UNIVERZA V LJUBLJANI
FAKULTETA ZA DRUŽBENE VEDE

Marko Anžič

KONKURENČNA OBVEŠČEVALNA DEJAVNOST GOSPODARSKIH DRUŽB

Magistrsko delo

Ljubljana, 2010

UNIVERZA V LJUBLJANI
FAKULTETA ZA DRUŽBENE VEDE

Marko Anžič

Mentor: red. prof. dr. Bogomil Ferfila

KONKURENČNA OBVEŠČEVALNA DEJAVNOST GOSPODARSKIH DRUŽB

Magistrsko delo

Ljubljana, 2010

POVZETEK

KONKURENČNA OBVEŠČEVALNA DEJAVNOST GOSPODARSKIH DRUŽB

Pričujoče magistrsko delo je primarno posvečeno proučevanju področja oz. dejavnosti, ki ga slovenska laična in tudi strokovna javnost skorajda ne pozna, kar pa ne velja za večino razvitih držav. Običajno se obveščevalno dejavnost razume in proučuje kot dejavnost, ki jo izvajajo državne obveščevalne službe, kar pa menim, da je bistveno preozek pogled. Obveščevalna dejavnost je dejavnost, ki jo lahko izvaja praktično vsaka organizacija. Takšno obveščevalno dejavnost predstavlja tudi konkurenčna obveščevalna dejavnost, ki jo sam razumem in opredeljujem kot legalni in etični sistematični proces spremljanja poslovnega okolja (s poudarkom na konkurentih in konkurenčnem okolju). Ta kot svoje orodje uporablja obveščevalni krog, katerega končni izdelki, na podlagi katerih je mogoče sprejemati osnovane odločitve, imajo namen pridobiti konkurenčno prednost gospodarski družbi na taktičnem ali strateškem nivoju. Tudi konkurenčno obveščevalno dejavnost lahko izvajajo različni subjekti; sam se osredotočam na gospodarske družbe. V delu je zaradi boljšega in celovitejšega razumevanja te dejavnosti predstavljena tudi zgodovina te dejavnosti in povezave ter vplivi informacijske revolucije in gospodarske obveščevalne dejavnosti. Pomemben poudarek preko celotnega dela dajem najpogostejšemu očitku tej sicer legalni in etični dejavnosti, to je vohunjenju oz. povezavi konkurenčne obveščevalne dejavnosti z vohunjenjem. Ker je to dejavnost, ki lahko pomeni določene odmike od legalnosti, so predstavljene tudi možne zlorabe in nadzor nad to dejavnostjo. Na podlagi treh empiričnih raziskav, proučene literature ter pogovorov s strokovnjaki sem poskusil čim bolje predstaviti to dejavnost tudi v Sloveniji.

Ključne besede: Konkurenčna obveščevalna dejavnost, obveščevalna dejavnost, vohunjenje

ABSTRACT

COMPETITIVE INTELLIGENCE IN COMPANIES

The present work is primarily devoted to the study of the activity which is almost unrecognized by the Slovenian non academic as well as academic public. However this does not apply for most developed countries. Generally the intelligence is understood and studied as an activity performed by national intelligence agencies, yet I believe this view is much too narrow. Intelligence is an activity that can be performed by virtually any organization. Such »type« of intelligence is also competitive intelligence, which I understand and define as legal and ethical systematic process of monitoring the business environment by focusing on competitors and competitive environment). As its tool it uses the intelligence cycle of which intelligence products, based on which decisions can be taken, are intended to gain competitive edge for the company at tactical or strategic level. Competitive intelligence can too be performed by different subjects; I concentrate on the companies. Due to better and more comprehensive understanding of this activity I present the history of competitive intelligence and its connections to the information revolution and the economic intelligence. Throughout the present work I especially emphasize the most frequent recrimination about this otherwise legal and ethical activity, i.e. espionage and its reference to the competitive intelligence. Since competitive intelligence is an activity which may involve some deviation from legality, possible misuses and control over this activity are presented. Based on three empirical studies, study of literature and discussions with experts, I wanted to present the state of competitive intelligence also in Slovenia.

Keywords: Competitive intelligence, intelligence, espionage

KAZALO

SEZNAM SLIK IN TABEL

UVOD

Zelo zanimivo je razmišljanje Jéquierja in Dedijerja (1987, 22-23), ki sta odlično zajela duh časa, v katerem je bil njun prispevek napisan. Avtorja menita, da je obveščevalna dejavnost ponavadi razumljena kot dejavnost, ki jo izvajajo nacionalne obveščevalne službe, ki so primarno zaskrbljene z vojaškimi ali strateškimi nalogami. Nacionalne obveščevalne službe, ki se ukvarjajo z notranjo ali zunanjo varnostjo, z zbiranjem informacij ali s protiobveščevalno dejavnostjo, predstavljajo zgolj vrh ledene gore obveščevalne dejavnosti v katerikoli družbi. Ta vrh je daleč najbolj proučevan in privlači javnost. Toda ta visoka »vidnost« nacionalnih obveščevalnih služb je odvrnila pozornost strokovne javnosti, novinarjev in zgodovinarjev od mnogo pomembnejšega in širšega področja obveščevalne dejavnosti, ki jo izvajajo korporacije, družbene skupine, zasebne institucije in vladne agencije.

Če je bilo to povsem razumljivo v času hladne vojne, ko je bila osredotočenost strokovne in laične javnosti povezana tudi ali predvsem s strahom mogočega izbruha »vroče« vojne (v hladni vojni so seveda imeli obveščevalna dejavnost in njeni izvajalci, obveščevalne službe, ogromno vlogo), pa naj bi ta koncepcija izgubljala na pomenu vse od tedaj naprej, kar je lepo ponazoril Podbregar (2008, 18). "S premikom od geopolitike h geoekonomiji v globalnem svetu informacijske dobe se je prostor obveščevalne dejavnosti razširil v podjetniško sfero." Pa temu v celoti vendarle ni bilo tako. Takoj po koncu hladne vojne smo bili in smo še vedno priča asimetriji varnostnih groženj s praktično nešteto vidikov. Po napadih, ki so se zgodili 11.09.2001, se je pojavila t.i. »vojna proti terorizmu«, ki jo od leta 2001 vodijo predvsem v ZDA, so jo vodili v Veliki Britaniji in je (skoraj) povsem zasenčila kakršnokoli drugo obveščevalno dejavnost, kot le to, ki je povezana z nacionalno varnostjo in predvsem s preprečevanjem terorizma. "Po 11. septembru 2001 se je tudi trend v obveščevalni dejavnosti, ki je potekal od konca hladne vojne, k ekonomsko konkurenčni dejavnosti, spremenil in se je spet povečala klasična – državna obveščevalna dejavnost… Trend sprememb obveščevalnih dejavnosti za potrebe podjetij in gospodarstva se je upočasnil" (Raščan 2005, 47). To vsekakor velja tudi za Slovenijo, kjer je proučevanje kakršnekoli druge obveščevalne

dejavnosti kot te, ki jo izvajajo (državne) obveščevalne službe, praktično zanemarljiva.

V nasprotju z opisanim je vseeno potrebno omeniti nekaj avtorjev v Sloveniji, ki so se lotili strokovnega proučevanja tudi z vidika obveščevalne dejavnosti v nedržavnem sektorju. Prvo monografijo v Sloveniji, po mojem vedenju, predstavlja diplomska naloga iz leta 1998, ki jo je napisala Ines Vrenko (tudi s pomočjo in nasveti slovitega Stevana Dedijerja, kar delu daje še toliko večji pomen) in nosi naslov Ekonomska in konkurenčna obveščevalna dejavnost. V letu 2008 je Damir Črnčec[1] s svojo doktorsko disertacijo Obveščevalna dejavnost v javnem in zasebnem sektorju (gospodarska vs. konkurenčna obveščevalna dejavnost) objavil šele drugo monografsko publikacijo, ki se podrobneje loteva tudi te tematike in na podlagi te disertacije leta 2009 še knjigo Obveščevalna dejavnost v informacijski dobi. Omeniti je potrebno tudi Antona Dvorška s strokovnimi članki in pa zbornik, ki se loteva primarno t.i. črne strani obveščevalne dejavnosti, to je vohunjenja (ur. Iztok Podbregar,[2] Vohunska dejavnost in gospodarstvo, 2008). Predvsem v zadnjem času se pojavlja tudi vedno več diplomskih del, ki se »dotikajo« tega področja, pa vendar je podhranjenost proučevane teme v Sloveniji več kot očitna, medtem ko to za tujo literaturo ne velja. Naj mi opravičijo morebitni neupravičeno nenavedeni, kar pa ne zamegljuje dejstva, da je tematika obveščevalne dejavnosti, ki ni v domeni države in njenih akterjev, v slovenskem prostoru močno podhranjena. Če govorimo o konkurenčni obveščevalni dejavnosti, ki zajema samo bistvo obveščevalne dejavnosti v gospodarskih družbah in je v tuji literaturi prepoznaven termin (ang. competitive intelligence), je strokovno proučevanje v Sloveniji skoraj neobstoječe.

Ta »podhranjenost«, skupaj s perspektivnostjo in zanimivostjo tematike, me je vodila tudi k proučevanju te tematike v magistrskem delu. V delu bom predstavil konkurenčno obveščevalno dejavnost preko obveščevalne dejavnosti, ki je v domeni države in še posebej njenega pomembnega dela – gospodarske obveščevalne dejavnosti. Kot osnova in začetek proučevanja menim, da je to prava pot, saj je očitno in nedvoumno, da se je konkurenčna obveščevalna dejavnost razvijala in

[1] Doc. dr. Damir Črnčec je direktor Obveščevalno varnostne službe Ministrstva za obrambo Republike Slovenije od leta 2005 dalje.
[2] Izr. prof. dr. Iztok Podbregar je bil, med drugim, v svoji karieri tudi načelnik generalštaba Slovenske vojske, direktor Slovenske obveščevalno-varnostne agencije in svetovalec predsednika Republike Slovenije za nacionalno varnost.

»učila« pri »klasični« obveščevalni dejavnosti. Nenazadnje so bili nekateri ključni posamezniki tega relativno novega področja prav iz teh vrst, terminologija pa v veliki meri sledi terminologiji, ki se uporablja v delih povezanih z nacionalno obveščevalno dejavnostjo.

Ker je konkurenčna obveščevalna dejavnost relativno nepoznan in teoretično slabo obdelan termin, je eden ciljev dela tudi jasno določiti, kaj ta termin zajema, kako se je razvijal in ga razmejiti od drugih terminov, ki se pojavljajo v zvezi s proučevanim področjem. Ta terminološka nedoločenost seveda ni edina zgolj temu področju, je pa v slovenskem prostoru zelo izrazita.

Naslednji cilj v delu je raziskati zgodovinski razvoj konkurenčne obveščevalne dejavnosti, tako v formalnem kot idejnem smislu. Potrebno je dobiti odgovor, zakaj sploh konkurenčna obveščevalna dejavnost in ali je kot taka vredna podrobne obravnave. Dober začetek razmišljanja v tej smeri predstavlja Podbregar (2008, 13), ko pravi:

> *Posamezniki in organizacije, tako profitne kot neprofitne, se v dinamičnem okolju v katerem živimo in ga kreiramo, srečujejo z vse večjo potrebo, ki bi jo na kratko lahko opisali s stavkom: »Potrebujem pravočasne, točne in uporabne podatke za odločanje«. Relativno preprost stavek, ki pa pred nas največkrat postavlja velike ovire, zahteva izjemno organiziranost in delovanje različnih teamov, skupin ter odlično infrastrukturo večkrat vezano na najsodobnejše informacijske tehnologije.*

V tem kontekstu se velikokrat izhaja tudi iz slavnega in neštetokrat ponovljenega izreka Sira Francisa Bacona iz leta 1597, ko je v svojem delu Meditationes Sacrae zapisal "scientia potentia est". Prevod se v sodobnem času uporablja kot "znanje je moč". Rek se nanaša na to, da se z znanjem ali izobrazbo potencial ali zmožnost nekoga povečata (http://en.wikipedia.org/wiki/Knowledge_is_power, 29. 1. 2009). Kahaner (1997, 22) gre še dlje, ko meni, da bo podjetje, ki zna podatek oz. informacijo pretvoriti v obveščevalni produkt, uspelo, podjetje, ki tega ne zna, pa bo propadlo.

S terminološko opredelitvijo in zgodovinskim razvojem konkurenčne obveščevalne dejavnosti bom postavil okvir, s katerim bom lahko proučeval stanje te dejavnosti v gospodarskih družbah v Sloveniji. Prvi poskus empirične raziskave v Sloveniji je izvedla Ines Vrenko leta 1998, ko je na podlagi poslanih vprašalnikov v 85 slovenskih podjetij (31 jih je na vprašalnik odgovorilo) izvedla empirično raziskavo. Logično nadaljevanje bi bilo seveda narediti nekaj podobnega tudi sedaj, 12 let pozneje, vendar sem se, tudi po posvetu z nekaterimi vodilnimi poznavalci tega področja v Sloveniji, odločil za drugačen pristop, ki bo ožje in bolj kvalitativno naravnan. Glavni razlogi za to odločitev so: nizka stopnja vrnitve vprašalnikov, težko je (iz)vedeti, kdo na tak vprašalnik odgovarja in katere ter kakšne so njegove kompetence o tej tematiki. Ker gre za relativno občutljivo področje, močno dvomim tudi v iskrenost odgovorov. Predvsem pa dvomim v terminološko razumevanje pojma in problematike, saj sta, kot že omenjeno, razumevanje in teoretično proučevanje tega področja v Sloveniji zelo nizka, pred 12 leti pa sta bili še nižji. Sam se bom lotil proučevanja stanja v Sloveniji predvsem na tri načine. S proučevanjem strokovne literature, s pogovori s kompetentnimi ljudmi ter s primerjavo empiričnih raziskav, ki so bile narejene na povezanih/sorodnih področjih. Na ta način bom poskusil pridobiti poglobljen vpogled v stanje v Sloveniji in smernice za prihodnje.

