UNIVERZA V LJUBLJANI
FAKULTETA ZA DRUŽBENE VEDE

Dejan Ulcej

PRIVATIZACIJA OBVEŠČEVALNE DEJAVNOSTI

Diplomsko delo

Ljubljana, 2008

UNIVERZA V LJUBLJANI
FAKULTETA ZA DRUŽBENE VEDE

Dejan Ulcej

Mentor: asist. dr. Uroš Svete
Somentor: asist. mag. Erik Kopač

PRIVATIZACIJA OBVEŠČEVALNE DEJAVNOSTI

Diplomsko delo

Ljubljana, 2008

PRIVATIZACIJA OBVEŠČEVALNE DEJAVNOSTI

Država čedalje bolj izgublja monopol nad zagotavljanjem varnosti svojih državljanov, zasebni sektor pa postaja vse močnejši in vplivnejši faktor, ki prevzema varnostne naloge, katere tradicionalno pripisujemo državi. Takšno je tudi področje obveščevalne dejavnosti, nad katerim je dominirala država vse od institucionalizacije prvih obveščevalnih aparatov. Spremembe varnostnega okolja so pokazale, da se je potrebno današnjim nedržavnim grožnjam zoperstavljati holistično, kar zahteva sodelovanje tako zasebnega kot državnega sektorja. Vodilno vlogo politične moči države je zamenjala ekonomska moč, ki pa je v rokah velikih korporacij, ki za takšno vlogo potrebujejo in razvijajo zmožnosti za pridobivanje informacij. Informacijska revolucija je tukaj odigrala pomembno vlogo, saj je kot tehnološki, socialni in ekonomski trend povzročila preoblikovanje zaprtega in omejenega sveta v sploščen svet, v katerem smo priča prostemu pretoku ljudi, kapitala, idej, groženj in informacij. Obveščevalna dejavnost se mora pri soočanju s prihodnostjo tako naslanjati na vse več informacij iz odprtih virov, ki so bistvenega pomena za oblikovanje končnih obveščevalnih produktov. Pridobivanje, obdelava in distribucija javno dostopnih informacij pa je področje, ki ga obvladujejo zasebne obveščevalne organizacije in ki zaradi svojih kompetenc opravljajo zunanje izvajanje obveščevalne dejavnosti za državne, naddržavne in nedržavne organizacije. V tem diplomskem delu bomo torej spoznali vse dimenzije privatizacije obveščevalne dejavnosti.

Ključne besede: obveščevalna dejavnost, obveščevalna dejavnost odprtih virov, privatizacija, zasebne obveščevalne organizacije, zunanje izvajanje.

PRIVATIZATION OF INTELLIGENCE

Private sector is becoming stronger and stronger in taking over security tasks, which have been traditionally assigned to the state, and on the other hand, state is losing its monopoly over the provision of safety of its citizens. That sphere of security also represents the intelligence activities over which state had dominated since institutionalization of first intelligence apparatuses. Changes of security circumstances have shown that nowadays threats have to be fought hollistically by cooperation between private and governmental sector. Political power had been replaced by economical power, which is now in hands of corporations, instead of states, and which for this purpose need to develop intelligence capabilities. Information revolution as technological, social, and economical trend has played here an important part, as it has changed closed and limited world into flatten one, in which we witness uncontrolled movement of people, capital, ideas, threats and information. Intelligence must rely on more and more open source information, as significant part of finished intelligence products. Acquisition, processing and distribution of free information is a field of discipline that private intelligence organizations, cause of its competencies, own and outsource for state, suprastate and private organizations. So, in this diploma, we are going to be acquainted with all dimensions of privatization of intelligence.

Tags: intelligence, open source intelligence, privatization, private intelligence organizations, outsourcing.

KAZALO

KAZALO SLIK IN TABEL

SEZNAM KRATIC

ARIA	AEGIS Research and Intelligence Advisory
ATAS	AEGIS Threat Assessment System
C4I	Command, Control, Communications, Computers and Information
CACI	Consolidated Analysis Centers Incorporated
DCI	Director of the Central Intelligence Agency
DIA	Defense Intelligence Agency
EGL	Eagle Global Logistics
ERP	Enterprise Resource Planning
EU	Evropska unija
GPW	Grayson, Pender, Wordsworth
HUMINT	Human Intelligence
IMGINT	Imagery Intelligence
IT	Information Technology (informacijska tehnologija)
MPRI	Military Professional Resources Incorporated
NATO	North Atlantic Treaty Organization
NAU	North American Union
NCIX	National Counterintelligence Executive
OSINT	Open Source Intelligence
OZN	Organizacija združenih narodov
PFI	Private Finance Initiative
RAND	Research and Development (Corporation)
SIGINT	Signals Intelligence
SRIC	Sanwa Research Institute and Consulting
SYCP	Slovenia Your Cooperation Partner
UNASUR	Union of South American Nations
USD	United States dollar
VB	Velika Britanija
ZDA	Združene države Amerike

1 UVOD

Človek je že v času plemenske skupnosti težil po pridobitvi informacij, ki so bile temeljnega pomena za preživetje v anarhičnem in darvinistično naravnanem okolju, v katerem je vladalo Hobbesovo načelo *homo homini lupus*. Kljub spreminjajočem se okolju človeka, se je ta potreba po preživetju in s tem potreba po informacijah ohranjala vse skozi zgodovino, kar so ob nastanku prvih nacionalnih držav dokazali tudi vladarji, ko so za potrebe po preživetju v vojnah zoper druge države institucionalizirali lastne obveščevalne aparate, kateri so se bolj ali manj razvijali vse tja do sredine 20. stoletja. Po drugi svetovni vojni so se obveščevalne službe začele izpopolnjevati, znotraj obveščevalnih sistemov in služb pa so se sprožili procesi specializacije, diferenciacije in profesionalizacije (Purg 2002, 27). Razpad bipolarne politične konstelacije, kateri so obveščevalne službe prilagajale svoje metode in sredstva, je povzročil pravo sploščitev sveta, ki je vplivala ne le na obveščevalno dejavnost, ampak na celoten univerzum varnosti. Prevladujoča vloga asimetričnega bojevanja, poplava informacij, premik h geoekonomiji in partikularizacija interesov znotraj družbe so prisilile človeka, da ponovno vzpostavi lastne neodvisne mehanizme potešitve potrebe po varnosti kot esencialnemu predpogoju razvoja *homo economicusa*. Ta potreba ni več le biološko-etnološka karakteristika, temveč tudi socialna in ekonomska. Posamezniki in organizacije so zdaj primorani poskrbeti sami zase na način, ki ga je dolga stoletja zagotavljala država, kajti izkušnje zadnjih let kažejo, da je država čedalje manj uspešna, vedno bolj draga in odtujena organizacija (Pečar 1997, 15). Zasebni sektor sedaj prevzema vlogo države na varnostnem področju, kar se kaže tudi pri krepitvi njegove vloge na področju obveščevalne dejavnosti in pri prevzemanju določenih metod dela in sredstev obveščevalnih služb, ki so do nedavnega pripadale izključno državi.

Pri vsem tem je pomembno poudariti, da vlade zahodnih držav takšnim trendom ne nasprotujejo, temveč jih poskušajo izkoristiti z namenom povečanja uspešnosti in učinkovitosti delovanja državnega aparata. Tako kot posameznik ali zasebna organizacija tako tudi državni organi in institucije vse bolj posegajo po varnostnih storitvah, ki jih na trgu ponujajo za to specializirani zasebni subjekti. S tem postaja za države vse bolj zanimivo sklepanje pogodb z zunanjimi izvajalci storitev, ki niso le učinkoviti pri opravljanju prevzetih nalog, ampak tudi konkurenčni. Prevzemanje tržnih zakonitosti v državni upravi ni novost in je povsem razumljivo, vendar pa ne povsem za tisti tabuiziran segment državne uprave, ki opravlja obveščevalna dejavnost.

Diplomsko delo poskuša temeljito in celovito predstaviti privatizacijo obveščevalne dejavnosti, zato je sestavljeno iz štirih osnovnih delov. Prvi del, ki je sestavljen iz prvih treh poglavij, je metodološki in zajema hipoteze ter opredelitev temeljnih pojmov. Drugi del diplomskega dela v celoti predstavlja četrto poglavje, ki se nanaša na spremembo varnostnega okolja in privatizacijo varnosti, kar vključuje novo varnostno paradigmo, nastop geoekonomije in pojav varnostnih storitev na tržišču. S tem poglavjem bom podal nekaj indicev za razumevanje predmeta proučevanja v nadaljevanju. Osrednji – tretji – del diplomskega dela v dveh poglavjih, petem in šestem, podrobneje obravnava privatizacijo obveščevalne dejavnosti in z njo povezane zasebne obveščevalne organizacije. V petem poglavju bo temeljito predstavljen fenomen nove obveščevalne paradigme – privatizacija obveščevalne dejavnosti ter njene ključne komponente, ki jih v grobem predstavljajo asimetrični pristop obveščevalnih služb pri soočanju z novimi grožnjami, informacijska revolucija, spremenjene metode dela in ekonomski vidik privatizacija obveščevalne dejavnosti; šesto poglavje pa bo namenjeno izključno tipologiji in opisu zasebnih obveščevalnih organizacij. Zadnji, četrti, del diplomskega dela predstavlja zaključni del, ki ga sestavljajo sedmo, osmo in deveto poglavje. V sedmem poglavju bom analiziral pravno podlago za obveščevalno dejavnost zasebnih subjektov v Republiki Sloveniji, v samem zaključku pa bodo sledile še verifikacija hipotez, sklepna beseda in predstavitev uporabljene literature pri stvarjenju tega diplomskega dela.

2 METODOLOŠKI OKVIR

2.1 Opredelitev predmeta proučevanja

Zmanjševanje vloge države pri zagotavljanju varnosti in opravljanju obveščevalne dejavnosti je latenten in površinsko raziskan fenomen, ki je posledica tektonskih sprememb na varnostnem področju in sodobnih družbenih trendov. V državah, kot so ZDA in Velika Britanija, kjer so privatizacijski procesi zakoreninjeni v zavest družbe in so običajno del kontinuitete dominacije zakona ponudbe in povpraševanja, ki ga dosledno obvladuje zasebni sektor, to ni le nov fenomen starih načel, temveč tudi logična posledica omenjenih sprememb na varnostnem in družbenem področju. Spet v drugih državah, kot je denimo Slovenija, ki je prešla iz sistema socialističnega samoupravljanja v sistem tržnega gospodarstva, pa je privatizacija obveščevalne dejavnosti fenomen, ki sicer že klije, ampak ne v zavesti družbe ali države. Zato je potrebno privatizacijo obveščevalne dejavnosti proučiti na splošni ravni, pri tem pa upoštevati varnostne, ekonomske, tehnološke, sociološke in druge dejavnike. Glavni gibalo tovrstne privatizacije je – kot že sam izraz pove – zasebni ali privatni sektor, ki pa ni omejen le na obveščevalno dejavnost na gospodarskem področju, temveč prevzema vse več nalog povezanih z nacionalno varnostjo, ki jih običajno *a priori* prištevamo obveščevalnim službam države. V tem diplomskem delu gre torej za korenit premik od državnega k zasebnemu pri proučevanju področja obveščevalne dejavnosti.

2.2 Cilji proučevanja

Cilji proučevanja so:

- definirati temeljne pojme v zvezi s privatizacijo obveščevalne dejavnosti;
- poiskati in analizirati ključne razloge za spremembe na varnostnem področju, ki so povzročili privatiziranje nekaterih varnostnih funkcij države, ter opredeliti pomembnejše rezultate te privatizacije;
- našteti, opredeliti in parcialno analizirati glavne vzroke in dejavnike za privatizacijo obveščevalne dejavnosti;
- redefinirati obveščevalno dejavnost in jo prilagoditi sodobnim konceptom in razmeram, v katerih zasebnih subjekti prevzemajo vse pomembnejšo vlogo;

- raziskati širši strateški kontekst, znotraj katerega lahko zasebne obveščevalne organizacije veliko prispevajo k nacionalni varnosti;
- navesti in opredeliti zasebne obveščevalne organizacije in specifične zasebne obveščevalne zmožnosti, ki bi jih lahko uporabile tako vlade kot tudi zasebne organizacije z namenom doseči večjo učinkovitost in uspešnost;
- analizirati pravne pogoje za privatizacijo obveščevalne dejavnosti v Republiki Sloveniji.

2.3 Hipoteze

- **H1**: Država izgublja monopol nad zagotavljanjem varnosti svojih državljanov, kar se kaže tudi na področju obveščevalne dejavnosti.

Sodobni trendi kažejo, da bo država na področju zagotavljanja varnosti vse več prostora prepuščala zasebnim subjektom, kar bo veljajo tudi za obveščevalno dejavnost. Ob vseh teh sodobnih globalnih procesih smo zato priča privatizaciji obveščevalne dejavnosti.

- **H2**: Obveščevalna dejavnost države ne bo preživela v konkurenci z obveščevalno dejavnostjo zasebnih organizacij.

Zasebne organizacije bodo prevzemale vse več nalog na področju obveščevalne dejavnosti, katere pa bodo opravljale tako za zasebne kot tudi za državne organizacije. Zaradi svoje konkurenčnosti bodo izrinile državne obveščevalne službe pri opravljanju obveščevalne dejavnosti in prevzele na tem mestu primarno vlogo.

- **H3**: Obstoječi pravni red Republike Slovenije ne onemogoča nadaljnjega razvoja obveščevalne dejavnosti zasebnih subjektov.

Ustavnopravni red v Republiki Sloveniji ima določena področja, ki bi jih lahko povezali z obveščevalno dejavnostjo zasebnih subjektov, v primerjavi z nekaterimi drugimi zahodnimi državami, urejena, vendar pa takšna ureditev ne onemogoča razvoja omenjene dejavnosti, kar pomeni, da obstaja pravna podlaga za delovanje zasebnih obveščevalnih organizacij.

2.4 Uporabljena metodologija

Pri izdelavi diplomskega dela sem uporabil več različnih raziskovalnih metod, in sicer:
(1) **metodo zbiranja primarnih in sekundarnih virov**, ki je predpogoj za uporabo nadaljnjih metod;
(2) **metodo analize in interpretacije primarnih virov**, s pomočjo katere sem raziskal uradne dokumente, pravne akte in zakonodajo, ki so mi koristili pri definiranju pojmov, razjasnitvi okoliščin, splošnemu razumevanju pravnih omejitev, pravic in dolžnosti v zvezi z obveščevalno dejavnostjo;
(3) **metodo analize in interpretacije sekundarnih virov**, na podlagi katere sem predelal in analiziral strokovne publikacije, kot so knjige, zborniki, članki ter druga raziskovalna dela tako v elektronski kot tudi v tiskani obliki, kar mi je koristilo pri pojasnjevanju tez, potrjevanju dejstev in pridobivanju podatkov in informacij;
(4) **deskriptivno metodo**, s katero sem opisal predvsem pojme, ki se nanašajo na obveščevalno dejavnost, ne glede na besedno vrsto;
(5) **metodo primerjalnega raziskovanja**, ki mi je pomagala predvsem pri proučevanju razlik med obveščevalno dejavnostjo zasebnih in državnih subjektov;
(6) **primerjalno-pravno metodo**, na podlagi katere sem naredil primerjalno analizo posameznih zakonov in drugih pravnih aktov;
(7) **metodo zgodovinske analize**, ki sem jo uporabil pri analiziranju nekaterih pomembnejših zgodovinskih primerov s področja obveščevalna dejavnosti;
(8) **študijo primerov**, uporaba katere je razvidna predvsem v poglavju o zasebnih obveščevalnih organizacijah.

3 TEMELJNI POJMI

Ključni pojmi tega diplomskega dela so: obveščevalna dejavnost, vohunstvo in obveščevalna služba. Pretežen del diplomskega dela je namenjen proučevanju obveščevalne dejavnosti in z njo povezanimi aktivnostmi, zato je pojem *obveščevalna dejavnost* ključni element pojmovnega aparata. Od obveščevalne dejavnosti moramo nujno ločevati *vohunstvo*, ki je kot pojem pomemben pri razumevanju razlik med metodami dela, sredstvi in cilji zasebnih in državnih obveščevalnih organizacij. Tretji temeljni pojem je *obveščevalna služba*, ki je za naše proučevanje pomemben kot subjekt obveščevalne dejavnosti.

3.1 Obveščevalna dejavnost

Vladimir Šaponja (1999, 9-10) definira **obveščevalno dejavnost** kot *»organiziran proces, ki zajema zbiranje in analitično obdelavo surovih podatkov in izdela celovit obveščevalni izdelek, ki ga uporabnik potrebuje pri oblikovanju in sprejemanju odločitev na državniškem, političnem, gospodarskem in varnostnem področju«*. Adam Purg pa povzema (Richelson v Purg 2002, 14) definicijo, ki opredeli obveščevalno dejavnost kot *»rezultat zbiranja, analiz, združevanja in interpretacije vseh razpoložljivih podatkov, ki zadevajo enega ali več vidikov tuje države oziroma operativnega področja, ki je neposredno ali potencialno pomembno za načrtovanje«*. Zbiranje podatkov je zavestno, načrtno, namensko, organizirano in usmerjeno k zadovoljevanju določene potrebe, ki je pomoč pri sprejemanju odločitev. Lahko poteka v več oblikah, in sicer javno ali tajno.[1] Pri obeh oblikah pa ga lahko opravljajo ali ljudje ali tehnična sredstva. Za izdelavo **končne obveščevalne informacije** je potrebna integracija zbranih podatkov v fazi analize (Purg 2002, 14).[2] Obveščevalna dejavnost je lahko organizirana v državnih in zasebnih institucijah.

Pojem obveščevalne dejavnosti lahko zaradi svoje širine obravnavamo **v širšem in ožjem smislu**. V širšem smislu je obveščevalna dejavnost organizirano pridobivanje novega znanja in informacij o dogodkih, pojavih in procesih v bivalnem ali poslovnem okolju, v naravi, v družbi, skratka o vsem okoli nas.[3] O obveščevalni dejavnosti v širšem smislu govorimo tudi takrat, ko obveščevalne organizacije za potrebe odločanja na *organiziran* in *institucionaliziran* način zbirajo, analizirajo in posredujejo končne izdelke. Delujejo samo pod pogoji, ki so dovoljeni državljanom in zbirajo samo tiste podatke, ki so javno dostopni (Šaponja 1999, 10–11). O obveščevalni dejavnosti v ožjem smislu pa govorimo takrat, ko jo izvajajo državne institucije, ki imajo zakonska pooblastila, da zbirajo tudi tajne podatke na

[1] Tajno pridobivanje podatkov pomeni pridobivanje tistih podatkov, ki javnosti niso na voljo in so tajni. Tajni podatki pa so tisti, ki jih država ali organizacija določi za tajne. Kot tajen lahko razglasi podatek tudi fizična oseba (npr. telefonska številka) (Šaponja 1999, 179).

[2] Pridobljen podatek namreč še ne predstavlja obveščevalne informacije, kar se pogosto zmotno enači ali celo zamenjuje. Razlikovati moramo med *podatkom*, ki je surov tekst, slika ali signal, *informacijo*, ki je pregledan podatek nekega splošnega interesa, kot so časopisi ali raziskovalna poročila, in *obveščevalno informacijo*, ki je obdelana in ovrednotena informacija v podporo odločanja (Shulsky v Steele 1996, 221). Podatki tako šele v obveščevalnem ciklusu postanejo obveščevalna informacija.

[3] Danes se skorajda vsakdo pogojno in nezavedno ukvarja z obveščevalno dejavnostjo oziroma obveščevalnim delovanjem. O različnih stvareh pridobivamo različne podatke, jih analiziramo, iz njih izpeljemo ocene in sklepe, ki nam pomagajo pri nadaljnjih odločitvah. Kljub temu pa ne moremo reči, da gre tukaj za obveščevalno dejavnost, saj **to ni organizirana dejavnost**. O tej bi lahko govorili le v primeru, da podatke zbira zasebna organizacija (Šaponja 1999, 11–12).

posebne načine. Te specializirane državne institucije so obveščevalno-varnostne in obveščevalne službe (Purg v Šaponja 1999, 26–27).

V tesni zvezi z obveščevalno dejavnostjo se pojavlja pojem **obveščevalni ciklus**, ki ga Šaponja (1999, 57) opredeli kot *»medsebojno povezane dejavnosti v procesu obveščevalne dejavnosti«* (Richelson v Purg 1994, 23). Krog sestavlja pet različnih stopenj: (1) načrtovanje in usmerjanje (opredelitev ciljev in objektov obveščevalnega delovanja); (2) zbiranje podatkov; (3) obdelava podatkov (spremembo ogromne količine podatkov v obliko, primernejšo za izdelavo obveščevalne informacije); (4) analiziranje (sprememba osnovne informacije v končno obveščevalno) in (5) posredovanje (naročnikom).[4]

3.2 Vohunstvo

Enciklopedija *Britannica* (2008, »espionage«) definira **vohunstvo** (angl. espionage) kot *»proces pridobivanja vojaških, političnih, komercialnih ali drugih tajnih podatkov s sredstvi, kot so vohuni, tajni agenti ali nelegalne prisluškovalne naprave. Vohunstvo se razlikuje od obveščevalne dejavnosti po svoji agresivni naravi in nezakonitem delovanju.«* V *Enciklopediji vohunstva, obveščevalne dejavnosti in varnosti* (Lerner in Lerner 2004, 298) najdemo definicijo, ki pravi, da je vohunstvo *»uporaba vohunov ali dejanje vohunjenja za pridobitev podatkov o načrtih, dejavnostih, zmogljivostih ali virih nasprotnika«*. Pogosto se vohunstvo zamenjuje z obveščevalno dejavnostjo, vendar pa se od te razlikuje po svoji tajni, agresivni in nevarni naravi delovanja. Je le ena izmed metod obveščevalne dejavnosti, nikakor pa ne more biti njen sinonim. Purg (2002, 16) opredeljuje vohunstvo kot ožji pojem obveščevalne dejavnosti, ki predstavlja zgolj deset do dvajset odstotkov v celotni obveščevalni dejavnosti. Avtor daje vohunstvu dva pomena, pravnega in političnega. Slednji pomen razlaga vohunstvo kot »*vsako dejavnost, s katero se poskuša priti do podatkov o dejstvih, ki jih skriva«* posameznik, ustanova ali država. Vohunstvo pa se danes lahko pravno okvalificira kot protizakonito, kaznivo in nemoralno dejanje (Purg 2002, 16; Šaponja 1999, 59). **Vohunstvo je torej prepovedano zbiranje tajnih in z zakonom zaščitenih podatkov**.

[4] John Keegan (2002, 5–6) navaja pet temeljnih stopenj obveščevalnega ciklusa, in sicer: (1) pridobivanje podatkov, (2) dostava podatkov, (3) sprejem podatkov, (4) interpretacija podatkov in (5) sprejemanje in izvrševanje (implementacija) odločitev na podlagi obveščevalnih informacij. Avtorji se pri definiranju obveščevalnega ciklusa razlikujejo predvsem v navajanju različnega števila posameznih stopenj ciklusa, običajno od treh do petih (Purg v Šaponja 1999, 12).

3.3 Obveščevalna služba

Podobno kot pojem obveščevalne dejavnosti tudi pojem **obveščevalne službe** nima enotne, splošne definicije (Purg 2002). Zato bom pri opredeljevanju obveščevalne službe izhajal iz njene dejavnosti – obveščevalne dejavnosti. Obveščevalna služba je, kot pravi Šaponja (1999, 24), organizirana v organizacijskih oblikah, torej v tako imenovanih **obveščevalnih organizacijah**. Slednje so lahko organizirane kot del državnega aparata in se imenujejo obveščevalne organizacije v ožjem smislu oziroma službe. Ker delujejo tajno, so to *tajne službe*. Obveščevalne službe lahko uporabljajo tako legalne možnosti za pridobivanje podatkov kot tudi posebne metode in sredstva dela, med drugimi tudi vohunstvo in »umazane posle« (Purg 2002, 17). Obveščevalne organizacije so lahko organizirane tudi kot samostojne nedržavne[5] ali zasebne organizacije znotraj večjih gospodarskih sistemov ali zasebnih agencij. Šaponja (1999, 24) te organizacije imenuje **obveščevalne organizacije v širšem smislu**, ki imajo različna imena in izvajajo obveščevalno dejavnost v širšem smislu.[6] Anton Grizold (1996, 111) definira obveščevalno službo kot *»posebno organizacijo, ki za državno oblast zbira, analizira in ocenjuje podatke in spoznanja o drugih državah ter o posameznikih in skupinah, ki ogrožajo nacionalno varnost. Obveščevalne službe v demokratičnih državah so servis za državno politiko, ki pri odločanju o strateških vprašanji potrebuje pravočasne in celovite informacije o dogajanjih v lastni in drugih državah ter strokovne ocene njihovega pomena.«* Grizoldovo definicijo bi lahko determinirali kot klasično definicijo pojma obveščevalne službe.

Obveščevalne službe, ki izvajajo vse stopnje obveščevalnega ciklusa imenujemo **strateške**, tiste, ki pa izvajajo samo določeno stopnjo obveščevalne ciklusa pa **taktične** obveščevalne službe (Šaponja 1999, 34–37).[7]

---

[5] Avtor je uporabil besedno zvezo »nevladne organizacije«, ki lahko danes pomeni nekaj drugega, zato sem uporabil pridevnik »nedržavne«. Splošne definicije za nevladno organizacijo še ni. V Evropi pa posplošeno ta izraz uporabljamo za nepridobitne, prostovoljne in neodvisne organizacije civilne družbe, kar pa izključuje nekatere pridobitne organizacije, ki se ukvarjajo z obveščevalno dejavnostjo (Divjak 2007).

[6] Adam Purg (2002, 17) je poudaril, da *»obveščevalna služba ni nujno le državni organ, saj jo razvijajo razna gibanja, stranke, večji gospodarski subjekti, nedržavna združenja, večje kriminalne združbe itd.«*. Iz tega lahko sklepamo, da organizacijska oznaka »služba« ni le v domeni države, in da t.i. »obveščevalna organizacija v širšem smislu« lahko tudi nosi organizacijsko ime »služba«. Poleg splošne organizacijske oznake »služba« se uporabljajo tudi oznake kot so agencija, urad, komite, oddelek, direkcija in drugi nazivi.

[7] Strateška obveščevalna dejavnost na vojaško-obrambnem področju se običajno deli na strateško obveščevalno dejavnost in na taktično obveščevalno dejavnost (Purg 2002, 15).

Za razumevanja vloge in pomena obveščevalnih služb v sistemu je pomembna tudi predstavitev **temeljnih funkcij obveščevalnih služb**, ki so determinirane z lastnostmi političnih sistemov. Purg (2002, 34–35) je opredelil naslednje poglavitne funkcije obveščevalnih služb:

- zbiranje, analiziranje in ocenjevanje podatkov in spoznanj o določenih subjektih in posredovanje teh podatkov in spoznanj nosilcem oblasti;
- tisti, ki sprejemajo odločitve in vodijo politiko, morajo biti temeljito informirani ter razpolagati z ustreznimi analizami o položaju v svetu, da lahko sprejemajo premišljene in odgovorne odločitve. Pri pogajanjih ima ustrezna in pravočasna informacija odločilno vlogo. Znanje je moč, tajno znanje pa tajna moč;
- obveščevalne službe so s predčasnimi informacijami koristne za načrtovanje in oblikovanje politike, konfliktne situacije itd.; obveščevalni podatki pa lahko oblikovalcem politike osvetlijo razpon opcij, tako da ti izberejo (praviloma) pravo;
- predvidevanje tega, kar se bo zgodilo na posameznem področju, je vsebinska funkcija službe. Na podlagi teh predvidevanj se lahko pristojni organi primerno pripravijo;
- pomembna determinanta postaja konkurenca. O konkurentih[8] je potrebno vedeti čim več, predvsem pa o njegovih šibkih točkah. Tukaj govorimo o podatkih o novih tehnoloških in bazičnih znanjih, novih patentih, načrtih za prihodnost, tehnologiji itd.;
- v novejšem obdobju obveščevalne službe delujejo tudi neobveščevalno (terorizem, likvidacije, »umazani posli«) v odnosu do vitalnih interesov nasprotnika, in sicer s prikritimi operacijami. Tukaj govorimo o bojevanju, temelječem na obveščevalni dejavnosti (angl. intelligence-based warfare) (Svete 2002, 79);
- odkrivanje tajnosti v medčloveških odnosih; obveščevalne službe odkrivajo nasprotne in ščitijo lastne službe, zlasti z informacijsko tehnologijo (Svete 2002, 80);
- obveščevalna služba ima tudi posredniško vlogo med državama, ki uradno nimata stikov (tako imenovana tajna diplomacija). Službe lahko pripravljajo teren za vzpostavitev uradnih stikov.

Poznamo več **metod in načinov zbiranja podatkov obveščevalnih služb**. Šaponja (1999, 80–82) se pri tem naslanja na ameriško literaturo in opredeli načine zbiranja podatkov v obveščevalni dejavnosti na naslednje posamezne discipline (v angleščini):

[8] Konkurenti kot posamezniki, organizacije, skupine ali države.

- HUMINT (**Hum**an **Int**elligence): Gre za disciplino, ki zbira podatke z uporabo človeških virov. Človek lahko prinaša tajne (z vohunstvom) in javne podatke.
- SIGINT (**Sig**nals **Int**elligence): Pomeni disciplino, ki s tehničnimi sredstvi zbira vse podatke in jih prenaša v obliki signalov oziroma elektromagnetnih valovanj. Disciplina ima svoje poddiscipline.[9]
- IMINT (**Im**agery **Int**elligence): Je disciplina, ki je specializirana za zbiranje podatkov v obliki podob oziroma slik ali fotografij (Lerner in Lerner 2004, 302).
- MASINT (**Meas**urement **Int**elligence): Disciplina, kjer lahko z uporabo visoko tehnoloških naprav izvajamo tehnološke meritve, vsebnosti določnih kemijskih elementov v zraku, vodi ali na zemlji, velikost predmetov in hitrost njihovega gibanja (letalo, podmornica ipd.). Tudi ta disciplina ima svoje poddiscipline.[10]
- OSINT (**O**pen **S**ource **Int**elligence): Gre za zbiranje podatkov iz javno dostopni virov, kot so elektronski mediji, javne baze podatkov, omrežja, tisk, literatura in podobno.[11]

4 SPREMEMBE VARNOSTNEGA OKOLJA IN PRIVATIZACIJA VARNOSTI

Za sodobno varnostno okolje so značilni predvsem nepredvidljivi dogodki, hitre spremembe, krize in grožnje varnosti. Ogrožajočih pojavov je v dandanašnjem varnostnem okolju vedno več, vedno večja pa je tudi njihova medsebojna povezanost in transnacionalnost (Prezelj 2007, 7). Robert D. Steele (2002a) takšno netradicionalistično pojmovanje groženj

[9] Poddiscipline SIGINT so: COMINT (Communication Intelligence) – specializirana je za prisluškovanje telekomunikacijam; ELINT (Electronic Intelligence) – odkriva in spremlja delovanje naprav, ki niso namenjene komunikaciji, njihovo delovanje pa pomeni, da nekdo izvaja obveščevalno dejavnost (sredstva za podporo elektronskega bojevanja, za protielektronsko bojvanje, za elektronsko bojevanje); RADINT (Radar Intelligence) – z uporabo radarjev ugotavlja in spremlja nasprotnikove aktivnosti (zaznavanje nasprotnikove radarske aktivnosti). Podkategorija ELINT je FISINT (Foreign Instrumentation Signals Intelligence), katerega del je tudi TELINT (Telemetry Intelligence). Primeri FISINT zajemajo signale, poslane s strani tujih organizacij pri testiranju ali pripravi zračno-vesoljskih, kopenskih in podvodnih sistemov. TELINT pomeni spremljanje na primer uporabe signalov za prenos informacije do raketno vodenih sistemov (Lerner in Lerner 2004, 299).

[10] Poddiscipline MASINT so: ACINT (Acoustic Intelligence) – pridobivanje in analiza podatkov iz zvočnih valov; IRINT (Infrared Intelligence) – uporablja se pri pošiljanju in sprejemanju zvokovnih sporočil; LASINT (Laser Intelligence) – pridobivanje podatkov s pomočjo laserja; NUCINT (Nuclear Intelligence) – pridobivanje podatkov iz radiacije iz radioaktivnih virov; OPINT (Optical Intelligence) – pridobivanje podatkov iz valov vidne svetlobe; RINT (Radiation Intelligence) – vključuje spremljanje elektromagnetnega valovanja (Lerner in Lerner 2004, 253–254; 304).

[11] Po mnenju Šaponje je ta disciplina najmlajša, njen razvoj pa povezuje z razvojem informacijsko-komunikacijske tehnologije v drugi polovici 20. stoletja. Vendar pa je bila ta disciplina prisotna že veliko prej. Zametke črpanja informacij iz javnih virov lahko najdemo že v 16. stoletju v Indiji, ko se je razvil sistem obveščanja, imenovan **harkara**. Ta je temeljil na prenosu informacij (v pisni in ustni obliki) iz sodišč nižje stopnje na višjo stopnjo, iz tega načina informiranja pa je nastal redni tedenski časopis. V sodobni terminologiji harkara predstavlja hkrati obveščevalno službo in novinarsko hišo (Keegan v Črnčec 2005, 28).

varnosti poimenuje kot novo paradigmo ogrožanja.[12] Takšnemu dojemanju sodobnega varnostnega okolja botrujejo tudi globalni ekonomski trendi, ki pomenijo prehod od geopolitičnega h geoekonomskemu razumevanju sveta. Posledice prevlade teh novih konceptov pa se kažejo v privatizaciji varnosti oziroma varnosti kot tržnemu blagu.

4.1 Nova paradigma ogrožanja

Varnost[13] in razvoj v 21. stoletju na splošno ogrožajo pomanjkanje vodnega bogastva in energentov, klimatske spremembe, ekološke katastrofe, panepidemije, transferi ilegalni migrantov, propadle države in državne zveze, etnična trenja med separatisti in državami, oportunistične kriminalne združbe, ki uspešno delujejo v kaotičnih pogojih in v razmerah anarhije, tihotapljenje ilegalnega orožja in uporaba nehumanega orožja ter kibernetskega bojevanja, elektronski vandalizem in terorizem (Prezelj 2002a, 427; Svete 2005, 59–60; Steele 2002a).[14] Gre za pretežno nevojaško naravo sodobnih groženj, ki so transnacionalnega značaja in imajo vpliv na mednarodno skupnost neodvisno od političnih mejá (Prezelj 2002b, 632). Te pojave običajno razvrščamo v skupine oziroma dimenzije (sektorje).[15] Stroka s področja obramboslovja in varnostnih študij poudarja povezanost teh različnih dimenzij ogrožanja varnosti, zato govorimo o večdimenzionalnosti in kompleksnosti ogrožanja nacionalne varnosti, čemur se morajo mehanizmi nacionalnovarnostnih sistemov[16] prilagoditi

[12] Po netradicionalističnem pojmovanju, ki se je razvilo po koncu hladne vojne, je *»ogrožanje varnosti kakršnokoli stanje, v katerem ni zagotovljen obstoj in uravnotežen razvoj določenega referenčnega objekta«* (Prezelj 2002b, 623).

[13] Varnost opredelimo kot stanje, v katerem je zagotovljen uravnotežen fizični, duhovni ter gmotni položaj posameznika v skupnosti v razmerjih do drugih posameznikov, družbenih skupnosti in narave (Grizold 1992).

[14] Po Steelu (2002, 8–11) obstajajo v dandanašnjem strateškem okolju štiri različne kategorije groženj: (1) »grožnje nasilnih držav«, ki jih predstavljajo napredne države s strateškimi konvencionalnimi in jedrskimi silami ter sofisticirano vojaško tehnologijo (ZDA, Rusija, Kitajska); (2) »grožnje nasilnih nedržavnih subjektov«, ki so danes najbolj pogoste in delujejo tako obrambno kot obveščevalno, predstavljajo pa jih teroristične in kriminalne organizacije, zoper katere se je potrebno boriti predvsem z HUMINT; (3) »grožnje nenasilnih nedržavnih subjektov« so masovne migracije (ilegalno priseljevanje), ki se nanašajo na milijone ljudi, to kategorijo pa lahko razumemo že skozi akademske, poslovne in druge nevladne študije; (4) »različne minljive grožnje«, kamor spadajo kompleksne grožnje, ki se nanašajo na kibernetsko in informacijsko vojskovanje. Te kategorije se v določeni meri tudi prekrivajo ali pa so povezane.

[15] Poznamo več dimenzij ogrožanja nacionalne varnosti: vojaška, gospodarska, policijsko-kriminalistična, ekološka, zaščitno-reševalna, teroristična, zdravstvena, informacijska, obveščevalna in migracijska (Prezelj 2007, 8).

[16] Po Grizoldu (1992, 68) **nacionalnovarnostni sistem** opredelimo kot strukturo, katere cilj je zagotavljanje varnosti na nivoju celotne družbe. Sodoben nacionalnovarnostni sistem je sestavljen iz varnostne politike, varnostne strukture in varnostnega samoorganiziranja. Z vidika sistemske teorije razvija kot pojavne oblike svojega delovanja varnostne mehanizme (obrambnega, notranje-varnostnega, zaščitno-reševalnega), vsak od njih pa posamične varnostne instrumente (obrambni oborožene sile in civilno obrambo, notranje-varnostni policijo, obveščevalne in obveščevalno-varnostne službe, inšpekcijske službe, organe odkrivanja in pregona itd.) (Poles 2006, 9).

