UNIVERZA V LJUBLJANI
FAKULTETA ZA DRUŽBENE VEDE

Jaroš Britovšek

PROTIOBVEŠČEVALNA DEJAVNOST V SODOBNI DRŽAVI

Diplomsko delo

Ljubljana 2007

UNIVERZA V LJUBLJANI
FAKULTETA ZA DRUŽBENE VEDE

Jaroš Britovšek

Mentor: Doc. dr. Iztok Prezelj

PROTIOBVEŠČEVALNA DEJAVNOST V SODOBNI DRŽAVI

Diplomsko delo

Ljubljana 2007

ZAHVALA

Zahvaljujem se svojim staršem in družini za vso podporo in vzpodbudo v času mojega študija.

Hvala tudi prijateljem za skupno pot skozi nepozabna študentska leta.

PROTIOBVEŠČEVALNA DEJAVNOST V SODOBNI DRŽAVI

Navzoče delo govori o protiobveščevalni dejavnosti v sodobni državi. Na začetku definira temeljne pojme in opiše razliko ter povezanost med protiobveščevalno, obveščevalno in varnostno dejavnostjo. Sledi opis glavnih protiobveščevalnih funkcij, kot so identifikacija in ocena groženj ter nevtralizacija in izkoriščanje nasprotnikove obveščevalne aktivnosti. Po teoretičnem delu opiše trenutne protiobveščevalne dejavnosti po posameznih državah, kot so ZDA, Rusija, Velika Britanija, Nemčija in Izrael. Predstavljene so njihove glavne obveščevalno varnostne službe, ki se ukvarjajo s tem področjem. Za tem so podani tudi primeri po posameznih državah. V zadnjem poglavju je opisana gospodarska protiobveščevalna dejavnost in posamezni primeri gospodarskega vohunjenja.

Ključne besede: protiobveščevalna dejavnost, obveščevalna dejavnost, varnostna dejavnost, vohunjenje, vohun, agent, protivohunstvo, gospodarska protiobveščevalna dejavnost.

COUNTERINTELLIGENCE IN A MODERN STATE

The present work is concerned with counterintelligence in a modern state. It starts by defining basic terms and explaining the relationship between counterintelligence, intelligence and security activities. It continues with the explanation of main counterintelligence functions such as identification and assessment of threats, as well as the neutralization and exploitation of the opponent's intelligence activity. After the theoretical part there follows a description of momentary counterintelligence activity in individual states such as the USA, Russia, Great Britain, Germany and Israel. Therein are represented the main intelligence and security agencies that deal with counterintelligence along with some specific counterintelligence cases. The last chapter describes economic counterintelligence as well as individual cases of economic espionage.

Key words: counterintelligence, intelligence, security, spying, spy, agent, counterespionage, economic counterintelligence.

KAZALO

SEZNAM KRATIC

AIPAC – ameriško-izraelski komite za javne zadeve (American Israel Public Affairs Committee)
BfV – nemška Zvezna služba za zaščito ustavne ureditve (Bundesamt fuer Verfassunschutz)
BGS – nemška Zvezna mejna zaščita (Bundesgrentzschutz)
BKA – nemški Zvezni kriminalistični urad (Bundeskriminalamt)
BND – nemška obveščevalna agencija (Bundesnachrichtendienst)
CI – protiobveščevalna služba, dejavnost (Counterintelligence)
CIA – ameriška Osrednja obveščevalna agencija (Central Intelligence Agency)
CIFA - ameriški Oddelek za protiobveščevalno dejavnost na bojišču (Department's Counterintelligence Field Activity)
FBI – ameriški Zvezni preiskovalni organ (Federal Bureau of Investigation)
FSB – ruska Zvezna varnostna služba (Federalna služba bezopasnosti)
GCHQ – britanski Vladni štab za komunikacije (Government communications headquarters)
GRU – ruska vojaška obveščevalna služba (Glavnoe Razvedivatelnoe Upravljenje)
MAD – nemška vojaška protiobveščevalna služba (Militärischer Abschirmdienst)
MI5 – britanska protiobveščevalna služba (Military Inteligence 5, Security Service)
MI6, SIS – britanska obveščevalna služba (Military Inteligence 6, Secret Intelligence Service)
NCIX – ameriška Nacionalna protiobveščevalna eksekutiva (National Counterintelligence Executive)
NRO – ameriški Izvidniški urad (National Reconnaissancde Office)
NSA – ameriška Nacionalno varnostna agencija (National Security Agency)
RF – Ruska federacija
SND – Skupnost neodvisnih držav
SVR – Zunanja obveščevalna služba (Sluzhba Vneshney Razvedki)
VB – Velika Britanija
ZDA – Združene države Amerike
ZRN – Zvezna republika Nemčija

1. UVOD

Obveščevalna dejavnost velja za drugo najstarejšo obrt na svetu. Človek je že od nekdaj potreboval uporabne podatke in informacije, ki so mu pomagali pri odločanju. To je prišlo še posebej do izraza pri prvih konfliktih in oboroženih spopadih, kjer je bilo poznavanje nasprotnika ključnega pomena za dosego zmage. Sčasoma se je človek začel zavedati potrebe po zaščiti lastnih skrivnosti. Tako se je začela kot obramba pred obveščevalno dejavnostjo razvijati protiobveščevalna dejavnost.

Protiobveščevalna dejavnost je pomemben del obrambe držav, organizacij, skupin ipd. pred nasprotniki. Slednji si prizadevajo pridobiti informacije o svojih tekmecih, da bi s tem pridobili prednost na določenem konkurenčnem področju. Področja so lahko vojaške, gospodarske in politične narave.

Obveščevalne in protiobveščevalne službe so imele zelo pomembno vlogo v času Hladne vojne, kjer sta bila vzpostavljena dva nasprotna si in konkurenčna politično-vojaška bloka. Po koncu Hladne vojne v začetku 90-ih let je prišlo do sprememb tako na političnem kot vojaškem področju. Groženj nista več predstavljala nasprotujoča si bloka, temveč posamezni etnični in lokalni spori, ki so posledično pripeljali tudi do mednarodnega terorizma. Slednji je postal glavno področje ogrožanja mednarodnega reda.

Tem spremembam so sledile tudi obveščevalne službe. Njihov primarni cilj je postal boj proti mednarodnemu terorizmu. Zaradi tega je prišlo do zmanjšanja sredstev in kapacitet v boju proti tujim obveščevalnim službam. V nalogi želim ugotoviti kaj se v času, ko je primarni sovražnik postal terorizem, dogaja z protiobveščevalno dejavnostjo. Ali obveščevalne službe res ne ogrožajo več držav?

Nalogo sem razdelil na sedem poglavij. V tretjem poglavju bom obrazložil pojma vohunstvo in vohuni oziroma agentje, ki predstavljajo pomembno področje delovanja protiobveščevalnih služb. Osnovni pojmi, kot so protiobveščevalna, varnostna in obveščevalna dejavnost, bodo podrobneje opisani v vsebinskem delu, in sicer v četrtem poglavju. V slednjem poglavju bom opisal tudi posamezne službe, ki se

ukvarjajo s temi dejavnostmi. Poskušal jih bom razmejiti in opisati njihovo soodvisnost.

Peto poglavje bom namenil protiobveščevalnim funkcijam. Zanima me predvsem, kakšne so osnovne funkcije in načela, po katerih delujejo protiobveščevalne službe, ter kakšnih metod se pri tem poslužujejo. Pri tem bom podal tudi primere delovanja.

Naslednje poglavje se nanaša na prakso protiobveščevalne dejavnosti. Analiziral bom protiobveščevalne sisteme oz. službe držav, kot so Združene države Amerike, Rusija, Velike Britanija, Zvezna republika Nemčija ter Izrael. Pri posameznih državah bom poskušal opisati primere protiobveščevalne dejavnosti, ki so se zgodili ob koncu 90-ih in v začetku 21. stoletja. Poudariti moram, da je težko določiti časovni okvir posameznih protiobveščevalnih delovanj, saj je težko ugotoviti, od kdaj in kako dolgo posamezne akcije trajajo.

V šestem poglavju bom analiziral gospodarsko protiobveščevalno dejavnost. Zaradi vse manjšega ogrožanja držav z konvencionalnimi oboroženimi spopadi, so se zaradi globalizacije konflikti preselili na gospodarsko področje. Države in podjetja so se začela bolj zanimati za gospodarsko stanje svojih konkurentov. S tem se je posledično razvila tudi gospodarska protiobveščevalna dejavnost.

2. METODOLOŠKI OKVIR

2. 1 OPREDELITEV PREDMETA PROUČEVANJA

Protiobveščevalna dejavnosti je bistvena pri obrambi pred tujimi obveščevalnimi službami. Ker je v sodobnem svetu konvencionalen neposreden konflikt manj verjeten, poskušajo države in drugi nedržavni subjekti (organizacije, podjetja) premagati svoje nasprotnike na posreden način, predvsem z obveščevalno dejavnostjo. Da se organizacije lahko zaščitijo pred to grožnjo, morajo vzpostaviti mehanizme protiobveščevalne dejavnosti. Znotraj protiobveščevalne dejavnosti je še posebej zanimiv njen aktiven del, imenovan tudi protivohunstvo, kjer se poskuša preprečiti nelegalno pridobivanje informacij. Zanima me predvsem, kako obsežno se protiobveščevalna dejavnost izvaja danes in kako resno se gleda na obveščevalne grožnje.

2. 2 CILJI PREUČEVANJA

Cilji preučevanja, ki jih želim doseči, so naslednji:

- Definirati protiobveščevalno dejavnost.
- Opredeliti strukturo protiobveščevalne dejavnosti; strukture protiobveščevalnih sistemov držav in predstavil študije primerov protiobveščevalne dejavnosti.
- Analizirati, kako se sodobne države zavarujejo proti ogrožanju nacionalne varnosti s strani obveščevalnih služb. S tem mislim predvsem na službe, ki se v določenim državah ukvarjajo s tem področjem.
- Opredeliti funkcije in metode protiobveščevalnega delovanja. Na kakšen način in s kakšnimi sredstvi poteka delo protiobveščevalnih služb.
- Opredelitev gospodarske protiobveščevalne dejavnosti. Ali obstaja realna možnost razvoja te dejavnosti in kdo so glavni akterji.

2. 3 HIPOTEZE

V diplomi sem postavil naslednje hipoteze:

- H1: Protiobveščevalna dejavnost se lahko izvaja tako v eni službi kot tudi v več obveščevalno varnostnih službah znotraj ene države;
- H2: Metode dela protiobveščevalne dejavnosti se ne razlikujejo od metod dela varnostnih in obveščevalnih služb;
- H3: Gospodarska protiobveščevalna dejavnost dobiva vedno večji pomen v sodobnem globalnem svetu.

2. 4 UPORABLJENA METODOLOGIJA

Pri pisanju diplomske naloge sem uporabil več družboslovnih metod in s tem poskušal povečati njeno kredibilnost. Metode so sledeče:

- Analiza primarnih, sekundarnih in terciarnih virov; primarni viri mi bodo omogočili vpogled v koncepte in zakonodaje na področju protiobveščevalne dejavnosti. Sekundarni viri mi bodo pomagali pri opisovanju protiobveščevalnih funkcij, medtem ko mi bodo terciarni viri (internet) v pomoč pri iskanju primerov protiobveščevalne dejavnosti.
- Deskriptivna metoda: s to metodo bom opisal protiobveščevalne pojme in protiobveščevalne sisteme posameznih držav.
- Študije primerov, strukture in dejavnosti; opisal bom posamezne primere delovanja protiobveščevalnih služb ter njihove strukture v različnih državah.

3. OSNOVNI POJMI

Osnovne pojme, kot so obveščevalna, protiobveščevalna in varnostna dejavnost, v tem poglavju ne bom opisal, ker sem jih zaradi obsežnosti predstavil v vsebinskem delu diplomske naloge. Pojma, ki se najpogosteje pojavljata na področju protiobveščevalne dejavnosti, sta vohunstvo in agent.

3. 1 Vohunstvo

Vohunstvo je po *Velikem splošnem leksikonu* »kaznivo dejanje, ki ga stori tisti, ki služi tuji državi ali tuji organizaciji ali njunemu agentu tako, da zbira zaupne vojaške, gospodarske ali uradne podatke ali dokumente ali jim jih sporoči ali izroči ali jim omogoči, da pridejo do njih. Kaznivo dejanje stori tudi tisti, ki v škodo RS ustvari za tujo državo ali tujo organizacijo obveščevalno službo ali jo vodi, kakor tudi tisti, ki stopi v takšno obveščevalno službo ali podpira njeno delo« (Veliki splošni leksikon 2006: 4821).

Vohunstvo ali »špijonaža« je po *Vojni enciklopediji*: »pridobivanje, prisvajanje in predaja občutljivih vojaških, političnih, ekonomskih, znanstvenih, službenih in drugih podatkov ter dokumentov tuji državi ali organizaciji, odvisno kako jim oseba služi«. Lahko pomaga vzpostaviti obveščevalno organizacijo, ki dela za tujo državo, imeti stike z njo ali jim omogočati delovanje. Čeprav zakoni posameznih držav opredeljujejo vohunjenje kot nezakonito, ga mednarodno pravo ne prepoveduje. Haški pravilnik o vojskovanju iz leta 1907 pravi, da se uporaba sredstev, potrebnih za pridobivanje obveščevalnih podatkov o sovražniku in ozemlju, ne smatra za kaznivo. Kljub temu vohun, ujet na delu, ne sme biti kaznovan brez predhodnega sojenja (Vojna enciklopedija 1970: 541).

Bolj splošno definicijo najdemo v *slovarju vojaških in podobnih izrazov*, kjer piše, da je vohunjenje dejanje ohranjanja, predaje, prenosa, komunikacije ali prejemanja informacij nacionalne obrambe z namenom ali sumom, da se lahko te informacije uporabijo proti lastni državi v korist tuje (Dictionary of Military and Associated Terms 2006: 187). Pomeni uporabo vohunov ali dejanje vohunjenja za pridobitev informacij

o načrtih, dejavnostih, zmogljivostih ali resursih o sovražniku oziroma nasprotni strani. Pogosto se zamenjuje z obveščevalno dejavnostjo, vendar se razlikuje po svoji tajni, agresivni in nevarni naravi delovanja (Encyclopedia of Espionage, Intelligence, and Security 2004: 413).

»Espionage« oz vohunjenje najdemo tudi v enciklopediji *Britannica*, ki opiše pojem kot: »proces pridobivanja vojaških, političnih, komercialnih ali drugih informacij tajnega značaja s sredstvi, kot so vohuni, tajni agentje ali nelegalne prisluškovalne naprave. Vohunstvo se razlikuje od obveščevalne dejavnosti po svoji agresivni naravi in nezakonitem delovanju« (Britannica 1994: 561).

Posebni podzvrsti vohunjenja sta ekonomsko in industrijsko vohunjenje. Ekonomsko vohunjenje, nekdaj poznano kot industrijsko vohunjenje, je vohunjenje, katerega namen je izboljšati položaj komercialnih in industrijskih podjetij. To se doseže s pridobivanjem informacij, ki niso dostopne preko javnih virov. Po drugi strani ekonomska obveščevalna dejavnost s strani vlad pridobiva informacije izključno preko javnih virov (Encyclopedia of Espionage, Intelligence, and Security 2004: 373).

3. 2 Vohuni in agentje

O rabi vohunov je govoril že kitajski teoretik Sun Cu v svojem delu *»Umetnost vojne«*. Uporaba metode vohunov naj bi bila humana, saj če nisi pripravljen plačevati za obveščevalne podatke, povzročiš veliko škodo, ker ravno predznanje omogoča boljše in hitre zmage nad nasprotnikom. To predznanje nam omogočajo vohuni. Sun Cu je ločil pet vrst vohunov: lokalne, notranje, dvojne, mrtve in žive. Lokalne vohune najamemo med domačini, notranje med nasprotnikovim uradništvom, dvojne med sovražnikovimi vohuni. Tako imenovani mrtvi vohuni predajajo sovražnim vohunom prirejene podatke, živi pa se po opravljeni nalogi vrnejo domov in poročajo. Sun Cu poudarja pomembnost in koristnost vohunskega dela in s tem njihovo primerno nagrajevanje, sicer se nam lahko ta netaktičnost maščuje. Paziti je treba, če obveščevalne podatke izveš, preden ti jih posreduje tvoj vohun, ker to nakazuje na njegovo nedoslednost in nestrokovnost. O sovražniku je dobro vedeti čim več: od socialnih vezi, slabosti, prednosti in le te uporabiti sebi v prid. Kot pomembno

dejavnost opiše Sun Cu odkrivanje sovražnih vohunov, kar bi danes spadalo pod protiobveščevalno področje. Gre za odkrivanje tujih vohunov, za podkupnine in pridobivanje na svojo stran ter možnosti uporabe le-teh zase kot dvojnih vohunov. S tem lahko sovražniku posreduješ napačne podatke, to so tako imenovani mrtvi vohuni. Pri tem je potrebno paziti, da se na prava mesta postavi inteligentne ljudi (Sun Cu 1996: 163–167).

V *Velikem splošnem leksikonu* najdemo definicijo za agenta, ki ima dva pomena: splošni in vojaški. Nas zanima vojaški, ki pravi, da je agent: » posameznik, ki v korist tuje obveščevalne, vojaško varnostne ali protiobveščevalne službe skrivoma zbira vojaške, politične ali gospodarske podatke (npr. mobilizacijske in vojaške načrte, podatke o bojni pripravljenosti, formaciji, orožju in moči oboroženih sil ipd.)« (Veliki splošni leksikon 2006: 43).

V *Vojni enciklopediji* najdemo poleg definicije tudi klasifikacijo posameznih agentov. Agent je torej oseba, ki deluje po navodilih države (njenih institucij), političnih in drugih organizacij in enot ter opravlja tajno delo. Lahko je diplomatski, konzularni, obveščevalni, protiobveščevalni, vojaški, policijski ipd. Diplomatski agent opravlja delo politične narave, najpogosteje med državami (njihovimi institucijami). Obveščevalni in protiobveščevalni agent je oseba, ki pridobiva politične, ekonomske, vojaške in druge podatke za obveščevalne centre ali organizacije, odvisno kdo opravlja in preprečuje takšno dejavnost. Agent lahko deluje v zameno za denarno nagrado ali na prostovoljni bazi, večinoma je izbran za takšno delovanje pod pritiskom (Vojna enciklopedija 1970: 59–60). V literature najdemo več izrazov za agenta, vse od špijon, tajni policist, zaupnik, tajni sodelavec, vohun ipd.

Tudi v *Vojni enciklopediji* najdemo delitve agentov. Osebo, ki hkrati deluje za dve državi, imenuje »dvojnik«, oseba, ki pripravi druge ljudi, da opravijo neko nezakonito delo, se imenuje »provokator«. Opisan je še »agent za zvezo«, ki služi za vzdrževanje zveze med posameznimi vrstami agentov in njihovim centrom. V Enciklopediji posebej opozorijo na definicijo 'špijona' oz. vohuna, ki je po 29. členu Haške konvencije iz leta 1890 sledeča: » vohun je oseba, ki tajno ali pod lažno krinko deluje na operacijskem področju nasprotne strani in pridobiva ali poskuša pridobiti podatke z namenom, da jih preda nasprotni strani. Vojaško osebje, ki je prodrlo na

operacijsko stran nasprotnika, se ne smatra za vohuna« (Vojna enciklopedija 1970: 60).

Agent: v obveščevalni rabi je to oseba, ki je pooblaščena ali kateri je bilo naročeno, da pridobiva podatke ali pomaga pridobivati informacije, ki služijo obveščevalnim ali protiobveščevalnim namenom (Joint Publication 1-02 2006: 10). V splošnem je agent oseba, ki je pooblaščena za delovanje v imenu nekoga drugega. Obveščevalni agent po drugi strani ni predstavnik obveščevalne agencije, kjer so člani agencije obveščevalni uradniki, operativci ali specialni agentje. Agent pa je oseba, ki je najeta ali rekrutirana izven službe. Obstaja več vrst neformalnih poimenovanj agentov, od tajnih ali agentov pod krinko, agentje provokatorji, agentje na mestu (agent-in-place), dvojni agentje in agentje vpliva.

Operativci so torej zaposleni pri določeni obveščevalni službi in dejansko vodijo ter dajejo naloge agentom, ki so rekrutirani od zunaj. Operativcem lahko po FBI terminologiji rečemo tudi specialni agentje[1]. Operativec ponavadi vodi več agentov, ki jim pravimo **mreža agentov**. To je tajna organizacija, ki deluje pod navodili glavnega agenta (Dictionary of Military and Associated Terms 2006: 11).

Tajni agent ali agent pod krinko je oseba, ki dela za določeno službo v tajnosti, tako da se torej osebe okoli njega tega razmerja ne zavedajo. Ker agentje večinoma delujejo v tajnosti, je takšna terminologija neposrečena. Boljša poimenovanja sta dvojni agent in agent na mestu (Encyclopedia of Espionage, Intelligence, and Security, 2004: 118).

Dvojni agent: agent, ki je v kontaktu z dvema nasprotnima obveščevalnima službama, pri čemer se samo ena zaveda dvojnega kontakta ali kvazi-obveščevalnega dela (Dictionary of Military and Associated Terms 2006: 169). Opravlja torej vohunsko delo za dve, ponavadi nasprotni si državi. Dvojni agentje pridobivajo informacije za obveščevalno službo s tajno infiltracijo v sovražno organizacijo. Organizacija navadno rekrutira dvojne agente iz vrst nasprotnih

[1] Na ta način je želel J. Edgar Hoover razlikovati delo FBI agenta od navadnega policista.

obveščevalnih služb, jih spreobrne ter uporabi kot vohune za lastne interese (Encyclopedia of Espionage, Intelligence, and Security 2004: 360).

Agent na mestu je podoben dvojnemu agentu, z razliko, da je dvojni agent rekrutiran s strani službe, agent na mestu pa se prostovoljno javi za sodelovanje. Obstajajo še druga poimenovanja za agente, kot so speči agentje, agentje provokatorji in agentje za vplivanje.

Speči agent se nastavi na določeno mesto in deluje pod krinko, vendar šele po določenem času, ko dobi ukaz za izvršitev določenega dejanja. Preden se mu poda ukaz, lahko speči agent čaka po več let ali celo življenje.

Agent provokator je nekdo, ki se infiltrira v neko skupino ali organizacijo z namenom, da sprovocira določena, ponavadi nezakonita dejanja in s tem kriminalizira delovanje organizacije[2].

