izpustiti skrajnih judovskih gibanj, ki s svojim delovanjem pogosto podpihujejo izraelsko-arabski spor in velikokrat ogrožajo varnost Izraela, njegovega sistema in družbe (atentat na premiera Itzaka Rabina leta 1995).

Zaradi dolgotrajne prisotnosti pglavitnih dveh virov ogrožanja se je v smeri zagotavljanja varnosti izoblikoval specifičen nacionalnovarnostni sistem. Predvsem kar zadeva boj proti terorizmu, lahko opredelim štiri osrednje elemente sistema nacionalne varnosti, ki so nosilci protiterorističnega delovanja in se vsebinsko dopolnjujejo.

Prvi element je izraelska vojska (*Israel defence force – IDF*), ki v protiterorističnem delovanju uporablja tako konvencionalne kot nekonvencionalne enote in metode bojevanja. Glavna področja aktivnosti izraelske vojske so zasnovana na (Grizold in drugi 1999: 224):

1. visoki stopnji pripravljenosti v primeru vojne,
2. antiteroristični kampanji,
3. boju proti palestinskim/muslimanskim terorističnim skupinam;
4. izgradnji oboroženih sil za primer oboroženih spopadov.

Znotraj vojske so pomembne enote za posebno delovanje, katerih primarna naloga so protiteroristične aktivnosti. Pripadniki teh enot delujejo tajno, nosijo arabska oblačila, se učijo dialektov na specifičnem območju, da bi bili čim bolj neopazni. Njihova naloga je predvsem zbiranje obveščevalnih podatkov in izvajanje tajnih akcij, ki pogosto pomenijo eksekucije posameznih pripadnikov terorističnih skupin.

V devetdesetih letih je Izrael uradno priznal obstoj dveh takšnih enot, imenovanih *Duvdevan* (Češnja) in *Shimshon* (Samson), ki sta delovali in še delujeta na avtonomnih palestinskih ozemljih (Gaza, Zahodni breg). Naslednja enota za posebno delovanje je t. i. Sayeret Matkal (izvidniška enota glavnega štaba), ki pa je namenjena za delovanje izven Izraela. V praksi se je večkrat izkazala v reševanju talcev iz ugrabljenih letal. Sicer pa ta enota spada pod okrilje vojaške obveščevalne službe Aman. Prav tako imata tudi mornarica in letalstvo svoje posebne enote, ki igrajo pomembno vlogo v boju proti terorizmu, predvsem kar zadeva reševanje talcev, izvidniške naloge in napade na posamezne teroristične centre in skrivališča (Eshel 2002: 21).

Drugi element nacionalnovarnostnega sistema, ki je angažiran v antiterorističnem delovanju, je civilna obramba, katere naloga je zaščita državljanov in premoženja v primeru terorizma in vojne. Civilna obramba izvaja pasivne ukrepe, ki preprečujejo vdor teroristov na izraelska poseljena območja. Prav tako ima v svoji sestavi posebne enote, namenjene odnosom z javnostjo. Njihova vloga je izvajanje informacijske cenzure, predvsem v času poteka vojaških akcij, vzdrževanje stika med izraelsko vojsko in javnostjo, nadzor nad mediji in dvigovanje morale v primeru izrednih razmer (Grizold in drugi 1999: 224).

Tretji element protiterorističnega boja so organi notranje varnosti, med katerimi prednjači obveščevalna skupnost¹⁵. Med obveščevalnimi službami je glavni nosilec boja proti terorizmu Shin Beth, ki opravlja to nalogo že od leta 1967, in sicer od tretje izraelsko-arabske vojne. Znotraj Shin Betha obstaja odsek za arabske zadeve, ki je specializiran za protiteroristično delovanje. Njegova naloga je vzpostavitev agenturne mreže na avtonomnih palestinskih ozemljih in v obmejnih območjih sosednjih držav, s pomočjo katere pridobijo obveščevalne podatke o aktivnostih terorističnih organizacij. Kadar pa sledi o terorističnih aktivnostih vodijo v druge države, glavno breme zbiranja podatkov in protiterorističnega delovanja prevzame Mossad. Prav tako tudi Aman deluje v boju proti terorizmu, predvsem preko že omenjenih enot za posebne naloge (Kahana 2002).

Zadnji element nacionalnovarnostnega sistema, ki igra pomembno vlogo v protiterorističnem delovanju in daje smisel že omenjenim elementom, pa je strategija boja proti terorizmu. Tako lahko izraelske protiteroristične aktivnosti razdelimo v tri kategorije ukrepov, in sicer na operativne oziroma ofenzivne, defenzivne in kaznovalne ukrepe (Eshel 2002; Ganor; Gazit 2002):

- Ofenzivne ukrepe izvajajo vojska in varnostne organizacije, in sicer proti terorističnim ciljem na njihovih območjih. Namen preventivnega delovanja je onemogočiti teroristično delovanje v fazi pripravljanja posameznih napadov. Za izvajanje ofenzivnih ukrepov se uporabljajo številne metode delovanja, od povsem konvencionalnih metod pa do nekonvencionalnega izvajanja tajnih operacij. Med konvencionalne metode spada zlasti uporaba zračnih sil za napade na poveljniške centre, poligone, skladišča, komunikacijske centre itd. V primeru, da se objekti terorističnih skupin nahajajo v gosto naseljenih ali težko dostopnih področjih, se za napade na te objekte uporabljajo kopenske

¹⁵ Obveščevalno skupnost Izraela sestavljajo naslednje službe: Mossad (Inštitut za obveščevalne in posebne naloge, *ha-Mossad le-Modiin ule Trafkidim Meyuhadim*), ki deluje v tujini, kamor spadajo vse države arabskega sveta; Shin Beth (Splošna varnostna služba, *Sherut ha-Bitacjon ha-Klali*), katere osnovni nalogi sta protiobveščevalna dejavnost in protiteroristična dejavnost (vključno s terorizmom, ki izvira iz palestinskih ozemelj); Aman (vojaška obveščevalna služba, *Agaf ha-Modi'in*), ki pridobiva obveščevalne podatke za potrebe vojske, prav tako pa deluje na palestinskih ozemljih in v sosednjih državah; Mamad (Center za politične raziskave Ministrstva za zunanje zadeve) spremlja politične procese predvsem na področju Bližnjega vzhoda (Požun 2004; Grizold in drugi 1999).

enote¹⁶. Ofenzivni ukrepi se izvajajo tudi s pomočjo mornarice, predvsem, kar zadeva napade na pristanišča in plovila, ki jih uporabljajo teroristi. Prav tako pa se mornarica uporablja za ognjeno podporo v primeru letalskih in kopenskih operacij.

- Defenzivni ukrepi so namenjeni zadrževanju in oteževanju posameznih poskusov terorističnih napadov. Trenutno najbolj ambiciozni in najdražji defenzivni ukrep je izgradnja razmejitvene cone, ki bo vključevala razmejitveni zid, sistem za zgodnje opozarjanje, zračni nadzor nad območjem in patrolje. Vendar so kljub vsem ukrepov najboljša preventiva pravočasne in natančne obveščevalne informacije. Defenzivni ukrepi so namenjeni tudi zmanjševanju škode pri morebitnih napadih, kar je koristno predvsem pri identifikaciji samomorilskih napadalcev in njihovih tarč.
- Kaznovalne ukrepe sestavljajo kazenskopravne aktivnosti, katerih namen je kazenski pregon načrtovalcev, izvajalcev in podpornikov terorističnih operacij. Takšni ukrepi vsebujejo aretacije, pripore, izgone, rušenje hiš obsojenih teroristov itd. Na samem ozemlju Izraela pa ti kaznovalni ukrepi odvrčajo državljane, da bi posegali po terorističnih metodah. Eshel med kaznovalne ukrepe dodaja tudi izvajanje atentatov na posamezne visoke predstavnike terorističnih organizacij. Vendar je umestitev načrtnih umorov med kaznovalne ukrepe lahko sporna, predvsem zato, ker te obsodbe in izvršbe potekajo v tajnosti in niso v pristojnosti sodišč. Tako bi jih bilo bolj smotrno umestiti med ofenzivne ukrepe, saj so predvsem preventivnega značaja in njihov namen je posredovati v strukturo terorističnih organizacij in onemogočiti njihovo normalno delovanje.

Nacionalnovarnostni sistem Izraela se je pet desetletij razvijal v smeri zoperstavljanja terorizmu. Uspešnost tega boja se kaže predvsem v razvoju izraelske ekonomije in dejstvu, da terorizem nima bistvenih učinkov nanjo. Nadalje se je v tem času izraelsko prebivalstvo podvojilo, prav tako je uspešno protiteroristično delovanje uspelo prepričati nekatere osrednje palestinske organizacije (PLO, Fatah), da opustijo teroristične aktivnosti; zadnji dokaz

¹⁶ Primer takšnega posredovanja je bila operacija Obrambni ščit (Defensive shield), kjer so sile v velikosti divizije obkolile široko območje na Zahodnem bregu, ga preiskale in uničile večino palestinske teroristične infrastrukture (Eshel 2002: 20-21).

uspešnega delovanja izraelskega sistema nacionalne varnosti so bile širitve izraelskih naselij na okupiranih območjih (Gazit 2002: 254-255).

Vendar dogodki zadnjih nekaj let kažejo na potrebo po spremembi v strategiji boja proti terorizmu. Izselitev izraelskega prebivalstva z območja Gaze, večanje palestinske avtonomije, ponovni splošni upor Palestincev, imenovan intifada »Al-aqsa«, in zmaga Hamasa na palestinskih volitvah kažejo na novo teroristično grožnjo, ki pa bolj spominja na vojno med dvema državama in dvema narodoma in terja od Izraela, da spremeni obstoječe metode delovanja proti terorizmu.

6 VLOGA OBVEŠČEVALNIH SLUŽB V BOJU PROTI MEDNARODNEMU TERORIZMU

6.1 PRIMER AMERIŠKE OBVEŠČEVALNE SLUŽBE CIA (*Central Intelligence Agency*)

Celotno obdobje devetdesetih let v času po koncu hladne vojne je sledilo globalnim spremembam, ki so nakazovale preobrat od geopolitike h geoekonomiji. Temu trendu se je prilagodila tudi celotna ameriška obveščevalna skupnost, s Cio na čelu. Tako se je vedno bolj poudarjala ekonomsko konkurenčna obveščevalna dejavnost, medtem pa je bila klasična, tj. državna obveščevalna dejavnost, rahlo zapostavljena (Raščan 2005: 47).

Zaradi neprilagojenosti novim političnim razmeram in večjega števila afer se je sredi devetdesetih let Cia znašla v resni krizi, zaradi katere so bili vse glasnejši posamezni politiki, ki v Cii niso videli potenciala za soočanje s sodobnimi izzivi in so želeli bistveno zmanjšati pristojnosti in obseg nalog. Ravno zaradi obstoječe krize, ki se je širila na celotno ameriško obveščevalno skupnost, je kongres leta 1994 ustanovil posebno komisijo¹⁷, z namenom, da bi reorganizirali obveščevalno skupnost. Ugotovitve te komisije so nekako povzemale takratno stanje v mednarodnem in nacionalnem okolju, kjer je obstajala potreba po novem in fleksibilnem obveščevalnem sistemu. Za dosego takšnega sistema so predlagali medsebojno sodelovanje obveščevalnih in varnostnih služb, predvsem preko Sveta za nacionalno varnost, glavnega koordinacijskega organa. Tovrstno sodelovanje naj bi pokrivalo tiste grožnje, ki predstavljajo vedno večjo neposredno nevarnost ameriški družbi, kot sta organizirani kriminal in terorizem. Druga pomembna ugotovitev se je navezovala na dejstvo, da prihaja do radikalnih sprememb v načinu vojskovanja, zato postane obveščevalna podpora Pentagona tako doma kot v tujini najvišja prioriteta ameriških obveščevalnih služb (Warner in McDonald 2005: 33-35).

Dejstvi, da je Cia v svoji sestavi že imela protiteroristični center, ki je deloval predvsem na operativni ravni, vendar vsaj do takrat ni bilo zaslediti večjih

¹⁷ Aspin-Brownova komisija je dobila ime po bivših obrambnih ministrih Lesu Aspinu in Haroldu Brownu, ki sta to komisijo tudi vodila.

interdisciplinarnih analiz, in delovna usmeritev Cie preko državnih meja, kar je še okrepilo njeno sodelovanje s Pentagonom, predvsem na kriznih območjih, sta omogočili ponovno vzpostavitev (primerne) vizije za delovanje v prihodnjem obdobju (Warner in McDonald 2005: 35; Raščan 2005: 88).