Za zadnji cilj dela sem si zastavil ugotoviti in predstaviti možne zlorabe s strani gospodarskih družb. Ta problem sta nakazala že Šaponja (1999, 35), ko pravi "/d/andanes je pravzaprav dokaj lahko nadzirati državne obveščevalne službe. Vse težje pa bo obvladovati številne zasebne obveščevalne organizacije, v katerih so zaposleni nekdanji uslužbenci državnih obveščevalnih služb. Teh služb namreč nihče ne nadzoruje" in Črnčec (2008, 271) "/t/rdim, da je v informacijski dobi potrebno vzpostaviti učinkovitejši sistem nadzora nad posegi v človekove pravice v zasebnem sektorju". Avtorja sta nedvoumno nakazala velik potencialni problem, ki je vsekakor vreden teoretične poglobitve. Z nakazanim pridemo do temne strani konkurenčne obveščevalne dejavnosti - vohunjenja in s tem povezanih kaznivih dejanj. Zanimivo se bo poglobiti v tezo, ali se kaj takega dogaja tudi pri gospodarskih družbah, ki izvajajo konkurenčno obveščevalno dejavnost. V tem kontekstu Brody (2008, 11) opozarja, da se izvajalci in teoretiki konkurenčne obveščevalne dejavnosti soočajo z namigovanji, da je ta dejavnost preprosto korporativno vohunjenje.

1 METODOLOŠKI PRISTOP

1.1 Opredelitev predmeta in ciljev proučevanja

Obveščevalna dejavnost je bila dolgo pojmovana skoraj izključno kot dejavnost, ki jo izvajajo obveščevalne službe držav. V zadnjih nekaj desetletjih to pojmovanje, tudi zaradi geopolitičnih in geoekonomskih premikov, počasi in zanesljivo tone v pozabo, proučevanje strokovne in deloma tudi laične javnosti pa se vedno bolj usmerja na »nedržavne« izvajalce obveščevalne dejavnosti. Po svetu se je v preteklih desetletjih precej uveljavila konkurenčna obveščevalna dejavnost - KOD (ang. competitive intelligence), kot dejavnost s katero (predvsem) gospodarske družbe poskušajo dosegati konkurenčno prednost in to vsaj deklarativno na legalen in etičen način. KOD je v Sloveniji precej nepoznan in teoretično neobdelan termin ter predstavlja dejavnost, za katero menim, da je tudi ali predvsem v času krize, ki smo ji priča, lahko dejavnost, ki gospodarski družbi lahko pomaga pri njenem uspešnem delovanju.

Zastavljeni cilji pričujočega dela so predvsem: predstaviti dejavnost imenovano KOD kot primarni predmet proučevanja v Sloveniji. V ta namen je potrebno dodobra opredeliti ta termin, definirati območje delovanja ter ga ločiti ter tudi povezati s sorodnimi ali različnimi dejavnostmi. Poleg teoretičnega vidika proučevanja bom poskusil predstaviti tudi praktični vidik, torej kako (če sploh) to dejavnost izvajajo slovenske gospodarske družbe oz. gospodarske družbe prisotne v Sloveniji. Termin obveščevalna dejavnost sproža najrazličnejše, predvsem pa negativne konotacije in povezovanje z nelegalno dejavnostjo – vohunstvom, zato je ta povezava ali popolna ločenost teh dveh dejavnosti vredna temeljite obravnave. To nas pripelje tudi do nadzora nad to dejavnostjo, za katerega težko trdimo, da je sploh obstoječ, in prav zato bom proučil tudi možne zlorabe KOD in nadzor nad to dejavnostjo.

1.2 Hipoteze

- Slovenske gospodarske družbe se zavedajo pomena konkurenčne obveščevalne dejavnosti in jo uporabljajo kot orodje, ki jim omogoča konkurenčno prednost na trgu.

- Nelegalna dejanja, predvsem vohunjenje, so neločljiv del konkurenčne obveščevalne dejavnosti, brez katerih le-ta ne more biti uspešna.

- Pravna praznina, teoretična neobdelanost in odsotnost mehanizmov nadzora omogočajo oz. ne preprečujejo zlorabe sicer legalne konkurenčne obveščevalne dejavnosti v nelegalne namene.

Prvo postavljeno hipotezo bom preverjal predvsem v zadnjem poglavju z naslovom Študija primera – Slovenija, podlaga za potrditev ali zavrnitev hipoteze, pa bo predstavljala celotno delo, saj je za relevantno oceno potrebno dobro poznati to področje kot tudi stanje v drugih državah.

Drugo hipotezo, ki je izredno pomembna za samo dejavnost in izvajalce te dejavnosti, bom preverjal predvsem s poglavji 4.1 Vohunstvo in gospodarska obveščevalna dejavnost, 5.5 Vohunjenje gospodarskih družb in 6. Možne zlorabe KOD s strani gospodarskih družb in nadzor nad njihovim delovanjem.

Zadnjo postavljeno hipotezo bom preverjal z ugotovitvami skozi celotno delo, predvsem pa v poglavjih 5. Konkurenčna obveščevalna dejavnost in 6. Možne zlorabe KOD s strani gospodarskih družb in nadzor nad njihovim delovanjem.

1.3 Uporabljene metode

V magistrskem delu bom uporabljal več različnih raziskovalnih metod. Pomemben del bo temeljil na analizi in interpretaciji sekundarnih virov. To raziskovalno metodo bom uporabil z namenom pridobitve čim več relevantnih informacij na področjih obravnave s strani kompetentnih avtorjev in bo prisotna skozi celotno delo.

Nadalje bom uporabljal analizo in interpretacijo primarnih virov, da bi dobil boljši pregled nad nekaterimi področji (gre predvsem za vprašanje, kako so s pravnega vidika urejena nekatera vprašanja).

Zgodovinskorazvojna analiza bo uporabljena predvsem v poglavju zgodovinskega pregleda konkurenčne obveščevalne dejavnosti.

V poglavju o stanju konkurenčne obveščevalne dejavnosti v Sloveniji bo uporabljena raziskovalna metoda študija primera ter raziskovalna metoda intervjuja, predvsem v obliki polstrukturiranega in usmerjenega intervjuja.

Primerjalno metodo bom uporabljal pri primerjanju proučevanega področja v različnih državah in med različnimi praksami na tem področju. Ponekod, kjer bo le-to potrebno, bom ostale raziskovalne metode dopolnil še s t.i. 'opisno (deskriptivno) metodo' in s tem zaokrožil obravnavano temo v celoto ter predstavil tudi ozadja določenih pojavov.

2 TEMELJNI POJMI

2.1 Obveščevalna dejavnost

Zakaj potreba po obveščevalni dejavnosti, slikovito razloži Šaponja (1999, 9). "Človek se sprva ni ukvarjal z definicijami. V vsakdanjem življenju, že v praskupnosti, je zelo hitro spoznal prednosti dobre obveščenosti in predvidevanja. To mu je prinašalo večji uspeh pri lovu, zmage v bojih in vojnah z drugimi plemeni. Sposobnost predvidevanja in dobra obveščenost sta mu omogočali lažje in boljše prilagajanje novemu okolju, večjo uspešnost in preživetje."

Na postavljeni odgovor zakaj, dobimo tako povsem enostaven odgovor – obveščevalna dejavnost se uporablja, ker uporabniku prinaša prednosti, včasih je bil to uspeh pri lovu, danes pač nacionalna varnost ali gospodarski uspeh/konkurenčna prednost. Šaponja (1999, 9-10) gre še korak naprej in povsem logično razjasni, zakaj se je ta dejavnost materializirala tudi v institucionalnem smislu. "Da bi človek svojo

prednost pred drugimi in svojo varnost še povečal, je organiziral obveščevalno dejavnost v urejen sistem zbiranja, hranjenja in obdelave podatkov. Za to dejavnost je zadolžil ljudi, ki so se ukvarjali samo s tem – začel je organizirati obveščevalno in varnostno službo."

"Obveščevalna dejavnost kot takšna je zgodovinska spremljevalka človeka od začetka civilizacije.[3] Že od samega začetka je velikokrat razumljena predvsem kot nekaj slabega, umazanega, nevrednega dostojanstvenega človeka, a hkrati nujno potrebna. Ta percepcija je prisotna že vsaj 2500 let..." (Črnčec 2008, 28). Avtor nadalje našteva primere iz zgodovine od stare Grčije, Peloponeških vojn, Julija Cezarja in Galske vojne, Kautilye pa do zametka prvega pravega sodobnega nacionalnega obveščevalnega sistema, ki je bil vzpostavljen v Angliji šestnajstega stoletja (Črnčec 2008, 28-30). Različni strokovnjaki navajajo še ogromno drugih primerov uporabe obveščevalne dejavnosti v zgodovini, vendar moj cilj ni predstaviti zgodovine te dejavnosti, ki je tako pestra in bogata, da se je o njej napisalo, se piše in se bo pisalo ogromno knjig, člankov… Želim le poudariti, da je obveščevalna dejavnost prisotna že »od nekdaj«. Kot drugo želim poudariti, da je percepcija te dejavnosti v očeh javnosti pretežno negativna, kar je z izkušnjo totalitarnega sistema (pa tudi »stare« demokracije imajo na sebi kar nekaj tovrstnih madežev) možno z lahkoto razumeti in ponotranjiti. "Obveščevalna dejavnost v ljudeh vzbuja različna čustva. Takšna, kot so izkušnje in vedenja posameznika o njej. Večkrat je mistificirana, mnogi se je izogibajo, včasih tudi ignorirajo. Nekaterim se zdi, da je obveščevalno-varnostna dejavnost daleč stran od njih, druge pa večkrat zajame celo paranoja, da so zlorabljeni v te namene" (Podbregar 2008, 13).

Na pojmovanje nelegalnosti opominja Purg. "V teoriji, znanstveni publicistiki in praksi mednarodnih odnosov so obveščevalno dejavnost oziroma zbiranje obveščevalno zanimivih informacij dolgo časa pojmovali kot izključno ilegalno, tajno, s tem pa tudi nedovoljeno obnašanje posameznika, organizacij in države" (Purg 1995, 31).

Če gledamo na obveščevalno dejavnost iz perspektive današnjega časa in tudi prihodnosti, moramo omeniti dva pomembna obdobja novejše zgodovine – hladno

[3] Mnogokrat se jo označuje tudi kot drugo najstarejšo obrt/dejavnost.

vojno in obdobje po terorističnih napadih 11.09.2001 v ZDA, ki sta izredno in temeljno vplivala na to dejavnost.

> *Sedanje obdobje lahko označimo kot obdobje konca »hladne vojne«, s tem pa je na nek način tudi konec obdobja ekspanzije obveščevalne dejavnosti, ki je svojo vlogo opravljala v procesu odkrite dominacije velesil. V ospredju so drugi problemi, ki terjajo drugačen pristop, kar se odraža tudi pri vsebini dela obveščevalnih služb. To se je pokazalo tudi po 11. 9. 2001, ko je bilo jasno, da sta se pomembno spremenila/okrepila vloga in pomen obveščevalnih služb, saj si učinkovitega boja proti mednarodnemu terorizmu in proti drugim oblikam ogrožanja varnosti v sodobnem svetu ni mogoče predstavljati brez ustrezne podpore teh služb, poleg tega pa je jasno, da so obveščevalne službe pomembna in obvezna sestavina sodobne in prihodnje varnostne arhitekture (Purg 2002, 7-8).*

Zakaj so zgoraj omenjeni teroristični napadi pomembni (med mnogimi drugimi posledicami, ki so jih sprožili) tudi za proučevano področje, je razvidno iz sledečega zapisa. "Po 11. septembru 2001 se je tudi trend v obveščevalni dejavnosti, ki je potekal od konca hladne vojne, k ekonomsko konkurenčni dejavnosti spremenil in se je spet povečala klasična – državna obveščevalna dejavnost. … Trend sprememb obveščevalnih dejavnosti za potrebe podjetij in gospodarstva se je upočasnil" (Raščan 2005, 47).[4]

Poskušal bom še definirati sam termin. Pogosto se navaja definicija Richelsona (1989 v Purg 2002, 14). "Obveščevalna dejavnost je najširši pojem in bi ga lahko opredelili kot rezultat zbiranja, analiz, združevanja in interpretacije vseh razpoložljivih podatkov, ki zadevajo enega ali več vidikov tuje države oziroma operativnega področja, ki je neposredno ali potencialno pomembno za načrtovanje". Purg (2002, 14-15) to definicijo nadalje razčleni:

[4] Izredno zanimiva je v tem kontekstu izjava nacionalnega obveščevalnega direktorja ZDA Dennisa C. Blaira, ko je na pričanju v Kongresu dne 12.02.2009 povedal, da je "globalna gospodarska kriza in nestabilnost, ki jo lahko povzroči prehitela terorizem, kot največjo grožnjo, ki grozi ZDA" (http://www.nytimes.com/2009/02/13/washington/13intel.html?_r=1). Skoraj neverjeten premik, ki si ga pod administracijo prejšnjega predsednika (George W. Bush) težko predstavljam in verjetno posledično pomeni vsaj delno preusmeritev obveščevalnih zmogljivosti na gospodarsko področje.