Agentje vpliva so osebe, ki ne delajo neposredno za obveščevalno službo, vendar so pripravljeni za njo delovati posredno. To so ljudje, ki so sponzorirani s strani obveščevalnih služb in želijo s svojim statusom ali vezami vplivati na določeno družbeno klimo[3] (Encyclopedia of Espionage, Intelligence, and Security 2004: 118).

Poznamo še posebno vrsto agenta, ki se mu reče »krt«. **Krt** je visoko zaposlen obveščevalni uradnik neke obveščevalne službe, ki izdaja podatke rivalski ali sovražni agenciji. V praksi se krt in agent na mestu razlikujeta predvsem po položaju, ki ga zasedata v organizaciji. Krti so ponavadi posamezniki, ki nosijo precej odgovornosti v agenciji, kjer so zaposleni, in so s tem informacije, ki jih predajo, večje vrednosti (Encyclopedia of Espionage, Intelligence, and Security, 2004: 279).

[2] Primer tega so agentje provokatorji, ki so koncu devetnajstega in začetku dvajstega stoletja vzpodbujali nasilje delavskih organizacij in s tem pritegnili pozornost policije.
[3] Desničarski intelektualci v ZDA, ki so sredi dvajsetega stoletja delali za Congress of Cultural Freedom, so bili sponzorirani s strani CIE z namenom, da vplivajo na javno mnenje v Zahodni Evropi. Tega se je posluževala tudi KGB z levičarskimi intelektualci.

4. OPREDELITEV PROTIOBVEŠČEVALNE DEJAVNOSTI

Najprej moram opozoriti na prevod protiobveščevalne dejavnosti iz angleščine v slovenščino. V *Začasnem angleško-slovenskem vojaškem priročnem slovarju* (ASVPS 1996: 35) pomeni 'counter intelligence' protiobveščevalno delovanje in protiobveščevalno službo. Tako v angloameriškem svetu uporabljajo izraz counter intelligence (kratica CI) za oba pojma. Problemi pri prevodih so v drugih državah, kjer se večinoma enačita protivohunska in protiobveščevalna dejavnost. Na spletni strani CI Center (The Centre for Counterintelligence and Security Studies) (Center za Protiobveščevalna in Varnostna vprašanja. Dostopno na: www.cicenter.com (20. april 2006)), je protiobveščevalna dejavnost opisana kot:

> *»identifikacija, prodor in nevtralizacija dejavnosti tujih obveščevalnih dejavnosti, ki so usmerjene v lastne državne interese, vrednote in cilje.«*

Podane so torej tri najpomembnejše naloge, s katerimi se sooča protiobveščevalna. (1) Identifikacija, ki jo lahko razlagamo kot razpoznavanje delovanja tujih služb, (2) prodor, kar po *Slovarju slovenskega knjižnega jezika* pomeni »postopno širjenje različnih vplivov na druga področja« (SSKJ. Dostopno na http://bos.zrc-sazu.si/cgi/a03.exe?name= sskj_testa&expression=penetracija&hs=1 (20. junij 2006)) in (3) nevtralizacija, se pravi »napraviti to dejavnost neškodljivo, nenevarno« (SSKJ. Dostopno na http://bos.zrc-sazu.si/cgi/a03.exe?name=sskj_testa&expression =nevtralizirati&hs=1 (20. junij 2006)). Slovenski strokovnjaki opišejo protiobveščevalno dejavnost kot:

> *»dejavnost, ki varuje državo pred delovanjem tujih obveščevalnih služb (lahko tudi posameznikov, skupin, organizacij), ki skušajo organizirano, zavestno in z nasilnimi sredstvi rušiti ali omajati ustavno ureditev« (Anžič 1997: 44).*

Opozoriti je potrebno, da je ta definicija precej splošna in ne opiše konkretnega dela oziroma funkcij delovanja protiobveščevalne. Drug slovenski avtor Vladimir Šaponja,

ki deli obveščevalno varnostne dejavnosti na zvrsti, kjer je protiobveščevalna zvrst ena izmed njih, jo opiše tako:

> *»protiobveščevalna zvrst je vrsta obveščevalne dejavnosti, ki je po svoji naravi represivna. Obveščevalna dejavnost se v tem primeru uporablja za odkrivanje, spremljanje, onemogočanje in v nekaterih primerih tudi preiskovanje kaznivih dejanj vohunstva, ki ga izvajajo tuje obveščevalne organizacije. Ne gre pa zgolj za odkrivanje vohunske dejavnosti, marveč tudi za ugotavljanje in spremljanje aktivnosti tujih obveščevalnih organizacij, kadar ne izvajajo vohunske dejavnosti. Protiobveščevalna zvrst ima tudi preventivno varnostno funkcijo«* (Šaponja 1999:58).

Šaponja tako omeni protivohunsko delovanje in opozori, da je to le del protiobveščevalne dejavnosti. Prepogosto pride do problema, da se protiobveščevalna dejavnost zamenjuje s pojmom protivohunstvo. Vendar je ta dva pojma potrebno ločevati. Protivohunstvo je namreč ožji pojem in samo del protiobveščevalne dejavnosti. Protiobveščevalna dejavnost se ukvarja z identificiranjem, razumevanjem in nevtralizacijo vsakršnega delovanja tujih obveščevalnih služb (Richelson 1999: 332). Slednja zajema namreč vse, kar počnejo tuje obveščevalne službe. Richelson tako poda še bolj podrobno razlago:

> *»protiobveščevalna dejavnost (Counterintelligence, CI) vsebuje pridobivanje informacij in aktivnosti za ocenitev delovanja tujih obveščevalnih in varnostnih služb ter nevtralizacijo sovražnih služb. Te aktivnosti vsebujejo tako tajno in odprto zbiranje podatkov kot analizo informacij, ki se nanašajo na strukture in dejavnosti tujih služb. Takšno zbiranje podatkov in analiza, v sodelovanju s tehničnim zbiranjem podatkov o sovražnem delovanju služb, se lahko uporabi za vodenje operacij zanikanja in prevar. Protiobveščevalna dejavnost je lahko tudi vpletena v neposreden prodor v sovražno obveščevalno službo in prekinitev njenih aktivnosti« (Richelson 1999:3).*

Vse, kar smo do sedaj opisali, je samo en del protiobveščevalne dejavnosti. Zgoraj opisane definicije omenjajo le aktivno naravo delovanja protiobveščevalne, obstaja pa še pasivna, ki se kaže v varnostnih ukrepih posamezne službe. Na dvojno naravo protiobveščevalne dejavnost naletimo pri Godsonu (Godson 1995: 2), ki pravi da je protiobveščevalna dejavnost:

> *»napor za varovanje lastnih skrivnosti, zaščita pred manipulacijam ter občasno izkoriščanje delovanja tujih obveščevalnih služb v lastno korist. Pri varovanju lastnih skrivnosti se država zanaša na varnostne procedure in protiukrepe. Varnostne procedure, ki so bolj pasivne narave, vključujejo omejitev oseb, ki imajo dostop do skrivnosti, zasliševanje ter vzpostavitev sistema, ki beleži izginjanje podatkov. Protiukrepi so varnostne procedure za zaščito pred določenimi taktikami tujih obveščevalnih služb. Protiobveščevalna poleg tega vsebuje tudi aktivne napore za identifikacijo, nevtralizacijo in možno izkoriščanje tujih obveščevalnih služb«.*

Iz te definicije lahko razberemo, da se protiobveščevalna dejavnost deli na dve komponenti, pasivno in aktivno. Pri tem je treba opozoriti, da definicija protiobveščevalne dejavnosti v ZDA, kot je zapisana v izvršnem odloku 12333 (Executive order 12333), ne priznava varnostne komponente protiobveščevalne dejavnosti:

> *»zbiranje informacij in vodenje aktivnosti za zaščito pred vohunjenjem, sabotažami, atentati, ki so storjeni v imenu tujih sil, organizacij ali oseb ali mednarodne teroristične dejavnosti, vendar ne vključuje osebne, fizične, dokumentacijske ali komunikacijske varnostne zaščite (Executive order 12333 1981).«*

Slednja definicija je politične narave in zajema samo en del ukrepov protiobveščevalne dejavnosti. Odlok prav tako postavlja protiobveščevalno dejavnost nasproti teroristični dejavnosti, kar pa ni pravilno. To bom skušal razložiti v naslednjih poglavjih.

Iz danega lahko izpeljemo sintezo definicij protiobveščevalne dejavnosti. Protiobveščevalna dejavnost varuje državo pred tujimi obveščevalnimi službami in njihovimi aktivnostmi. Sestavljajo jo tako pasivni ukrepi, kot so varnostni postopki, in aktivni, ki vsebujejo identifikacijo, prodor ter manipulacijo tujih obveščevalnih služb v lastno korist. V enciklopediji *Britannica* najdemo najprimernejšo definicijo pojma protiobveščevalne dejavnosti:

> *»Protiobveščevalno dejavnost sestavljajo informacije in dejavnosti, ki so povezane z zaščito lastnih informacij in skrivnosti lastnih obveščevalnih dejavnosti. Njen namen je preprečiti tujim vohunom in ostalim agentom prodreti v vladne kroge, vojsko ali obveščevalne agencije. Protiobveščevalna dejavnost prav tako deluje na področju zaščite pred terorizmom, varovanja visoke tehnologije in preprečevanja mednarodne trgovine z drogami. Lahko pripomore tudi pri zbiranju obveščevalnih podatkov, saj lahko nasprotnikovi poizkusi vdora v varnostne sisteme izdajo podatke o njegovih tehnikah, opremi in operacijskih postopkih. Protiobveščevalna dejavnost pa lahko služi tudi pri zavajanju nasprotnikove obveščevalne dejavnosti, saj so krti in dvojni agenti del resničnosti protiobveščevalne dejavnosti«* (Britannica 1994: 783).

Slednjo lahko vzamemo za najprimernejši opis protiobveščevalne aktivnosti. V nalogi se bom pri nadaljnji obravnavi te specifične obveščevalno-varnostne aktivnosti poskušal držati te definicije.

4. 1 PROTIOBVEŠČEVALNA KOT OBVEŠČEVALNA DEJAVNOST

Vemo, da je protiobveščevalna dejavnost zrcalna obveščevalni dejavnosti, zato bom v tem poglavju poskušal razložiti pojem obveščevalne dejavnosti in vzpostaviti odnos med tema konceptoma. Richelson definira obveščevalno dejavnost kot:

> »izdelek, ki izhaja iz zbiranja, predelovanja, povezovanja v celoto, analize, vrednotenja in razlage danih informacij, ki se nanašajo na tuje države in področja.«

Obveščevalna dejavnost (Intelligence) se nanaša na informacije, ki jih vlada spoznava kot pomembne za svoje vojaške, zunanje in varnostne interese. Večkrat se omenja samo kot vohunstvo, vendar jo sestavlja veliko širši spekter aktivnosti. Vsebuje vse od zbiranja, analiziranja in širjenja informacij (tako informacij odprtega in zaprtega tipa); v smislu izkoriščanja informacij kot je tajno vplivanje na dogodke tako, da delujejo v prid lastnim interesom (npr. širjenje dezinformacij) in preprečevanje delovanja obveščevalnih služb nasprotnikov (protiobveščevalna dejavnost).

Glavni elementi obveščevalne dejavnosti so zbiranje podatkov, analiza podatkov, prikrite akcije in protiobveščevalna dejavnost**.** Strogo gledano spada pod obveščevalno dejavnost samo zbiranje in analiza podatkov in njihova transformacija v obveščevalno informacijo. Vendar se tako tajne akcije kot protiobveščevalna dejavnost prepletata z obveščevalno dejavnostjo (Richelson 1999: 3).

Purg in Anžič razumeta obveščevalno dejavnost v širšem in ožjem smislu. V ožjem smislu naj bi zajemala le javno ali tajno zbiranje in analizo ter interpretacijo podatkov, ki so pomembni za državo ali pa predmet zanimanja obveščevalnih služb. v širšem smislu pa k obveščevalni dejavnosti spadajo še tajne akcije[4] in protiobveščevalna dejavnost (Anžič 1997: 42), (Purg 1995: 31).

[4] Razlikovati je potrebno med tajnim zbiranjem podatkov in tajnimi akcijami. Pri prvem gre za to, da je poudarek na tajnosti dejavnosti, pri drugih pa za to, da se zaščiti naročnik oziroma da je poudarek na tajnosti naročnika.

Šaponja (Šaponja 1999: 19) deli obveščevalno dejavnost glede na namen uporabe ali cilje. Ti so lahko informativne, represivne ali varnostno-preventivne narave. Na podlagi tega so nastale pri obveščevalni dejavnosti posamezne zvrsti: obveščevalna, protiobveščevalna, varnostna in vojaška:

> *»Obveščevalna zvrst je tako vrsta obveščevalne dejavnosti, katere namen je pridobivanje podatkov v tujini iz različnih področij (političnega, gospodarskega, znanstvenega, obrambno-strateškega in drugih). Po svoji naravi je informativne in ne represivne narave«(Šaponja 1999: 57).*

Iz povedanega lahko sklepamo, da je protiobveščevalna dejavnost del širše obveščevalne dejavnosti, saj tudi sama uporablja zbiranje in analizo podatkov o tujih službah. Prav tako pa je element obveščevalne dejavnosti, kar pomeni varnostno komponento in soočanje obveščevalnih služb s svojimi nasprotniki.

4. 2 PROTIOBVEŠČEVALNA KOT VARNOSTNA DEJAVNOST

Protiobveščevalna dejavnost je ožji pojem varnostne dejavnosti, je eden njenih delov. Varnostna dejavnost zajema namreč več vidikov varovanja države oz. institucije. Purg jo označi kot:

> *»Preprečevanje, preiskovanje in odpravljanje določenih oblik ogrožanja varnosti neke dobrine, v tem primeru države. V primerjavi z obveščevalno dejavnostjo, ki pomeni predvsem zbiranje podatkov, njihovo analiziranje in obveščanje, je zagotavljanje varnosti oziroma varnostna dejavnost predvsem ukrepanje, in sicer pretežno na način ter z metodami in sredstvi, ki se razlikujejo od načina in sredstev obveščevalne dejavnosti. Varnostno dejavnost kot funkcijo države opravljajo policija in druge varnostne službe« (Purg 1995: 34–35).*

Purg loči delovanje obveščevalne in varnostne dejavnosti predvsem na metodah dela in ukrepanju. Protiobveščevalna dejavnost spada pod to kategorijo, kadar ima pooblastila za ukrepanje proti tujim službam. Podobno definicijo poda Anžič, ki opiše varnostno dejavnost kot:

> *»dejavnost, ki pretežno temelji na ukrepanjih (tudi preventivnih) na osnovi »policijskih« pooblastil*[5]*, vključno tudi s pravico uporabe posebnih operativnih metod in sredstev dela. Te pa se razlikujejo od tistih metod in sredstev dela, ki jih tudi uporabljajo obveščevalne službe. Gre torej za to, da varnostne službe s svojo dejavnostjo, odkrivajo, preiskujejo, preprečujejo itd., medtem ko obveščevalne službe zbirajo, dokumentirajo in analizirajo informacije in podatke«(Anžič 1997: 43).*

Tako tudi Anžič razlikuje dejavnost na osnovi uporabe posebnih metod dela. Šaponja, ki jo imenuje varnostna zvrst, po drugi strani razlikuje dejavnosti tudi v smislu objekta preiskovanja:

> *»varnostna zvrst je vrsta obveščevalne dejavnosti, kjer se obveščevalna dejavnost uporablja proti organiziranem kriminalu, terorizmu, nedovoljeni trgovini in proizvodnji mamil, orožja in sredstev za množično uničevanje. Namenjena je tudi za odkrivanje, preprečevanje in varovanje pred raznimi oblikami političnega ekstremizma, radikalizma, katerega cilj je nasilno rušenje ustavne ureditve. Izvajajo jo obveščevalno-varnostne in varnostne službe.«*

Objekti varnostne zvrsti tako niso obveščevalne služba, ker te spadajo po Šaponji pod kategorijo protiobveščevalne zvrsti, ki je enakovredna varnostni. To se mi ne zdi upravičeno, ker tuje obveščevalne službe lahko prav tako ogrožajo ustavno ureditev države in so potemtakem objekt varnostne zvrsti.

[5] Policija ima z zakonom predpisane naloge. Pooblastila, ki so dana policiji, so ponavadi upravičenja, ki jih nimajo drugi organi oziroma državljani. V večini primerov bi s storitvjo takšnih dejanj kršili pozitivnopravno zakonodajo. Državljan npr. stori prekršek, če z vozilom prekorači hitrost, policist pa jo sme v upravičenih primerih bistveno prekoračiti (Žaberl 2006: 22).

Opozoriti velja, da protiteroristična dejavnost ne spada pod okrilje protiobveščevalne dejavnosti, razen če se obveščevalna služba ne poslužuje terorizma kot sredstva ali pa teroristična organizacija poseduje obveščevalne službe. Protiteroristična dejavnost je prav tako ožji pojem varnostne dejavnosti (Purg 1995: 35). V ZDA poskušajo to dejavnost spraviti pod okrilje protiobveščevalne. Čeprav Gleghorn pravi, da ne smemo enačiti protiteroristične in protiobveščevalne dejavnosti, je možno v njegovi definiciji protiobveščevalne zaslediti želje po enačenju teh dveh pojmov. Protiobveščevalno opiše kot:

> *»skupek aktivnosti za odkrivanje, ocenitev, nevtralizacijo in izkoriščanje sovražne akcije s strani tujih obveščevalnih služb in terorističnih organizacij.« (Gleghorn 2003: 10)*

Vendar pa sta protiobveščevalna in protiteroristična dejavnost različna koncepta, ki oba sodita pod okrilje varnostne in tudi obveščevalne dejavnosti. Pomemben element ločevanja teh dveh aktivnosti je objekt proučevanja.

Na podlagi definicij lahko ocenim, da je protiobveščevalna dejavnost tako del obveščevalne in varnostne dejavnosti. V prvem primeru uporablja metode zbiranja in analize podatkov, v drugem pa preiskuje in preprečuje dejavnosti tujih obveščevalnih služb, ki prav tako ogrožajo ustavno ureditev.

4. 3 PROTIOBVEŠČEVALNA SLUŽBA

4. 3. 1 Razvoj protiobveščevalne službe.

V sužnjelastniškem obdobju je bil državni aparat slabo razvit, varnostne naloge so neposredno izvajali vladarji in njim neposredno podrejeni služabniki. V Šparti so npr. efori nadzirali obnašanje sužnjev. V atenski državi so uslužbenci skrbeli za nadzor nad sužnji s pomočjo vohunov, ki so se imenovali sikofani. Podobno je bilo v rimski državi, kjer so vohuni imeli pravico do dela lastnine osebe, katero so izdali. Poleg teh aktivnosti ni bilo posebne organizacije, ki bi se ukvarjala z varovanjem.

V fevdalni državi, v času absolutnih monarhij, ko se je gradil državni aparat, se pojavijo prve organizirane varnostne službe. Leta 1539 je v Angliji vzpostavljena tako imenovana Visoka komisija, ki se je na začetku ukvarjala s pregledom vseh sumljivih oseb v Londonu in med drugim tudi cenzuro pisem. V istem času, leta 1539, je v Benetkah Kolegij trojice s pomočjo vohunov sledil dejavnostim ne samo državljanov temveč tudi uslužbencev izvršnih organov Republike.

V 17. stoletju, v času absolutističnih monarhij, se razvije državni aparat, v katerem so organizirani posebni organi za varnostno dejavnost. V tem smislu je francoski kralj Louis XIV. marca 1667 v Parizu oblikoval tajno policijo za boj proti svojim političnim nasprotnikom. V Franciji se je proces končnega konstituiranja posebne službe končal leta 1795, ko so bili izdani predpisi, ki so določali, da je policija odgovorna za notranjo varnost države. V toku 19. stoletja so se vzporedno s politično policijo, ki je bila usmerjena v delovanje proti notranjim političnim nasprotnikom, razvile prve formacije protiobveščevalne dejavnosti. V tem trendu nastane v Avstriji leta 1850 Oddelek za evidenco, ki leta 1870 prevzame tudi protiobveščevalne naloge. V Rusiji se je leta 1866 oblikoval »Oddelek za zaščito državne varnosti in razvoja« Ohrana, ki je poleg vloge politične policije opravljala tudi protiobveščevalno dejavnost.

V času ameriške državljanske vojne med leti 1861 in 1865 je bila ustanovljen »Secret service« z namenom, da se zaščiti glavne politične figure v državi. V Londonu je leta 1886 formiran »Scotland Yard« za boj proti tujim obveščevalnim službam. V Franciji je bila kot protiobveščevalna služba ustanovljena Direkcija za nadzor teritorija (DTS).

Značilno za nastajanje teh organizacij je, da so najprej delovale z majhnim številom ljudi v prestolnicah, pozneje so ustanovile svoje organe v drugih večjih mestih. Na koncu teh procesov so imele izpostave po vsej državi, odvisno od administrativne ureditve.

Na začetku 20. stoletja se v vseh razvitih državah formirajo posebne organizacije za protiobveščevalno dejavnost in ustanove za boj proti notranjim političnim sovražnikom. Varnostna dejavnost se je razdelila na dve smeri; ena se je angažirala za boj proti tujim obveščevalnim službam – protiobveščevalna služba, druga za boj proti notranjim političnim nasprotnikom – politična policija. Na slednjo lahko gledamo kot na današnjo policijo ali službe za ustavno zaščito ipd.

Protiobveščevalna dejavnost je bila koncentrirana v sestavu vojaške organizacije države, saj so bile v tistih časih cilji tujih obveščevalnih služb predvsem vojske in njihove zmogljivosti. Ker se predmet obveščevalne dejavnosti razširil na celoten spekter države, se je tudi protiobveščevalna dejavnost temu primerno razširila in prilagodila. Razvoj je šel tudi v smeri oblikovanja vojaške protiobveščevalne službe in protiobveščevalne službe za zaščito celotne države (Đorđević 1980: 100–102).