(Prezelj 2002a, 427; 2007, 8).[17] Keys (v Prezelj 2007, 9) označuje pojav povezanosti med različnimi grožnjami varnosti kot domino učinek (angl. domino effect), zato pravimo, da sta globalizacija in lokalizacija dve plati iste medalje. Steele (2002a, 5–8) te netradicionalne grožnje na splošno pojasnjuje kot *»tekmo med hitrim in vztrajnim razvojem na eni, ter neenakomerni in destabilizirajoči populacijski eksploziji na drugi strani«*.

Staro paradigmo ogrožanja, ki je slonela na konceptu ogroženosti s strani velesile in njenih zaveznikov ter pomembnosti vloge strateških jedrskih in konvencionalnih sil, je po razpadu bipolarnega sistema na prehodu iz osemdesetih v devetdeseta leta prejšnjega stoletja zamenjala **nova paradigma ogrožanja**, ki izpostavlja nove vire ogrožanja nacionalne varnosti,[18] ki jih predstavljajo predvsem dinamični, nekonvencionalni, nejasni, kompleksni, vseobsegajoči, večdimenzionalni in večinoma nedržavni ali naddržavni akterji, katerih ogrožanje ni indoktrinirano, ne upošteva določil mednarodnega vojnega prava in ni omejeno na kakršnekoli politične ali geografske meje.[19] Steele jo zato označuje kot **asimetrično** (Steele 2002a, IV).[20]

Kljub prenosu težišča s tradicionalnih na netradicionalne grožnje pa »stari viri« ogrožanja varnosti niso popolnoma izginili. Širitev zveze NATO in vpliva ZDA proti vzhodu ter krepitev Ruske federacije pod vplivom Putinove politike sta dejavnika, ki sprožata številna politična namigovanja k začetku nove hladne vojne.[21] Po drugi strani pa se svet srečuje z vse močnejšimi regionalnimi silami, kot so recimo Kitajska, Iran, Brazilija ali Severna Koreja, ki poskušajo znotraj mednarodne skupnosti utrditi svoj položaj z ali ekonomskimi ali politično-ideološkimi sredstvi, v čemer (predvsem) zahodni svet vidi grožnjo lastni varnosti.

---

[17] O kompleksni grožnji varnosti govorimo takrat, ko ekstremno stopnjevanje grožnje varnosti v eni dimenziji vpliva na stopnjevanje groženj varnosti iz drugih dimenzij, ne glede na nacionalne meje (Prezelj 2002a, 428).

[18] Grizold (1992, 65) definira **nacionalno varnost** kot varnost državnega naroda, ki zajema: varnost nacionalnega ozemlja (vključno z aerotorijem in akvatorijem), zaščito življenja ljudi in njihove lastnine, ohranitev in vzdrževanje nacionalne suverenosti ter uresničevanja temeljnih funkcij družbe (socialnoekonomske, kulturne, ekološke, gospodarske in druge).

[19] Tako kot so pred konstituiranjem modernih nacionalnih teritorialnih držav imele legitimno moč ne-prostorske organizacije – cerkev, gilde, fevdalci – podobno se danes kvazidržavne, nedržavne ali poldržavne sile z ramo ob rami ranjene teritorialne države spopadajo za ozemlja, vire in prebivalstvo (Balažic 2001, 242).

[20] Svete (2002, 21) znotraj konteksta asimetričnega vojskovanja razlikuje asimetrične grožnje (angl. asymmetric threats) od asimetričnih virov ogrožanj. Prve se bolj nanašajo na vire ogrožanja kot na same grožnje, medtem ko so se asimetrični viri ogrožanja nanašajo *»na vse tiste vire, ki se lahko potencialno uporabijo v konceptu asimetričnega vojskovanja«*. Imenuje jih tudi **asimetrični varnostni izzivi**.

[21] Trenja med ruskimi in ameriškimi varnostnimi interesi, ki se pojavljajo pri »evropskih varnostnih vprašanjih« in med katerimi najbolj izstopata namestitev protiraketnega ščita na Poljskem in na Češkem, v kateri vidi Rusija predvsem grožnjo lastni varnosti, ter avgustovska vojna v Gruziji, ki predstavlja območje kolizije ruskih in ameriških (zahodnih) interesov, krepijo nezaupanje med velesilama.

Eno izmed ključnih groženj nacionalni in mednarodni varnosti dandanes predstavlja **terorizem**,[22] katerega uvrščamo med kompleksne kompleksne večstranske ogrožajoče pojave zaradi številnih vzrokov, metod in posledic (Prezelj 2006, 177; 2007, 79).[23] V mednarodnem okolju ima terorizem vidnejšo vlogo predvsem v zadnjih tridesetih letih. Katastrofa »9/11« pa je pokazala, da se z doktrinami iz časa hladne vojne ni moč učinkovito zoperstavljati.

4.1.1 »Vojna proti terorizmu«

Teroristični napadi 11. septembra 2001 v ZDA veljajo kot prelomnica pri proučevanju varnostnih prvin in podprvin v 21. stoletju. Gre za dogodek, ob katerem sta se pokazali sterilnost in zakrnelost nacionalnovarnostnega sistema ZDA, znotraj katerega obveščevalne in obveščevalno-varnostne službe niso dosledno izvajale svoje vsebinske funkcije in zanemarile načelo preventivnosti. Zaradi tega se je ponovil primer »Pearl Harbor«, svet pa se je z ZDA na čelu znašel v **»vojni proti terorizmu«**, ki predstavlja enega izmed ključnih stimulansov sprememb na področju obveščevalne dejavnosti in varnostnega okolja na sploh.[24]

Od 11. septembra 2001 dalje v zvezi z bojem proti terorizmu govorimo o **sistemski zaščiti**. To je koncept pri katerem gre *»za načrten in sistematično organiziran preventivni pristop, ki temelji na oblikovanju in odzivanju varnostnih mehanizmov, še preden pride do ogrožanja«* (Anžič 2002, 457). Za uresničitev tega koncepta je potrebno dvoje: *predvidevanje* in *analiza ogrožanj*, vključujoč *oceno škode* oziroma izgub. Cilj tega koncepta je identificirati vire ogrožanja, čemur sledi analiza groženj, nato nevtralizacija škodljivih učinkov in končno doseči ravnovesje med tveganjem in nadzorom (Anžič 2002, 457–458). Obveščevalne in obveščevalno-varnostne službe dobivajo torej v boju zoper terorizem pomembno, če ne najpomembnejšo vlogo. Po 11. septembru je treba po besedah Steela (2002a, 22)

[22] Terorizem lahko na splošno opredelimo kot nasilno, prekrito in na presenečenju temelječo taktiko nedržavnih skupin, ki jih lahko sponzorirajo, podpirajo, plačujejo in varujejo države in zasebne organizacije, večinoma naperjeno proti ranljivim ciljem simbolnega ali osebnega pomena v državi (Manning 2006, 61–62).

[23] Anžič (2002, 458) navaja, da so vzroki za terorizem lahko motivirani politično, etnično, nacionalno, gospodarsko, versko vojaško in drugače. Lahko gre za zgolj individualne ali kolektivne prestižne interese. Vzroke lahko delimo na dve skupini: (1) notranji (etnično preganjanje, politično zatiranje, nacionalizem, verski fanatizem itd.) in (2) zunanji (sodobna gospodarska, politična in druga protislovja, ozemeljski spori, gospodarski in politični in drugi ekspanzionizmi, interesi organiziranega kriminala itd.).

[24] Anžič (2002, 464) poudarja, da pojem »vojna proti terorizmu«, ki ga pogosto uporabljajo politiki in novinarji, ne pomeni vojne po sociooloških, antropoloških in polemoloških definicijah, ampak odločenost v ukrepanjih zoper terorizem. Tudi Manning (2006, 62) poudarja, da je terorizem lahko vključen v vojno, vendar pa sam po sebi ne more biti vojna in se proti njemu ne da dobesedno bojevati.

netradicionalne grožnje jemati resneje in omogočiti skupno rabo obveščevalnih informacij in participacijo zasebnega sektorja pri odkrivanju groženj in protiteroristični dejavnosti.

V zvezi z »vojno proti terorizmu« pa se pojavlja zanimiv fenomen. Terorizem s sejanjem strahu vzpodbuja potenciranje potreb po varnosti in s tem povpraševanje po varnostnih storitvah. Tako ima »stanje strahu in nevarnosti« vpliv na rast poslovanja, ki so ga deležne številne korporacije s ponujanjem varnostnih storitev. V tem času smo zato priča pravi eksploziji na trgu varnostnih storitev (Shamsi 2006). Zaradi intenzivne mednarodne prisotnosti in vpliva terorizma in poslovanja, *posel in terorizem vstopata v recipročno razmerje*, kar se kaže predvsem v Iraku, kjer je v povojni obnovi prisotnost uporništva z elementi terorizma (angl. insurgency) instantna in s tem potreba po varnosti toliko večja.[25] Varnostna podjetja so po eni strani uvidela moč terorizma kot dobičkonosnega posla, po drugi strani pa se srečujejo z negativnimi posledicami poslovanja (Irak).[26]

4.2 Od geopolitike h geoekonomiji

Pomemben proces, ki je bistven za razumevanje krepitve zasebnih akterjev v intradržavnih, mednarodnih in globalnih odnosih nasploh, in ki je sovpadal s tektonskimi premiki na varnostnem področju, je bil prehod od geopolitičnega proučevanja odnosov med prostorom in političnim človekom k proučevanju odnosov prostora s *homo economicusom* (Balažic 2001, 238). Na varnostnem področju pa je ta premik pomenil prehod na proučevanje razmerja med nacionalno varnostjo in ekonomijo (Kopač 2007, 55). Govorimo o tako imenovanem prehodu **od geopolitike h geoekonomiji** (Balažic 2001, 238; Kopač 2007, 55; Luttwak v Treverton 2003, 46–47; Sigurdson 1992, 5).

Balažic (2001, 238) pravi, da za *»razliko od političnega prostora, ovrednotenega s stalnostjo, zamejenostjo in zaprtostjo, ekonomski prostor skozi logiko ponudbe in povpraševanja odlikujeta gibanje in odprtost. Če je bila prej ekonomija instrument politike, se*

[25] Po nekaterih ocenah iz leta 2005 naj bi v povojnem Iraku delovalo od 20.000 do 45.000 oseb iz zasebnega varnostnega sektorja z vseh koncev sveta, zaradi česar so iraškemu konfliktu nadeli ime »prva zasebna vojna«. Po podatkih ameriškega projekta »Center for Public Integrity's Windfalls of War« je več kot 150 ameriških podjetij dobilo pogodbe v vrednosti 48,7 milijard dolarjev za delo v povojnima Iraku in Afganistanu. Pri tem naj bi večino predstavljala zasebna vojaška podjetja, ki po številu predstavljajo drugi največji kontingent »koalicije voljnih« v Iraku – za ameriškimi in pred britanskimi silami (Schreier in Caparini 2005, 2).

[26] V letu 2001 so gospodarski subjekti predstavljali kar 90 odstotkov vseh tarč napadov terorističnih organizacij na ameriške cilje. Po drugi strani pa so podjetja zasebnega sektorja, ki se ukvarjajo z varnostnimi storitvami, zaslužila več sto milijard dolarjev letno (Reiter Neal 2008).

zdi, da zdaj ekonomija instrumentalizira politiko: politični konflikti so spopad za naravna bogastva in komunikacije, so skratka konflikti za moč, toda najprej ekonomsko moč.« V sodobni mednarodni skupnosti je namreč gospodarska konkurenčnost bolj pomembna od vojaške sile (Kegly in Wittkopf v Grizold in Kopač 2007, 16), relativna gospodarska rast pa ima odločilno vlogo pri določanju moči države in je zato ključen element nacionalne varnosti (Kennedy v Kopač 2007, 59).[27] V skladu z geopolitiko imajo države monopol moči znotraj svojih meja, kar pomeni, da teritorij nacionalne države predstavlja moč. Vendar pa danes za ekonomski uspeh ni več ključno ozemlje, ampak tehnološke inovacije in na znanju temelječa proizvodnja, kar tudi zmanjšuje teritorialne pretenzije in agresijo (Held v Kopač 2007, 56).[28] Po besedah Balažica (2001, 239) je ravno **globalizacija**[29] na prelomu stoletja tista, ki ruši to klasično pojmovanje teritorialne države.

Teritorialne nacionalne države v zadnjih desetletjih tako izgubljajo nadzor nad časom in prostorom, ob neustavljivi globalizaciji pa se vse bolj decentralizirajo in deteritorializirajo, kar jih bo privedlo do krize identitete. Balažic (2001, 239) pravi, da državo vse bolj *»zaobhajajo svetovni tokovi kapitala, dobrin, storitev, tehnologij, komunikacij in informacij, skoz globalizacijo ekonomije, medijev, elektronskih komunikacij in kriminala pa državo vse bolj presegajo nad-nacionalne institucije*«. Razmerje moči v svetu se iz držav prenaša na globalna podjetja in mednarodne nedržavne organizacije, slednjim pa države pri oblikovanju svojih političnih in gospodarskih ciljev posvečajo vse več pozornosti (Balažic 2001, 239; Grizold in Kopač 2007, 16–17; Kotnik-Dvojmoč 2000, 654–655; Svete 2005, 25). Gre za trend, ki je bolj viden v srednjih in manjših državah (Luttwack v Sigurdson 1992, 6). Braithwaite (v Shearing 2006, 27) pravi, da poteka tako imenovana **korporativizacija sveta**, kar pomeni, da so glavne regulatorske zmožnosti vse bolj v rokah korporacij (bančnih,

[27] Pri geoekonomiki razmerje med ekonomijo in nacionalno varnostjo tako temelji torej na *»podobnih realističnih stališčih kot tradicionalen način povezovanja ekonomskih vprašanj z varnostjo in pri analiziranju ekonomske dimenzije ogrožanja nacionalne varnosti enostavno zamenjuje vojaško terminologijo z ekonomsko«* (Kopač 2007, 55). Po besedah Kopača (2007, 55) geoekomoisti dejansko razumejo ekonomsko tekmovanje med državami kot bojevanje z drugačnimi sredstvi.

[28] Če povedano apliciramo na primeru Slovenije z njenimi gospodarskimi subjekti, lahko rečemo, da je naša država »geopolitični pritlikavec«, gledano geoekonomsko pa je lokalna »velesila« jugovzhodne Evrope. *»Večji delež na enotnem globalnem trgu predstavlja ekonomsko »orožje« in za uporabo ekonomskih instrumentov država lažje doseže svoje politične cilje. Velika Srbija, Hrvaška, Albanija itd. so arhaični geopolitični programi, Velika Slovenija pa je sodobni geoekonomski koncept.«* (Balažic 2001, 238)

[29] Ekonomist Robert Samuelson je opredelil globalizacijo kot svetovno konvergenco ponudbe in povpraševanja, George Soros pa kot velikanski krožni sistem, ki se nanaša na trgovino, finance, komunikacije, obliko vladanja, kulturo, delo ter prosti čas (Svete 2002, 12–13).

industrijskih in trgovskih), kar bo imelo politično-varnostne posledice.[30] Sredi devetdesetih let 20. stoletja se je namreč prvič zgodilo, da so bile velika večina največjih »gospodarstev« na svetu ravno večnacionalne korporacije in ne države.[31]

Ključne dejavnike, ki odločujoče vplivajo na omenjene okoliščine v sodobnem svetu, lahko razvrstimo v naslednje kategorije (Grizold in Kopač 2007, 15; Kotnik-Dvojmoč 2000, 648; Sigurdson 1992, 6): (1) liberalizacija trgovanja in povečanje konkurenčnosti; (2) regionalizacija, ki vodi v oblikovanje trgovsko-političnih blokov in nadaljnje povezovanje teh spet z drugimi;[32] (3) krepitev večnacionalnih korporacij in slabitev nacionalnih držav; (4) povečanje neenakosti in asimetričnosti globalnega razvoja; (5) povečanje nesorazmernosti v razpoložljivosti finančnih sredstev in investicijskih sposobnosti držav; (6) neuravnoteženost v trgovinski menjavi; (7) povečevanje zadolženosti posameznih držav; (8) povečevanje deleža državnega proračuna, namenjenega financiranju zunanjih storitev, ki jih izvaja zasebni sektor, na račun deleža, namenjenega financiranju storitev države; (9) razvoj in razmah informacijsko-komunikacijske tehnologije.

4.3 Varnost kot tržno blago

Spremembe na mednarodnem varnostnem področju so povzročile pravo preobrazbo nacionalnovarnostnih sistemov držav. Razpad bipolarnega sistema, pojav novih tipov ogrožanj, neizprosna »vojna proti terorizmu«, globalizacija ter prehod h geoekonomiji na področju varnosti so v znamenju nove varnostne paradigme sprožile številne neustavljive procese znotraj sistemov nacionalne varnosti, ki spreminjajo vlogo države pri zagotavljanju varnosti. Nacionalna država ni več glavni protagonist v vojaških zadevah in prav tako ne edini porok varnosti svojih državljanov in z njo povezanimi dejavnostmi, kajti to vlogo vse bolj

[30] Svetovna mreža večnacionalnih korporacij ni več podrejena državnemu nadzoru, njihova neodvisnost pa je že tako velika, da so celo vladne odločitve odvisne od delovanja težko nadzorljivih ekonomskih sil (Kotnik-Dvojmoč 2002, 654–655).

[31] Braithwaite in Drahos (v Shearing 2006, 28) govorita tukaj globalizacijski regulaciji kot zgodbi o dominaciji. Po njunem mnenju so današnji globalni zakonodajalci predvsem možje, ki vodijo največje korporacije ter ZDA in EU. Manjšine in državljani tretjega sveta pa so tisti, ki se ravnajo po zakonih. Kot pravi Chomsky: ko močnejši zahtevajo regulacijo običajno hočejo zaščititi svoj monopol, ko pa zahtevajo deregulacijo pa pomeni, da se hočejo obvarovati pred plačevanjem tegob, ki so jih povzročili navadnim državljanom.

[32] Evropska unija (EU) s 493 milijoni prebivalcev predstavlja denimo evropski blok, med ZDA, Kanado in Mehiko nastaja tako imenovana Severnoameriška unija (NAU), Latinska Amerika pa je s sprejetjem ustanovne listine UNASUR naredila korak k združevanju po vzgledu EU-ja, kar pomeni, da bomo imeli na teh koncih sveta tri trgovsko-politične entitete (EU, NAU, UNASUR), katerih rezultat bo verjetno združitev vseh treh trgov. K tem trem trgom se bo verjetno pridružila rastoča in vse močnejša Vzhodna Azija, tako da lahko v prihodnosti pričakujemo neke vrste globalno integracijo gospodarstev (Sigurdson 1992, 5).

prevzemajo – a je še nekaj časa ne bodo popolnoma prevzeli – subjekti iz zasebnega sektorja (Svete 2002, 23; 2005, 25).[33] Država se mora tovrstne institucionalne demonopolizacije zavedati in jo sprejeti kot dejstvo, vendar pa mora varnost še naprej obravnavati kot pravno kategorijo in zagotavljali ustavnopravno zavarovanje in nedotakljivost človekovih pravic z ustreznimi normativnimi mehanizmi (Bučar 1997, 4). Po besedah Sveteta (2005, 25) *»legitimnost sodobne države in njene politike zato izvira iz njene funkcije kot ponudnika javnega dobra«*.

Že nekaj časa velja splošno dejstvo, da vlade same ne določajo več, če sploh kdaj so v celoti, kakšno vrsto varnosti potrebujejo ljudje, katerim vladajo. Nedržavni subjekti, kot so podjetja, nevladne organizacije in posamezni državljani, se vse bolj zavedajo svojih potreb po varnosti, ki pomeni temelj za uresničevanje spet drugih potreb, in tako posledično sami izbirajo tiste subjekte in načine, ki jim bi jo tako ali drugače zagotavljali (Crawford 2006, 111; Pečar 1997, 13).[34] Potrebe po varnosti pa naraščajo *»hitreje, kot pa bi mogla država s svojim načinom delovanja zadostiti povpraševanju po tej dobrini«* (Bučar 1997, 7). Varnost danes pojmujemo kot blago oziroma dobrino, do katere ima vsak posameznik podobno kot do kake druge dobrine pravico, kar tudi pomeni, da se lahko državljani ukvarjajo z zagotavljanjem varnosti podobno kot s proizvodnjo drugega blaga oziroma storitev, ki so predmet ponudbe in povpraševanja kot katerekoli druge storitve (Bučar 1997, 6).

Novejše zgodovinske in sociološke raziskave so razkrile kompleksno mrežo zasebnih in hibridnih agencij, ki so vedno soobstajale z državo in izkoriščale fleksibilnost trga ter zadovoljevale nepotešene potrebe po varnosti. Les Johnston (v Dupont in Wood 2006, 241) govori o porastu velikih *zasebnih varnostnih podjetij*, katere sam imenuje »globalni varnostni konglomerati« in kateri igrajo ključno vlogo v »vojni zoper terorizem«. Ti industrijski konglomerati so dejansko korporacije s konvencionalnimi korporacijskimi strukturami, svoje storitve ponujajo v številnih tujih državah ali kar preko spleta, ustvarjajo močne poslovne

[33] Nedržavni akterji so prevzeli vlogo vladanja ne samo nad drugim zasebnim entitetam, temveč do neke mere tudi državi. Zaradi tega država ni nujno hkrati glavni porok ali glavna grožnja (Shearing 2006, 27–28).
[34] Tovrsten fenomen se pojavlja predvsem v bogatejših postindustrijskih družbah, za katere je značilna izjemno visoka razdeljenost tako v pogledu vrednot kot materialnih interesov, kar Bučar (1997, 9) opredeljuje kot *»globalni problem prehoda v novo svetovno-nazorsko paradigmo«*. Večje kot je v neki družbi soglasje o temeljnih vrednotah in manjša kot je interesna razdeljenost, manjša je potreba po varnostni, pa tudi po obveščevalni dejavnosti.

mreže in korporativne vezi, prevzemajo manjša podjetja in imajo prek lobiranja močan politični vpliv (Holmqvist 2005, 4), zato jih tudi imenujemo **transnacionalne korporacije**.[35]

V zvezi z opisano metamorfozo sodobnega sistema nacionalne varnosti in deetatizacijo posameznih državnih vlog govorimo o procesu **privatiziranja (privatizacije) varnosti**.[36] S tem imamo na splošno v mislih **zmanjševanje vloge države pri financiranju, proizvajanju ali distribuciji varnostnih storitev**. V povezavi z zunanjim izvajanjem pa gre za prenos varnostnih funkcij države na zasebne organizacije, konkretneje pa prenos določenih dejavnosti institucij države s področja varnosti na zasebne organizacije s prodajo ali s sklenitvijo pogodbe o zunanjem izvajanju le-teh.[37] Privatizacijo na področju varnosti bi lahko po Zalarju (1997, 40) opredelili kot *»povečanje participacije zasebnega sektorja v državnem sektorju prek nadzorstvenih procesov demonopolizacije in komercializacije, prek povečanja konkurence in s tem profesionalizacije«* zasebnih varnostnih organizacij. Na privatizacijo varnosti ne smemo gledati samo kot na družbeni proces, temveč tudi kot pravico posameznika, saj *»gre za institucionalizirano možnost, da posamezniki s svojim delom prisvajajo dobrine zunanjega sveta«* (Zalar 1997, 41). Privatizacija varnosti prinaša več tržišča, manjšo porabo državnega denarja, manj vmešavanja države in prepuščanje nekaterih dejavnosti v zunanje izvajanje nedržavnim subjektom, ki jih opravljajo na drugačen način in

[35] Pojem »transnacionalna korporacija« se nanaša na ekonomsko entiteto, ki deluje v več kot eni državi, ali skupino ekonomskih entitet, ki delujejo v dveh ali več državah, ne glede na njihov pravni status v domači državi ali v državi, kjer delujejo (Johnston 2006, 35–36).

[36] Veliki slovar tujk (Tavzes 2006, 925) opredeljuje pojem »privatizacija« takole: **privatizácija** -e *ž* [angl. *privatization* iz lat. *privatus* zaseben iz lat. *privare* vzeti komu kaj] **1.** prisvajanje, jemanje za svoje; **2.** pojmovanje, da je kaka javna funkcija zasebna stvar posameznika, ki jo opravlja; **3.** postopek pretvarjanja državne in družbene lastnine v zasebno lastnino fizičnih in pravnih oseb. Iz prvih dveh opredelitev bi lahko v povezavi z državnimi organizacijami s področja varnosti govorili o prisvajanju oziroma uzurpaciji s strani oblasti, kot se je to denimo dogajalo v času med obema vojnama v Nemčiji, Italiji in Sovjetski zvezi, ko so partijski voditelji zlorabljali obveščevalne službe v namene krepitve osebne oblasti. Če pa izhajamo iz tretje opredelitve, lahko za izhodišče vzamemo Zalarjev (1999, 21–22) koncept o »razdržavljenju«, znotraj katerega se izvajajo procesi prenosa bodisi državne lastnine ali določenih funkcij države na zasebne fizične in pravne osebe. Privatizacija kot proces razdržavljanja na splošno pomeni **zmanjševanje vloge države pri financiranju, produciranju ali distribuciji določenih dobrin oziroma storitev**. Iz tega lahko sklenemo, da privatizacija, kot večplasten pojem, konkretno pomeni (1) prenos storitev, ki so pripadale javnemu sektorju (državna uprava je del javne uprave, ta pa je del javnega sektorja) na zasebne organizacije s sklenitvijo pogodbe o zunanjem izvajanju dejavnosti in (2) kot prevzemanje določenih dejavnosti državnih institucij s strani zasebnih poslovnih subjektov z ustanavljanjem lastnih pravno-organizacijskih oblik znotraj zasebnega sektorja, ki to dejavnost opravljajo v skladu z domačo zakonodajo

[37] Privatizacijo moramo razlikovati od zunanjega izvajanja (angl. outsourcing). Glavna razlika med zunanjim izvajanjem storitev in privatizacijo pa je v *nadzoru*; pri privatizaciji je popoln nadzor nad storitvami prenesen na zasebno organizacijo, medtem ko so pri zunanjem izvajanju prenesene samo storitve, nadzor, vključujoč vodenje in sprejemanje odločitev, pa ne (Cubberley in Skrzeszewski 1999, 3–4).

za denar. Varnostno tržišče pa prinaša tudi *»krizo zakonitosti, boj za obstanek, nelojalno konkurenco, vdiranje v zasebnost in kršitve človekovih pravic«* (Pečar 1997, 15).[38]

Vzpon sodobne zasebne varnostne industrije[39] se je začel v zgodnjih devetdesetih letih prejšnjega stoletja s pojavom zasebnih varnostnih podjetij z jasno korporativno organizacijsko strukturo. Temu vzponu so botrovali številni razlogi. Miyazava (v Zalar 1997, 46) vidi vzpon varnostne industrije kot naravno posledico velike akumulacije korporativnega kapitala, ki zahteva posebno zaščito. Caroline Holmqvist (2005, 2) pa izpostavi slednje kot najpomembnejše dejavnike razvoja zasebne varnostne industrije:

(1) *dominantna vloga svobodnega trga* po hladni vojni, ki je dala zagon močnemu trendu zunanjega izvajanja (angl. outsourcinga) tradicionalno državnih funkcij;
(2) *zmanjševanje obsega nacionalnih vojská* po svetu, ki je za sabo pustilo ogromno število bivšega osebja iz vojske in drugih državnih institucije;
(3) *postopen umik velikih sil* iz številnih držav v razvoju po hladni vojni in posledičen porast števila propadlih držav.

Medtem ko so omenjeni razlogi odigrali ključno vlogo pri tem procesu »privatiziranja varnosti«, se razlage za vzpon varnostne industrije razlikujejo znotraj različnih varnostnih kontekstov.[40] Bolj kot je država nemočna v upiranju nevarnostim in grožnjam, večji je razmah zasebnih varnostnih storitev, ki postajajo nadomestilo za tisto, kar zamuja država (Pečar 1997, 20). To je še posebej značilno za šibke ali propadajoče države, kjer se posamezniki in/ali organizacije obračajo na zasebne subjekte zaradi pomanjkljivega delovanja ali odsotnosti delovanja varnostnih institucij države, s čimer zasebne varnostne organizacije zgolj zapolnijo nastali »varnostni vakuum«. V nasprotju s propadajočimi državami pa je situacija v močnih

[38] Kot alternativo pojmu »privatizacija« pa Kevin R. Kosar (2006, 23) znotraj konteksta omenjenih sprememb navaja pojem »marketizacija«, ki pomeni strategijo menedžmenta s katero poskušajo vodilni raje izboljšati delovanje neke državne agencije kot pa zamenjati jo z zasebno organizacijo. Za ta koncept se včasih tudi uporablja pojem »komercializacija«. Na splošno gledano pomeni marketizacija prevzem metod in vrednot trga za vodenje dejavnosti.

[39] Zasebno vojaško in varnostno industrijo običajno poimenujemo kar s splošnim pojmom »zasebna varnostna industrija«.

[40] Drugi avtorji s tega področja vidijo pojav zasebnih varnostnih storitev kot logično nadaljevanje privatizacije proizvodnje vojaške opreme (vojaške industrije) v Evropi in Severni Ameriki. Kot primer lahko navedemo, ko podjetja, ki prodajajo vojaško opremo in orožje, hkrati ponujajo storitve, kot so vzdrževanje orožje ali usposabljanje z njim (Krahmann v Holmqvist 2005, 2). Schreier in Caparini (2005, 4–5) denimo navajata tudi vpliv sprememb strateške in tehnološke narave, ki so jih vzpodbudile Zalivska vojna in vojne na Balkanu v devetdesetih letih 20. stoletja. V omenjenih konfliktih smo lahko bili priča uporabi vrhunske tehnologije, ki pa je pronicala v vojaške strukture predvsem iz zasebnega sektorja. Ravno zaradi sofisticiranosti oborožitvenih sistemov in napredne tako imenovane »poveljuj in nadzoruj« (angl. command and control) računalniške opreme, so zahteve po strokovnjakih iz zasebnega sektorja bistveno večje.

ali tako imenovanih »učinkovitih« državah drugačna, saj tukaj zasebni akterji delujejo suplementarno v odnosu do funkcij varnostnih institucij države oziroma so le-tem v podporo (Krahmann v Holmqvist 2005, 2–3).

Po mnenju soustvarjalcev zbornika *Democracy, Society and the Governance of Security* (Wood in Dupont 2006) je najbolj problematičen vidik privatizacije na področju varnostnih storitev *fragmentacija*, ki se pojavlja v obliki vključevanja in izključevanja. Članstvo v »varnostnem klubu« zagotavlja dostop do boljše in kakovostnejše varnosti, hkrati pa zagotavlja tudi, da so »tvegane populacije« zadržane na pravšnji distanci.[41] Ta ekskluzivna ekonomija varnosti izvira iz deficita demokracije, ki spodkopava oboje, sposobnost državne politike, da ponudi tako javno dobro kakor tudi, da si deli skupno usodo z posameznimi družbenimi skupinami. Loader in Walker pri tem pa opozarjata, da varnost ne sme biti dobrina peščice v izolaciji od ostalega predela družbe, saj s tem rojeva pogoje še večje nevarnosti (glej Dupont in Wood 2006, 241–242). Zalar (1997, 40) poudarja, da *»vsi pojavi izločanja – bodisi »navzgor« bodisi »navzdol« – delujejo dezintegrativno in niso v službi splošne blaginje«*, zato v takem družbenem stanju ne moremo govoriti niti o varstvu načela enakosti niti načela svobode.

4.3.1 Zunanje izvajanje varnostnih storitev

Ko govorimo o delegiranju varnostnih storitev iz državnega v zasebni sektor, imamo v mislih **zunanje** (pogodbeno) **izvajanje varnostnih storitev** (angl. **outsourcing** ali contracting out).[42] Na splošno lahko *outsourcing* definiramo kot **prenos nekdaj notranjih dejavnosti oziroma storitev organizacije na zunanjega izvajalca**.[43] Na področju varnostne

[41] Vendar pa je treba vedeti, da imajo bogatejši večje zahteve po varnostnih storitvah, zaradi česar dobijo od države manj varnosti na enoto, kar predstavlja antagonizem med zasebniško in državno varnostjo, ki se ustvarja na temelju premoženja oz. bogastva, pri čemer nujno odpovedujejo vsa načela enakosti in pravičnosti (Pečar 1997, 18).

[42] Pojem **outsourcing** je angleški kompozitni izraz, sestavljen iz treh angleških besed, in sicer iz »outside« (zunaj), »resource« (vir) in »using« (uporaba), ki s spojitvijo v besedno zvezo »outside resource using« lahko pomeni *uporabljanje zunanjih virov*, vsebinsko natančneje, *zunanje izvajanje dejavnosti*.

[43] Tesno z zunanjim izvajanjem dejavnosti je povezan pojem »zunanje izvajanje nalog« (angl. outtasking), ki pa je nekoliko ožji pojem in pomeni, da najamemo pogodbene izvajalce za izvedbo samo določenih nalog znotraj oddelka ali organizacije, pri čemer ohranjamo nadzor in odgovornost za celoten proces dejavnosti (Roeben 2004, 5–6). Ravno zaradi tega se mi zdi pri »outsourcingu« raba slovenske sintagme »zunanje izvajanje dejavnosti« bolj primerna kot »pogodbeno izvajanje dejavnosti«, katero lahko zasledimo pri nekaterih drugih slovenskih avtorjih. Prav tako se mi zdi za izvajalca dejavnosti bolj smiselna raba izraza »zunanji izvajalec« kot »pogodbenih izvajalec« ali samo »pogodbenik«. Poleg omenjenega in iz razlogov povezanih z delojemalci, ki sklepajo pogodbe o delovnem razmerju z delodajalci, je »pogodbenik« neprimeren izraz tudi zato, ker če dela ne

dejavnosti torej država ohrani odgovornost za financiranje varnostnih storitev, a najame subjekt iz zasebnega sektorja za izvajanje teh storitev, pri tem pa ohranja *nadzor* nad standardi izvajane funkcije oziroma storitev. Glavno poslovno načelo tega koncepta je, da so zunanji izvajalci sposobni opravljati iste storitve oziroma dejavnosti *bolj učinkovito*. Storitve, ki jih opravljajo zunanji izvajalci običajno ne predstavljajo primarno dejavnost državne institucije in so za to institucijo postranskega pomena (Schreier in Caparini 2005, 97; Chorafas 2003).[44]

Bistvene **prednosti zunanjega izvajanja dejavnosti** so: (1) *povečana funkcionalnost organizacije*, ki prenese določeno dejavnost na zunanjega izvajalca, s tem pa lahko razvija svojo prvotno funkcijo, (2) *zmanjševanje stroškov* organizacije in s tem (3) *ohranjanje ali povečanje kakovosti*, kajti zunanja dela običajno zaupamo strokovnjakov, ki so specializirani za to in svoje področje dela dobro obvladajo, kar pomeni tudi (4) *časovno zagotovitev* izvedbe del, pri čemer je potrebno vedeti, da se zunanji izvajalec s pogodbo zaveže, da bo svoje delo opravil ne le kakovostno, temveč tudi v določenem roku. Pomembna kategorična prednost je tudi (5) *prilagodljivost, fleksibilnost* in večja *sposobnost odzivanja* na spremembe pogojev in zahtev (Chorafas 2003, 5). Pomemben faktor na področju zunanjega izvajanja varnostnih storitev je *konkurenčnost* (tekmovalnost). Ta pospešuje inovativnost, nove tehnike menedžmenta, vpeljavo nove opreme in novih metod dela ter omogoča državi ponovno sklepanje pogodb z različnimi izvajalci in za različne stopnje storitev (Schreier in Caparini 2005, 97).[45]

Zunanje izvajanje dejavnosti pa ima tudi svoje **slabosti**, predvsem z vidika naročnika. V razvitih državah se po mnenju Holmqvistove (2005, 25) na področju zunanjega izvajanja varnostnih storitev pojavljajo štirje ključni problemi: (1) *Problem določitve in sklenitve jasnih mandatov in vloge zasebnih varnostih podjetij*: Sodobna zasebna varnostna podjetja so prilagodljive entitete, ki s prilagajanjem situaciji prevzemajo nove naloge, kar lahko povzroči

---

opravlja glavni zunanji izvajalec, ki je sklenil pogodbo, ampak subjekt, ki ga najame zunanji izvajalec, ne rečemo, da potem delo opravlja podpogodbenik, ampak podizvajalec.

[44] Zunanje izvajanje je zanimivo tudi za ostale gospodarske panoge, zato naročnik ni vedno država. Za zunanje izvajanje se odločajo tudi druga zasebna podjetja in nevladne organizacije, predvsem zaradi nižjih stroškov dela in večje efektivnosti primarne dejavnosti organizacije. Prav tako ni nujno, da je zunanji izvajalec zasebno podjetje, saj lahko določene dejavnosti bolje opravljajo tudi javne ali hibridne agencije.