Dogodki 11. septembra 2001 pa so ponovno privedli do preiskav, da bi ugotovili, kaj je v obveščevalni skupnosti in še posebej v Cii zatajilo, da je lahko prišlo do tako hude katastrofe. Preiskava, ki je bila usodna za preoblikovanje obveščevalne skupnosti, je potekala pred neodvisno nacionalno komisijo o terorističnih napadih na Združene države (9/11 komisija). Na podlagi ugotovitev¹⁸ te komisije so vzpostavili institucijo direktorja za nacionalno obveščevalno dejavnost (*Director of national intelligence*), ki je prevzel vse pristojnosti v zvezi z delovanjem in koordiniranjem celotne obveščevalne skupnosti, do sedaj v pristojnosti direktorja centralne agencije (*Director of central intelligence*). Prav tako se je tudi ta funkcija preimenovala, in sicer v direktorja Centralne obveščevalne agencije (*Director of Central intelligence agency*), ki je sedaj odgovoren samo za vodenje Cie. Nadalje so na nacionalni ravni, in sicer neposredno pod direktorjem za nacionalno obveščevalno dejavnost, vzpostavili Nacionalni protiteroristični center, katerega glavni namen je analiziranje delovanja domačih in tujih terorističnih organizacij in izdelava strateških načrtov za boj proti terorizmu. Tako je Nacionalni protiteroristični center postal »hibridna« organizacija, ki naj bi vzpostavila medsebojno sodelovanje raznih obveščevalnih in varnostnih organizacij, vsaj na področju protiterorističnega boja (Warner in McDonald 2005: 37-38; Negroponte 2006: 6).

Z vzpostavitvijo novih nacionalnih obveščevalnih institucij, ki so neposredno podrejene Beli hiši, je Cia nedvomno izgubila velik delež svojega političnega vpliva. Na podlagi novega zakona, ki ureja ameriško obveščevalno organiziranost, pa ima Cia nova področja delovanja, in sicer (*Intelligence reform and terrorism prevention act, 2004*):

¹⁸ Številni zaključki te komisije so veljali kot smernice pri sprejemanju nadaljnjih strateških dokumentov in zakonov (*National strategy for homeland security – 2002, The national security strategy of the USA – 2002, National strategy for combating terrorism – 2003, Intelligence reform and terrorism prevention act of 2004, The national intelligence strategy of the USA – 2005*), ki so opredeljevali vsebinsko in organizacijsko reformo obveščevalne skupnosti.

- Zbiranje obveščevalnih informacij, predvsem preko uporabe človeških virov (HUMINT), vendar brez policijskih pooblastil.
- Analiziranje in posredovanje obveščevalnih informacij, ki se navezujejo na nacionalno varnost.
- Vzpostavitev ustreznega sistema usmerjanja in koordinacije za zbiranje obveščevalnih podatkov izven državnih meja, v sodelovanju z vsemi drugimi institucijami, ki imajo pooblastilo za obveščevalno delovanje izven ozemlja ZDA.
- Opravljanje drugih nalog, ki jih opredelita direktor za nacionalno obveščevalno dejavnost in predsednik ZDA.

V nadaljnjem procesu reorganizacije so znotraj organizacijske strukture Cia uvedli novo tajno obveščevalno strukturo, imenovano Nacionalna tajna služba (*National clandestine service*), katere glavni namen je centralizirati vse aktivnosti zbiranja obveščevalnih podatkov preko človeških virov, in sicer na nacionalni ravni (CIA press releases and statements, 2005). Tako je Cia ne glede na relativno izgubo politične moči znova vzpostavila močno osrednjo pozicijo v celotni obveščevalni skupnosti (Goss, 2005b). Vendar celotna matrica tajnega zbiranja obveščevalnih podatkov še vedno izvira iz obdobja hladne vojne, zato se tudi na tem področju uveljavljajo spremembe. V času hladne vojne je bila glavna naloga operativnih agentov poiskati primeren vir informacij, kasneje pa to osebo prepričati, da postane vohun za Cio. Ta sistem je dokaj uspešen, ko je potrebno pridobiti informacije o delovanju in namenih »nasprotne« vlade ali države, saj obstaja veliko potencialnih virov, ki so pripravljeni na sodelovanje. Kar pa zadeva mednarodni terorizem, tovrstni pristopi ne delujejo, saj je zelo težko stopiti v stik s posameznikom, ki bi želel sodelovati z obveščevalno službo in prenašati informacije o delovanju teroristične organizacije. Zato bo Cia morala v določeni meri spremeniti metodologijo pridobivanja podatkov. To pomeni razvijanje novih krink, novih pristopov za približanje potencialnim virom, novih metod komuniciranja in načinov zaščite agentov, ki bodo izvajali te potencialno nevarne naloge (Hulnick 2006: 312).

Spremembe so opazne tudi v samem načinu delovanja organizacije in njenih agentov. Prve novosti so se pojavile pri procesu rekrutacije, kjer se veliko truda namenja za pridobivanje mladih in kakovostnih kadrov. Za izvajanje operativnih

zadev pa so primerne tudi osebe iz tujine. Za usposabljanje ustreznih kadrov pa je v postopku tudi ustanovitev posebne univerze za obveščevalno dejavnost. Če si je Cia uspela zagotoviti stalen priliv kakovostnih mladih ljudi, pa je do pred kratkim imela težave pri zaposlovanju starejših ljudi, ki so zaradi svojih izkušenj bistvenega pomena za protiteroristično delovanje. Pojavila se je potreba po pridobivanju kadra, ki že poseduje tista znanja in izkušnje, ki omogočajo učinkovit spopad z mednarodnim terorizmom. To so ljudje, ki so vrsto let delovali in živeli v arabskih državah. S poznavanjem kulture in mentalitete sodelujejo tako pri usposabljanju osebja kot v posameznih fazah obveščevalnega ciklusa (Hulnick 2006: 308-309).

Nadalje Cia deluje v smeri delovanja, saj se odpirajo številne nove baze po vsem svetu, da bi bili čim bližje kriznim žariščem in pridobiti čim več relevantnih informacij o delovanju terorističnih organizacij iz neposredne bližine. Za kvalitetno operativno in analitično delo je bistvenega pomena, da so agentje seznanjeni z jeziki in določeno kulturo, kar bistveno olajša pridobivanje in razumevanje informacij. Tako prihaja tudi do vključevanja osebja iz samega območja operacij v jedro agencije (Goss, 2005b).

Če želi Cia izvajati uspešen protiteroristični boj, bo morala spremeniti in posodobiti tudi sistem usposabljanja. Hulnick ugotavlja, da se proces usposabljanja v agenciji ni spremenil vsaj že od sredine šestdesetih let in da se uporablja enaka logika usposabljanja kot na začetku hladne vojne. Vsak agent, ki se sooča s pojavom mednarodnega terorizma, mora posedovati tako operativna kot analitična znanja in ni smiselno, da se že v procesu usposabljanja kandidati delijo na bodoče operativce in analitike (Hulnick 2006: 311).

Kar zadeva spremembe, ki posegajo na področje zbiranja podatkov, pa uvedba brezpilotnih letal pomeni velik korak naprej. Ta letala lahko krožijo nad določenim območjem tudi do 24 ur, v tem času pa realno časovno prenašajo slike v analitični center. Brezpilotna letala so veliko bolj prilagodljiva in njihova uporaba je bistveno cenejša kot uporaba vohunskih satelitov. Sicer so sateliti še vedno osnovno sredstvo za opazovanje strateških ciljev, vendar se je pri spremljanju aktivnosti terorističnih organizacij brezpilotno letalo izkazalo za veliko bolj učinkovito orodje. Vendar se ta letala ne uporabljajo samo v namene zbiranja obveščevalnih podatkov, temveč so

dobila tudi svoje bojne naloge. Cia jih uporablja za izvajanje atentatov na posamezne visoke predstavnike terorističnih organizacij (Hulnick 2006: 308).

V okviru reforme obveščevalnega procesa znotraj Cie pa prihaja tudi do vse večje uporabe »rdečih skupin«¹⁹. Sistem rdečih skupin kot orodje za protiteroristično delovanje poskuša vpeljati ameriško ministrstvo za obrambo, vendar se tudi Cia poslužuje podobnega pristopa. Trije različni tipi rdečih skupin, ki bi lahko bili koristni za Cio, so (The Role and Status of DoD Red Teaming Activities, 2003):

- Nadomeščanje nasprotnikov (teroristov) – rdeče skupine igrajo vlogo teroristov in upornikov na terenu. Ta pristop se uporablja predvsem v fazi usposabljanja in priprav za terensko delo. Njihov namen je izboljšati spretnosti, odkriti šibke točke procesa zbiranja podatkov in povečati razumevanje morebitnih odzivov terorističnih organizacij.
- Razumevanje teroristov – rdeče skupine kritizirajo posamezna predvidevanja, strategije, načrte in procese ter ponujajo alternativne poglede na situacijo. Namen rdečih skupin v tej fazi je kritična analiza obveščevalnega procesa, da bi predvideli težave in se izognili presenečenjem.
- Dodatno posvetovalno telo – rdeče skupine pogosto predstavljajo neodvisno svetovalno telo, ki ima na voljo enake obveščevalne podatke, kot se uporabljajo v obveščevalnem ciklusu. Rdeče skupine so namenjene za kontrolo kakovosti izvajanja obveščevalnega procesa.

Uporaba rdečih skupin je postala še posebej pomembna v zadnjem obdobju, ko je potrebno razumeti nasprotnika, s katerim se ZDA soočajo v vojni proti terorizmu, še posebej njegove zmožnosti in možne odgovore na ameriške akcije. Zato mora Cia uporabljati to metodo na dveh ravneh, in sicer na operativni in na strateški ravni. Operativna uporaba rdečih skupin je namenjena izboljšanju obveščevalne dejavnosti in izboljšanju izvajanja aktivnosti na terenu, medtem ko je na strateškem nivoju Cia sama postavljena v vlogo rdeče skupine, saj mora delovati za potrebe sprejemanja odločitev na državnem nivoju. To pa pomeni, da mora priskrbeti argumentirane in

¹⁹ *Red teams in red teaming*. Rdeče skupine že dolgo uporabljajo v posameznih podjetjih in vladnih institucijah; njihov namen je zmanjšati posamezna tveganja in povečati priložnosti. Ustanovijo jih zaradi preverjanja učinkov in vidikov vsakega posameznega načrta, programa in predvidevanja (The Role and Status of DoD Red Teaming Activities, 2003).

objektivne analize stanja, oblikovati alternativne poti reševanja problemov, upoštevati nasprotna mnenja in omogočiti izvajanje sprejete odločitve.

Tovrstno spreminjanje ameriške obveščevalne skupnosti, še posebej Cie, je bila nujna in pomembna poteza v duhu širše nacionalne strategije, katere končni cilj je zmaga nad mednarodnim terorizmom. Za razumevanje vloge, ki jo v boju proti terorizmu igra Cia, pa ni dovolj zgolj spremljanje sprememb, temveč je potrebno pogledati v nacionalne strateške dokumente in poiskati vlogo Cie v njih.

Kot sem že napisal v poglavju o nacionanovarnostnem sistemu ZDA, je Amerika v strategiji nacionalne varnosti uvedla koncept preemtivnega napada. Če pa želi Cia slediti tem strateškim premikom, mora implementirati popolnoma nov model izvajanja obveščevalne dejavnosti, ki ga je Cogan poimenoval »strategija ofenzivnega lova«²⁰. Pričakuje se, da bodo v 21. stoletju spopadi potekali med državnimi akterji na eni strani in nedržavnimi akterji na drugi stani. Ti sedanji in prihodnji konflikti pa bodo zaradi predvidevane asimetričnosti bojevanja pomenili preobrat v dojemaju obveščevalne dejavnosti. Prvi korak k temu je pojav strategije ofenzivnega lova, ki jo lahko označimo kot obveščevalno in operativno manifestacijo nove strateške doktrine Busheve administracije, združeni v celoto. Takšna strategija daleč presega zmožnosti posamezne obveščevalne službe, vključno s Cio. Strategija ofenzivnega lova pomeni združitev obveščevalne dejavnosti z operativno dejavnostjo, kar zahteva tesno sodelovanje Cie in posebnih enot ameriške vojske. Strategija pa vključuje nekatere nove metode delovanja, ki pred napadi 11. septembra 2001 niso bili v široki uporabi. Te metode pa ne pomenijo samo izsleditev teroristov in če je potrebno tudi njihovo smrt, ampak predvsem neupoštevanje lokalnih posebnosti in pravil delovanja lokalnih obveščevalnih in varnostnih organov.²¹ Povedano drugače, obveščevalci v 21. stoletju bodo postali »lovci« in ne »iskalci« informacij. To pomeni, da bodo namesto čakanja na informacije agresivno pridobivali ustrezne obveščevalne podatke, ki bodo omogočili odkrivanje teroristov in njihovo eliminacijo. Strategija

²⁰ Offensive hunt strategy.

²¹ Kmalu pa začetku napada na Afganistan je predsednik Bush odobril »lov« na bin Ladna in najvišje predstavnike teroristične mreže Al Kaida. Takoj za tem je bilo v Afganistan poslano večje število agentov Cie, ki so stopili v stik z nasprotniki talibanskega režima in organizirali oborožen upor. V pričanju pred kongresom, 17. 10. 2002, je takratni direktor Cie George Tenet dejal, da je odločitev, da se pošlje Cio v osrčje zatočišča teroristov, najbolj pripomogla k protiteroristični dejavnosti. S tem ko je na terenu prisotnih veliko agentov, se spreminjajo pravila za teroriste in teroristi postanejo »plen« (Cogan 2004: 316-317).

ofenzivnega lova pomeni tudi pošiljanje agentov v tiste države, s katerimi ZDA niso v vojni, ali celo v države, s katerimi imajo ZDA dobre odnose. Tako se bo lov na voditelje terorističnih organizacij odvijal ne glede na stališče in morebitno ponujeno pomoč gostujoče države. Praksa je pokazala, da se je v Afganistanu ta strategija kljub nekaterim težavam relativno dobro obnesla in se že pripravljajo načrti in raziskave, kako bi sodelovanje med Cio in vojsko lahko še bolj okrepili (Cogan 2004: 315-319). Postavlja pa se vprašanje, kakšen vpliv ima uporaba te strategije na odnose v mednarodni skupnosti, saj tako Cia kot posebne enote vojske ne upoštevajo obstoječih norm mednarodnih odnosov. Prav tako menim, da so te metode pridobivanja obveščevalnih podatkov in izvajanja operativnih nalog velika nevarnost za človekove pravice in vzpodbujajo še bolj radikalne odzive terorističnih organizacij in lokalnega prebivalstva.