4. 3. 2 Opredelitev protiobveščevalne službe

Po mnenju večine avtorjev sodi protiobveščevalna služba pod obveščevalno-varnostne službe. Stopar opiše obveščevalno-varnostne službe kot:

> *»službe, urade ali agencije, ki se ukvarjajo z zbiranjem, vrednotenjem, obdelavo in posredovanjem za državo pomembnih podatkov, pri čemer uporabljajo specifične metode in sredstva dela. Vse tovrstne službe namreč zbirajo podatke in informacije, pri čemer uporabljajo širok spekter metod in sredstev dela. To pomeni, da izvajajo obveščevalno dejavnost, hkrati pa tudi varnostno dejavnost znotraj službe, v državi ali za potrebe države v tujini« (Stopar 2002: 1).*

Na podlagi te definicije deli Stopar obveščevalno varnostne službe na obveščevalne in varnostne, pri čemer obveščevalne službe zbirajo, vrednotijo, obdelujejo in posredujejo zbrane podatke o tujini s ciljem zagotavljanja zunanje varnosti države in njenih interesov (Stopar 2002: 1). Varnostne službe pa so po mnenju Stoparja:

> *»za razliko od obveščevalnih pristojne za izvajanje aktivnosti s področja varovanja ustavne ureditve, boja proti tujim obveščevalno varnostnim službam, preprečevanja aktivnosti ekstremnih in terorističnih organizacij, ilegalne trgovine z orožjem, radioaktivnimi snovmi, jedrsko tehnologijo, drogami, belim blagom, begunske problematike in drugih področij interesa, ki lahko vplivajo na zagotavljanje notranje varnosti države in njenih interesov. Varnostne službe so tako pristojne za preprečevanje, preiskovanje in odpravljanje določenih oblik ogrožanja države in njenih interesov« (Stopar 2002: 1).*

Ožja pojma kot pojem varnostna služba sta protiobveščevalna služba[6], ki je ozko specializirana za boj proti delovanju tujih obveščevalno varnostnih služb, in služba za varstvo ustavne ureditve, ki je pristojna za preprečevanje aktivnosti ekstremnih in

[6] Protiobveščevalne službe se delijo na civilne in obrambne, pri čemer so obrambne protiobveščevalne službe pristojne le za izvajanje aktivnosti znotraj obrambno vojaškega sistema.

terorističnih organizacij, ilegalne trgovine z orožjem, radioaktivnimi snovmi, jedrsko tehnologijo, drogami, belim blagom, begunsko problematiko in drugih področjih interesa.

Poleg protiobveščevalnih služb in služb za varstvo ustavne ureditve šteje Stopar v skupino varnostnih služb tudi policijske enote in posebne organizacijske enote tožilcev, sodišč in drugih ustanov, ki so namenjene izvajanju preventivnih ukrepov in pregona domnevnih storilcev kaznivih dejanj, pri čemer lahko, za razliko od večine drugih obveščevalno varnostnih služb, uporabljajo policijska pooblastila (Stopar 2002: 1–2). Po drugi strani meni Šaponja, da je protiobveščevalna služba lahko del služb za ustavno ureditev države. Slednjo definira kot obveščevalno-varnostno službo, ki:

> *»lahko izvaja protiobveščevalno in varnostno zvrst obveščevalne dejavnosti. Glavna funkcija je boj proti podtalnim in tajnim oblikam ogrožanja ustavne ureditve, boj proti terorizmu, posebnim oblikam organiziranega kriminala ipd. Uslužbenci teh služb imajo pogosto tudi preiskovalna pooblastila. Po svoji naravi so to represivne službe. Delujejo lahko le v domovini in morajo tesno sodelovati z drugimi službami, zlasti obveščevalnimi« (Šaponja 1999: 58).*

Nadalje opiše protiobveščevalno službo kot tisto službo, ki:

> *»izvaja protiobveščevalno zvrst obveščevalne dejavnosti. Osnovna funkcija je preprečevanje in odkrivanje vsakovrstnega delovanja tujih obveščevalnih služb v državi (obveščevalna služba to izvaja v tujini). Protiobveščevalne službe so organizirane kot samostojne, lahko pa tudi kot del služb za varstvo ustavne ureditve. Štejemo jih med obveščevalnovarnostne službe. Lahko imajo preiskovalna pooblastila, podobna varnostnim službam, če tako določa notranji pravni red« (Šaponja 1999: 58).*

Šaponja meni, da je najprimernejša delitev služb, delitev na obveščevalne in obveščevalno-varnostne službe. Protiobveščevalna služba se po mnenju Šaponje tako nahaja med obveščevalno-varnostnimi službami, skupaj s Službami za varstvo ustavne ureditev in posebnih enot policije, tožilstev itd. (Šaponja 1999: 26–27). Đorđević splošno opiše protiobveščevalno službo kot:

> *»specializirano organizacijo gibanja ali države, ki odkriva in onemogoča delovanje obveščevalnih služb nasprotnika ali sovražnika, organizira in dela na zaščiti tajnih podatkov o strukturi gibanja ali države, dezinformiranju sovražnika ter deluje kot del varnostnega sistema države ali gibanja« (Đorđević 1989: 201).*

Spodaj podani tabeli prikazujeta dva pogleda umestitve protiobveščevalne službe:

Tabela 4. 3. 2. 1: delitev služb po Stoparju

Obveščevalno varnostne službe				
Obveščevalne službe	**Varnostne službe**			
	Protiobveščevalna služba	*Služba za varstvo ustavne ureditve*	*Policijske enote*	*Posebne organizacijske enote tožilcev*

Vir: Stopar (2002)

Tabela 2.: delitev služb glede na zvrst po Šaponji

Obveščevalna dejavnost	
Obveščevalno varnostne službe	**Obveščevalne službe**
Službe za varstvo ustavne ureditve	*Obveščevalne službe na civilnem področju*
Protiobveščevalne službe	*Obveščevalne službe na vojaškem in obrambnem področju*
Posebne notranjeorganizacijske enote policije, državnih tožilstev itd.	

Vir: Šaponja (1999: 27)

Iz povedanega lahko sklepam, da obstajata dva pogleda na umestitev protiobveščevalnih služb. Po mnenju Stoparja delimo obveščevalno-varnostne službe na obveščevalne in varnostne, kjer protiobveščevalna služba spada med slednje. Po

drugi strani, meni Šaponja, da spada protiobveščevalna služba samo pod obveščevalno-varnostne službe, ker pri svojem delu prav tako uporablja obveščevalno dejavnost in opravlja varnostno funkcijo.

4. 3. 3 Delitev protiobveščevalne službe

Đorđević (Đorđević 1985: 105–107) ugotavlja, da je v procesu razvoja protiobveščevalna služba zgradila organizacijo in metode dela glede na razvoj družbe in potrebe učinkovitejšega zoperstavljanja dejavnostim nasprotnih obveščevalnih služb in razdelitev funkcij in dela v državni organizaciji. V procesu so nastajali različni vidiki protiobveščevalne dejavnosti, ki so pozneje prerasli v posebne službe ali pa postali segmenti dejavnosti obveščevalnih služb. Raziskovanje posameznih delov protiobveščevalnih služb ima teoretične in praktične razloge. Teoretični razlogi so v tem, da se razloži vsebina dela vsake od njih, poišče razlike v področjih dela in najde organizacijske rešitve glede na preteklost in sedanjost. Takšne analize omogočajo praktična znanja o možnem delovanju in usmeritvah protiobveščevalne dejavnosti. Glede na te cilje se protiobveščevalne službe delijo na ofenzivne, defenzivne, resorne in teritorialne[7].

Ofenzivna protiobveščevalna služba se osredotoča na odkrivanje delovanja obveščevalnih služb nasprotnikov na njegovem teritoriju. Glavna značilnost ofenzivne protiobveščevalne službe je ta, da svoje metode dela in sredstva uporablja na teritoriju nasprotnikove države, s čimer ogroža njegovo suverenost. Cilji ofenzivnega delovanja so v odkrivanju metode in sredstva nasprotnikove obveščevalne službe z prodiranjem v njeno centralo ali centre, v strukture, iz katerih se organizira in vodi ofenzivna obveščevalna dejavnost. Ti cilji se uresničujejo na takšen način, da se odkrije ali postavi agenta v strukture nasprotnikove obveščevalne ali protiobveščevalne službe. Preko takšnih virov odkritij se pride do najbolj pomembnih podatkov. Drugi vidik delovanja ofenzivne protiobveščevalne službe je, da zbira in analizira podatke o lastnem izvoru podatkov, ki se nahajajo v strukturah sovražnika.

[7] Možne so tudi še druge delitve. Delitev protiobveščevalne službe na vojno in civilno, kjer je kriterij objekt zaščite. Možna je tudi delitev služb na operativne in neoperativne protiobveščevalne službe. Operativna služba raziskuje nasprotno službo in uporablja represivna sredstva. Neoperativna služba samo zbira podatke, izvršitev določenih ukrepov izvajajo drugi organi (policija, sodstvo …)

Cilj tega delovanja je, da se pravočasno odkrijejo nameni sovražnika, ki naj bi odkril in uničil naše izvore podatkov v njegovih strukturah. V zgodovini protiobveščevalna služba ni nikjer obstajala kot posebna organizacija. Bila je le del aktivnosti, vgrajena, ali kot sektor dela varnostne službe oz. tudi kot del ofenzivne obveščevalne službe.

Defenzivna protiobveščevalna služba uporablja svoje metode, sredstva in delo na teritoriju lastne države v boju proti nasprotniku ali sovražni obveščevalni službi. »Defenzivnost« službe se kaže le v delovanju na svojem ozemlju oziroma znotraj mej lastne teritorialne suverenosti. Vendar je zaradi učinkovitosti dela del njene aktivnosti usmerjen ofenzivno, predvsem glede na usmerjenost in nastop. Zgodovina razvoja protiobveščevalne službe kaže na to, da se je sprva gledalo nanjo kot »dejavnost vodilnih struktur« družbe ali države, pozneje pa se oblikuje v posebno organizacijo ali sektor delovanja varnostne službe. Kot posebna organizacija obstaja tam, kjer deluje kot zaščita pristojnih organov, kot so vojaška protiobveščevalna služba, služba na zunanjem ministrstvu.

Resorna protiobveščevalna služba deluje na zaščiti določenega resorja ali njegovih delov. To so organi, ki spadajo v varnostno najbolj občutljive segmente državne strukture. Cilj protiobveščevalne službe je, da onemogoči infiltracijo nasprotnikove agenture v te organe in ščiti tajne informacije o njih. S svojimi sredstvi in metodam ščiti prostore organa in osebja, ki je tam zaposleno.

Teritorialna protiobveščevalna služba s svojimi metodami, sredstvi in protiobveščevalnim delovanjem ščiti teritorij določene države. Poleg zaščite prostora s svojimi silami pokriva tudi druge državne strukture, razen tistih, ki imajo lastne protiobveščevalne ali varnostne službe. Zaradi učinkovitega delovanja je pomembno, da je teritorialna protiobveščevalna služba prisotna na vseh delih državnega teritorija. Služba tako gradi svojo organizacijsko shemo, ki je odvisna od administrativno teritorialne delitve države, da je lahko preko svojih organizacijskih enot prisotna na celotnem prostoru. V večini varnostnih sistemov se teritorialna protiobveščevalna služba kaže kot sektor, ki spada pod varnostno službo. Organizacijska shema se od vrha piramide širi: od oblasti do okrožij, območij.

5. PROTIOBVEŠČEVALNE FUNKCIJE

Đorđević našteje štiri najpomembnejše protiobveščevalne funkcije:

(1) Odkriva in onemogoča delovanje obveščevalnih služb nasprotnika, tako da s svojim delom, sredstvi in metodami identificira agente nasprotnikove obveščevalne službe in njihovo delovanje.

(2) Identificira obveščevalce nasprotnikove obveščevalne službe, določi njihove osebne značilnosti, kvalitete in druge podrobnosti.

(3) Določa strukture, objekte in prostore, ki so tarča nasprotnikove obveščevalne dejavnosti. S tem odkriva namere in metode dela nasprotnika itd. S pridobljenim znanjem o delovanju nasprotnika protiobveščevalna služba dograjuje in korigira lastno dejavnost, s svojim delom pomaga pooblaščenim političnim organom, da sprejmejo ustrezne ukrepe, s katerimi se vzpostavi učinkovitejši celotni varnostni sistem države ali gibanja.

(4) Organizira, načrtuje in deluje na zaščiti lastne tajnosti in političnih struktur. Ščiti določena delovna mesta, ki se nahajajo v strukturah države ali gibanja in ki so varnostno občutljiva, ker imajo dostop do tajnih informacij (kabinet voditeljev, štabi in poveljstva oboroženih sil, projektne pisarne in centri za obdelavo podatkov itd.). Takšna delovna mesta je moč ščititi na štiri načine: osebno, z zaščitnim režimom, s tehničnimi in fizičnimi sredstvi. Objekti pod protiobveščevalno zaščito so varnostno občutljiv del struktur gibanja ali države. Ti objekti so varnostno občutljivi, ker znotraj njihovih struktur krožijo tajni podatki, ki so posebnega interesa za državo ali gibanja. Zaščitnim ukrepom so v takšnih ustanovah in organizacijah podrejeni tisti njihovi deli, od katerih je odvisno delovanje celotne organizacije. To so lahko določena delovna mesta, proizvodni stroji, viri energije itd. Poleg zaščite določenih delovnih mest, notranji sistem protiobveščevalne službe sestavlja tudi režim gibanja oseb, ki niso zaposlene na objektu, režim proti tujcem, protidiverzantsko zaščito, fizično varovanje in zaščito tajnega izvora podatkov.

(5) Dezinformira nasprotnika ali sovražnika. To delo protiobveščevalna služba opravlja s svojimi sredstvi in metodami. Dezinformiranje se realizira z dajanjem nasprotniku ali sovražniku lažnih obvestil na najbolj ugoden način s ciljem, da se ga zavede in tako pride do napačnih zaključkov in akcij. Poleg protiobveščevalne službe, ki načrtuje in organizira dezinformiranje nasprotnika, se lahko tem

dejavnostim pridružijo tudi druge strukture družbe. V tem smislu se lahko uporabijo množični mediji ali posamezni državljan. V vojni lahko to aktivnost izvaja vsak posamezen vojak (Đorđević 1980: 103–105).

V skladu z ameriškim vojaškim protiobveščevalnim priročnikom FM 34-60 in Marine Corps MCWP 2-14 obstajajo štiri pomembne protiobveščevalne funkcije: (1) operacije, (2) preiskave, (3) zbiranje podatkov in poročanje, ter (4) analiza, izdelava in predaja informacij. Ofenzivne protiobveščevalne operacije so usmerjene proti vohunjenju, sabotažam, podtalnim delovanjem ter terorističnim grožnjam. Te aktivnosti se tako delijo na protivohunske, protisubverzijske, protisabotažne, protiteroristične operacije ter operacije eksploatacij (izkoriščanj) in nevtralizacije. Protiobveščevalne preiskave se nanašajo na osebje, varnostne zadeve, vohunjenje, sabotaže, terorizem, podtalno delovanje ter prebežnike. Zbiranje podatkov in poročanje obsega tudi sodelovanje z sorodnimi službami. Analiza in izdelava služita kot podpora operacijam in preiskavam (FM 34-60, Department of the Navy, MCWP 2000: 2–14).

Richelson prav tako opredeli štiri glavne protiobveščevalne funkcije: (1) zbiranje informacij o tujih obveščevalnih in varnostnih službah in njihovih aktivnostih z javnim in tajnim zbiranjem podatkov, (2) evalvacija prebežnikov, (3) raziskave in analize, ki se nanašajo na strukture, osebje in operacije tujih obveščevalnih in varnostnih služb, ter (4) operacije, ki so namenjene za motenje in nevtralizacijo sovražnih služb (Richelson 1999: 333).

Godson, ki govori o učinkoviti protiobveščevalni kot ofenzivno defenzivni, opiše glavne funkcije oziroma načela protiobveščevalne dejavnosti kot naslednja: (1) centralna koordinacija in strategija, (2) protiobveščevalna analiza, (3) protiobveščevalno zbiranje podatkov ter (4) eksploatacija (izkoriščanje). Pri centralni koordinaciji poudari pomen koordiniranih in dobro vodenih programov zbiranja podatkov, eksploatacij in analitičnih načrtov. Strategija naj bi potrebovala »en um«, ki je lahko individualen ali skupinski. Protiobveščevalna analiza služi za določitev varnostne ranljivosti države, identifikacijo nasprotnikov, njihovih zmogljivosti in interesov. Prav tako se analiza uporablja za razpoznavanje tajnih metod, ki jih uporablja tuja vlada za manipulacijo in akcije in v podporo protiobveščevalnim

operacijam. Protiobveščevalno zbiranje podatkov zajema integracijo več obveščevalnih virov, tako javnih kot tajnih. Tajno zbiranje podatkov preko človeških virov s pomočjo prebežnikov, fizičnega nadzora, dostopnih agentov (access agent), dvojnih agentov, prijateljskih služb in nelegalnih agentov. Novejša[8] kategorija zbiranja podatkov je tehnična protiobveščevalna dejavnost. Eksploatacija[9] pomeni izrabo protiobveščevalnih podatkov za uvajanje varnostnih ukrepov in ukrepov za manipulacijo ter izkoriščanje in delovanje tujih obveščevalnih služb v svoj prid, tako imenovane protiukrepe (Godson 1995: 184–237).

Delitev protiobveščevalne dejavnosti na dva enakovredna dela ni tuja tudi drugim avtorjem. Tako najdemo delitev protiobveščevalne na varnostni del in protivohunstvo. Varnostni del je bolj pasivne in obrambne narave, medtem ko je protivohunstvo ofenzivna, agresivna stran protiobveščevalne dejavnosti. Protivohunstvo sestavljajo identifikacija določenega nasprotnika in vedenje o določeni operaciji, ki jo izvaja. Osebje se mora nato zoperstaviti tem operacijam z infiltracijo v sovražne obveščevalne službe (imenovano prodor) in z različnimi oblikami manipulacije. Varnostni del protiobveščevalne vključuje zasliševanje in preverjanje osebja ter izdelava programov varovanja obveščevalno občutljivih informacij (Assassination Archives and Research Center: *IX. CIA COUNTERINTELLIGENCE: A Counterintelligence: An Introduction*. Dostopno na http://www.aarclibrary.org/publib/church/reports/book1/pdf/ChurchB1_9_Counterintel.pdf (1. julij 2006)).

Drugi menijo, da protiobveščevalno dejavnost sestavljajo **aktivni** in **pasivni** ukrepi. Cilj slednjih je preprečiti dostop nasprotnikov do občutljivih podatkov in informacij. Te imenujemo *varnostni ukrepi*. Varnostni ukrepi vsebujejo pet tipov varovanja: *osebna, fizična, komunikacijska, računalniška in tehnična varnost*. Vsi ti tipi varovanja so namenjeni preprečevanju dostopa ali izrabe osebja, dokumentov, komunikacij ali operacij. Varnostne ukrepe sestavljajo: sistem klasifikacije informacij, procesov ali območij; raziskave in preverjanje civilnih uslužbencev, zaposlenih in vojaškega

[8] Glavni igralci dvajsetega stoletja v zbiranju podatkov preko človeških virov so postali profesionalni uradniki, ki uživajo diplomatsko imuniteto ter vodijo agente, ki te imunitete nimajo. Te agente tuje obveščevalne službe težje prepoznajo in so znani kot nelegalni agentje (Godson, 1995: 221-222).
[9] Bistvo tehnične protiobveščevalne dejavnosti je poizvedovanje o prioritetah in kapacitetah tehničnih sistemov obveščanja tujih obveščevalnih služb.

osebja; preiskave; pregledovanje sumljivih agentov, nadzor dejavnosti in nevtralizacija prisotnosti tujih obveščevalnih služb.

Aktivni ukrepi so namenjeni razumevanju sovražnih služb in njihove »modus operandi« s ciljem motenja in uporabe njihove dejavnosti v svoj prid. Najpogosteje se omenja protivohunstvo, vendar aktivne ukrepe sestavljajo še nadzor in obveščevalne operacije. Z nadzorom se želi ugotoviti, kam tuji agenti zahajajo, s kom se dobivajo in kaj počnejo. Nadzor mora biti prikrit, kar je sicer težko in drago, ker zahteva večjo skupino ljudi. Cilj obveščevalnih operacij je zbiranje podatkov neposredno od sovražnika s pomočjo tehničnih in človeških sredstev. Zbiranje podatkov se izvaja z izpraševanjem prebežnikov, rekrutiranjem agentov, uporabo dvojnih agentov, penetracija v tuje službe s ciljem motenja, dezinformiranja in manipuliranja teh služb v lastno korist (DCAF 2004).

Nekateri se ne strinjajo s tem, da spadajo varnostni ukrepi pod okrilje protiobveščevalne dejavnosti. Protiobveščevalna dejavnost naj bi bila produkcija znanja in ni namenjena samo protiobveščevalni (razen znanja, ki je potrebno za boljše delovanje same protiobveščevalne), temveč predvsem tožilcem, zakonodajalcem, poveljnikom, v glavnem tistim organom, ki so odgovorni za vzpostavljanje varnostnih ukrepov. Zaradi tega naj bi protiobveščevalno dejavnost in varnostne ukrepe jasno ločevali. Varnostni mehanizmi so namreč obrambni ukrepi, postavljeni s strani izvršne oblasti za zaščito pred tistimi, od katerih protiobveščevalna išče informacije (CIA.gov: *Counterintelligence for National Security.* Dostopno na https://www.cia.gov/csi/kent_csi/docs/v02i4a10p_0001.htm (11. november 2006)).

Gleghorn ugotavlja, da kljub očitnim razlikam v opredelitvi funkcij protiobveščevalne dejavnosti s strani različnih virov, protiobveščevalno dejavnost lahko razdeli na dve temeljni funkciji: (1) Identifikacija in zoperstavljanje grožnjam, ki jih povzročajo tuje obveščevalne službe[10] in (2) izraba nasprotnikovih obveščevalnih služb v lastno

[10] Gleghorn poleg obveščevalnih služb omeni še teroristične organizacije, ki pa sem jo v tem odstavku opustil zaradi prejšnjih ugotovitev, da teroristične organizacije niso predmet protiobveščevalne dejavnosti, razen če same opravljajo obveščevalno dejavnost.

korist. Gleghorn poskuša sestaviti sintezo vseh definicij funkcij protiobveščevalne dejavnosti.

Prva funkcija naj bi tako zahtevala primerno zbiranje podatkov in preiskavo, ki bi zaznala in identificirala potencialno obveščevalno grožnjo. Vsebovala naj bi tudi natančno in jasno analizo primernih obveščevalnih podatkov. Druga funkcija vsebuje vsakršne ukrepe, ki so potrebni za operacije »nevtralizacije« ali »izrabe« (eksploatacije) nasprotnika v lastno korist. Operacije nevtralizacije sestavljata dve glavni kategoriji: (1) varnostni programi in (2) protiukrepi. Medtem ko bolj pasivni varnostni programi preprečujejo dostop obveščevalnih služb do občutljivih informacij od znotraj, so protiukrepi namenjeni preprečevanju dostopa do informacij od zunaj. Primeri protiukrepov so prikrivanje, skrivanje in prevara. Operacije izrabe so bolj prikrite in tajne narave ter pomenijo uporabo človeških in tehničnih virov. Najpomembnejši metodi pri operacijah izrabe sta »krt« in »dvojni agent«. Pri prvemu gre za prodor v tujo obveščevalno službo, drugi ponavadi pomeni odkritje tujega agenta v lastnih vrstah, ki se ga prepriča, da deluje za nas. Pri obeh metodah se službe poslužujejo metod manipulacij in prevar tujih obveščevalnih služb v lasten prid (Gleghorn 2003: 19–26).