Zbiranje pomeni namensko zbiranje podatkov, ki jih lahko koristijo analitik, operativni delavec ali naročnik. Zbiranje lahko poteka v več oblikah, ki se med seboj prekrivajo (javno in tajno pridobivanje podatkov), opravljajo pa ga ljudje ali tehnična sredstva. Tajno zbiranje zajema pridobivanje podatkov, ki v javnosti niso na voljo. Podobno kot pri javnem zbiranju lahko tudi pri tem načinu uporabljamo človeške in tehnične vire. Analiza zajema integracijo zbranih podatkov ali neobdelanih informacij iz vseh virov za izdelavo končne - obveščevalne informacije.

V tej in večini drugih definicij opazimo, da je to dejavnost, ki sledi obveščevalnemu krogu, ki bo podrobneje predstavljen v nadaljevanju. Ta definicija sledi obveščevalni dejavnosti kot dejavnosti države in zanjo velja ugotovitev Jéquierja in Dedijerja (1987, 22-23), da je obveščevalna dejavnost ponavadi razumljena kot dejavnost, ki jo izvajajo nacionalne obveščevalne službe, ki so primarno zaskrbljene z vojaškimi ali strateškimi nalogami. Nacionalne obveščevalne službe, ki se ukvarjajo z notranjo ali zunanjo varnostjo, z zbiranjem informacij ali s protiobveščevalno dejavnostjo, predstavljajo zgolj vrh ledene gore obveščevalne dejavnosti v katerikoli družbi. Ta vrh je daleč najbolj proučevan in privlači javnost. Toda ta visoka vidnost nacionalnih obveščevalnih služb je odvrnila pozornost strokovne javnosti, novinarjev in zgodovinarjev od mnogo pomembnejšega in širšega področja obveščevalne dejavnosti, ki jo izvajajo korporacije, družbene skupine, zasebne institucije in vladne agencije.

Podobno ugotavlja tudi Agrell (1987, 37), ki poda za to dejstvo tudi prepričljivo razlago. V preteklosti je bila obveščevalna dejavnost sinonim za vladno obveščevalno dejavnost, kar je omogočilo vzpon mogočnih agencij, ki so delala v globoki tajnosti. To ni bilo presenetljivo, saj je bila obveščevalna dejavnost primarno v domeni države. Nadalje avtor ugotavlja, da se to spreminja vsaj v pomembnejših industrializiranih državah, kjer nacionalne korporacije in multinacionalke delujejo na enaki stopnji kot državne institucije.

V tem kontekstu je uporabnejša definicija (pa čeprav še starejša od prejšnjih zapisov),[5] ki jo najdemo v Intelligence-Policy & Process (1985 v Šaponja 1999, 9). "Obveščevalna dejavnost je 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." V tej definiciji lahko ponovno razberemo dejavnost obveščevalnega kroga in njegov končni produkt ter uporabnika, kateremu je le-ta namenjen za odločanje na štirih področjih. Od tega so tri področja (skoraj) ekskluzivna področja zanimanja nacionalnih obveščevalnih organizacij, gospodarsko področje pa je predmet zanimanja širšega kroga uporabnikov.

Kar je mogoče nekoliko skrito oz. pomanjkljivo v zgornji definiciji pa povsem nedvoumno razjasni Šaponja (1999, 10).

> *Obveščevalna dejavnost je eden najpomembnejših elementov v procesu odločanja. … Organizirana je lahko v državnih ali javnih oziroma v zasebnih institucijah. … Mnogokrat slišimo mnenje, da lahko o obveščevalni dejavnosti govorimo le tedaj, kadar jo izvaja obveščevalnovarnostna služba oziroma državna institucija, in to le tedaj, kadar uporabljajo pri dejavnosti tajne načine zbiranja podatkov. Gre za zastarele poglede na to in v svetu takšna razmišljanja že tonejo v pozabo.*

Nadalje to tezo razvija Purg in kar je še pomembnejše, svojo tezo empirično podkrepi. "Iz primerjalnega pregleda teorije in prakse s tega področja je razvidno, da je imela nekdaj obveščevalna dejavnost na vojaškem področju pomembnejšo (primarno) vlogo, v sodobnosti pa marsikje prehaja težišče na politično, predvsem pa na gospodarsko področje" (2002, 31).

Ker je iz zgornjih zapisov več kot evidentno, da obveščevalna dejavnost ni izključno v domeni držav oz. njenih obveščevalnih organizacij, se mi zdi ustrezno poiskati definicijo, ki bo to dejavnost zajela ustrezno in odgovarjajoče današnjemu času. V tem kontekstu se mi zdi ustrezna razdelitev in definicija Šaponje (1999, 10-12), ko pravi, da lahko o obveščevalni dejavnosti govorimo kot o:

[5] Namenoma uporabljam nekatere starejše zapise in definicije.

… dejavnosti v širšem in ožjem smislu. V širšem smislu jo lahko opredelimo kot organizirano pridobivanje novega znanja in informacij o dogodkih, pojavih in procesih v bivalnem ali poslovnem okolju, v naravi, družbi, skratka o vsem, kar se dogaja okrog nas. … O obveščevalni dejavnosti govorimo v širšem smislu torej takrat, kadar obveščevalne organizacije za potrebe odločanja na organiziran in institucionaliziran način zbirajo, analizirajo in posredujejo končne izdelke. Delujejo samo pod pogoji in na načine, ki so dovoljeni vsem državljanom. Govorimo o običajnih načinih zbiranja podatkov, ki vključujejo podatke, ki so javno dostopni. … Kadar pa obravnavamo obveščevalno dejavnost, ki jo izvajajo državne institucije, ki imajo zakonska pooblastila, da zbirajo tudi tajne podatke na posebne načine, govorimo o obveščevalni dejavnosti v ožjem smislu.

Definiciji obveščevalne dejavnosti v širšem in ožjem smislu sta ustrezni tudi z vidika proučevanja obveščevalne dejavnosti gospodarskih družb, saj je meja med legalno obveščevalno dejavnostjo gospodarskih družb, t.j. konkurenčno obveščevalno dejavnostjo in njeno temno platjo – vohunstvom, nedvoumna in jasna.

Ker se v angleškem jeziku za obveščevalno dejavnost uporablja izraz »intelligence«, je potrebno opozoriti, da prevod obveščevalna dejavnost ni edina možna uporaba tega termina na tem področju.

Sam pojem obveščevalna dejavnost (ang. Intelligence) je moč razumeti na tri načine:

1. *nanaša se na zgornjo plast informacijske piramide, zmožnost sprejemanja ocen in prilagajanja na okoliščine na koherenten način;*
2. *lahko se nanaša na aktivnosti, povezane s pridobivanjem podatkov nacionalnih obveščevalnih struktur in*
3. *širše (britanska uporaba) – industrijsko podjetje ali katerakoli druga družbena organizacija (Črnčec 2008, 28).*

Tudi Lowenthal (2000, 8) podaja tri možnosti, kako razumeti termin »intelligence«, toda nekoliko drugače:

- Kot proces: sredstvo s katerim se določeni tipi informacij potrebujejo in zahtevajo, zberejo, analizirajo in posredujejo ter način, na katerega se določeni tipi prikritih akcij načrtujejo in izvedejo.
- Kot produkt: gre za produkt zgornjih dveh procesov, torej kot produkt analize in kot sama obveščevalna operacija.
- Kot organizacija: gre za organizacijske enote, ki izvajajo njihove številne funkcije.

Ker angleški termin kot sam ni moč vedno enako prevajati in je večpomenski, je potrebno prepoznati kontekst, v katerem se pojavlja in ga pravilno umestiti v okvir, kar sem in bom v nadaljnjem besedilu poskušal tudi sam.

Tretja možnost prevoda ang. termina »intelligence« nas usmeri na organizacijo, ki izvaja obveščevalno dejavnost. Najpogostejša sta izraza obveščevalna služba (v Sloveniji je primer takega poimenovanja Obveščevalno varnostna služba Ministrstva za obrambo Republike Slovenije – OVS MORS) in obveščevalna agencija oz. samo agencija (v Sloveniji se tako imenuje Slovenska obveščevalno-varnostna agencija – SOVA, še mnogo bolj znana in razvpita je Osrednja obveščevalna agencija – CIA v ZDA).

Delitev oz. razlikovanje obveščevalnih služb navaja naslednji avtor:

Obveščevalne službe se razlikujejo predvsem glede na:

- *področje dela in položaj v sistemu (civilne in vojaške obveščevalne službe; službe znotraj posameznih ministrstev ali kot posebne vladne službe);*
- *stopnjo ofenzivnosti, ki je v razponu od pridobivanja podatkov pa vse do izvajanja raznih akcij (tako doma kot v tujini);*
- *velikost - od manjših enot do velikih obveščevalnih sistemov (ki zaposlujejo tisoče delavcev);*
- *usmerjenost - po posameznih področjih dela in po geografskih območjih ter*
- *notranjo organiziranost (kakšen princip organiziranja imajo - štabni, linijski, projektni ipd.) (Purg 2002, 17).*

S tem seveda niso izčrpane vse možnosti, ne glede poimenovanja, ne glede razlikovanja. "Poleg splošne organizacijske oznake »služba« se uporabljajo tudi oznake »agencija, urad, komite, direkcija«" (Purg 2002, 17). V do sedaj navedenih terminih je osredotočenost na državni vidik organizacije, zato je zanimivo, kaj o tem pravi Šaponja. "Obveščevalna dejavnost je organizirana v posebnih organizacijskih oblikah, obveščevalnih organizacijah. … Zaradi narave njihovega delovanja, jih imenujemo tudi tajne službe. Organizirane so lahko tudi kot samostojne nevladne organizacije, najpogosteje znotraj večjih gospodarskih sistemov ali zasebnih agencij" (1999, 24). Veseli dejstvo, da so posebej izpostavljeni tudi nekateri nedržavni akterji, izključno te pa ima v mislih Dvoršak in jih v organizacijskem smislu opredeli kot "poizvedovalne oddelke" (2003,1). Kot termin, ki ne prejudicira organizacijske oblike obveščevalne dejavnosti v javnem ali zasebnem sektorju se kot najustreznejši izkaže obveščevalna organizacija.

Lowenthal (2000, 2-5) našteva štiri glavne razloge zaradi katerih obstajajo obveščevalne službe:[6]

- da se izogne strateškim presenečenjem;
- da se priskrbi dolgoročno strokovno znanje;
- da se podpre proces oblikovanja politik;
- da se obvaruje tajnost informacij, potreb in metod.

Glavni poudarek, ki sem ga želel podati v poglavju o obveščevalni dejavnosti je predvsem ta, da je obveščevalna dejavnost nekaj, kar ni povezano zgolj z državnimi obveščevalnimi službami, temveč jo je potrebno razumeti v širšem kontekstu in, da to dejavnost izvajajo tudi nedržavne obveščevalne organizacije.

2.2 Obveščevalni krog[7]

Kot smo ugotovili v prejšnjem poglavju je obveščevalni krog v samem jedru obveščevalne dejavnosti in preprosto tako pomemben za razumevanje področja obveščevalne dejavnosti, da ga je potrebno podrobneje opisati.

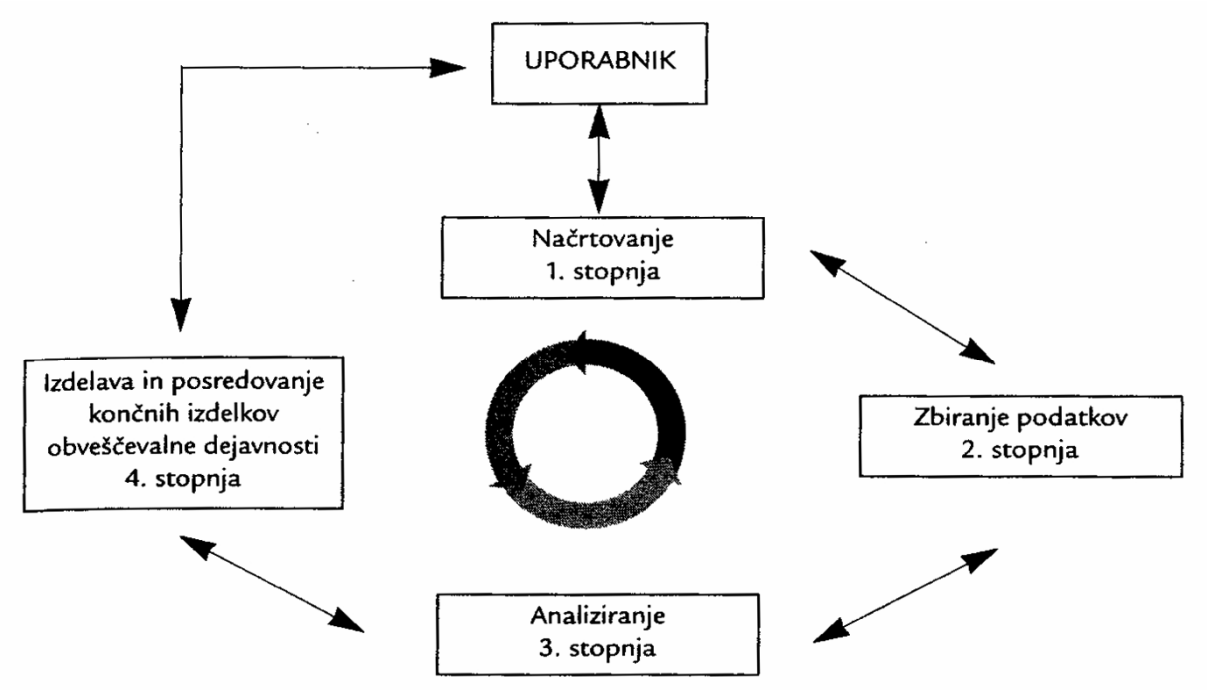
[6] Čeprav ima avtor v mislih državne obveščevalne službe, so ti razlogi širše veljavni.
[7] Uporablja se tudi termin obveščevalni cikel ali proces obveščevalne dejavnosti.