Nadalje ke v Nacionalni strategiji za boj proti terorizmu zastavljen širok načrt delovanja nacionalnovarnostnega sistema, imenovan *4D strategy*²². V tej strategiji, ki predvideva uporabo vseh razpoložljivih sredstev v boju proti terorizmu, in sicer v štirih postopnih korakih, se je Cia znašla v prvi bojni črti, predvsem zaradi specializacije v tajnem pridobivanju podatkov s pomočjo človeških virov, kar vključuje tudi izvajanje tajnih akcij, in pooblastil, da deluje v tujini. Štirje koraki tega načrta pa (National strategy for combating terrorism, 2003):

1. **Premagati teroriste in njihove organizacije;** v tej fazi je naloga Cie predvsem identifikacija terorističnih organizacij in njihovih dejavnikov (človeški, materialni, finančni, komunikacijski in ideološki). Prioriteto pa predstavljajo tiste organizacije, ki imajo globalni domet delovanja in kažejo aspiracije po posedovanju in uporabi orožja za množično uničenje.
2. **Preprečiti sponzorstvo, podporo in zatočišče za teroriste;** tukaj prevladuje uporaba političnih in diplomatskih sredstev za prepričevanje posameznih držav, da se aktivneje vključijo v mednarodni boj proti terorizmu. Na tem mestu Cia sodeluje s tujimi obveščevalnimi službami, jim nudi pomoč in sodeluje v procesu izobraževanja.
3. **Spremeniti obstoječe stanje, ki ga izkoriščajo teroristične organizacije;** ta korak pomeni preprečevanje regionalnih kriz, vzpodbujanje političnega,

²² Defeat, deny, diminish and defend.

socialnega in ekonomskega razvoja. Takšno delovanje vpliva na terorizem predvsem iz ideološkega vidika kot pomembnega motivatorja. Tukaj pa nastopi Cia, ki s svojimi tajnimi akcijami vodi »vojno idej«, v kateri poskuša na lokalnem območju izpodbijati legitimnost delovanja terorističnih organizacij.

4. **Zaščiti ameriške državljane in interese doma in v tujini;** tudi tukaj je naloga Cie iskanje in odkrivanje potencialnih groženj s strani terorističnih organizacij, ki so primarno usmerjene proti ameriškim interesom v tujini oziroma proti državljanom in institucijam (ambasade, podjetja in druge organizacije), ki se nahajajo izven ameriškega ozemlja.

Izhajajoč iz vloge, ki jo ima Cia v boju proti terorizmu, je oblikovala tri skupine terorističnih organizacij, in sicer glede na stopnjo nevarnosti, ki jo predstavljajo za ameriški nacionalnovarnostni sistem. V prvi skupini se nahaja Al Kaida, ki vedno znova poskuša prebiti varnosti sistem in izvesti napad na ameriškem ozemlju. Na drugem mestu so posamezne skrajne islamske organizacije (Hamas, Hezbollah, pakistanske milice, islamski Jihad, Jemaah islamia, Abu Sayaf itd.), ki so povezane z Al Kaido, vendar delujejo bolj v muslimanskem svetu in predstavljajo nevarnost ameriškim in zahodnim interesom v tej regiji. V tretji skupini pa se nahajajo organizacije, ki delujejo v drugih svetovnih regijah, so avtonomne, vendar jim kot model delovanja in inspiracija velikokrat služi Al Kaida. Rezultati njihovega delovanja pa so bili vidni predvsem v Evropi, in sicer v bombnih napadih v Veliki Britaniji in Španiji (Goss, 2005a; Negroponte, 2006).

Zaradi velike politične, vojaške in ekonomske angažiranosti ZDA v Iraku in Afganistanu pa je moč zaslediti tudi izjemno veliko aktivnost Cie v teh dveh državah. Tukaj agencija deluje predvsem v podporo posameznim vojaškim akcijam koalicijskih enot in novo postavljenim političnim režimom, ki se vsakodnevno spopadajo z uporniškimi gibanji in terorističnimi napadi. Ozemlji teh dveh držav (še posebej Iraka) se vse pogosteje uporabljata za vadišče terorističnih organizacij, kar pomeni, da se tukaj močno krepi infrastruktura teh skupin, ki pa pridobivajo vedno večjo podporo in zatočišče med domačini. Tukaj izurjeni »vojaki« pa nato odidejo v vse regije sveta, vključno z Ameriko, kjer čakajo na navodila za nove napade. Cio in z njo celoten ameriški nacionalnovarnostni sistem čakajo še številni izzivi, če bodo ZDA želele

doseči svoj cilj, in sicer zavarovati svoje ozemlje, prenesti vojno v tujino in v njej zmagati.

6.2 PRIMER BRITANSKE OBVEŠČEVALNE SLUŽBE SIS (*Secret Intelligence Service*)²³

Dejavnost tajne obveščevalne službe SIS se izključno navezuje na pridobivanje obveščevalnih informacij o delovanju britanskih nasprotnikov v tujini.

Podrobno opredelitev nalog SIS določa Zakon o obveščevalnih službah iz leta 1994, ki naloge SIS razdeli na tri vsebinska področja (*Intelligence services act, 1994*):

- zaščita nacionalne varnosti, s poudarkom na obrambni in zunanji politiki Velike Britanije,
- gospodarsko blagostanje VB,
- podpora pri preprečevanju hujšega kriminala.

Zakon postavlja SIS pod neposreden nadzor Ministrstva za zunanje zadeve, ki ima tudi izključno nalogodajno pravico, v okviru že omenjenih vsebinskih področij. Zakon prav tako določa, da SIS opravlja tudi druge naloge, ki se navezujejo na delovanje sovražnih subjektov izven britanskega ozemlja. V praksi to pomeni izvajanje tajnih akcij, ki velikokrat vključujejo atentate, sabotaže, širjenje dezinformacij in podobna dejanja, ki bi se v normalnih okoliščinah v VB preganjala na podlagi kazenske zakonodaje (*Intelligence services act, 1994*).

Prav tako pomemben zakon, ki obveščevalni službi povečuje določena pooblastila v protiterorističnemu delovanju, pa je Zakon o preiskovalnih pooblastilih (*Regulation on investigatory powers act*) iz leta 2000. Le-ta omogoča prestrežanje komunikacij, pridobivanje in objavo informacij, povezanih s komunikacijami, izvajanje nadzora nad posamezniki in uporabo tajnih človeških virov. Nadalje dopušča uporabo tehničnih sredstev, s katerimi se lahko pridobijo elektronske informacije, ki so zaščitene s šiframi. Vsi dokazi, pridobljeni z navedenimi postopki pa se lahko uporabijo v kazenskem

²³ V širši javnosti bolj znana pod imenom MI6 (*Military intelligence*), saj je bil njen izvor povezan z vojaško obveščevalno dejavnostjo.

postopku, kar ni bila praksa do sprejetja tega zakona (Regulation on investigatory powers act, 2000).

Pred sprejetjem Zakona o obveščevalnih službah vlada VB uradno ni priznavala obstoja tajne obveščevalne službe in je njene aktivnosti tajila. V času hladne vojne je glavno nalogo SIS predstavljalo delovanje na območju Sovjetske zveze in ostalih članic Varšavskega pakta. Po razpadu vzhodnega bloka pa je največ pozornosti usmerila v pomoč britanskim gospodarskim subjektom. Podobno kot v primeru Cie je tudi SIS sledila trendu ekonomske obveščevalne dejavnosti. Številni avtorji tako ugotavljajo, da so agenti tajne obveščevalne službe večino svojega dela podrejali doseganju ekonomskih koristi britanskih korporacij, toliko manj pa zbiranju informacij, ki bi pripomogle k večji stopnji nacionalne varnosti (Keegan 2004; Todd in Bloch 2003: 110-117).

Novo nastale varnostne razmere v devetdesetih letih pa so imele za posledico ponoven vzpon irskega terorizma, kar je zahtevalo večjo pozornost celotne britanske obveščevalne skupnosti. Vendar je na tem področju prihajalo do številnih rivalstev in trenj med SIS, varnostno službo (MI5), posebnim oddelkom metropolitanske policije in posebnim oddelkom severnoirske policije. Ti spori so se večkrat kazali na neučinkovitost pravočasnega zbiranja obveščevalnih podatkov, kar se je odražalo v uspešno izvedenih terorističnih napadih. To pa je še bolj negativno vplivalo na podobo SIS v javnosti (Urban 1996).

V drugi polovici devetdesetih let je takratno vodstvo SIS začelo dojemati terorizem in še posebej mednarodni terorizem kot osrednjo grožnjo nacionalni varnosti. Zato so spremenili notranjo strukturo službe in jo prilagodili protiterorističnemu delovanju. Prišlo je do vzpostavitve oddelka za globalne naloge, v katerem so se združili nekateri od oddelkov, ki so bili organizirani po geografskem načelu. Prav tako sta se združila oddelka odgovorna za Afriko in Bližnji vzhod, ter oddelka za Daljni vzhod in zahodno poloblo. Izboljšana je bila tudi operativna podpora tajnim operacijam v tujini (Todd in Bloch 2003: 26).

Po 11. septembru 2001 pa postanejo glavna tarča SIS islamske ekstremistične skupine. Služba okrepi že vzpostavljene agenturne mreže, na primer v Afganistanu,

Iraku, Jemnu itd. in vzpostavi nove, predvsem v državah, kjer so se kazale aktivnosti skrajnega islama. Naloga teh mrež je pravočasno opozarjanje v primeru zaznanih aktivnosti terorističnih organizacij, predvsem Al Kaide, še posebej proti VB, njenim interesom in njenim zaveznikom²⁴.

Že pred dogodki 11. septembra 2001 je SIS pomemben del svojih sredstev namenila protiterorističnemu delovanju. Neposredno po odmevnih napadih pa so se sredstva skoraj podvojila, v naslednjih štirih letih pa potrojila (Intelligence and Security Committee 2002; Intelligence and Security Committee 2004). Napadi v New Yorku in Washingtonu so bistveno vplivali tudi na kadrovske potrebe SIS. Po napadih je služba večje število svojih izkušenih agentov poslala v novo nastali protiteroristični center v Londonu, ki je kasneje prerasel v skupni analitični center za terorizem (JTAC). Tudi večina stalnih in začasnih izpostav v tujini se je skoraj izključno posvetila Al Kaidi, Osami bin Ladnu in talibanskemu režimu v Afganistanu. Takšna prerazporeditev kadrovskih virov ob obstoječem osebju pa je pomenila zastoj na drugih področjih delovanja, kot so odkrivanje orožja za množično uničevanje in mednarodnega organiziranega kriminala (Intelligence and Security Committee 2002).

Da bi lahko zadostila vedno večjim potrebam po analizi zbranih podatkov, je po vzoru Cie začela obširen program zaposlovanja ljudi, ki so predstavniki etničnih manjšin. Še posebej pomembni so tisti kandidati, ki prihajajo iz arabskih etničnih skupin. Tako je leta 2004 kar 9 % vseh kandidatov izhajalo iz manjšinskih skupnosti. Leta 2005 pa se je ta odstotek dvignil na 15 % (Intelligence and Security Committee 2005).

Teroristični napadi v ZDA so povzročili spremembe tudi pri metodah, ki jih je SIS uporabljala v protiterorističnem delovanju. Prišlo je do večjega sodelovanja z britansko vlado in drugimi zavezniškimi državami, predvsem kar zadeva zaznavanje posameznih virov ogrožanja. Nadalje je SIS skupaj z britansko varnostno službo (MI5) okrepila sodelovanje z drugimi zahodnoevropskimi obveščevalnimi in varnostnimi službami, predvsem zaradi skupnih operacij. Prav tako so se vzpostavljali in poglobljali stiki z obveščevalnimi službami, ki prihajajo iz neevropskih

²⁴ Za primer uspešnega zbiranja informacij o delovanju terorističnih organizacij, ki pa žal ni bil upoštevan, štejem namig, ki ga je leta 1999 pridobila SIS, da namerava skupina blizu Osami bin Ladnu izvesti napad v ZDA, pri katerem bi na nekonvencionalni način uporabili potniška letala (Thackrah 2004:10).

držav. Zaradi aktivne politike na področju protiterorističnega delovanja in številnih mednarodnih aktivnosti je bilo potrebno usposobiti dodatno administrativno in organizacijsko infrastrukturo in posodobiti informacijsko tehnologijo, ki je bila do takrat na voljo (Intelligence and Security Committee 2002).