5. 1 Identifikacija in ocena groženj

Prva dva bistvena elementa delovanja protiobveščevalnih služb sta *identifikacija sovražne službe* in *ocena groženj.* Ta dva elementa pokrivata številne protiobveščevalne aktivnosti, predvsem protiobveščevalne preiskave in operacije zbiranja podatkov. Slednja je pomembna predvsem zato, da se lahko učinkovito določi lokacija sovražne dejavnosti nasprotnikovih služb, pri tem pa je pomembno, da se integrirano uporabi sredstva, kot so tehnično zbiranje podatkov, javno in prikrito zbiranje podatkov preko človeških virov. Druga sestavina, ocena grožnje, je pomembna naloga, ki pomeni analizo grožnje in lastne ranljivosti pred sovražnimi službami. Z analizo se lahko oceni in poda predloge za izboljšanje varnosti in izvajanje protiukrepov, s katerimi se grožnja lahko zmanjša. Takšno delovanje potrebuje raznovrstno in razumljivo podatkovno bazo, ki vsebuje tako informacije o operacijah »prijateljskih » in sovražnih služb ter usposobljene analitike.

Protiobveščevalna analiza omogoča podlago za izvajanje operacij proti nasprotniku. Specifične analize, ki govorijo o nasprotnikovih zmožnostih, namenih in dejanskih operacijah se uporabljajo za oceno ranljivosti nasprotnika in podajo smernice, ki služijo protiobveščevalni. Kjer je možna kombinacija več operacij usmerjenih v eno tarčo, mora analitik upoštevati sodelovanje s »sestrsko službo[11]«, da se prepreči površno sodelovanje podvajanja nalog. Informacije o delovanju, zmožnostih, namenih in *modus operandi* tujih obveščevalnih služb morajo biti vedno pripravljene za operativno delovanje. Enako velja za ugotovitve o ranljivosti lastne infrastrukture ali osebja, da se lahko hitreje sprejmejo protiukrepi (Gleghorn 2003: 21–22).

5. 2 Nevtralizacija in izkoriščanje nasprotnikove aktivnosti

Naslednji dve bistveni nalogi sta *operacija nevtralizacije in operacija izkoriščanja*. Godson opiše učinkovito protiobveščevalno dejavnost kot »ofenzivno – defenzivno«, kar pomeni razdelitev teh dveh nalog glede na ofenzivno in defenzivno naravo. Operacije nevtralizacije zato definiramo kot obrambne ukrepe, s katerimi se prepreči ali ovira dostop do občutljivih informacij. Operacije za izkoriščanje so po drugi strani definirane kot ofenzivne, njihov cilj pa je obrniti nasprotnikove operacije sebi v prid. Kljub razmejitvi teh dveh operacij pa ostajata nevtralizacija in izkoriščanje dve strani istega kovanca, ki služita za oviranje delovanja nasprotnika tako z ofenzivnimi in defenzivnimi ukrepi, podprtimi z obveščevalnim zbiranjem podatkov in analizo (Gleghorn 2003: 23).

5. 2. 1 OPERACIJE ZA NEVTRALIZACIJO OBVEŠČEVALNE AKTIVNOSTI

Operacije za nevtralizacijo lahko razdelimo na dve kategoriji: (1) varnostni programi, s katerimi se omejuje dostop do občutljivih programov na določenem področju, in (2) protiukrepi, s katerimi se prepreči dejavnosti nasprotne obveščevalne službe že z distance (Godson 1995: 230).

[11] To so agencije v službi iste države.

Varnostni programi kot funkcija nevtralizacije ovirajo dostop »insajderjem«, npr. zaposlenim, ki imajo dostop do občutljivih informacij (Gleghorn 2003:23). Eni od takšnih načinov pasivnih varnostnih programov so tečaji in usposabljanja uslužbencev za prepoznavanje vohunstva ipd. V ZDA uslužbenci dobijo navodila, kako lahko prepoznajo sovražno obveščevalno dejavnost, kakšni so indikatorji in kako naj ukrepajo. Vse to je del celotnega pristopa k protiobveščevalni dejavnosti v državi.

Na spletni strani Urada za varovanje tajnih podatkov Republike Slovenije (Urad za varovanje tajnih podatkov RS, Delovna področja. Dostopno na http://www.uvtp.gov.si/index.php?id=374, (2. junij 2006)) najdemo naslednja področja varovanja zaupnih podatkov: (1) osebno varovanje, ki pomeni varnostno preverjanja oseb, ugotavlja se lojalnost, zanesljivost oseb ter okoliščine, zaradi katerih bi oseba lahko bila podvržena izsiljevanju; (2) fizična varnost, katerega cilj je preprečiti fizičen dostop do podatkov in se deli na organizacijske, varnostno-tehnične ukrepe (protivlomna zaščita, mehanska zaščita, sistem video nadzora) ter ukrepe fizičnega varovanja, kjer varnostniki opravljajo neposredno kontrolo oseb, vozil itd.; (3) dokumentacijska varnost zajema tako primerno označitev, sledenje tajnemu podatku skozi življenjski ciklus uporabe kot tudi primerno hranjenje in ne nazadnje evidentirano uničenje; (4) informacijska varnost INFOSEC vsebuje tako ukrepe varovanja tajnosti v računalniških sistemih oziroma računalniško varnost – COMPUSEC (varnost strojne opreme, varnost programske opreme in varnost programsko-strojne opreme) kot ukrepe varovanja tajnosti v komunikacijskih sistemih oziroma komunikacijsko varnost – COMSEC (varnost prenosnih sistemov – TRANSEC, varnost kriptografskih metod in naprav – CRYPTOSEC, varnost pri elektromagnetnem sevanju elektronskih naprav – EMSEC). Med omenjene ukrepe sodi tudi odkrivanje, dokumentiranje in zoperstavljanje vsem oblikam groženj, usmerjenim tako proti tajnim podatkom kot proti sistemom, ki tajne podatke obravnavajo. Poleg teh področij varovanja sta tu omenjena še (6) industrijska varnost ter (7) usposabljanje.

Medtem ko pasivni varnostni programi preprečujejo sovražni obveščevalni službi fizičen in osebni dostop do občutljivih informacij od znotraj, protiukrepi na drugi strani onemogočajo dostop sovražnika do potencialnih informacij od zunaj. Operativni

primer tega delovanja sta prikrivanje in prevara, ki ju uporabljajo za zmožnosti delovanja nasprotnikovega IMINT sistema**.** Drug način je poročanje o kontaktih s tujci. Odreditev, da morajo vsi uslužbenci, ki imajo stik z občutljivimi informacijami, poročati o svojih stikih s tujci. S tem se lahko prepreči rekrutacija agentov s strani tujih služb.

Proti tehničnim zbiranjem podatkov, elektronskim prisluškovanjem in nadzorovanjem, se zagotovi varnost s posebno poddisciplino, znano kot tehnični protiukrepi (technical surveillance countermeasures)[12] (Gleghorn 1995: 25). Srbi naj bi na primer prisluškovali dejavnostim NATA v Bosni in Hercegovini ter tako sledili njihovim aktivnostim glede lova na haškega obtoženca Radovana Karađića. To lahko razloži zakaj ga S-forju še do danes ni uspelo najti (Kroeger 2002).

Učinkoviti protiukrepi morajo biti celostni pri nevtralizaciji nasprotnikove aktivnosti, kar pomeni, da morajo delovati na več frontah in usklajeno. Operacije nevtralizacije nasprotnikove aktivnosti so lahko uspešne le z učinkovitim kombiniranjem varnostnih programov in protiukrepov.

Čeprav so operacije za nevtralizacijo bolj obrambne in pasivne narave, lahko kljub temu uporablja aktivne ukrepe, kot so obrambne operacije zbiranja podatkov. Obrambne operacije zbiranja podatkov so protiobveščevalna zbiranja podatkov s pomočjo človeških virov in so aktivno vpletene v zmanjšanje učinkovitosti delovanja vohunjenja nasprotnika. Drugi primeri protiobveščevalnega zbiranja, ki bi lahko podirale operacije za nevtralizacijo, so zasliševanje in poročanje s strani nenamenskih (non-tasked) človeških virov, imenovanih tudi naključni viri, kot so: posamezniki, ki prostovoljno predajo informacije; nenamerni viri (vsak posameznik, ki priskrbi informacije protiobveščevalni službi in se tega ne zaveda); prebežniki, vojni ujetniki; begunci in emigranti; intervjuvanci (posamezniki, ki so bili v stiku s preiskavo) prijateljskih, sestrskih služb. Vsi ti našteti primeri pripomorejo protiobveščevalni uporabi *operacij za nevtralizacijo*, čeprav so nekateri viri uporabni za bolj agresivne *operacije za izkoriščanje* (Gleghorn 2003: 25–26). Modernejši primer uporabe prebežnikov iz nasprotnih organizacij je prebeg nekdanjega tesnega sodelavca

[12] S to poddisciplino se sistemtično opravlja fizične in elektronske preglede določenih območij s posebno opremo za ugotavljanje prisluškovalnih naprav.

voditelja Talibanov v Afganistanu Mohammada Omarja, Mohammada Khakhsarja. Najprej je deloval kot vrhovni obveščevalni oficir gibanja, nato pa kot namestnik notranjega ministra in bil pristojen za varnost. Zaradi nestrinjanja z potezami talibanske vlade je prestopil stran Severne Alianse. Bil je vir informacij za CIO glede delovanja talibanske organizacije in njenega sodelovanja z Osama Bin Ladnom (Khilafah.com 2001).

5. 2. 2 OPERACIJE ZA IZKORIŠČANJE OBVEŠČEVALNE AKTIVNOSTI

Operacije za izkoriščanje so bolj skrivnostni ukrepi protiobveščevalne dejavnosti. Te operacije uporabljajo v veliki meri enake vire informacij in se predvsem osredotočajo na izkoriščanje prikritih človeških in tehničnih virov, da bi s tem škodovale tuji obveščevalni službi.

Primarni cilj teh operacij je degradacija učinkovitosti nasprotnikove obveščevalne ali varnostne službe. Ta cilj se lahko doseže na dva načina: (1) manipulacija z nasprotnikom (njegovimi službami) ali (2) z motenjem nasprotnikovih normalnih operacij. Slednje pomeni motenje zmožnosti zbiranja podatkov in ga je tudi lažje doseči kot prvega, in sicer npr. z aretacijami vpletenih oseb ali z razkritjem njihovih akcij. Diplomate, ki so jih zasačili pri vohunjenju, se lahko izžene in se jih označi kot »personae non gratae«, se pravi za nezaželene osebe (Gleghorn 2003: 26–27).

20. januarja leta 2000 je poljski zunanji minister obvestil ruskega veleposlanika v Varšavi, da je bilo devet ruskih diplomatov označenih kot «personae non gratae«, ker so bili leta 1999 vpleteni v obveščevalne aktivnosti, ki so bile usmerjene v vitalne interese Republike Poljske. Takoj za tem je sledil še izgon devet poljskih diplomatov iz Moskve, ker naj bi opravljali dejavnosti, ki niso bile v skladu s statusom diplomata. Dejansko je šlo za dejanje maščevanja (Rohozinska 2000).

Veliko težja je manipulacija z nasprotnikom, predvsem skozi daljše obdobje. (Godson 2003: 223). Manipulacija vsebuje prevaro kot eno esencialnih tehnik pri delu. Da bi bilo možno nasprotnika, ki je v ves čas v alarmnem stanju, prevarati, je potrebno zelo

dobro poznavanje tako nasprotnika kot sebe. Še težje je to doseči, če se sovražnik zaveda, da je tarča protiobveščevalne službe.

Krti in dvojni agentje so najznačilnejša ofenzivna metoda dela operacij za izkoriščanje nasprotnika. Krt je v obveščevalnem žargonu oseba, ki jo je bilo uspelo prodreti v nasprotno organizacijo (obveščevalno, varnostno službo ali celo v vlado). Ponavadi je visok uslužbenec obveščevalne službe, ki predaja informacije nasprotni ali sovražni službi (Encyclopedia of Espionage, Intelligence, and Security 1991: 279). Obstaja več načinov rekrutacije »krta«. Eden težjih je poskus službe, da nastavi tuji službi svojega agenta kot vabo, se pravi, da jim ponuja določene informacije in ga ta nevede sprejme medse. Drug način je neposredna rekrutacija uslužbenca nasprotne službe, kjer ta še naprej opravlja svoje delo, zraven pa vohuni za službo, ki ga je rekrutirala.

Odkritje agenta sovražne službe v lastnih vrstah ponuja priložnost za uporabo te osebe kot dvojnega agenta. To je sicer zelo težko doseči, še težje pa vzdrževati. Nadzor nad agentom, ki je prestopil stran, je zelo kompleksna dejavnost in teži k zagotavljanju, da agent ohranja lojalnost službi, ki ga je odkrila. Odgovoriti je treba na vprašanja: ali je prestop resen, ali gre za vabo, kako zanesljiv je agent ipd.

Eden od vidikov zagotavljanja učinkovitosti agenta je ta, da se poskrbi za njegovo varnost, potrebuje zagotovilo, da ga matična služba ne odkrije. Drug vidik zagotavljanja učinkovitosti je preverjanje informacij, ki jih od takšnega agenta pridobivamo. Tako se najlažje ugotovi, če je kaj narobe, torej če je bil dvojni agent zasačen in je mogoče spet prestopil stran. Ta pojav imenujemo »trojni agent«, kjer lahko določena oseba večkrat prestopi stran.

Kljub zapletenosti in tveganju so lahko operacije dvojnih agentov sorazmerno varne pred odkritji, če so seveda premišljeno vodene. Eden od načinov zmanjšanja tveganja je, da se po odkritju agenta v lastnih vrstah, njega ne obvesti. Na ta način se lahko agenta, ki se ne zaveda, da je bil odkrit, vodi v smeri lastnih interesov tako, da se ga prikrajša za določene informacije, podaja se mu lažne podatke, pri tem pa je pomembno, da nič ne posumi. Tako se lahko doseže dobre rezultate, brez da bi formalno rekrutirali agenta v lastne vrste. Večji uspeh bi seveda bil, če se pripravi

agenta, da zamenja stran in vohuni za nas. Eden od vzrokov, zakaj bi bil prestop bolj učinkovit, je ta, da agent pozna svojo službo, pozna njene pomanjkljivosti in prednosti in jih tako lahko lažje izkorišča. Pri tem je potrebno upoštevati možnost, da se agent lahko spet obrne in zamenja stran, kar lahko povzroči še večjo škodo. Kljub temu ostaja metoda dvojnega agenta ena najpomembnejših metod operacij za izkoriščanja nasprotnika pri protiobveščevalni dejavnosti (Gleghorn 2003: 21–31).

V ZDA sta po koncu hladne vojne postala najbolj odmevna primera »krt« in hkrati dvojnega agent Hanssen Robert Philip in Ana Bellen Montes (Defence Security Service: *Espionage Cases 1975-2004*. Dostopno na: http://www.dss.mil/training/espionage/REC.pdf (3. junij 2006)).

5. 2. 2. 1 Hanssen, Robert Philip

Hanssen, Robert Philip, uslužbenec FBI več kot 27 let, je bil obtožen 20. februarja 2001 kaznivega dejanja vohunjenja za Rusijo, kar je domnevno počel več kot 15 let. Aretiran je bil v parku blizu svojega doma v Vienni v Virginiji v trenutku, ko je odložil torbo na skritem mestu. Torba je vsebovala sedem tajnih dokumentov. Večji del svoje kariere je Hanssen delal v protiobveščevalni in je tako lahko izrabil tam pridobljena znanja. Obtožen je bil kaznivega dejanja vohunjenja in zarote. Hanssen je predal, najprej Sovjetom in nato Rusom, več kot 6000 strani zaupnih dokumentov in identiteto treh ruskih agentov, ki so delali za ZDA. Dvema od teh so sodili v Rusiji in ju usmrtili. Po mnenju sodišča jim je uslužbenec FBI priskrbel več informacij o projektih ameriške obveščevalne skupnosti in podrobnosti o obrambnih jedrskih zmogljivostih ZDA. V zameno je v tem obdobju dobil s strani Rusov 1,4 milijona dolarjev z vključno preko 600.000 dolarjev gotovine in diamantov v vrednosti 800.000 dolarjev, shranjenih na ruskem bančnem računu. Hanssena so odkrili šele, ko so zanj izvedeli s strani vira iz ruske obveščevalne službe. Rusi niso nikoli vedeli za Hanssenovo pravo ime. Njegovo kodno ime je bilo »Ramon« ali »Garcia«. Hanssen naj bi se povezal z Rusi na začetku leta 1979, prekinil stike 1980, vendar obnovil sodelovanje leta 1985, ko je poslal nepodpisano pismo KGB oficirju na sovjetski ambasadi v Washingtonu. Pismo je vsebovalo imena treh sovjetskih dvojnih agentov, ki so delovali v ZDA. Čeprav so motivi Hanssena nejasni, se zdi, da so vsebovali

samopotrditev, nezadovoljstvo z delom pri FBI in potrebo po denarju. Z ženo sta preživljala številno družino z njegovo plačo in do 1992 je bil zadolžen že za 275.000 dolarjev. Hanssen je izkoriščal računalniški sistem FBI za prodajanje zaupnih informacij. Prijatelji in sodelavci niso znali razložiti, kako je domnevno globoko veren oče šestih otrok in zaprisežen antikomunist lahko vodil dvojno življenje. Velik del njegovih nezakonitih prihodkov je šlo za lokalne striptizete. Julija 2001 je prišlo do sporazuma, kjer je Hanssen priznal vohunjenje in polno sodeloval z preiskovalci, da se je tako izognil smrtni kazni. 11. maja 2002 je bil obsojen na dosmrtno ječo.

5. 2. 2. 2 Montes, Ana Belen

Montes, Ana Belen, višja obveščevalna analitičarka v DIA (Defense Intelligence Agency) je Kubi izdajala občutljive, zaupne vojaške in obveščevalne informacije več kot 16 let, preden je bila aretirana 21. septembra 2001. Njena dejavnost se je končala zaradi povečanega nadzora, ki je bil posledica terorističnega napada 11. septembra 2001 in skrbi, da je Kuba posredovala informacije drugim narodom. Montesova je bila stara 44 let, neporočena in državljanka ZDA, po rodu iz Puerto Rica. Preden je začela delati za Kubanski direktorat za obveščanje, je bila zaposlena na Pravosodnem ministrstvu. Še danes se ne ve, ali je bila v sodelovanje prisiljena ali je delovala prostovoljno. Tam so jo spodbujali, naj si poišče službo, kjer bo imela več dostopa do zaupnih informacij. Tako je bila leta 1985 premeščena na delo v DIA. Pri svojem delu se je posvečala latinskim vojaškim obveščevalnim službam. Leta 1992 je postala DIA analitik za Kubo. Prestala je najmanj en poligrafski test, preden se je lotila vohunjenja. Montesova se je dobivala s Kubanci vsake tri ali štiri mesece v ZDA ali na Kubi, kjer so si izmenjali informacije in navodila. Kubanci so bili v stiku z njo tudi s šifriranimi visokimi frekvenčnimi radiji, ki jih je ona sprejemala z kratko valovnim radiem. V svoj prenosni računalnik je vtipkala kodo, ki jo je dobila preko valov, nato pa z dešifrirnim diskom prebrala sporočilo. Za pošiljanje dešifriranih številk na osebnem klicniku (pager) kubanskih uradnikov v Združenih narodih je uporabljala telefonske govorilnice v Washingtonu. Ker ni sledila njihovim strogim navodilom, kako izbrisati sledi sporočil na trdem disku računalnika, je pustila za sabo dokaze o svojih aktivnostih. V letih vohunjenja je Kubancem izdala imena štirih ameriških vojaških obveščevalcev (ki so za las ušli), podrobnosti o vsaj enem vstopnem programu,

obrambnih izdatkih za Kubo in slike zračnih nadzorov. Imela je dostop do Intelinka in informacij šestdesetih agencij in oddelkov zvezne vlade, ki so povezani v to omrežje. Montesova je sodelovala z različnimi obveščevalnimi službami, da so ji tako zmanjšali kazen. Njeni odvetniki so trdili, da je vohunila iz simpatije do Kube in da ni prejela drugega denarja kot povrnitev stroškov za letalske karte in nakup njenega prenosnega računalnika. 16. oktobra 2002 je bila obsojena na 25 let zapora in 5 let pogojne kazni.

6. PROTIOBVEŠČEVALNA DEJAVNOST V ZDA, RUSKI FEDERACIJI, VELIKI BRITANIJI, ZVEZNI REPUBLIKI NEMČIJI IN IZRAELU

6. 1 PROTIOBVEŠČEVALNA DEJAVNOST V ZDA

Nacionalna Protiobveščevalna Eksekutiva (National Counterintelligence Executive) (NCIX) vodi protiobveščevalno dejavnost za vlado Združenih držav Amerike in je neposredno podrejena Direktorju nacionalne obveščevalne skupnosti (Director of National Intelligence). NCIX omogoča protiobveščevalni skupnosti[13] boljšo identifikacijo, oceno, prioritete ter zoperstavljanje grožnjam, ki jih predstavljajo tuje vlade, teroristične skupine in druge nedržavne tvorbe. Prav tako naj bi pripomogla k učinkovitosti in celostni integraciji vseh protiobveščevalnih aktivnosti. NCIX vodi Nacionalni protiobveščevalni odbor (National Counterintelligence Policy Board). (NCIX.gov: *Office of the National Counterintelligence Executive*. Dostopno na: http://www.ncix.gov/about/index.html (4. junij 2006)).

NCIX sestavljajo višji uradniki protiobveščevalne in drugi specialisti iz celotne obveščevalne skupnosti ZDA. Med drugim NCIX razvija, koordinira in izdeluje: vsakoletno oceno delovanja tujih obveščevalnih služb, nacionalno CI strategijo za vlado, prioritete, proračun za protiobveščevalno dejavnost, oceno škode vohunjenja

[13] Obveščevalna skupnost ZDA (Intelligence Community IC) je zveza izvršnih vej služb in organizacij, ki delujejo ločeno in skupaj v obveščevalni dejavnosti, ki je potrebna za zunanjo politiko in nacionalno varnost ZDA (US Intelligence Communitty: *Definiton of the Intelligence Community*. Dostopno na: http://www.intelligence.gov/1-definition.shtml (5. junij 2006)).

in širi protiobveščevalno zavest, usposabljanje in politiko (NCIX.gov: *Description*. Dostopno na: http://www.ncix.gov/about/ONCIXDescription.pdf (4. junij 2006)).