[45] Vendar pa lahko po drugi strani zaradi »prevelike« konkurenčnosti nastane problem že pri razpisu, ko eden izmed ponudnikov sprva ponudi svoje storitve »po najugodnejši ceni« in s tem lažje dobi pogodbo pred dražjimi ponudniki. Zatem, ko se dobitnik pogodbe otrese konkurence in ko naročnik zaupa svoje storitve novem izvajalcu, pa se lahko zgodi, da se slednji začne znova pogajati za višjo ceno. Zaradi tega naročnik (država) postane odvisna od privatnega monopola, kar na dolgi rok pomeni višje in dodatne stroške, pomanjkanje dinamike in slabšo kakovost storitev (Hartley v Schreier in Caparini 2005, 100).

pomanjkanje nadzora nad delovanjem teh podjetij. Čeprav je s pogodbami skoraj vse določeno, se te večinoma ne spuščajo v podrobnosti dela zunanjega izvajalca, zaradi česar lahko ta podjetja opravljajo naloge in uporabljajo sredstva, ki niso bila predvidena s pogodbo.[46] V takih pogodbah je treba jasno določiti, kaj je in kaj ni sprejemljivo (Holmqvist 2005, 25–26); (2) *Pomanjkanje odgovornosti zasebnih varnostnih podjetij*: Odgovornost posameznikov za nezakonito opravljanje storitev, vojne zločine ali poseganje v človekove pravice lahko hitro postane odgovornost vlade, tako tiste, katera je sklenila pogodbo, kot tiste, ki ima oblast na območju, kjer podjetje deluje.[47] Takšen je »primer Abu Ghraib« (Holmqvist 2005, 27–28);[48] (3) *Problem transparentnosti in nadzora nad zunanjimi izvajalci*: Večina glavnih menedžerjev v zasebnih varnostnih podjetij je dobro povezanih med sabo in z vladnimi uradniki. Zato je za ta podjetja značilno močno politično lobiranje in znatna donatorska podpora v času političnih kampanj, kar pomeni prednost pri dobivanju pogodb in s tem hkrati manjšo transparentnost (Isenberg v Holmqvist 2005, 30).[49] Tako ni nujno, da pogodbe res predstavljajo pravo vrednost in pravega izvajalca.[50] Problem transparentnosti je še toliko večji, ko storitve izvajajo podizvajalci, kar pa je redna praksa večjih varnostnih multinacionalk in pomeni razpršitev odgovornosti ter onemogočanje nadzor nad pravimi izvajalci. Problem v zvezi s transparentnostjo se pojavljajo tudi zaradi finančnih informacij, katere imajo zasebni subjekti pravico varovati (Schreier in Caparini 2005, 102); (4) *Problemi koordinacije znotraj zasebnega sektorja ter med varnostnimi podjetji in redno vojsko*: Integracija različnih virov in interesov pri dolgoročni strategiji je bistvenega pomena. Pri koordinaciji redne vojske in zasebnih varnostnih podjetij v skladu s strateškimi usmeritvami

[46] Ameriško podjetje *DynCorp* je na primer leta 2003 z zunanjim ministrstvom ZDA sklenilo 50 milijonov dolarjev vredno pogodbo, v skladu s katero naj bi zagotovilo 1000 svetovalcev pri organizaciji in pomoči iraškim kriminalistično-preiskovalnim organom in sodnim institucijam. Kasneje se je izkazalo, da so štirje zaposleni iz tega podjetja, ki so sodelovali pri policijskih operacijah na domu in v pisarnah bivšega voditelja Ahmeda Chalabija junija 2004, bili opremljeni s puškami in neposredno vodili policijske operacije, katere s pogodbo niso bile predvidene. Osebje iz taistega podjetja v Iraku sodelovalo tudi v protiuporniških akcijah, čeprav tega pogodba ni predvidevala (Holmqvist 2005, 25–26).

[47] V primeru Iraka imajo pogodbeniki imuniteto pred lokalnimi organi po Odredbi 17 (izdani junija 2003 in obnovljeni 27. junija 2004) (Holmqvist 2005, 27), kot civilisti pa ne morejo biti subjekti niti vojaškega sodišča niti Ženevske konvencije in bi morali, teoretično gledano, biti podrejeni lokalnemu sodstvu (Johnston 2006, 44).

[48] Dober primer neodgovornega ravnanja je primer spolnih zlorab v zaporu Abu Ghraib v Iraku. Pri zlorabah zapornikov v Abu Ghraibu leta 2004 naj bi bila soodgovorna vsaj dva delavca iz ameriških podjetij *CACI International* in *Titan Incorporated*, ki sta v Iraku za ameriško obrambno ministrstvo pogodbeno opravljala storitve, kot sta zasliševanje zapornikov in tolmačenje (Holmqvist 2005, 27–28).

[49] Nekateri viri pravijo, da naj bi bilo med letoma 1998 in 2003 podeljenih le 40 odstotkov vseh pogodb ameriškega obrambnega ministrstva na osnovi »poštene in odprte tekmovalnosti« (Isenberg v Holmqvist 2005, 30). V ZDA namreč obstaja lobistična organizacija *International Peace Operations Association*, ki aktivno podpira interese nekaterih večjih varnostnih podjetij (Johnston 2006, 42).

[50] Glede netransparentnosti predstavlja podjetje *Halliburton* zelo dober primer. *Agencija za revidiranje pogodb o obrambi* je pred kratkim sporočila, da *Halliburton* ni mogel prikazati 42 odstotkov od štirih milijard dolarjev računov, ki so jih poslali na Pentagon, večinoma zaradi podizvajalcev, o katerih pa zaradi poslovne zaupnosti *Halliburton* ne želi govoriti. Kljub temu, *Halliburton* še vedno sklepa pogodbe z vojsko (Johnston 2006, 41–43).

lahko nastanejo težave zaradi razlik v organizacijski kulturi in medsebojnega nezaupanja (Isenberg v Holmqvist 2005, 32). Primer težave pri praktični koordinaciji so pojavi denimo že pri sami identifikaciji oziroma nejasnemu razlikovanju med funkcijami vojakov in varnostnikov, poleg tega pa so nejasne tudi linije poveljevanja in zvez.[51]

Nejasnost procesov sklepanja pogodb in zmedenost pri razlikovanju med civilnim in vojaškim osebjem sta v bistvu povezani s širšimi vladnimi strategijami. Vladi omogočata, da se spretno izogne javno občutljivim in politično spornim situacijam.[52] Zunanji izvajalci varnostnih storitev namreč **niso politično odgovorni** za svoja dejanja ali dejavnost v celoti, kar povzroča resno zaskrbljenost nad spoštovanjem človekovih pravic. Zunanji izvajalci varnostnih storitev prav tako niso subjekti mednarodnega vojnega in humanitarnega prava.[53] Pomembno je, da država v prepuščanju varnostnih dejavnosti posameznim zasebnim organizacijam ne dovoljuje več, kot je v njeni lastni pristojnosti (Pečar 1997, 16).[54]

4.3.2 Zasebna varnostna podjetja

Večina strokovnjakov uporablja besedno zvezo »zasebna varnostna podjetja« kot splošni izraz za vsa zasebna podjetja znotraj varnostne industrije (Holmqvist 2005, 5–6). Kljub pomanjkanju konsenza lahko na splošno opredelimo dva osnovna tipa zasebnih varnostnih podjetij, in sicer (1) *zasebna vojaška podjetja* in (2) *zasebna varnostna podjetja v ožjem smislu*. Nekateri sem pridodajajo tudi tretji tip zasebnih varnostnih podjetij, spet drugi pa ponujajo drugačno tipologijo znotraj varnostne industrije.[55] Najemniški vojaki, paravojaške

[51] Osebje ameriških zasebnih varnostnih podjetij lahko uporabi orožje samo v samoobrambi ter pri zaščiti konvojev in osebja (Johnston 2006, 45).
[52] To še posebej velja za ZDA, kjer kongres niti ne prejema dokumentov o pogodbah, ki so vredne manj kot 50 milijonov USD, Pentagon pa ne ve niti podatkov, koliko ljudi plačuje preko zasebnih podjetij. S tem obstaja verjetnost, da se varnostnike mobilizira v »vojaških zadevah« brez vednosti kongresa in javnosti, kot se je to recimo dogajalo v Kolumbiji v »vojni proti drogam« (Johnston 2006, 45–46).
[53] Uslužbenci zasebnih vojaških in varnostnih podjetij denimo niso zaščiteni v skladu s 3. Ženevsko konvencijo, ker ne nosijo redne uniforme in niso del vojaške hierarhije in strukture poveljevanja, zatorej niso dolžni delovati v skladu s konvencijami. Te prav tako ne moremo opredeliti kot najemnike, saj definicija za najemnike pravi, da morajo delati za tujo vlado na konfliktnem območju, v katerem njihova država ne sodeluje, kar se v primeru ZDA v Iraku izkaže za pravno neskladnost (Schreier in Caparini 2005, 56–57).
[54] Iz vidika uporabnika/naročnika pa sta najpomembnejša faktorja pri izbiri zunanjega izvajalca **zaupanje** in **varnost** (posla), brez teh dveh je odnos »naročnik – ponudnik« obsojen na propad. Temu odnosu morajo potem slediti dober nadzorni sistem, ki nam omogoča pregled nad delom in stroški, ter strokovno opravljeno delo.
[55] Michael Page in drugi (2005, 2) opredeljujejo še tretji tip zasebnih varnostnih podjetij, imenovan »ponudniki nesmrtonosnih storitev« (angl. Non-lethal Service Providers). Zanimivo tipologijo po vojaški analogiji ponuja tudi Peter Warren Singer, ki pravi, da znotraj varnostne industrije obstajajo trije tipi zasebnih vojaških firm: (1) *vojaške izvajalske firme* (angl. Military Provider Firms), ki ponujajo bojne storitve, (2) *vojaško-svetovalne firme*

grupacije, warlordi, prostovoljci iz tujine, obrambno-industrijska podjetja in drugi ne spadajo v varnostno industrijo. Tipologija s tremi ali več tipi zasebnih varnostnih podjetij ni del splošnega strokovnega konsenza, zato je uporaba takšne tipologije neprimerna.

Zasebna vojaška podjetja so po definiciji Scotta Goddarda (v Schreier in Caparini 2005, 18) *»registrirana civilna podjetja, ki so specializirana za pogodbeno izvajanje vojaškega usposabljanja (inštrukcij in simulacijskih programov), vojaških podpornih operacij (logistične podpore), zagotavljanje operativnih zmogljivosti (svetovanja posebnim enotam, vodenja in poveljevanja, vzpostavitve in vzdrževanja komunikacij, ter izvajanja obveščevalnih funkcij), in/ali zagotavljanje vojaške opreme legitimnim domačim ali tujim entitetam«*. Zasebna vojaška podjetja so lahko tako transnacionalne korporacije kot tudi manjša podjetja.[56] **Zasebna varnostna podjetja v ožjem smislu** pa Goddard (v Schreier in Caparini 2005, 26) definira kot *»registrirana civilna podjetja, ki so specializirana za pogodbeno izvajanje komercialnih storitev za domače in tuje in entitete z namenom zavarovati osebje in humanitarno ter industrijsko premoženje v okviru predpisov domače zakonodaje«*. Pravimo, da zasebna varnostna podjetja v ožjem smislu ponujajo *defenzivne storitve*, medtem ko zasebna vojaška podjetja opravljajo *ofenzivne storitve*.[57]

Zasebna varnostna podjetja v ožjem smislu ločimo tudi po geografskem načelu, na tista, ki delujejo *doma*, in tista, ki delujejo *v tujini*. Delujoča doma kategorično delimo v tri sektorje: (1) *sektor varovanja* (angl. guarding sector), ki zaposluje varnostnike različnih objektov (letališča, nakupovalni centri, športne arene, parkirišča itd.); (2) *elektronski varnostni in nadzorstveni sektor*, ki vključuje alarmne, detektorske in nadzorne sisteme (nadzor poteka preko opreme); (3) *sektor preiskovanja in kriznega menedžmenta*, kamor štejemo zasebno preiskovanje (detektivska dejavnost), kriminalistično preiskovanje, varovanje pomembnega osebja in svetovanje pri kriznem menedžmentu, zasebno in industrijsko vohunjenje, obveščevalno in protiobveščevalno dejavnost (Van Bergen Thirion v Schreier in Caparini 2005, 27). V tretji sektor lahko prištevamo tudi **zasebna obveščevalna podjetja** (agencije, službe), ki se kot zasebna podjetja ukvarjajo s pridobivanjem in analizo

(angl. Military Consulting Firms), ki ponujajo svetovanje in storitve usposabljanja ter (3) *vojaške podporne firme* (angl. Military Support Firms), ki opravljajo podporne in logistične naloge (Singer v Holmqvist 2005, 5).

[56] Večina teh podjetij je slamnatih, ki ne vzdržujejo svojih sil, ampak skrbijo za podatkovne baze kvalificiranega osebja in specializiranih podizvajalcev.

[57] Ta razlika med tipoma je vedno bolj meglena, saj imajo nekatera podjetja karakteristike obeh tipov, prav tako lahko isto osebje dela v obeh tipih podjetij. Nekatera vojaška podjetja se skrivajo pod imenom »varnostna«, varnostna pa pod »svetovalna«, da bi tako pritegnila manjšo pozornost medijev (Lilly 2000, 14).

podatkov iz večinoma javno dostopnih virov in v sodelovanju z drugimi strokovnimi institucijami (obveščevalno dejavnostjo odprtih virov), nato pa končne obveščevalne informacije uporabljajo v komercialne namene.[58]

Naročniki storitev zasebnih varnostnih podjetij so predvsem (1) vlade v konfliktnih regijah, (2) vlade, ki podpirajo vlade v konfliktnih regijah, (3) nadnacionalne multilateralne organizacije z nalogami ohranjanja miru, (4) humanitarne organizacije, (5) korporacije in podjetja ter (6) nedržavni oboroženi akterji (Lilly 2000, 15–20).[59]

Poleg omenjenih konvencionalnih dejavnosti na področju varnosti, so zasebna varnostna podjetja prevzela tudi bolj specifične funkcije; recimo izvajanje policijskih nalog[60] in upravljanje s kriminalom.[61] Ena izmed pomembnih nalog, ki jo izvajajo predvsem zasebna varnostna podjetja v ožjem smislu, je tudi *napovedovanje poslovnih tveganj* in podpora pri zmanjševanju škode, ki nastane pri teh tveganjih. Za ta podjetja je značilna **komodifikacija informacije** oziroma pretvorba nekomercialne informacije v komercialno. Več o dejavnostih in storitvah zasebnih varnostnih podjetij, ki jih izvajajo na tujem, naročnikih teh storitev in primerih podjetij, ki te storitve ponujajo, je prikazano v spodnji tabeli (glej Tabelo 4.1).

[58] Takšno podjetje je denimo *Kroll*, ki se ukvarja med drugimi s poslovno obveščevalno dejavnostjo, elektronskim odkrivanjem, upravljanjem s podatki, detektivsko dejavnostjo in drugimi varnostnimi storitvami (Johnston 2006, 35–36).

[59] Večina zasebnih varnostnih podjetij zatrjuje, da sodelujejo zgolj z mednarodno priznanimi vladami. Vendar pa obstajajo domneve, da naj bi podjetje *Sandline International* leta 1998 izrazilo željo oborožiti in pomagati Osvobodilni vojski Kosova v boju s Srbi. Takšnih primerov je kajpak še več (Goulet v Lilly 2000, 15).

[60] Les Johnston (v Bayley in Shearing 2001) pravi, da zasebni ponudniki varnostih storitev izvajajo skorajda vse naloge, ki so bile nekoč v celoti v domeni državne policije, kar vključuje patruljiranje, straženje, preiskovanje, izboljševanje pogojev za pregon kriminala, svetovanje na področju preventive, nadziranje neurejenih situacij in drugo. Privatni izvajalci tako imenovanih »policijskih nalog« (angl. policing) imajo veliko prednost pred državnimi, in sicer, oni lahko izbirajo, katere naloge bodo opravili in katere ne, medtem ko državni organi ne morejo izbirati in morajo zagotavljati opravljanje policijskih nalog na vseh ravneh in v vseh primerih. Gre za obveznost, ki se sčasoma porazdeljuje med zasebni in državni sektor. Shearing in Stenning govorita tukaj o različnih mentalitetah, kajti zasebno opravljanje policijskih nalog izraža drugačno mentaliteto kot državno. Obstaja konsenz, da je zasebno opravljanje policijskih nalog usmerjeno bolj v preprečevanje kriminala kot pa samo sankcioniranje zanj (Bayley in Shearing 2001).

[61] Pojavili so se tudi komercialni zapori in centri, ki se poslovno ukvarjajo s tako imenovanimi »prebivalstvenimi problemi«. V Veliki Britaniji že od leta 1970 vodi Britanski center za priseljence podjetje *Group 4 Falck*. V zadnjem obdobju so se v ZDA in drugih državah začeli uveljavljati tudi posebni programi kot je recimo britanski program imenovan *Zasebna finančna iniciativa* (PFI), ki predstavljajo nov zagon komercialne dejavnosti v zaporniškem sistemu. V ZDA je 6,5 % zveznih in državnih zapornikov v zasebnih zaporih, v Veliki Britaniji 9%, v Avstraliji pa okoli 18%. Kljub temu, pa je največ – kar 120.000 – zapornikov v zasebnih zaporih ravno v ZDA. *The Corrections Corporation of America*, ki deluje s 59. zapori v dvajsetih državah, nadzira skoraj polovico tega segmenta trga (Johnston 2006, 38–39).

Tabela 4.1: Primerjava dejavnosti zasebnih vojaških podjetij in zasebnih varnostnih podjetij v ožjem smislu, ki delujejo v tujini

Dejavnosti in storitve	Naročniki	Primeri
ZASEBNA VOJAŠKA PODJETJA		
Svetovanje: (1) pri reformiranju in prestrukturiranju oboroženih sil ter vzpostavljanju demokratičnega nadzora nad oboroženimi silami; (2) strokovna pomoč obrambnim ministrstvom na področju obrambnega načrtovanja, kakor tudi pri dobavi orožja in opreme; (3) pri vzpostavitvi sistemov vodenja in poveljevanja, razvoju doktrin; (4) strateško, operativno in taktično načrtovanje.	Vlade, pristojni resorji	MPRI, Vinnel, Cubic, Strategic Communications Labrtories
Usposabljanje (glavna dejavnost teh podjetij): vojaško usposabljanje, usposabljanje specialnih enot, izobraževanje častnikov, posebno protiteroristično usposabljanje.	Vlade, oborožene sile	Executive Outcomes, MPRI, Blackwater
Logistična podpora (najbolj razširjena): (1) pomoč pri dostavi humanitarne pomoči; (2) namestitev in vzdrževanje vojašnic, taborišč (begunskih in vojaških); (3) dostava dnevne prehrane; (3) dostava pošte, (4) prečiščevanje vode; (5) prevoz trupel v domovino; (6) prevoz uradnikov; (7) dostava goriva na kopnem in v zraku; (8) zagotavljanje IT opreme in administriranje omrežij.	Vlade, oborožene sile, humanitarne organizacije, OZN	MPRI, Kellog Brown & Root, DynCorp, EGL, Pacific A&E, Omega Air Inc
Vzdrževanje: tehnična podpora in vzdrževanje sodobnih oborožitvenih sistemov, popravilo opreme in orožja.	Oborožene sile	Textron
Obveščevalna dejavnost, izvidništvo, nadzor: (1) zagotavljanje komercialnih informacij; (2) analize konkurenčne obveščevalne dejavnosti; (3) sledenje in nadzorovanje preprodajalcev drog; (4) nadzorovanje meja; (5) zračni nadzor; (6) tolmačenje in prevajanje pri operacijah in zasliševanjih.	Oborožene sile	Diligence LLC, Trident, CACI, DynCorp, BMD
Demineriranje: (1) čiščenje kasetnih bomb, neeksplodiranih teles, min; (2) svetovanje in izobraževanje o tveganju; (3) uničevanje eksploziv.	OZN	Ronco Consulting Corp, Demex Services
ZASEBNA VARNOSTNA PODJETJA V OŽJEM SMISLU (v tujini)		
Svetovanje: (1) ocenjevanje tveganosti in varnostno planiranje za lego rudnikov in izkoriščanje energije; (2) svetovanje in asistenca pri aktivnostih povezanih z varnostjo, usposabljanjem, logistiko, organizacijo.	Humanitarne organizacije, korporacije	Control Risks Group, Secopex, DynCorp
Usposabljanje: (1) lokalnih varnostnih sil v reševanju talcev, varovanju infrastrukture in ljudi, kriznem menedžmentu; (2) lokalne policije.	Vlade, varnostne sile	TASK International
Obveščevalna dejavnost: (1) zagotavljanje ocen tveganj; (2) protiobveščevalna dejavnost; (3) nadzor nad prisluškovanjem, (4) zračni nadzor.	Vlade, korporacije, oborožene sile, OZN	Northbridge Services Group Ltd., Rubicon International
Varovanje ključnih lokacij in štabov: (1) varovanje administrativnih objektov, letališč; (2) odkrivanje eksploziv s psi; (3) varnost za vladne in zasebne operacije.	Vlade, korporacije	ITT, Blackwater, Diligence LLC, Custer Battles
Varovanje kritične infrastrukture: (1) naftnih polj in naftovodov; (2) električne napeljave; (3) obalne in varnostne infrastrukture.	Vlade, korporacije, oborožene sile	Erinys International, Hart Group Ltd.
Varovanje konvojev in humanitarne pomoči: (1) razvoz denarja; (2) varovanje konvojev skozi tvegana območja; (3) varovanje vladnih predstavnikov, predstavnikov humanitarnih in nevladnih organizacij, podjetij.	Vlade, nadnacionalne organizacije, OZN, korporacije	Control Risks Group, Genric Ltd., Northbridge Service Group
Osebna varnost in spremstvo za VIP in visoke uradnike: (1) predsednikov in voditeljev držav; (2) kraljevih družin; (3) humanitarnih delavcev; (4) poslovnežev.	Vlade, OZN, humanitarne organizacije, korporacije	DynCorp, Blackwater Security Consulting, Kroll

Vir: Schreier in Caparini 2005, 23-25; 31-33.

Raziskave, ki so jih opravili desetletje nazaj, so ovrednotile ameriški trg varnostnih storitev na približno 37,9 milijarde ameriških dolarjev (USD) v letu 1990, medtem ko je tovrstni trg v Evropi v letu 1992 predstavljal le 19,9 milijarde USD.[62] Skupno sta ta dva trga predstavljala 57,8 milijarde USD. Danes je globalni trg varnostnih storitev, brez storitev svetovanja in ostalih preiskovalnih storitev, ocenjen na okoli 111,6 milijard USD, pri čemer tretjino celotnega globalnega trga predstavljajo ZDA, nekaj več kot dve petini pa EU (Johnston 2006, 36–37).[63] Do leta 2010 naj bi ob povprečni letni 7-odstotni rasti trg zrasel na dobri 202 milijardi USD (Holmqvist 2005, 7). Pomembno pa je omeniti, da najvišja letna rast na trgu varnostnih storitev (nekje okoli 10 do 11 odstotkov) ni v Evropski uniji ali v ZDA, temveč zunaj teh držav.

Kot rečeno je pomemben dejavnik konkurenčnosti zasebnih varnostnih podjetij tudi *zaposleni kader*, ki ga predstavljajo predvsem nekdanji uslužbenci oboroženih sil, policije, obveščevalnih služb, varnostnih služb ter drugih državnih varnostnih institucij.[64]

5 PRIVATIZACIJA OBVEŠČEVALNE DEJAVNOSTI: FENOMEN NOVE OBVEŠČEVALNE PARADIGME

Obveščevalna dejavnost posameznikov in zasebnih organizacij ni fenomen, ki bi vzklil z vzponom sodobne varnostne industrije v devetdesetih letih 20. stoletja. Tovrstno dejavnost so omenjeni subjekti opravljali že v daljni preteklosti, tudi v okviru vojaških in varnostnih organizacij. Dejansko lahko rečemo, da je do pravno-formalne institucionalizacije državnega obveščevalna aparata v Angliji konec 17. stoletja bila obveščevalna dejavnost (v širšem ali ožjem smislu) v domeni vladarjev in njihovih »vohunov«, trgovcev in popotnikov ter duhovščino. Po tem obdobju se je obveščevalna služba le še krepila, vendar pa obveščevalna dejavnost ni nikoli v celoti ostala v domeni države.

Ko govorimo o obveščevalni dejavnosti v obdobju od konca druge svetovne vojne pa nekje do padca berlinskega zidu in pogojno[65] do terorističnih napadov 11. septembra 2001 v

[62] Raziskava je omejena na naslednje evropske države: Francija, Nemčija, Italija, Španija in Velika Britanija.
[63] Podatek se nanaša na leto 2006. Avtor pa za to leto navaja, da je globalni trg varnostnih storitev vreden okoli 60 milijard angleških funtov, kar je po povprečnem letnem menjalnem tečaju iz leta 2006 pomenilo, da je bil 1 funt vreden 1,86 ameriškega dolarja.
[64] Zaradi boljših plačil se je veliko bivših pripadnikov britanskih posebnih sil SAS odločilo delati v zasebnih vojaških podjetjih, saj lahko ti zaslužijo kar 1.000 funtov dnevno, nekdanji komandosi pa lahko zaslužijo kar sedemkrat več kot njihovi bivši kolegi zdaj zaslužijo v Iraku (Johnston v Wood in Dupont 2006, 42).

ZDA, imamo v mislih obdobje *stare obveščevalne paradigme*, ki je uspešno parirala varnostnim razmeram znotraj bipolarne politične konstelacije. Glavne kategorične značilnosti te konzervativne doktrine so:

- **Obstoj enega in glavnega sovražnika**. Vse aktivnosti obveščevalnih in obveščevalno-varnostnih služb so bile uperjene proti enemu glavnemu sovražniku, ki ga je v primeru ZDA predstavljala Sovjetska zveza z zaveznicami, in obratno. Države zaveznice so temu fokusu sledile in podpirale obveščevalne aktivnosti ideološko sorodne velesile (Steele 2002a; George 2007; Treverton 2003, 98).
- **Prednostna uporaba tehničnih sredstev**. Obveščevalna dejavnost se je zanašala na tajna in zelo draga tehnična sredstva za pridobivanje podatkov, kot so recimo sateliti in napredna izvidniška letala s kamerami, zaradi česar sta se intenzivno razvijali satelitska in slikovna obveščevalna dejavnosti. Uporaba tehničnih sredstev je zasenčila HUMINT (Steele 2002a; Encyclopaedia Britannica 2008, »intelligence«).
- **Poudarek na tajnih podatkih in metodah**. Glavni pomen se je pripisoval tajnim virom in tajnim podatkom, pridobljenih s tajnimi metodami. Sovjetska zveza je bila »zaprta družba« in zato so ameriške obveščevalne informacije temeljile predvsem na tajnih – »zaprtih« – podatkih. Obveščevalna dejavnost je bila tako usmerjena v pridobivanje tajnih vojaških podatkov oziroma skrivnosti, v varovanje lastnih virov in metod ter v preprečevanje, da bi nasprotnik dostopal do vojaških tajnih podatkov (Treverton 2003, 221; George 2007; Steele 2002a).
- **Ločenost in centraliziranost zbiranja in analize podatkov**. Ker so obveščevalne in obveščevalno-varnostne službe pridobivale s pomočjo tehničnih virov »omejene« podatke, sta bila zbiranje in analiza teh podatkov dve ločeni nalogi, opravljeni s strani ločenih skupin. Analiza in zbiranje podatkov sta bila relativno centralizirana (Treverton 2003, 221).
- **Zaprta narava obveščevalnih organizacij**. Ta je rezultat naslanjanja na tajne vire. Zaprta narava in tajnost znotraj obveščevalnih organizacij strmita k temu, da bi ločila organizacijo fizično, intelektualno in emocionalno od procesa odločanja. Zaradi zaprtosti obveščevalnih služb tudi do sodelovanja z zunanjo stroko ni prihajalo, še

[65] Pogojno zato, ker so se do takrat uporabljale še vedno iste metode in sredstva, medtem ko so bili na vidiku že novi koncepti delovanja.

posebej pa se je ta zaprtost pokazala v ločenosti obveščevalnih služb od oblikovalcev politik (George 2007; Agrell 1992, 104).[66]

- **Pomanjkanje kreativnosti in inovativnosti**. Tovrstno pomanjkanje je rezultat zaprte organizacije. Posledica tega so bili nastajajoči problemi pri obveščevalni analizi. Obveščevalna kultura, ki temelji na hierarhični ureditvi in tajnosti, strmi k omejevanju prostega pretoka idej ter omejevanju pluralizma in odprte kritike, ki so osnovna načela znanosti, novinarstva in politike (Agrell 1992, 104).
- **Ozko definiran krog uporabnikov informacij**. Skozi čas hladne vojne so bili glavni naročniki in uporabniki obveščevalnih informacij uradniki vlade, ki so bili del ozko definiranih vojaških in političnih zadev (Treverton 2003, 221).
- **Usmerjenost v končne obveščevalne produkte**. Naročniki (posledični uporabniki) obveščevalni informacij so se osredotočali zgolj na gola dejstva in dokončne obveščevalne produkte, ki pa so zaradi skoposti informacij lahko bili nepopolni (George 2007).[67]
- **Ločenost med notranjo in zunanjo obveščevalno dejavnost** (Treverton 2003, 224).[68]

Sodobno okolje danes spodkopava prav vse atribute stare obveščevalne paradigme, to pa se bo še toliko bolj dogajalo v prihodnosti, čemur se ne bo izognila nobena država. V obdobju hladne vojne takšen koncept obveščevalne dejavnosti ni bil slab, vendar pa je slab za dandanašnje razmere, (1) ko se morajo obveščevalne službe osredotočiti na **več groženj**, (2) ko imajo **več naročnikov** obveščevalnih informacij, saj med naročnike (uporabnike) že lahko štejemo podjetja in tuje vlade, (3) in ko **tajni podatki ne zagotavljajo več monopolnega položaja** (Treverton 2003, 220–221; 232).[69] Obveščevalna dejavnost ni več izključno državni monopol, ker tudi glavni akterji v sodobnem okolju niso več države, kar sovpada z zatonom tradicionalnega koncepta države kot edinega poroka varnosti. Govorimo o porazu stare obveščevalne paradigme in rojstvu **nove obveščevalna paradigme**, ki jo poleg novih konfliktov zaznamujejo še informacijska revolucija in pomembna vloga odprtih virov, večja zmožnost prenosa podatkov in informacij, »odprtje« obveščevalnih skupnosti, ekonomičnost

[66] Veliko obveščevalnih zmot, ki so vodile do nerazumevanja in napačnih interpretacij, je v bistvu posledica nezmožnosti povezave dveh kultur (Agrell 1992, 104).
[67] Zgodovina hladne vojne je večji meri zgodovina zaključkov, izpeljanih na podlagi zavajajočih obveščevalnih informacij (Agrell 1992, 104).
[68] Takšna ureditev izhaja iz doktrine hladne vojne, ki je locirala grožnjo varnosti ZDA zgolj v tujini, čemur je obveščevalna dejavnost tudi sledila (Treverton 2003, 224).
[69] Kot pravi Roger Z. George (2007), glavni cilj družbe ni odpraviti staro paradigmo, ampak jo dopolniti z novim načinom soočanja z izzivi 21. stoletja.

delovanja, soodvisnost in kooperativnost delovanja znotraj in izven obveščevalne skupnosti, sodelovanje v okviru nadnacionalnih struktur, kreativnost in inovativnost pri delu, širši krog uporabnikov informacij ter nezakonito poseganje v zasebnost (Steele 2002a; Steinberg in drugi 2003, 1; Treverton 2003, 225–232; Črnčec 2008).

Srčika sprememb, ki jih je prinesla nova obveščevalna paradigma, je **odprtost** (angl. openness).[70] Ta se kaže s presežnim multipliciranjem podatkov in informacij, ki bodo – namesto tajnih podatkov – glavna naloga obveščevalnih služb.[71] V svetu, ki je pred obveščevalno dejavnostjo, odprtost ne bo le zaželena, ampak bo tudi *imperativ*. Obveščevalne službe si bodo olajšale delo z vpeljavo zunanjih uslužbencev (izvajalcev) izven državnega sektorja, iz znanstvenih institucij, korporacij, iz tako imenovanih možganskih trustov in drugih nedržavnih organizacij. »Odprte« okoliščine bodo na področju obveščevalne dejavnosti tudi pokazale, da državne obveščevalne službe ne bodo mogle tekmovati z zasebnimi organizacijami za kompetentne analitike (Treverton 2003, 228–229).

Vse te karakteristike, ki jih skupaj poimenujemo pod izrazom »nova obveščevalna paradigma«, pomenijo tektonske spremembe na področju obveščevalne dejavnosti. Znotraj te paradigme se latentno povečuje vloga zasebnega sektorja, zato pravimo, da se v sodobnem okolju odvija **privatizacija obveščevalne dejavnosti**, ki bi jo lahko ob uporabi splošne definicije opredelili kot *zmanjševanje vloge države pri financiranju, opravljanju ali distribuciji obveščevalnih storitev oziroma obveščevalne dejavnosti*. Po besedah Andrewa Rathmella (2002, 74) privatizacija obveščevalne dejavnosti vključuje štiri komponente: *cilje*, *vire*, *metode* in *stroške*. Tako rekoč imamo opravka (1) z asimetričnimi varnostnimi izzivi, (2) z informacijsko revolucijo, (3) s spremenjenimi metodami obveščevalne dejavnosti, ki prihajajo iz civilne družbe, ter (4) z ekonomskim dejavnikom, ki sproža tendence po zmanjševanju stroškov v »odprtem svetu«, v katerem bo, po besedah Williama Colbya (v Sigurdson 1992, 5), nekdanjega direktorja Cie, *»gospodarska rast zahtevala številne avtonomne in premišljene odločitve, ki jih lahko dosežemo le z integracijo procesa odločanja s sodobno obveščevalno dejavnostjo«*. Stevan Dedijer, oče poslovne obveščevalne dejavnosti,

[70] Če si sposodimo in prevedemo naslov dela Thomasa L. Friedmana (2006), dobimo pomembno dejstvo – svet je sploščen. Treverton (2003, 226–227) poudarja, da gre pri odprtosti za tako imenovano »Hobsonovo izbiro«: države se lahko zaprejo pred globalno trgovino in tehnološkim razvojem in tako ostanejo osiromašene ali pa poiščejo način, da postanejo bogate, vendar samo pod pogojem, da se odprejo.

[71] Ko govorimo, da bodo informacije delo obveščevalnih služb, ne mislimo, da bodo obveščevalne službe vse te informacije proizvedle same. Če povzamem besede nekdanjega namestnika DCI, Richarda Kerra, lahko rečemo, da se mora *»obveščevalna skupnost naučiti, da ne nadzira več svojih lastnih virov«* (Treverton 2003, 226–227).

in Colby sta ugotovila, da se vse vrste obveščevalne dejavnosti spreminjajo tako hitro in korenito, da lahko našo dobo označimo kot čas nove večplastne **obveščevalne revolucije**, kakršne v zgodovini še ni bilo, ki pa se kaže ravno v privatizaciji obveščevalne dejavnosti (Dedijer 2005, 125; 2003, 4).

5.1 Asimetrični varnostni izzivi obveščevalnih služb

Po koncu konfrontacije med Zahodom in Vzhodom, še toliko bolj pa s terorističnimi napadi 11. septembra 2001 v ZDA, je civiliziran svet kot rečeno dobil novega in bolj kompleksnega sovražnika.[72] Pritisk časa in prostora ter prostega pretoka ljudi, orožja, strupenih snovi, drog, znanja in idej je preoblikoval način pojavljanja groženj in način, kako mora obveščevalna služba delovati (Friedman v George 2007). Pojavile so se ogrožajoče nedržavne organizacije, ki so razvile lastne sofisticirane obveščevalne in protiobveščevalne oddelke z zaposlovanjem bivših uslužbencev nekdanjih obveščevalnih služb socialističnih držav. Te so postale prava protiutež sodobnim obveščevalnim službam (Encyclopaedia Britannica 2008, »intelligence«).[73] Četudi je večina teh terorističnih akcij bila izvedena po istem vzorcu, obveščevalne službe niso bile kos takšnim **asimetričnim varnostnim izzivom**.[74] Teoretiki sodobne varnostne teorije in praks protiterorizma so namreč nekoliko preveč usmerjeni v enostavne analize, tehnične rešitve, vojaške in policijske aktivnosti ter zadrževanje pridobljenih podatkov in informacij zgolj zase ali v skrbno določenih skupinah.[75]

---

[72] Ti sovražniki so predvsem nedržavne entitete, kot so teroristične organizacije, mamilarski karteli, militantne organizacije, skrajne verske grupacije in drugi.

[73] Skrajna islamska teroristična organizacija al-Qaeda, ki je 11. septembra 2001 izvedla teroristične napade na Svetovni trgovski center v New Yorku in na Pentagon v Arlingtonu v ZDA, je imela organizirano svojo obveščevalno infrastrukturo, ki je skrbela za urjenje in varnost teroristov na Bližnjem Vzhodu, v Evropi in v ZDA. Dokazi, ki so jih objavili po vojaškem posredovanju v Afganistanu, so pokazali, da je al-Qaeda uporabljala napredno računalniško strojno opremo, s katero je lahko terorističnim celicam pošiljala šifrirana sporočila in zasledovala ameriške satelite za fotografsko izvidništvo (Encyclopaedia Britannica 2008, »intelligence«).

[74] Dandanes na obrambnem in varnostnem področju veliko govorimo o **asimetriji**, ki se ne nanaša na kvantitativne indikatorje družbene moči in primerjavo naravnih in družbenih virov ali oborožitvenih sistemov, pač pa na neprimerljivost, neenakost, različnost sodelujočih v konfliktih, izraženih pri uporabi sredstev za doseganje ciljev, metodah uporabe teh sredstev ter realnem položaju ali znotraj družbe ali znotraj mednarodne skupnosti (Svete 2002, 22). Ko govorimo o spopadanju sodobnih obveščevalnih služb držav z nedržavnimi organizacijami, govorimo o bojevanju, ki mu vlada načelo asimetrije. Tovrstno bojevanje lahko umestimo v širši okvir **asimetričnega vojskovanja**. Po besedah Metza in Johnsona (v Svete 2002, 25) v domeni vojaških zadev in nacionalne varnosti predstavlja asimetrija delovanje, organiziranje in razmišljanje, drugačno od nasprotnikovega, z namenom maksimizirati lastne prednosti ter izkoristiti nasprotnikove šibkosti, pridobiti pobudo ali zagotoviti širše možnosti delovanja.