Ob intenzivnejših mednarodnih povezavah in hitrejši obdelavi zbranih podatkov se je okrepil tudi tisti del SIS, ki izvaja tajne operacije. Tajno protiteroristično delovanje pogosto zahteva tesno sodelovanje z vojsko, kar se je pokazalo tudi v operacijah v Afganistanu in Iraku, kjer so agentje SIS izvajali tajne akcije v zaledju nasprotnikovih sil (The Economist, 17. 5. 2005). V ta namen SIS vzdržuje posebne enote, ki so vedno na voljo, popolnjene po so tudi z ustrezno opremo, ki omogoča izvajanje tajnih akcij na terenu. Takšni dve enoti sta SBS (*Special Boat Service*) in SAS (*Special Air Service*), ki sta prišli najbolj do izraza ravno v Afganistanu in Iraku (Todd in Bloch 2003: 112).

Za kakovostno izvedbo zastavljenih nalog uporablja SIS tajno metodologijo zbiranja informacij in prav tako v tajnosti ohranja imena virov informacij in imena agentov, tudi po koncu njihovega aktivnega delovanja. Ta politika delovanja se obrestuje v večji stopnji zaupanja virov in tudi v boljši kredibilnosti zbranih informacij (bbc.co.uk 2003).

Vendar je ne glede na obstoječo politiko v preteklosti prihajalo do številnih odmevnih afer, ki so močno omajale podobo SIS in ogrozile veliko operacij, življenj agentov in njihovih virov. Zadnja večja napaka, ki si jo je »privoščila« SIS, izvira iz aktivnosti v Iraku, kjer je služba sodelovala pri odkrivanju iraškega orožja za množično uničevanje in pri iskanju povezav med iraškim režimom in Al Kaido. Tako je zaradi težnje po čimprejšnjem posredovanju informacij odpovedal interni sistem za kakovost zbranih podatkov, ki je odgovoren za preverjanje virov, kar je posledično pripeljalo do posredovanja netočnih informacij, pridobljenih s strani nekredibilnih virov.

Posledica te afere je bilo oblikovanje posebne Butlerjeve preiskovalne komisije, ki je v končnem poročilu predlagala določene spremembe v obveščevalnem procesu. Prišlo do vzpostavitve posebne pisarne za vzdrževanje kakovosti, katere naloga je nadzor kakovosti nad obveščevalnimi podatki, ki prihajajo v SIS, njihovo obdelavo in posredovanjem obveščevalnih informacij končnim porabnikom.

Druga sprememba se je navezovala na dostopnost zbranih podatkov s strani drugih obveščevalnih služb znotraj britanske obveščevalne skupnosti. Težava je bila v nepripravljenosti SIS, da zbrane podatke deli z drugimi organizacijami, predvsem zaradi medsebojne tekmovalnosti in iz strahu pred odtekanjem informacij. V želji po izboljšanju sodelovanja se je SIS še bolj intenzivno vključila v JTAC.

Prav tako pride do večje racionalizacije dela, in sicer pod motom, »da se, primerne odločitve sprejemajo na primernih nivojih, s strani pravih ljudi«. Pred tem je bil najvišji organ preobremenjen z vsemi področji dela, kar je zavlačevalo delovne postopke in onemogočalo hitro prilagajanje nastalim razmeram. Posledično je prišlo do vzpostavitve srednjega menedžmenta, ki je prevzel operativni nivo vodenja (Corera 2005: 51).

V obdobju po koncu hladne vojne se je SIS znašla v nezavidljivem položaju, saj so je pretresale številne afere, počasno prilagajanje novim virom ogrožanja in nezmožnosti upiranja političnim vplivom. Očiten primer slednjega je dejstvo, da obveščevalne informacije niso pomagale oblikovati britanske politike do Iraka, temveč je politika oblikovala obveščevalne informacije. Na takšnih napakah pa se izgublja smiselnost delovanja služb, saj so, kot trdi Phythian, obveščevalne službe učinkovite le takrat, ko se jim lahko zaupa, in največji »zločin«, ki ga lahko obveščevalec naredi, je, da prilagodi svoje poročilo tako, da ugotovi politični garnituri na oblasti (Phythian 2005: 671). Posledica tega nezaupanja pa je izguba pomembne vloge SIS v britanski obveščevalni skupnosti, saj jo tudi na področju obveščevalne dejavnosti v tujini vse bolj nadomešča varnostna služba (MI5). Vloga SIS je zmanjšana na izvajanje zelo tajnih operacij v tujini in ohranjanje tajnih stikov s sorodnimi obveščevalnimi službami ter nekaterimi ekstremističnimi skupinami, medtem ko je glavno vlogo boja proti terorizmu z JTAC kot osrednjim organom prevzela MI5.

6.3 PRIMER RUSKE OBVEŠČEVALNE SLUŽBE SVR (*Služba vnešnogo razvedki*)

Zunanja obveščevalna služba Ruske federacije (SVR) je bila prvi element bivšega KGB, ki je vzpostavil samostojno strukturo delovanja in prevzel večino operacij v tujini, vključno z zbiranjem podatkov in njihovo obdelavo. Relativno hitra vzpostavitev operativnosti SVR je bila posledica že zelo avtonomnega prvega direktorata znotraj KGB, ki je opravljal obveščevalne dejavnosti v tujini.

SVR je bila ustanovljena leta 1991, in sicer s posebnim dekretom predsednika, ki je SVR neposredno podredil predsedniku RF. Kasneje pa je služba zaradi boljše učinkovitosti delovanja prešla pod pristojnost ministrstva za zunanje zadeve (Bennett 2000: 6). Leta 1992 je z novim zakonom o kazenskem pregonu SVR pridobila številna nova pooblastila. Tako je imela služba dovoljenje za prestrežanje vseh oblik komunikacije, pregled prostorov in nadzor na osumljenci. Tako velika pooblastila za obveščevalno službo so vsekakor nenavadna, zato je bilo jasno, da SVR ne bo izvajala samo obveščevalne, ampak bo v svojo pristojnost pridobila nekatere protiobveščevalne naloge. V tem času je prišlo tudi do opredelitve prioriternih področij, ki so po eni strani zahtevale usmeritev SVR v ekonomsko obveščevalno dejavnost²⁵, po drugi strani pa je šlo za nadaljevanje »hladnovojne« obveščevalne dejavnosti²⁶ (Campbell 1994).

Leta 1995 pa je bil sprejet zakon o operativni in preiskovalni dejavnosti, ki pa je že nakazoval spremembe v uporabi posebnih metod in sredstev za izvajanje nalog SVR. Zakon predvideva, da lahko SVR uporablja te metode in sredstva samo v primeru, kadar gre za zaščito lastne organizacije in varovanja podatkov. Tako je služba izgubila protiobveščevalne pristojnosti, ki so bile prenesene na Zvezno varnostno službo (FSB) (Federalnij zakon ob operativno-razysknoj dejatelnosti, 1995). Naslednje leto pa je ruska дума potrdila zakon o zunanji obveščevalni dejavnosti, ki je omogočil pravno osnovo delovanja SVR in podrobneje opredelil naloge in metode delovanja. S tem zakonom so postale osrednje naloge SVR zbiranje informacij na političnem, ekonomskem, vojaško-strateškem, znanstvenem, tehničnem in

²⁵ Pridobivanje ekonomskih obveščevalnih podatkov, ki bi pomenili prednost v primerjavi s trgovinskimi partnerji; industrijsko vohunstvo.

²⁶ Širjenje politične misli v Južni in Srednji Ameriki ter Afriki, razbijanje zahodnoevropskih povezav. deligitmiranje zahodnih vlad, želja po izolacionistični politiki ZDA.

ekološkem področju. Prav tako je služba zadolžena tudi za opravljanje varnostne dejavnosti, in sicer za potrebe institucij Ruske federacije, ki so nastanjene izven ruskih meja. Na področje varnostne dejavnosti pa spadajo tudi ruski državljani, ki imajo zaradi narave svojega dela dostop do zaupnih informacij. Tako je mogoče iz zakona razbrati, da je SVR tipična aktivna obveščevalna služba, ki ob osnovnem zbiranju podatkov izvaja tudi tajne akcije v tujini (Federalnij zakon o vnešnji razvedke, 1996).

Nove prioritete in meddržavno soočanje z varnostnimi tveganji zahtevajo vzpostavitev številnih stikov tudi s tujimi obveščevalnimi službami, predvsem pri preprečevanju novih virov ogrožanja, kot so širjenje orožja za množično uničevanje, mednarodni terorizem in organizirani kriminal. SVR tako vzpostavlja odnose z namenom, da bi prišlo do izmenjave obveščevalnih informacij in izpeljave skupnih nalog. Osnovno pravilo sodelovanja pa je partnerski odnos med SVR in sodelujočimi službami ter zaščita lastnih interesov. Ob poglobljenem sodelovanju s službami iz držav Nata²⁷ pa je opazna usmeritev na države SND, ki danes predstavljajo največjo nevarnost za Rusijo, predvsem zaradi organiziranja terorističnih organizacij in načrtovanja njihovih aktivnosti na ozemljih teh držav²⁸.

Boj proti mednarodnemu terorizmu, kot ena izmed osrednjih nalog SVR, je razviden že iz obstoječih prioritet delovanja, saj je mednarodni terorizem identificiran kot največja grožnja ruski državi in njenim interesom. Vendar pa se SVR kot eden izmed osnovnih nosilcev protiterorističnega delovanja pojavi šele v zveznem zakonu o boju proti terorizmu, ki je bil sprejet leta 1998. Ta zakon določa, da je glavna naloga SVR v protiterorističnem delovanju zagotavljanje varnosti ruskim institucijam v tujini, njihovim uslužbencem in članom družin. Prav tako pa je služba zadolžena za zbiranje podatkov o aktivnostih tujih in mednarodnih terorističnih organizacij (Federalnij zakon Rossijskoj Federaciji o borjebe s terorizmom, 1998).

Kar zadeva neposredno zbiranje podatkov o mednarodnemu terorizmu, pa je po besedah direktorja službe glavna naloga SVR proučevanje finančne plati delovanja

²⁷ Kjer posebno mesto zavzema Turčija s svojo obveščevalno službo (MIT). SVR je uspela vzpostaviti močno sodelovanje z MIT, predvsem kar se tiče skupnega boja proti islamskemu ekstremizmu v regiji, kljub nekaterim sumom, o turški pomoči čečenskim skrajnežem (Todd in Bloch 2003: 145).

²⁸ Intervju s Sergejem Lebedevim, direktorjem SVR, za agencijo Interfax, 20. 12. 2002; SVR Operations, 1997

terorističnih organizacij. To pomeni, da služba nadzoruje pomembne finančne tokove teroristov in njihove povezave s kriminalnimi združbami. Zato je posebna pozornost namenja tudi dogajanju v Čečeniji, še posebej, kar zadeva ekstremistične aktivnosti in obstoj nevarnosti za teritorialno integriteto RF. Ker pa ruska zakonodaja ne omogoča delovanja SVR na ozemlju RF, se je služba primarno osredotočila na odkrivanje in spremljanje virov pomoči, ki se nahajajo v tujini in omogočajo nadaljnje operativno delovanje čečenskih upornikov. Pomembna naloga je tudi odkrivanje in oviranje tihotapskih poti, ki dejansko omogočajo, da material, denar in ljudje sploh lahko pridejo do uporniških oziroma terorističnih taborov²⁹.

Za izvajanje nekaterih operativnih akcij, med katere spada tudi že omenjeno oviranje transportnih poti, pa znotraj SVR obstaja majhna enota za protiteroristično delovanje, imenovana »prapor«. Ta enota ima korenine že v prvem direktoratu bivšega KGB. Njena primarna naloga se do danes ni bistveno spremenila. Enota je namenjena za izvajanje infiltracij, sabotaž, atentatov in za delovanje na sovražnem ozemlju. Sicer je enota v obdobju po koncu hladne vojne doživljala določene spremembe, saj so jo pogosto premeščali, in sicer iz SVR v FSB, kasneje pa še pod ministrstvo za notranje zadeve, vendar se zaradi neuspešne vključitve v obstoječe sisteme omenjenih institucij ponovno vrne pod okrilje SVR³⁰. Toda zaradi visoke tajnosti delovanja enote je v javnosti izjemno malo podatkov o njenem delovanju (Galeotti 2002: 49; SVR Organization 1997).

Za izvajanje obveščevalnih in operativnih nalog, še posebej tistih, ki se navezujejo na protiteroristično delovanje, pa je potrebna ustrezna kadrovska struktura. V devetdesetih letih prejšnjega stoletja je SVR doletela podobna usoda kot ostale obveščevalne službe po svetu. Imele so veliko preveč zaposlenih ljudi, ki pa niso bili primerno izobraženi in usposobljeni za soočanje s sodobnimi viri ogrožanja. Prav tako zaradi spremenjenih družbenih vrednot ni bilo prevelikega zanimanja za zaposlitev v SVR s strani mladih ljudi. Vendar so po besedah direktorja službe Lebedeva uspeli ustaviti negativni trend in ponovno beležijo visoko zanimanje za

²⁹ Intervju s Sergejem Lebedevim, direktorjem SVR, za agencijo Interfax, 19. 12. 2005.