»National Counterintelligence Policy Board« je bila ustanovljena z ustanovnim aktom (Authorization act) leta 1995 (odstavek 811) in dopolnjena z National Counterintelligence Act iz leta 2002 (Section 903). Glavne naloge so oblikovanje politike in procedur na področju protiobveščevalne dejavnosti. Dodatne naloge Odbora kot medagencijskega elementa so zagotavljanje diskusij in revizij zadev, ki se nanašajo na CI Ehancement Act (Zakon za spodbujanje protiobveščevalne dejavnosti) iz leta 2002, podaja nasvete glede prioritet Nacionalne CI strategije, rešuje konflikte med elementi CI skupnosti. Če je potrebno, lahko tudi ustanavlja medslužbene podskupine. Na podlagi National Counterintelligence Enhancement Act 2002 »National CI Policy Board« sestavljajo (1) National Counterintelligence Executive, (2) višji uradniki (senior) vlade Združenih držav. Te so: Ministrstvo za pravosodje, Zvezni preiskovalni biro FBI; Ministrstvo za obrambo, Joint Chief of Staff, Zunanje ministrstvo, Ministrstvo za energijo, Centralna obveščevalna agencija CIA, Ministrstvo za domovinsko varnost ter vsako ministrstvo, služba ali element vlade Združenih držav, ki jo določi predsednik ZDA (NCIX.gov: *National Counterintelligence (CI) Policy Board.* Doostopno na http://www.ncix.gov/about/NatlCIPolicyBoardDesc.pdf (4. junij 2006)).

Med slednje spadajo še obveščevalna služba letalskih sil ZDA (Air Force Intelligence), Vojaška obveščevalna služba (Army Intelligence), obveščevalna služba Obalne straže (Coast Guard Intelligence), Obrambna obveščevalna služba (Defense intelligence Agency), Finančno ministrstvo (Department of the Treasury), Drug Enforcement, Vlada (Administration), Obveščevalna služba Marinskega korpusa (Marine Corps Intelligence), National Geospatial-Intelligence Agency, Nacionalni izvidniški urad (National Reconnaissance Office), Nacionalna varnostna agencija NSA (National Security Agency), Mornariška obveščevalna služba (Navy Intelligence) (US Intelligence Community: *Members of the Intelligence Community*. Dostopno na http://www.intelligence.gov/1-members.shtml (5. junij 2006)).

V okviru obveščevalne skupnosti ZDA so osnovne naloge s področja protiobveščevalnega dela in zaščite ustavne ureditve, ki jih izvaja Zvezni preiskovalni

biro (FBI). Ena od temeljnih dejavnosti FBI je odkrivanje in preprečevanje dejavnosti pripadnikov in agentur tujih obveščevalnih služb na ozemlju ZDA (Purg, 2002: 80). FBI je edina zvezna služba, ki ima pravico preiskovati tuje protiobveščevalne primere znotraj meja ZDA. Posebej izurjeni protiobveščevalni strokovnjaki sledijo operacijam tujih obveščevalnih služb, jih nevtralizirajo, preiskujejo kršitve zveznih zakonov proti vohunjenju, zlorabi podatkov, in drugih zadev, ki se nanašajo na nacionalno varnost. S podporo drugih agencij in služb izvaja FBI tudi preiskave vohunjenja v tujini, če je subjekt narave državljan ZDA. Protiobveščevalni program teži k zaščiti nacionalne kritične tehnologije, infrastrukture in informacij. Kraja intelektualne lastnine in tehnologije s strani tujih strank ali vlad neposredno ogroža razvoj in proizvodnjo ameriških proizvodov, kar pa posredno vpliva na ekonomsko in politično moč države. V tem smislu je FBI obširno povečal število preiskav, ki se nanašajo na ekonomsko vohunjenje (FBI.gov, 2003). Centralna obveščevalna agencija CIA in Zvezni preiskovalni biro FBI tesno sodelujeta na področju protiobveščevalne dejavnosti (CIA.gov, 2006).

Primarno protiobveščevalno dejavnost izven ZDA izvaja CIA. Vendar CIA ne izvaja več sistematične in programsko usmerjene protiobveščevalne misije, niti ne vodi pomembnejših, strateško ofenzivnih protiobveščevalnih operacij proti nasprotnikovim obveščevalnim službam. Osredotoča se predvsem na obrambni vidik; Protiobveščevalni Center CIE in drugi protiobveščevalni elementi Direktorata za operacije so prvenstveno usmerjeni v zaščito operacij CIE.

Ministrstvo za obrambo in njene protiobveščevalne enote, ki se nahajajo v vojaških organizacijah, so usmerjene v zaščito oboroženih sil. Oddelek za protiobveščevalno dejavnost na bojišču (Department's Counterintelligence Field Activity (CIFA)) sicer povezuje in koordinira protiobveščevalno dejavnost, vendar nima pooblastil in kapacitet za širše protiobveščevalne operacije (GPOaccess.gov 2005).

6. 1. 2 Študija primerov protiobveščevalne dejavnosti v ZDA

Podal bom nekatere primere protiobveščevalne dejavnosti v ZDA, ki je sicer zelo obširna. Dva tipična primera delovanja dvojnega agenta in krta sta bila opisana že v prejšnjem poglavju.

Regan, Brian Patrick, nekdanji obveščevalni analitik Letalstva, je bil aretiran 3. avgusta 2001 na mednarodnem letališču Dulles, ko se je želel vkrcati za let v Švico. S sabo je imel informacije o raketnih izstreliščih v Iraku in kontaktne informacije ambasad v Švici. Regan, ki je vstopil v letalstvo pri sedemnajstih, je začel delati za National Reconnaissance Office leta 1995, kjer je upravljal Intelink, zaupno medmrežje za obveščevalno skupnost. Po upokojitvi v vojski leta 2001 se je zaposlil kot obrambni pogodbenik pri TRW in pozneje deloval pri NRO. Regan je imel dostop do tajnih podatkov vse od leta 1980. Na njegovem domačem računalniku so našli pisma, v katerih je za denar ponujal podatke Libiji, Iraku in Kitajski. 20. februarja 2003 je bil obsojen na dosmrtno ječo brez pogojne kazni. Po obsodbi je FBI lociral 19 območij, kjer je Regan zakopal več kot 20.000 strani tajnih dokumentov, pet CD-jev in pet video kaset, vseh namenjenih za prodajo. Motiv za to delovanje naj ne bi bil samo denar, temveč tudi nezadovoljstvo na delu in odnos s sodelavci.

Tri osebe, ki so preko svojega podjetja predajale zaupne informacije nacionalno varnostne narave raziskovalnim inštitutom v Ljudski Republiki Kitajski: predsednik družbe Xu Weibo, a/k/a Kevin Hu je bil osojen na 44 mesecev zaporne kazni in mora po izpustitvi živeti še dve leti pod nadzorom; žena Xiu Ling Chen, a/k/a Linda Chen je dobila 18 mesecev zapora in dve leti nadzora; podpredsednik in brat žene Hao Li Chen, a/k/a Ali Chan pa 30 mesecev in dveletni nadzor (U.S. Department of Justice 2006).

Shasban Hafiz Ahmad Ali Shaaban je bil obsojen vohunjenja za Irak. Leta 2002 je potoval v Bagdad, kjer se je dogovoril za prodajo imena obveščevalcev ZDA Iraku za tri milijone dolarjev, želel je tudi pridobiti iraško podporo pri ustanovitvi arabske televizije v ZDA, ki bi delovala proiraško (U.S. Department of Justice 2006a).

Združenim državam ne vohunijo samo sovražniki temveč tudi zavezniške države. Lawrence A. Franklin, nekdanji uslužbenec Ministrstva za obrambo z oddelka za Irak v Pentagonu je bil skupaj z Steven J. Rosenu in Keith Weissmanu, nekdanjima uslužbencema American Israel Public Affairs Committee (AIPAC), obdolžen zarote in nezakonitega prilaščanja zaupnih dokumentov. Za njimi naj bi stala država Izrael (U.S Department of Justice 2006b).

6. 2 PROTIOBVEŠČEVALNA DEJAVNOST V RUSKI FEDERACIJI

Ruska federacija ima obveščevalno-varnostne službe razdeljene na zunanje in notranje. Glavni zunanji obveščevalni službi sta Zunanja obveščevalna služba (SVR) in Vojaška obveščevalna služba (GRU), notranjo obveščevalno dejavnost opravljajo Zvezna varnostna služba (FSB), Državna tehnična komisija (Gostekhkomissiya) ter Zvezna zaščitna služba (FSO) (Agentura.ru: *Special Services of Russia.* Dostopno na http://www.agentura.ru/english/dosie/ (10. januar 2007)).

Glavno vlogo protiobveščevalni dejavnosti v Rusiji nosi Zvezna varnostna služba (Federal'naya Sluzhba Bezopasnosti) FSB. V skladu z zakonom »o organih zvezne varnostne službe v RF« je FSB sestavljena iz varnostnih sil Ruske federacije, ki v svojih okvirih zagotavljajo osebno, družbeno in državno varnost. FSB je zvezni organ vlade, organizacija, ki je podrejena neposredno ruskemu predsedniku. Glavni dejavnosti Zvezne varnostne službe sta: (1) protiobveščevalna dejavnost in (2) nadzor kriminala. Poleg tega lahko FSB izvaja obveščevalno dejavnost, in sicer »v okviru svojih pooblastil in v sodelovanju z organi Ruske federacije, ki so zadolženi za zunanjo obveščevalno dejavnost z namenom, da pridobi informacije o varnostnih grožnjah Ruske federacije« (Agentura.ru: *Federal security service (FSB).* Dostopno na http://www.agentura.ru/english/dosie/fsb/ (10. januar 2007)).

Septembra 2004 je prišlo do reforme strukture Zvezne varnostne službe. Nastalo je osem služb in dva direktorata. Organa znotraj FSB, ki sta zadolžena za protiobveščevalno dejavnost, sta protiobveščevalna služba in direktorat, slednji zadolžen za vojaško protiobveščevalno aktivnost (Soldatov 2007).

FSB aktivno sodeluje z sorodnimi službami znotraj ruskega obveščevalnega sistema, še posebej z zunanjo obveščevalno službo SVR. Preko nje izvaja ofenzivno protiobveščevalno dejavnost. Cilj SVR je zbiranje in procesiranje informacij o realnih in potencialnih možnostih, akcijah in namenih tujih držav, organizacij ali oseb, ki bi lahko vplivale na vitalne interese Ruske federacije (Agentura.ru: *SVR Foreign Intelligence Service.* Dostopno na http://www.agentura.ru/english/dosie/svr/ (10. januar 2007)). Struktura FSB je razdeljena na službo za stike z javnostjo in pet departmajev, od katerih je drugi zadolžen za zunanjo protiobveščevalno dejavnost. Poleg departmajev je v sestavi še SVR Akademija (Agentura.ru: *SVR structure*. Dostopno na http://www.agentura.ru/english/dosie/svr/structure/ (10. januar 2007).

6. 2. 2 Študija primerov delovanja protiobveščevalne dejavnosti v Ruski federaciji

31. oktobra 2001 je bil generalni direktor delniške družbe »Elers elektron« Victor Kalaydina, obsojen na 14 let zapora. Bil je spoznan za krivega vohunjenja za ZDA. 53-letni poslovnež je bil aretiran leta 1998 s strani FSB. Uslužbenci FSB so ugotovili, da je Kalaydin med obiskom v Francji prodal uslužbencu podjetja General Dynamics Faridu Rafi, podroben opis varnostne zaščite tanka »Arena« (Agentura.ru: *Victor Kalyadin is condemned for espionage.* Dostopno na http://www.translate.ru/url/tran_url.asp?lang=ru&direction=re&template=General&cp1=CP1251&cp2=NO&autotranslate=on&transliterate=on&url=http%3A%2F%2Fwww.agentura.ru%2Ftimeline%2F2001%2Fkalyadin%2F (10. januar 2007)).

6. Aprila 2001 je protiobveščevalna služba FSB na območju Stavropola razkrila dva turška skavta. Delovala sta neodvisno drug od drugega, vsak s svojimi specifičnimi nalogami. Eden od odkritih, Khaki Mutlodogan, je prispel v Stavropol iz Bolgarije. Deloval je pod krinko kot lastnik podjetja v Trabzonu, kjer je delal kot prevajalec.

Drugi vohun, Nesrin Uslu, je končala študij na oddelku za slavistiko na univerzi v Ankari. Prav tako je delala kot prevajalka pri podjetju Idil. Preiskava je pokazala, da je dejansko zbirala ekonomske podatke o območju. Uslu je pozneje ponudila svoje

usluge FSB (Agentura.ru: *On Stavropole have caught two turkish spies*. Dostopno na http://www.translate.ru/url/tran_url.asp?lang=ru&direction=re&template=General&cp1=CP1251&cp2=NO&autotranslate=on&transliterate=on&url=http%3A%2F%2Fwww.agentura.ru%2Ftimeline%2F2001%2Ftur%2F (10. januar 2007)).

9, aprila 2001 je zvezna protiobveščevalna služba oznanila, da je bila v ugrabitev ruskega letala TU-154 leta 1996 vpleten turški specialni oddelek. Prej so bili za ugrabitev krivi izključno Čečeni (Agentura.ru: *FSB: turkish special services are involved in capture of plane, TU-154.* Dostopno na http://www.translate.ru/url/tran_url.asp?lang=ru&direction=re&template=General&cp1=CP1251&cp2=NO&autotranslate=on&transliterate=on&url=http%3A%2F%2Fwww.agentura.ru%2Ftimeline%2F2001%2Fsamolet%2F (10. januar 2007)).

Leta 2002 je zvezna služba FSB, pridobila informacije o namenih ameriške centralne obveščevalne službe CIA, ki naj bi želela pridobiti informacije o ruskem razvoju orožja, in vojaško-tehničnem sodelovanju Rusije s članicami SND (Skupnost neodvisnih držav). FSB je za te namene izvedela pravočasno. Aprila 2001 je ruski znanstvenik s kodnim imenom Viktor prispel na ameriški konzulat, da bi izvedel določene informacije o sorodnikih v ZDA. Na veleposlaništvu naj bi bil omamljen in tako primoran predati določene podatke uslužbencem ambasade. Pod varstvom FSB je še enkrat stopil v kontakt z veleposlaništvom in deloval kot dvojni agent (Agentura.ru: *The third secretary of embassy of teh USA is caught on recruitment of the scientist*. Dostopno na http://www.translate.ru/url/tran_url.asp?lang=ru&direction=re&template=General&cp1=CP1251&cp2=NO&autotranslate=on&transliterate=on&url=http%3A%2F%2Fwww.agentura.ru%2Ftimeline%2F2002%2Fsavant%2F (11. januar 2007)).

Moskovsko okrožno vojaško sodišče je na osem let zapora obsodilo polkovnika Aleksandra Sypacheva, ki je bil ruski obveščevalni skavt. Obdolžen je bil predaje državne skrivnosti Centralni obveščevalni službi CIA. Sypachev je sam vzpostavil stik z ameriško ambasado in jim ponudil sodelovanje. Nameraval jim je predati zaupne podatke o strukturi zaposlenih v ruski obveščevalni službi. To so preprečili agentje FSB (Agentura.ru: *For espionage on CIA military scout is condemned*. Dostopno na http://www.translate.ru/url/tran_url.asp?lang=ru&direction=re&template=General&cp1=CP1251&

cp2=NO&autotranslate=on&transliterate=on&url=http%3A%2F%2Fwww.agentura.ru%2Ftimeline%2F2002%2Fsypachev%2F (11. januar 2007)).

27. februarja 2003 se je na moskovskem okrožnem vojaškem sodišču začelo sojenje Aleksandru Zaprozhskim, ki je bil častnik pri zunanji obveščevalni službi in osumljen vohunjenja za ZDA. Aretiran je bil leta 2001 v Moskvi. Leta 2003 je bil spoznan za krivega veleizdaje in obsojen na 18 let zapora (Agentura.ru: *The scout Zaporozhye is condemned for espionage in favour of the USA*. Dostopno na http://www.translate.ru/url/tran_url.asp?lang=ru&direction=re&template=General&cp1=CP1251&cp2=NO&autotranslate=on&transliterate=on&url=http%3A%2F%2Fwww.agentura.ru%2Ftimeline%2F2003%2Fzaporojsky%2F (11. januar 2007)).

6. avgusta 2004. je rusko zunanje ministrstvo oznanilo kot »persona non grata« vojaškega atašeja litvanskega veleposlaništva v Moskvi. Polkovnik Butkus naj bi bil vpleten v dejavnosti, ki škodujejo interesom Rusije (Agentura.ru: *The military attache of Lithuania is sent from Moscow.* Dostopno na http://www.translate.ru/url/tran_url.asp?lang=ru&direction=re&template=General&cp1=CP1251&cp2=NO&autotranslate=on&transliterate=on&url=http%3A%2F%2Fwww.agentura.ru%2Ftimeline%2F2004%2Flitvaattache%2F (11. januar 2007)). To naj bi bil dejansko povračilen korak zaradi izgona ruskega vojaškega atašeja iz Litve.

6. 3 PROTIOBVEŠČEVALNA DEJAVNOST V VELIKI BRITANIJI

Združeno kraljestvo ima tri obveščevalno-varnostne službe; Secret Intelligence Service (SIS), Government Communication Hesdquarters (GCHQ) in Security Service – Varnostna služba. Podlaga za delovanje prvih dveh služb je Zakon o obveščevalnih službah iz leta 1994 (Intelligence Services Act 1994), za Varnostno službo velja Zakon o varnostni službi iz leta 1989 in 1994 (Security Service Acts 1989 and 1994). Operacije se izvajajo v skladu z Zakonom o pravilniku preiskovalnih organov (Regulation of Investigatory Powers Act 2000). Poleg teh služb obstaja še Obrambni obveščevalni štab (Defence Intelligence Staff), ki je sestavni del Ministrstva za obrambo (National Intelligence Machinery 2000).

Služba, ki je zadolžena za protiobveščevalno dejavnost v Veliki Britaniji je Security Service, imenovana tudi MI5. Security Service je zadolžena za »zaščito VB pred grožnjami nacionalne varnosti, kot so vohunjenje, terorizem, sabotaže, aktivnosti, ki jih izvajajo agenti tujih sil, in pred dejavnostmi, katerih namen je rušitev ali spodkopavanje parlamentarne demokracije z političnimi, industrijskimi ali nasilnimi sredstvi« (Uradna stran MI5: *Role & Organisation*. Dostopno na http://www.mi5.gov.uk/output/Page18.html (10. junij 2006)).

Glavna področja delovanja Security Service so: protiteroristična dejavnost, varnostno svetovanje, protivohunstvo, delo na področju preprečevanja širjenja orožja za množično uničevanje, organizirani kriminal, sodelovanje s sorodnimi službami ter druga področja. Resursi za protivohunstvo so se v zadnjih letih precej okrnili in znašajo danes približno 6 % celotnih kapacitet Security Service (Uradna stran MI5: *Our major areas of work*. Dostopno na http://www.mi5.gov.uk/output/Page19.html (10. junij 2006)).

V Veliki Britaniji se je cilj vohunjenja premaknil s političnih in vojaških sfer v gospodarske. Ocenjeno je, da naj bi v VB delovalo okoli 20 tujih služb, od katerih največjo skrb povzročata Rusija in Kitajska. Security Service tako tudi svetuje podjetjem pri varovanju njihovih skrivnosti pred tujimi obveščevalnimi službami (Uradna stran MI5: *Espionage*. Dostopno na http://www.mi5.gov.uk/ output/Page11.html (10. junij 2006). Neposredne protiobveščevalne naloge izvaja Special Branch, ki spada pod Scotland Yard in predstavlja nekakšno vrsto policije za tujce (Purg 1999: 84–85).

Poleg Secret Service se z protiobveščevalno dejavnostjo ukvarjajo še druge britanske službe. Secret Intelligence Service, znana tudi kot MI6, zbira obveščevalne informacije v tujini (Uradna stran Secret Intelligence Service: *About us*. Dostopno na http://www.sis.gov.uk/output/Page2.html, (10. junij 2006)), vendar obstaja v okviru službe Oddelek za varnost, ki protiobveščevalno ščiti britanska predstavništva v tujini (Purg 1999: 84). Velika Britanija ima tudi obveščevalne službe v vseh treh rodovih svojih oboroženih sil, ki imajo v svojem sestavu tudi protiobveščevalne službe (Purg 1999: 85).

6. 3. 1 Študija primerov delovanja protiobveščevalne dejavnosti v Veliki Britaniji

V Veliki Britaniji po letu 2000 ni bilo odmevnejšega primera vohunjenja. Secret Service zadolžena za protiobveščevalno delovanje se, zlasti po terorističnih napadih na londonsko podzemno železnico, osredotoča na protiteroristično področje, predvsem na islamski terorizem.

Kljub temu ostaja grožnja delovanja tujih obveščevalnih služb še vedno prisotna. V letnem poročilu 'Intelligence and Security Committtee' (ISC) za leto 2004—2005, je bila kot že leta poprej izražena skrb, da se sredstva za protivohunsko delovanje zmanjšujejo. Da se Velika Britanija izpostavlja varnostnemu tveganju, priznavata tudi glavni direktor Secret Service in notranji minister. Protiobveščevalna dejavnost v Veliki Britaniji trpi predvsem na račun protiteroristične dejavnosti (ISC 2005). Države naj bi kljub koncu Hladne vojne še vedno uporabljale svoje vohunske mreže za pridobivanje tajne vladne informacije, ali kradejo podjetniške skrivnosti. Glavni direktor Secret Service je sicer že obljubljal povečanje sredstev za protivohunsko delovanje (BBC Online 2004).

Luknjo v sistemu s pridom izkorišča Rusija, ki naj bi spet nadaljevala z aktivno obveščevalno dejavnostjo v Veliki Britaniji. Britanski notranji minister David Blunkett naj bi bil na to večkrat opozorjen s strani MI5. Rusi bi potemtakem pregledovali premike vojaškega letalstva v VB, pri vohunjenju za vojaškimi strokovnjaki pa naj bi uporabljali internet. Alex Standish, urednik Jane's Intelligence Digest, ugotavlja, da je v VB vedno več ruskih diplomatov, ki se jih na takšen ali drugačen način da povezati s SVR, rusko zunanjo obveščevalno službo (Strategypage 2004).

Več kot vojaški in politični pozornosti se posveča ekonomski protiobveščevalni dejavnosti. MI5 je preiskovala strokovnjaka za informacijsko tehnologijo Anthony Benfielda, kar naj bi bilo del širše preiskovalne akcije. Akcija naj bi potekala proti osebam, osumljenim predaje tajnih računalniških podatkov britanskih podjetij francoskim (BBC Online 2000).