Obveščevalni krog poteka v več zaporednih stopnjah ciklične narave. Število posameznih stopenj kroga ni splošno sprejeto in različni avtorji navajajo različno število stopenj in tudi same stopnje so različno poimenovane. Šaponja (1999, 12) ugotavlja, da:

> *Razlike nastajajo, ker nekateri avtorji posamezne stopnje, najpogosteje stopnjo analitične obdelave podatkov, razdeljujejo bolj podrobno. Na splošno pa lahko rečemo, da ima ciklus štiri stopnje in sicer:*
>
> - *načrtovanje – 1. stopnja;*
> - *zbiranje podatkov – 2. stopnja;*
> - *analitična obdelava podatkov in izdelava obveščevalnih izdelkov – 3. stopnja;*
> - *posredovanje končnih izdelkov obveščevalne dejavnosti uporabnikom – 4. stopnja.*

Grafično je obveščevalni krog, kot ga pojmuje Šaponja, predstavljen na sliki 2.1.

Slika 2.1: Obveščevalni krog



Vir: Šaponja (1999, 67)

Proces se začne z načrtovanjem, s katerim se določi kako, s kakšnimi sredstvi in katere podatke je treba zbrati. Naslednja stopnja je zbiranje podatkov. Zbrane podatke se posreduje analitičnim službam, ki podatke ovrednotijo in analizirajo, kar se odvija v tretji stopnji. Zbiralcem podatkov naložijo dodatno zbiranje podatkov, bodisi zato, ker jih imajo še vedno premalo, da bi lahko izdelali končni izdelek, bodisi zato, ker z analizo ugotovijo, da jih je potrebno dodatno preveriti. Razlogov za dodatno zbiranje podatkov je poleg teh dveh osnovnih lahko še več. Četrta stopnja ciklusa je izdelava končnega izdelka kot rezultata celotnega obveščevalnega procesa, in sicer na podlagi analiz zbranih podatkov. Oblike končnih izdelkov so zelo različne in se prilagajajo namenu uporabe in uporabniku. Medsebojno se razlikujejo glede na to, ali gre za obveščevalne ali varnostne službe. Ciklus se lahko ponovno začne tudi takrat, kadar uporabnik z dobljenim odgovorom ni zadovoljen in želi še bolj poglobljeno analizo (Šaponja 1999, 67).

Pet stopenjski obveščevalni krog s kratko razlago posameznih stopenj podaja Richelson (1989 v Purg 2002, 14):

Pojem obveščevalni ciklus zajema zbiranje in obdelavo podatkov ter njihovo posredovanje ustreznim organom. Krog je sestavljen iz petih delov.

1. *Načrtovanje in usmerjanje zajema menedžment celotnega postopka pridobivanja obveščevalnih podatkov - od identifikacije potrebe po podatkih do izročitve obveščevalnega izdelka naročniku. V okviru strateškega načrta se opredelijo cilji in objekti obveščevalnega delovanja, z operativnim načrtom pa določijo podrobnosti (kaj, zakaj, kako, ...).*
2. *Zbiranje zajema pridobivanje surovih izdelkov, iz katerih se nato izdela končni obveščevalni podatek. Ta postopek v grobem zajema zelo različne oblike zbiranja podatkov, med njimi so: javni viri, elektronski mediji, fotografiranje, človeški viri, posebne metode in oblike zbiranja podatkov - tajno sodelovanje, odkup podatkov in predmetov, zbiranje s tehničnimi sredstvi – npr. s pomočjo satelitov in letal, nadzor telekomunikacijskih sredstev, nadzor pisemskih pošiljk, prisluškovanje v prostoru, tajno sledenje in opazovanje, tajno tonsko in foto dokumentiranje.*

3. *Obdelava se nanaša na spremembo ogromne količine podatkov v obliko, ki je primernejša za izdelavo obveščevalne informacije ter zajema prevajanje, dekodiranje ter sortiranje podatkov tako po vsebini kot količini.*
4. *Analiziranje pomeni spremembo osnovne informacije v končni obveščevalni podatek, pri čemer integrira vse razpoložljive podatke, poleg tega pa se jih lahko tudi interpretira in oceni.*
5. *Posredovanje pomeni distribucijo in izročitev končnega obveščevalnega podatka uporabnikom oziroma tistim, ki so sprožili postopek zbiranja informacij.*

Izredno pomembno pri obveščevalni dejavnosti na splošno in pri obveščevalnem krogu konkretno je opredeliti subjekte, ki igrajo pomembno vlogo – usmerjevalec, uporabnik in naročnik.

> *Za pravilno razumevanje obveščevalnega ciklusa in delovanja obveščevalnovarnostnih in varnostnih služb je potrebno natančno opredeliti pojem usmerjevalca, uporabnika in naročnika. Usmerjevalci dajejo obveščevalnovarnostnim in varnostnim službam osnovne smernice za delo, ki temeljijo na zakonih, državnih strategijah na nacionalnovarnostnem, zunanjepolitičnem in ekonomskem področju. Ta vloga večinoma pripada zakonodajni ali pa izvršilni veji oblasti. Odvisna je od ustavnopravne ureditve političnega sistema oziroma od razmerij med upravno-izvršilno in zakonodajno vejo oblasti, ki tudi sicer vlada v državi. Uporabniki obveščevalnih izdelkov so navadno določeni z zakonom ali s podzakonskimi akti. To so organi ali osebe, ki so zaradi narave svojega dela pooblaščeni oziroma upravičeni do obveščevalnih izdelkov, ker jih potrebujejo za nemoteno opravljanje svojega dela. Nemalokrat uporabniki nimajo pooblastil za naročanje izvajanja obveščevalnih aktivnosti oziroma zbiranja podatkov. Taka pooblastila imajo naročniki, ki lahko obveščevalnovarnostnim in varnostnim službam naročajo izvajanje določenih aktivnosti - zbiranje podatkov oziroma izdelavo končnih obveščevalnih izdelkov, ki so prav tako določeni z zakoni (Šaponja 1999, 68-69).*

Podbregar (2008, 31-32) opredeli še, v katerih fazah se pojavljajo ti subjekti.

V fazi načrtovanja igra najpomembnejšo vlogo politika, ki mora opredeliti svoje cilje, ki jih želi doseči tudi s pomočjo obveščevalne dejavnosti. Seveda mora obveščevalna služba v tej fazi jasno povedati kakšne resurse ima na voljo, kar pomeni, da na nek način pomaga pri definiranju ciljev. Fazi zbiranja podatkov in analitične obdelave sta v izključni domeni obveščevalne službe, v fazi posredovanja pa ponovno nastopi politika kot končni uporabnik obveščevalnega izdelka. Tak izdelek je pogosto osnova za nadaljnje načrtovanje in krog se ponovno začne, zato tudi ime obveščevalni ciklus.

Bistvo obveščevalne dejavnosti na splošno in še posebej obveščevalnega kroga je končni izdelek, ki je posredovan končnemu uporabniku, pa naj bo to politika ali pa direktor gospodarske družbe. To je tisto ključno, zakaj sploh izvajati obveščevalno dejavnost. "Izdelki obveščevalne dejavnosti so rezultat celotnega obveščevalnega delovanja in ne samo zbiranja podatkov (operativne informacije). Te izdelke imenujemo analitične in končne izdelke obveščevalne dejavnosti. Izdelujejo jih v obveščevalnovarnostnih in tudi v varnostnih službah. Glede na to imajo različna imena" (Šaponja 1999, 55).

Naj navedem še duhovito prispodobo obveščevalnega kroga, kot ga navaja Šaponja. "V prispodobi rečeno - obveščevalni ciklus je ožemalnik, ki na koncu izžame sok - kvaliteten končni izdelek kot rezultat celotne obveščevalne dejavnosti. Kolikor več obratov ima ožemalnik, toliko več soka izteče" (Šaponja 1999, 67).

Ker ima obveščevalni krog tako veliko pomembnost oz. pomeni samo bistvo obveščevalne dejavnosti, so v naslednjih podpoglavjih podrobneje predstavljene posamezne faze (štiri stopenjskega) obveščevalnega kroga – načrtovanje, zbiranje podatkov, analiziranje, izdelava/posredovanje.

2.2.1 Načrtovanje

Šaponja (1999, 74-78) razdeli prvo stopnjo obveščevalnega ciklusa – načrtovanje na: strateški, operativni in taktični načrt.

V strateškem načrtu služba (obveščevalna op. M.A.) opredeli način in postopke, kako bo naloge, ki izhajajo iz delovnih usmeritev usmerjevalca, izvedla in kaj za njihovo izvedbo potrebuje. Strateški načrti so običajno razdeljeni na dva dela, in sicer na splošni del, ki je vsebinski, in na del, ki zajema organizacijske, kadrovske, materialne in finančne zadeve. … Strateški načrti se nanašajo na službo kot celoto in so podlaga za oblikovanje operativnih načrtov v posameznih stopnjah obveščevalnega ciklusa. Strateške načrte dela potrdijo usmerjevalci dela obveščevalnovarnostnih in varnostnih služb tudi njihovi uporabniki. … V nasprotju s strateškimi načrti se (operativni op. M.A.) nanašajo na izvajanje konkretnih nalog. … /I/zhajajo iz analize stanja in možnosti, ki so na razpolago. … V nasprotju s strateškimi načrti, ki jih potrdijo in verificirajo uporabniki ali celo najvišji organi oblasti, operativne načrte potrdijo in dovoljujejo, pa tudi nadzorujejo njihovo izvajanje najožji vrhovi obveščevalnovarnostnih služb. … Taktični načrt pomeni načrtovanje konkretnih postopkov oziroma operativnih opravil za izvajanje konkretne naloge, ob upoštevanju taktičnih načel in pravil (Šaponja 1999,74-77).

2.2.2 Zbiranje podatkov

Dejstvo je, da je zbiranje podatkov najbolj izpostavljen[8] vidik celotne obveščevalne dejavnosti, k čemur je svoj velik del prispevala tudi filmska industrija ter vohunske knjige, pa tudi čisto realna odkritja dela obveščevalnih organizacij. Pogosto laična javnost celo enači obveščevalno dejavnost prav s to stopnjo obveščevalnega kroga. Zbiranje podatkov je seveda izredno pomembno in če se navežem na zgornjo prispodobo - iz slabih pomaranč (tudi ob najboljšem sokovniku), pač ni dobrega soka.

Šaponja (1999, 84-146) naredi klasifikacijo, treh skupin disciplin zbiranja podatkov,[9] znotraj katerih našteje še njihove pojavne oblike:

8 Kljub temu, da je najbolj tajen oz. ravno zaradi tega.

9 Pogosto se pri disciplinah zbiranja podatkov navaja ameriško klasifikacijo s celo vrsto terminov kot so: HUMINT (Human Intelligence), SIGINT (Signals Intelligence), COMINT (Communication Intelligence), ELINT (Electronic Intelligence), IMINT (Imagery Intelligence), MASINT (Measurement Intelligence), OSINT (Open Source Intelligence), TECHINT - Technical Intelligence, TELINT - Telemetry Intelligence, SIGSEC - Signals Security, PHOTOINT - Photographic Intelligence, ACOUSTINT ali ACINT - Acoustical Intelligence, MC&G - Mapping, Charting&Geodesy Intelligence, LASINT - Laser Intelligence, NUCINT - Nuclear Intelligence, RINT - Radiation Intelligence (povzeto po Šaponja (1999, 80-82) in Purg (2002, 28)).