³⁰ Primer delovanja specialne enote v tujini je atentat na bivšega predsednika Čečenije Yandarbieva, ki so ga ruski tajni agenti ubili v Katarju, in sicer s podtaknjeno bombo (Elbaz 2005).

ustvarjanje kariere v zunanji obveščevalni službi³¹. Služba počasi uresničuje kadrovske politike, ki jo je zastavil nekdanji direktor Primakov: »Iščemo in bomo iskali ljudi z lastnimi idejami o razvoju sveta in o vlogi njihove države ter vlade v tem svetu. Ti ljudje morajo imeti občutek za Rusijo, to so ljudje, ki jo želijo videti kot močno državo, ki pa ne bo zlorabljala svoje moči za zastraševanje drugih držav ali igranje vloge svetovnega policista« (Campbell 1994).

SVR predstavlja del kompleksne obveščevalne skupnosti RF, ki je še danes pod vplivom slave nekdanje KGB, kar se odraža tudi v prioritethih usmeritvah služb. Pogoste so reforme, ki ne prinesejo bistvenih sprememb v delovanje, ravno nasprotno, v večini primerov prinašajo trenja in spore med obveščevalne in varnostne službe. Po besedah Soldatova je rezultat teh procesov neučinkovitost služb, kar se kaže v veliki tajnosti in nedostopnosti. Tako je SVR najbolj tajna organizacija v Rusiji. Prav tako pa ne igra kakšne pomembnejše vloge v protiterorističnem delovanju, saj je varnostna služba FSB prevzela osrednjo vlogo v boju proti terorizmu, tako doma kot v tujini.³² Podobno kot pri SIS lahko opazim, da je tudi vloga SVR zreducirana na izvajanje nekaterih tajnih akcij in opravljanje posameznih obveščevalnih nalog, vse po »navodilih« FSB.

6.4 PRIMER IZRAELSKÉ OBVEŠČÉVALNE SLUŽBE MOSSAD (*ha-Mossad le-Modiin ule-Tafkidim Meyuhadim*)

Inštitut za obveščevalne in posebne naloge, na kratko Mossad, je izraelska obveščevalna služba, namenjena za delovanje v tujini. Njene dejavnosti so zbiranje obveščevalnih podatkov s pomočjo človeških virov, tajne operacije in protiterorizem. Osrednja pozornost je namenjena arabskim državam in raznim organizacijam po vsem svetu, ki predstavljajo grožnjo za nacionalno varnost Izraela. Med že omenjenimi nalogami se Mossad ukvarja tudi s tajnim preseljevanjem Judov, iz držav (večinoma iz arabskih), ki so tradicionalno nenaklonjene judovskemu prebivalstvu, v Izrael (Mossad the Institute for Intelligence and Special Tasks, 2006).

³¹ Intervju s Sergejem Lebedevim, direktorjem SVR, za agencijo Interfax, 19. 12. 2005.

³² Osebna korespondenca preko elektronske pošte z novinarjem Andrejem Soldatovom, 15. 5. 2006.

Mossad, kot ga poznamo danes, je bil ustanovljen leta 1951, s strani takratnega izraelskega premiera Davida Ben Guriona, ki je dal Mossadu osnovne smernice delovanja: »za našo državo, ki je vse od njenega nastanka pod udarom sovražnikov. Obveščevalna dejavnost predstavlja prvo linijo obrambe, zato moramo znati prepoznavati stvari, ki se dogajajo okrog nas«. Tako so glavne naloge predstavljale boj proti terorizmu, zbiranje obveščevalnih podatkov o namerah sosednjih arabskih držav in izvajanje tajnih akcij proti tem državam.

Na področju boja proti terorizmu je Mossad doživel vrhunec v 70. letih prejšnjega stoletja, ko je izsledil in likvidiral vse načrtovalce napada na izraelske športnike na olimpijskih igrah v Munchenu, leta 1972. Vendar se po uspehih med hladno vojno Mossad ni prilagodil novo nastalim razmeram, ki pa so jih dobro izkoristile razne teroristične skupine. Posledica tega je bila izguba primata v boju proti terorizmu, kjer osrednjo vlogo prevzame varnostna služba Shin Beth in vojaška obveščevalna služba Aman.³³ Sledila je serija reform, ki jih je uvedel novi direktor Mossada Halevy. Vendar so bile te reforme v neskladju z osnovno usmeritvijo obveščevalne službe. Tako je Halevy spreminjal Mossadovo organizacijsko strukturo, oblikoval večje skupine oddelkov in okrepil administracijo ter notranjo varnost. Premalo pa se je zavzemal za reformo agenturne mreže in tistega dela službe, ki izvaja operacije na terenu. Zato so bile prekinjene skoraj vse Mossadove operacije v tujini, predvsem pa v arabskih državah. Zaradi interesov vodstva službe, da Mossad prevzame vlogo glavnega obveščevalnega analitičnega organa v izraelski obveščevalni skupnosti, in zaradi novo nastalih političnih razmer v Izraelu so se začela trenja med izraelskimi obveščevalno-varnostnimi službami.

Posledično je leta 2000 nastal dokument, imenovan *Magna Carta 2*, ki je določil razmejitve med področji delovanja izraelskih obveščevalnih služb. S tem dokumentom se kot območje delovanja Mossada opredelijo tista geografska območja, ki niso v neposrednem stiku z izraelskim ozemljem. Vendar so v ta geografska območja vključene tudi vse arabske države (Kahana 2002: 421).

³³ "Vrhunec" nesposobnosti in izgube verodostojnosti Mossada so pokazale številne porazne akcije v sredini 90. let, ko so njegovi agenti neuspešno izvedli poskus atentata na enega izmed vodij Hamasa. Prav tako so bili neuspešni pri izvajanju prisluškovanja drugemu visokemu predstavniku Hamasa v Švici. V obeh primerih so agente aretirali in sledila je mednarodna obsodba Izraela ter odstop direktorja Mossada (Ben-David 2004).

V času druge intifade pa so se še boljše pokazali problemi Mossada, ko služba ni niti poskusila delovati proti finančnim transakcijam terorističnih organizacij. Prav tako je zelo podcenjevala Al Kaido, njene interese in zmožnosti.

Ponavljajoče težave Mossada in nesposobnost pridobivanja hitrih in verodostojnih informacij so leta 2002 ponovno povzročile spremembe na direktorskem mestu. Novi direktor je postal Dagan, ki v nasprotju s svojim predhodnikom prihaja iz bolj operativnega okolja in ima polno podporo političnega vodstva Izraela, da ponovno vzpostavi operativno sposobnost službe (Ben-David 2004: 46-47).

Novo vodstvo je delno spremenilo tudi celotno strukturo Mossada, in sicer z razdelitvijo službe na dva dela, administrativnega in operativnega (Kahana 2002: 417-418; Levkov 2001: 55-57):

- Administrativni del opravlja vse administrativne in logistične naloge, potrebne za normalno delovanje službe. Razdeljen je na naslednje oddelke:
 - Komunikacije – sodobna komunikacijska mreža, prav tako namenjena pridobivanju obveščevalnih podatkov s pomočjo signalov (SIGINT).
 - Dokumentacija – oddelek, namenjen za zagotavljanje primernih dokumentov za izvajanje operacij (npr. potni listi prijateljskih držav).
 - Analize – oddelek, namenjen obdelavi obveščevalnih podatkov in izdelavi končnih obveščevalnih izdelkov, večinoma namenjenih za podporo obveščevalnim operacijam.
- Operativni del pa je zadolžen za izvajane tajnih operacij, predvsem v arabskih državah. Razdeljen je na naslednje oddelke:
 - *Tzomet* – oddelek, zadolžen za pošiljanje agentov v tujino.
 - *Neviot* – enota, namenjena za pridobivanje obveščevalnih podatkov s pomočjo tehničnih sredstev (TECHINT).
 - *Tevel* – mednarodni oddelek Mossada, namenjen za vzpostavljanje neformalnih stikov z državami, s katerimi Izrael nima uradnih odnosov.
 - *Tsafirim* – oddelek, ki skrbi za judovske skupnosti v »problematičnih« državah in v primernih okoliščinah omogoči preselitev teh skupnosti v Izrael.
 - *Yahalolim* – oddelek, namenjen vzdrževanju stikov z agenti, ki delujejo pod globoko krinko, predvsem v arabskih državah.

- Služba za varnost tajnih operacij, ki izvaja neposredno zaščito operativcev na terenu.

Ob dveh osnovnih zadolžitvah Mossada pa obstaja še posebna enota, imenovana *Metzada*, katere naloga je delovanje na ozemlju arabskih držav, kjer agenti izvajajo tajne operacije, med katere spadajo tudi likvidacije posameznikov in sabotáže. Te operacije se pogosto izvajajo v sodelovanju z drugimi tajnimi enotami za posebno delovanje (enote izraelske vojske).

S spremembo vodstva in organizacijske strukture Mossada je prišlo tudi do spremembe v opredelitvi ciljev. Danes služba večino svojih sredstev namenja boju proti terorizmu in zbiranju informacij o iranskem jedrskem programu.

Kar zadeva delovanje proti terorizmu lahko aktivnosti Mossada razdelimo na tri področja:

- **Zbiranje obveščevalnih podatkov o terorističnih aktivnostih z lastnimi sredstvi.** Mossad ponovno oživlja svojo mrežo agentov po arabskih državah, predvsem z rekrutiranjem novih agentov arabskega porekla (Strindberg 2004: 26). Cilj tega zbiranja je pridobitev taktičnih in strateških obveščevalnih informacij. Med taktične informacije spadajo zelo specifični podatki o posameznih teroristih, načrtih za točno določen teroristični napad, uporabljenih sredstvih in o času ter kraju napada. Strateške obveščevalne informacije pa pomenijo informacije o temeljnih dejavnikih terorističnega delovanja (rekrutiranje, financiranje, materialna podpora, komuniciranje in ideologija).
- **Izvajanje tajnih akcij zoper teroristične organizacije.** Med tajne akcije v prvi vrsti spadajo eksekucije³⁴, sabotáže in ugrabitve. Eksekucije pomenijo korenit poseg v vodstveno strukturo organizacije in vnašajo razdor med različnimi frakcijami, če obstajajo, ter nezaupanje med člani gibanja, predvsem zaradi strahu pred izdajalci. Eksekucije prav tako silijo teroristične organizacije, da svoje glavne sedeže selijo v bolj oddaljene države, kar onemogoča normalno komunikacijo in delovanje organizacije.

³⁴ Imenovanju Dagana za direktorja Mossada je sledila serija atentatov na visoke predstavnike skrajnih islamskih gibanj. Največ prahu je dvignil atentat na aktivista Hamasa, ki je bil izvršen v glavnem mestu Sirije. Ta akcija kaže na trenutno slabši položaj Sirije in na pripravljenost Izraela, da boj proti terorizmu prenese na ozemlje drugih držav (Strindberg 2004; Sobelman 2004).

Tudi sabotaže otežujejo delo teroristov, še posebej, če so tarče sabotaž poveljniški in komunikacijski centri, skladišča, transportna sredstva in finančne transakcije.

Mossad pogosto prakticira ugrabitve posameznih teroristov, ki predstavljajo bogat vir informacij. Cilj teh ugrabitev je predvsem dvojen, pridobitev relevantnih informacij in poskus »spreobrnitve« posameznika, ki bi postal dvojni agent Mossada (Gazit 2002: 240-241).

- **Mednarodno sodelovanje.** Mossad ima že dolgo tradicijo uspešnega sodelovanja, predvsem z zahodnimi obveščevalnimi in varnostnimi službami (CIA, MI5, MI6, BND itd.). Posebna pozornost je namenjena sodelovanju z ameriškimi obveščevalnimi službami, kjer prednjači Cia, predvsem zaradi primerljivega sistema delovanja in političnih vezi med ZDA in Izraelom. Sodelovanje Mossada s tujimi obveščevalnimi službami je dokaj kompleksno. Sodelovanje poteka na taktični³⁵ kot tudi strateški³⁶ ravni. Mossad prav tako igra vlogo izraelskega predstavništva, in sicer v državah, s katerimi Izrael nima vzpostavljenih formalnih odnosov. Vendar je najbolj zanimivo sodelovanje z obveščevalnimi službami nekaterih arabskih držav, ki so bile do nedavnega sovražno razpoložene do Izraela. Primer takšnega sodelovanja je jordanska obveščevalna služba, za katero se sumi, da je po navodilih Mossada izvedla nekaj atentatov in sabotaž v Siriji (Strindberg 2004: 26-27). Zelo pomembno je tudi sodelovanje s turško obveščevalno službo, preko katere so Izraelci prišli do pomembnih podatkov o terorističnih aktivnostih v sosednjih državah.

Mossad si je s svojimi odmevnimi operacijami in osrednjo vlogo, ki jo je imel v ohranitvi obstoja Izraela, utrdil mesto med četverico »velikih« obveščevalnih služb. Vendar tudi Mossadu ni uspela hitra in uspešna prilagoditev novim razmeram po koncu hladne vojne. Nekaj velikih napak, storjenih sredi 90. let, je zelo omajalo ugled te obveščevalne službe. Danes se Izrael ponovno bori z že znanim nasprotnikom – terorizmom, ki se je spretno prilagodil novim razmeram in še bolj internacionaliziral svoje aktivnosti. Takšne razmere kličejo po močni obveščevalni službi, sposobni

³⁵ Sodelovanje Mossada in Cie v preiskovanju delovanja Al Kaide v vzhodni Afriki oziroma sodelovanje Mossada in MI5 pri preiskavi uboja dveh Britancev v Tel Avivu (Ben-David 2004: 49).