[75] Analitični okvirji temeljijo pretežno na kratkoročnih ugotavljanjih posledic terorističnih napadov, namesto na dolgoročnih ali vsaj srednjeročnih. Konceptualni razvoj raziskav o terorizmu je šibek tudi zato, ker je dostop do določenih podatkov omejen. Tajnost podatkov je zaradi pravnih razlogov seveda nujna, vendar pa razumljiva le

Zato je zelo pomembno, da se *identificirajo skupna interesna področja* vseh obveščevalnih in obveščevalno-varnostnih služb ter različnih znanstvenih institucij in zasebnih organizacij.[76] V »vojni proti terorizmu« bo tako potrebno dati poudarek in prednost tistim analizam terorističnih organizacij, ki dejansko predstavljajo grožnjo, obveščevalne skupnosti pa bodo morale sprejeti bolj *fleksibilno in decentralizirano organizacijsko strukturo*, ki bo omogočila sodelovanje z zasebnimi obveščevalnimi organizacijami (Anžič 2002, 459–460; Steele 2002a; Treverton 2003; Todd in Bloch 2003; George 2007).[77]

Po besedah Reiter Nealove (2008) je vključenost zasebnega sektorja v protiteroristično dejavnost razvidna z dveh vidikov:

- kot vir iniciativ proti terorizmu za javni sektor, vključujoč skupno rabo informacij in varovanje kritične infrastrukture,[78]
- kot katalizator za inovacije pri raziskavah in protiterorističnih taktik.

5.2 Informacijska revolucija

Nagel razvoj informacijsko-komunikacijske tehnologije v zadnjih nekaj desetletjih je povzročil revolucionarne spremembe na področju komuniciranja in na splošno pretoka podatkov, informacij in znanja. **Informacijsko-komunikacijska tehnologija**, ki temelji na mikroelektroniki, je tako *»pomemben rezultat znanstveno-tehnološkega napredka in eden glavnih elementov razvoja«* celotne družbe v drugi polovici 20. stoletja (Svete 2006, 102).[79]

---

za tiste podatke, ki v taki obliki zagotavljajo (inter)nacionalne varnostne interese in zaščito virov (Anžič 2002, 459–460).

[76] Zasebni sektor predstavlja tako imenovan *cordon sanitaire* oziroma prvo nacionalno »bojno linijo« pri zoperstavljanju netradicionalnim grožnjam, kakršna je denimo terorizem, poleg tega pa je glavni akter pri varovanju kritične infrastrukture. Zaradi tega je zasebni sektor tudi tisti prvi, ki zbira in obdeluje podatke o omenjenih grožnjah, na podlagi katerih lahko bistveno pripomore k pravočasnemu in efektivnemu odzivanju na grožnje celotne obveščevalne skupnosti (Steele 1996, 224).

[77] Za razliko od preostalih zahodnih držav so v ZDA obveščevalne službe in obveščevalno skupnost nasploh centralizirali s sprejetjem Zakona o reformiranju obveščevalne skupnosti in preprečevanju terorizma (angl. Intelligence Reform and Terrorism Prevention Act), ki velja od 17. decembra 2004. Obveščevalni direktor je tako postal glavni mož koordinacije vseh petnajstih komponent obveščevalne skupnosti in prvi obveščevalni svetovalec predsednika in zakonit svetovalec o obveščevalnih zadevah znotraj Sveta za nacionalno varnost (The Office of the Director of National Intelligence 2008).

[78] Po definiciji Evropske komisije **kritična infrastruktura** predstavlja tiste obrate, storitve in premoženja fizične in informacijske tehnologije, katerih okvara ali uničenje bi resno vplivalo na zdravje, varnost ali gospodarsko blaginjo državljanov ali na učinkovito delovanje države. Kritična infrastruktura vključuje energetske naprave in omrežja, komunikacijske in informacijske tehnologije, finance, zdravstvo, hrano, vodo, prevoz, proizvodnjo, skladiščenje in prevoz nevarnih snovi ter vlado (Evropska komisija 2004).

[79] Ravno uporaba informacijskih in drugih sodobnih tehnologij v oborožitvenih sistemih in oboroženih silah v sedemdesetih letih 20. stoletja je povzročila famozno revolucijo v vojaških zadevah (angl. **R**evolution in **M**ilitary **A**ffairs) (Svete 2006, 102).

Razvoj informacijske tehnologije gre naglo naprej, čas med odkritjem in uporabo nove tehnologije pa se bo v skladu z Moorovim zakonom[80] še naprej skrajševal; prosti pretok informacij bo tako recipročno vplival na hitrejši razmah tehnologije po svetu, na žalost tudi potencialno destruktivne tehnologije (Barger 2005, 20). Prihodnost nadaljnjega razvoja pa je povsem na strani elektronskega komuniciranja.[81] Vsem tem »revolucionarnim spremembam« na področju informacijsko-komunikacijske tehnologije pa vlada **pravilo nepredvidljivih posledic** (Triglav 1996, 27–28).

Ena izmed teh nepredvidljivih posledic je *sprostitev in pospešitev pretoka ogromne količine podatkov in informacij*, ki postajajo z razvojem informacijsko-komunikacijske tehnologije dostopne vedno širšemu krogu ljudi (Jaklič v Džombić 2006, 14). Internet ali medmrežje ponuja uporabniku neomejeno bogastvo (vse bolj zanesljivih) informacij ter storitev in dejavnosti.[82] Tovrsten informacijsko-tehnološki trend imenujemo **informacijska revolucija**, ki je začela prevzemati svojo vlogo v sedemdesetih letih prejšnjega stoletja in traja še vedno. Kljub eminentni vlogi razvoja informacijsko-komunikacijske tehnologije pa informacijske revolucije ne moremo opredeliti zgolj kot *tehnološki* trend, saj gre predvsem za *ekonomski* in *socialni* trend.[83]

Peter Drücker (v Steele 2002a, 31–32), oče sodobnega menedžmenta, je leta 1998 dejal:

> Naslednja informacijska revolucija je na dobri poti. Vendar pa se ne dogaja tam, kjer jo iščejo informacijski znanstveniki, informacijski direktorji in nasploh informacijska industrija. To ni revolucija tehnologije, strojev, tehnik, programske opreme ali hitrosti. To je revolucija KONCEPTOV. Doslej – že več kot 50 let – se je informacijska revolucija osredotočala na »T« v kratici »IT« (op. D.U., informacijska tehnologija). Naslednja informacijska revolucija pa postavlja vprašanji: Kaj je POMEN informacij in kaj je njihov NAMEN? In to hitro vodi v redefiniranje nalog, ki jih moramo opraviti s pomočjo informacij, in s tem v redefiniranje institucij, ki opravljajo te naloge.

[80] Gordon Moore, soustanovitelj podjetja Intel, je že v šestdesetih letih prejšnjega stoletja dejal, da se bo moč procesorjev vsakih 18 mesecev pri njihovih konstantnih cenah podvojila. Ob enem izhaja iz Moorovega zakona še ena pomembna ugotovitev, in sicer, da se bodo ob konstantni hitrosti procesorjev njihove cene vsako leto in pol prepolovile. Ravno hiter tehnološki razvoj in upad cen informacijsko-komunikacijske tehnologije sta glavna razloga, da je tovrstna tehnologija prodrla v skoraj vse pore družbenega življenja (Svete 2005, 18–19).

[81] Razvoj elektronike spodbuja širjenje t.i. tehnološke civilizacije. Ta civilizacija oblikuje vsiljivo kulturno enakost, ki ogroža lokalne kulture prvine in posebnosti, izvor moči pa je v zabavni industriji (Triglav 1996, 30).

[82] Splet je bogat z viri, vendar pa je prikrajšan zanesljivosti. Sčasoma naj bi se spletni brskalniki izboljšali in prikazovali vse bolj zanesljive podatke in informacije (Treverton 2003, 104).

[83] Pierre Piganiol (1992, 27) pravi, da je informacijska revolucija nastopila *»natanko ob času, ko smo potrebovali nova orodja upravljanja kompleksnosti okolja v ekonomskem, političnem, tehničnem in tudi družbenem smislu. Nekateri to obdobje poimenujejo tudi era obveščevalne dejavnosti, saj naj bi danes imel vsak dostop do vsega znanja človeštva.«*

5.2.1 Pomen in namen informacij v sodobni družbi

Življenja brez informacij si ni moč predstavljati. Če se hoče posameznik ali organizacija odzivati na spremembe v okolju in se jim prilagajati, mora nujno poznati dejansko stanje okolja, za kar pa potrebuje informacije, ki jih mora vsebinsko opredeliti, ovrednotiti in ugotoviti njihov pomen in posledice, ki bodo nastale zaradi njih (Svete 2006, 106; Purg 2002, 27). Gre za nekakšno odvisnost od informacij, ki pa bo vztrajno in kontinuirano rasla še naprej in to na vseh področjih našega življenja. Odsotnost oziroma pomanjkanje informacij lahko za organizacijo predstavlja negativno odvisnost (Bentley 1998), ali konkretneje, *»brez informacij ni mogoče delovanje nobene organizacije v kompleksnem okolju«* (Svete 2006, 106). Informacije same pa še ne izoblikujejo **znanja**, kajti to nastane šele, *»ko vzpostavimo sistem odnosov, ki povezujejo vse elemente, za katere se zanimamo, in so povezani s številnimi bolj ali manj utemeljeni sodbami o relevantnosti teh odnosov«* (Piganiol 1992, 27). V zvezi s tem pravimo, da obstaja **kognitivna hierarhija**, katere glavni elementi so podatki, informacije, znanje in razumevanje (Svete 2002, 13–14). Stevan Dedijer (2005, 128) na najvišji nivo te kognitivne kompleksnosti postavi **obveščenost (inteligenco)**, ki jo opredeli kot sposobnost človeških možganov (organizacije), *»da si pridobi nove informacije in znanje, naredi presojo in prilagoditev okolju, razvija nove koncepte in strategije ter na podlagi pridobljenih informacij deluje na razumen in učinkovit način«*. Pretvorba podatkov v informacije, razumevanje in znanje so kot osnova kognitivnega procesa nujen pogoj, da družbe, organizacije in posamezniki oblikujejo svoj odnos do realnega sveta in na podlagi tega sprejemajo odločitve (Mayer-Schönberger in Broding v Svete 2006, 105). Tisti, ki so v preteklosti razpolagali z zanesljivimi in pravočasnimi podatki ter jih ustrezno analizirali in pretvorili v informacije, so vršili moč nad onimi, ki takih podatkov niso imeli ali pa jih niso ustrezno kontekstualizirali. Pomen informacij je danes torej več kot jasen: *kdor poseduje informacije ima moč.* Tukaj govorimo o tako imenovani **informacijski moči**, ki jo lahko opredelimo kot *»rezultat posedovanja znanja, ki ga drugi nimajo, ga pa potrebujejo ali želijo«* (Svete 2006, 106). Informacije, ki jih posedujemo in jih nihče ne potrebuje ali ne želi, so brez vrednosti oziroma moči (Svete 2006, 106–107). Takšnih informacij pa je danes ogromno. Bolj kot s pomanjkanjem se v kibernetskem prostoru srečujemo s preobilico podatkov in informacij (Purg 2002, 28).[84] Po nekaterih ocenah naj bi se število shranjenih

[84] Glede na podatke ameriškega analitskega podjetja *International Data Corporation* naj bi bilo lansko leto na spletu ustvarjenih in kopiranih za okoli 281 eksabajtov podatkov, kar znese 45 gigabajtov podatkov na zemljana; trend povečevanja se bo v naslednjih letih še stopnjeval (Roush 2008).

podatkov in informacij v medmrežju vsake dve leti kar podvojilo (Treverton 2003, 9; 103).[85] Po mnenju Bentleya (1998, 80–83) danes že govorimo o doseženi stopnji **informacijske preobremenitve**, kar preprosto pomeni, da imamo na voljo preveč informacij, zaradi česar je vse bolj vprašljiva tudi **verodostojnost informacij**. Za obveščevalne organizacije torej bolj kot pridobivanje predstavlja večji problem **verifikacija podatkov** (Treverton 2003, 9–10). Stroški za zbiranje, upravljanje in dostopanje do informacij naraščajo sorazmerno z naraščanjem informacij, ki jih potrebujemo za upravljanje, ne glede na vrednost teh informacij. Bolj kot količina informacij in podatkov pa sta pomembnejša kakovost in ločevanje med različnimi tipi informacij. Informacija kot taka namreč ne obstaja, ampak jo na osnovi podatkov ustvarijo ljudje. Nye in Keohane kot vir moči opredelita 3 pojavne oblike informacij (glej Svete 2006, 107–108):

(1) **Prosto dostopne informacije** (angl. free information) so tiste informacije, ki jih avtorji ustvarijo in posredujejo, ne da bi zahtevali ali pričakovali finančno kompenzacijo (znanstvene informacije, propaganda itd.; javne in sive informacije);

(2) **Komercialne informacije** (angl. commercial information) so informacije, ki jih ljudje oblikujejo in posredujejo, ob tem pa zahtevajo ali pričakujejo plačilo;[86]

(3) **Strateške informacije** (angl. strategic information) so stare toliko kot obveščevalna dejavnost. Strateške informacije zagotavljajo prednost njihovemu oblikovalcu samo v primeru, ko nasprotnik teh informacij ne posreduje. Pri teh informacijah je pomembna vsebina in ne kvantiteta.

*»**Eksplozija količine prosto dostopnih informacij je morda najbolj dramatičen učinek informacijske revolucije.** Hitra rast elektronske trgovine in povečana globalna konkurenčnost pa bosta druga pomembna učinka informacijske revolucije.«* (Svete 2006, 107) Vedeti, kdo ve (angl. know who knows), vedeti, kako filtrirati vso maso javno dostopnih podatkov ter izdelava obveščevalnih ocen usmerjenih v prihodnost so postale bistvene naloge obveščevalnih organizacij v informacijski dobi (Steele 2002, 19; Herring 1992, 165). Zato je za te organizacije pomembno, da imajo veliko **sposobnost učinkovitega selekcioniranja** preobilice informacij; ločevanja dejstev od polresnic in neresnic. Ob tem jim je informacijska tehnologija samo v pomoč, ne more biti pa nadomestilo za kontekstualizacijo informacij

[85] Po ocenah *Bontisa* naj bi se do leta 2010 vso svetovano znanje podvojilo na vsake 11 ur (Radovanović 2004, 20).

[86] Če so tovrstne informacije na medmrežju, *»potem je potrebno zagotoviti spoštovanje avtorskih pravic, kar pomeni, da oblikovalci informacij s strani uporabnikov dobijo določeno nadomestilo«* (Svete 2006, 107).

(Svete 2005, 131).[87] Pri dostopanju do informacij se moramo zato zavedati, katere informacije zahtevamo.[88] Uspešno dostopanje do želenih informacij je odvisno od tega, da vemo: *katere* informacije želimo; *kje* jih lahko najdemo; *kako* jih pridobimo; *kako* se *odzvati*, ko so na voljo; ter *kdaj nimajo* več *vrednosti* in jih lahko zavržemo (Bentley 1998). Za nas so bistvene tako imenovane **prednostne informacije**, ki so zasnovane na uporabnosti in zaupanju v sprejemljiv rezultat odločitve, bolj kot na točnosti informacije. Glavni faktor pri izbiri informacij je **čas**.[89] Oblikovalci politik se bodo tako zaradi pomanjkanja časa vse bolj obračali na obveščevalne organizacije, ki se ukvarjajo s selekcijo in analizo podatkov, med temi pa se bo pojavila konkurenca (Treverton 2003, 10). Glavna značilnost informacijske družbe je, da največ ljudi opravlja **informacijske poklice**. Pri tem mislimo na delo, pri katerem se ljudje pretežno ukvarjajo z izdelavo, obdelavo in prenosom informacij (Gradišar in drugi v Džombić 2006, 6). Velimir Srića (v Džombić 2006, 20) razdeli informacijske poklice v štiri skupine, in sicer na: (1) proizvajalce informacij, (2) obdelovalce informacij, (3) prenašalce informacij in (4) poklice s področja informacijske infrastrukture.[90] Ti poklici dobivajo v kontekstu nove obveščevalne paradigme vse pomembnejšo vlogo in predstavljajo pravo konkurenco državnim obveščevalnim uslužbencem, še posebej na področju analize in obdelave podatkov.

Za vse želene informacije in podatke pa ne velja prosti pretok oziroma vsesplošna dostopnost, temveč jih lahko nadzoruje le nekaj ljudi ali institucij. Običajno gre pri omejevanju informacijskega toka za podatke v zvezi z nacionalno varnostjo, osebne podatke, poslovne skrivnosti, sodne dokumente, podatke o bančnih računih in o zasebnih pogovorih (Svete 2006, 107).[91] Pridobivanje takšnih tajnih podatkov je večinoma nezakonito in ga lahko

[87] Računalniki niso zmožni določati naše cilje. Lahko nam pomagajo pri kreativnem razmišljanju in definiranju naših ciljev, vendar pa smo v končni fazi mi tisti, ki sprejmemo končno odločitev (Piganiol 1992, 26).

[88] Dedijer (2005, 128) govori tukaj o problemu identifikacije, ki je *»pogosto poenostavljen, zgodovina pa kaže, da nekatere od največjih obveščevalnih napak izhajajo iz napak v procesu identifikacije. Take napake se rade zgodijo, ko je nasprotnik ali sovražnik nov in nepoznan. Del težav izhaja iz dejstva, da proces identifikacije ni racionalen, ampak intuitiven, ki zahteva domišljijo in občutljivost ter sposobnost zaznavanja prihajajočih sprememb.«*

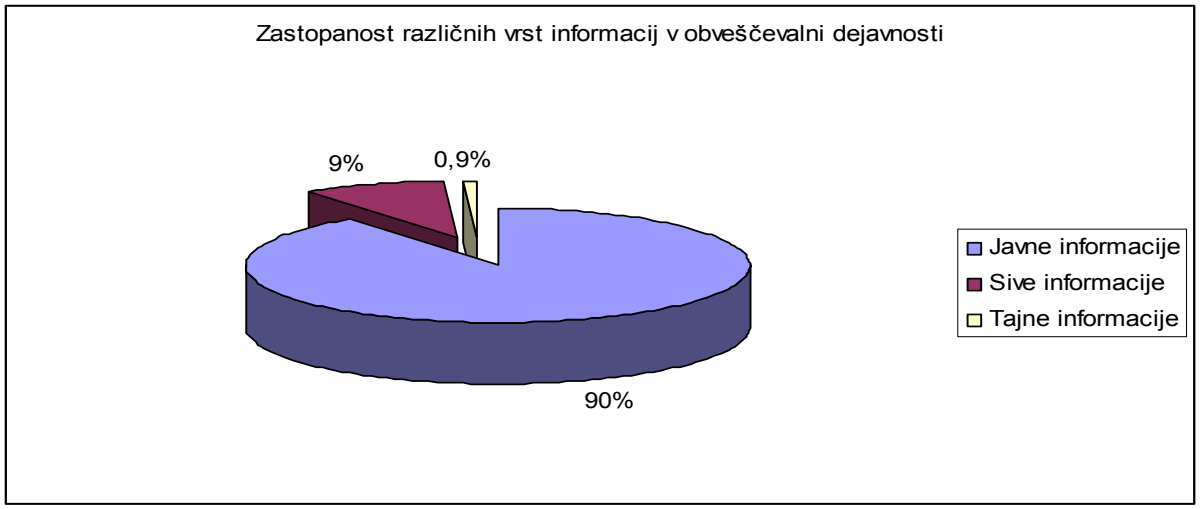
[89] Najboljši čas za pridobitev informacij je tisti trenutek, v katerem je potrebno sprejeti odločitev. *»Če bi potrebne informacije pridobili predčasno, bi bile v trenutku odločitve že prestare, če pa bi jih pridobili kasneje, bi predstavljale zgolj prepozno spoznanje.«* (Džombić 2006, 41)

[90] *Proizvajalci* (znanstveniki, raziskovalci) ustvarjajo nove ali pa preoblikujejo obstoječe informacije glede na potrebe naročnika. *Obdelovalci*, ki jih je 3–4 krat več kot proizvajalcev, so tisti, ki v procesu obdelavo vhodno informacijo preoblikujejo v izhodno tako, da se na osnovi nje lahko odločajo in sprejemajo odločitve upravljavci in nadzorniki od strateškega do taktičnega nivoja. *Prenašalci*, katerih je 2 krat manj kot proizvajalcev, posredujejo informacije uporabnikom (profesorji, mediji). *Poklici s področja informacijske infrastrukture* pa predstavljajo predvsem razvoj in vzdrževanje telekomunikacijskih in računalniških omrežij (Gradišar in drugi v Džombić 2006, 20).

[91] Tako denimo Busheva administracija iz nacionalno-varnostnih razlogov ohranja nadzor nad trinajstimi glavnimi strežniki, ki omogočajo delovanje celotnega internetnega prometa (Moore v Svete 2006, 106).

opredelimo kot **vohunjenje**.[92] Fokus obveščevalne dejavnosti v informacijski dobi je uperjen v **prosto dostopne informacije ali javne informacije, in ne v zaupne**, katerih pomen ljudje po nepotrebnem poveličujejo in jih pogosto zamenjujejo s tako imenovanimi sivimi informacijami. V zvezi s tem nam Dedijer ponuja sledečo tipologijo informacij: (1) **javne (bele) informacije**, ki so dejansko *prosto dostopne informacije* in predstavljajo 90 odstotkov vseh informacij v obveščevalni dejavnosti; (2) **sive informacije**, ki niso publicirane ali široko distribuirane, so pa legalno dostopne; le vedeti je treba, da obstajajo in poiskati ustrezni komunikacijski kanal, predstavljajo pa 9 odstotkov vseh informacij v obveščevalnih dejavnosti; (3) **tajne (črne) informacije**, ki jih pridobivamo z vohunstvom in predstavljajo 0,9 odstotka vseh informacij v obveščevalni dejavnosti. Tukaj so še **neobstoječe informacije**, ki predstavljajo 0,1 odstotka vseh informacij v obveščevalni dejavnosti (Dedijer 2005, 128–129; Reed v Friedman 2002, 17).

Slika 4.1: Zastopanost različnih vrst informacij v obveščevalni dejavnosti



Vir: Dedijer 2005, 129.

5.2.2 Obveščevalna dejavnost odprtih virov

Ko govorimo o pridobivanju, analizi in posredovanju obveščevalnih informacij, ki temeljijo na odprtih virih[93] (angl. open source), imamo v mislih **obveščevalno dejavnost**

[92] Če pa se zgodi, da konkurent ali nasprotnik zaradi napake iz malomarnosti izda svoje skrivnosti, potem takšna pridobitev tajnih podatkov **ni kazniva** (Piganiol 1992, 35).

[93] **Odprti vir** pomeni javno dostopne informacije v natisnjeni ali elektronski obliki. Informacije odprtih virov so lahko prenesene preko radia, televizije ali časopisov, ali pa so distribuirane drugače: s komercialnimi podatkovnimi bazami, elektronsko-poštnimi omrežji ali prenosljivimi elektronskimi mediji (CD, DVD, USB). Lahko so posredovane širši javnosti, preko množičnih medijev ali pa samo določeni javnosti v obliki sive

odprtih virov (angl. **O**pen **S**ource **Int**elligence – OSINT).[94] Osnova dejavnosti so torej prosto dostopne informacije in podatki.[95] Odprte informacije pridobivamo iz medijev (javnih in komercialnih), podatkov javnih institucij (informacije javnega značaja), s satelitskim opazovanjem in nadziranjem preko javno dostopnih aplikacij (Google Earth), profesionalnih in akademskih dokumentov in dogodkov, prostorskih slikovnih dokumentov (atlas, zemljevid), zasebnih publikacij, knjižnic in medmrežja. Sive informacije so najcenejše in najkakovostnejše informacije, saj predstavljajo bližnjico do uporabnih znanstvenih, političnih, socio-ekonomskih in vojaških disciplin; te informacije predstavljajo nekakšno »prikrito znanje«, ki ga je treba najti (George 2007).[96] Organizacije, ki so **tipične proizvajalke velikih količin sivih informacij**, so: raziskovalne ustanove (laboratoriji, inštituti, centri odličnosti), vlade, zasebni založniki (skupine pritiska in politične stranke), nevladne organizacije, korporacije, gospodarske zbornice in sindikati, možganski trusti in akademska skupnosti.

OSINT se razlikuje od akademskih, poslovnih in novinarskih raziskav, saj gre za obveščevalni ciklus (organiziran proces), katerega rezultat so obveščevalne informacije povezane v znanje, ki je v podporo pri sprejemanju odločitev posameznika ali organizacije. Vendar pa se te taiste ustanove poleg raziskav ukvarjajo tudi z obveščevalno dejavnostjo

---

literature. V kakršnikoli obliki je, odprti vir ne vsebuje informacij in podatkov, ki so: tajni po svojem izvoru; so predmet lastninskih omejitev; so produkt občutljivih kontaktov z drugimi osebami; ali so pridobljene s prekritimi sredstvi (Steele 2002, 64).

[94] Obveščevalno dejavnost odprtih virov lahko opredelimo kot **organiziran proces, ki vključuje (1) iskanje, selekcioniranje in pridobivanje brezplačnih (ter kupovanje komercialnih) informacij iz raznolikih javno dostopnih virov, (2) preverjanje in verifikacijo, (3) procesiranje in analiziranje teh, (4) izdelavo končnih obveščevalnih informacij ter (5) njihovo pravočasno distribucijo določenemu občinstvu za posebne obveščevalne zahteve** (Best in Cumming 2007; Steele 2007).

[95] Za prosto dostopne informacije (in podatke) lahko uporabljamo tudi izraze odprte informacije, informacije odprtih virov, javno dostopne informacije ter javne (bele) ali sive informacije; plačljive imenujemo komercialne informacije. Robert D. Steele (2007, 131–132) razlikuje med podatki odprtih virov, informacijami odprtih virov, obveščevalnimi informacijami odprtih virov in uveljavljenimi obveščevalnimi informacijami odprtih virov. *Podatki odprtih virov* (angl. **O**pen **S**ource **D**ata) so surove tiskovine, prenos, ustno poročanje ali druga oblika podatka iz primarnega vira. Lahko je fotografija, magnetofonski zapis, slika komercialnega satelita ali osebno pismo posameznika. *Informacije odprtih virov* (angl. **O**pen **S**ource **In**formation) so sestavljene iz podatkov, ki jih lahko združimo z uredniškim procesom, s katerim nekatere podatke filtriramo, drugim pa damo veljavnost in jih predstavimo. Te informacije so splošne informacije, ki so običajno široko distribuirane. Časopise, knjige, revije, prenose, splošna dnevna poročila in medmrežje štejemo kot vir informacij odprtih virov. *Obveščevalne informacije odprtih virov* (angl. **O**pen **S**ource **Int**elligence) so informacije, ki so premišljeno ločene, obdelane in distribuirane izbrani javnosti, predvsem poveljnikom, oblikovalcem politik in drugim, ki sprejemajo odločitve, z namenom, da bi pripomogle k reševanju določenega vprašanja. So končni obveščevalni produkt. *Uveljavljene obveščevalne informacije odprtih virov* (angl. **V**alidated **O**pen **S**ource **Int**elligence) so obveščevalne informacije odprtih virov, ki jim je pripisana visoka stopnja zanesljivosti. Lahko so izdelane z obveščevalno dejavnostjo ob uporabi vseh virov, kar pomeni, da imajo uslužbenci, ki izdelajo te informacije dostop tudi do tajnih virov informacij. Prihajajo lahko tudi iz zelo zanesljivih odprtih virov, katerih gotovost ni vprašljiva.

[96] Takšne informacije so kseroksirani dokumenti, reprinti znanstvenih člankov, pogovori z dobro informiranimi specialisti, oglaševalne brošure, pamfleti, neuradni vladni dokumenti, letna poročila, raziskovalna poročila, delovni listi, študije, tržne ankete, in tako dalje (Dedijer 2005, 129; Jardines 2002, 9)

odprtih virov (Steele 2007, 131–139; Best in Cumming 2007; National Defense Authorization Act for Fiscal Year 2006). Tovrstna disciplina obveščevalne dejavnosti pomeni **doktrinarni premik od obveščevalnih skrivnosti k obveščevalnim informacijam** (Treverton 2003, 246). Čeprav nekateri temu dejstvu oporekajo, se izkušeni uslužbenci obveščevalnih služb strinjajo, da je moč večino informacij pridobiti iz odprtih virov in jih uporabiti pri izdelavi celovitih obveščevalnih produktov, kar je tudi bistven prispevek te discipline (Dedijer 2005, 128–129; Reed v Friedman 2002, 17).[97] Odprte vire informacij so državne obveščevalne in vojaške organizacije[98] uporabljale že v preteklosti, le da jih je zdaj (pre)več, so bolj raznolike, manj zanesljive in elektronsko objavljene (Jardines 2002, 9–17; Steele 2002b, 68–69).[99]

Informacije odprtih virov so izdelane ali objavljene večinoma **za potrebe zasebnega sektorja**, zato je večina najboljših javno dostopnih informacij v rokah zasebnega sektorja (podjetja, možganski trusti), ki hrani te podatke v podatkovnih bazah, vzdrževanih na stroške zasebnega kapitala (Studeman 2002, 61). Ravno zasebni sektor je tisti, ki ponuja najcenejša in najhitrejša opozorila oziroma **informacije v pravem času** (angl. real-time information) in zmožnosti podajanja obveščevalnih ocen (Steele 2002a, 18). V zasebnem sektorju obstajajo dobre obveščevalne zmožnosti, zatorej večina strokovnjakov za upravljanje s temi informacijami prihaja izven obveščevalnih služb in vlade nasploh (Steele 2002a, 21; Treverton 2003, 116).[100] Na področju **vojaških operacij** so denimo informacije odprtih virov,

[97] Prosto dostopne informacije so ohranjale skromno vlogo znotraj večjih obveščevalnih skupnosti in bolj odločilno vlogo znotraj manjših obveščevalnih skupnosti, realnost pa je, da so sredi devetdesetih let anglosaksonske obveščevalne skupnosti izkoriščale manj kot 10 odstotkov tistega, kar je moč dobiti v zasebnem sektorju (Steele 1996, 213).

[98] Zanimiv je primer iz falklandske vojne med Veliko Britanijo in Argentino leta 1982, ko so angleški častniki pridobivali podatke o nasprotniku kar iz zasebnih publikacij. Angleška Vojaška obveščevalna služba namreč ob začetku vojne z Argentino, aprila 1982, v svojem arhivu ni imela nobenih podrobnih poročil ali kakršnihkoli dokumentov o argentinskem letalstvu, mornarici in vojski. Častniki posebnih enot so imeli le poročila, ki so nastala na podlagi podatkov iz dela *Jane's Fighting Ships* in zbornika podatkov z Inštituta za strateške študije imenovanega *Military Balance*. Iz te literature so tako črpali grobe podatke o argentinskih bojnih ladjah, o enotah ter oborožitvenih sistemih, ki pa so zgolj količinsko prikazani (Keegan 2004, 304–305).

[99] Dober primer uporabe teh virov v preteklosti najdemo pri nekdanji ameriški obveščevalni službi OSS, ki je nekoč nastavila dva svoja uslužbenca v sobo z novinarji časopisa *The New York Times*. Na vse, kar so lahko odgovorili iz tega javnega vira informacij, je bilo označeno kot skrivnost in razposlano kot vsebinski rezultat zelo dobro izpeljane HUMINT operacije, ki je bila navidezno zelo draga, samo da bi pridobili dodatna sredstva (Copeland v Steele 1996, 213).

[100] Dober primer razumevanja pomembnosti odprtih informacij zasebnih organizacij za vojaške potrebe najdemo pri konfliktu v Somaliji. Ameriške obveščevalne službe namreč o Somaliji niso imele dovolj uporabnih internih obveščevalnih informacij. Najhitrejši način za pridobitev osnovnega »enciklopedičnega« znanja, ki bi pripomoglo k nadaljnjemu procesu pridobivanja podatkov in za zagotovitev uporabnih (celovitih) obveščevalnih informacij poveljnikom, ki so delovali na tem območju, je bila pomoč strokovnjakov in podatkovnih baz iz zasebnega sektorja. Tako je lahko predstavnik Združenih narodov čez noč dobil ekspresno pošto v vrednosti 5.000 USD, ki je vsebovala: (1) od podjetja *Jane's Information Group*: prostorsko dovršen zemljevid Somalije, na katerem so bila vrisana območja devetih klanov; bojni ukaz za vsak klan posebej na enem listu papirja; izvlečke vseh člankov s citati o Somaliji v obliki kratkega odstavka v zadnjih dveh letih; (2) od podjetja *Oxford*

ki jih nudi zasebni sektor, koristne ker: (1) so dobra podpora vojaškim, humanitarnim in protiterorističnim operacijam, saj se OSINT od vseh disciplin najbolj prilagaja situacijam;[101] (2) naročniki prihranijo precej stroškov povezanih z zbiranjem in obdelavo, ko kupijo poceni, posodobljene in hitro dobavljive komercialne informacije, pri tem pa se izognejo politični odgovornosti tajnega pridobivanja; (3) predstavljajo podporo skupnim koalicijskim in mednarodnim operacijam, ko je potrebno obvarovati interese lastne obveščevalne skupnosti ali pa so – nasprotno – temelj civilno-vojaškega sodelovanja in okostje tajnega bilateralnega deljenja obveščevalnih informacij (Steele 2002b, 65; 2007, 130; Sharfman 1996, 203). Pomembno vlogo pri uporabi odprtih virov pa dobivajo tudi slikovne komercialne informacije, ki jih proizvajajo **komercialni sateliti**, poslani v orbito Zemlje. Ti predstavljajo neodvisen vir informacij za recimo nadziranje in objavljanje aktivnosti različnih držav in nedržavnih organizacij. Uporabniki teh so denimo humanitarne organizacije (nadzor beguncev), mediji (nedostopna območja), agrikulturne organizacije (iskanje rodovitne zemlje), podjetja (industrijsko vohunstvo) in druge vladne ter nevladne organizacije. *Cena* in *kakovost* komercialnih fotografij bosta ključna faktorja izbire (Dehqanzada in Florini 2002, 43–50; Treverton 2003, 242).[102]

Iz zgoraj povedanega lahko sklenemo, da si zasebni sektor počasi »prisvaja« (privatizira) obveščevalne aktivnosti in da bo tako večina osnovnega procesiranja odprtih informacij izpeljana **zunaj državnih služb**, rezultat tega procesiranja pa bo država pridobila ali odkupila od služb, ki se s tem ukvarjajo (Treverton 2003, 124). Upravičeno lahko uporabimo besede Petra Schwartza (v Friedman 2002, 19), priznanega futurista, ki je dejal, da *»pred nami vzhaja tekmovalen informacijski trg, v katerem bo obveščevalna dejavnost zasebnih subjektov poceni, hitra in bo ušla izpod nadzora«*.

Analytica: 22 strani poročil, primernih za predsednike in premierje, ki so pokrivali 3 osnovna področja: operacije Združenih narodov v Somaliji, politiko ZDA do Somalije in ameriške operacije povezane s Somalijo; tak produkt je omogočal orientacijo na strateški in politični ravni; (3) od organizacije *The Economist Intelligence Unit*: kopijo poročila o tveganju v državi, ki je vključeval pomembne povzetke informacij o potencialnih težavah z logistiko, vključno z omejitvami pristanišč in letališč za strateško pristajanje (Steele 2002b, 69; Treverton 2003, 116).

[101] V smislu podpore zagotavljajo: strateške zgodovinske in kulturne vpoglede, informacije o infrastrukturi in trenutnih pogojih na operativni ravni ter taktično pomembne komercialne geoprostorske informacije, ki jih nacionalne obveščevalne službe ne zagotavljajo (Steele 2007, 130).

[102] Še vedno bodo prevladovale fotografije, posnete z nizkimi preleti letal nad domačimi in zavezniškimi teritoriji, skoraj polovica teh pa bo posnetih za državne ustanove po svetu (Dehqanzada in Florini 2002, 43–50; Treverton 2003, 242). Komercialna fotografija z visoko resolucijo z možnostjo procesiranja je na voljo že od 10 do 40 dolarjev na kvadratni kilometer (Steele v Allen 2002, 14). Vojaškim organizacijam bodo te fotografije pomagale identificirati sovražnikove ranljivosti, vojaške načrte, prikazale bodo učinkovitosti napadov in razvrstile prednostne cilje za misije. Iraška vojska naj bi uporabila *SPOT*-ove satelitske fotografije v resoluciji 10 metrov za načrtovanje napada in ocenjevanje učinkovitosti napadov v osemletni iraško-iranski vojni in kuvajtski krizi avgusta 1990.