1. Operativne discipline - skupino operativnih disciplin zbiranja operativnih in vsebinskih podatkov sestavljajo discipline, ki jih izvajajo ljudje neposredno ali posredno in je zanje potrebno operativno delovanje):
    - tajno sodelovanje;
    - tajni odkup predmeta ali podatkov;
    - tajno sledenje in opazovanje;
    - tajno fotografiranje in video snemanje;
    - tajno prisluškovanje telekomunikacij;
    - tajno prisluškovanje in snemanje pogovorov;
    - kontrola računalniških sistemov bank;
    - kontrola pisem in drugih pošiljk;
    - delovanje pod krinko;
    - sodelovanje s tujimi partnerskimi službami.
2. Tehnične discipline - tehnične discipline za zbiranje podatkov uporabljajo različna tehnična sredstva in moderno tehnologijo, ki podpira ali omogoča uporabo teh sredstev:
    - prisluškovanje;
        - prisluškovanje komunikacijam,
        - uporaba radarskih naprav,
        - odkrivanje in zasledovanje radijskih oddajnikov in radarjev.
    - discipline zbiranja slikovnih podatkov;
    - merjenje količin.
3. Discipline zbiranja javno dostopnih podatkov - posebne discipline zbiranja podatkov se ukvarjajo z zbiranjem podatkov, ki so javno dostopni in zanje ni potrebno uporabljati tehničnih ali operativnih disciplin:
    - sredstva javnega obveščanja;
    - računalniški mediji in baze podatkov;
    - drugi načini zbiranja javno dostopnih podatkov.

Zgoraj opisana klasifikacija je zelo ustrezna tudi z vidika proučevanja KOD, saj bo zelo lepo vidno, s katerimi disciplinami zbiranja podatkov je podatke legalno zbirati in kje se ta meja že prestopa.

Veliko, če ne celo večina avtorjev, tudi v današnjem času razvoja tehnologije osrednje in najpomembnejše mesto posveča človeku. "Kjerkoli pridobivaš podatke, vedno si najuspešnejši, če jih pridobivaš po različnih kanalih od katerih je kljub internetu in sodobni informacijski družbi človek (HUMINT) še vedno ključnega pomena, enako kot pred 2.500 leti v času kitajskega generala" (Dvoršak 2003, 2). Iztok Podbregar mi je v pogovoru izpostavil zelo pomembno dejstvo, ki se ga včasih s primerjanjem tehnologije naproti človeku pri zbiranju podatkov spregleda. Pomen HUMINT-a je bil, je in ostaja izredno pomemben in ni je tehnologije, ki bi lahko kaj takega spremenila, pa vendar velja enako tudi v obratni smeri. Ni dobrega HUMINT-a brez poznavanja in uporabe sodobnih informacijsko komunikacijskih tehnologij.

Vsaka od navedenih disciplin zbiranja podatkov je vsekakor pomembna, obravnavati vse podrobneje pa bi presegalo namen in smisel pričujočega dela. Vendar bom nekoliko bolj izpostavil discipline zbiranja javno dostopnih podatkov, saj so za proučevano temo izrednega pomena, kajti le za to disciplino lahko zatrdimo, da je nedvoumno legalna, torej bi morala biti osrednja disciplina zbiranja podatkov, ki se je lahko poslužujejo gospodarske družbe.[10]

Podbregar (2008, 69) sistematično zbiranje podatkov iz javnih virov deli na:

- javni viri informacij (open source information — OSINF);
- obveščevalne informacije na podlagi javnih virov (open source intelligence - OSINT).

"Pri javnih virih informacij (OSINF) gre za proces zbiranja informacij za nadaljnje obdelovanje in analiziranje. Pri obveščevalnih informacijah na podlagi javnih virov (OSINT), pa gre za proces zbiranja, selekcioniranja in analiziranja ter predstavljanja oziroma posredovanja informacij iz javnih virov, ki poteka v realnem času" (Podbregar 2008, 70). Kljub možni nadaljnji delitvi bom vse nadalje navedeno razumel in uporabljal s terminom »pridobivanje podatkov iz javnih virov«.

[10] S tem seveda ne želim trditi, da je npr. HUMINT obvezno nelegalna disciplina zbiranja podatkov, vendar je »hoja po meji« ob takšnem delovanju zelo hitro zelo tanka.

Zakaj je pridobivanje podatkov iz javnih virov tako pomembno in še pridobiva na pomembnosti, je moč razbrati tudi iz sledečega. "Najbolj zanimivo je, da vedno več podatkov, ki so nekoč bili skrbno varovane skrivnosti industrije in države, te same objavljajo v javnih medijih in na druge načine in tako postajajo domnevno varovane skrivnosti dostopne vsakomur, ki je zainteresiran in ki zna iz mozaičnih podatkov sestavljati celoto (Open Source Intelligence – OSINT)" (Dvoršak 2003, 2-3).

Podbregar (2008, 69) ugotavlja sledeče. "Končni obveščevalni produkti, ki jih pripravijo analitiki obveščevalnih služb temeljijo na pretežnem delu podatkov iz javnih virov, odvisno od primera do primera, a že stare ocene so, da je delež javno dostopnih podatkov med 80 in 90, po nekaterih ocenah pa celo 95 odstotki. A ta manjkajoči delež je običajno ključen za dobre obveščevalne informacije".

Med vrste javnih virov Podbregar (2008, 70) uvršča:

- baze javnih virov agencije,
- dnevni in periodični domači in tuji tisk,
- knjige (strokovne, splošne) iz knjižničnega gradiva agencije in druge,
- zemljevidi,
- video kasete,
- elektronski mediji (CD, DVD, MP3....),
- svetovni splet,
- radio in televizija (infoklip ali spremljanje programa)
- drugo.

Pregled nikakor ni popoln, zgolj za vtis, kako velika je lahko količina tako pridobljenih podatkov. Iz tega seveda izhaja tudi glavni problem. "Ključni problemi javnih virov se zgoščajo okrog vprašanj, kako obvladati preobilje informacij, ki so na voljo, kako v tem preobilju čim hitreje, če že ne v realnem času, selekcionirati ključne relevantne in zgoščene informacije, ki so potrebne za to, da bodo analitikom omogočila pravočasno pripravo kvalitetnih obveščevalnih izdelkov" (Podbregar 2008, 71).

Če se strinjamo z Lowentalom (2000, 5), da je zasledovanje tajnih informacij glavna opora državne obveščevalne dejavnosti, je ustrezno reči, da je zasledovanje javnih

informacij glavna opora gospodarskih družb, ki izvajajo obveščevalno dejavnost.

V luči KOD se moramo sprijazniti,[11] da je pridobivanje podatkov iz javnih virov pretežni in glavni vir pridobivanja podatkov, zanimivejši pa je zato pogled na protiobveščevalnem področju.[12] "Mogoče se je strinjati s tezo, da obveščevalna služba lahko dobi precej podatkov na podlagi analize javnih virov, trditi, da je mogoče s to metodo doseči uspehe tudi pri protiobveščevalnem delu, pa je absurdno. Agenta tuje obveščevalne službe je možno odkriti le z uporabo posebnih metod in sredstev…" (Podbregar 2008, 34).

2.2.3 Analiziranje

Shulsky dobro pojasni, zakaj pridobivanje podatkov nikakor ni dovolj in zakaj korak analiziranja. "Ni pomembno kako so informacije pridobljene, nikoli ne govorijo same zase. Z drugimi besedami, analiza informacij je potrebna, da bi bile takšne informacije koristne. … V veliki večini primerov so zbrane informacije nepopolne, dvoumne in dovzetne za zelo različne interpretacije" (Shulsky 1993, 8).

Fleisher in Bensoussan (2003, 12) opisujeta analizo kot:

> */V/ečplastno, multidisciplinarno kombinacijo znanstvenih in neznanstvenih procesov s katerimi posamezniki interpretirajo podatke ali informacije z namenom zagotovitve pomembnih spoznanj. Uporablja se za izpeljavo korelacij, ocenjevanje trendov in vzorcev, identificiranja vrzeli v zmogljivostih, in predvsem ugotavljanje in ocenjevanje priložnosti, ki so na voljo organizaciji. Analiza odgovori na kritično »pa kaj?« (ang. so what?) vprašanje pri zbranih podatkih in omogoči vpogled, utemeljen na potrebah odločevalcev.*

Šaponja (199, 152) razdeli analitični proces na dve osnovni stopnji:

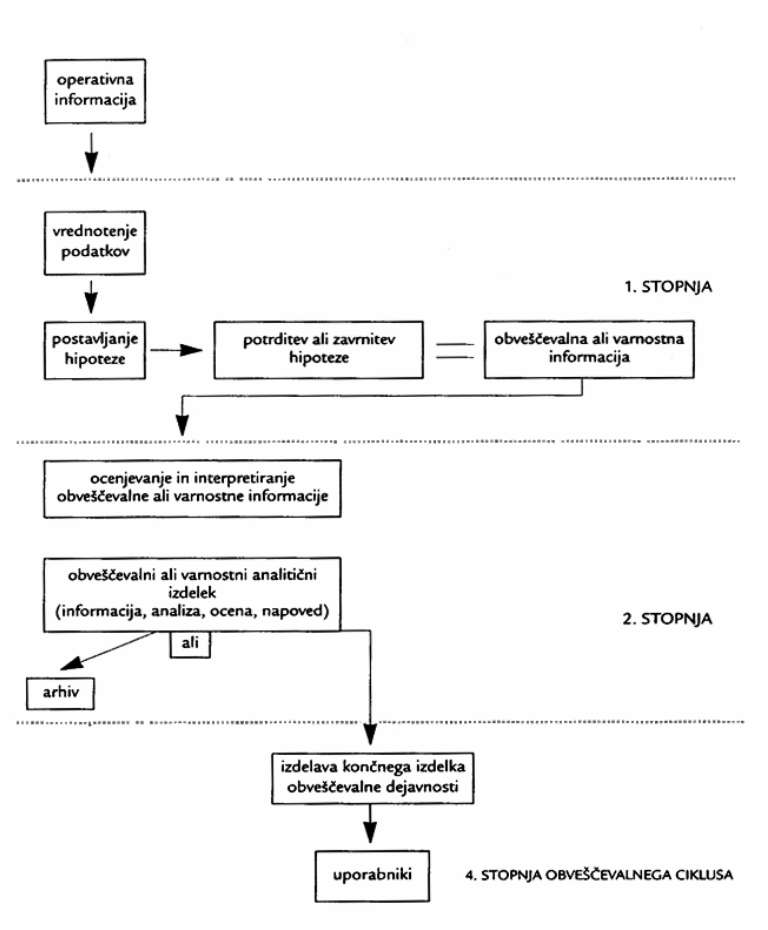
1. vrednotenje zbranih podatkov oziroma operativnih informacij in izdelava informacij kot osnovnih analitičnih izdelkov;

[11] V kolikor ne želimo prestopati meje legalnega.
[12] Odvisno od prakse različnih gospodarskih družb lahko termin KOD opredeljuje tudi protiobveščevalno dejavnost.

2. interpretiranje oziroma ocenjevanje informacij in izdelovanje drugih analitičnih izdelkov (Šaponja 1999, 152):

Ta proces je grafično prikazan na sliki 2.2.

Slika 2.2: Analitična stopnja obveščevalnega kroga



Vir: Šaponja (1999, 152)

2.2.4 Izdelava in posredovanje

Kot zadnji korak (oz. stopnja), pa vendar zaradi ciklične narave lahko tudi »spet« prvi, obveščevalnega kroga navajam izdelavo in posredovanje. Ta korak Šaponja opisuje kot sledi. "V tej stopnji obveščevalnega delovnega procesa dobijo analitični izdelki obliko, ki je za uporabnika najbolj primerna, obliko, ki jo določa zakon.[13] Glede na

[13] To velja za državne obveščevalne službe, vendar sam obravnavam tematiko obveščevalne dejavnosti širše. Pri gospodarskih družbah bi lahko namesto zakona enako vlogo imel npr. pravilnik, navodilo… ali pa to sploh ni formalno opredeljeno.

zahteve in vrsto naročnikov ter vrsto službe izbere vodstvo najprimernejši analitični izdelek ali več takih izdelkov skupaj. Poseben oddelek službe ali njegov del zadolži, da izdelek ustrezno oblikuje" (Šaponja 1999, 169).

Izdelan in posredovan končni izdelek mora biti takšen, da je na podlagi le-tega mogoče ukrepati oz. pomeni neko dodano vrednost za odločevalca. Če le-ta z njim ni v celoti ali deloma zadovoljen, se začne nov obveščevalni krog. Problem se pojavi, ko odločevalec ni dovolj usposobljen ali dojemljiv, da bi ta končni izdelek lahko uporabil, ali pa seveda, če končni izdelek ni dovolj kvaliteten, ali ne omogoča ukrepanja/delovanja. V tem primeru je bilo ogromno dela (kadar je obveščevalni krog kvalitetno in strokovno izpeljan) vrženega »stran«. Strokovnjaki KOD zato ogromno energije vlagajo v pojasnjevanje in utemeljevanje pomembnosti svoje dejavnosti, razvijanje odnosov in redne stike z odločevalci, da se kaj takega ne bi zgodilo. Smisel kakršnekoli obveščevalne dejavnosti je povsem porušen v kolikor pride do nezaupanja na ravni odločevalec – izvajalci obveščevalne dejavnosti. Šaponja v tem kontekstu izpostavlja dejstvo, ki se ga je potrebno zavedati. "Znano je, da oblikovalci politike ne želijo slišati ničesar o njeni neuspešnosti. Obveščevalne in varnostne službe jih morajo pogosto informirati prav o dejstvih, ki so rezultat neučinkovite politike uporabnikov. Vodstva služb se v takih primerih zelo rada odločijo, da uporabnikov o tem sploh ne informirajo (Šaponja 1999, 176).