Intelligence and Security Committee Annual Report, ki letno poroča o delovanju lastnih obveščevalno-varnostnih služb, že od leta 2000 opaža, da se tradicionalno vohunjenje s strani tujih vlad ni znižalo (ISC 2001). Leto poprej je bilo 20 % kapacitete Secret Service usmerjenih v protiobveščevalno delovanje (ISC 2000). Poročilo v naslednjih letih ugotavlja znižanje sredstev protiobveščevalni dejavnosti na račun protiteroristične. V letih 2001—2002 so sredstva, ki so pripadala protiteroristični dejavnosti, znašala 23 %, protiobveščevalni samo 16 % (ISC 2002). Trend redistribucije sredstev se nadaljuje tudi v naslednjih letih (ISC 2003). Zato sledi v letih 2003—2004 bolj izčrpno poročilo o protiobveščevalni dejavnosti. Poročilo ugotavlja, da se obveščevalna dejavnost tujih držav v Veliki Britaniji ni zmanjšala ter da največje grožnje predstavljata Rusija in Kitajska. Delež sredstev za protiobveščevalno dejavnost znotraj Secret Servica je takrat znašal le še 11 %, ob tem izražajo skrb za nacionalno varnost zaradi zanemarjanja protiobveščevalnega dela (ISC 2004).

V času zmanjševanja sredstev za protiobveščevalno delovanje, je prišlo v letih 2001 in 2002 do dveh vohunskih incidentov. Leta 2001 je varnostnik Rafael Bravo priznal, da je poskušal ukrasti vojaške skrivnosti in jih prodati naprej Rusom. Prodati jih je poskušal agentu MI5, ki je deloval pod krinko. Aretiran je bil s strani Special Branch na sestanku z omenjenim agentom (BBC Online 2001).

Naslednje leto je vohunjenje za Ruse priznal letalski inženir Ian Parr. Parr je bil zaposlen pri BAE system Avionics. Tudi on je padel v past agentom MI5 in sicer v lokalnem baru, kjer naj bi se sestal z domnevnim ruskim obveščevalcem. Tajne informacije je želel prodati za okoli 130.000 funtov (BBC Online 2002).

Oba primera nista imela v ozadju političnega ali vojaškega interesa, šlo je predvsem za izdajo državne skrivnosti z namenom pridobitve finančnih ugodnosti. Denar je pri tajni obveščevalni dejavnosti oziroma vohunjenju zelo močan motivator.

6. 3 PROTIOBVEŠČEVALNA DEJAVNOST V ZRN

Zvezna Republika Nemčija poseduje naslednje obveščevalno varnostne službe: Zvezna obveščevalna služba (BND – Bundesnachrichtendienst), Zvezni kriminalistični urad (BKA – Bundeskriminalamt), Zvezna mejna zaščita (BGS – Bundesgrentzschutz) Zvezna služba za zaščito ustavne ureditve (BfV - Bundesamt fuer Verfassunschutz) in Vojaška protiobveščevalna služba (MAD - Militärischer Abschirmdienst) (Purg 2002: 78).

Ključna služba, ki v Zvezni republiki Nemčiji opravlja protiobveščevalno dejavnost, je Zvezna služba za zaščito ustavne ureditve. Ukvarja se izključno z zadevami zaščite države. Podrejena je vladi, uradno pa je pod nadzorom Ministrstva za notranje zadeve. Na ravni zveznih dežel obstajajo pokrajinski uradi za zaščito ustave, ki tesno sodelujejo z zvezno službo. BfV raziskuje, zbira in ocenjuje podatke o dejavnostih, ki so usmerjene na rušenje ali spremembo ustavne ureditve (Purg, 2002: 78). Področja dela (Uradna spletna stran BfV: *Arbeitsfelder*. Dostopno na http://www.verfassungsschutz.de/de/arbeitsfelder/, (5. junij 2006)) Zvezne službe za zaščito ustave so: desni politični ekstremizem (neonacisti, skinheadi ipd.), levičarski politični ekstremizem (razne levičarske organizacije stranke, Avtonomi itd.), politični ekstremizem tujcev v ZRN (islamisti ipd.), scientološka cerkev in tuje obveščevalne službe[14]. Slednje so področje protiobveščevalne dejavnosti.

Zvezna obveščevalna služba BND je primarno pristojna za zbiranje obveščevalnih informacij in podatkov v tujini s političnega, gospodarskega, vojaškega in drugih področij (Purg 2002: 78). Služba je neposredno podrejena vladi, ki tudi določa prioritete zbiranja podatkov. Je edina služba V Nemčiji, ki opravlja obveščevalno dejavnost v tujini. Kljub temu, da doma nima pristojnosti, lahko zbira podatke na domačem teritoriju, če se ti nanašajo na zunanjost. BND nima policijskih pooblastil (Uradna spletna stran Bundesnachrichten dienst: *Die Nachrichtendienste der Bundesrepublik Deutschland.* Dostopno na http://www.bnd.bund.de/nn_355342/DE/Unser__Auftrag/Zusammenarbeit/Zusammenarbeit__node.html__nnn=true, (5. junij 2006)). Sestavljena

[14] Nemci nimajo izraza za protiobveščevalno dejavnost in to aktivnost enačijo z protivohunstvom (Spionageabwehr).

je iz osem oddelkov, od katerih je zadnji, osmi oddelek pristojen za varnost, varovanje tajnih podatkov in protivohunstvo (Uradna spletna stran Bundesnachrichten dienst: *Abteilung 8 – Sicherheit, Geheimschutz und Spionageabwehr*. Dostopno na http://www.bnd.bund.de/nn_354670/DE/Wir__Ueber__Uns/Struktur/Abteilung8/Abteilung8__node.html__nnn=true, (5. junij 2006)).

Prav tako opravlja protiobveščevalno dejavnost v ZRN Vojaška protiobveščevalna služba MAD (Militärischer Abschirmdienst). MAD je del Oboroženih sil in je notranja obveščevalno-varnostna služba, ki dejansko opravlja enake naloge v Zvezni armadi (Bundeswehr), kot jih opravlja Zvezna služba za zaščito ustavne ureditve BfV izven vojske. MAD enako zbira informacije o tajnem delovanju tujih vlad, ki so usmerjene proti Bundeswehr. O teh dejavnostih poroča svojim nadrejenim in na podlagi informacij sprejema varnostne ukrepe (Uradna spletna stran Bundeswehr: *MAD*, dostopno na http://www.bundeswehr.de/portal/a/bwde/streitkraefte/_streitkraeftebasis/mad, (5. junij 2006)).

6. 3. 1 Študija primerov delovanja protiobveščevalne dejavnosti v ZRN

Zvezna republika Nemčija ostaja še vedno cilj obveščevalnih služb tujih vlad. Od leta 2000 predstavljajo največjo grožnjo obveščevalne službe Skupnosti neodvisnih držav, predvsem Ruska federacija in Belorusija. Rusija želi ponovno postati velesila in s tem namenom vohuni za svojimi »prijatelji«. Sledijo države severne Afrike, Bližnjega ter Daljnega vzhoda. Iran deluje v Nemčiji predvsem v smeri nevtralizacije delovanja iranskih opozicijskih skupin. Med drugim je bil 8. oktobra 2001 zaradi suma vohunjenja aretiran 43-letni iranski državljan. Iranec je kot konstruktor delal v večji letalski družbi na jugu Nemčije, kjer je želel pridobiti podatke, s katerimi na svojem delovnem mestu ne bi mogel imeti stika.

V ZRN je aktivna tudi Sirija, ki prav tako preganja svojo opozicijo v tujini, preko diaspore ji je uspelo vzpostaviti agenturne mreže. 5. decembra sta bila v Bonnu in Maunzu prijeta dva državljana Sirije. Obtožena sta bila preiskovanja oseb, ki so

emigrirali iz Sirije in se niso strinjali z režimom. Podobne dejavnosti opravljajo v ZRN tudi Irak in Libija.

Z Daljnega vzhoda sta predvsem Kitajska in Severna Koreja državi, ki opravljata obveščevalno dejavnost v Nemčiji. Kitajska je aktivna na tradicionalnih področjih vohunjenja, kot so politična, vojaška, industrijska in predvsem znanstvena. Kitajska teži k čim večjemu gospodarskem razvoju in pri tem uporablja tehnološke skrivnosti. Podobno želi Severna Koreja pri vohunjenju pridobiti določene tehnološke prednosti, znana je predvsem po želji po oborožitvi z orožjem za množično ubijanje

Leta 2002 je bilo sproženih 31 preiskav s strani zveznega tožilca. Osem oseb je bilo aretiranih, proti šestim je bila izdana tiralica. V istem času so nemška sodišča obsodila tri obtožence državne izdaje in ogrožanja varnosti (BfV bericht 2001: 263–283).

Naslednje leto poročilo ugotavlja povečanje aktivnosti iraških obveščevalnih služb. Navezali so stike z skrajnimi desničarji v Nemčiji, da bi s tem širili antiameriško in antiizraelsko koalicijo. Leta 2002 je bilo sproženih 31 preiskav s strani zveznega tožilca, 30 zaradi suma vohunjenja in eno zaradi državne izdaje. Ena oseba je bila priprta, višje sodišče v Düsseldorfu jo je obsodilo državne izdaje (BfV bericht 2002: 220–237).

29. septembra 2003 je bil nemški Iranec, ki je od leta 1991 do 2003 po ukazih iranske obveščevalne službe VEVAK povzročal nemire med iransko izseljeniško opozicijo, obsojen na dve leti in šest mesecev zapora. Do začetka vojne v Iraku marca 2003 je bila obveščevalna dejavnost v Nemčiji zelo aktivna. Veleposlaništvo so ob začetku vojne zaprli, obveščevalne službe pa so po padcu Husseina razpustili.

Obveščevalne službe Severne Koreje so aktivne na področju pridobitve tehnologije za množično uničevanje. Aprila 2003 je uspelo preprečiti preprodajo takšnih materialov. Aluminijske cevi, ki so potrebne za izdelavo centrifug za bogatenje Urana, so bile namenjene iz Hamburga na Kitajsko nato v Severno Korejo (BfV Bericht 2003: 190–195).

Leta 2004 je zvezni tožilec sprožil 25 preiskav v zvezi z delovanjem tujih obveščevalnih služb. Deset oseb je bilo aretiranih. Istega leta so bile štiri osebe obsojene državne izdaje in ogrožanja nacionalne varnosti (BfV Bericht 2004: 266).

V letu 2005 ostajajo v obveščevalnem delovanju glavni v ZRN Rusi. Dejavni so tako na političnem kot na vojaškem obveščevalnem področju, kjer sta bila uslužbenca GRU pod diplomatsko identiteto primorana predčasno zapustiti Nemčijo. Na področju ekonomije Ruse najbolj zanima evropsko energetsko vprašanje. Cilj Kitajcev je predvsem gospodarsko vohunjenje Nemčiji, ki velja za eno vodilnih zahodnih ekonomij. Severna Koreja želi izboljšati svoj nuklearni program z znanjem zahoda in sestavinami. Druge države, kot so Iran, Sirija in Libija, težijo k nevtralizaciji emigrantskih opozicijskih skupin, ki živijo v Nemčiji. V letu 2005 je bilo tako v zvezi z obveščevalnim delovanjem tujih držav sproženih 29 preiskav. Štiri osebe so aretirali, ena je bila obsojena vohunjenja (BfV Bericht 2005: 275–297).

6. 4 PROTOBVEŠČEVALNA DEJAVNOST V IZRAELU

Izrael sestavljajo naslednje obveščevalno-varnostne službe: MOSSAD – Central Institut for Intelligence and Special Duties – osrednja obveščevalna služba, ki je pristojna za delo v tujini, med področji dela je tudi boj proti terorizmu; AMAN – vojaška obveščevalna služba – Israeli Defence Forces Intelligence Branch, AMAN tudi usmerja dejavnosti specializiranih obveščevalnih služb – Air Force Intelligence in Naval Intelligfence. V okviru Ministrstva za zunanje zadeve je Center za raziskovanje in planiranje, ki pripravlja obveščevalne analize in informacije, poleg tega naj bi se ukvarjal tudi z zbiranjem podatkov preko diplomatskih kanalov. ŠABEK – General Security Services (opomba: uporablja se tudi izraz ŠIN BET) je služba notranje varnosti, katere glavna dejavnost je usmerjena v protiobveščevalno delo in boj proti terorizmu (Purg 2002: 132–133).

V začetku leta 2000 so direktorji Amana, Mossada in ShinBetha podpisali sporazum, ki naj bi zagotovil vzpostavitev reda v delovanju subjektov v izraelski obveščevalno-varnostni skupnosti. Ta sporazum je poznan pod imenom Magna Carta 2 in določa polje odgovornosti posameznega subjekta. Tako je Aman postal glavna

obveščevalna služba v zadevah zbiranja in ocenjevanja podatkov. Mossad je postal zadolžen za pošiljanje in vodenje agentov v oddaljene države, vštevši vse arabske. Shin Beth je še naprej zadolžen za protiobveščevalno dejavnost na domačih tleh. Zaradi še vedno nejasne ločenosti področij dela izraelskih služb še vedno prihaja do prepletenosti delovanja služb na določenih področjih (Kahana v Požun 2004: 67).

Služba, pristojna za protiobveščevalno dejavnost v Izraelu, je tako Shin Bet. Po podpisu Magne Carte 2 leta 2000 so glavne naloge Shin Betha postale: preprečevanje in boj zoper palestinski terorizem, protiteroristična dejavnost; preprečevanje vsakršnih podtalnih dejavnosti na vsem ozemlju države, vključno z arabskimi sektorji; varovanje pomembnih osebnosti in institucij ter protiobveščevalna dejavnost.

Shin Beth je razdeljen na dva dela: operativni del in del za podporo, ki vključuje tehnične, administrativne in pomožne službe. Operativni del je nadalje razdeljen na tri sektorje: sektor za varnost in zaščito, sektor za arabske zadeve ter sektor za protiobveščevalno dejavnost, ki se imenuje Shabak. Ponekod v literaturi zasledimo, da se s tem imenom imenuje celotna služba Shin Beth, kar kaže na pomembnost dejavnosti, s katero se ukvarja ta sektor. V pristojnosti tega sektorja je torej protiobveščevalna dejavnost, ki vsebuje: odkrivanje in preprečevanje obveščevalne (vohunske) dejavnosti tujih služb in organizacij, nadzorovanje dejavnosti tujih diplomatsko-konzularnih predstavništev v Izraelu in nadzor tujih delegacij, skupin in posameznikov, ki se iz različnih razlogov nahajajo v Izraelu (Požun 2004: 42).

6. 4. 1 Študija primerov delovanja protiobveščevalne dejavnosti v Izraelu

Izrael je primer države, katere protiobveščevalna dejavnost je usmerjena v teroristične organizacije, kakršna je Hezbolah. Leta 2002 je bil rezident centralnega Izraela obtožen vohunjenja proti Izraelu. Nissim Naser je emigriral iz Libanona pred desetimi leti, njegov oče je bil libanonski Šiit, mati pa Židinja (IsraelINN.com 2002).

Obtožen je bil predaje večje količine občutljivih informacij Hezbolahu preko svojega brata. Hezbolah je preko njega želel zemljevid mesta Tel Aviv, kjer so prikazane

pomembnejše strateške točke, sliko člana družine, ki je zaposlen v izraelskih varnostni silah, preko katerega bi poskušali priti do vez z višjimi oficirji izraelskih oboroženih sil. S tem bi lahko pridobili informacije o različnih vojaških operacijah in o možnih reakcijah izraelskih sil na teroristične napade. Obtožnica ga bremeni tudi izdaje načrtov Izraela o atentatih na pomembnejše teroristične pripadnike v Libanonu in Judeji, Samariji in Gazi (IsraelINN.com 2002a). Oktobra 2002 so izraelske varnostne sile pridržale polkovnika Omar al-Hayeba, ki naj bi bil tisti oficir, ki je predajal informacije Hezbolahu (IsraelINN.com 2002b).

To ni bil edini primer, ko je Hezbolah vohunil s pomočjo drog. Februarja leta 2003 so Izraelci razbili mrežo Arabcev in Židov, ki so v zamenjavo za informacije dobivali drogo od Hezbolaha. Zadnji dve leti naj bi tako šest izraelskih Arabcev iz mesta Rajar, ki leži na meji med Libanonom in Izraelom, ter trije izraelski Židje prodajali občutljive informacije Hezbolahu v zameno, da se zaščiti njihova dejavnost z drogami (IsraelINN.com 2003). V dejavnost s tihotapljenjem drog so bili vmešani tudi pripadniki izraelskih oboroženih sil.

Šiitska teroristična organizacija Hezbolah je močno povezana z Iranom, ki je v precej konfliktnih odnosih z Izraelom. Leta 2004 so Izraelci pridržali Muhammada Ali Ahmed Sayid Ghanema, ki naj bi vohunil za Iran. Ghanem je arabski državljan Izraela in naj bi bil rekrutiran med svojim obiskom Savdske Arabije s strani iranske obveščevalne službe (IsraelINN.com 2006).

Obveščevalno poročilo piše, da je Hezbolah na področju infiltracije v Izrael aktiven že več kot štiri leta. Priložnost za takšno aktivnost so Iranci in Hezbolah videli v Izraelskih Arabcih, ko so se izraelske sile umaknile iz Libanona maja, leta 2000 (IsraelINN.com 2004).

Za Izraelom vohunijo tudi Palestinci. Dva Arabca iz predmestja Jeruzalema Beit Tzafafa sta bila obtožena vohunjenja za Palestinsko upravo. Z obljubami o denarju in drogah naj bi želela rekrutirati dve vojakinji izraelskih oboroženih sil v svojo vohunsko mrežo[15]. Priznala sta svoje veze z Jibril Rajoubovo varnostno službo, eden od njiju

[15] Pri tem naj bi šlo za romantično zvezo z eno od vojakinj, drugo naj bi oskrbovali z drogami (IsraelINN 2002c).

naj bi prenašal informacije o dogajanju v predmestju. Dokumente so prestregli izraelski agenti med operacijo »Obrambni ščit«. Pri tem se je pokazalo, kako lahek dostop imajo Palestinci do izraelskega prebivalstva prav zaradi svobode potovanja, ki se jim ga dodeli, in dejstva, da so zaposleni v Izraelu (IsraelINN.com 2002d).

Obveščevalno dejavnost v Izraelu uporablja tudi palestinska organizacija Hamas. Dva arabska zobozdravnika naj bi vohunila za Hamas. V stik z organizacijo naj bi prišla v Romuniji, od takrat sta predajala informacije tej skupini.

Poleg državne in teroristične protiobveščevalne dejavnosti se Izrael ukvarja tudi s korporacijsko protiobveščevalno dejavnostjo. Izraelska policija je 29. maja 2005 aretirala 18 ljudi, med njimi pomembne poslovneže in zasebne detektive, ker naj bi pri infiltraciji v računalniške sisteme konkurence uporabljali visoko razvito tehnologijo. Pri tem so uporabljali računalniške programe kot so »Trojanski konji« (Israelinsider.com 2005).

Najbolj nenavaden primer je primer Elhanan Tannenbauma. Tannenbaum, nekdanji major izraelskih oboroženih sil, je prebil tri leta v ujetništvu Hezbolaha. Ko se je vrnil v domovino, ni prestal poligrafskega testa in je s tem vzbudil sume glede okoliščin, v katerih je bil ugrabljen. Uslužbenci Shin Beta ne verjamejo njegovi verziji prihoda v Bejrut, kjer naj bi bil ugrabljen. Prav tako se jim zdi sumljivo, da ni v treh letih ujetništva nič izdal. Dejstvo, da ga Hezbolah ni mučil, kaže na to, da je Tannenbaum sodeloval z njimi. Ta primer je povzročil veliko polemik v izraelski družbi (Israelinsider.com 2004).

7. GOSPODARSKA PROTIOBVEŠČEVALNA DEJAVNOST

Kot sem že v prejšnjih poglavjih pokazal, ne obstaja enotna definicija protiobveščevalne dejavnosti. V splošnem se lahko opiše kot identifikacija in nevtralizacija grožnje, ki jih predstavljajo nasprotne obveščevalne službe ter manipulacija teh služb v lasten prid. Drugače povedano pomeni del obveščevalne službe, ki pokriva zmanjševanje učinkovitosti tujih služb, zaščito informacij pred ekonomskim in industrijskim vohunjenjem.

Podjetjem se lahko, če ne pazijo na svoje lastniške informacijske pravice, zgodijo številne stvari. Največja nevarnost je, da podjetje propade zaradi izgube tekmovalne prednosti na trgu. Če podjetja ne ščitijo lastnih kritičnih informacij, izgubijo delež na trgu, »know how« tehnologijo in trpijo udarec ugleda podjetja in njegovih znamk, kar posledično vodi v upadanje zaupanja investitorjev, poslovnih sodelavcev ter celo lastnih zaposlenih.

Pojavljajo se tri vprašanja: (1). Kaj želijo naši tekmeci odkriti o nas in zakaj? (2) Kako nameravajo to storiti? (3) Kakšne protiukrepe imamo pripravljene?
Ko se odgovori na ta vprašanja, se lahko postavljajo okvirji varovanja in izvajanja protiobveščevalne dejavnosti.

Podjetja se dandanes vedno bolj poslužujejo tako imenovane konkurenčne ali korporacijske obveščevalne dejavnosti (competitive or corporate intelligence) o tekmecih, tako si priborijo boljši položaj na trgu. Pri tem lahko uporabljajo legalne/etične ali nelegalne/neetične tehnike zbiranja podatkov. Lahko pa tudi kombinacijo obojega. Problem je, če se podjetja zavejo obveščevalnega napada šele potem, ko je prepozno, ko tekmec npr. že zažene proizvodnjo z izdelki narejenih s pomočjo ukradene tehnologije. Zaradi teh in podobnih groženj morajo korporacije razširiti protiobveščevalne aktivnosti na vseh stopnjah v lastni organizaciji.

Razlikovati je potrebno med ekonomskim vohunjenjem in podjetniško obveščevalno dejavnostjo. Prvo je nelegalna tajna aktivnost, ki je usmerjena v pridobitev občutljivih finančnih, trgovskih ali ekonomskih informacij, kot so lastniške ekonomske informacije ali kritične tehnologije. Zbiranje informacij na legalen in odprt način se

imenuje konkurenčna obveščevalna (competitive intelligence) ali podjetniška obveščevalna dejavnost. To je koordinirana in organizirana dejavnost za zbiranje informacij o tekmecih, dobaviteljih, potrošnikih in specifični industriji z namenom pridobitve konkurenčne prednosti. Poudarek pri slednji je predvsem na legalnem in etičnem zbiranju informacij.