5.3 Spremembe obveščevalnih metod

Obveščevalna dejavnost odprtih virov zagotavlja obveščevalnim službam tiste informacije, brez katerih ni moč niti začeti niti dokončati oblikovanja obveščevalnih informacij. Vendar pa je za obveščevalne službe ključ do izdelave dobrih obveščevalnih informacij v uporabi in analizi vseh virov, tajnih in odprtih, ki skupaj zagotavljajo **celovit obveščevalni produkt, temelječ na vseh virih** (angl. all-source product), kakršnega tudi zahteva naročnik oziroma uporabnik (Nye v Jardines 2002, 10; Piganiol 1992, 35; Treverton 2003, 16; Rathmell 2002, 75; Steele 2007, 130; 1996, 222; Šaponja v Purg 2002, 28).[103] Posamezni viri so namreč razpršeni, zato samo mozaik različnih virov, ki so oblikovani skozi čas, pripomore k zanesljivi in celoviti rešitvi zahtev (Steele 2002a, 25).[104] Za integracijo informacije v obsežno sliko pa so potrebni znanje, izkušnje in usposobljenost (Piganiol 1992, 35).[105]

Za zagotovitev celovitih obveščevalnih produktov iz vseh virov je potrebna tudi drugačna metodologija obveščevalnih služb in organizacijska struktura pridobivanja in analize tajnih in odprtih informacij. V obdobju »razpršenih informacij«, ko organizacije postajajo vse bolj odprte, preprosto ni več mogoča centralizirana struktura zbiranja, procesiranja, analiziranja in distribuiranja informacij (Steele 1996, 218; Baumard 1992, 86). Odprtost v obveščevalnih službah danes briše »stare« meje med zbiranjem in analizo podatkov in vodi v **decentralizirano obveščevalno skupnost**, ki je povezana z nedržavnimi organizacijami. Takšna sploščenost pa vpliva tudi na same interne strukture, predvsem *pridobivanja* in *analiziranja*. Tisti, ki pridobivajo podatke, morajo biti tesno povezani s tistimi, ki jih analizirajo, in obratno. Tisti, ki pa uporabljajo obveščevalne informacije, pa morajo biti povezani tako z zbiralci kot analitiki. Če ta povezava ne obstaja, se obveščevalna organizacija

[103] Višji uslužbenci obveščevalnih služb v ZDA in v drugih zahodnih državah so že v devetdesetih letih prejšnjega stoletja zatrjevali, da so obveščevalne informacije tajnih virov relativno neuporabne za vsakodnevne potrebe, zaradi česar so se obveščevalne službe začele zanimati za dostop do informacijskih virov zasebnih podjetij. Zelo dober primer iz tistega časa tudi odseva te potrebe in pomanjkljivosti. Steele (1996, 215) parafrazira enega izmed letalskih poveljnikov v operaciji »puščavska nevihta« takole: *»Če je točnost informacije 85-odstotna, pravočasna in jo lahko delim z ostalimi, je to veliko bolj uporabno, kot pa izvleček iz tajnih podatkov, ki ga je preveč, pride prepozno in potrebuje varovanje ter tri varnostne častnike, da ga prenašajo po bojišču.«*

[104] Nezmožnost izpeljave celovitih zaključkov je bila glavna šibkost obveščevalnih služb v hladni vojni (Agrell 1992, 104).

[105] Eden izmed sklepov ameriške Komisije za orožje za množično uničevanje je bil, da so odprti viri informacij *»ključnega pomena za razumevanje družbenih, kulturnih in političnih trendov, vendar pa so pomanjkljivo uporabljeni. Večina obveščevalnih izzivov danes in jutri (...) bo transnacionalnih in vodenih s strani nedržavnih akterjev. Obveščevalna skupnost mora razmišljati bolj kreativno in predvsem strateško.«* (George 2007)

ne more prilagoditi zunanjim situacijam, ne more poznati pravih željá naročnika in je dovzetna za informacijske šume (Treverton 2003, 228).[106] Kljub vsemu, pa bo vohunstvo kot tajna dejavnost še naprej pomembno pri pridobivanju podatkov.[107] Po eni strani se je nujno naslanjati na odprte vire informacij za razumevanje konteksta, po drugi strani pa se morajo obveščevalne službe držav še naprej osredotočati na skrivnosti, saj so to edine organizacije, ki so institucionalizirane posebej za zbiranje skrivnosti oziroma podatkov, ki niso dosegljivi »z drugimi sredstvi« (Hall v Steele 1996, 219).[108] Podobno velja za analizo odprtih virov, saj ta ne pomeni nadomestila za tradicionalne analize obveščevalnih služb; analitik uporablja odprte vire, da bi identificiral posamezne vrzeli v svojem znanju in postavil tajne podatke v kontekst ter tako izpopolnili končne obveščevalne informacije (Tyrrell 2002, 5). Po besedah Trevertona (2003, 127; 243–244) bi v obveščevalnih službah morali tisti analitiki, ki obravnavajo določena vprašanja na *taktični* ravni, biti bliže tajnim podatkom, medtem ko bi morali tisti, ki se ukvarjajo s *strateškimi* vprašanji (analize kompleksnih političnih, paravojaških, družbenih, ekonomskih in tehnoloških tem), biti bliže uporabnikom informacij ter v stiku s številnimi strokovnjaki, ki delajo na podlagi odprtih virov na univerzah, v korporacijah, možganskih trustih in drugih nedržavnih organizacijah.[109] Analitični produkt mora poleg zmožnosti *predvidevanja prihodnosti* (podajanja ocen) odsevati tudi pečat skupnega dela državnih in nedržavnih obveščevalnih organizacij. Integracijski proces nastajanja takšnega analitičnega produkta pa imenujemo **koordinacija**.

Pomembno dejstvo, ki ga je treba omeniti in je posledica elektronske distribucije podatkov, je način posredovanja obveščevalnih informacij **naročniku** oziroma **uporabniku** obveščevalnih informacij. Tradicionalno posredovanje informacije je temeljilo na **strukturi usmerjenega posredovanja informacij** (angl. push architecture), ko je obveščevalni analitik uporabniku posredoval tiste informacije, za katere je verjel, da jih potrebuje, in tistim, za

[106] Primer nepovezanosti med zbiralci (opazovalci) podatkov in analitiki je denimo Natovo bombardiranje Beograda leta 1999, ko so bombe zadele kitajsko veleposlaništvo. V tem primeru so namreč obveščevalni analitiki fotografij uporabljali zemljevide in satelitske podobe iz leta 1992, ko je taista stavba bila še srbski vojaški objekt in ne kitajska ambasada, kar je privedlo do napačnih ocen. Analitiki so bili torej odrezani od opazovalcev (Treverton 2003, 10).

[107] Zvezne agencije v ZDA še vedno ustvarijo več kot 260.000 uradnih skrivnosti vsako leto in to število se letno še povečuje (Steinberg in drugi 2003, 7).

[108] Steele (1996, 222) poda zanimiv predlog, ko pravi, da *»zbiranje skrivnosti ni težko, če se osredotočiš na njihovo zbiranje še preden postanejo skrivnosti«*.

[109] Nekatera dejstva kažejo, da se denimo v ZDA obveščevalne službe ne ukvarjajo več toliko s tajnimi operacijami, temveč je njihove težišče dela zdaj v analitičnem oziroma strateškem planiranju. »Strateška obveščevalna dejavnost« (angl. strategic intelligence) je vezana na delovanje Sveta za nacionalno varnost in omogoča, da so *»obveščevalne službe oči in ušesa predsednika ZDA«* (Gunzenhauser v Purg 2002, 28).

katere je verjel, da jih morajo dobiti (Sharfman 1996, 201–202; Treverton 2003, 224).[110] Elektronska porazdelitev informacij pa je omogočila tako imenovano **strukturo lastnega izbora informacij** (angl. pull architecture), kar pomeni, da analitiki izdelajo velike količine informacij in jih shranijo v nekakšne podatkovne »rezervoarje«, uporabniki pa iz teh »rezervoarjev« izberejo tiste, ki jih potrebujejo. Odločitev o tem, katere informacije, kako podrobne, v kakšnem formatu in v kakšnem času bodo prišle do uporabnika, sprejema uporabnik sam, in ne analitik. Uporabniki obveščevalnih informacij postajajo tako sami svoji analitiki (Sharfman 1996, 203–206; Treverton 2003, 16).[111] Glavni učinek te strukture bi se moral pokazati po eni strani v povečanju zahtev po izvrstnih analizah, po drugi strani pa v prejemanju *boljšega odziva* (angl. feedback).[112] Uporabnik informacij torej danes pogosteje stopa v stik z analitikom, zbiralcem in v nekaterih primerih tudi z virom, samo z namenom, da bi pridobil pravočasen in zanesljiv odgovor (Steele 1996, 223; Treverton 2003, 108).

5.3.1 Načelo »potrebe po delitvi«

Zaprta organizacijska kultura, tajnost delovanja, metod in sredstev, ter ozek krog uporabnikov informacij obveščevalnih služb je zaznamovalo tako imenovano načelo **potrebe po védenju** (angl. need to know). Delovanje po tem načelu je oviralo prost pretok informacij znotraj razdeljene skupnosti pomembnih državnih in zasebnih akterjev (Steinberg in drugi 2003, 1; Črnčec 2005, 29). Tendence po sprostitvi pretoka in skupne rabe vseh razpoložljivih informacij in podatkov so se okrepile po terorističnih napadih 11. septembra 2001 (Črnčec 2005, 29; Steele 1996, 216–217; 225).[113] Strokovnjaki in politiki zdaj zagovarjajo koncept odprte *distribuirane obveščevalne dejavnosti* (Steele 2002a, 30), kjer namesto načela potrebe po védenju vlada načelo **potrebe po delitvi** (angl. need to share), po katerem sodelovanje, skupna raba, pretok in izmenjava informacij zajemajo ne le državne institucije, ampak tudi

[110] Tako so uporabniki dobili kakršnekoli informacije, za katere je analitik menil, da mu bodo v pomoč. Informacije so običajno prispele, ko so pač prispele, kar ni nujno, da so prispele takrat, ko jih je potreboval. Čeprav pri tej strukturi analitiki upoštevajo zahteve in prioritete uporabnikov, so takšni procesi omejeni, saj analitiki stežka ugotavljajo, kaj uporabnikove prioritete pravzaprav pomenijo v praksi. Zato morajo analitiki te prioritete dobro poznati, kar pomeni iz analitikove perspektive pravi izziv (Sharfman 1996, 201–202).

[111] Tudi podjetja kot so *Google*, *Yahoo!*, *Amazon.com* in *TiVo* so se naučila, da razcvet podjetja ne temelji toliko na strukturi usmerjenega posredovanja svojih produktov in storitev pred svoje uporabnike, ampak bolj na ustvarjanju pogojev, ki omogočajo uporabniku, da sam izbere tisto, kar si želi. In šele nato se ta podjetja odzivajo z olajšanjem dostopa do tistega, kar so sami izbrali (Friedman 2006, 183).

[112] Elektronska distribucija informacij po principu strukture lastnega izbora informacij je verjetno glavni razlog za *sploščitev hierarhije* in nasploh organizacije (Sharfman 1996, 208–210).

[113] Ameriška administracija je spoznala, da obveščevalne službe pred 11. septembrom niso dostavljale **informacij v pravem času**. Številni strokovnjaki in politiki so opozorili, da so napadi 11. septembra 2001 posledica resnih problemov skupne rabe in delitve informacij, in sicer med obveščevalno skupnostjo in pomembni službami zunaj te skupnosti (Steinberg in drugi 2003, 1–2).

druge izobraževalne, znanstvene, gospodarske in nevladne organizacije.[114] Odprta izmenjava podatkov in informacij tako simultano obvešča vse pomembnejše družbene akterje pri zagotavljanju nacionalne varnosti (Treverton 2003, 17; Steele 1996, 225; Baumard 1992, 86; Črnčec 2005, 29).[115] Danes smo priča vzpostavljanju odprte in široke informacijske skupnosti ali informacijske mreže (Črnčec 2005, 29) ali virtualne skupnosti[116] (Steinberg in drugi 2003, 5; Steele 1996, 220), ki povezuje vse proizvajalce, distributerje in prejemnike informacij zasebnega in državnega sektorja.[117] Izmenjavanje informacij pa ne poteka le intra-državno, ampak tudi globalno; v okviru transnacionalnih in nadnacionalnih organizacij (OZN, NATO, EU).[118] Kljub temu pa načelo »potrebe po védenju« – kot osnovni princip delovanja tajnih obveščevalnih služb – ni popolnoma odpravljeno, saj je še vedno potrebno varovati občutljive podatke (osebni podatki, poslovne skrivnosti), kar pa nam omogočajo sofisticirana orodja za ravnanje s podatki, ki so sposobna prikazati netajne verzije tajnih podatkov in »metapodatke«, brez da bi razkrila vir in občutljivo vsebino (Steinberg in drugi 2003, 8).

5.3.2 Nevarnost poseganja v človekove pravice

Varnost že sama po sebi narekuje potrebo po informacijah. Lahko jo povečamo že s prosto dostopnimi informacijami, ki jih nadgradimo z analizo in predelamo v končne

[114] Načelo »potrebe po delitvi« pa niti ni tako novo, saj se je uveljavljalo že prej znotraj zasebnega sektorja pri vzpostavljanju omrežij. Zasebni sektor je sprva nadomestil velike procesno-podatkovne sisteme z osebnimi računalniki. Nato je začel povezovati osebne računalnike v široka omrežja. Uporabnikom so dovolili, da dajo podatke v skupno rabo in si jih delijo med sabo (Treverton 2003, 115).

[115] Korporacije so močno vpletene pri ustvarjanju analitičnih produktov, ki so osnova najbolj pomembnega in občutljivega nacionalnovarnostnega dokumenta, Predsedniškega dnevnega poročila (angl. President's Daily Brief). Predsedniško dnevno poročilo je skupek najbolj pomembnih analiz, ki jih naredi 16 agencij, ki sestavljajo obveščevalno skupnost. Osebja urada Obveščevalnega direktorja pregleda ta poročila in jih pripravi za predsednika vsak dan, kot najaktualnejše in najbolj točne ocene najpomembnejših nacionalnih varnostnih tem. Prav to poročilo je tisto, ki je 6. 8. 2001 opozorilo, da je Bin Laden odločen napasti v ZDA (Hillhouse 2007).

[116] Steele (1996, 220) govori o obstoju »informacijskega kontinuuma«, ki ga sestavljajo vse šole, univerze, knjižnice, podjetja in njihove podatkovne baze, zasebni detektivi, informacijski posredniki, mediji, vse državne ustanove na vseh ravneh delovanja in obveščevalna skupnost. Vse te organizacije skupaj tvorijo neko znanje, ki ga je treba deliti med sabo in ga bogatiti, saj je kontinuum poceni, fleksibilen in odziven, za učinkovito delovanje pa je potrebna nacionalna informacijska strategija, ki bi podrla meje med vsemi temi organizacijami.

[117] Države že sprejemajo zakonodajo, ki ustvarjajo institucionalizirana ekspertna omrežja, ki delujejo na podlagi odprtih informacij kot primarnega vira informacij ter interdisciplinarnosti, povezujejo pa obveščevalno skupnost z zunanjimi državnimi in zasebnimi organizacijami. Ameriški urad Obveščevalnega direktorja (angl. Director of Central Intelligence) je 11. julija 2006 izdal Direktivo obveščevalne skupnosti 301 o vzpostavitvi Nacionalnega podjetja za odprte vire (angl. National Open Source Enterprise). Na podlagi ciljev, ki si jih je zadala ta institucija, naj bi odprti viri postali primarni viri, katere bi združila pod eno streh znotraj ameriške obveščevalne skupnosti, posebej pa bi usposabljala ljudi za pridobivanje odprtih informacij (George 2007). Novi Center za integracijo teroristične grožnje (angl. Terrorist Threat Integration Center), ki je pod nadzorom Obveščevalnega direktorja, pa je zadolžen za sintetiziranje obveščevalnih podatkov iz vseh virov (Steinberg in drugi 2003, 3).

[118] Internet je alternativni model za globalno obveščevalno dejavnost, ki sloni na distribuiranem zbiranju, procesiranju, analizi in obveščevalnih informacijah v skupni rabi (Steele 2002b, 24).

ugotovitve ter jih damo v pretok med zasebnim in javnim sektorjem, ki tako učinkovito zvišajo količnik varnosti. Vendar pa to ne velja za podatke in informacije, za pridobitev katerih je potrebno poseči v ustavno zaščitene področje zasebnosti. Takšna pooblastila imajo le obveščevalne in obveščevalno-varnostne službe, ne pa tudi organizacije civilnega prava. Vpletanje slednjih pri pridobivanju zasebnih podatkov bi pomenilo kršenje zasebnosti (Steinberg in drugi 2003, 6; Bučar 1997, 7). Pravica do **zasebnosti**[119] je ena izmed **temeljnih človekovih pravic** in prav obveščevalne in obveščevalno-varnostne službe so tiste, ki so največkrat v koliziji z lastnimi interesi in pravico posameznika do zasebnosti, saj s pomočjo posebnih ukrepov zbirajo in analizirajo tudi osebne podatke.[120] V zasebnost posameznika se ne sme vmešavati nihče, kar je v pravnih državah tudi ustavno in zakonsko določeno.[121] Država za poseganje v zasebnost opravičuje kot *»zavarovanje enako zaščitenih, a neposredno ogroženih pravic drugih državljanov ali celo družbe kot celote«* (Bučar 1997, 6). Po besedah Bučarja take pravice država ne more (ne sme) prepustiti nikomur drugemu, razen institucijam, ki jih je sama ustanovila in ki so pod njenim nadzorom. *»Ne more pa česa podobnega dovoliti nikakršni drugi zasebni ali paradržavni organizaciji, ker enostavno zanika samo sebe, če bi komurkoli dovolila, da z njenim privoljenjem krši ustavni red.«* (Bučarja 1997, 6)

V kontekstu privatizacije obveščevalne dejavnosti postaja najbolj pereč problem **informacijska zasebnost**, ki je *»sinonim za varstvo osebnih podatkov*[122] *in ena od sestavin zasebnosti«* (Brezovšek in Črnčec 2007, 195).[123] Informacijska tehnologija danes omogoča prikrito zbiranje, obdelavo in nadzor nad ogromnimi količinami osebnih in drugih podatkov, kar predstavlja nevarnost, da se takšni podatki kopičijo v rokah posameznikov ali zasebnih

[119] Po Kaučiču (v Brezovšek in Črnčec 2007, 194) je zasebnost *»nemoteno in svobodno uveljavljanje osebnega in družinskega življenja brez vmešavanja ali nadziranja v imenu države ali drugih subjektov«*.

[120] Nekatere spremembe v ZDA po 11. septembru 2001 so povzročile pravo zaskrbljenost nad potencialnimi trenji med sredstvi nacionalne varnosti, zasebnostjo in vladno odprtostjo, kar je posledica predvsem sprejetja Patriotskega zakon oktobra 2001, Zakona o informacijah o kritični infrastrukturi ter Zakona o domovinski varnosti iz novembra 2002 (Steinberg in drugi 2003, 3–4). V poročilu Skupnega raziskovalnega centra Evropske unije o razvoju digitalnih tehnologij je zapisano, da povečani varnostni ukrepi, ki so posledica dogodkov 11. septembra posegajo v zasebnost posameznikov (Brezovšek in Črnčec 2007, 204–205). Med pisanjem tega diplomskega dela pa je ameriški senat potrdil predlog zakona o prisluškovanju brez sodnih nalogov, s katerim dobivajo (zasebna!) telekomunikacijska podjetja proste roke pri prisluškovanju in imuniteto pred tožbami državljanov, ki so posledica prisluškovanja še iz časa »neformalnega« prisluškovanja (POP TV 2008).

[121] Posegi v zasebnost posameznika so dopustni le z odločitvijo sodišča in ob upoštevanju uporabe najmilejših ukrepov za dosego cilja (Brezovšek in Črnčec 2007, 193).

[122] Osebni podatek je katerikoli podatek, ki se nanaša na posameznika, ne glede na obliko, v kateri je izražen (Zakon o varstvu osebnih podatkov, 6. čl.).

[123] Varstvo osebnih podatkov obsega zbiranje, obdelovanje in prenos osebnih podatkov. *»Varstvo osebnih podatkov je tudi kategorija, ki se v širšem kontekstu umešča v okvir, imenovan zaščita podatkov. Zaščita podatkov obsega […] varstvo posameznikove informacijske zasebnosti in zavarovanje podatkov.«* (Brezovšek in Črnčec 2007, 196)

organizacij (podjetij), saj je te vse težje zavarovati pred zlorabami (Svete 2005, 202). Tisti, ki ima možnost, da poveže različne kategorije osebnih podatkov v podatkovnih bazah, ima neomejene možnosti poseganja v njegovo zasebnost. V ZDA dokazano obstajajo IT podjetja, ki s sofisticirano programsko opremo obdelujejo pridobljene osebne podatke in jih celo prodajajo državnim preiskovalnim organom, čemur ostro nasprotujejo številne organizacije za zaščito državljanskih pravic in opozarjajo, da gre za kršenje zasebnosti in zlorabo osebnih podatkov. Za te zlorabe pa so krivi najbolj uporabniki sami, ki zaupajo osebne podatke; sodišča v ZDA, ki obravnavajo tožbe zoper ta podjetja, zagovarjajo namreč stališče, da *ko enkrat oseben podatek posredujejo podjetju, to ni več osebni podatek, ampak podatek podjetja* (McKay 2005; Bushell 2005).[124]

Do prisvajanja osebnih podatkov lahko pride tudi v medmrežju, ki uporabniku *a priori* ne zagotavlja varnosti, saj sta njegova tehnična in programska konstrukcija usmerjeni v izmenjavo informacij in ne v zagotavljanje tajnosti informacij, kar pa omogoča vsakomur z IT znanjem (ali hekerju), da uporabi številna programska orodja, ki so namenjena prestrezanju, nadzoru in razkrivanju podatkov, ki se pretakajo po medmrežju (angl. malicious programs) (Svete 2005, 202–203). Zato si mora vsakdo, ki je vključen v medmrežje, zaščito zagotoviti in jo tudi razumeti sam, ali pa je žrtev hekerjev (Brezovšek in Črnčec 2007, 202–203).

5.4 Ekonomski vidik privatizacije obveščevalne dejavnosti

Obveščevalna dejavnost kot del nacionalnovarnostnega sistema ni prav nič imuna na globalne trende, ki so prevetrili področje varnosti. Geoekonomsko razumevanje sveta, krepitev vloge korporacij na varnostnem področju, uvajanje tržnih načel v javni upravi, komercializacija informacij in svetovna zmaga kapitalizma so tiste spremembe, ki jih lahko

[124] Prakse zbiranja in prodaje osebnih podatkov so vzbudile pozornost, ko je ameriški IT gigant *ChoicePoint* priznal, da je zaradi vdora hekerjev izgubil kar 145.000 osebnih podatkov, ki vključujejo imena, naslove, številke socialnega zavarovanja, kreditne izpiske in druge osebne podatke (McKay 2005; Bushell 2005). Omenjeno podjetje poseduje 10 milijard zapisov o posameznikih in podjetjih, ki so jih ti (ne)vede posredovali sami. Te podatke nato prodaja kar štiristotim izmed tisoč najbolj uspešnih ameriških podjetij. Prav tako ima sklenjene pogodbe s kar 35. vladnimi agencijami, vključno z organi odkrivanja in pregona kriminala. Običajno se uradniki teh organov zagovarjajo, da jim hitra pridobitev podatkov omogoča hitrejšo in cenejšo obravnavo kriminalnih dejanj. Število informacijskih agentov, ki zbirajo te podatke za denar, pa narašča. Kupci so predvsem kriminalistično-preiskovalne službe, ki se vse pogosteje obračajo na zasebni sektor (McKay 2005). Zloraba podatkov pa ne pozna mejá. Britanski *The Gurdian* je maja 2003 poročal, da naj bi Busheva administracija plačala *ChoicePointu* milijone dolarjev za zbiranje osebnih podatkov o prebivalstvu drugih držav. Nekaj vlad se je že pritožilo, da naj bi podatki bili pridobljeni ilegalno. Podjetje je leta 2002 dobilo vsaj 11 milijonov dolarjev od ameriškega pravosodnega ministrstva za oskrbovanje s podatki iz večinoma Latinske Amerike, ki se nanašajo na detajle, kot so davčni izpisi in krvne skupine posameznikov (Bushell 2005).

kvalificiramo kot ekonomsko komponento privatiziranja obveščevalne dejavnosti. Vedeti moramo, da je kapital tisti, ki usmerja *razvoj* kake dejavnosti, in ta kapital je v rokah posameznikov – zasebnikov. V začetku devetdesetih let 20. stoletja je majhno število mednarodnih korporacij nadziralo 50 odstotkov vseh stroškov raziskav in razvoja, ta korporativni nadzor pa se še krepi na račun nacionalnih interesov ter neprofitnih in znanstvenih organizacij.[125] Uporaba raziskav in razvoja kot vira informacij tako postaja vse pomembnejše obveščevalno orodje transnacionalnih korporacij, saj le-te nadzirajo pretok teh »novonastalih« informacij. Zato morajo korporacije razviti svoje sposobnosti do take mere, da lahko vse te pridobljene informacije in podatke analizirajo in jih s pomočjo *inteligentnih* ljudi (zaposlenih) pretvorijo v znanje ter ga uporabijo pri sprejemanju strateških odločitev. To znanje pa daje konkurenčno prednost na trgu. Blaise Cronin (v Sigurdson 1992, 8) je takšne korporacije poimenoval **inteligentne korporacije**.[126] Bančništvo in trgovina sta dve globalni aktivnosti, v katerima imajo inteligentne korporacije že dolgoletne obveščevalne izkušnje, da bi se obdržale na trgu (Sigurdson 1992, 7–8).[127] Po drugi svetovni vojni so japonska podjetja (jap. sogo shosha) postavile na noge japonsko gospodarstvo. Zaposleni so namreč vzpostavili in ohranjali stike z vladnimi, poslovnimi in strokovnimi krogi, hodili na konference v tujino in doma, ter razvili pravo korporativno kulturo, ki je temeljila na pridobivanju podatkov in informacij iz različnih virov (preko seminarjev, osebnih kontaktov, tiska, medmrežja), kar se je izkazalo v izjemno uspešnem poslovanju in konkurenčnosti na trgu.[128] Po mnenju Nakagawe (1992, 40–42) so ta japonska podjetja dober primer inteligentnih korporacij za informacijsko družbo 21. stoletja, ki bo »obveščevalno vodeno« (angl. intelligene-driven), in

[125] Korporativni nadzor nad razvojem in raziskavami se širi na tri načine. Kot prvo, internacionalizacija raziskav in razvoja se razvija vzporedno z neposrednimi tujimi investicijami in občasno zagotavlja pomembno podporo pri internacionalizaciji proizvodnje. Kot drugo, velika podjetja imajo v številnih državah močan vpliv na nacionalne razvojne programe ali celo neposredno sodelujejo v teh programih. Kot tretje, sama podjetja vzpostavljajo strateška partnerstva z drugimi podjetji (Sigurdson 1992, 7). Peter Manning je pred leti pripomnil, da je ameriška vlada v sodelovanju s korporacijami (predvsem z obrambnega področja) razširila svojo definicijo »nacionalnega interesa« z vključitvijo idej podjetij, kakršna so recimo *Control Risk*, *Kroll*, *Pinkerton* in *Securitas*, katera imajo velike potenciale za raziskave in razvoj (Johnston 2006, 38).

[126] Cronin (v Sigurdson 1992, 8) definira inteligentne korporacije takole: *»Inteligentna korporacija je tista, ki je sposobna rešiti poslovne probleme, preživeti in se konec koncev tudi razvijati. Poskušala bo predvidevati mikro in makro spremembe v okolju, prepoznati vrednost institucionalnega »vedeti-kako«, ustvarjati socialno mreženje … in bo vneta raziskovalka javnih in zakonsko zaščitenih informacij. Informacije o naročnikih bodo povezane … da bi izdelali bogatejše, večdimenzionalne slike o naročnikovih potrebah in preferencah. To bo omogočilo podjetnikom prepoznavati spremembe okusa v javnosti, nadzorovati premoženje, prilagoditi cenovne strategije in učinkovito izvajanje oglaševalskih kampanj.«*

[127] Lagerstamova (v Sigurdson 1992, 8) za bančništvo navaja, da so v glavnem spremenljivi menjalni tečaji in spremenljivi finančni trgi prisilili finančne menedžerje, da so razvili obveščevalna orodja.

[128] Leta 1991 je devet glavnih japonskih podjetij obvladovalo skoraj 50 odstotkov celotnega japonskega izvoza, 60 odstotkov uvoza in skoraj tretjino vseh neposrednih investicij v tujini; to so bile hkrati največje storitvene industrije na svetu, njihov promet pa je bil enak približno tretjini celotnega japonskega bruto domačega proizvoda (Nakagawa 1992, 40–42).

hkrati dober dokaz pomembnosti obveščevalne dejavnosti na gospodarskem področju. **Gospodarska obveščevalna dejavnost**,[129] kot lahko na široko poimenujemo obveščevalno dejavnost na gospodarskem področju, ima tako tudi vpliv na nacionalno varnost, saj trdni ekonomski temelji ne pomenijo le blaginjo, temveč tudi dobro oporo vojaški in politični moči ter pri zagotavljanju varnosti (Kopač 2007, 56–59; Luong 2007, 163; McCarthy 2005, 50; Purg 2002, 29).[130] Obveščevalna dejavnost na gospodarskem področju je v zahodni literaturi običajno poimenovana kot **poslovna in konkurenčna obveščevalna dejavnost** (angl. **b**usiness and **c**ompetitive **i**ntelligence – BI in CI).

5.4.1 Poslovna in konkurenčna obveščevalna dejavnost

Poslovno in konkurenčno obveščevalno dejavnost običajno omenjamo skupaj, ko govorimo o obveščevalnih aktivnostih na gospodarskem področju.[131] Po Pirttimäkiju in drugimi (2006, 32) lahko **poslovno obveščevalno dejavnost** definiramo kot »*organiziran in sistematični proces s katerim organizacije pridobivajo, analizirajo in posredujejo informacije iz obeh virov, notranjih in zunanjih, pomembne za njihove poslovne aktivnosti in sprejemanje poslovnih odločitev«*.[132] Poslovna obveščevalna dejavnost izhaja iz »tendenc po izboljšanju poslovanja«, **konkurenčna obveščevalna dejavnost** pa izhaja iz »razumevanja konkurence na trgu« in je popolnoma prilagojena komercialnemu svetu. Slednjo lahko definiramo kot *»sistematičen, dolgoročen proces, s katerim etično in legalno pridobivamo podatke o kupcih*, *konkurentih, tekmecih, osebju, tehnologijah in o vsem poslovnem svetu«* (Shaker in Gembicki

[129] Gospodarska (ali ekonomska) obveščevalna dejavnost (angl. economic intelligence) je širok pojem in jo lahko definiramo kot organizirano pridobivanje pomembnih **gospodarskih informacij**, vključujoč tehnološke podatke, finančne, zasebne komercialne in vladne informacije, katerih pridobitev s strani tujih interesentov posredno ali neposredno pripomore k relativnemu povečanju produktivnosti ali izboljšanju konkurenčnosti države, iz katere izhaja organizacija ali podjetje, ki pridobiva tovrstne informacije. Gospodarsko obveščevalno dejavnost ne smemo enačiti z gospodarskim vohunjenjem (Luong 2007, 163).

[130] Takšno perspektivo gospodarske moči, ki izhaja iz nacionalnega interesa, zagovarjajo države kot so Ruska federacija, Nemčija, Švedska, Francija, Kitajska in Japonska. Po mnenju McCarthya (2005, 50) se ZDA in VB šele »prebujajo« pri dojemanju gospodarske moči kot esencialne komponente nacionalne varnosti. Po besedah Herberta E. Meyerja (v Nakagawa 1992, 45) *»bi moral biti sistem poslovne obveščevalne dejavnosti v prihodnosti veliko večji kot nacionalni obveščevalni sistem«*.

[131] Angloameriška terminologija za poslovno in konkurenčno obveščevalno dejavnost uporablja običajno enoten izraz in/ali ju enači.

[132] Pirttimäki s sodelavci (2006, 83–90) opredeli omenjeni pojem še kot *»menedžersko orodje, s pomočjo katerega organizacije upravljajo in izboljšajo informacije ter tako sprejemajo bolj efektivne poslovne odločitve«*. Obveščevalni oddelki v podjetjih lahko ustvarijo dobre obveščevalne informacije, vendar pa je bistveno, da jih uprava razume in ceni, kajti v nasprotnem primeru ne bodo uporabne. Izbira pravega obveščevalnega formata je odgovornost obveščevalnega menedžerja. Razumevanje podjetniškega menedžmenta in način motiviranja menedžerjev, da so aktivni, je izziv za vsakega direktorja oddelka za poslovno obveščevalno dejavnost (Herring 1992, 167).

v Odendaal 2004, 2). Poslovno in konkurenčno obveščevalno dejavnost izvajajo tako vladne (državne) kot tudi zasebne organizacije, vse bolj pa postaja veščina zasebnega sektorja, saj cilj te obveščevalne dejavnosti običajno predstavlja zasebna družba. Glede na namen pridobljenih gospodarskih informacij, Treverton (2003, 109) te deli na: (1) *taktične* (uporaba za sprejemanje nadaljnjih odločitev) ali *strateške* (uporaba z namenom izboljšati vzorec politike skozi čas); (2) *ofenzivne* (uporaba za zaščito državnih interesov) ali *defenzive* (uporaba z namenom uveljavljanja državnih interesov zoper nasprotnika); (3) *vladne* (namenjene podpori države) ali *zasebne* (namenjene podpori podjetjem).[133] Večina informacij in podatkov, ki jih pridobimo s poslovno in konkurenčno obveščevalno dejavnostjo, je legalno pridobljena iz odprtih virov.[134] Tajne metode pa se uporabljajo pri **gospodarskem vohunstvu** (angl. economic espionage) (Agrell 1992, 105–106; Luong 2007, 163).[135] Loung (2007, 163) ga opredeli kot *»uporabo nelegalnih, tajnih, prisilnih ali varljivih sredstev s strani tuje vlade ali njenih zastopnikov, z namenom pridobiti gospodarske obveščevalne informacije«*.[136] Naročnik gospodarskega vohunstva je torej vlada, kar pomeni, da lahko tovrstna dejavnost poslabša meddržavne odnose, kakor se je to dogajalo v primeru ZDA in Francije. Slednja je obtožila Washington, da naj bi s pomočjo obveščevalnih služb preko sistema *Echelon*[137] pridobival podatke o francoskih podjetjih in jih posredoval svojim podjetjem, kar so ZDA tudi same očitale Franciji. Bolj zaskrbljujoče je vohunjenje, ko je naročnik zasebnik oziroma zasebna organizacija. V tem primeru govorimo o **industrijskem ali korporativnem vohunstvo** (angl. industrial or corporate espionage). S pomočjo različnih virov (Braine 2003; Guttman 1995, 26; Krantz 2005) lahko rečemo, da je industrijsko vohunstvo pridobivanje skrivnosti o lastnini

[133] Tako lahko na primer državna obveščevalna služba izkoristi priložnost in pridobi nekaj podatkov o tujem podjetju in jih uporabi v korist domačih podjetij. Treverton (2003, 109–110) na primer tako pridobljene gospodarske informacije poimenuje taktično-ofenzivno-zasebne informacije. Vlada lahko podatke, ki so zanimivi za domačo industrijo, pridobi po napaki konkurence, ko jim ta predstavlja svojo industrijo.

[134] Kot pravi Steele (1996, 218–219), ni mogoče niti iz političnih niti iz finančnih razlogov, da bi zasebnim podjetjem pomagali z oskrbovanjem s tajnimi podatki. Gospodarsko vohunstvo je potrebno z razlogom, da »osvetli politično igrišče« vladni administraciji. Pridobivanje tajnih podatkov na račun davkoplačevalskega denarja in v zameno za deleže v podjetjih, vpliv na menedžment in zaposlovanje lahko postane problematično.

[135] Za gospodarsko vohunstvo se uporablja tudi izraz »zunanje industrijsko vohunstvo« (angl. foreign industrial espionage), ker se pridobiva poslovne informacije izključno v tujini

[136] Po ameriškem Zakonu o gospodarskem vohunstvu (Economic Espionage Law 1996) je poslovna skrivnost opredeljena kot *»vsi tipi in oblike finančnih, poslovnih, znanstvenih, tehničnih, gospodarskih ali inženirskih podatkov, vključujoč vzorce, načrte, dognanja, izume, formule, skice, prototipe, metode, tehnike, procese, postopke, programe ali kode, ne glede na to, ali so jasne ali nejasne, in ne glede na to, ali so shranjene, sestavljene ali spravljene fizično, elektronsko, grafično, fotografsko ali pisno, katere je lastnik z razumnimi sredstvi zaščitil, in ki imajo neodvisno ekonomsko vrednost«*.

[137] Echelon je sofisticiran telekomunikacijski in informacijski nadzorni sistem vzpostavljen med ZDA, Kanado, Veliko Britanijo in Avstralijo, ki omogoča prestrezanje satelitskih, mikrovalovnih, celičnih in optičnih povezav v Evropi in med Evropo, Avstralijo, Kanado, Novo Zelandijo in Severno Ameriko. Gre torej za SIGINT in IMGINT. Pojavljajo se domneve, da naj bi od sistema imela korist nekatera ameriška podjetja, ki so prejemala od vlade ZDA obveščevalne informacije (McCarthy 2005, 51; Braine 2003, 9). ZDA naj bi preko sistema Echelon nadzorovale kar 80 odstotkov vseh komunikacij na svetu (POP TV 2008).

in tehnologijah nekega podjetja s tajnimi sredstvi in s strani zasebne družbe, z namenom doseči konkurenčno prednost na trgu.[138] Vohunstvo torej ni le v domeni države in postaja predmet privatizacije.