Toda, ko se vzpostavi ta samocenzura izvajalcev obveščevalne dejavnosti, menim, da le-ta ne more biti več ustrezno učinkovita in/ali uspešna, zato so zgoraj omenjeni napori strokovnjakov KOD lahko celo ključni za uspešno in učinkovito izvajanje KOD.

2.3 Gospodarska družba

Preden sploh definiram termin gospodarska družba, je potrebno odgovoriti na vprašanje, ki se logično zastavlja. Ali ni sam termin KOD tak, da se logično sklepa, kdo ga uporablja oz. na kaj se nanaša? V preteklosti in tudi danes se večinoma ta termin uporablja v kontekstu, kot ga uporabljam tudi sam (vendar z dodatkom glede subjekta), vendar postaja (če že ni) jasno, da KOD uporabljajo tudi v javnem sektorju in pri neprofitnih organizacijah. Van de Kraats (2009, 20-23) tako pravilno ugotavlja, da zanimanje za KOD v neprofitnem in javnem sektorju vsekakor narašča in to pri

najrazličnejših organizacijah. Avtor (prav tam) kot primer organizacij, ki že uporabljajo KOD, navaja World Wildlife Fund, Medicins Sans Frontieres, mesta in dežele, ki želijo privabiti turiste in celo muzeje (in tako tekmujejo med seboj – so konkurenti) ipd.

Precej redko se v kontekstu proučevanja tega področja uporablja termin gospodarska družba, pogosteje avtorji uporabljajo termine kot zasebni/privatni/nejavni sektor, korporacija, podjetje, firma, gospodarstvo… Menim, da skoraj pri vseh terminih, avtorji opisujejo enak ali zelo podoben predmet proučevanja, ki pa ga nekoliko drugače poimenujejo. Sam sem se odločil za termin gospodarska družba, preprosto iz razloga, ker imamo zakon o gospodarskih družbah (ZGD-1-UPB3). ZGD natančno določa ta pojem. V 3. členu tako piše:

> *(1) Po tem zakonu je gospodarska družba pravna oseba, ki na trgu samostojno opravlja pridobitno dejavnost kot svojo izključno dejavnost.*
> *(2) Pridobitna dejavnost po tem zakonu je vsaka dejavnost, ki se opravlja na trgu zaradi pridobivanja dobička.*
> *(3) Gospodarske družbe (v nadaljnjem besedilu: družba) iz prvega odstavka tega člena se organizirajo v eni izmed oblik:*
> *- kot osebne družbe: družba z neomejeno odgovornostjo, komanditna družba in tiha družba, ali*
> *- kot kapitalske družbe: družba z omejeno odgovornostjo, delniška družba, komanditna delniška družba in evropska delniška družba.*
> *(4) Družbe iz prejšnjega odstavka se štejejo za gospodarske družbe, tudi če v skladu z zakonom v celoti ali deloma opravljajo dejavnost, ki ni pridobitna.*

Ker bom v nadaljnjem besedilu povzemal različne avtorje, se različnosti terminov (vendar skoraj enakega predmeta proučevanja) ni moč izogniti, pa vendar menim, da imajo avtorji in jaz sam v mislih tako podoben predmet proučevanja (če že ne enak), da to tudi iz vidika konsistentnosti ne bo predstavljalo večjih pomanjkljivosti.

2.4 Varnostna dejavnost gospodarskih družb

V spodnjem navedku razberemo definicijo varnostne dejavnosti z vidika države in v primerjavi z obveščevalno dejavnostjo.

> *Varnostna dejavnost pomeni preprečevanje, preiskovanje in odpravljanje določenih oblik ogrožanja varnosti neke dobrine, v tem primeru države. V primerjavi z obveščevalno dejavnostjo, ki predvsem pomeni zbiranje podatkov, njihovo analiziranje in obveščanje, je zagotavljanje varnosti oziroma varnostna dejavnost predvsem ukrepanje, in sicer pretežno na način ter z metodami in sredstvi, ki se razlikujejo od načina, metod in sredstev obveščevalne dejavnosti. Varnostno dejavnost kot funkcijo države opravljajo policija in druge varnostne službe (Purg 2002, 18).*

Varnostno dejavnost kot poslovno funkcijo je opredelil že Fayol. "Med klasičnimi predstavniki organizacijske znanosti je varnostno (ožje varstveno) funkcijo opredelil kot posebno poslovno funkcijo le Henry Fayol, tvorec linijske organizacijske strukture. Eksplicitno je navedel, da je vloga varnostne funkcije varovanje premoženja in ljudi, pri čemer gre za varstvo pri delu, požarno varstvo, zaščito pred sabotažami in zaščito poslovne tajnosti"[14] (Vršec 1993, 35).

Avtor nadalje razvija zgoraj zapisano:

> *Potemtakem je varnostna funkcija relativno samostojna poslovna funkcija, ki z varnostnim konceptom, s prodorno varnostno politiko in s profesionalnim varnostnim sistemom obvladuje temno plat delovanja podjetja. Hkrati pa je varnostna funkcija kot posebna poslovna funkcija interdisciplinarne narave, ker skrbi za čim bolj varen in nemoten potek izvajanja ostalih poslovnih funkcij (Vršec 1993, 36).*

Vršec (1993, 113) prepoznava štiri ključne varnostne dejavnosti podjetja:

[14] Izraz poslovna tajnost je bil v uporabi v starejši slovenski zakonodaji, medtem ko je v novejši v uporabi izraz poslovna skrivnost. Nekateri avtorji (npr. Kop 1995) pa predlagajo kot ustreznejši termin gospodarska skrivnost.

*Nadaljnje proučevanje varnostnih vprašanj v podjetjih nas je privedlo do spoznanja, da morajo v podjetju delovati štiri varnostne dejavnosti (*glej tabelo 2.1 op. M.A.*). Četrta je nastala iz tretje, iz katere je izločeno varovanje znanja, izkušenj in dokumentacije. Tako je nastal model varnostnih dejavnosti z vsebinsko in strukturno ustreznejšo členitvijo zaščitnih ukrepov v podjetju. … Nakazane so tudi oblike in načini zaščite, s katerimi je možno določiti realizacijo posameznih zaščitnih ukrepov. Npr.: zaščito zemljišča in stavb lahko izvedemo z večimi oblikami zaščite - ekološko, protipožarno, gradbeno in še kakšno - neposredno pa s fizično, tehnično in z zavarovalno premijo kot načini zaščite.*

Z vidika proučevane tematike je še posebno pomembna varnostna dejavnost D – Varovanje znanja; izkušenj; dokumentov, čeprav je seveda le celostni pristop smiseln in sploh učinkovit.

Tabela 2.1: Ključne varnostne dejavnosti podjetja

OBLIKE ZAŠČITE: protipožarna, protivlomna, protisabotžna, protidiverzijska, ekološka, logistična, ergonomska, gradbena, pravna, zdravstvena, socialna, psihološka in proti naravni ogroženosti	(Ključne) VARNOSTNE DEJAVNOSTI	NAČINI ZAŠČITE
	A - VAROVANJE PREMOŽENJA	neprofesionalno: • samozaščita varnostna kultura, civilna zaščita
	a_1 - zaščita zemljišča in stavb	
	a_2 - zaščita strojev, naprav, orodij, opreme, instrumentov, prevoznih sredstev, inventarja	
	a_3 - zaščita surovin, materiala, izdelkov, polizdelkov zalog, nedokončane proizvodnje	
	a_4 - zaščita denarja in vrednostnih papirjev, terjatev, posojil	
	B - VAROVANJE ZAPOSLENIH	profesionalno: • notranja kontrola • revizija
	b_1 - zaščita zaposlenih pri delu	
	b_2 - zaščita pravic zaposlenih	
	b_3 - zaščita statusa zaposlenih	
	b_4 - zaščita iniciative zaposlenih	
	b_5 - zaščita težko nadomestljivih strokovnjakov	
	C - VAROVANJE PROCESOV	profesionalno: • fizična, • tehnična kombinirana elektronska zaščita • zavarovanje pri zavarovalnici
	c_1 - zaščita proizvodnega procesa	
	c_2 - zaščita tehnično-tehnološkega in razvojnega procesa	
	c_3 - zaščita logističnega procesa	
	c_4 - zaščita poslovnega procesa	
	c_5 - zaščita tržnega procesa	
	c_6 - zaščita informacijskega procesa	
	D - VAROVANJE ZNANJA; IZKUŠENJ; DOKUMENTOV	NAČINI ZAŠČITE
	d_1 - zaščita intelektualne in industrijske lastnine	
	d_2 - zaščita ugleda podjetja	
	d_3 - zaščita poslovnih skrivnosti	
	d_4 - preprečevanje gospodarskega vohunjenja	
	d_5 - poizvedovanje po inovacijskem znanju	

Vir: Vršec (1993, 111)

Vršec glede na letnico nastanka njegovega dela logično še ne izpostavlja posebnega pomena nevarnostim, ki smo jim priča v današnjem digitaliziranem svetu, kar pa izpostavljata Egan in Mather (2005, 10).

> *Kraja informacijske lastnine je veliko tveganje pri varovanju informacij. Če je intelektualna lastnina v elektronski obliki, jo je veliko lažje ukrasti. Če so ti podatki shranjeni v računalnikih, ki so povezani v internet, jih lahko tatovi ukradejo od koder koli na svetu. Po raziskavi CSI/FBI Computer Crime and Security Survey (Računalniški kriminal in varnost) iz leta 2003 je najvišjo škodo povzročila prav kraja intelektualne lastnine.*

Ista avtorja (2005, 201) nadalje ugotavljata še: "Kiberprostor bo eno od bojišč prihodnosti. Države s pomembnimi vojaškimi sredstvi se bodo morale spopadati z grožnjami s področij, na katerih do zdaj ni bilo nevarnosti. Povečevanje zanašanja na računalniške sisteme pri komunikacijah, poslovanju in upravljanju osnovne infrastrukture še povečuje nevarnost." Čeprav avtorja v pričujočem navedku navajata države, povsem enako velja tudi za gospodarske družbe. Za ilustracijo navajam podatek, ki nedvomno da misliti o potencialnih nevarnostih. "Samo virus Love Bug je leta 2000 povzročil škodo v višini 8,75 milijarde dolarjev" (Egan in Mather 2005, 10).

"S stališča varovanja podjetja kot celote govorimo o zaščiti intelektualne in industrijske lastnine, zaščiti poslovnih skrivnosti in poizvedovanju za inovacijami. Načrtna zaščita tega - na prvi pogled nevidnega - premoženja prinaša podjetju znatne ekonomske, tehnološke, poslovne in moralne koristi" (Vršec 1993, 124). Zanimivo je, da je avtor izpostavil tudi zaščito pred poizvedovanjem za inovacijami, kar pripelje to dejavnost v kontekstu KOD na protiobveščevalni teren in to je vprašanje, ki se iz vidika KOD postavlja strokovnjakom – ali v okviru KOD izvajati tudi protiobveščevalno dejavnost.

2.5 Poslovna skrivnost

"S poslovnimi skrivnostmi ima človek opravka vse od takrat, ko je moral skrbeti za preživetje. Ko je bil še lovec, je bila njegova poslovna skrivnost npr. to, kako najzanesljiveje in najhitreje ujeti eno ali drugo vrsto živali" (Španinger 2008, 450).

Poslovna skrivnost je v luči pričujočega dela zelo pomembna zaradi dejstva, da je prav poslovna skrivnost največkrat na udaru, ko govorimo o vohunjenju. Vršeč (1993, 128) ugotavlja, da sta "… zaščita poslovnih skrivnosti in ekonomsko vohunjenje že dolgoletna sopotnika …", pa naj bo to kadar se do poslovne skrivnosti neke gospodarske družbe želi dokopati obveščevalna organizacija neke države ali gospodarske družbe. Podobno ugotavlja tudi Kop (1995, 52).

> *Poslovne skrivnosti ogrožajo vsi tisti, ki si od njih obetajo korist. Njihova pravnoorganizacijska oblika pri tem ne igra nobene vloge, saj je z našega stališča res vseeno, ali je tisti, ki jih ogroža, samostojni podjetnik, delniška družba ali pa družba z omejeno odgovornostjo. Stopnja ogroženosti ni nič manjša, če eno ali drugo podjetje še sploh ne obstaja, ampak se šele pripravlja na ustanovitev.*

Kdo vse lahko ogroža poslovne skrivnosti, je že skoraj zastrašujoče:

> *Za naše poslovne skrivnosti niso zainteresirani samo lastniki, managerji, poizvedovalni oddelki (intelligence units) in drugi zaposleni iz konkurence (oblikovalci, razvojniki in podobno), temveč tudi potencialni kupci naših delnic ali kar celega podjetja, dobavitelji, ki si želijo izboriti boljši položaj, pa odjemalci, ki želijo utrditi pogajalski položaj, ali pa novinarji, detektivske in poizvedovalne agencije. Lahko pa so to tudi razne nevladne organizacije, ki jih moti delovanje korporacije (ekološka gibanja kot npr. Greenpeace, protiglobalistične organizacije in skupine, ki se borijo proti velikim korporacijam, bojevniki proti uporabi jedrske energije, bojevniki za zdravo hrano) ali celo sekte. Včasih so to lokalne skupnosti ali sindikalne organizacije in podobno. Naše informacije pa lahko uporablja kriminalno podzemlje ali pa teroristične skupine in organizacije. Največja grožnja se običajno skriva kar v zaposlenih in njihovi brezbrižnosti ali neodgovornosti (Jelen 2009, 276).*

Opisno opredelitev poslovne skrivnosti navaja sledeči avtor.