Vse večji pomen dandanes pridobivajo informacijski in na visoki tehnologiji temelječi produkti. Trgovina in intelektualna lastnina[16] prav tako postajata pomemben del svetovne trgovine. Lastniške pravice se vse bolj priznava kot ene najpomembnejših vrednosti podjetja. Informacijska podjetja morajo poleg tehnoloških ščititi tudi svoje finančne in komercialne informacije, ki jim zagotavljajo konkurenčnost pred tekmeci. Da bi se zavedali, kako težko je varovati informacije, si je potrebno pogledati njihove značilnosti. Te so lahko vidne (model, dokument, načrt itd.) ali pa jih zaznamo z vonjem, okusom ter dotikom. Intelektualna lastnina ščiti inovacije človeškega uma. Tu leži resnična moč bogastva in potrebuje posebne tehnike varovanja.

V prvem poglavju sem že omenjal, da ima protiobveščevalna dejavnost dve komponenti, aktivno in pasivno. To pride še bolj do izraza pri podjetniški protiobveščevalni dejavnosti. Pasivna teži k preprečevanju nasprotnikove dejavnosti in vsebuje obrambne in preventivne protiukrepe, kot so poročanja o grožnjah, tehničnimi protiukrepi (TSCM) in testiranje prodora ali penetracije v podjetje. Aktivna se razlikuje od pasivne. Ko je grožnja odkrita, bo aktivna protiobveščevalna dejavnost sprožila preiskavo in operacije za nevtralizacijo kakršnih koli novih groženj. Lahko se jo uporabi kot metodo zbiranja podatkov, kjer moramo, če hočemo izvedeti namere tekmecev, poznati njihove sposobnosti, proračun in resurse.

Za obveščevalne službe postajajo podjetniške in ekonomske tarče veliko bolj pomembnejše kot vojaške in politične. Vsako podjetje, ki posluje v mednarodni areni, je lahko tarča korporativnega vohunjenja. James Woolsey jr. je, ko je bil direktor CIE, izjavil, da je ekonomija postala najbolj vroče področje v obveščevalni dejavnosti. Pierce Marcon, nekdanji šef francoske Generalne direkcije za zunanjo varnost (Direction Generale de la Securite Exterieur) (DGSE), je v intervjuju ameriškemu

[16] Nekateri ju opisujejo kot nove globalne valute.

novinarju povedal, da »so v ekonomiji tekmeci in ne zavezniki«. Ena od nalog Prvega direktorata ruske zunanje obveščevalne službe (SVR) je mednarodna ekonomija. Japonska zunanja trgovinska organizacija (JETRO), ustanovljena leta 1957 za promocijo trgovine pod okriljem japonskega ministrstva za zunanjo trgovino, je po mnenju zahodnih obveščevalnih služb ena najboljših »obveščevalnih služb« na tem področju.

Podjetje mora poznati sebe in svoje tekmece. Določiti mora, katere informacije je potrebno zaščititi, zaznati ranljivosti in določiti časovni obseg varovanja informacij. Podjetje, ki ima samo strogo fizično varovanje, lahko uniči en sam agent, ki prodre v to podjetje. Podjetje je ranljivo, tudi če ima lojalen in vesten kader, a ne skrbi za ustrezno zaščito informacij. Tako samo fizično varovanje podatkov in zaupanja vreden kader še nista dovolj za ustrezno protiobveščevalno obrambo.

Obstaja več metod vohunjenja: nepooblaščen vstop, tajno opazovanje, elektronsko prisluškovanje, analiza »smeti«, vlomi, izsiljevanja, podkupnine, kraje dokumentov in grožnja prodora tujega agenta ali rekrutacije zaposlenih. Slednja, ko zaposleni delajo za konkurenco, velja za najbolj nevarno. Motivi za vohunjenje so lahko materialni, emocionalni in ideološki. Ti so lahko nezadovoljstvo na delovnem mestu, problemi z odvisnostjo, denarne težave ipd. Industrijski vohun bo, da bo našel primerno tarčo, izpeljal operacionalno analizo podjetja in osebja. Tega se osebje navadno ne zaveda. Grožnje se lahko se lahko zmanjšajo z uporabo protiobveščevalnih protiukrepov (Bernhardt 2003: 85–91).

Najbolj očitni znaki, da je podjetje tarča vohunjenja oz. obveščevalne dejavnosti, so naslednji: (1) konkurenca ve za nove projekte, zaupne posle, trgovske skrivnosti in strategije podjetja; (2) pojavljajo se različna poizvedovanja o podjetju in novih projektih s strani tujcev, kot so »študenti, raziskovalci in drugi«; (3) na podjetju se pojavijo tehnični serviserji, ki jih nihče ni poklical; (4) ista konkurenca vedno znova premaga podjetje pri poslovnih pogodbah; (5) v podjetju se odkrijejo prisluškovalno nadzorne naprave; (6) pojavljajo se neprestane želje iz tujine, da bi si ogledali podjetje; (7) konkurenca premaga podjetje na trgu z zelo podobnim produktom; (8) zaupni materiali, informacije in oprema, kot so prenosni računalniki, so ukradeni v sumljivih okoliščinah; (9) ključni kader zapusti podjetje in se zaposli pri konkurenci;

(10) osebje poroča o nadzoru, poskusih rekrutacije ali sumljivih poizvedbah in obnašanju; (11) konkurenca vzpostavlja obveščevalne oddelke; (12) konkurenca zaposluje številne analitike ali vzpostavlja nove enote, ki se ukvarjajo z korporativno strategijo, industrijo in konkurenčno analizo (competitive analysis) (Whitehead, 2003).

7. 1 Študija primerov gospodarske protiobveščevalne dejavnosti

NCIX izdaja vsakoletno poročilo o tujem ekonomskem in industrijskem vohunjenju v ZDA. Najpogostejši cilji so informacijski sistemi, senzorji in laserji, elektronika, aeronavtična tehnologija. Največjo grožnjo na tem področju predstavljajo države kot so Kitajska, Japonska, Izrael, Francija, Koreja, Tajvan ter Indija (IWS - The Information Warfare Site: *Annual Report to Congress on Foreign Economic Collection. and Industrial Espionage 2000*).

Leta 2000 naj bi izguba stroškov zaradi ekonomskega vohunjenja v ZDA znašala od 100 do 250 milijard dolarjev. Največ izgub gre podjetjem, ki se ukvarjajo z razvojem in raziskavami. Istega leta se na seznamu držav, ki opravljajo ekonomska vohunjenja v ZDA, pridružil Pakistan (IWS - The Information Warfare Site: *Annual Report to Congress on Foreign Economic Collection. and Industrial Espionage 2001*). V letu 2001 poročilo opaža porast zanimanja za kritično vojaško tehnologijo, s katero bi tuje države pridobile na lastnih obrambnih zmogljivostih (IWS - The Information Warfare Site: *Annual Report to Congress on Foreign Economic Collection and Industrial Espionage 2002*). Kot leto poprej je bila tudi v letih 2002 in 2003 glavna tarča vohunjenja vojaška tehnologija. Več kot 90 % informacij, ki so bile zaželene, ni bilo zaščitenih z oznako zaupno (IWS - The Information Warfare Site: *Annual Report to Congress on Foreign Economic Collection and Industrial Espionage 2003*).

Leta 2004 naj bi bilo v ZDA v industrijskem in ekonomskem vohunjenju aktivnih okoli 100 držav, podobno kot leto poprej. Poročila navajajo tudi metode in načine tujih akterjev pri pridobivanju zaupnih podatkov in svetujejo pri boljši obrambi pred industrijskim vohunjenjem (IWS - The Information Warfare Site: *Annual Report to Congress on Foreign Economic Collection and Industrial Espionage 2004*).

Francoska vlada je leta obtožila Združene države Amerike, da uporabljajo nadzorno-komunikacijski sistem Echelon, ki je bil vzpostavljen med Hladno vojno za vohunjenje proti francoskim podjetjem. Echelon nadzorno mrežo, ki lahko prisluškuje telefonskim pogovorom, faksom in elektronskim sporočilom po vsem svetu, zdaj ZDA menda uporabljajo za nadzor komercialnih tekmecev. Pri tem procesu naj bi sodelovali tako ZDA kot Velika Britanija, Nova Zelandija, Kanada in Avstralija. Informacije, zbrane s pomočjo Echelona, naj bi pripomogle k izgubi posla francoskega podjetja Thomson na področju radarjev v Braziliji ter s tem izgubi šest milijard vrednega posla za evropski Airbus konzorcij proti ameriškem Boeingu. Prej naštete države so kakršno koli gospodarsko vohunjenje zanikale (BBC Online 2000a).

Leta 2000 so hekerji vdrli v Microsoftov računalniški sistem in morda pridobili dostop do izvorne kode njihovih programov. Dostop do teh podatkov naj bi imeli tri mesece in bil lahko ukradli blueprinte Windowsov in Office programov. V Microsoftu so povedali, da gre za dejanje industrijskega vohunjenja in da bodo naredili vse, kar je v njihovi moči, da zaščitijo lastno intelektualno lastnino. Do zdaj sicer še ni bilo nobenih dokazov, da bi bil kateri Microsoftov program prenovljen ali uničen. Wall Street Journal je poročal, da naj bi varnostni uslužbenci odkrili, da je bila izvorna koda poslana iz računalnišega omrežja v Redmondu v Washingtonu na elektronski naslov v St. Petersburg v Rusiji (BBC Online 2000b).

Računalniški strokovnjaki so sporočili, da naj bi hekerji pri tem uporabili virus imenovan Qaz. Slednji naj bi se prvič pojavil na Kitajskem in je tako imenovani črv, ki dela dvojnike samega sebe in se s tem širi po omrežju. Ko je enkrat nameščen, omogoča nepooblaščen dostop do omrežij. Najverjetneje je virus vstopil v Microsoftov sistem kot navadna elektronska pošta, potem pa se je začel množiti. To so tako imenovani trojani, imenovani po trojanskem konju iz grške mitologije (BBC Online 2000c).

V ZDA so kraje in predaje skrivnosti kitajskemu podjetju obtožili znanstvenika in poslovneža podjetja Lucent. Dva pripadnika kitajske nacionalnosti in en državljan ZDA so bili leta 2001 aretirani s strani FBI in obtoženi korporacijskega vohunjenja. Možje so domnevno želeli ukrasti glasovne in data software ter jih predati podjetju

Datang Telecom Technology, ki je v lasti kitajskih oblasti. Ameriške oblasti so priznale, da nimajo dokazov o kršitvah omenjenega kitajskega podjetja (BBC Online 2001a).

Eden večjih strahov industrijskega vohunjenja postajajo mobilni telefoni oz. v njih vgrajene kamere. Popularnost telefonov s kamerami, kjer lahko v trenutku posnamemo sliko in jo pošljemo naprej, je povzročila strah za varnost v delovnem okolju. Večina podjetij ne dopušča več nošenja in rabe mobilnih telefonov v njihovih zgradbah in kapacitetah ali vsaj skušajo omejiti njihovo uporabo (Lane 2004).

Korporacijsko vohunjenje se dogaja tudi v kozmetičnih panogah. Procter & Gamble, vodilni proizvajalec v kozmetiki za lase, je priznal vohunjenje za svojim najbližjim tekmecem, Unileverjem. Da bi pridobil skrivnosti lepih las, naj bi preiskovali smeti Unileverja. Za ta namen naj bi najeli zasebne detektive. Da bi pridobili še več informacij, naj bi najemal ljudi, ki bi se predstavljali kot tržni analitiki in tako pridobivali nove informacije. Vir blizu pogajanj med podjetjema govori o mreži sodelavcev in agentov, ki so pridobivali podatke iz konkurenčnega podjetja. Korporacijsko vohunjenje, ki zajema vse od prisluškovanja, računalniškega vdiranja, brskanja po smeteh ipd., je po mnenju ameriških raziskovalcev iz skupine Fotures vedno bolj razširjeno. Raziskava omenjene skupine pravi, da naj bi 60 % podjetij imelo organiziran sistem zbiranja informacij o tekmecih. 82 % podjetij, katerih dohodki so višji od 10 milijard, sistematsko uporablja takšen sistem (BBC Online 2001b).

Še nekaj primerov industrijskega vohunjenja v zadnjem času. Lockheed Martin, mogočna letalska korporacija, je v letu 2003 obtožila svojega tekmeca Boeing vohunjenja v tekmi za posel z US Air Force. Podjetje Locheed Martin je trdilo, da je Boeing pridobil na tisoče zaupnih dokumentov, ki se nanašajo na ponudbo za 2 milijardni vojaški raketni program v letu 1998. Zaradi tega naj bi Pentagon prepovedal sodelovanje Boeingu na raketnem vojaškem programu. Prepoved so ukinili šele leta 2005, ko sta podjetji sklenili premirje in sodelovanje.

Leta 2002 je zaradi obtožb vohunjenja nad švedskim telekomunikacijskim in obrambnim velikanom Ericssonom izbruhnil diplomatski prepir med Švedsko in Rusijo. Švedska je izgnala dva ruska diplomata, potem ko je švedska policija aretirala

tri osebe med predajo zaupnih informacij podjetja kontaktom v Rusiji. Moskva je pozneje, kot odgovor na to dejanje, izgnala dva švedska diplomata. Čeprav je Ericsson znan po svoji mobilni tehnologiji, je bil tudi ključni proizvajalec napredne tehnologije pri anglo-švedskem vojaškem letalu Gripen. Manjkajoči dokumenti pa vendar niso bili povezani s slednjim projektom (BBC Online 2005).

Moderna, predvsem informacijska tehnologija, omogoča nove razsežnosti vohunjenja. Poleg virusov in črvov je postal spyware še ena nova moteča točka za podjetja. Problem je, da se podjetja teh napadov sploh ne zavedajo. Zaradi svojega potenciala za vzajemno vohunjenje, predstavlja spyware večjo varnostno grožnjo, kot se sploh zavedamo.

Dober primer kraje poslovnih informacij je primer izraelskega avtorja Amnom Jackonta, ki je dele svoje še ne napisane knjige našel na internetu. In ker Jackont ni delil svojega dela z nikomer, je poklical policijo, na kar so pozneje izvedeli, da je bilo njegovo delo ukradeno s strani nekdanjega zeta, ki je pri tem uporabljal trojanskega konja z imenom »Rona«.

Nadaljnje preiskave, ki so sledile po državi na podlagi prej omenjenega vira, so pokazale še druge okužene računalnike in podjetja. Žrtve so bili vsi od vodilnih delavcev v telekomunikacijskem podjetju države do Hewlet-Packarda. Ta incident je sprožil aretacije skoraj dvajsetih oseb, ukradenih naj bi bilo od sto do tisoč dokumentov iz različnih izraelskih firm. Zaseženih je bilo preko sto strežnikov, na katerih so se nahajali ukradeni podatki.

Podjetja se v veliko primerih sploh ne zavedajo, da so objekt vohunjenja s pomočjo Spywara, druga podjetja, ki zaznajo te aktivnosti, o tem ne želijo govoriti. Vendar obstajajo nekatera poročila, ki opisujejo podobne incidente. Webroot Software je leta 2004 objavilo, da so nekatere banke v New Yorku tarča programa, ki je bil narejen, da pridobi geslo in okuži samo specifične finančne institucije. Istega leta je podjetje MessageLabs odkrilo trojanskega konja, ki je bil ustvarjen z namenom, da napada določene dele programa, ki se ga uporablja za izdelavo letal.

Čeprav so poročila o teh incidentih za enkrat redka, to še ne pomeni, da se to ne dogaja v večjem številu podjetji. Napadalci so postali dovolj zviti in poučeni, da so si izmislili nove načine za uporabo keylogger programov, ki zapisujejo udarce po tipkovnici na računalniku žrtve. Programi se lahko uporabljajo za pridobitev gesel, branje elektronske pošte ali pa enostavno za sledenje delu uporabnikov.

Pisci Spywara lahko uporabljajo trojanske konje, da pridobijo dostop do računalnikov z razdalje in izvršijo kodo, ki jim omogoča iskanje informacij na določenem disku ali znotraj omrežja.

Čeprav se programe, kot je Spyware, da odkriti z določenimi antispyware programi, je težje ugotoviti, ali je šlo za korporacijsko vohunjenje ali ne. Edini razlog, da so odkrili trojana v Izraelu, je bila posledica srečnih naključij. Napadalci so se naučili, kako premagati skenerje, ki se jih uporablja pri odkrivanju spywara, kar povzroča še težje vzdrževanje varnosti v podjetjih. Klasično industrijsko vohunjenje se je premaknilo na omrežja, kjer namesto brskanja po koših tovarn, vohuni brskajo po koših operacijskih sistemov in programov podjetij (Millard 2005).

Vsi ti primeri kažejo na dejstvo, da obveščevalna dejavnost in vohunjenje nista samo domena države, temveč tudi nedržavnih subjektov, kot so podjetja. Število podobnih primerov se vse bolj veča, kar posledično pripelje do potrebe po večji varnosti in protiobveščevalni zaščiti pred tekmeci.

8. ZAKLJUČEK

Moj prva hipoteza se je glasila: »*Protiobveščevalna dejavnost se lahko izvaja v eni službi in je lahko razpršena med več različnih obveščevalno varnostnih služ*b«. To hipotezo lahko po študiji petih držav potrdim. Protiobveščevalna dejavnost ni domena samo protiobveščevalnih služb, temveč tudi drugih obveščevalno-varnostnih, saj se vse soočajo z grožnjami prodora v lastne vrste s strani tujih služb. Dokazi za to so obveščevalne službe, ki vsebujejo oddelke za protiobveščevalno dejavnost. Te so npr. CIA v ZDA in MI6 v Veliki Britaniji. V zvezni republiki Nemčiji poleg Zvezne službe za zaščito ustavne ureditve opravljajo protiobveščevalno delo tudi Zvezna obveščevalna služba BND in Vojaška protiobveščevalna služba MAD.

Druga hipoteza se je glasila: »Metode dela protiobveščevalne dejavnosti se ne razlikujejo od metod dela varnostnih in obveščevalnih služb«. Te hipoteze ne morem popolnoma sprejeti, niti je ne morem ovreči. Protiobveščevalna služba se lahko poslužuje metod obveščevalnih služb, kot je pridobivanje informacij, in varnostnih služb, kot je zaščita informacij. Kakšne metode ima protiobveščevalna služba je odvisnost od pravne ureditve po posameznih državah. V nekaterih državah imajo protiobveščevalne službe možnost aretacije, v drugih pri tem sodelujejo s policijo.

Pri pisanju naloge sem ugotovil, da lahko protiobveščevalno delo razdelimo na pasivni in aktivni del. Prvi je mišljen kot zaščita informacij, drugi pa kot aktivno delovanje v smeri dezinformiranja in nagajanja nasprotniku. Pri tem uporabljajo specifične metode, kot so dvojni agentje, krti ipd. Poudariti je potrebno, da se protiobveščevalne, obveščevalne in varnostne službe poslužujejo podobnih metod, kadar se ukvarjajo s podobno dejavnostjo. Ime službe še ne pomeni, da se služba ukvarja strogo s svojo dejavnostjo. Tako obveščevalne kot varnostne službe lahko uporabljajo protiobveščevalne metode dela v svojem delovanju.

Tretja hipotezo: »Gospodarska protiobveščevalna dejavnost dobiva vedno večji pomen v sodobnem globalnem svetu korporacij« lahko potrdim, ker so nove tarče obveščevalne dejavnosti v sodobnem svetu ravno gospodarski subjekti in se kot taki vedno bolj ščitijo pred izgubo informacij. Naraščanje primerov vohunjenja v podjetjih

in rast zasebnih varnostnih služb nakazujeta na povečevanje tega trenda. Dokaz za to so vsakoletna poročila NCIX o tujem ekonomskem in industrijskem vohunjenju v ZDA, kjer se opaža povečano vohunjenje v ameriških podjetij. Do natančnih podatkov o vohunjenju v korporacijah po svetu je težko priti, ker želijo podjetja kakršnekoli incidente prikriti, da bi s tem ohranile ugled organizacije.

Zaščita skrivnosti, informacij bo vedno ostala pomembna dejavnost za politične, vojaške in ekonomske organizacije. Zato lahko iz navedenega sklepam, da protiobveščevalna dejavnost kljub večji pozornosti protiterorističnem delovanju v sodobnem svetu ne izgublja na pomenu. Vse pomembnejše področje delovanja protiobveščevalne dejavnosti postaja gospodarstvo. Poudariti je potrebno, da protiobveščevalna dejavnost sama po sebi ne obstaja brez obveščevalne. Kamor se selijo interesi obveščevalnih služb, tja se seli tudi protiobveščevalna dejavnost.

Skozi nalogo sem tudi spoznal, da je težko postaviti ločnice med posameznimi pojmi, kot so protiobveščevalna, obveščevalna in varnostna dejavnost. Vse spada pod sklop obveščevalno varnostne dejavnosti. Organizacija, ki opravlja obveščevalno varnostno dejavnost, hkrati uporablja obveščevalno aktivnost, kjer išče podatke, protiobveščevalno aktivnost, s tem mislim predvsem na zaščito pred obveščevalno dejavnostjo drugih organizacij, in varnostno aktivnost, ki pomeni represivni element celotne dejavnosti.

Pomembno se je zavedati, da se ne more določene službe enačiti z določeno dejavnostjo. Poznamo več vrst služb, ki se ukvarjajo z obveščevalno varnostno dejavnostjo. Avtorji jih postavljajo v predale po svojih kriterijih. Sam menim, da lahko službe delimo predvsem glede na cilj oz. objekt delovanja. Obveščevalne službe so najsplošnejši pojem in lahko predstavljajo kakršnokoli organizacijo, ki jo zanimajo informacije, podatki. Protiobveščevalne službe zanimajo tuje obveščevalne službe, protiteroristične službe se ukvarjajo s terorističnimi organizacijami, policija in kriminalistične službe se ukvarjajo s kriminalom in kriminalnimi združbami. Pri tem je treba poudariti, da vse te službe uporabljajo obveščevalno, protiobveščevalno in varnostno dejavnost.

Iz danega sklepam, da protiobveščevalna dejavnost ni področje ene same službe, temveč del delovanja vseh obveščevalno varnostnih služb. Tako uporabljajo protiteroristične enote protiobveščevalno dejavnost pred prodorom agentov terorističnih skupin v lastne vrste. Prav tako se protiobveščevalne dejavnosti poslužuje policija v boju proti organiziranem kriminalu, ki želi imeti svoje ovaduhe v policijskih vrstah in obratno.