5.4.2 Prerazporeditev sredstev in dela

Sredstva, namenjena za delovanje obveščevalne skupnosti, so se od konca hladne vojne občutno zmanjševala, in sicer vse tja do 11. septembra 2001. Od tega obdobja dalje se je proračun namenjen obveščevalni dejavnosti zopet povečeval predvsem na račun »vojne proti terorizmu«.[139] Obveščevalne skupnosti zdaj namenjajo vse več pozornosti obveščevalni dejavnosti odprtih virov, kajti kompleksnega sovražnika se ne da premagati s tehniko, globalna pokritost z vohuni pa je nemogoča (Steele 2002a, 21).[140] OSINT je kot dejavnost poceni, še najbolj pa ga obvladuje zasebni sektor, zaradi česar se država – podobno kot pri ostalih varnostnih storitvah – odloča za **zunanje izvajanje obveščevalne dejavnosti**, katerega dober primer predstavljajo prav ZDA. Kot pravi Shorrock (2007), je ameriška obveščevalna dejavnost, kot kdajkoli poprej, vse bolj odvisna od zunanjih zasebnih izvajalcev. Dopisnik ameriškega Obveščevalnega direktorja (DNI), Ronald P. Sanders, pravi, da je večmesečna študija odkrila, da 25 % celotnega dela obveščevalnih služb opravljajo zunanji izvajalci

[138] Škoda zaradi industrijskega vohunstva naj bi v ameriških podjetjih v letu 1999 bila ocenjena na 2 milijardi USD mesečno. Istega leta sta *Ameriška družba za industrijsko varnost* in podjetje *PricewaterhouseCoopers* naredila raziskavo in ugotovila, da naj bi kraja poslovnih skrivnosti 1000 najuspešnejših ameriških podjetij stala več kot 45 milijard USD. Glavni akter pa naj bi bila ravno Francija (Braine 2003, 8). V letnem poročilu ameriškega Urada nacionalne protiobveščevalne eksekutive (NCIX) poudarjajo, da je povezave med tujimi vladami in zasačenimi tatinskimi subjekti, ki kradejo poslovne skrivnosti, večkrat nemogoče dokazati, kar je potrebno upoštevati pri izbiri razlage vohunstva. Podatki ameriške Obrambno-varnostne službe (angl. Defense Security Service – DSS) v poročilu NCIX iz leta 2003 pravijo, da je bilo v letu 2003 od vseh nezakonitih poskusov pridobitve podatkov o ameriški vojaški tehnologiji le 15 % takih, ki neposredno vključujejo tuje vlade, in 25 % takih, ki so jih izvedle druge organizacije, ki delajo za tujo vlado. Ostali nezakoniti poskusi so bili izvedeni s strani posameznikov v lastno korist (14 %) in s strani predstavnikov zasebnih organizacij v njeno korist (31 %). V ostalih primerih (15 %) je naročnik neznan (Office of the National Counterintelligence Executive 2004).

[139] Od leta 2001 so se stroški obveščevalne dejavnosti v ZDA povečali za okoli 40 odstotkov letno (Shorrock 2007), v Avstraliji pa so se sredstva, namenjena obveščevalni dejavnosti, povečala iz 332 milijonov USD v letih 2000–2001 na 659 milijonov USD v letih 2004–2005 (Australian Government – Inquiry into Australian Intelligence Agencies 2004).

[140] V ameriškem Nacionalnem laboratoriju Los Alamos so v začetku devetdesetih let 20. stoletja ugotovili, da lahko za 100.000 USD in ob izključni uporabi OSINT ta daje boljše ocene o produkciji in razširjanju drog po svetu kot ameriška obveščevalna skupnost s sredstvi v višini od 12 do 15 milijonov dolarjev in ob istimi napori (Steele 1996, 216). Ko je Steele delal še kot civilni predstavnik za vzpostavitev 20 milijonov dolarjev vrednega obveščevalnega centra *The US Marine Corps Intelligence Center*, je odkril, da bi lahko kar 80 odstotkov vseh obveščevalnih zahtev marincev izpolnili z uporabo javnih virov informacij, pri čemer bi nastali stroški v grobi vrednosti 20.000 USD, kar predstavljajo članarine pri podjetjih *LEXIS/NEXIS*, *Jane's Information Group*, *EasyNet* in številnih drugih zasebnih podjetij (Steele 1996, 215). Ameriška obveščevalna skupnost naj bi v prvi polovici devetdesetih let 20. stoletja porabila manj kot 1 odstotek svojega proračuna za odprte vire (Steele 1996, 226).

(Shane 2007). V nekaterih agencijah predstavljajo ti že večinsko osebje, v DIA na primer okoli 51 % (maj 2007), v Pentagonovem Uradu za vojaško protiobveščevalno dejavnost pa je kar 70 % uslužbencev zunanjih izvajalcev (Shorrock 2007; Hillhouse 2007).[141] Za zasebne obveščevalne organizacije naj bi Washington letno porabil 45 milijard USD, medtem ko v letu 2000 le 17,5 milijard USD (KBOO Community Radio 2007; Shorrock 2007; Scahill 2008). Hillhousova (2007) piše, da je Urad obveščevalnega direktorja maja 2007 razkril, da je kar 70 % celotnega proračuna obveščevalne skupnosti namenjenega zunanjim izvajalcem, kar predstavlja radikalno prerazporeditev sredstev v korist privatnega sektorja. Bolj kot delež proračuna pa je zaskrbljujoč podatek, da med 50 in 60 odstotkov delovne sile Ciinega najpomembnejšega direktorata (Direktorata za operacije) – Nacionalne tajne službe (angl. National Clandestine Service), ki je odgovorna tudi za vohunjenje, predstavljajo zaposleni iz zasebnih korporacij (Hillhouse 2007)! Čeprav naj bi zunanji izvajalci izvajali predvsem podporne in upravljavske funkcije, ti opravljajo torej tudi glavne funkcije državnih obveščevalnih služb, s čimer se potem spet pojavi vprašanje politične odgovornosti (Carroll 2007).[142]

6 ZASEBNE OBVEŠČEVALNE ORGANIZACIJE

Privatizacija obveščevalne dejavnosti ne more potekati brez subjektov privatizacije. Večina strokovne literature zgolj na splošno opredeljuje te subjekte, in sicer kot zasebne organizacije in posameznike iz akademske, poslovne ali kakšne druge sfere zasebnega življenja, ki opravljajo obveščevalno dejavnost. Klasična tipologija, ki bi jasno opredelila te subjekte, ne obstaja, zato je potrebno na podlagi vsebine, predstavljene v prejšnjih poglavjih, oblikovati smiselno tipologijo zasebnih obveščevalnih organizacij ter opredeliti njihove značilnosti.

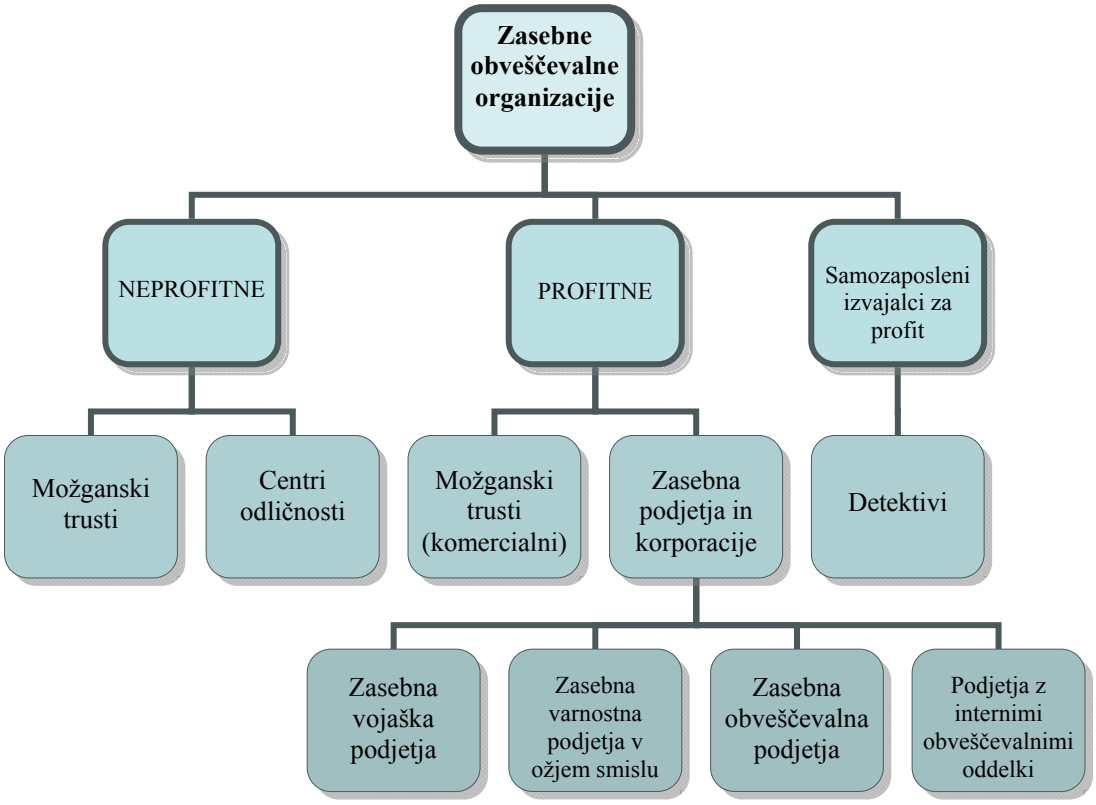
[141] Korporacija *Booz Allen* je z *Science Applications International Corp.*, *General Dynamics, Lockheed Martin*, *Northrop Grumman*, *CACI International* in s številnimi drugimi podjetji ter s 3,7 milijardami dolarjev dohodkov v letu 2005 eden največjih zunanjih izvajalcev. *Booz Allen* naj bi zaposloval več kot 1.000 bivših uslužbencev državnih obveščevalnih služb. Na spletni strani podjetja je avtor našel podatek, da naj bi podjetje zaposlovalo več kot 10.000 oseb, ki so opravili varnostno preverjanje. Med letoma 1997 in 2002 (nanašajoč se na poročilo Zveze ameriških državljanskih svoboščin) je *Booz Allen* v okviru programa *Terrorism Information Awareness* sklenil pogodbe v vrednosti več kot 64. milijonov USD. Med njihovimi naročniki največjega predstavlja NSA, ki nadzira notranje in zunanje komunikacije (telefonski klici in e-sporočila državljanov ZDA) (Shorrock 2007).

[142] James Carroll (2007) še navaja, da naj bi se v zvezi s tem pojavil zanimiv fenomen: uslužbenci državnih obveščevalnih služb, ki jih je na davkoplačevalski račun usposobila država, odhajajo in se zaposlujejo v zasebnih podjetjih, ki opravljajo iste naloge za bistveno večje plačilo, ampak še vedno za istega naročnika.

6.1 Tipologija zasebnih obveščevalnih organizacij s primeri

Pri tipologiji in opredelitvi zasebnih obveščevalnih organizacij bom izhajal iz treh izhodišč, in sicer: (1) da **obveščevalna organizacija** (izvajalec) izhaja iz opredelitve obveščevalne organizacije v širšem smislu po Šaponji (1999, 24); (2) pri opredelitvi zasebne organizacije, ki se ukvarja z obveščevalno dejavnostjo, bom upošteval kriterij **lastništva** in motiv gospodarjenja ter dejstvo, da gre za **nedržavne obveščevalne organizacije**; (3) za zasebne obveščevalne organizacije (in izvajalce) velja, da te izvajajo **obveščevalno dejavnostjo odprtih virov** v skladu s pravnim redom večine zahodnih držav.

Slika 6.2: Pregled obveščevalnih organizacij in izvajalcev v zasebni lasti



Glede na lastništvo in motiv gospodarjenja lahko obveščevalne organizacije (izvajalce) delimo na: **organizacije v lasti države** (obveščevalne organizacije v ožjem pomenu), **neprofitne organizacije v zasebni lasti** s statusom pravne osebe (neprofitne zasebne obveščevalne organizacije), **profitne organizacije v zasebni lasti** s statusom pravne osebe (profitne zasebne obveščevalne organizacije) in **samozaposlene izvajalce** (fizične osebe, ki se

ukvarjajo z obveščevalno dejavnostjo) (Trunka in drugi 2003).[143] Zaradi upoštevanja izhodišča o zasebnem lastništvu bom predstavil samo tiste organizacije, ki so v zasebni lasti. Pogojno bom vključil tudi centre odličnosti, ki jih k obveščevalnim organizacijam prišteva Steele (1996, 219–220).[144] Grafični pregled tipologije zasebnih obveščevalnih organizacij je predstavljen na Sliki 6.2.

6.1.1 Neprofitne obveščevalne organizacije v zasebni lasti

Med neprofitne obveščevalne organizacije v zasebni lasti uvrščamo: *možganske truste* in (pogojno) *centre odličnosti*.

Možganski trust (angl. think tank) je po *Slovarju slovenskega knjižnega jezika* (2005) definiran kot *»skupina ljudi, ki opravlja raziskovalno, svetovalno delo v kaki dejavnosti«*. Možganski trusti so običajno institucionalizirani (kot organizacije, raziskovalni inštituti, korporacije), ukvarjajo pa se z vprašanji in s temami s področij politike, varnosti, ekonomije, znanosti ali tehnologije, poslovanja in vojaškega svetovanja. Kot organizacije zbirajo, sintetizirajo in ustvarjajo vrsto informacijskih produktov za politično osebje, v korist medijev, interesnih skupin, poslovnih subjektov, mednarodne civilne družbe in splošne javnosti. Razlikujejo se po velikosti, strukturi, pomembnosti in po področju raziskovanja, kar povzroča probleme pri definiranju. Lahko delujejo (1) v okviru vlade (nekaterih ruski in kitajski možganski trusti), (2) kot neodvisne neprofitne organizacije, (3) ali pa so del korporacij (Japonska). Za nas sta zanimiva druga dva tipa, saj so ti običajno v zasebni lasti. Angloameriško razumevanje možganskih trustov temelji na logiki »svobodnega mišljenja«, finančno pa so odvisni od različnih sponzorjev in financerjev, zaradi česar se jih razume kot relativno avtonomne in neodvisne organizacije, vključene v analize različnih področij.[145]

[143] Danes poznamo javne (državne), hibridne in zasebne organizacije, vsako skupino organizacijo pa delimo na profitne in neprofitne organizacije (Trunka in drugi 2003).

[144] Pogojno zato, ker ni nujno, da gre za pravni subjekt in zasebni subjekt. Centri odličnosti so v Sloveniji organizirani večinoma v okviru javnih zavodov, inštitutov in univerz. Tak je denimo Center odličnosti Okolje tehnologije, ki deluje v okviru Inštituta Jožef Štefan in se financira iz strukturnih in kohezijskih skladov, del potrebnih sredstev kot lastni vložek pa prispevajo člani centra. Zaradi tega center odličnost ne moremo kvalificirati kot zasebno strukturo (Lojen 2008). Centri odličnosti so lahko organizirani v okviru zasebnih univerz in inštitutov, ki so običajno povezani z verskimi organizacijami, ali pa v okviru večjih korporacij, kakršna je denimo Microsoft, zaradi česar jih lahko kvalificiramo kot zasebne.

[145] Možganski trusti so relativno avtonomni, ker so finančno odvisno od drugih državnih in zasebnih organizacij. Financirajo jih lahko tudi vlade, vendar pa poskušajo ohraniti svojo raziskovalno svobodo in se izogibajo zavezanosti kakršnimkoli specifičnim interesom. Raje poskušajo vplivati na politiko ali jo informirati o

Neprofitni možganski trusti so večinoma oproščeni davka, sredstva pa porabljajo za svoje delo in ne ustvarjajo dobička. Tretji tip možganskih trustov, profitnih, običajno ponujajo storitve svetovanja (Stone in Denham 2003, 3–4). Od akademskih izobraževalnih institucij se razlikujejo po tem, da niso vključeni v izobraževalni proces (»univerze brez študentov«), razen redkih izjem, kot je denimo možganski trust *RAND* (Stone in Denham 2003, 3–5).

Za primer možganskega trusta lahko vzamemo *Hudsonov inštitut*, ki je zaseben, neodvisen, neprofiten raziskovalni možganski trust, ustanovljena leta 1961. Financira se iz donacij podjetij in posameznikov. Inštitut analizira in pripravlja priporočila o javnih politikah za poslovne in vladne organizacije in javnost nasploh. Hudsonov inštitut zagotavlja strateške rešitve za prihodnost skozi interdisciplinarnost in študije na področjih mednarodnih odnosov, obrambe, ekonomije, kulture, znanosti, tehnologije in prava. S pomočjo publikacij, konferenc in političnih priporočil skuša vplivati na svetovne voditelje vlad in podjetij. Inštitut je sprevidel kompleksnost razpada Sovjetske zveze, vzpona Kitajske in pojava islamskega radikalizma, zato se osredotoča na običajno spregledane medsebojne vplive kulture, demografije, tehnologije, trgov in političnega vodstva. Deluje tako doma kot v tujini. Inštitut je v devetdesetih letih prejšnjega stoletja pomagal novonastalim baltiškim gospodarstvom; doma so pomagali pri ustvarjanju zakona o reformah za blaginjo, ki je postal model uspešnih reform za blaginjo na sredini devetdesetih let 20. stoletja; danes pa razvijajo programe političnih in gospodarskih reform za preoblikovanje muslimanskega sveta (Foreign Affairs Online 2006).[146]

Center odličnosti (angl. center of excellence) je visokokakovostna multidisciplinarna skupina raziskovalcev iz akademske sfere (univerz, inštitutov), gospodarstva ter ponekod tudi iz vladnih institucij, ki zagotavlja kritično maso znanja in ustrezno raziskovalno infrastrukturo. Lahko gre za institucionalizirano, fizično skupino raziskovalcev ali virtualno skupnost v medmrežju. Centri odličnosti so lahko organizirani v okviru javnih ali zasebnih zavodov, v okviru slednjih pa predvsem v primerih, ko delujejo znotraj korporacij. Centri odličnosti se ukvarjajo s pridobivanjem podatkov in informacij, analizo teh in pretvorbo

posameznih temah skozi intelektualno argumentiranje in analizo, kot pa se ukvarjati z neposrednim lobiranjem (Stone in Denham 2003, 3–4).

[146] Trenutna raziskovalna področja tega možganskega trusta so: globalne zadeve (varnostne strategije prihodnosti, prihodnost muslimanskega sveta, politika Bližnjega Vzhoda, evropske študije, evrazijska politika, vzpon Azije in odnosi z ZDA, človekove pravice in verska svoboda, severnoameriške varnostne študije); znanost, okolje in tehnologija (svetovne teme o prehrani, globalno segrevanje, okoljske študije); pravo, kultura in družba; mednarodno vladanje (OZN in politika Bližnjega Vzhoda); gospodarstvo in energetska politika. (Hudson Institute 2008)

ugotovitev v nek končni produkt (znanje). Centri odličnosti so usmerjeni primarno v krepitev sposobnosti prenosa in obvladovanja novih tehnologij. Centri odličnosti prispevajo k razvoju inovacijskega okolja z učinkovitejšim prenosom znanja v produkte, storitve in procese z visoko dodano vrednostjo ter s pospeševanjem zagona in razvoja novih tehnološko usmerjenih dinamičnih podjetij. Financirani so s strani sponzorjev, običajno s strani poslovnih subjektov, ali pa v okviru strukturnih in kohezijskih skladov. Profitnih centrov odličnosti ni (SYPC 2006; Lojen 2008).

Dober primer centra odličnosti je *Intelligroupov center odličnosti* (angl. Intelligroup's Center of Excellence), ki pomaga Intelligroupovim uporabnikom pri soočanju z vitalnimi poslovnimi potrebami. Omenjeni center odličnosti zagotavlja upravljanje z ERP rešitvami, ki zagotavljajo večjo raven integracije mnogih vidikov poslovanja (finance, človeški viri, vzdrževanje). Center odličnosti zagotavlja kontinuirane izboljšave poslovnih procesov, da bi obogatil poslovne uporabnike, končne uporabnike in IT operacije z ERP izkušnjami. Skladno s poslovnimi cilji podjetjem zagotavljajo rešitve in podporo, ki pripomorejo k poslovnemu uspehu in povečanju vrednosti iz obstoječih ERP investicij. Center odličnosti svojim strateškim partnerjem omogoča možnost izboljšanja ponudbe in zagotavljanja največjih možnih poslovnih in tehnoloških koristi ter koristi uporabnikov. Intelligroupov center odličnosti kot glavne komponente ponudbe navaja: poslovne analize, izboljšanje poslovnih in tehnoloških procesov, nadgradnje, nove aplikacije, pomoč uporabnikom, menedžment znanja, svetovanje, testne in kontinuirane izboljšave, optimizacijo in nadziranje ključnih indikatorjev kvalitete storitev/blaga. Center je razvil aplikacijo »myAdvisor«, orodje za menedžment znanja, s katerim omogočajo samo-učenje, ponovno uporabo znanja in zajemanje znanja področnih in poslovnih procesov (Intelligroup 2006).

6.1.2 Profitne obveščevalne organizacije v zasebni lasti

Med profitne obveščevalne organizacije štejemo *komercialne možganske truste* in *zasebna podjetja in korporacije*. Komercialni možganski trusti za razliko od nekomercialnih svoje končne obveščevalne izdelke prodajajo za dobiček državnim in zasebnim subjektom.[147]

[147] Za komercialne možganske truste bi lahko rekli, da delujejo podobno kot neprofitni možganski trusti, a podobno kot svetovalna podjetja, ki ponujajo analitične in svetovalne storitve v zameno za plačilo. Kljub pravno-formalni neodvisnosti se lahko ti možganski trusti odpovejo neodvisnosti v korist korporacije, kar jih uvrsti med profitne možganske truste (Stone in Denham 2003, 3–4).

Zasebna podjetja in korporacije, ki se ukvarjajo z obveščevalno dejavnostjo, pa lahko v grobem razdelimo na: (1) zasebna vojaška podjetja, (2) zasebna varnostna podjetja v ožjem smislu, (3) zasebna obveščevalna podjetja (agencije) in (4) podjetja z internimi obveščevalnimi oddelki (običajno večja podjetja in korporacije).

Podjetje z internimi obveščevalnimi oddelki je lahko katerokoli večje podjetje.[148] Raziskava podjetja *Gfk Gral-Iteo* iz leta 2003 v Sloveniji je pokazala, da se s poslovno in konkurenčno obveščevalno dejavnostjo znotraj podjetij in korporacij ukvarjajo oddelki ali službe za prodajo in marketinški oddelki. Sledijo jim oddelki za tržne raziskave in službe za strateško načrtovanje, šele nato pa zunanja podjetja (Vrenko Peruško 2004). Podjetja so glede tega področja precej občutljiva in zato tudi nerada priznavajo obveščevalne aktivnosti. Z gotovostjo pa lahko rečemo, da sem spadajo vsa večja podjetja v Sloveniji.

Primer profitnega možganskega trusta je *The Sanwa Research Institute and Consulting (SRIC) Corporation*. Gre za enega izmed največjih japonskih komercialnih možganskih trustov, ki je bil ustanovljen leta 1985 kot neodvisna podpora banki *The Sanwa Bank, Ltd.*, eni izmed vodilnih japonskih bank (Stone in Denham 2003, 165). SRIC zagotavlja specializirane svetovalne in raziskovalne storitve tako za javne kot tudi zasebne organizacije. SRIC zaposluje 450 raziskovalcev in svetovalcev, v letu 1998 pa je zabeležil rekordno prodajo v vrednosti 72 milijonov USD. Glava področja delovanja so: mednarodne raziskave in svetovanje (strateško načrtovanje in organizacijske spremembe, menedžment informacijskih sistemov, inventurni nadzor in izboljševanje proizvodnje, financiranje malih in srednje velikih podjetij, prodor na tuje trge, mednarodno povezovanje in prevzemanje), svetovanje pri ustvarjanju korporativnih strategij (kratkoročni, srednjeročni in dolgoročni načrti, iskanje strateških ciljev, svetovanje pri prodaji, marketingu, človeškimi viri in organizacijskem preoblikovanju), raziskovanje javnih politik (infrastruktura, tržne in industrijske politike, izobraževanje, okolje), mestni in regionalni razvoj (analize, načrtovanje in oblikovanje regionalnega gospodarskega razvoja), industrijsko raziskovanje (raziskave, analize in napovedovanje tržnih trendov, multimedijska in komunikacijska tehnologija, svetovanje na zdravstvenem področju) ter finančno raziskovanje in svetovanje (raziskovanje in

[148] Po raziskavi, opravljeni s strani podjetja Gfk Gral-Iteo leta 2003 v Sloveniji, ki je zajela 39 podjetij, se je s poslovno in konkurenčno obveščevalno dejavnostjo ukvarjalo kar 60 odstotkov vseh podjetij z več kot 3,3 milijona evrov prihodka v letu 2003, 46 odstotkov podjetij s prihodkom v rangu od 830.000 evrov do 3,3 milijona evrov v letu 2003, ter 17 odstotkov podjetij z manj kot 830.000 evrov prihodka v letu 2003 (Vrenko Peruško 2004).

napovedovanje na finančnih trgih, svetovanje pri poslovnih strategijah za finančne institucije, razvoj in novi finančni produkti) (Engineering and Consulting Firms Association 2008).

Kot primer zasebnega vojaškega podjetja pa lahko vzamemo podjetje *Northbridge Services Group*, katerega direktor je Robert W. Kovacic in je registrirano v Dominikanski Republiki z uradi v VB in Ukrajini. Podjetje je specializirano za zagotavljanje varnostnih storitev za potrebe vlad, multinacionalk, nevladnih organizacij, zasebnega sektorja in posameznikov. Glavne dejavnosti podjetja so: svetovanje (strateško, operativno, taktično planiranje, operativne analize, analize groženj, načrtovane kriznega menedžmenta), usposabljanje (temeljno in napredno, usposabljanje specialnih enot, deminerjev in uslužbencev za psihološke in obveščevalne operacije), operativna podpora (podpora C4I, zračna podpora, podpora posebnih enot, logistika, razoroževanje vojskujočih se strani, ognjena podpora, zdravstvena podpora, nadzorovanje volitev), humanitarne operacije, strateško komuniciranje (odnosi z javnostjo, mednarodno lobiranje, politične analize), podpora redu in miru v konfliktih (protiterorizem, boj proti organiziranemu kriminalu, operacije ohranjanja in uveljavljanja miru), obveščevalna dejavnost. Pri obveščevalni dejavnosti gre za zagotavljanje širokega spektra elektronskih, fotografskih in HUMINT obveščevalnih informacij. Za organizacije, ki želijo ohraniti interne obveščevalne oddelke, podjetje zagotavlja primerne strukture za zbiranje podatkov, pri čemer te strukture vzdržuje s svetovanjem in s posodabljanje informacij (Northbridge Services 2008).

Primer zasebnega varnostnega podjetja v ožjem smislu je denimo podjetje *Aegis*, zasebna britanska varnostna korporacija iz Londona, ki zagotavlja strateško podporo vladam in komercialnemu sektorju s storitvami na področju varnosti in storitvami, povezanimi z obveščevalno dejavnostjo. Zagotavlja svetovanje v zvezi z mednarodnim terorizmom, varnostjo in kompleksnimi geopolitičnimi temami. Glavne naloge korporacije so: analiza tematskega in geopolitičnega tveganja; zbiranje podatkov, analiza in interpretacija obveščevalnih informacij; dajanje ocen tveganosti in ogrožanj; zagotavljanje političnih in varnostnih ocen ter iskanje primerne fizične lokacije za podjetja ter lokalne izvajalce storitev. Glavna vloga *Aegisa* v Iraku je zagotavljanje obveščevalnih informacij o dogajanju v državi drugim varnostnim podjetjem. Znotraj korporacije *Aegis* deluje obveščevalna enota (podjetje) *AEGIS Research and Intelligence Advisory* (ARIA), ki se ukvarja s strateškim svetovanjem in poslovno obveščevalno dejavnostjo. Specializirano je za raziskovanje, obveščevalno dejavnost in analizo poslovnega tveganja, interpretiranje politik mednarodnega sklepanja

poslov, dajanje ocen ogrožanj (terorizem, kriminal, politična nestabilnost), bolj pa se osredotoča na manj predvidljive in politično občutljive komponente tveganj, kot so geopolitika, ideologija, politične osebnosti in skupine, ter druge državne oblike nevarnosti in ekstremizma. ARIA vodi lastno podatkovno bazo o terorizmu, ki se dnevno posodablja, ter ponuja na medmrežju temelječe storitve ATAS, ki zagotavljajo oceno terorističnega ogrožanja pristanišč širom po svetu. Zaposleni v *Aegisu* prihajajo večinoma iz vojske, nekaj pa jih je tudi iz obveščevalnih služb (AEGIS 2008).

Za primer zasebnega obveščevalnega podjetja lahko izberemo podjetje *GPW (Grayson, Pender, Wordsworth)*. Gre za neodvisno podjetje, ki se ukvarja s poslovno obveščevalno in detektivsko dejavnostjo. Podjetje zagotavlja svojim naročnikom obveščevalne in detektivske storitve, ki jih na spletni strani podjetja kategorizirajo v tri skupine: »storitve pred dogodki« (pomoč naročnikom pri sprejemanju poslovnih odločitev pred investiranjem, agitiranju za pogodbe in prevzemanju podjetij), »storitve v teku dogodkov« (podpora pri sovražnih prevzemih, pomoč pri reševanju delničarskih problemov, konkurenčna obveščevalna dejavnost, pomoč pri strategijah podjetij), »storitve po dogodkih« (podpora pri mednarodnih sporih, iskanje in odkrivanje dobičkonosnih poslov, preiskovanje in detektivska dejavnost v zvezi z internimi prestopki ali sleparstvom, protiobveščevalna in protivohunska dejavnost, preiskovanje računalniškega kriminala). Stranke podjetja GPW so multinacionalke, javna in zasebna podjetja, pravne službe, investicijske in komercialne banke, finančne institucije, krovni skladi, zavarovalnice ter premožnejši in pomembnejši posamezniki iz vseh kontinentov. Dela prav tako za javni sektor, vključujoč vladne institucije in agencije ter zakonodajna telesa. Zmožnost podjetja, da opravlja storitve po celem svetu, je podprta z mrežo različnih virov. GPW ima po celem svetu aktivne operativce, ki zbirajo informacij v pravem času (angl. real-time) (GPW 2008).

6.1.3 Samozaposleni izvajalci obveščevalne dejavnosti

Med samozaposlene izvajalce obveščevalne dejavnosti lahko štejemo **detektive**, ki opravljajo ta poklic samostojno. Po Zakonu o detektivski dejavnosti lahko detektivi svoj poklic opravljajo tudi v detektivski družbi. Detektivi opravljajo detektivsko dejavnost, ki jo naša zakonodaja opredeljuje kot dejavnost zbiranja in posredovanja informacij, pridobljenih v skladu s pravicami, ki jih detektivom daje ta zakon (Zakon o detektivski dejavnosti, 3. čl.).

Gre torej za dejavnost zbiranja, analiziranja in posredovanja podatkov (Brvar 1997, 28; Zavod Republike Slovenije za zaposlovanje 2008), kar bi lahko opredelili kot obveščevalno dejavnost v širšem smislu.

V Sloveniji je detektivska dejavnost dobro razvita, zato bom uporabil naključni slovenski primer. Zasebni detektiv *Matjaž Škrabl* med drugimi opravlja naslednje storitve: izdelava strokovnih mnenj na podlagi ekspertov in forenzičnih raziskav za požare, mamila, nezgode, varovanje in drugo; ugotavljanje lojalnosti zaposlenih; preiskovanje zavarovalniških goljufij; pridobivanje dokaznega gradiva s fotografiranjem, video in avdio snemanjem; preiskovanje tatvin; ugotavljanje kršitev s področij koriščenja pravic v državnih in zasebnih organizacijah; preverjanje zakonske zvestobe; svetovanje in ustrezna pravna pomoč; sistematično zbiranje podatkov o poslovnih in fizičnih subjektih iz različnih virov, analiziranje in dokumentiranje teh informacij; pridobivanje informacij o bonitetah poslovnih partnerjev ter o bivališčih dolžnikov in pogrešanih oseb; raziskave trga in možne ovire pri poslovni dejavnosti; preventivno izobraževanje ter storitve po želji naročnika v skladu z Zakonom o detektivski dejavnosti in ostalo zakonodajo Republike Slovenije. Detektiv deluje tudi v državah bivše Jugoslavije, in sicer v skladu z zakonodajo države gostiteljice (Privatni detektiv z licenco – Matjaž Škrabl 2007).

6.2 Značilnosti zasebnih obveščevalnih organizacij

Zasebne obveščevalne organizacije se od obveščevalnih služb državnega sektorja razlikujejo po številnih značilnostih opravljanja obveščevalne dejavnosti. Pri strnitvi ključnih značilnosti, ki sem jih navedel skozi diplomsko delo, bom za obveščevalne organizacije v ožjem smislu (državne) uporabljal izraz obveščevalne službe, ker v slovenščini ta izraz konotira »državno«, medtem ko bom za obveščevalne organizacije v širšem smislu (zasebne) uporabljal izraz zasebne obveščevalne organizacije.

Zasebne obveščevalne organizacije so po **pravno-organizacijski obliki** pravne in/ali fizične osebe ali samo organizacijske enote podjetij, obveščevalne službe pa so opredeljene kot vladne službe ali kot organi v sestavi ministrstva.

Če upoštevamo **tip organizacije**, ugotovimo, da gre pri zasebnih obveščevalnih organizacijah za odprti tip (prilagodljiva, sodelujoča, procesna koordinacija) in/ali naključni tip organizacije (inovativna, neodvisna, iniciativna koordinacija), pri obveščevalnih službah pa za bolj zaprti (tradicionalna, avtokratična, hierarhična koordinacija), v prenovljeni obliki pa tudi za bolj sinhroniziran tip organizacije (učinkovita, harmonična, povezana koordinacija).

Organizacijske značilnosti zasebnih obveščevalnih organizacij so prilagodljivost, fleksibilnost in deljivost informacij (odprti tip) ter kreativna domiselnost in izkoriščanje osebnih sposobnosti (naključni tip). Značilnost obveščevalnih služb pa je predvsem stabilna varnost (zaprti tip), pri »posodobljenih« obveščevalnih službah pa tudi tiha uspešnost in skladno izvajanje.

Odločitve, ki jih sprejemajo v zasebnih obveščevalnih organizacijah, temeljijo bolj na soglasju, skupinskem procesu, pogajanjih (odprti tip) in so neformalne ter individualne (naključni tip), medtem ko so v obveščevalnih službah odločitve formalne in gredo po sistemu »od zgoraj navzdol« in glede na vlogo (zaprti tip); lahko pa so tudi nepogajalske, predhodno določene in »vsiljene« z vizijo (sinhroniziran tip).

Poslanstvo zasebnih obveščevalnih organizacij je: obveščanje širšega ali ožjega kroga javnosti, prispevek k razvoju posameznih znanstvenih disciplin in tehnologije ter delovanje pri zaščiti nacionalnih interesov na varnostnem, političnem in gospodarskem področju. Za obveščevalne službe pa pravimo, da je njihovo poslanstvo predvsem v delovanju pri zaščiti nacionalnih interesov na varnostnem, političnem in gospodarskem področju (zagotavljanju nacionalne varnosti).

V zasebnih obveščevalnih organizacijah je **motiv delovanja** zaslužek – dobiček (pri profitnih) in osebno uveljavljanje ter prispevek k razvoju določene discipline (pri profitnih in neprofitnih). V obveščevalnih službah pa je motiv delovanja varnost državljanov.

Pri opravljanju obveščevalne dejavnosti se zasebne obveščevalne organizacije lahko opirajo le na odprte **vire informacij in podatkov**, medtem ko se obveščevalne službe opirajo tako na odprte kot tudi tajne vire.

Zasebne obveščevalne organizacije za razliko od obveščevalnih služb ne smejo posegati po tajnih nezakonitih **metodah** (gospodarsko/industrijsko vohunstvo), saj je to nemoralno in se sankcionira v skladu z domačo zakonodajo, organizacija pa izgubi ugled.[149] Morebitni zasačeni vohuni zasebnih obveščevalnih organizacij niso zaščiteni niti po mednarodnih konvencijah niti po državni zakonodaji. Po zakonodaji države, kjer so vohunili, se jih obravnava kot tatove.

Obveščevalna dejavnost odprtih virov, katero obvladujejo zasebne obveščevalne organizacije, je **cenejša in zahteva manj časa** za izdelavo končnih obveščevalnih informacij v primerjavi z obveščevalno dejavnostjo obveščevalnih služb, ki tradicionalno temelji na tajnih virih in zahteva **več časa in sredstev** (SIGINT, IMGINT), zaradi česar se obveščevalne službe odločajo za nakup cenejših in bogatejših obveščevalnih produktov zasebnih obveščevalnih organizacij (Hulnick 2002).

Za zasebne obveščevalne organizacije je bolj značilna **struktura lastnega izbora informacij**, medtem ko je za obveščevalne službe značilna **struktura usmerjenega posredovanja informacij**.

Zasebne organizacije imajo ponekod **lažji dostop** do informacij kot obveščevalne službe.[150] Poleg tega, dejavnost zasebnih obveščevalnih organizacij **ni pod nadzorom**, kot ta velja v demokratičnih družbah za obveščevalne in obveščevalno-varnostne službe, in tako zasebne obveščevalne organizacije **niso politično** odgovorne nikomur.