³⁶ Podpis dvostranskih sporazumov med Izraelom in 39 državami o medsebojnem obveščevalnem sodelovanju. Sporazumi obvezujejo podpisane države k sodelovanju in omogočajo izvajanje skupnih obveščevalnih operacij. Sodelovanje pa predstavlja izmenjavo točno določenih obveščevalnih podatkov, urjenje protiterorističnih enot, izvajanje skupnih tajnih operacij itd. (Todd in Bloch 2003: 157-159).

posredovanja kakovostnih in pravočasnih podatkov iz tujine, ki bodo omogočili hitro in dobro zaščito pred terorističnimi napadi. Spremembe, ki se kažejo znotraj Mossada v današnjem času, nakazujejo na to, da je ta obveščevalna služba ponovno na poti do nekdanje slave.

7 MEDNARODNO SODELOVANJE OBVEŠČEVALNIH SLUŽB V BOJU PROTI MEDNARODNEMU TERORIZMU

V sodobnem varnostnem okolju si je praktično nemogoče zamisliti zagotavljanje nacionalne varnosti izključno v okvirih nacionalnega varnostnega sistema. Zato se leti pod pritiski globalizacijskih trendov vse bolj poslužujejo mehanizmov zagotavljanja varnosti znotraj številnih nadsocijalnih institucij, kot so OVSE, OZN, NATO, EU itd. Dejstvo je, da koncept varnosti ni omejen na nacionalna ozemlja, ampak se zaradi številnih nadsocijalnih oblik ogrožanja varnosti, od katerih je mednarodni terorizem v ospredju, varnost zagotavlja preko državnih meja (Podbregar 2004: 32).

Glede izziva, ki ga predstavljajo teroristične organizacije za zagotavljanje varnosti, pa je sodelovanje med obveščevalnimi službami postalo prej pravilo kot izjema. Pri izvedbi mednarodnega sodelovanja trčimo na enega izmed temeljev delovanja obveščevalnih služb, in sicer da lahko »njene informacije (obveščevalne službe op. avtorja) uporablja le vodstvo te države in da predstavljajo tajnost za vse ostale države« (Dragutinović v Purg 1995: 60).

Ne glede na ta temelj delovanja pa so tako v preteklosti kot v sedanjosti pogosto opazni bolj ali manj intenzivni primeri sodelovanja obveščevalnih služb, predvsem kadar so države ogrožene s strani skupnega »sovražnika«.

Najprej je potrebno ugotoviti, zakaj se obveščevalne službe odločajo za mednarodno sodelovanje na področju boja proti terorizmu. Danes je sodobni terorizem kompleksen mednarodni proces, ki se izjemno hitro prilagaja spreminjajočemu se mednarodnemu okolju. Zato je neprestano več potencialnih podatkov, kot jih lahko ena sama služba zbere. Prav tako lahko posamezne službe zberejo edinstvene podatke, ki so ostalim nedosegljivi, predvsem kar zadeva določeno regijo ali lokacijo. Še večja potreba po sodelovanju se kaže na področju zbiranja podatkov s pomočjo človeških virov (HUMINT) zaradi jezikovnih, kulturnih in narodnostnih specifik. Pomemben dejavnik, ki prispeva h krepitvi sodelovanja, pa je omejen finančni vir. Zato imajo lahko manjše službe, ki so specializirane na določenem področju, dostop do podatkov globalnega pomena (podatki, zbrani s tehničnimi sredstvi), do katerih ga

zaradi omejenih virov financiranja drugače ne bi imele (Herman 1996: 204; Shpiro 2001).

Purg sodelovanje obveščevalnih služb utemeljuje na spoštovanju načel enakopravnosti služb in na obrambi interesov lastnih držav. Tudi legitimnost in legalnost opredeljuje kot pomembna kriterija delovanja in medsebojnega sodelovanja obveščevalnih služb (Purg 1995: 60-61). Ta načela so podlaga za oblikovanje ogrodja, znotraj katerega poteka obveščevalno sodelovanje. Vzpostavljeno in institucionalizirano ogrodje, ki ga Aldrich označuje kot svet v svetu, ki mu vlada posebna »diplomacija« in je opredeljeno z dovršenimi dogovori, razumevanjem in sporazumi, mora omogočiti kakovostno sodelovanje obveščevalnih služb (Aldrich 2004: 737).

Purg razvršča vsebino, obliko in metode mednarodnega sodelovanja med obveščevalnimi službami na način, ki ga je mogoče uporabiti tudi po načelu sodelovanja na področju boja proti terorizmu (Purg 1995: 61).

- Po vsebini lahko sodelovanje razvrstimo na tri področja:
 - **Izmenjavo podatkov, ocen in informacij.** Varovanje obveščevalnih virov in primarnih obveščevalnih podatkov je zelo uveljavljen dogovor, za katerega je zelo malo verjetnosti, da bi se spremenil. Posledično obveščevalne službe ne bodo privolile v splošno izmenjavo izredno pomembnih obveščevalnih podatkov, temveč bodo izmenjavale podatke na podlagi predhodne selekcije in na bilateralnem nivoju. Pri multilateralnem nivoju sodelovanja pa pridejo predvsem v poštev izmenjave ocen, končnih obveščevalnih izdelkov, analiz itd. (Aldrich 2004: 732).
 - **Vzajemno izobraževanje in usposabljanje.** Prakso izobraževanja in usposabljanja uvajajo predvsem tiste službe, ki želijo razširiti svoj politični vpliv³⁷. Za tovrstno dejavnost je skicevanje na nevarnost množičnega terorizma zelo prikladno, saj je velika večina držav bolj ali

³⁷ Vse štiri obveščevalne službe, ki sem jih preučeval, poskušajo »izvažati« svoje metode delovanja, istočasno pa izvajajo proces indoktrinacije drugih služb, predvsem v tistih državah, ki se nahajajo na interesnih območjih »velikih« držav. Tako Cia krepi svoj vpliv med državami ameriškega interesnega območja, v veliki meri se ji pridružuje SIS. Skupaj predstavljata osnovo širšega anglosaksonskega obveščevalnega sodelovanja, imenovanega UKUSA. Dalje ruska SVR poskuša okrepiti svoj vpliv v državah bivše Sovjetske zveze. Mossad pa se usmerja v zmerne islamske države in njihove obveščevalne službe ter intenzivno sodeluje z njimi, predvsem na področju usposabljanja za boj proti terorizmu.

manj intenzivno pripravljena na »izobraževanje« o boju proti terorizmu. Na takšen način močne obveščevalne službe prihajajo do ključnih informacij o interesih in sestavi agenturne mreže gostujočih služb.

- **Sodelovanje pri skupnih projektih na različnih področjih** (tehnično, operativno itd.). Tovrstno sodelovanje je lahko kratkoročno ali dolgoročno orientirano. Pri kratkoročnem sodelovanju so v ospredju operativni projekti, ki zajemajo spremljanje in delovanje v primeru znanih aktivnosti določene teroristične organizacije. Dolgoročno sodelovanje pa je bolj tehničnega³⁸ in političnega značaja, ker potrebuje več finančnih, tehničnih in kadrovskih virov za svojo uresničitvev.
- Po obliki poznamo dva tipa sodelovanja:
 - **Bilateralno sodelovanje.** Predstavlja osnovo mednarodnega sodelovanja obveščevalnih služb. Poteka na nivoju stikov dveh služb in velikokrat temelji na izgradnji medsebojnega zaupanja, kar je dolgotrajen proces. Ta oblika sodelovanja je, zaradi velikega zaupanja in dejstva, da največkrat samo v takšni obliki sodelovanja pride do izmenjave primarnih obveščevalnih podatkov in celo do izmenjave informacij o virih, pogosto zavita v skrivnost. Kljub temu so znana dejstva o izjemno močnih povezavah med Cio in SIS ter med Cio in Mossadom.
 - **Multilateralno sodelovanje.** Je sicer manj tajno, ne tudi manj pomembno. Tukaj sicer ni splošna praksa, da bi prihajalo do intenzivnega izmenjavanja primarnih obveščevalnih podatkov, ampak je moč zaznati hitrejše sodelovanje v specifičnih primerih in učinkovitejšo izmenjavo omejenih podatkov (Aldrich 2004: 737). Prav tako je tovrstno sodelovanje primerno za oblikovanje skupnih politik in strategij na področju boja proti terorizmu. Pri multilateralnem sodelovanju pa obstajata vsaj dva tipa. V preteklosti so obstajale in še obstajajo posebne institucije, ki so delovale na nivoju obveščevalnih služb, namenjenih koordiniranju medsebojnega delovanja.³⁹ Naslednji

³⁸ Oblikovanje sistema ECHELON.

³⁹ Skupini KILOWATT in MEGATONE, ki sta bili prva foruma predvsem evropskih obveščevalnih služb, katerih glavni namen je bila izmenjava informacij o terorističnih aktivnostih (Shlomo 2001).

nivo sodelovanja pa so nadnacionalne organizacije, ki v svoji strukturi vsebujejo posebne oddelke, namenjene izmenjavi obveščevalnih informacij.

- Stiki med službami lahko potekajo brez ali z vednostjo odgovornih državnih organov.

Pogosto se dogaja, da obveščevalne službe predstavljajo neformalno diplomacijo, in sicer v državah, ki medsebojno nimajo ustreznih diplomatskih odnosov. Lahko pa se zgodi, da obveščevalne službe vzpostavijo medsebojne stike tudi popolnoma brez vednosti ustreznih državnih organov, kar pogosto pomeni prekoračenje pooblastil službe.

V primeru mednarodnega terorizma je razmišljanje samo v okviru nacionalnih meja nezadostno. Obveščevalne službe bodo prisiljene k še večji stopnji mednarodnega sodelovanja in izmenjavi primernih obveščevalnih podatkov. Vendar bodo aktivnosti obveščevalnih služb in njihovo mednarodno sodelovanje pod močnim vplivom mednarodnega okolja, ki ga determinirajo mednarodno pravo, človekove pravice, interesi posameznih držav, nevarnost širjenja konfliktov in strah pred številnimi nedolžnimi žrtvami v primeru novih napadov (Karmon 1998).

8 ZAKLJUČEK

V svoji prvi delovni hipotezi sem trdil, da so teroristični napadi 11. septembra 2001 prisilili države, da prilagodijo lastne nacionalnovarnostne sisteme sodobnim virom ogrožanja, predvsem mednarodnemu terorizmu.

Na podlagi študije primerov štirih nacionalnovarnostnih sistemov sem ugotovil, da je osrednja skupna točka vseh sistemov nacionalne varnosti prisotnost tranzicije v iskanju novega modela zagotavljanja nacionalne varnosti, ki izvira iz pojava novih oblik ogrožanja.

Vse štiri države postavljajo grožnjo, ki jo predstavlja mednarodni terorizem, na visoko mesto, zato lahko trdim, da je danes mednarodni terorizem prioriteta, s katero se ukvarjajo politične in varnostne institucije analiziranih držav.

Kar zadeva spremembe v sistemih nacionalne varnosti, lahko rečem, da so se večinoma izvajale po zelo odmevnih terorističnih napadih in ne neposredno zaradi konca hladne vojne in percepcije novih oblik ogrožanja. Vsi dokumenti, ki govorijo o spremembi mednarodnega varnostnega okolja in o pojavu novih virov ogrožanja omenjajo boj proti terorizmu kot eno izmed glavnih nalog, vendar kot sem ugotovil, so bili pretresljivi teroristični napadi tisti, ki so sprožili procese spreminjanja nacionalnovarnostnega sistema.

Nadalje sem v analizi posameznih sistemov ugotovil, da se z bojem proti terorizmu ne ukvarja samo en organ, temveč je to kompleksen interdisciplinarni proces, ki v svoje delovanje vključuje vse prvine in podprvine sistema nacionalne varnosti. Še posebej je izpostavljena vloga obveščevalnih in varnostnih služb, oboroženih sil, civilne obrambe in varnostne politike.

Težava se pojavi pri koordinaciji dela vključenih inštitucij in pri izmenjavi ustreznih informacij, ki izvirajo iz obveščevalne dejavnosti. V vseh sistemih so doumeli nujnost oblikovanja neodvisnega koordinacijskega telesa s širšimi pooblastili, predvsem kar zadeva določanje nalog posameznim organom, vendar je praksa delovanja tega

telesa precej drugačna. V ZDA obstaja nacionalni protiteroristični center (NCTC), zadolžen za izmenjavo obveščevalnih podatkov, ki se navezujejo na terorizem, a ta center nima nikakršnih pooblastil v primeru protiterorističnega delovanja. Takrat glavno vlogo prevzame Ministrstvo za domovinsko varnost, ki usklajuje delovanje Zveznega preiskovalnega biroja (FBI), Nacionalne varnostne službe (NSA) in številne druge inštitucije, ki imajo v spektru svojih nalog opredeljen boj proti terorizmu. Na drugačno ureditev naletimo v vseh treh drugih državah, kjer osrednjo vlogo v boju proti terorizmu igra notranja varnostna služba oziroma organ v njeni sestavi. V VB to vlogo igra MI5 oziroma preko nje Skupni analitični center za terorizem (JTAC). V RF je koordinacijska vloga v domeni FSB in podobno tudi v Izraelu, kjer je Shin Beth osrednja organizacija v boju proti terorizmu. V primeru čezmejnega delovanja proti terorizmu pa v vseh primerih osrednjo vlogo prevzamejo obveščevalne službe.