V diplomskem delu sem opisal funkcije delovanja protiobveščevalne dejavnosti. Najbolj logična se mi zdi delitev na pasivni in aktivni del. Pasivni je varovanje pred prodorom agentov v lastne vrste, aktivni pa so operacije, s katerimi se želi vplivati na vedenje in delovanje nasprotnika. Obe funkciji lahko zaznamo v vseh obveščevalno varnostnih službah.

Kot sem že omenil se službe ločujejo glede na cilj in objekt obravnave. V sodobnem svetu, času globalizacije se objekti zanimanja prestavljajo na ekonomsko območje. Tudi same obveščevalno varnostne službe so spoznale svojo novo vlogo in se tem primerno odzivajo. Podjetja uporabljajo obveščevalno varnostne metode pri doseganju svojih ciljev. Iščejo informacije, se ščitijo pred tujim zanimanjem podjetij, varujejo lastne informacije, osebje itd.

V svoji diplomski nalogi želim poudariti, naj se ne ločuje posameznih obveščevalno varnostnih dejavnosti, ker so dejansko sestavni deli posamezne organizacije in so med sabo tako prepletene, da bi ločitev pomenila nazadovanje in celo nevtralizacijo funkcionalnosti same obveščevalno varnostne organizacije. Pri tem se moramo zavedati, da je slednja pomemben del širše entitete in lahko s tem ogrozi obstoj celotne širše organizacije, kot so podjetja, države, skupnosti itd.

9. VIRI

Knjige:

1. Anžič, Andrej (1997): *Varnostni sistem Republike Slovenije.* Ljubljana: Uradni list Republike Slovenije.
2. Bernhardt, Douglas (2003): *Competitive Intelligence, Acquiring and using strategic intelligence and counterintelligence*. Financial Times, Prentice Hall.
3. Đorđević, Obren Ž. (1980): *Osnovi državne bezbednosti: opšti deo*. Beograd: Viša škola unutrašnjih poslova.
4. Field Manual 34-60 (1995): *Counterintelligence.* Washington, D.C.: Department of the Army.
5. Furan, Branimir in Marjan Mahnič (1996): *Začasni ANGLEŠKO-SLOVENSKI VOJAŠKI PRIROČNI SLOVAR*. Ljubljana: Uprava za razvoj MORS.
6. Gažević, Nikola, ur. (1970): *Vojna enciklopedija*. Beograd: Redakcija vojne enciklopedije.
7. Godson, Roy (1995): *Dirty tricks or trump cards: U.S. covert action and counterintelligence*. Washington, London: Brassey's.
8. Joint Publication 1-02 (2006): *Dictionary of Military and Associated Terms*. Department of Defense, Joint Chief of State.
9. Lerner, K. Lee in Brenda L. Wilmoth, ur. (2004): Encyclopedia of Espionage, Intelligence, and Security. Thomson Gale Encyclopedia.
10. Mortimer, Adler J., ur. (2005): *The New Encyclopedia Britannica Vol 21*. Chicago: Encyclopaedia Britannica.
11. Pogačnik, Aleš in Klemen Podobnik, ur. (2006): *Veliki splošni leksikon*. DZS: Ljubljana.
12. Požun, Janko (2004): *Obveščevalno-varnostni sistem Izraela*. Ljubljana: FDV.
13. Purg, Adam (1995): *Obveščevalne službe: povezave med obveščevalnimi službami in državno suverenostjo v luči iskanja modela sodobnega obveščevalnega sistema Republike Slovenije*. Ljubljana: Enotnost.
14. Richelson, Jeffrey (1999): The U.S. intelligence community, Boulder (Colo.): Westview Press.
15. Sun, Cu (1996): *Umetnost vojne.* Ljubljana: Amalietti.
16. Šaponja, Vladimir (1999): *Taktika dela obveščevalnovarnostnih služb*. Ljubljana: Visoka policijsko-varnostna šola.

17. Žaberl, Miroslav (2006): Temelji policijskih pooblastil. Ljubljana: Fakulteta za policijsko-varnostne vede.

Dokumenti:

18. BfV Bericht (2001): *Bundesamtes für Verfassungsschutz: Verfassungschutzbericht*. Dostopno na http://www.verfassungsschutz.de/de/publikationen/verfassungsschutzbericht/vsbericht_2001/ (22. december 2006).
19. BfV Bericht (2002): *Bundesamtes für Verfassungsschutz: Verfassungschutzbericht*. Dostopno na http://www.verfassungsschutz.de/de/publikationen/verfassungsschutzbericht/vsbericht_2002/ (22. december 2006).
20. BfV Bericht (2003): *Bundesamtes für Verfassungsschutz: Verfassungschutzbericht.* Dostopno na http://www.verfassungsschutz.de/de/publikationen/verfassungsschutzbericht/vsbericht_2003/ (22. december 2006).
21. BfV Bericht (2004): *Bundesamtes für Verfassungsschutz: Verfassungschutzbericht.* Dostopno na http://www.verfassungsschutz.de/de/publikationen/verfassungsschutzbericht/vsbericht_2004/ (22. december 2006).
22. BfV Bericht (2005): *Bundesamtes für Verfassungsschutz: Verfassungschutzbericht.* Dostopno na http://www.verfassungsschutz.de/de/publikationen/verfassungsschutzbericht/vsbericht_2005/ (22. december 2006).
23. DCAF (2004): Geneva Centre for the Democratic Control of Armed Forces: *Fact Sheet For The Meeting of the PFP Consortium Security Sector Reform Working Group*. Dostopno na http://www.dcaf.ch/pfpc/ev_stockholm_040325_fs_law3.pdf (24. november 2006).
24. Executive order 12333 (1981). Dostopno na http://www.hanford.gov/oci/maindocs/ci_r_docs/eo12333.pdf (3. april 2006)
25. GPOaccess.gov (2005): *Report of the Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction,*

Chapter 11: Counterintelligence. Dostopno na http://www.gpoaccess.gov/wmd/pdf/chapter11_fm.pdf (5. junij 2006).

26. ISC (2000): *Intelligence and Security Committee, Annual Report 1999-2000*. Dostopno na http://www.archive.officialdocuments.co.uk/document/cm48/4897/4897-02.htm#gen79 (13. januar 2007).
27. ISC (2001): *Intelligence and Security Committee, Interim Report 2000-01.* Dostopno na http://www.archive.officialdocuments.co.uk/document/cm51/5126/5126.pdf (13. januar 2007).
28. ISC (2002): *Intelligence and Security Committee, Annual Report 2001-2002.* Dostopno na http://www.cabinetoffice.gov.uk/publications/reports/intelligence/Intelligence.pdf (13. januar 2007).
29. ISC (2003*): Intelligence and Security Committee Annual Report 2002-2003.* Dostopno na http://www.cabinetoffice.gov.uk/publications/reports/intelligence/annualir0203.pdf (13. januar 2007).
30. ISC (2004): *Intelligence and Security Committee Annual Report 2003-2004*. Dostopno na http://www.cabinetoffice.gov.uk/publications/reports/intelligence/annualir0304.pdf, (13. januar 2007).
31. ISC (2005): *Intelligence and Security Committee, Annual Report 2004-2005.* Dostopno na www.cabinetoffice.gov.uk/publications/reports/intelligence/iscannualreport.pdf (13. januar 2007).
32. IWS - The Information Warfare Site: *Annual Report to Congress on Foreign Economic Collection and Industrial Espionage (2000).* Dostopno na http://www.iwar.org.uk/ecoespionage/resources/senate/annual-reports/industrial-espionage-00.htm (14. januar 2007).
33. IWS - The Information Warfare Site: *Annual Report to Congress on Foreign Economic Collection and Industrial Espionage (2001).* Dostopno na http://www.iwar.org.uk/ecoespionage/resources/senate/annual-reports/industrial-espionage-01.htm (14. januar 2007).
34. IWS - The Information Warfare Site*: Annual Report to Congress on Foreign Economic Collection and Industrial Espionage (2002)*. Dostopno na http://www.iwar.org.uk/ecoespionage/resources/senate/annual-reports/industrial-espionage-02.htm (14. januar 2007).
35. IWS - The Information Warfare Site: *Annual Report to Congress on Foreign Economic Collection and Industrial Espionage (2004)*. Dostopno na

http://www.iwar.org.uk/ecoespionage/resources/senate/annual-reports/industrial-espionage-04.htm (14. januar 2007).

36. IWS - The Information Warfare Site: *Annual Report to Congress on Foreign Economic Collection. and Industrial Espionage (2003).* Dostopno na http://www.iwar.org.uk/ecoespionage/resources/senate/annual-reports/industrial-espionage-03.htm (14. januar 2007).

Članki:

37. Agentura.ru: *For espionage on CIA military scout is condemned*. Dostopno na http://www.translate.ru/url/tran_url.asp?lang=ru&direction=re&template=General&cp1=CP1251&cp2=NO&autotranslate=on&transliterate=on&url=http%3A%2F%2Fwww.agentura.ru%2Ftimeline%2F2002%2Fsypachev%2F (11. november 2007).

38. Agentura.ru: *FSB: turkish special services are involved in capture of plane TU-154.* Dostopno na http://www.translate.ru/url/tran_url.asp?lang=ru&direction=re&template=General&cp1=CP1251&cp2=NO&autotranslate=on&transliterate=on&url=http%3A%2F%2Fwww.agentura.ru%2Ftimeline%2F2001%2Fsamolet%2F (10. januar 2007).

39. Agentura.ru: *On Stavropole have caught two turkish spies*. Dostopno na http://www.translate.ru/url/tran_url.asp?lang=ru&direction=re&template=General&cp1=CP1251&cp2=NO&autotranslate=on&transliterate=on&url=http%3A%2F%2Fwww.agentura.ru%2Ftimeline%2F2001%2Ftur%2F (10. januar 2007).

40. Agentura.ru: *The military attache of Lithuania is sent from Moscow*. Dostopno na http://www.translate.ru/url/tran_url.asp?lang=ru&direction=re&template=General&cp1=CP1251&cp2=NO&autotranslate=on&transliterate=on&url=http%3A%2F%2Fwww.agentura.ru%2Ftimeline%2F2004%2Flitvaattache%2F, (11. januar 2007).

41. Agentura.ru: *The scout Zaporozhye is condemned for espionage in favour of the USA*. Dostopno na http://www.translate.ru/url/tran_url.asp?lang=ru&direction=re&template=General&cp1=CP1251&cp2=NO&autotranslate=on&transliterate=on&url=http%3A%2F%2Fwww.agentura.ru%2Ftimeline%2F2003%2Fzaporojsky%2F (11. januar 2007).

42. Agentura.ru: *The third secretary of embassy of teh USA is caught on recruitment of the scientist.* Dostopno na

http://www.translate.ru/url/tran_url.asp?lang=ru&direction=re&template=General&cp1=CP1251&cp2=NO&autotranslate=on&transliterate=on&url=http%3A%2F%2Fwww.agentura.ru%2Ftimeline%2F2002%2Fsavant%2F (11. januar 2007).

43. Agentura.ru: *Victor Kalyadin is condemned for espionage*. Dostopno na http://www.translate.ru/url/tran_url.asp?lang=ru&direction=re&template=General&cp1=CP1251&cp2=NO&autotranslate=on&transliterate=on&url=http%3A%2F%2Fwww.agentura.ru%2Ftimeline%2F2001%2Fkalyadin%2F, (10. januar 2007).
44. BBC Online (2000): *Mobile giant plays down MI5 probe.* Dostopno na http://news.bbc.co.uk/2/hi/business/952908.stm (11. junij 2006).
45. BBC online (2000a): *France accuses US of spying*. Dostopno na http://news.bbc.co.uk/2/hi/654210.stm (25. december 2006).
46. BBC online (2000b): *Hackers hit Microsoft*. Dostopno na http://news.bbc.co.uk/2/hi/business/993826.stm (25. december 2006).
47. BBC online (2000c): *Microsoft software stolen*. Dostopno na http://news.bbc.co.uk/2/hi/business/993933.stm (25. december 2006).
48. BBC Online (2001): *Guard admits stealing secrets*. Dostopno na http://news.bbc.co.uk/2/hi/uk_news/1715497.stm (15. julij 2006).
49. BBC online (2001a): *Lucent scientists charged*. Dostopno na http://news.bbc.co.uk/2/hi/business/1311711.stm (25. december 2006).
50. BBC online (2001b): *Shampoo giant caught spying.* Dostopno na http://news.bbc.co.uk/2/hi/business/1518901.stm (25. december 2006).
51. BBC Online (2002): *Plane engineer admits spying*. Dostopno na http://news.bbc.co.uk/2/hi/uk_news/england/2528207.stm (15. julij 2006).
52. BBC Online (2004): *Terror fight diverts spy effort*. Dostopno na http://news.bbc.co.uk/2/hi/uk_news/politics/3849803.stm (11. junij 2006).
53. BBC online, (2005): *Secret world of industrial espionage.* Dostopno na http://news.bbc.co.uk/2/hi/business/4595745.stm (25. december 2006).
54. Israelinsider (2005): *Trojangate: Top Israeli execs arrested for using virus to spy on each other*. Dostopno na http://web.israelinsider.com/Articles/Briefs/5702.htm (11. junij 2006).
55. Israelinsider.com (2004): *Tannenbaum affair "one of worst ever in Israel's history"*. Dostopno na

http://web.israelinsider.com/bin/en.jsp?enPage=ArticlePage&enDisplay=view&enDispWhat=object&enDispWho=Article%5El3330&enZone=Security&enVersion=0& (11. junij 2006).

56. IsraelNN.com (2002): *Partial Lifting of Gag Order on Spy Case*. Dostopno na http://www.israelnationalnews.com/news.php3?id=25875 (11. junij 2006).
57. IsraelNN.com (2002a): *Israeli Charged in Spying for Hezbollah.* Dostopno na http://www.israelnationalnews.com/news.php3?id=25895 (11. junij 2006).
58. IsraelNN.com (2002b): *IDF Officer Remanded on Suspicion of Spying*. Dostopno na http://www.israelnationalnews.com/news.php3?id=32339 (11. junij 2006).
59. IsraelNN.com (2002c): *Beit Safafa Suspect Was Romantically Involved With Suspects.* Dostopno na http://www.israelnationalnews.com/news.php3?id=29765 (11. junij 2006).
60. IsraelNN.com (2002d): *Two Israeli-Arabs Charged With Spying for PA*. Dostopno na http://www.israelnationalnews.com/news.php3?id=29398 (11. junij 2006).
61. IsraelNN.com (2003): *Spying for drugs*. Dostopno na http://www.israelnationalnews.com/news.php3?id=39057 (11. junij 2006).
62. IsraelNN.com (2004): *Israeli Arab Caught Spying For Iran*. Dostopno na http://www.israelnationalnews.com/news.php3?id=73214 (11. junij 2006).
63. IsraelNN.com (2004a): *Intelligence Report: Hizbullah Active in Israel for Four Years*. Dostopno na http://www.israelnationalnews.com/news.php3?id=73272 (11. junij 2006).
64. Khilafah.com (2001): *Taliban defector was a CIS informant for years*. Dostopno na http://prisonplanet.com/taliban_defector_was_cia_informant_for_years.html (2. junij 2006).
65. Kroeger, Alix (2002): *Bosnian Serbs 'eavesdrop on Nato*. Dostopno na http://news.bbc.co.uk/2/hi/europe/2004989.stm (2. junij 2006).
66. Lane, Megan (2004): *The camera phone backlash.* Dostopno na: http://news.bbc.co.uk/2/hi/uk_news/magazine/3793501.stm (25. december 2006).
67. Millard, Elizabeth (2005): *Spyware as Corporate Espionage Threat*. Dostopno na http://www.newsfactor.com/story.xhtml?story_id=103000029V6L, (23. januar 2007).

68. Rohozinska Joanna: *Central Europe Review: Last Week in Poland*. Dostopno na : http://www.ce-review.org/00/4/polandnews4.html (2. 6. 2006).
69. Soldatov, Andrei (2004): *FSB Reform: Changes Are Few and Far between*. Dostopno na http://english.mn.ru/english/issue.php?2004-38-1 (10. januar 2007).
70. Stopar, Mirko (2002): *Obveščevalno varnostna dejavnost v 21. stoletju – novi izzivi in priložnosti.* Dnevi Varstvoslovja. Ljubljana: Visoka policijsko-varnostna šola.
71. Strategypage (2004): *From the Independent, via todays' Drudge Report: Russian Spying in Great Britain back to Cold War Levels*. Dostopno na http://www.strategypage.com/messageboards/messages/47-1684.asp (11. junij 2006).
72. Whitehead, Steve (2003): *Corporate counterintelligence – protecting business information*. Dostopno na http://securitysa.com/regular.aspx?pklRegularId=1366&pklIssueId=589, (25. december 2006).

Ostali Internetni viri:

73. Agentura.ru: *Federal security service (FSB).* Dostopno na http://www.agentura.ru/english/dosie/fsb/ (10. januar 2007).
74. Agentura.ru: *Special Services of Russia*. Dostopno na http://www.agentura.ru/english/dosie/ (10. januar 2007).
75. Agentura.ru: *SVR Foreign Intelligence Service*. Dostopno na http://www.agentura.ru/english/dosie/svr/ (10. januar 2007).
76. Agentura.ru: *SVR structure*. Dostopno na http://www.agentura.ru/english/dosie/svr/structure/ (10. januar 2007)
77. Center za Protiobveščevalna in Varnostna vprašanja. Dostopno na www.cicenter.com (20. junij 2006).
78. CIA.gov: *CIA Today: What do we do*. Dostopno na http://www.cia.gov/cia/publications/cia_today/ciatoday_03.shtml (5. junij 2006).
79. CIA.gov: *Counterintelligence for National Security*. Dostopno na https://www.cia.gov/csi/kent_csi/docs/v02i4a10p_0001.htm (11. 11. 2006).

80. Defence Security Service: *Espionage Cases 1975 -2004*. Dostopno na http://www.dss.mil/training/espionage/REC.pdf (3. junij 2006).
81. FBI.gov: *Counterintelligence*. Dostopno na http://www.fbi.gov/libref/factsfigure/counterintell.htm (5. junij 2006)
82. Gleghorn E. Todd (2003): *Exposing The Seams: The Impetus For Reforming U.S. CounterintelligenceE*. Monterey, California: Naval Postgraduate School. Dostopno na http://www.ccc.nps.navy.mil/research/theses/gleghorn03.pdf (21. junij 2006).
83. MCWP (2000): *Counterintelligence, U.S. Marine Corps.* Dostopno na: http://www.fas.org/irp/doddir/usmc/mcwp2-14.pdf (23. november 2006).
84. National Intelligence Machinery (2000): *The Stationary Office*. Dostopno na http://www.archive.officialdocuments.co.uk/document/caboff/nim/0114301808.pdf (10. junij 2006).
85. NCIX.gov: *National Counterintelligence (CI) Policy Board*. Dostopno na http://www.ncix.gov/about/NatlCIPolicyBoardDesc.pdf (4. junij 2006).
86. NCIX.gov: *Office of the National Counterintelligence Executive, Description*. Dostopno na: http://www.ncix.gov/about/ONCIXDescription.pdf (4. junij 2006).
87. NCIX.gov: *Office of the National Counterintelligence Executive*. Dostopno na http://www.ncix.gov/about/index.html (4. junij 2006).
88. SSKJ (2000): Slovar slovenskega knjižnega jezika. Dostopno na: http://bos.zrc-sazu.si/sskj.html (20. junij 2006).
89. The Assassination Archives and Research Center*: X. CIA COUNTERINTELLIGENCE: A Counterintelligence: An Introduction*. Dostopno na http://www.aarclibrary.org/publib/church/reports/book1/pdf/ChurchB1_9_Counterintel.pdf (1. julij 2006).
90. The Department of Defense (2006): *Dictionary of Military and Associated Terms*. Joint Publication 1-02. Dostopno na http://www.fas.org/irp/doddir/dod/jp1_02.pdf (15. marec 2007).
91. U.S. Department of Justice (2006): *Four Owners/Operators of Mount Laurel Company Sentenced for Illegally Selling National-Security Sensitive Items to Chinese Interests.* Dostopno na http://newark.fbi.gov/dojpressrel/2006/nk050106.htm (23. oktober 2006).
92. U.S. Department of Justice (2006a): *Central Indiana Man Sentenced For Working With Former Iraqi Intelligence Officers.* Dostopno na

http://indianapolis.fbi.gov/dojpressrel/ pressrel06/intelligence052606.pdf (23. oktober 2006).

93. U.S. Department of Justice (2006b): *News release*. Dostopno na http://www.usdoj.gov/usao/vae/Pressreleases/01-JanuaryPDFArchive/06/20060120franklinnr.pdf (23. oktober 2006).
94. Urad za varovanje tajnih podatkov RS: *Delovna področja*. Dostopno na http://www.uvtp.gov.si/index.php?id=374 (2. junij 2006).
95. Uradna spletna stran BfV: *Arbeitsfelder*. Dostopno na http://www.verfassungsschutz.de/de/arbeitsfelder/ (5. junij 2006).
96. Uradna spletna stran Bundesnachrichten dienst: *Abteilung 8 - Sicherheit, Geheimschutz und Spionageabwehr*. Dostopno na http://www.bnd.bund.de/nn_354670/DE/Wir__Ueber__Uns/Struktur/Abteilung8/Abteilung8__node.html__nnn=true (5. junij 2006).
97. Uradna spletna stran Bundesnachrichten dienst: *Die Nachrichtendienste der Bundesrepublik Deutschland*. Dostopno na http://www.bnd.bund.de/nn_355342/DE/Unser__Auftrag/Zusammenarbeit/Zusammenarbeit__node.html__nnn=true (5. junij 2006).
98. Uradna spletna stran Bundeswehr: *MAD.* Dostopno na http://www.bundeswehr.de/portal/a/bwde/streitkraefte/streitkraeftebasis/mad, (5. junij 2006).
99. Uradna stran MI5: *Espionage*. Dostopno na http://www.mi5.gov.uk/output/Page11.html (10. junij 2006).
100. Uradna stran MI5: *Our major areas of work*. Dostopno na http://www.mi5.gov.uk/output/Page19.html (10. junij 2006).
101. Uradna stran MI5: *Role &Organisation*. Dostopno na http://www.mi5.gov.uk/output/Page18.html (10. junij 2006).
102. Uradna stran Secret Intelligence Service: *About us*. dostopno na http://www.sis.gov.uk/output/Page2.html, (10. junij 2006).
103. US Intelligence Community: *Definiton of the Intelligence Community.* Dostopno na http://www.intelligence.gov/1-definition.shtml (5. junij 2006).
104. US Intelligence Community: *Members of the Intelligence Community*. Dostopno na http://www.intelligence.gov/1-members.shtml, (5. junij 2006).