Zelo pomemben je tudi **vir financiranja**, ki se bo v prihodnosti verjetno še najbolj spreminjal. Zasebne obveščevalne organizacije se financirajo iz lastnih storitev (profitne) ali s pomočjo sponzorjev in donatorjev (neprofitne), medtem ko so obveščevalne službe odvisne od državnih proračunov, iz katerega po eni strani črpajo vse manj sredstev zaradi zmanjševanja vloge države pri zagotavljanju varnosti in posledične stroškovne racionalizacije znotraj javnega sektorja, po drugi strani pa so ti državni proračuni vse bolj glavni vir financiranja zasebnih obveščevalnih organizacij (primer ZDA). To pa je lahko dober indic, da

[149] Komercialno vohunstvo (zasebni sateliti, medmrežje), ki je manj vsiljivo, je sprejemljivo dokler se da pred njim zaščititi (požarni zid). V zasebnem sektorju je ena izmed tajnih metod tudi t.i. »črna propaganda«, ki temelji na izmišljenih in prikrojenih podatkih, na podtikanjem laži ter na uporabi drugih prevar (Hulnick 2002).

[150] Obveščevalne službe dajejo zasebnim možganskim trustom, kot je recimo RAND, posamezne projekte o mednarodnih gospodarskih temah predvsem zaradi tega, ker imajo analitiki RAND-a lažji dostop do Svetovne banke in Mednarodnega monetarnega fonda ter drugih zasebnih bankirjev (Treverton 2003, 233–234).

bodo zasebne obveščevalne organizacije v prihodnosti **vse bolj konkurenčne obveščevalnim službam** držav, vsaj dokler bo obstajal kapitalizem; uporabnik – *homo economicus* – pa bo kot zadnji odločil, za kakšno kakovost bo plačeval komu in po kakšni ceni.

7 OBVEŠČEVALNA DEJAVNOST ZASEBNIH SUBJEKTOV V REPUBLIKI SLOVENIJI: ANALIZA PRAVNE PODLAGE

V Sloveniji trenutno še manjka zavesti o privatizaciji obveščevalne dejavnosti, glede na obseg slovenskih virov o tej tematiki pa je slabše obdelana tudi na papirju. Nekateri zasebni subjekti v Sloveniji (detektivi, podjetja) so dejansko že subjekti privatizacije obveščevalne dejavnosti, vendar pa se tega ali ne zavedajo ali ne priznavajo, ker se obveščevalno dejavnost v Sloveniji konceptualno še vedno pripisuje državnim službam.[151] Takšen koncept se bo kmalu znašel v škripcih sodobnih trendov, tako kot v večini zahodnih držav do zdaj, zato je potrebno privatizacijo obveščevalne dejavnosti v Sloveniji sprejeti kot logičen in pravno utemeljen proces znotraj tržno usmerjenih demokratičnih držav.

Privatizacija obveščevalne dejavnosti in varnosti nasploh je utemeljena v sami Ustavi Republike Slovenije.[152] Pravica do pridobivanja javno dostopnih informacij in podatkov (javnih in sivih) je aksiom demokratične družbe in hkrati predpogoj za razvoj obveščevalne dejavnosti odprtih virov. Pravica do pridobivanja tajnih podatkov, poslovnih skrivnosti ali osebnih podatkov pa je pravno omejena. Z uzurpacijo te pravice lahko kršimo ustavnopravni red ter posegamo v temeljne človekove pravice, zaradi česar je prav, da smo s pravnimi akti s področja pridobivanja tovrstnih podatkov in informacij prej dobro seznanjeni.

[151] To je razvidno tudi pri opredeljevanju služb, ki se ukvarjajo z obveščevalno dejavnostjo, katere se še vedno deli na obveščevalno-varnostne (ali varnostno-obveščevalne) in varnostne službe, kar bo povzročilo pravo zmedo ob vzklitju tistih zasebnih obveščevalnih organizacij, ki po svoji funkciji in dejavnosti ne bodo varnostne.

[152] Z vidika izvajalcev za profit so ti privatizacijski procesi utemeljeni v pravnem dejstvu, da gre za uresničevanje pravice do svobode dela (Ustava Republike Slovenije, 49. čl.) in svobodne podjetniške pobude (Ustava Republike Slovenije, 74. čl.), ki je postala z odločbo Ustavnega sodišča z dne 9.6.1994 iztožljiva človekova pravica (Zalar 1997, 46-47). Z vidika izvajalcev, ki se ukvarjajo z nepridobitno obveščevalno dejavnostjo, pa gre za uresničevanje svobode izražanja (Ustava Republike Slovenije, 39. čl.), svobode znanosti in umetnosti (Ustava Republike Slovenije, 59. čl.) ter pravice iz ustvarjalnosti (Ustava Republike Slovenije, 60. čl.).

7.1 Osebni podatki in informacijska varnost

Ustava Republike Slovenije (Ustava RS) v 35. členu varuje pravice zasebnosti in osebnostne pravice; po 37. členu je zagotovljena tajnost pisem in drugih občil, pri čemer lahko samo zakon predpiše, da se na podlagi odločbe sodišča za določen čas ne upošteva to varstvo tajnosti pisem in drugih občil in nedotakljivost človekove zasebnosti, če je to nujno za uvedbo, ali potek kazenskega postopka ali za varnost države. Po 38. členu pa zagotavlja varstvo osebnih podatkov in določa, da je zbiranje, obdelovanje, namen uporabe, nadzor in varstvo tajnosti osebnih podatkov določeno z zakonom. Pomembno vlogo ima tudi 39. člen, ki poleg svobode izražanja zagotavlja še pravico do pridobitve informacije javnega značaja.

Zaradi (pre)splošnosti 39. člena Ustave RS je bil sprejet **Zakon o dostopu do informacij javnega značaja**, kateri ureja postopek, ki vsakomur omogoča prost dostop in ponovno uporabo informacij javnega značaja, s katerimi razpolagajo javni organi.[153] Po 5. členu so informacije javnega značaja prosto dostopne pravnim ali fizičnim osebam, pod enakimi pogoji.[154]

Zakon o varstvu osebnih podatkov določa pravice, obveznosti, načela in ukrepe, s katerimi se preprečujejo neustavni, nezakoniti in neupravičeni posegi v zasebnost in dostojanstvo posameznika pri obdelavi podatkov.[155] Če pridobimo osebne podatke iz javno dostopnih virov (Facebook, telefonski imenik), postanemo upravljavec zbirke osebnih podatkov, kar nas zavezuje k spoštovanju ostalih določb zakona, ki se nanašajo na upravljavce zbirk podatkov.[156] Ta zakon se po 7. členu, ki opredeljuje *izjeme pri uporabi tega zakona*, ne uporablja za obdelavo osebnih podatkov, ki jo izvajajo posamezniki izključno za osebno uporabo oziroma za domače potrebe. Pravno podlago za o*bdelavo podatkov v zasebnem*

[153] Po 4. členu (Zakon o dostopu do informacij javnega značaja) je informacija javnega značaja tista informacija, ki izvira iz delovnega področja organa, nahaja pa se v obliki dokumenta, zadeve, dosjeja, registra, evidence ali drugega dokumenta, ki ga je izdal organ. Arhivsko gradivo ni informacija javnega značaja. Ponovna uporaba informacije javnega značaja pa pomeni uporabo za pridobitne ali nepridobitne namene.

[154] Po 6. členu (Zakon o dostopu do informacij javnega značaja) lahko organ dostop do teh informacij zavrne. Delni dostop pa po 7. členu pomeni, da je del dokumenta (tajni podatki, poslovne skrivnosti, osebni podatki) izločen (Zakon o dostopu do informacij javnega značaja).

[155] Obdelava podatkov pomeni v skladu s 6. členom zakona (Zakon o varstvu osebnih podatkov) *kakršnokoli delovanje ali niz delovanj, ki se izvaja v zvezi z osebnimi podatki*.

[156] Po 6. členu je *upravljavec osebnih podatkov* fizična ali pravna oseba ali druga oseba javnega ali zasebnega sektorja oziroma oseba, določena z zakonom, ki določa namene in sredstva obdelave osebnih podatkov (Zakon o varstvu osebnih podatkov).

sektorju določa 10. člen zakona.[157] V 17. členu zakon obravnava *obdelavo osebnih podatkov za zgodovinsko, statistično in znanstveno-raziskovalne namene*.[158] Nekoliko vprašljiv je 36. člen, ki govori o *omejitvi pravic posameznika*, ki obveljajo iz razlogov, kateri predstavljajo poslanstvo nekaterih zasebnih podjetij in organizacij.[159] Če so osebni podatki namenjeni *neposrednemu trženju*, potem velja upoštevati 72. in 73. člen tega zakona. Prvi pogoj za dopustnost neposrednega trženja po zakonu je, da ponudnik osebne podatke, ki jih uporablja za namene trženja, pridobi bodisi iz javno dostopnih virov bodisi v okviru zakonitega opravljanja dejavnosti. Katere osebne podatke lahko izvajalec trženja uporablja, določa 72. člen zakona.[160] Splošne določbe glede *videonadzora* pa določa 74. člen.[161] V členu ni opredeljeno, kaj je videonadzorni sistem, ki izvaja videonadzor, zato tudi ni jasno, ali je uporaba komercialnih satelitskih slik, ki se lahko nanašajo na posameznika, po tem zakonu dovoljena. Prav tako ni jasno, kje in v katerih oblikah mora biti obvestilo objavljeno. Če pa upoštevamo 7. člen in denimo snemamo drugega posameznika, tvegamo odškodninsko tožbo

[157] Osebni podatki v zasebnem sektorju se lahko obdelujejo, če obdelavo osebnih podatkov in osebne podatke, ki se obdelujejo, določa zakon ali če je za obdelavo določenih osebnih podatkov podana *osebna privolitev posameznika*, na katero se nanaša osebni podatek. Ne glede na prejšnjo določbo se lahko v zasebnem sektorju obdelujejo osebni podatki posameznikov, ki so z zasebnim sektorjem sklenili pogodbo ali pa so na podlagi pobude posameznika z njim v fazi pogajanj za sklenitev pogodbe, če je obdelava osebnih podatkov potrebna in primerna za izvedbo pogajanj za sklenitev pogodbe ali za izpolnjevanje pogodbe. Ne glede na prvi odstavek 10. člena se lahko v zasebnem sektorju obdelujejo osebni podatki, če je to nujno *zaradi uresničevanja zakonitih interesov zasebnega sektorja* in če ti interesi očitno prevladujejo nad interesi posameznika, na katerega se nanašajo osebni podatki (Zakon o varstvu osebnih podatkov, 10. čl.).

[158] Osebni podatki se lahko ne glede na prvotni namen zbiranja nadalje obdelujejo za zgodovinsko, statistično in znanstveno-raziskovalne namene, vendar pa se morajo ti podatki posredovati uporabniku v *anonimizirani obliki*, če zakon ne določa drugače ali če posameznik, na katerega se nanašajo osebni podatki, ni predhodno poslal pisne privolitve, da se lahko obdelujejo brez anonimiziranja. Rezultati obdelave morajo biti *objavljeni v anonimizirani obliki*, razen če zakon določa drugače ali če je posameznik za objavo v neanonimizirani obliki podal pisno privolitev ali če je za takšno objavo podano pisno soglasje dedičeve umrle osebe po tem zakonu (Zakon o varstvu osebnih podatkov, 17. čl.).

[159] Po 36. členu je mogoče z zakonom pravice posameznikov iz 19. (obveščanje posameznika o obdelavi osebnih podatkov), 30. (pravica posameznika do seznanitve) in 32. člena (pravica do dopolnitve, popravka, blokiranja, izbira in ugovora) tega zakona izjemoma omejiti iz razlogov varstva suverenosti in obrambe države, *varstva nacionalne varnosti* in ustavne ureditve države, varnostnih, političnih in *gospodarskih interesov države*, izvrševanja pristojnosti policije, *preprečevanja*, *razkrivanja, odkrivanja, dokazovanja* in *pregona kaznivih dejanj* in prekrškov, odkrivanja in kaznovanja kršitev etničnih norm za določene poklice, iz monetarnih, proračunskih ali davčnih razlogov, zaradi nadzora nad policijo in varstva posameznika, na katerega se nanašajo osebni podatki, ali pravic in svoboščin drugih. Takšne omejitve se lahko določijo **samo v obsegu, ki je nujen za dosego namena**, zaradi katerega se določa omejitev (Zakon o varstvu osebnih podatkov, 36. čl.).

[160] Upravljavec osebnih podatkov lahko za namene **neposrednega trženja** uporablja le naslednje osebne podatke, ki jih je zbral v skladu s prejšnjim odstavkom: *osebno ime, naslov stalnega ali začasnega prebivališča, telefonsko številko, naslov elektronske pošte ter številko telefaksa*. Na podlagi osebne privolitve posameznika pa lahko upravljavec osebnih podatkov obdeluje tudi druge osebne podatke, občutljive osebne podatke pa le *ob pisni privolitvi* posameznika (Zakon o varstvu osebnih podatkov, 72. čl.).

[161] Oseba, ki izvaja videonadzor, mora o tem objaviti *obvestilo*, ki mora biti *vidno in razločno* in objavljeno na način, ki omogoča posamezniku, da se seznani z njegovim izvajanjem najkasneje, ko se nad njim začne izvajati videonadzor. Tretji odstavek 74. člena določa, da mora obvestilo iz prejšnjega odstavka vsebovati informacije: (1) da se izvaja videonadzor; (2) naziv osebe, ki ga izvaja; (3) telefonsko številko za pridobitev informacije, kje in koliko časa se shranjujejo posnetki iz vidonadzornega sistema (Zakon o varstvu osebnih podatkov, 74. čl.).

ali uvedbo kazenskega postopka. Po 80. členu tega zakonu so opredeljeni tudi *biometrijski ukrepi v zasebnem sektorju* .[162] *Rok shrambe osebnih podatkov* je omejen po 21. členu.[163]

Zakon o elektronskem poslovanju in elektronskem podpisu definira podatke v elektronski obliki, elektronsko sporočilo, (varen) elektronski podpis, informacijski sistem, in druge pojme,[164] ter *izenačuje dokumente/podatke v fizični obliki z dokumenti/podatki v elektronski obliki*, ki je ustrezno zaščitena, overjena in podpisana (12. in 13. člen zakona).

Zakon o elektronskih komunikacijah med drugimi ureja zaščito tajnosti in zaupnosti elektronskih komunikacij in druga vprašanja povezana z njimi. Po 103. členu so operaterji dolžni zagotavljati *zaupnost komunikacij*.[165] V skladu s 105. členom, ki govori o *prikazu identitete kličočega priključka in priključka v zvezi* lahko naročnik zahteva izsleditev klicev.[166] Po členih od 107. do 107.e lahko operater *zakonito prestreza komunikacije* in hrani

[162] Zasebni sektor lahko izvaja biometrijske ukrepe le, če so nujno potrebni za opravljanje dejavnosti, za varnost ljudi ali premoženja ali za varovanje tajnih podatkov ali poslovne skrivnosti. Biometrijske ukrepe lahko izvaja *le nad svojimi zaposlenimi*, če so bili predhodno o tem pisno *obveščeni* (Zakon o varstvu osebnih podatkov, 80. čl.).

[163] Po izpolnitvi namena obdelave se morajo osebni podatki **zbrisati, uničiti, blokirati ali anonimizirati**, če niso opredeljeni kot arhivsko gradivo oziroma če zakon ne določa drugače (Zakon o varstvu osebnih podatkov, 21. čl.).

[164] Podatki v elektronski obliki so v skladu z 2. členom tega zakona *podatki, ki so oblikovani, shranjeni, poslani, prejeti ali izmenljivi na elektronski način*. **Elektronsko sporočilo** je niz podatkov, ki so poslani ali prejeti na elektronski način, kar vključuje predvsem elektronsko izmenjavo podatkov in elektronsko pošto. **Elektronski podpis** je niz podatkov v elektronski obliki, ki je vsebovan, dodan ali logično povezan z drugimi podatki, in je namenjen preverjanju pristnosti teh podatkov in identifikaciji podpisnika. **Informacijski sistem** je programska, strojna, komunikacijska in druga oprema, ki deluje samostojno ali v omrežju in je namenjena zbiranju, procesiranju, distribuciji, uporabi in drugi obdelavi podatkov v elektronski obliki. **Varen elektronski podpis**, overjen s kvalificiranim potrdilom, je po 15. členu zakona enakovreden lastnoročnemu podpisu in ima zato enako veljavnost in dokazno vrednost (Zakon o elektronskem poslovanju in elektronskem podpisu).

[165] Zaupnost komunikacij se po 103. členu nanaša na (1) vsebino komunikacij; (2) podatke o prometu in lokacijske podatke, povezane s komunikacijo; (3) dejstva in okoliščine v zvezi s prekinitvijo povezave ali s tem, da povezava ni bila vzpostavljena. Operater in vsakdo, ki sodeluje pri zagotavljanju in izvajanju njegove dejavnosti, je dolžan varovati zaupnost komunikacij tudi po prenehanju opravljanja dejavnosti, pri kateri jo je bil dolžan varovati. Vse oblike nadzora oziroma prestrezanja, kot so *prisluškovanje, poslušanje, snemanje, shranjevanje in posredovanje komunikacij iz prvega odstavka* tega člena **prepovedane**, razen če je to dovoljeno v skladu s 4. odstavkom tega člena ali v skladu s 107. do 107.e (zakonito prestrezanje komunikacij) členom tega zakona oziroma, če je takšna oblika nadzora oz. prestrezanja nujno potrebna za prenos sporočil (npr. elektronska pošta, storitev SMS). N**aročnik ali uporabnik lahko komunikacijo snema**, vendar mora pošiljatelja oziroma prejemnika komunikacije o tem obvestiti. Dovoljeno je tudi *snemanje komunikacij* in z njimi povezanih podatkov o prometu v okviru zakonite poslovne prakse z namenom, da se zagotovi dokaz o tržni transakciji ali katerikoli drugi *poslovni komunikaciji*, ali v okviru organizacij, ki sprejemajo klice v sili, zaradi njihove registracije, identifikacije in reševanja. Uporaba elektronskih komunikacijskih omrežij za shranjevanje podatkov ali pridobitev dostopa do podatkov, shranjenih v terminalni opremi naročnika ali uporabnika, je dovoljena samo pod pogojem, da je bil uporabnik ali naročnik razumljivo **obveščen** o upravljavcu in namenih obdelave teh podatkov (Zakon o elektronskih komunikacijah).

[166] Če naročnik pisno zahteva od operaterja, da izsledi zanj zlonamerne ali nadležne klice, sme operater začasno beležiti izvor vseh klicev. Operater mora podatke o sledenju shraniti in o rezultatu sledenja obvestiti naročnika in mu jih *na utemeljeno zahtevo tudi izročiti*. Pod pogoji in na način iz 107. člena pa jih mora izročiti tudi pristojnim organom (Zakon o elektronskih komunikacijah, 105. čl.).

podatke na podlagi odredbe sodišča. Ob koncu hranjenja podatkov morajo operaterji te uničiti. V 109. členu tega zakona so opredeljene *neželene komunikacije*, ki pomenijo vdiranje v informacijsko zasebnost.[167] Operaterji pridobivajo, uporabljajo in hranijo samo tiste podatke o naročnikih, ki jih določa 110. člen.[168]

Gospodarske družbe lahko do podatkov o komunikacijah zaposlenih pridejo tudi na podlagi **Splošnega akta o razčlenjenem računu**, to je, specifikacije z razčlenjenimi klici, ki je tako podrobna, da omogoči preverjanje računa za uporabo telefonskih storitev ali posameznih klicev.[169]

Kazenski zakonik Republike Slovenije v 137. členu določa sankcije za *neupravičeno prisluškovanje in zvočno snemanje*, v 138. členu pa *neupravičeno slikovno snemanje*.[170] S 140. členom so predvidene sankcije za *nedovoljeno uporabo zasebnih pisanj* brez dovoljenja pooblaščene osebe. V 143. členu je opredeljena *zloraba osebnih podatkov* in predvidene sankcije zanjo,[171] v 221. členu pa *napad na informacijski sistem*, ki se nanaša na

[167] Uporaba samodejnih klicnih sistemov za opravljanje klicev na naročnikovo telefonsko številko brez človekovega posredovanja (klicni avtomati), faksimilnih naprav ali elektronske pošte za namene neposrednega trženja je *dovoljena samo na podlagi naročnikovega predhodnega soglasja*. Ne glede na določbe prejšnjega stavka lahko fizična ali pravna oseba, ki od kupca svojih izdelkov ali storitev pridobi njegov elektronski naslov za elektronsko pošto, ta naslov uporablja za neposredno trženje svojih izdelkov ali storitev, vendar mora kupcu dati *možnost*, da kadarkoli na *brezplačen in enostaven način zavrne* uporabo njegovega elektronskega naslova. (Zakon o elektronskih komunikacijah, 109. čl.).

[168] Operater zbira o svojih naročnikih (1) osebno ime ali ime firme naročnika, (2) dejavnost naročnika, (3) naslov, (4) naročniško številko, (5) naziv naročnika ali naslov njegove elektronske pošte, (6) na podlagi plačila še dodatne podatke, če to želi naročnik in ne posega v pravice tretjih oseb, (7) davčno in matično številko. Operater lahko te podatke uporablja le za sklepanje, izvajanje, spremljanje in prekinitev naročniške pogodbe, zaračunavanje storitev ter pripravo in izdajanje naročniških imenikov v skladu s tem zakonom. Te podatke se mora ob prenehanju naročniškega razmerja hraniti še eno leto od takrat, ko je bil naročniku izstavljen obračun za opravljene storitve, če je v tem času izdana odredba pristojnega organa za hranjenje in posredovanje teh podatkov, pa še toliko časa, kot je določeno v tej odredbi (Zakon o elektronskih komunikacijah, 110. čl.).

[169] Vendar pa je pravno vzdržno le, če se ti podatki uporabljajo le za kontrolo obračunavanja in plačevanja telefonskih storitev, vsaka druga uporaba bi pomenila kršitev 8. ali 16. člena Zakona o varstvu osebnih podatkov ter 8. člena Evropske konvencije o varstvu človekovih pravic in temeljnih svoboščin.

[170] Po 137. členu se kaznuje tistega, ki neupravičeno s posebnimi napravami prisluškuje pogovori ali izjavi, ki mu ni namenjena, ali jo zvočno snema, ali jo neposredno prenaša tretji osebi. Enako se kaznuje, kdor zvočno snema njemu namenjeno zaupno izjavo drugega brez njegovega soglasja z namenom, da bi tako izjavo zlorabil, ali omogoči tretji osebi, da se seznani s posnetkom. Po 138. členu je predvidena kazen za tega, ki neupravičeno slikovno snema ali naredi slikovni posnetek drugega ali njegovih prostorov brez njegovega soglasja in pri tem občutno poseže v njegovo zasebnost ali kdor tako snemanje neposredno prenaša tretji osebi ali ji omogoči, da se s posnetkom seznani (Kazenski zakonik Republike Slovenije).

[171] Kazenski zakonik RS predvideva sankcije za tistega, ki uporabi osebne podatke, ki se obdelujejo na podlagi zakona, v neskladju z namenom njihovega zbiranja ali brez osebne privolitve osebe, na katero se osebni podatki nanašajo. Nezakonit je tudi nepooblaščen vstop v računalniško vodeno zbirko podatkov z namenom pridobiti kakšen osebni podatek. Sankcije so predvidene tudi za tega, ki na medmrežju objavi ali omogoči objavo osebnih podatkov žrtev kaznivih dejanj, žrtev kršitev pravic in zaščitenih prič. V skladu s 143. členom se kaznuje tudi tega, kdor prevzame identiteto druge osebe in pod njenim imenom izkorišča njene pravice, pridobiva premoženjsko korist ali prizadene njeno osebno dostojanstvo (Kazenski zakonik Republike Slovenije).

informacijsko varnost.[172] Po 237. členu Kazenskega zakonika RS pa je predvidna kazen za tistega, ki *vdre v poslovni informacijski sistem*. Na podlagi 306. člena Kazenskega zakonika, ki se nanaša na *izdelovanja in pridobivanje orožja in pripomočkov, namenjenih za kaznivo dejanje*, je predvidena kazen tudi za pripomočke vdiranja v informacijske sisteme.[173]

7.2 Poslovne skrivnosti in tajni podatki

Zakon o gospodarskih družbah v 39. členu opredeljuje pojem *poslovne skrivnosti*,[174] v 40. členu pa je opredeljeno *varstvo poslovne skrivnosti*, ki se v zvezi s tem nanaša tudi na zunanje izvajalce neke družbe.[175]

Na tajnost podatkov v zvezi z gospodarsko dejavnostjo se nanaša tudi 5. člen **Zakona o tajnih podatkih**, ki omogoča razglasitev tajnosti podatkov z namenom preprečiti škodljive posledice za gospodarstvo države.[176] Vsak podatek, ki se mu določi tajnost pa ni tajni podatek.[177] Dostop do tajnih podatkov imajo v skladu s 3., 4., 7., 31. ter 31.a členom samo

[172] Po 221. členu se kaznuje tega, ki vdre v informacijski sistem ali neupravičeno prestreže podatek ob nejavnem prenosu v informacijski sistem ali iz njega. Kaznuje se tudi tega, ki v informacijskem sistemu neupravičeno uporabi, spremeni, preslika, prenaša, uniči ali v informacijski sistem neupravičeno vnese kakšen podatek, ovira prenos podatkov ali delovanje informacijskega sistema (Kazenski zakonik Republike Slovenije).

[173] Kazen je predvidena tudi za tega, ki z namenom storitve kaznivega dejanja poseduje, izdeluje, prodaja, daje v uporabo, uvaža, izvaža ali kako drugače zagotavlja pripomočke za vdor ali neupravičen vstop v informacijski sistem (Kazenski zakonik Republike Slovenije, 306. čl.).

[174] Za poslovno skrivnost se štejejo podatki, za katere tako določi družba s pisnim sklepom. S tem sklepom morajo biti seznanjeni družbeniki, delavci, člani organov družbe in druge osebe, ki morajo varovati poslovno skrivnost. Za poslovno skrivnost se štejejo tudi podatki, za katere je očitno, da bi nastala občutna škoda, če bi zanje izvedela nepooblaščena oseba. Družbeniki, delavci, člani organov družbe in druge osebe so odgovorni za izdajo poslovne skrivnosti, če so vedeli ali bi morali vedeti za tako naravo podatkov. **Za poslovno skrivnost se ne morejo določiti podatki, ki so po zakonu javni ali podatki o kršitvi zakona ali dobrih poslovnih običajev** (Zakon o gospodarskih družbah, 174. čl.).

[175] Družba s pisnim sklepom določi način varovanja poslovne skrivnosti in odgovornost oseb, ki morajo varovati poslovno skrivnost. Poslovne skrivnosti družbe morajo varovati tudi osebe zunaj družbe, če so vedele ali če bi glede na naravo podatka morale vedeti, da je podatek poslovna skrivnost. Prepovedano je ravnanje, s katerim bi oseba zunaj družbe poskušala pridobiti podatke, ki so poslovna skrivnost družbe (Zakon o gospodarskih družbah, 40. čl.).

[176] Za tajnega se določi podatek, ki je tako pomemben, da bi z njegovim razkritjem nepoklicani osebi nastale, ali bi očitno lahko nastale, škodljive posledice za varnost države ali za njene politične ali gospodarske koristi in se nanaša na: (1) javno varnost; (2) obrambo; (3) zunanje zadeve; (4) obveščevalno in varnostno dejavnost državnih organov Republike Slovenije; (5) sisteme, naprave, projekte in načrte, pomembne za javno varnost, obrambo, zunanje zadeve ter obveščevalno in varnostno dejavnost državnih organov Republike Slovenije; (6) znanstvene, raziskovalne, tehnološke, gospodarske in finančne zadeve, pomembne za javno varnost, obrambo, zunanje zadeve ter obveščevalno in varnostno dejavnost državnih organov Republike Slovenije (Zakon o tajnih podatkih, 5. čl.).

[177] Podatek, ki mu je bila tajnost določena zato, da bi se prikrilo storjeno kaznivo dejanje prekoračitev ali zloraba pooblastil, ali prikrilo kakšno drugo nezakonito dejanje ali ravnanje, **ni tajen** (Zakon o tajnih podatkih, 6. čl.).

tiste osebe, ki opravljajo določene državniške funkcije in ki imajo dovoljenje za dostop do tajnih podatkov.[178]

Zakon o industrijski lastnini v 8. členu opredeljuje uradno *tajnost* spisov v zvezi s patentno prijavo *in vpogled v* patentne *prijave*.[179]

Tudi **Obligacijski zakonik** po 5. členu (*načelo vestnosti in poštenja*) določa, da morajo udeleženci v obligacijskih razmerjih v prometu ravnati v skladu z dobrimi poslovnimi običaji (poslovno moralo), kar pa je precej meglena določba.

Kazenski zakonik Republike Slovenije v 142. členu opredeljuje *neupravičeno izdajo poklicne skrivnosti*,[180] po 236. členu predvideva sankcije za *izdajo in neupravičeno pridobitev poslovne skrivnosti*,[181] po 238. členu pa določa kazen za *zlorabo notranje informacije*.[182] Kazenski zakonik v 147., 148. in 149. členu obravnava *kršitev avtorskih pravic*.[183]

---

[178] Do tajnih podatkov lahko v skladu s 3. členom dostopajo predsednik vlade, predsednik republike, poslanec, državni svetnik, župan in občinski svetnik, minister in predstojnik vladne službe, ki je neposredno odgovoren predsedniku vlade, varuh človekovih pravic in njegov namestnik, guverner, njegov namestnik in vice guverner centralne banke, član računskega sodišča, sodnik, državni tožilec, generalni državni pravobranilec in informacijski pooblaščenec. Te osebe dobijo dovoljenje z začetkom funkcije in podpisom izjave, da so seznanjene s tem zakonom in drugimi predpisi, ki urejajo varovanje tajnih podatkov, in da se zavezujejo s tajnimi podatki ravnati v skladu s temi predpisi. Po 4. členu ima dostop do tajnih podatkov brez dovoljenja pri opravljanju svoje funkcije nadzora Komisija Državnega zbora Republike Slovenije za nadzor nad delom varnostnih in obveščevalnih služb (Zakon o tajnih podatkih).

[179] Spisi v zvezi s patentno prijavo in prijavo modela so do objave patentne prijave v uradnem glasilu urada oziroma do registracije modela *uradna tajnost*. V spise, ki so uradna tajnost, je mogoče vpogledati le s soglasjem prijavitelja. Vpogled v spis se brez soglasja prijavitelja dovoli tisti osebi, ki dokaže, da jo je v zvezi z njenim dejanji prijavitelj pisno opozoril na svojo prijavo in obseg zahtevanega varstva (Zakon o industrijski lastnini, 8. čl.).

[180] Na zasebno tožbo se začne pregon tega, ki neupravičeno izda skrivnost, za katero je izvedel kot zagovornik, odvetnik, zdravnik, duhovnik, socialni delavec, psiholog ali kot kakšna druga oseba pri opravljanju svojega poklica. Kazen pa *ni predvidena za tega, kdor izda skrivnost zaradi splošne koristi ali upravičenega interesa javnosti* ali koristi koga drugega, če je ta korist večja kakor ohranitev skrivnosti ali če je z zakonom določena odveza dolžnosti varovanja skrivnosti (Kazenski zakonik Republike Slovenije, 142. čl.).

[181] Po 236. členu se kaznuje osebo, ki **neupravičeno v nasprotju s svojimi dolžnostmi glede varovanja poslovne skrivnosti sporoči ali izroči komu podatke, ki so poslovna skrivnost**, **ali mu kako drugače omogoči, da pride do njih, ali jih zbira z namenom, da jih izroči nepoklicani osebi** (Kazenski zakonik Republike Slovenije).

[182] Kaznivo je, kdor notranjo informacij, ki bi lahko pomembno vplivala na ceno vrednostnega papirja ali drugega finančnega instrumenta, uvrščenega na organiziran trg v Republiki Sloveniji ali v vsaj eni državi članici Evropske unije ali za katero je bil vložen predlog za uvrstitev na tak trg, ne glede na to, ali se z njim trguje na tem trgu ali ne, **pridobi v zvezi s svojim položajem** pri izdajatelju vrednostnega papirja ali lastniškim deležem v kapitalu izdajatelja vrednostnega papirja, svojo zaposlitvijo ali pri opravljanju dejavnosti in jo izkoristi zase ali za koga drugega za pridobitev ali odsvojitev tega vrednostnega papirja ali drugega finančnega instrumenta. Enako se kaznuje osebo, ki notranjo informacijo sporoči nepoklicani osebi ali na podlagi notranje informacije priporoči tretji osebi pridobitev ali odsvojitev tega vrednostnega papirja ali drugega finančnega instrumenta, ter tega, ki nepooblaščeno pride do notranje informacije (Kazenski zakonik Republike Slovenije, 238. čl.).

[183] Bistvena sta 148. in 149. člen. Po 148. členu se kaznuje tega, ki z namenom prodaje neupravičeno uporabi eno ali več avtorskih del ali njihovih primerkov večje premoženjske vrednosti. V skladu s 149. členom pa se

Protipravna pridobitev oziroma *izdaja tajnih podatkov* je opredeljena v 260. členu,[184] *kršitev tajnosti postopka*, kjer lahko pride tudi do izdaje osebnih podatkov ali razkritja identitete, pa je opredeljena v 287. členu kazenskega zakonika.[185] Kot že rečeno, pa se mora zasebni sektor biti še posebej izogibati uporabi *vohunstva*, ki ga opredeljuje 358. člen Kazenskega zakonika.[186]

Zakon o detektivski dejavnosti ureja detektivsko dejavnost in določa pogoje za njeno opravljanje. V skladu z 8. členom sme detektiv pridobivati informacije na podlagi pogodbe s stranko in njenega pooblastila, iz katerega je razvidno področje zbiranja iz 9. člena zakona, namen zbiranja informacij in obseg pooblastila.[187] Za opravljanje detektivske dejavnosti potrebuje detektiv licenco, ki mu jo izda zbornica. Upravljavec zbirke podatkov je v skladu z 10. členom in na podlagi dokazila (pogodbe ali pisnega pooblastila) o konkretni nalogi dolžan dati detektivu podatke iz registrov in evidenc.[188] Detektiv je dolžan ravnati s podatki, pridobljenimi na podlagi 9. in 10. člena, skladno z *zakonom o varstvu osebnih podatkov*. Po 12. členu zakona je detektiv v zadevah, ki jih opravlja, zavezan k molčečnosti, zbrani podatki

---

kaznuje tega, ki neupravičeno reproducira, da na voljo javnosti, razširja ali da v najem eno ali več izvedb, fonogramov, videogramov, rtv-oddaj ali podatkovnih baz večje premoženjske vrednosti (Kazenski zakonik Republike Slovenije).

[184] Nezakonito je, če oseba sporoči ali izroči komu tajne podatke ali mu kako drugače omogoči, da pride do njih, ali zbira take podatke, zato da jih izroči nepoklicani osebi. Sankcionira se tudi, kdor protipravno pride do tajnih podatkov oziroma kdor take podatke brez dovoljenja javno objavi (Kazenski zakonik Republike Slovenije, 260. čl.).

[185] Kaznivo je, kdor neupravičeno izda, kar je izvedel v postopku pred glavno obravnavo ali na obravnavi pred sodiščem, na ustni obravnavi v upravnem postopku ali postopku o prekršku ali postopku parlamentarne preiskave, za kar je z zakonom določeno, da se ne sme objaviti, ali pa je bilo z odločbo pristojnega organa ali sodišča odločeno, da ostane tajno. Kazniva je tudi objava osebnih podatkov otroka, udeleženca v postopku, ali druge informacije s katerimi bi se razkrila identiteta (Kazenski zakonik Republike Slovenije, 287. čl.).

[186] Kaznivo je opravljanje *vohunstva za tujo državo ali tujo organizacijo ali tujega agenta* ali omogočanje, da pride do tega. Prav tako je kaznivo ustvarjanje obveščevalne službe ali njeno vodenje za tujo državo ali tujo organizacijo v škodo Republike Slovenije. Kazniva je tudi vključitev vanjo ali podpora njenemu delu (Kazenski zakonik Republike Slovenije, 358. čl.).

[187] Detektiv lahko pridobiva informacije neposredno od osebe, na katero se podatki nanašajo, lahko pa tudi od drugih oseb, ki so pripravljeni dati podatke *prostovoljno*, in iz sredstev javnega obveščanja, in sicer: (1) o pogrešanih ali skritih osebah, dolžnikih, avtorjev anonimk, povzročiteljev škod; (2) o ukradenih in izgubljenih predmetih; (3) o dokaznem gradivu za zavarovanje ali dokazovanje pravic in stranke pred pravosodnimi in drugimi organi; (4) o zvestobi delavcev pri izvajanju konkurenčne klavzule; (5) o podatkih o uspešnosti in poslovnosti pravnih oseb; (6) o kaznivih dejanjih in storilcih, ki se preganjajo na zasebno tožbo; (7) o disciplinskih kršitvah in kršiteljih; (8) o kandidatih za zaposlitev, v okviru soglasja kandidata za zaposlitev. Pri pridobivanju informacij mora detektiv predhodno opozoriti, da oseba podatke daje prostovoljno (Zakon o detektivski dejavnosti, 9. čl.).

[188] Po 10. členu so to: (1) evidenca registriranih vozil; (2) register stalnega prebivalstva; (3) evidenca zavarovancev (podatki o zaposlitvi); (4) slovenski ladijski register in register zrakoplovov. Detektiv ima pravico vpogleda v sodne in upravne spise, v primerih, ko ima po zakonu to pravico stranka, ki ga je pooblastila. Za pridobitev podatkov po tem členu ni potrebno, da je oseba, na katero se podatki nanašajo, predhodno seznanjena s tem, da se bodo pridobili podatki o njej po tem členu (Zakon o detektivski dejavnosti).

in informacije pa so *poslovna tajnost*; tudi po opravljeni storitvi za stranko.[189] V skladu s 13. členom, detektiv ne sme uporabljati *metod in sredstev*, ki jih v skladu z zakonom uporabljajo državni organi. Prav tako ne sme opravljati dejavnosti za domače in tuje državne organe ter politične stranke. Po 19. členu je dejavnost detektivske družbe (pravna oseba) *omejena na opravljanje detektivskega poklica*, zato je za profitne zasebne obveščevalne organizacije v Slovenijo bolje, da se registrirajo kot take družbe, saj obveščevalna dejavnost odprtih virov ter poslovna in konkurenčna obveščevalna dejavnosti nista zakonsko opredeljena.