Zanimiva je tudi primerjava vloge vojske v protiterorističnem delovanju. Čeprav se vojska v vseh štirih nacionalnovarnostnih sistemih omenja kot pomemben faktor, pride njen vpliv do izraza predvsem v primeru RF in Izraela. Prav tako se samo v teh dveh državah pojavlja oblika nadzora nad mediji, kar zadeva poročanje o terorističnih aktivnostih oziroma protiterorističnih akcijah.

Naslednja skupna točka teh držav oziroma njihovih sistemov je agresivna varnostna politika, ki v imenu boja proti terorizmu brezkompromisno omogoča uporabo skoraj vseh obstoječih sredstev, velikokrat na račun krčenja človekovih pravic. Če primerjam posamezne strategije boja proti terorizmu, opazim načrtno krčenje človekovih pravic in svoboščin ter temeljev pravne države. Tako so v ZDA vzpostavili tajna sodišča, v VB možnost časovno nedoločenega pripora in izгона, v RF sistem protiugrabitve in napad na civilna transportna sredstva, če gre za sum ugrabitve, in v Izraelu načrtno eksekucije in getoizacijo palestinskih ozemelj. V vseh primerih pa so organi prisile pridobili večja pooblastila in močne finančne injekcije.

Na podlagi izvedene primerjalne analize ugotavljam, da lahko kljub nekaterim razlikam v oblikovanju in delovanju nacionalnovarnostnega sistema identificiram temeljne skupne točke boja proti mednarodnemu terorizmu. Te točke so: stalno spreminjanje sistema, potreba po koordinaciji, sodelovanje več institucij, sprejemanje ustrezne zakonodaje, omejevanje in krčenje človekovih pravic itd.

Vse te spremembe pa so se začele izvajati v obdobju po 11. septembru 2001, zato lahko potrdim zastavljeno delovno hipotezo. Ta datum pomeni prelomnico v percepciji nevarnosti, ki jo predstavlja mednarodni terorizem. Vse države so po tem datumu korenito posegle v sistem boja proti terorizmu, še posebej ZDA, ki je bila neposredno najbolj prizadeta.

V drugi delovni hipotezi sem trdil, da obveščevalne službe v boju proti terorizmu posvečajo vedno večjo pozornost zbiranju obveščevalnih podatkov s pomočjo človeških virov.

V obdobju hladne vojne so obveščevalne službe pri svojem delu v veliki meri uporabljale metode zbiranja podatkov s pomočjo tehničnih sredstev, kar je bilo v skladu s takratnim dojemanjem druge države kot glavnega vira ogrožanja in skladno z lastno politiko zagotavljanja nacionalne varnosti. V današnjem obdobju pa smo priča sodobnim virom ogrožanja, ki silijo obveščevalne službe k spremembam metod delovanja in preusmeritvi osrednje pozornosti od sovražnih obveščevalnih služb in držav k boju proti mednarodnemu terorizmu.

Podobno kot pri analizi nacionalnovarnostnih sistemov tudi pri obveščevalnih službah ugotavljam, da le-te še niso najboljše pripravljene na delovanje v novih varnostnih razmerah, ki zahtevajo drugačno logiko delovanja kot doslej. Vse štiri službe, ki ob svoji primarni dejavnosti, zbiranju obveščevalnih podatkov, opravljajo tudi širok spekter drugih nalog, od katerih je večina označenih kot tajne operacije, se soočajo s tranzicijskimi težavami. Tako ugotavljam, da se ob koncu hladne vojne pojavi trend ekonomske obveščevalne dejavnosti, ki velikrat pomeni osrednjo dejavnost obveščevalnih služb, kar ob pojavu sodobnih virov ogrožanja še bolj poglobi tranzicijske težave obveščevalnih služb.

Bistveni problem, na katerega sem naletel pri analizi delovanja obveščevalnih služb, je nezadostno sodelovanje in izmenjava obveščevalnih podatkov z drugimi organi nacionalnovarnostnega sistema. Velikokrat je to posledica nepripravljenosti vodstva služb za bolj pristno sodelovanje, predvsem zaradi občutka izgube vodilne vloge pri oblikovanju nacionalnovarnostne politike in pri zagotavljanju nacionalne varnosti. Takšen primer zasledimo pri Cii, ki je z reformo izgubila koordinacijsko vlogo v

obveščevalni skupnosti, ali pri Mossadu, ki sta mu osrednjo protiteroristično vlogo odvzela Aman in Shin Beth. Podobne težave se kažejo tudi v SIS in SVR, predvsem zaradi povečevanja pristojnosti varnostnih služb. Tako se vloga obveščevalnih služb velikokrat zreducira zgolj na zbiranje neobdelanih obveščevalnih podatkov.

Če bi obveščevalne službe znova želele doseči pomemben položaj znotraj nacionalnovarnostnega sistema, morajo razumeti temeljne dejavnike terorizma. Iz prakse je razvidno, da so obveščevalne službe omenjenim petim dejavnikom začele posvečati večino svojih zmogljivosti, predvsem kar zadeva zbiranje podatkov in izvajanje tajnih akcij. Skupna značilnost vseh petih dejavnikov pa je velika tajnost, fleksibilnost in neizsledljivost. To pa so tiste lastnosti sodobnega mednarodnega terorizma, ki od obveščevalnih služb zahtevajo večje vložke na področju zbiranja podatkov s pomočjo človeškega faktorja.

Vse štiri službe so kot osrednjo teroristično grožnjo identificirale skrajne islamske skupine in temu dejstvu tudi prilagodile svoje metode delovanja. Opazno je povečano rekrutiranje novih agentov z arabskim poreklom, ki se lažje znajdejo na terenu in zato tudi bolj uspešno izvedejo zastavljene naloge. Nadalje se večji poudarek namenja jezikovnemu in kulturnemu izobraževanju, kar ponovno omogoča lažje pridobivanje obveščevalnih podatkov in boljše ter hitrejše razumevanje le-teh.

Če lahko na podlagi predstavljene analize potrdim drugo delovno hipotezo, pa se glede učinkovitosti delovanja obveščevalnih služb zastavlja novo vprašanje, in sicer, kako zagotoviti ustrezno sodelovanje služb z drugimi akterji nacionalnovarnostnega sistema, odgovornimi za protiteroristično delovanje. Ponujata se dva možna pristopa, in sicer vzpostavitev mreženja, kjer vsi vpeti organi delijo vse obveščevalne podatke, ki se navezujejo na specifično področje. Tako dobimo pregled nad vsemi razpoložljivimi podatki in se izognemo podvajanju. Drugi način pa je oblikovanje hierarhičnega in restriktivnega sistema, ki z ustrezno zakonodajo določa delovna področja in postopek posredovanja pridobljenih podatkov. Vendar je izbira ustreznega sistema odvisna od zunanjih in notranjih dejavnikov v nacionalnovarnostnem sistemu.

V tretji delovni hipotezi trdim, da sodelovanje in izmenjava informacij med obveščevalnimi službami omogočata večjo uspešnost boja proti mednarodnemu terorizmu.

Sodobni terorizem je zelo »uspešen« globalizacijski proces, ki pri svojih aktivnostih ne upošteva nacionalnih meja. Globalnost delovanja osrednje grožnje nacionalni varnosti zahteva tudi mednarodno orientacijo v delovanju obveščevalnih služb. Če sem pred tem omenil težave pri sodelovanju obveščevalnih služb znotraj nacionalnovarnostnega sistema, je situacija pri mednarodnem sodelovanju še toliko težja. Službe so prisiljene sodelovati z drugimi in z njimi izmenjavati pomembne obveščevalne podatke, predvsem zaradi specifik delovanja posameznih služb in nezmožnosti pridobivanja podatkov izključno z lastnimi zmogljivostmi. Če pa želimo govoriti o kakovostnem mednarodnem sodelovanju, mora biti vzpostavljeno medsebojno zaupanje, ki je temelj izmenjave občutljivih obveščevalnih podatkov in virov. Zato se tovrstne izmenjave dogajajo predvsem na bilateralnem nivoju, kjer je manjše tveganje, da pride do izdaje in zlorabe podatkov. Pri proučevanju obveščevalnih služb sem ugotovil, da se njihovo mednarodno sodelovanje še posebej izpostavlja predvsem v interesu skupnih akcij, usposabljanja in izmenjave podatkov. Tako lahko obveščevalne službe z medsebojnim sodelovanjem prispevajo k dvigovanju kolektivne zavesti o nevarnosti mednarodnega terorizma in k oblikovanju nadnacionalnih varnostnih mehanizov, ki lahko omejijo delovanje terorizma na globalnem nivoju. Zato lahko potrdim tudi tretjo delovno hipotezo.

V glavni hipotezi, ki združuje misli vseh delovnih hipotez, trdim, da so s pridobivanjem pravočasnih in uporabnih informacij o nameri in delovanju terorističnih organizacij in/ali teroristov posameznikov obveščevalne službe najpomembnejši akter nacionalnovarnostnega sistema v uspešnem boju proti mednarodnemu terorizmu.

Na podlagi vsebine in sklepnih razmišljanj v diplomskem delu lahko glavno hipotezo potrdim le delno. Res je, da pravočasne in uporabne informacije omogočijo oblikovanje ustrezne obrambe pred terorističnimi napadi toda kot se je večkrat izkazalo v praksi, lahko odsotnost pravočasnih informacij oziroma celo njihovo neupoštevanje pripelje do katastrofalnih posledic.

V nasprotju s prvim delom hipoteze pa ne morem potrditi drugega dela, in sicer da so obveščevalne službe najpomembnejši akter v boju proti mednarodnemu terorizmu. Praksa je pokazala, da kljub pogostemu omenjanju obveščevalnih služb kot osrednjih institucij za protiteroristično delovanje največji del tega delovanja pripada varnostnim službam.

Vendar sem glede na mednarodno razširjenost terorizma in medsebojne povezanosti držav v mednarodnem okolju pričakoval, da bodo obveščevalne službe bolj v ospredju boja proti terorizmu. Menim, da je vzrok za takšno stanje še zmeraj v nezadostni reformi obveščevalnih služb in nacionalnovarnostnih sistemov. Države prav tako večino pozornosti posvečajo oblikovanju varnostnih ukrepov, ki naj bi prispevali k zmanjševanju posledic napadov in ranljivosti nanje, vse premalo pozornosti pa se posveča tistim ukrepom, ki bi vzpodbujali opuščanje terorističnih aktivnosti. In ravno v takšni preventivni vlogi vidim prihodnost obveščevalnih služb, ki bodo s pridobivanjem kakovostnih informacij omogočale oblikovanje in izvajanje nacionalnih politik, katerih osrednji cilj bo omogočanje trajnostnega razvoja vsakega posameznika in celotne družbe.

9 LITERATURA

Primarni viri

1. A National Security Strategy for a New Century (1997), White House, D.C.
2. FBI policy and guidelines, http://www.fbi.gov/publications/terror/terror2000_2001.htm (23. 6. 2005).
3. Federalnij zakon ob operativno-razysknoj dejatelnosti (1995): Moskva, Sobranje zakonodateljstva Rossijskoj Federaciji, št. 144-F3, ot 12. 8. 1995.
4. Federalnij zakon o borjebe s terorizmom (1998): Moskva, Sobranje zakonodateljstva Rossijskoj Federaciji, št. 130-FZ, ot 3. 7. 1998.
5. Federalnij zakon o vnešnej razvedke (1996): Moskva, Sobranje zakonodateljstva Rossijskoj Federaciji, št. 5-F3, ot 10. 1. 1996.
6. Goss, Porter J. (2005): Global Intelligence Challenges 2005: Meeting Long-Term Challenges with a Long-Term Strategy. Testimony of Director of Central Intelligence Porter J. Goss Before the Senate Select Committee on Intelligence, http://www.cia.gov/cia/public_affairs/speeches/2004/Goss_testimony_02162005.html (7. 2. 2006).
7. Goss, Porter J. (2005): Remarks by Director of the Central Intelligence Agency Porter J. Goss to CIA Employees, http://www.cia.gov/cia/public_affairs/speeches/2005/Goss_address_09232005.html (7. 2. 2006).
8. Intelligence and Security Committee (2002): *Annual Report 2001-2002*. <http://www.cabinetoffice.gov.uk/publications/reports/intelligence/Intelligence.pdf> (8. 5. 2006).
9. Intelligence and Security Committee (2004): *Annual Report 2003-2004*. <http://www.cabinetoffice.gov.uk/publications/reports/intelligence/annualir0304.pdf> (8. 5. 2006).
10. Intelligence and Security Committee (2005): *Annual Report 2004-2005*. <http://www.cabinetoffice.gov.uk/publications/reports/intelligence/iscannualreport.pdf> (8. 5. 2006).
11. Intelligence Reform and Terrorism Prevention Act (2004), Passed by the House of Representatives, Public Law 107-296, 17 December.