V sedanjem času poslovne skrivnosti varujejo določene podatke, znanja in vednosti pred konkurenco na trgu. S poslovno skrivnostjo so zavarovana znanja o načinu in postopku organiziranja določenega dela, tehnologije, informacije o poslovnih partnerjih, zaposlenih, finančnih podatkih in vrste drugih informacij, ki so se v gospodarskih družbah zbirale in nastajale več let (Španinger 2008, 451).

Kop (1995, 43) jo definira kot: "Poslovna skrivnost podjetja so vse materializirane in nematerializirane stvaritve, ki jih poseduje in za katere tistim, ki jih za opravljanje svojega dela v podjetju (nujno) ne potrebujejo, ni treba vedeti. Stvaritve zajemajo tudi podatke". Za praktične namene pa je avtor (prav tam) še bolj ekspliciten. "Poslovna skrivnost je vse, kar bi konkurenca rada vzela s seboj!", kar se mi zdi še posebej primerno iz praktičnega vidika in dober napotek gospodarskim družbam naj imajo v mislih tudi to, ko se odločajo, kaj bodo opredelili kot poslovno skrivnost.

ZGD v 39. členu (pojem poslovne skrivnosti) definira pojem poslovne skrivnosti na sledeč način:

(1) 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.
(2) Ne glede na to ali so določeni s sklepi iz prejšnjega odstavka, se za poslovno skrivnost 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.
(3) Za poslovno skrivnost se ne morejo določiti podatki, ki so po zakonu javni ali podatki o kršitvi zakona ali dobrih poslovnih običajev.

Nadalje je v 40. členu ZGD (varstvo poslovne skrivnosti) navedeno tudi varstvo poslovne skrivnosti:

(1) S pisnim sklepom iz prvega odstavka prejšnjega člena družba določi način varovanja poslovne skrivnosti in odgovornost oseb, ki morajo varovati poslovno skrivnost.

(2) Podatke, ki so poslovna skrivnost družbe, morajo varovati tudi osebe zunaj družbe, če so vedele ali če bi glede na naravo podatka morale vedeti, da je podatek poslovna skrivnost.
(3) Prepovedano je ravnanje, s katerim bi osebe zunaj družbe poskušale v nasprotju z zakonom in voljo družbe pridobiti podatke, ki so poslovna skrivnost družbe.

Zgoraj navedene zakonske določbe in povezavo s preprečevanjem vohunstva pojasnita Podbregar in Žirovnik (2006, 52).

Krog ljudi, na katere se nanaša zakonska dolžnost varovanja poslovne skrivnosti, lahko delimo na dve skupini. V prvo skupino sodijo družbeniki, delavci, člani organov in druge osebe, ki so znotraj družbe in za družbo opravljajo delo na podlagi civilno pravnih pogodb. Prav tako pa so dolžne varovati poslovno skrivnost osebe zunaj družbe, ki na kakršen koli način zvejo za podatek, ki je predmet poslovne skrivnosti in vejo, ali pa bi po naravi podatka morale vedeti, da gre za poslovno skrivnost. Prav z razširitvijo dolžnosti varovanja poslovne skrivnosti na osebe zunaj družbe se preprečuje gospodarsko vohunstvo.

Značilnosti poslovnih skrivnosti našteva Kop (1995, 47-50):

- Neopaznost odtujitve

Nič ne manjka, in vendar našo poslovno skrivnost nekdo souporablja in nam dela škodo.

- Izguba za vedno

Ko konkurent izve za našo poslovno skrivnost, jo ve tudi, če nam mora vrniti npr. kopije tehnične dokumentacije našega stroja.

- Dolgi časi

Poslovne skrivnosti se lahko odtujujejo po delčkih (mozaična metoda), kar lahko traja leta; znan je primer, ko je to trajalo kar trideset let. Poleg te časovne razlike pa je za prakso morda še pomembnejša časovna razlika med trenutkom začetka odtujevanja in trenutkom, ko smo za odtujevanje izvedeli. Ta čas je lahko zelo dolg.

- Način prehajanja

Tisti, ki se hoče polastiti tuje materialne dobrine, skuša to storiti v razmerah, ki mu ob majhnem tveganju zagotavljajo, da ga pri dejanju nihče ne bo videl in da tudi kasneje nihče ne bo mogel ugotoviti, da je to storil prav on. Noč, zakrit obraz, uporaba rokavic, pripravljenost na uporabo orožja v primeru nevarnosti, uporaba vlomilskega orodja. Pri prehajanju poslovnih skrivnosti v neprave roke je to povsem drugače. Tu ne nastopajo »lopovi in žandarji«, temveč izobraženi, olikani in spoštovani ljudje, ki jim okolica zaupa. Med seboj se dobro poznajo in so celo prijateljsko povezani. Ne zakrivajo si obraza in ne potrebujejo vlomilskega orodja. Poslovne skrivnosti prehajajo v prijateljskem ozračju.

Kop (1995, 55) navaja sledeče načine ogrožanja poslovnih skrivnosti:

Tisti, ki hoče izvedeti naše poslovne skrivnosti in/ali jih uporabiti v svojo korist in našo škodo, ima na razpolago več možnosti. Izbira najustreznejše oz. kombinacije je odvisna od konkretnega primera. Včasih je uporaben en sam način, v drugih primerih vodi do »uspeha« kombinacija.

- *Zloraba*

O zlorabi govorimo, kadar nekdo, ki zaradi svojega dela ali siceršnjega razloga upravičeno pozna poslovno skrivnost, to izrabi v svoj prid in v škodo imetnika skrivnosti. Do zlorab večjega obsega pride predvsem, kadar se nekdo pripravlja, da bi z uporabo poslovnih skrivnosti svojega delodajalca zagotovil uspeh svojemu prihodnjemu podjetju oz. si zagotovil dober izhodiščni položaj pri prihodnjem delodajalcu.

- *Izdaja*

Pri izdaji gre za to, da nekdo, ki pozna poslovno skrivnost, to da na razpolago zainteresirani tretji osebi. Motivi za takšno dejanje so zelo različni in niso vedno povezani z materialnimi koristmi, vsaj na prvi pogled ne.

- *Gospodarsko vohunstvo*

Gospodarsko vohunstvo imenujemo uporabo prikritih metod za spoznanje poslovnih skrivnosti. Le redko se pojavlja v čisti obliki, saj je v večini primerov kombinirano z izdajo.

Pomen varovanja poslovne skrivnosti, ki se v primeru neuspeha lahko za podjetje konča celo usodno, poudarja naslednji avtor.

Z varovanjem podatkov o poslovnih skrivnostih gospodarska družba varuje svojo prednost na trgu in zaradi tega imajo poslovni podatki pomembno ekonomsko vrednost na sodobni stopnji gospodarskega razvoja. Poslovne skrivnosti so obrambno in napadalno sredstvo gospodarskega subjekta v tržni tekmi, zaradi česar zakonodajalec posveča tej problematiki posebno pozornost. Marsikateri uspeh lahko posamezna gospodarska družba pripiše varovanju poslovne skrivnosti. Hkrati pa je lahko tudi propad podjetja posledica neskrbnega ravnanja s poslovno skrivnostjo (Ivanjko, 2003: 2 v Španinger 2008, 451).

Sedaj, ko poznamo kaj je poslovna skrivnost, njene značilnosti in načine ogrožanja, je koristno vedeti, kako se izogniti nevarnostim, ki se v povezavi s poslovnimi skrivnostmi porajajo.

Splošne smernice za varovanje poslovnih skrivnosti so predvsem naslednje:

- *Če ne vemo, ali je kakšna zadeva v zvezi s podjetjem poslovna skrivnost ali ne, jo moramo obravnavati kot poslovno skrivnost.*
- *Vedno in povsod upoštevamo načelo »ni treba vedeti«. To načelo pomeni, da ne smemo govoriti o poslovnih skrivnostih z nikomer, ki mu tega za opravljanje dela v podjetju ni treba vedeti. To se nanaša brez izjeme na vsakogar, torej tudi na osebe z višjih in najvišje ravni v podjetju.*
- *Zavedati se moramo, da lahko preide poslovna skrivnost v roke nepoklicanim tudi z uporabo tako imenovane mozaične metode, zato nepoklicanim ne smemo dajati delčkov za sestavo mozaika.*
- *Večanje ugleda podjetja s tem, da poslovnim prijateljem in drugim kažemo svoje poslovne skrivnosti, je lahko zelo škodljivo. Prav je, če drugi vedo, da nam gre dobro, ni jim pa treba vedeti, zakaj nam gre dobro.*
- *Pomembnih poslovnih skrivnostih ne govorimo po telefonu in jih nešifriranih ne prenašamo po javnem prenosnem omrežju (Kop 1995, 187).*

Za zaključek poglavja o poslovni skrivnosti je primerna še ena zanimiva in poučna misel.

Da namreč poslovna skrivnost ostane skrivnost, ni samo v interesu njenega imetnika, temveč tudi v interesu celotnega narodnega gospodarstva, kajti pri neupravičenem prehodu poslovne skrivnosti lahko nastane škoda obema … Iz tega izhajata naslednja bistvena razloga za varovanje in zaščito poslovnih skrivnosti:

- *preprečiti gospodarsko škodo pri imetniku poslovnih skrivnosti,*
- *preprečiti gospodarsko škodo narodnemu gospodarstvu (Kop 1995, 56).*

"Z varovanjem in zaščito svojih poslovnih skrivnosti torej ne preprečujemo gospodarske škode le svojemu podjetju, temveč tudi celotnemu narodnemu gospodarstvu. Naša odgovornost je zato še večja" (prav tam). Dodajam še misel, da v kolikor se strinjamo s to mislijo, je potrebno razmisliti tudi o smiselnosti večje vključitve državnih organov v varovanje poslovnih skrivnosti oz. preprečevanje predvsem tujim državnim ali zasebnim organizacijam krajo vsaj vitalnih poslovnih skrivnosti. To pa je nekaj, kar nekatere države aktivno in načrtno počnejo, pri čemer v določeni meri tudi Slovenija ni izjema, kot mi je v pogovoru povedal Iztok Podbregar. Kot ilustracijo navajam, da je leta 2007 Jonathan Evans, generalni direktor britanske varnostne službe MI5, osebno pisal 300 vodilnim v britanskih podjetjih in jih opozoril, da je njihova informacijska infrastruktura napadena s strani organizacij, ki jih podpira kitajska vlada (http://www.timesonline.co.uk/tol/news/uk/crime/article7009749.ece).

Črnčec (2009, 214) meni, da se je potrebno lotiti nadgradnje obveščevalnega sistema Slovenije in kot enega izmed petih ukrepov zapiše. "…natančno preučiti kakšne možnosti lahko ponuja gospodarska obveščevalna dejavnost, ki jo v skladu z zakonom izvaja SOVA, poslovnim subjektom v zasebnem sektorju ter kaj od tujih primerjalnih rešitev bi bilo sprejemljivo za Slovenijo". Tudi sam menim, da bi bil to korak v pravo smer. Kot kaže zgoraj navedeni primer generalnega direktorja britanske varnostne službe, pa je kaj takega mogoče storiti tudi na neformalni »ad hoc« način.

3 INFORMACIJSKA REVOLUCIJA

Z različnimi termini, pa vseeno pomensko enako, razmišljata o informacijski revoluciji naslednja avtorja. "Razvoj storitev, kot so elektronska pošta, svetovni splet, novičarske skupine in sinhrono komuniciranje oz. klepetanje (ang. chating), najbolje odraža informacijsko revolucijo" (Svete 2005, 20). "Informacijska doba, informacijski čas, družba znanja, informatika, internet, informacijska (komunikacijska) tehnologija, mobilna telefonija so le nekateri pojmi, ki zaznamujejo zdajšnje obdobje informacijske revolucije" (Črnčec 2009, 47).

Implikacije pa so lepo vidne iz naslednjega odstavka:

> *Informacijska doba traja dobrih trideset let. Ne glede na to, ali verjamete v revolucije, je jasno, da se stopnja družbenih sprememb povečuje in zdaj na to najbolj vpliva naša sposobnost, da obdelamo informacije. Učinek informacijske tehnologije je očiten v našem vsakodnevnem življenju, doma in na delovnem mestu, v trgovinah in bankah, v šolah, visokih šolah in univerzah. Novi načini obdelovanja in avtomatizacije informacij se širijo, ljudje pa se sprašujejo, kako jih najbolje uporabiti in kako bodo vplivali na njihove otroke (Heap 2000 v Črnčec 2009, 48).*

Eno od implikacij (in to v svetovnem vidiku ogromno) vidi Nye (2004, 18), ko ocenjuje, da je vodilna vloga ZDA v informacijski revoluciji ob koncu 20. st. omogočila revolucijo v vojaških zadevah (ang. revolution in military affairs). Zmožnost uporabiti informacijsko tehnologijo za izdelavo natančno vodenih orožij, nadzorovanja v realnem času, obsežne zmogljivosti nadzorovanja regionalnih bojišč in izboljšani sistemi poveljevanja in nadzora so omogočili ZDA, da se povzpne kot edina vojaška supersila na svetu.