Predstavljena zakonodaja je grob okvir, znotraj katerega lahko zasebni sektor razvije svoje obveščevalne zmožnosti za izvajanje obveščevalne dejavnosti v širšem smislu. Kršitev kateregakoli od navedenih pravnih aktov ne pomeni le sankcioniranje in razvrednotenja ugleda, temveč tudi potencialno tiho legitimizacijo poseganja v človekove pravice.

8 ZAKLJUČEK

Predstavljeno zmanjševanje vloge države in povečevanje vloge zasebnega sektorja na področju varnosti torej dokazuje, da država vse bolj izgublja monopol nad zagotavljanjem varnosti svojih državljanov. Koncept politične moči je strohnel, zamenjal pa ga je koncept ekonomske moči. Ekonomija, kot nekdanji instrument politike, sedaj instrumentalizira politiko, edina logika, ki je sprejemljiva v odprtem svetu, pa je logika ponudbe in povpraševanja. Zasebni sektor je tako vse močnejši in vplivnejši faktor v globalnem okolju, v katerem po tržnih načelih in v okviru svojih zmožnosti ponuja drugim subjektom, tako državnim kot nedržavnim, storitve s področja varnosti, kamor štejemo tudi obveščevalno dejavnost. Demonopolizacija se kaže tudi pri oblikovanju varnostnih politik in varnostnih struktur nacionalnovarnostnih sistemov, v katerih zasebni subjekti predstavljajo vse večjo prioriteto. Z veliko gotovostjo lahko torej *prvo hipotezo potrdimo*.

Druga hipoteza pravi, da obveščevalna dejavnost države ne bo preživela v konkurenci z obveščevalno dejavnostjo zasebnih organizacij. Poskušajmo potrditi ali zavrniti to hipotezo z vidika tistega, ki mu je obveščevalna dejavnost namenjena – uporabnika. Naročnik oziroma uporabnik obveščevalnih organizacij je tisti, ki vpliva na razvoj obveščevalnih služb in razvoj

[189] V skladu z 12. členom je detektiv dolžan podati kazensko ovadbo pristojnemu organu, če pride do podatka o storitvi kaznivega dejanja, ki se preganja po uradni dolžnosti. Detektiv je dolžan po izpolnitvi pogodbe stranki izročiti vse v okviru pogodbe zbrane podatke (Zakon o detektivski dejavnosti).

obveščevalne dejavnosti nasploh. Danes je uporabnikov več, v grobem pa jih lahko razdelimo na državne uradnike (državni sektor) na eni ter fizične in pravne osebe (zasebni sektor) na drugi strani. Prvi dandanes ne zahtevajo zgolj tajnih podatkov, temveč celovite informacije oziroma obveščevalne produkte, temelječe na vseh virih, ki so uporabni in omogočajo vpogled v prihodnost. Drugi uporabniki, ti iz zasebnega sektorja, pa so odvisni od obveščevalnih informacij, ki so (večinoma) produkt obveščevalne dejavnosti odprtih virov. Ker pa v obveščevalni dejavnosti državnih organov predstavljajo tajne informacije zgolj manj kot odstotek vseh pridobljenih informacij in ker je odprtih informacij vedno več, bo potrebno zagotoviti na tem področju precej več strokovnjakov, ki obvladujejo in znajo dobro izkoriščati odprte vire. Izkušnje in statistični podatki kažejo, da je takšnih več v zasebnem sektorju. Korporacijske obveščevalne službe so po mnenju Šaponje (v Purg 2002, 28) postale »*kvalitetna konkurenca klasičnim, državnim službam – in to ne le po vsebini dela, temveč tudi po učinkovitosti*«. Kljub temu pa ne smemo prezreti vohunstva, na področju katerega pa ima primat država, pri čemer ima na voljo metode in sredstva, ki jih zasebni sektor v skladu z zakonodajami ne more in ne sme uporabljati. Trenutno obstaja preveč domnev in premalo dokazov, da bi lahko rekli, da zasebni sektor prevzema naloge na področju vohunstva, a vendarle dovolj, predvsem tistih iz ZDA, da poseganja po metodah tajnih služb s strani zasebnega sektorja ne moremo zanikati. Vedeti je treba, da sta politična neodgovornost in nižji stroški izvajanja ključni konkurenčni prednosti zasebnega sektorja, ki zaenkrat (še) ne nista prepričljivejši od pooblastil državnih obveščevalnih služb. Zaključimo lahko torej, da bo obveščevalna dejavnost države kljub vse večji konkurenci iz zasebnega sektorja še naprej obstojala, vendar pa se bosta ti dve prednosti vse bolj uveljavljali na račun poseganja v temeljne človekove pravice. *Hipoteze zato ne moremo niti potrditi niti zanikati*.

Tako kot preostale zahodne države, bo tudi Slovenijo prej kot slej zajel val privatizacije obveščevalne dejavnosti. Tukaj gre zgolj za vprašanje časa, druga – institucionalna – vprašanja, pa sem hotel razrešiti s tretjo hipotezo, da obstoječi pravni red Republike Slovenije ne onemogoča nadaljnjega razvoja obveščevalne dejavnosti zasebnih subjektov. Ta razvoj je seveda neke vrste konceptualni sinonim za privatiziranje obveščevalne dejavnosti, pridevnik »nadaljnji« pa pomeni, da zasebni sektor pri nas že izvaja obveščevalno dejavnost in da jo bo še toliko bolj v prihodnosti. Glede na pravni red, ki sem ga skozi zakonodajo predstavil v sedmem poglavju, lahko rečemo, da ne obstajajo ovire za nadaljnji razvoj obveščevalne dejavnosti, ki temelji na odprtih virih. Poslovna in konkurenčna obveščevalna dejavnost nista posebej urejeni, detektivska dejavnost pa prevzema logiko

obveščevalne dejavnosti odprtih virov in je temu primerno tudi regulirana. Ker v Sloveniji obstaja še dovolj manevrskega prostora za razvoj obveščevalne dejavnosti odprtih virov in ker je ta manevrski prostor zagotovljen z ustavnopravnim redom Republike Slovenije, lahko *tretjo hipotezo potrdimo*.

Smo torej v obdobju privatizacije obveščevalne dejavnosti, ki predstavlja globalen proces in dejstvo, katerega je treba sprejeti. Človekova potreba po informacijah, ne glede na to ali ta potreba izhaja iz državnega ali zasebnega sektorja, je s pojavom novih negotovosti iz okolja prevelika, da bi se slepili in spodkopavali koncept krepitve zasebnega sektorja na področju obveščevalne dejavnosti. Proces privatizacije poteka globalno neenakomerno ter po definiciji okolja, v katerem se odvija. V ZDA in Veliki Britaniji se privatizacija obveščevalnega področja odvija srdito in dinamično, saj je tudi tamkajšnje okolje moč opisati s tema dvema pridevnikoma. Okolje zahodnih držav je dejansko tržišče, kjer vlada nenapisan zakon povpraševanja in ponudbe, in po katerem se ljudje ravnajo na vseh področjih družbenega življenja. Zasebnemu sektorju pomenijo takšne okoliščine vodo na mlin, kar se bo še najbolje izkazalo pri privatizaciji ne le obveščevalne dejavnosti, temveč celotnega varnostnega področja. Država je tukaj razcepljena. Po stroškovni, strokovni in politični plati ji participacija zasebnega sektorja na tem področju ugaja, po plati politične moči, pa se boji izgubljanja vpliva. Svobodne gospodarske pobude po tržnih zakonitostih ni niti legitimno niti legalno omejevati, je pa zato potrebno ohranjati nadzor. Država v sodobnem svetu ne more nadzirati potreb državljanov, ampak mora skrbeti, da vsi procesi, ki prihajajo iz zasebnega sektorja in zadovoljujejo te potrebe, potekajo v skladu z ustavnopravnim redom. Tako kot v razvitih državah, pa bo tudi pri nas veljajo, da bomo priče tako imenovani »tihi revoluciji« (Shearing v Zalar 1997, 42), na katero relevantni politični akterji sploh ne bodo ustrezno reagirali.

Posameznikovi interesi bodo nadvladali družbene, poroštvo varnosti bo povsem v rokah zasebnikov, država pa bo odmrla. Nacionalnost bo zamenjal poklic. Meje med državami bodo nadomestile meje ekonomskih regij, znotraj katerih bo varnost korporacij pomenila varnost regije. Za korporacije bodo značilne obveščevalne službe, notranje in zunanje, ki bodo uporabljale vsa sredstva in metode. Vse te obveščevalne prakse korporacij bodo uzakonjene, saj jih bodo ljudje iz korporacij pisali sami. Ljudje ne bodo akreditirani po političnih funkcijah, temveč po vrednosti na trgu. Osebni podatek bo poslovna skrivnost. To bo srednji ekonomski vek, konec vseh privatizacij.

9 LITERATURA

1. *AEGIS*. Dostopno prek: http://www.aegisworld.com (5. julij 2008).
2. Agrell, Wilhelm. 1992. Global Watch – world events and business intelligence. V *The Intelligent Corporation: The privatisation of intelligence*, ur. Jon Sigurdson in Yael Tagerud, 99–106. London, Los Angeles: Taylor Graham.
3. Allen, Charles. 2002. The Role of Open Source as the Foundation for Successful All-Source Collection Strategies. V *NATO Open Source Intelligence Reader*, 12–16. Dostopno prek: http://www.oss.net/dynamaster/file_archive/030201/254633082e785f8fe44f546bf5c9f1ed/NATO%20OSINT%20Reader%20FINAL%2011OCT02.pdf (28. april 2008).
4. Anžič, Andrej. 2002. Mednarodni terorizem – varnostni izziv in dileme. *Teorija in praksa* 39 (3): 454–466.
5. *Australian Governemt – Inquiry into Australian Intelligence Agencies*. 2004. Dostopno prek http://www.pmc.gov.au/publications/intelligence_inquiry/chapter2/needs.htm (13. julij 2008).
6. Balažic, Milan. 2001. Velika Slovenija: klasični in novi geopolitični koncepti. *Teorija in praksa* 38 (2): 231–243.
7. Barger, Deborah G.. 2005. *Toward a Revolution in Intelligence Affairs*. Santa Monica: The RAND Corporation. Dostopno prek: http://www.rand.org/pubs/technical_reports/2005/RAND_TR242.pdf (28. maj 2008).
8. Baumard, Philippe. 1992. Shifting intelligence needs. V *The Intelligent Corporation: The privatisation of intelligence*, ur. Jon Sigurdson in Yael Tagerud, 83–97. London, Los Angeles: Taylor Graham.
9. Bayley, David H. in Clifford D. Shearing. 2001. *The New Structure of Policing: Description, Conceptualization, and Research Agenda*. Dostopno prek: http://www.ncjrs.gov/txtfiles1/nij/187083.txt (25. april 2008).
10. Bennett, Jody Ray. 2008. *Private intel, the new gold rush*. Dostopno prek: http://www.isn.ethz.ch/news/sw/details.cfm?id=19141 (17. april 2008).
11. Bentley, Trevor J.. 1998. *Managing Information – avoiding overload*. London: The Chartered Institute of Management Accountants.

12. Bergeron, Pierrette in Christine A. Hiller. 2002. Competitive Intelligence. V *Annual Review of Information Science and Technology*, ur. Blaise Cronin, 353–390. Medford: Information Today.
13. Best, Richard A. in Alfred Cumming. 2007. *Open Source Intelligence (OSINT): Issues for Congress*. Dostopno prek: http://ftp.fas.org/sgp/crs/intel/RL34270.pdf (15. maj 2008).
14. Braine, Kevin. 2003. Entente commerciale? How the US and the French do business… *Risk Advisory*, maj. Dostopno prek: http://www.riskadvisory.net/uploads/File/TRAG%20newsletter/Risk%20Advisory%20-%20Issue%202.pdf (16. maj 2008).
15. Brezovšek, Marjan in Damir Črnčec. 2007. *Demokratična uprava in tajnost podatkov*. Ljubljana: Fakulteta za družbene vede.
16. Brvar, Bogo. 1997. Zakon o detektivski dejavnosti dopušča ogrožanje informacijske zasebnosti posameznika. V *Zasebno varovanje in detektivska dejavnost: dileme in perspektive*, ur. Andrej Anžič, 23–35. Ljubljana: Visoka policijsko-varnostna šola.
17. Bučar, France. 1997. Varnost kot dobrina. V *Zasebno varovanje in detektivska dejavnost: dileme in perspektive*, ur. Andrej Anžič, 3–10. Ljubljana: Visoka policijsko-varnostna šola.
18. Bushell, Sue. 2005. *Privatising Intelligence? It's Criminal*. Dostopno prek: http://www.cio.com.au/index.php/id;1887768580;fp;4;fpid;21 (14. april 2008).
19. Carroll, James. 2007. Outsourcing Intelligence. *The Boston Globe*, 27. avgust. Dostopno prek: http://www.boston.com/news/globe/editorial_opinion/oped/articles/2007/08/27/outsourcing_intelligence/ (11. junij 2008).
20. Chorafas, Dimitris N.. 2003. *Outsourcing, Insourcing and IT for Enterprise Management*. Basingstoke, New York: Palgrave Macmillan.
21. Crawford, Adam. 2006. Policing and security as »club goods«: the new enclosures?. V *Democracy, Society and the Governance of Security*, ur. Jennifer Wood in Benoit Dupont, 111–138. Cambridge, New York: Cambridge University Press.
22. Crowther, Jonathan, ur. 1995. *Oxford Advanced Learner's Dictionary of Current English*. Oxford: Oxford University.
23. Cubberley, Maureen in Stan Skrzeszewski. 1999. *Discussion Paper on Outsourcing in Canadian Heritage Institutions (Libraries and/or Museums)*. Dostopno prek: http://www.pch.gc.ca/progs/arts/pdf/outpap_e.pdf (21. februar 2008).

24. Črnčec, Damir. 2005. Potreba po deliti z ostalimi. *Revija Obramba* 37 (2): 28–30.
25. Črnčec, Damir. 2008. Doktorski seminar: Obveščevalna dejavnost v javnem in zasebnem sektorju: gospodarska vs. konkurenčna obveščevalna dejavnost. Ljubljana, 18. maj.
26. Dedijer, Stevan. 2003. *Development & Intelligence 2003-2053: Working Paper Series*. Lund: Lund University. Dostopno prek http://www.lri.lu.se/pdf/wp/2003-10.pdf (24. marec 2008).
27. Dedijer, Stevan. 2005. Obveščevalna knjižnica v obveščevalnem živčnem sistemu Slovenije? *Organizacija znanja* 10 (3): 124–129.
28. Dehqanzada, Yahya A. in Ann M. Florini. 2002. Secrets for Sale: How Commercial Satellite Imagery will change the World. V *NATO Open Source Intelligence Reader*, 39–55. Dostopno prek: http://www.oss.net/dynamaster/file_archive/030201/254633082e785f8fe44f546bf5c9f1ed/NATO%20OSINT%20Reader%20FINAL%2011OCT02.pdf (28. april 2008).
29. Democracy Now!. 2007. *Mike McConnel, Booz Allen and the Privatization of Intelligence*. New York, 12. januar. Dostopno prek http://www.democracynow.org/2007/1/12/mike_mcconnel_booz_allen_and_the (5. maj 2008).
30. Divjak, Tina. 2007. *Nevladne organizacije v Sloveniji*. Dostopno prek: http://www.fikus.si/index.php?option=com_content&task=view&id=2&Itemid=10 (11. februar 2008).
31. Dupont, Benoit in Jennifer Wood. 2006. Conclusion: The future of democracy. V *Democracy, Society and the Governance of Security*, ur. Jennifer Wood in Benoit Dupont, 241–248. Cambridge, New York: Cambridge University Press.
32. Džombić, Jasmina. 2006. *Upravljanje z informacijami*. Diplomsko delo. Ljubljana: Fakulteta za varnostne vede.
33. *Encyclopaedia Britannica 2008*. 2007. Rugeley: Focus Multimedia.
34. *Engineering and Consulting Firms Association*. Dostopno prek: http://www.ecfa.or.jp/english/pdf/sric.pdf (4. julij 2008).
35. Evropska komisija. 2004. *Sporočilo Komisije svetu in Evropskemu parlamentu – Varovanje kritične infrastrukture v boju proti terorizmu*. Dostopno prek: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52004DC0702:SL:HTML (5. maj 2008).

36. Foreign Affairs Online. 2006. *Think Tanks and Research Institutes*. Dostopno prek: http://people.virginia.edu/~rjb3v/T-tanks.html (4. julij 2008).
37. Friedman, Richard S.. 2002. Review Essay – Open Source Intelligence. V *NATO Open Source Intelligence Reader*, 17–23. Dostopno prek: http://www.oss.net/dynamaster/file_archive/030201/254633082e785f8fe44f546bf5c9f1ed/NATO%20OSINT%20Reader%20FINAL%2011OCT02.pdf (28. april 2008).
38. Friedman, Thomas L.. 2006. *The World is Flat: A Brief History of the Twenty-first Century*. New York: Farrar, Straus, Giroux.
39. George, Roger Z.. 2007. *Meeting 21st Century Transnational Challenges: Building a Global Intelligence Paradigm*. Dostopno prek: https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol51no3/building-a-global-intelligence-paradigm.html (23. maj 2008).
40. *GPW*. Dostopno prek: http://www.gpwltd.com (5. julij 2008).
41. Grizold, Anton. 1992. Oblikovanje slovenske nacionalne varnosti. V *Razpotja nacionalne varnosti: obramboslovne raziskave v Sloveniji*, ur. Anton Grizold, 59–93. Ljubljana: Fakulteta za družbene vede.
42. Grizold, Anton. 1996. Posameznikova varnost in obveščevalne službe. V *Zbornik strokovno znanstvenih razprav 10*, ur. Andrej Anžič, 108–115. Ljubljana: Ministrstvo za notranje zadeve Republike Slovenije.
43. Grizold, Anton in Erik Kopač. 2007. Suvremeni izazovi sigurnosti u globaliziranom svijetu. V *Etničke manjine i sigurnost u procesima globalizacije*, ur. Siniša Tatalović, 11–28. Zagreb: Politička kultura.
44. Guttman, Barbara. 1995. *An Introduction to Computer Security: The NIST Handbook*. Washington: U.S. Government Printing Office. Dostopno prek: http://csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf (28. februar 2008).
45. Herring, Jan P.. 1992. The unique role of the future in intelligence. V *The Intelligent Corporation: The privatisation of intelligence*, ur. Jon Sigurdson in Yael Tagerud, 161–181. London, Los Angeles: Taylor Graham.
46. Hillhouse, R.J.. 2007. Outsourcing Intelligence. *The Nation*, 24. julij. Dostopno prek: http://www.thenation.com/doc/20070730/hillhouse (11. junij 2008).
47. Holmqvist, Caroline. 2005. *Private Security Companies: The Case for Regulation*. Solna: SIPRI. Dostopno prek: http://books.sipri.org/files/PP/SIPRIPP09.pdf (25. februar 2008).
48. *Hudson Institute*. Dostopno prek: http://www.hudson.org/ (4. julij 2008).

49. Hulnick, Arthur S.. 2002. *Risky business: private sector intelligence in the United States*. Dostopno prek: http://www.allbusiness.com/management/benchmarking-strategic-planning/245534-1.html (16. maj 2008).
50. *Intelligroup*. Dostopno prek: http://www.intelligroup.com (4. julij 2008).
51. Jardines, Eliot A.. 2002. Understanding Open Source. V *NATO Open Source Intelligence Reader*, 9–17. Dostopno prek: http://www.oss.net/dynamaster/file_archive/030201/254633082e785f8fe44f546bf5c9f1ed/NATO%20OSINT%20Reader%20FINAL%2011OCT02.pdf (28. april 2008).
52. Johnston, Les. 2006. Transnational security governance. V *Democracy, Society and the Governance of Security*, ur. Jennifer Wood in Benoit Dupont, 33–51. Cambridge, New York: Cambridge University Press.
53. *Kazenski zakonik Republike Slovenije* (KZ-1). Ur. l. RS 55/2008. Dostopno prek: http://zakonodaja.gov.si/rpsi/r05/predpis_ZAKO905.html (14. julij 2008).
54. KBOO Community Radio. 2007. *National Applications Office and the Privatization of Intelligence*. Portland: 12. december. Dostopno prek: http://kboo.fm/audio/download/4694/_60 (12. februar 2008).
55. Keegan, John. 2004. *Intelligence in War: The value – and limitations – of what the military can learn about the enemy*. New York: Vintage Books.
56. Kopač, Erik. 2007. Ekonomsko ogrožanje nacionalne varnosti. V *Model celovitega ocenjevanja ogrožanja nacionalne varnosti Republike Slovenije*, ur. Iztok Prezelj, 51–78. Ljubljana: Ministrstvo za obrambo, Direktorat za obrambne zadeve, Sektor za civilno obrambo.
57. Kosar, Kevin R.. 2006. *Privatization and the Federal Government: An Introduction*. Dostopno prek: http://www.fas.org/sgp/crs/misc/RL33777.pdf (15. februar 2008).
58. Kotnik – Dvojmoč, Igor. 2000. Spremembe ekonomskega dejavnika in varnost v sodobnem svetu. *Teorija in praksa* 37 (4): 646–671.
59. Krantz, Richard. 2005. *Industrial Espionage Becomes Favorite Way to Achieve Quick Gains*. Dostopno prek: http://www.voanews.com/english/archive/2005-04/2005-04-29-voa1.cfm?CFID=13237529&CFTOKEN=96310900 (16. maj 2008).
60. Lerner, K. Lee in Brenda Wilmoth Lerner, ur. 2004. *Encyclopedia of Espionage, Intelligence, and Security*. Detroit: Gale.
61. Lilly, Damian. 2000. *The Privatization of Security and Peacebuilding: a framework for action*. Dostopno prek: http://www.reliefweb.int/rw/lib.nsf/db900SID/LGEL-5F9JUE/$FILE/intalert-privatisation-sep02.pdf?OpenElement (12. februar 2008).

62. Lojen, Sonja. 2008. Elektronska pošta. Mežica, 8. julij.
63. Luong, Minh A.. 2007. The Challenges of Economic Intelligence. V *Handbook of Intelligence Studies*, ur. Loch K. Johnson, 163–170. London, New York: Routledge.
64. Manning, Peter K.. 2006. Two case studies of American anti-terrorism. V *Democracy, Society and the Governance of Security*, ur. Jennifer Wood in Benoit Dupont, 52–85. Cambridge, New York: Cambridge University Press.
65. McCarthy, Shaun. 2005. A private, public partnership. *Jane's Intelligence Review* november: 50–51.
66. McCormick Tribune Foundation. 2006. *Understanding the Privatization of National Security*. Dostopno prek: http://www.abanet.org/natsecurity/understanding_privatization_2006.pdf (17. april 2008).
67. McKay, Jim. 2005. *Outsourcing Intelligence*. Dostopno prek: http://www.govtech.com/gt/articles/96792 (11. junij 2008).
68. *Northbridge Services*. Dostopno prek: http://www.northbridgeservices.com (5. julij 2008).
69. Nakagawa, Juro. 1992. Intelligence, trade and industry. V *The Intelligent Corporation: The privatisation of intelligence*, ur. Jon Sigurdson in Yael Tagerud, 39–51. London, Los Angeles: Taylor Graham.
70. *National Defemse Authorization Act for Fiscal Year*. 2006. Dostopno prek: http://www.dod.mil/dodgc/olc/docs/PL109-163.pdf (6. maj 2008).
71. Odendaal, Bernardus Johannes. 2004. *Competitive Intelligence with Specific Reference to the Challenges facing the Competitive Intelligence Professional in South Africa*. Magistrsko delo. Pretorija: Fakulteta za humanistične vede. Dostopno prek: http://upetd.up.ac.za/thesis/available/etd-02092005-112230/unrestricted/00dissertation.pdf (28. februar 2008).
72. Office of the National Counterintelligence Executive. 2004. *Annual Report to Congress on Foreign Economic Collection and Industrial Espionage – 2003*. Dostopno prek: http://www.iwar.org.uk/ecoespionage/resources/senate/annual-reports/fecie_fy03.pdf (3. marec 2008).
73. Page, Michael, Simon Rynn, Zack Taylor in David Wood. 2005. *SALW and Private Security Companies in South Eastern Europe: A Cause or Effect of Insecurity?* Beograd: SALW. Dostopno prek: http://www.seesac.org/reports/psc.pdf (12. februar 2008).

74. Pečar, Janez. 1997. Varnostnopolitični in nadzorstveni pogledi na zasebno varstvo. V *Zasebno varovanje in detektivska dejavnost: dileme in perspektive*, ur. Andrej Anžič, 11–22. Ljubljana: Visoka policijsko-varnostna šola.
75. Pirttimäki, Virpi, Antti Lönnqvist in Antti Karjaluoto. 2006. Measurement of Business Intelligence in a Finnish Telecommunications Company. *The Electronic Journal of Knowledge Management* 4 (1): 83–90. Dostopno prek: http://www.ejkm.com/volume-4/v4-i1/Pirttimaki-Lonnqvist-Kajaluoto.pdf (3. marec 2008).
76. Poles, Ljubo. 2006. Prioritete poveljnikov in njihov vpliv na bojno pripravljenost. *Bilten Slovenske vojske* 8 (2): 7–34.
77. POP TV. 2008. *24UR*. Ljubljana, 10. avgust.
78. Prezelj, Iztok. 2002a. Ogrožanje nacionalne varnosti Republike Slovenije in vključevanje v NATO. *Teorija in praksa* 39 (3): 426–441.
79. Prezelj, Iztok. 2002b. Konceptualizacija nacionalnih varnostnih interesov. *Teorija in praksa* 39 (4): 621–637.
80. Prezelj, Iztok. 2006. Teroristično ogrožanje nacionalne varnosti Republike Slovenije. *Ujma* 20: 177–181.
81. Prezelj, Iztok. 2007. Uvod v ocenjevanje ogrožanja nacionalne varnosti. V *Model celovitega ocenjevanja ogrožanja nacionalne varnosti Republike Slovenije*, ur. Iztok Prezelj, 7–26. Ljubljana: Ministrstvo za obrambo, Direktorat za obrambne zadeve, Sektor za civilno obrambo.
82. *Privatni detektiv z licenco – Matjaž Škrabl*. Dostopno prek: http://www.detect.si/ (10. julij 2008).
83. Purg, Adam. 1994. *Obveščevalne službe, politični sistemi in državna suverenost*. Doktorska disertacija. Ljubljana: Fakulteta za družbene vede.
84. Purg, Adam. 2002. *Primerjalni obveščevalni sistemi*. Ljubljana: Visoka policijsko-varnostna šola.
85. Radovanović, Dragana. 2004. *Intelligence & Lund – What lessons Lund can learn in order to become an intelligent city*. Lund: Univerza v Lundu. Dostopno prek: http://www.entovation.com/whatsnew/Intelligence___Lund.pdf (11. junij 2008).
86. Rathmell, Andrew. 2002. The Privatisation of Intelligence: A Way Forward for European Intelligence Cooperation – »Towards a European Intelligence Policy«. V *NATO Open Source Intelligence Reader*, 56–63. Dostopno prek: http://www.oss.net/dynamaster/file_archive/030201/254633082e785f8fe44f546bf5c9f1ed/NATO%20OSINT%20Reader%20FINAL%2011OCT02.pdf (28. april 2008).

87. Ravbar, Matjaž. 2007. Vladimir Vauhnik: znameniti slovenski obveščevalec. *Revija Obramba* 39 (6): 57–59.
88. Reiter Neal, Stacy. 2008. *Perspectives on Terrorism – Business as Usual? Leveraging the Private Sector to Combat Terrorism*. Dostopno prek: http://www.terrorismanalysts.com/pt/index.php?option=com_rokzine&view=article&id=31&Itemid=54 (5. maj 2008).
89. Roeben, Dietrich F. O.. 2005. *Planning and Controlling the Outsourcing of Maintenance and Technical Services*. Norderstedt: Bookds on Demand GmbH. Dostopno prek: Google Books Search.
90. Roush, Wade. 2008. *IDC Tracks Your »Digital Shadow«* | *Xconomy*. Dostopno prek: http://www.xconomy.com/boston/2008/03/11/idc-tracks-your-digital-shadow/ (28. maj 2008).
91. Scahill, Jeremy. 2008. Balckwater's Private Spies. *The Nation*, 5. junij. Dostopno prek: http://www.thenation.com/doc/20080623/scahill (3. julij 2008).
92. Schreier, Fred in Marina Caparini. 2005. *Privatising Security: Law, Practice and Governance of Private Military and Security Companies*. Geneva: Geneva Centre for the Democratic Control of Armed Forces. Dostopno prek: http://www.dcaf.ch/_docs/occasional_6.pdf (27. februar 2008).
93. Shamsi, Sherry. 2006. *In Defence of Marxism – Terrorism, Security Business and Britain*. Dostopno prek: http://www.marxist.com/terrorism-security-business181206.htm (13. februar 2008).
94. Shane, Scott. 2007. Government Keeps a Secret After Studying Spy Agencies. *The New York Times*, 26. april. Dostopno prek: http://www.nytimes.com/2007/04/26/washington/26contracting.html?_r=2&adxnnl=1&oref=slogin&adxnnlx=1213192981-er668CNy1UQ5uRC4jHvz5g&oref=slogin (11. junij 2008).
95. Sharfman, Peter. 1996. Intelligence Analysis in the Age of Electronic Dissemination. V *Intelligence Analysis and Assessment*, ur. David A. Charters, Stuart Farson in Glenn P. Hastedt, 201–211. London, Portland: Frank Cass.
96. Shearing, Clifford. 2006. Reflections on the refusal to acknowledge private governments. V *Democracy, Society and the Governance of Security*, ur. Jennifer Wood in Benoit Dupont, 11–32. Cambridge, New York: Cambridge University Press.
97. Shorrock, Tim. 2007. The spy who came in from the boardroom. Salon.com, 8. januar. Dostopno prek:

http://www.salon.com/news/feature/2007/01/08/mcconnell/index.html (12. junij 2008).

98. Sigurdson, Jon. 1992. Introduction – The changing role of national intelligence. V *The Intelligent Corporation: The privatisation of intelligence*, ur. Jon Sigurdson in Yael Tagerud, 5–13. London, Los Angeles: Taylor Graham.
99. *Slovar slovenskega knjižnega jezika*. 2005. Ljubljana: Državna založba Slovenije.
100. *Splošni akt o razčlenjenem računu*. Ur. l. RS 18/2002. Dostopno prek: http://zakonodaja.gov.si/rpsi/r08/predpis_AKT_278.html (15. julij 2008).
101. Steele, Robert D.. 1996. Private Enterprise Intelligence: Its Potential Contribution to National Security. V *Intelligence Analysis and Assessment*, ur. David A. Charters, Stuart Farson in Glenn P. Hastedt, 212–228. London, Portland: Frank Cass.
102. Steele, Robert D.. 2002a. *The New Craft of Intelligence: Achieving Asymmetric Advantage in the Face of Nontraditional Threats*. Carlisle: Strategic Studies Institute, U.S. Army War College.
103. Steele, Robert D.. 2002b. Open Source Intelligence: What is it? Why is it important to the military? V *NATO Open Source Intelligence Reader*, 56–63. Dostopno prek: http://www.oss.net/dynamaster/file_archive/030201/254633082e785f8fe44f546bf5c9f1ed/NATO%20OSINT%20Reader%20FINAL%2011OCT02.pdf (28. april 2008).
104. Steele, Robert D.. 2007. Open Source Intelligence. V *Handbook of Intelligence Studies*, ur. Loch K. Johnson, 163–170. London, New York: Routledge.
105. Steinberg, James B., Mary Graham in Andrew Eggers. 2003. Building Intelligence to Fight Terrorism. *The Brookings Institution Policy Brief* 125. Dostopno prek: http://www.brookings.edu/comm/policybriefs/pb125.pdf (28. april 2008).
106. Stone, Diane in Andrew Denham. 2004. *Think Tank Traditions: Policy Research and the Politics of Ideas*. Manchester, New York: Manchester University Press.
107. Stringer, Kevin D.. 2007. Business Concepts for the Security Sector: Benchmarking, Core Competencies, and Outsourcing. *Baltic Security & Defence Review* 9: 210–235.
108. Studeman, William. 2002. Teaching the Giant to Dance: Contradictions and Opportunities in Open Source within the Intelligence Community. V *NATO Open Source Intelligence Reader*, 56–63. Dostopno prek:

http://www.oss.net/dynamaster/file_archive/030201/254633082e785f8fe44f546bf5c9f1ed/NATO%20OSINT%20Reader%20FINAL%2011OCT02.pdf (28. april 2008).

109. Svete, Uroš. 2002. *Vloga in pomen informacijske tehnologije v sodobnem asimetričnem vojskovanju*. Magistrsko delo. Ljubljana: Fakulteta za družbene vede.

110. Svete, Uroš. 2005. *Varnost v informacijski družbi*. Ljubljana: Fakulteta za družbene vede.

111. Svete, Uroš. 2006. Strateški značaj informacijsko-komunikacijske tehnologije u suvremenom međunarodnom okolišu. *Polemos: časopis za interdisciplinarna istraživanja rata i mira* 9 (2): 101–118. Zagreb: Hrvatsko sociološko društvo.

112. *SYPC*. 2006. Dostopno prek: http://www.sycp.si/sycp/Networking_RTD.wlgt (4. julij 2008).

113. Šaponja, Vladimir. 1999. *Taktika dela obveščevalnovarnostnih služb*. Ljubljana: Visoka policijsko-varnostna šola.

114. Tavzes, Miloš, ur. 2006. *Veliki slovar tujk*. Ljubljana: Cankarjeva založba.

115. *The Office of the Director of National Intelligence*. 2008. Dostopno prek: http://www.odni.gov (14. april 2008).

116. Todd, Paul in Jonathan Bloch. 2003. *Global Intelligence: The World's Secret Services Today*. London: Zed Books.

117. Treverton, Gregory F.. 2003. *Reshaping National Intelligence for an Age of Information*. Cambridge, New York: Cambridge University Press.

118. Triglav, Joc. 1996. Informacijska revolucija. *Življenje in tehnika* 47: 27–39.

119. Trunk Širca, Nada, Mitja I. Tavčar in Niko Abrahamsberg. 2003. *Management nepridobitnih organizacij*. Koper: Fakulteta za management.

120. Tyrrell, Patrick. 2002. Open Source Intelligence: The Challenge for NATO. V *NATO Open Source Intelligence Reader*, 3–8. Dostopno prek: http://www.oss.net/dynamaster/file_archive/030201/254633082e785f8fe44f546bf5c9f1ed/NATO%20OSINT%20Reader%20FINAL%2011OCT02.pdf (28. april 2008).

121. Vrenko Peruško, Ines. 2004. *Business intelligence: oči in ušesa uspešnih podjetij*. Dostopno prek: http://www.gfk.si/4_2_lclank.php?cid=1210 (13. maj 2008).

122. *Zakon o detektivski dejavnosti* (ZDD-UPB1). Ur. l. RS 7/2003. Dostopno prek: http://zakonodaja.gov.si/rpsi/r09/predpis_ZAKO3569.html (14. julij 2008).

123. *Zakon o dostopu do informacij javnega značaja* (ZDIJZ-UPB1). Ur. l. RS 96/2005. Dostopno prek: http://zakonodaja.gov.si/rpsi/r06/predpis_ZAKO3336.html (15. julij 2008).

124. *Zakon o elektronskem poslovanju in elektronskem podpisu* (ZEPEP-UPB1). Ur. l. RS 98/2004. Dostopno prek: http://zakonodaja.gov.si/rpsi/r03/predpis_ZAKO1973.html (15. julij 2008).

125. *Zakon o elektronskih komunikacijah* (ZEKom-UPB1). Ur. l. RS 13/2007. Dostopno prek: http://zakonodaja.gov.si/rpsi/r01/predpis_ZAKO3781.html (14. julij 2008).

126. *Zakon o gospodarskem vohunstvu – Economic Espionage Law*. 1996. Dostopno prek: http://www.loyola.edu/dept/politics/intel/pl104294.pdf (15. februar 2008).

127. *Zakon o gospodarskih družbah* (ZGD-1). Ur. l. RS 42/2006. Dostopno prek: http://zakonodaja.gov.si/rpsi/r01/predpis_ZAKO4291.html (14. julij 2008).

128. *Zakon o varstvu osebnih podatkov* (ZVOP-1-UPB1). Ur. l. RS 94/2007. Dostopno prek: http://zakonodaja.gov.si/rpsi/r06/predpis_ZAKO3906.html (14. julij 2008).

129. Zalar, Boštjan. 1997. (Ne)legitimnost privatizacije državnega aparata prisile. V *Zasebno varovanje in detektivska dejavnost: dileme in perspektive*, ur. Andrej Anžič, 37–56. Ljubljana: Visoka policijsko-varnostna šola.

130. Zalar, Boštjan. 1999. *Privatizacija in človekove pravice*. Ljubljana: Fakulteta za družbene vede.

131. *Zavod Republike Slovenije za zaposlovanje*. 2008. Dostopno prek: http://www.ess.gov.si/SLO/Ncips/OpisiPoklicev/DETEKTIV.pdf (7. julij 2008).