12. Intelligence Services Act (1994), http://www.opsi.gov.uk/ACTS/acts1994/Ukpga_19940013_en_1.htm (12. 2. 2006).
13. Interfax (2002): Intervju z direktorjem SVR, Sergejem Lebedevim ob 82. obletnici obstoja SVR, 20. 12. 2002.
14. Interfax (2005): Intervju z direktorjem SVR, Sergejem Lebedevim ob 85. obletnici obstoja SVR, 19. 12. 2005.
15. National Intelligence Machinery (2000). London: The Stationary office.
16. National Security Strategy (2002), White House, D.C.
17. National Strategy for combating Terrorism (2003), White House, D.C.
18. National Strategy of Homeland Security (2002), White House, D.C.
19. Negroponte, John D. (2006): Annual Threat Assessment of the Director of National Intelligence for the Senate Select Committee on Intelligence, http://www.dni.gov/testimonies/20060202_testimony.pdf (15. 3. 2006)
20. Regulation on investigatory powers act (2000), <http://www.opsi.gov.uk/acts/acts2000/20000023.htm> (12. 2. 2006)
21. Soldatov, Andrei (2006), novinar, korespondenčni intervju o vlogi SVR v boju proti terorizmu, 15. 5. 2006.
22. The Role and Status of DoD Red Teaming Activities (2003), Department of Defence, D.C., <http://www.acq.osd.mil/dsb/reports/redteam.pdf> (25. 2. 2006).
23. U.S. Army, Field manual 100-20, Stability and Support operations, »Chapter 8: Combatting Terrorism.« <http://www.bol.ucla.edu/~chuugle/combat.htm> (15. 6. 2005).

Sekundarni viri

1. Ahlin, Martin *et al.*, ur. (2000) *Slovar slovenskega knjižnega jezika*. Ljubljana: DZS.
2. Aldrich, J. Richard (2004) Transatlantic Intelligence and Security Cooperation. *International Affairs* 80(4), 731-753.
3. Anžič, Andrej (1996): *Vloga varnostnih služb v sodobnih parlamentarnih sistemih – nadzorstvo*. Ljubljana: ČZP Enotnost.
4. Anžič, Andrej (1997): *Varnostni sistem Republike Slovenije*. Ljubljana: Uradni list Republike Slovenije.

5. Anžič, Andrej (2002): Mednarodni terorizem – varnostni izziv in dileme. *Teorija in praksa* 39(3), 454-466.
6. bbc.co.uk (2003): MI6 – the Secret Intelligence Service. <http://www.bbc.co.uk/print/crime/fighters/mi6.shtml> (17. 3. 2006).
7. Ben-David, Alon (2004): Israel reactivates Mossad. *Jane's intelligence review* 16(1), 46-49.
8. Bennett, Gordon (2000): The SVR, Russia's Intelligence Service. <http://www.fas.org/irp/world/russia/svr/c103-gb.htm> (16. 3. 2006).
9. Blanche, Ed (2002): Terror attacks threaten Gulf's oil routes. *Jane's Intelligence Review*, 14(12), 6-11.
10. Campbell, Andrew (1994): Yevgenni Primakov and the SVR. *Australia & World Affairs* 21(4), 15-26.
11. Cogan, Charles (2004): Hunters not Gatherers: Intelligence in the Twenty-First Century. *Intelligence and National Security* 19(2), 304-321.
12. Corera, Gordon (2005): UK makes changes to Secret Intelligence Service. *Jane's Intelligence Review* 17(2), 48-51.
13. Cralley, William E. et al.,. (2004): *Understanding Terrorism Lessons of the past – Indicators for the future*. Alexandria: Institute for defence analyses.
14. Črnčec, Damir (2004): Obveščevalno-varnostna dejavnost vs. človekove pravice in temeljne svoboščine po 11. septembru 2001. V Branko Lobnikar (ur.) *Dnevi varstvoslovja*, 58-66. Ljubljana: Univerza v Mariboru, Fakulteta za policijsko-varnostne vede.
15. Drake, C. J. M. (1998): The role of ideology in terrorists' target selection <http://www.st-andrews.ac.uk/academic/intrel/research/cstpv/pdf/files/the20%role20%of20%ideology20%in.pdf> (29. 7. 2005).
16. Dupuy, Trevor Nevitt et al., ur. (1993): *International Military and Defence Encyclopedia*, 3. izd. Washington in New York: Brasse's.
17. Eedle, Paul (2002): Al-Qaeda takes fight for »hearts and minds« to the web. *Jane's Intelligence Review* 14(8), 24-26.
18. Elbaz, Michael (2005): Russian secret services links with Al-qaeda, <http://www.axisglobe.com/aricle.asp?article=269> (5. 3. 2006).
19. Eshel, David (2002): Israel refines its pre-emptive approach to counterterrorism. *Jane's intelligence review* 14(9), 20-22.

20. Galeotti, Mark (2002): Russian special forces. *Jane's intelligence review*, 14(5), 48-49.
21. Ganor, Boaz (1998): Defining terrorism: Is one man's terrorist another man's freedom fighter? <http://www.ict.org.il/articles/articledet.cfm?articleid=49> (25. 7. 2005).
22. Ganor, Boaz: Background – The Components of Counter-Terrorism. <http://www.ict.org.il> (25. 2. 2006).
23. Gazit, Shlomo (2002): Israel. V Yonah, Alexander (ur.) *Combating terrorism, Strategies of Ten Countries*, 227-259. Michigan: University of Michigan.
24. Grizold, Anton (1992): *Razpotja nacionalne varnosti: obramboslovne raziskave v Sloveniji*. Ljubljana: Univerza v Ljubljani, Fakulteta za družbene vede.
25. Grizold, Anton (ur.) (1998): *Perspektive sodobne varnosti*. Ljubljana: Univerza v Ljubljani, Fakulteta za družbene vede.
26. Grizold, Anton (1999): *Obrambni sistem Republike Slovenije*. Ljubljana: Ministrstvo za notranje zadeve, Visoka policijsko-varnostna šola.
27. Grizold, Anton, Ferfila, Bogomil (2000): *Varnostne politike velesil*. Ljubljana: Univerza v Ljubljani, Fakulteta za družbene vede.
28. Grizold, Anton; Tatalović, Siniša; Cvrtila, Vlatko (1999): *Suvremeni sistemi nacionalne sigurnosti*. Zagreb: Fakultet političkih znanosti.
29. Halilović, Zlatko (2004): Terorizem in sredstva za množično uničevanje. V Branko Lobnikar (ur.) *Dnevi varstvoslovja*, 154-163. Ljubljana: Univerza v Mariboru, Fakulteta za policijsko-varnostne vede.
30. Herman, Michael (1996): *Intelligence power in peace and war*. Cambridge: Cambridge University Press.
31. Hulnik, Arthur S. (2006): U.S. Intelligence Reform: Problems and Prospects. *International Journal of Intelligence and Counterintelligence* 12(2), 302-315.
32. Kahana. Ephraim (2002): Reorganizing Israel's Intelligence Community. *International Journal of Intelligence and Counterintelligence* 15(3), 415-428.
33. Karmon, Ely (1998): Intelligence and the Challenge of Terrorism in the 21st Century. <http://www.ict.org.il> (14. 9. 2005).
34. Keegan, John (2004): *Intelligence in War: Knowledge of the Enemy from Napoleon to Al-Qaeda*. Washington: The Washington Post Co.

35. Keet, Maria C. (2003): *Terrorism and game theory*. Limerick: University of Limerick. <http://www.dcs.napier.ac.uk/~cs203/TerrorismGameTheory.pdf> (23. 6. 2005).
36. Krunic, Zoran (1997): *Strategija posrednega nastopanja*. Ljubljana: Založba Unigraf.
37. Krunic, Zoran (1999): Obveščevalno-varnostni sistem Velike Britanije. *Borec* 51(577-578), 206-237.
38. Levkov, Milivoje (2001): *Izraelska tajna služba*. Beograd: »Filip Višnjic«.
39. Martin, L. John. (1985): The Media's role in international terrorism. <http://pegasus.cc.ucf.edu/~surette/mediasrole.html> (17.5.2005).
40. Miholic, Andrej (2004): *Logistične značilnosti sodobnih terorističnih skupin* (diplomsko delo). Ljubljana: Univerza v Ljubljani, Fakulteta za družbene vede.
41. Mossad the Institute for Intelligence and Special Tasks (2006). <http://www.fas.org/irp/world/israel/mossad/index.html> (15. 3. 2006).
42. Phythian, Mark (2005): Still a Matter of Trust: Post-9/11 British Intelligence and Political Culture. *International Journal of Intelligence and Counterintelligence* 18(4), 653-681.
43. Požun, Janko (2004): *Obveščevalno-varnostni sistem Izraela* (diplomsko delo). Ljubljana: Fakulteta za družbene vede.
44. Podbregar, Iztok (2004): Vloga obveščevalnih služb v boju proti mednarodnemu terorizmu. V Branko Lobnikar (ur.) *Dnevi varstvoslovja*, 30-34. Ljubljana: Univerza v Mariboru, Fakulteta za policijsko-varnostne vede.
45. Polk, William R. (1997): *Neighbors & strangers: the fundamentals of foreign affairs*. Chicago in London: The university of Chicago Press.
46. Polmar, Norman; Allen, Thomas B. (1998): *Spy book: The encyclopedia of espionage*. New York: Random house.
47. Prezelj, Iztok (2005): *Nacionalni sistemi kriznega menedžmenta*. Ljubljana: Fakulteta za družbene vede.
48. Purg, Adam (1995): *Obveščevalne službe*. Ljubljana: ČZP Enotnost.
49. Purg, Adam (1997): *Boj proti mednarodnemu terorizmu*. Ljubljana: Ministrstvo za notranje zadeve, Visoka policijsko-varnostna šola.
50. Purg, Adam (2001): Vloga obveščevalnih in varnostnih služb v političnih sistemih: primer Ruske federacije. *Teorija in praksa* 38(1), 103-118.

51. Purg, Adam (2002): *Primerjalni obveščevalni sistemi*. Ljubljana: Univerza v Mariboru, Visoka policijsko-varnostna šola.
52. Purg, Adam (2004): Spremembe varnostno-obveščevalnega sistema v luči boja proti mednarodnem terorizmu po 11. 9. 2001: študija primera Ruske federacije. *Varstvoslovje* 6(2), 163-170.
53. Raščan, Stanislav (2005): *Spremembe varnostne politike ZDA po 11. septembru 2001*. Ljubljana: Fakulteta za družbene vede.
54. Richardson, Louise (2000): Terrorists as transnational actors. V Max Taylor (ur.) in John Horgan (ur.) *The future of terrorism*, 209-219. London in Portland: Frank Cass.
55. Richelson, Jeffrey (1999): *The U.S. intelligence community*. Boulder: Westview Press.
56. Shahar, Yael (2001): Tracing bin Laden's Money: Easier said than done, <http://www.ict.org.il/articles/articledet.cfm?articleid=387> (20. 4. 2005).
57. Shpiro, Shlomo (2001): The Communication of Mutual Security: Frameworks for European-Mediterranean Intelligence Sharing. Ramat Gan: Bar-Ilan University, <http://www.nato.int/acad/fellow/99-01/shpiro.pdf#search='nato%20intelligence%20shpiro> (25. 3. 2006).
58. Smith, Daniel (2004): Background on the Role of Intelligence in Rooting Out Terrorism. <http://www.cdi.org/terrorism/intelligence-role-pr.html> (3. 11. 2004).
59. Sobelman, Daniel (2004): Damascus killing reflects changes in Mossad. *Jane's intelligence review* 16(11), 28-29.
60. Soldatov, Andrei; Borogan, Irina (2005): Terrorism prevention in Russia: one year after Beslan. Agentura.Ru Studies and Research Centre. <http://agentura.ru/english/dosie/terrorismprevention/preventsystem.pdf> (25. 2. 2006).
61. Stopar, Mirko (2002): Boj proti mednarodnemu terorizmu – vloga in pomen oboroženih sil. V Lobnikar, Branko (ur.) *Dnevi varstvoslovja*, 1-9. Ljubljana: Univerza v Mariboru, Fakulteta za policijsko-varnostne vede.
62. Strindberg, Anders (2004): Khalil assassination sours relations with Jordan. *Jane's intelligence review* 16(11), 26-29.
63. SVR Operations (1997). <http://fas.org/irp/world/russia/svr/ops.htm> (25. 2. 2006).
64. SVR Organization (1997). <http://fas.org/irp/world/russia/svr/org.htm> (25. 2. 2006).

65. Šaponja, Vladimir (1999): *Taktika dela obveščevalnovarnostnih služb*. Ljubljana: Univerza v Ljubljani, Visoka policijsko-varnostna šola.
66. Thackrah, J. R. (2004): *Dictionary of terrorism*. London in New York: Routledge.
67. The Economist (2005): Reforming Britain's Intelligence Services. *The Economist*, 17. 5. 2005.
68. Todd, Paul; Bloch, Jonathan (2003): *Global Intelligence. The World's Secret Services Today*. New York: Zed books.
69. Urban, Mark (1996): *UK Eyes Alpha: The Inside Story of British Intelligence*. London: Faber and Faber Ltd.
70. Warner, Michael; McDonald, J. Kenneth (2005): US Intelligence Community Reform Studies since 1947. <http://www.fas.org/irp/cia/product/reform.pdf> (23. 1. 2006).
71. Whine Michael (1999): Cyberspace A new medium for communication, command and control by extremists. <http://www.ict.org.il/articles/articledet.cfm?articleid=76> (18. 5. 2005)