Friedman (2005/2008, 57-58) v svoji zelo vplivni knjigi Izravnavanje sveta celo izpostavlja informacijsko revolucijo kot ključni dejavnik padca Berlinskega zidu. "… če bi moral pokazati na en sam dejavnik, bi izbral informacijsko revolucijo, ki se je začela v začetku osemdesetih let prejšnjega stoletja. Totalitarni sistemi so odvisni od

monopola nad informacijami in vse preveč informacij je zaradi razmaha faksov, telefonov in nazadnje osebnih računalnikov začelo curljati skozi železno zaveso".

Že samo iz do sedaj napisanega vidimo, kako velike so implikacije informacijske revolucije v današnjem svetu. Z vidika proučevanja KOD pa je informacijska revolucija izrednega pomena, saj je omogočila velik razvoj in napredek te dejavnosti, tako kvalitativno kot kvantitativno, in verjetno ni slučaj, da je razvoj sodobne KOD časovno sovpadel z informacijsko revolucijo, čeprav to ni edini ali izključni vzrok nastanka KOD.

Svetovna avtoriteta na področju proučevanja konkurence, Michael E. Porter,[15] in Victor E. Millar sta že leta 1985 zapisala, kako vpliva informacijska revolucija na konkurenčnost.

> *Informacijska revolucija vpliva na konkurenco na tri bistvene načine:*
>
> - *Spreminja strukturo industrije in s tem spreminja pravila konkurence.*
> - *Ustvarja konkurenčno prednost s tem, da daje podjetjem nove možnosti s katerimi lahko prekosijo tekmece.*
> - *Ustvarja celotne nove poslovne panoge, pogosto znotraj že obstoječega delovanja podjetja (Porter in Millar 1985, 74).*

Posledice, ki jih informacijska revolucija prinaša, pa sta nedvoumno zapisala v spodnjem odstavku in brez dvoma menim, da sta imela prav.

> *O pomembnosti informacijske revolucije ni dvoma. Vprašanje ni, ali bo imela informacijska tehnologija pomemben vpliv na konkurenčni položaj podjetja, vprašanje je, kdaj in kako bo ta vpliv »udaril«. Podjetja, ki predvidevajo moč informacijske tehnologije bodo imela nadzor nad dogodki. Podjetja, ki pa ne bodo dovzetna, bodo prisiljena sprejemati spremembe, ki jih sprožajo drugi in se bodo znašla v konkurenčnem zaostanku (Porter in Millar 1985, 96).*

[15] Michael E. Porter velja za svetovno avtoriteto na področju proučevanja konkurenčnosti, njegovi znameniti knjigi Competitive Strategy (1980) in Competitive Adventage (1985) veljata za eni izmed najvplivnejših poslovnih knjig in sta (predvsem knjiga Competitive Strategy) navajani kot temelj na katerem se je razvijala KOD.

Iz zapisanega lahko lažje opredelimo, zakaj si informacijska revolucija zasluži obravnavo, ko govorimo o KOD. Če izpostavim dve, po mojem mnenju najpomembnejši lastnosti, gre za to, da je informacijska revolucija omogočila načine zbiranja, obdelave in širjenja informacij, kot si jih pred tem niti zamisliti nismo mogli[16] ter spremenila pravila igre konkurenčnosti.

3.1 Informacijsko-komunikacijska tehnologija

V prejšnjem poglavju sem poskusil prikazati nekatere značilnosti in posledice informacijske revolucije, katere temeljni in bistveni del seveda sestavlja informacijska tehnologija (IT) oz. informacijsko-komunikacijska tehnologija (IKT), kar ugotavlja tudi Wilson (1998 v Svete 2005, 17).

> *… IKT obravnavamo kot osnovo informacijske revolucije, ki je najbolj očitna v povečevanju zmogljivosti računalnikov, digitalizaciji podatkov in informacij ter konvergenci nekoč ločenih družbenih podsistemov v novo entiteto produkcijskih, distribucijskih in aplikativnih aktivnosti. Digitalizacija informacijskih procesov je tako omogočila združitev računalnikov, telekomunikacij, televizije in interneta v enotno multimedijsko (komunikacijsko) okolje, prav tako pa povzročila širjenje IKT tehnologije (predvsem njenega informacijskega dela) v skoraj vse družbene sektorje in aktivnosti, od zdravstva do transporta in izobraževanja.*

Svete (2005, 16) zelo dobro in s povzemanjem številnih strokovnjakov opredeli IKT na sledeč način.

> *IKT opredeljujejo številne znanosti, tako družboslovne kot naravoslovne. Za lažje razumevanje nadaljnje razprave in zaradi narave razvoja in uporabe v skoraj vseh družbenih sferah in podsistemih, je potrebna široka opredelitev IKT. Nanaša se torej na zbiranje, obdelavo in prikaz podatkov, prav tako pa vključuje tudi komunikacijski element, ki omogoča prenos podatkov. Tehnologije za obdelavo podatkov obsegajo tako združevanje podatkov in*

[16] V šaljivem tonu dodajam, da se verjetno z mano ne bodo mogli strinjati tisti, ki so prebrali znamenito knjigo Georga Orwella - 1984.

njihovo analizo kot tudi podporo pri odločevalskem procesu (Alberts, 1996; Wilson, 1998). Označuje prodor moderne elektronske, predvsem računalniške in komunikacijske tehnologije v metode obdelave informacij. Izvor termina sega v 70. leta 20. stoletja (Bosch, 2000: 86-87), bistveno pri njegovem širšem razumevanju pa je, da ne govorimo samo o tehnično-infrastrukturnem strojnem vidiku in napravah. Upoštevati moramo predvsem vidik programske opreme, ki daje napravam uporabno vrednost, in človeški dejavnik, ki programsko in strojno opremo seveda uporablja. Programski in strojni vidik je torej nujno povezati z uporabo pri doseganju želenih ciljev (tehnološka aplikabilnost oz. družbena uporabnost). Zato lahko IKT opredelimo kot sposobnost, znanje, spretnost oz. tehniko, da predvsem z uporabo strojev in naprav, ki omogočajo informacijske dejavnosti, dosežemo želene učinke (Svete 2005, 16).

V poročilu Mednarodne telekomunikacijske zveze - Merjenje informacijske družbe: IKT razvojni indeks (ang. International Telecommunication Union - Measuring the Information Society: The ICT Development Index) iz leta 2009, ki meri razvitost IKT v 154 državah sveta je zapisano, da je bilo ob koncu leta 2008 več kot 4 milijarde naročnin na mobilno telefonijo,[17] 1,3 milijarde priključkov fiksne telefonije in blizu ¼ svetovnega prebivalstva, ki uporablja internet, čeprav so, kot ugotavlja poročilo, razlike med regijami in razvitimi ter razvijajočimi državami zelo velike. Navedeno predstavlja skoraj neverjetne številke, ki so bile pred dobrim desetletjem preprosto nepredstavljive, ob tem, da se še večajo. Slovenija je glede na IKT razvojni indeks za leto 2009 med 154 državami zasedala visoko 28. mesto, čeprav je v primerjavi z letom 2007 nazadovala za 6 mest. Glede na ta indeks je vodilna svetovna država Švedska, ki ji sledita Južna Koreja in Danska, prav na repu pa so Gvineja-Bisao, Čad in Niger (prav tam).

Črnčec (2009, 58) pojasni, zakaj večja razvitost in uporaba IKT s seboj prinaša tudi (večje) nevarnosti.

[17] To ni enako 4 milijardam ljudi, ki bi uporabljali mobilni telefon, saj je penetracija mobilne telefonije v kar nekaj državah (med njimi se je pred kratkim pojavila tudi Slovenija) nad 100% in s tem seveda logični sklep, da ima kar nekaj ljudi več kot eno naročnino na mobilni telefon.

Dejstvo pa ostaja, da bolj ko je informacijska družba odvisna od uporabe IT, bolj je s tem tudi ranljiva za grožnje, naperjene zoper IT. Paradoksalno je IT kot sredstvo družbenega razvoja in napredka, ki v veliki meri spreminja družbene odnose, hkrati tudi največje orodje in orožje tistih, ki ne želijo informatizacije in globalizacije, saj si ne želijo družbe, kjer imajo ljudje sami dostop do informacij, ki jih zanimajo, ter si na podlagi njih lahko ustvarijo svoje mnenje, ki pa verjetno ne bo takšno, kot si ga želi oblast.

Kljub temu, da mobilno telefonijo uporablja precej več ljudi kot internet, se vseeno strinjam s sledečim. "Med vsemi informacijsko-komunikacijskimi tehnologijami pa ima uporaba interneta največje družbene implikacije" (Svete 2005, 19). In to velja tudi v primeru KOD (in tudi njene »temne plati« vohunstva), kar je razvidno tudi iz spodnjega odstavka.

IKT ne ponuja le okna, temveč kar glavna vrata priložnosti za nove poslovne izzive. Nujen sopotnik pa so tveganja in nevarnosti, ki jih prinašajo; tudi na področju ekonomske obveščevalne dejavnosti in vohunstva. Lahko bi si drznili postaviti trditev, da na tem področju še prav posebej. Pomislimo samo na internet: kaj vse lahko izvemo o našem konkurentu s povezovanjem informacij, ki jih dobimo na različnih strežnikih in različnih straneh; še najmanj na njegovi domači strani. Na primer, o njegovih zaposlenih se lahko pozanimamo z brskalniki kot sta Google ali Yahoo. Če pa mimo varoval skočimo še korak globlje, npr. do notranjih mrež, izvemo lahko več, kot o svojem podjetju ve večina zaposlenih (Jelen 2009, 239).

Tudi Svete opozarja na povezavo med IKT in vohunjenjem.

Poleg vpliva, ki ga ima uporaba IKT na sam način delovanja obveščevalnih služb, pa je pomembno opozoriti tudi na nova področja njihovega delovanja, ki so delno povezana z novimi tehnologijami, delno pa so posledica spremenjenih varnostno-političnih razmer po koncu hladne vojne. Med najpomembnejšimi novimi nalogami v večini držav je gotovo gospodarsko vohunjenje … (Svete 2005, 195).

Celovite varnostne implikacije uporabe IKT so predstavljene v tabeli 3.2 in ugotavljam, da je vse navedeno tudi potencialni vir ogrožanja gospodarske družbe. S tem postane povsem jasno, da je IKT po eni strani nujna za uspešno delovanje vsake gospodarske družbe, vendar obenem tudi (potencialni) vzrok ogrožanja.

Tabela 3.2: Varnostne implikacije uporabe IKT – človeški faktor – viri ogrožanja, motivacija in način delovanja

Človeška grožnja (vir)	**Namen (motivacija)**	**Metode, način delovanja**
Hekerji, krekerji	Izziv, lastni ego, uporništvo	Hacking, sistemski vdori, neavtorizirani vstopi v sistem
Računalniški kriminal	Uničevanje informacij Pridobitništvo (finančno) Neavtorizirano spreminjanje podatkov Nelegalno razkrivanje informacij	Računalniški kriminal Prevare Informacijsko podkupovanje »Spoofing« sistemski vdor
Terorizem	Izsiljevanje Uničevanje podatkov Izkoriščanje Maščevanje	Informacijsko bojevanje Sistemski napad (denial of service) Vdori v sisteme Nepooblaščeno spreminjanje sistemov
Industrijsko vohunjenje (družbe, tuje vlade, drugi vladni interesi)	Konkurenčna prednost Ekonomsko izkoriščanje	Ekonomsko vohunjenje Kraja podatkov, informacij Vdori oz. kršitve zasebnosti Vdori v sistem Nepooblaščeni dostopi v sistem (dostop do zaupnih, zakonsko zaščitenih in/ali tehnološko povezanih informacij)
Insiderji oz. zaposleni (slabo izobraženi, nepazljivi, nepošteni, zahrbtni, odpuščeni)[131]	Radovednost Ego Obveščevalna dejavnost Finančne koristi Maščevanje Nenamerne napake pri vnosu podatkov, programske napake	Napad na zaposlene Izsiljevanje Brskanje po zasebnih informacijah Zlorabe računalnikov Prevare in kraje Informacijsko podkupovanje Vnos ponarejenih, uničenih podatkov Prisluškovanje Zahrbtna koda (virusi, logične bombe, trojanski konji) Prodaja osebnih informacij Sistemske napake oz. hrošči Vdori v sisteme Sistemske sabotaže Nepooblaščeni vstopi v sistem

Vir: Wenger in Metzger (2004 v Svete 2005, 210)

Ob koncu poglavja bi izpostavil še naslednje:

Hiter tehnološki razvoj, še posebej na področju informacijsko-komunikacijskih tehnologij (IKT), ponuja osupljivo izbiro vedno novih možnosti pridobivanja

občutljivih informacij, na primer z elektronskim prisluškovanjem, skritim zvočnim ali slikovnim snemanjem, prestrezanjem elektronske pošte, vdiranjem v digitalne baze podatkov in podobno. Oprema, ki je bila včasih dostopna le obveščevalnim službam, je danes komercialno blago, zakonsko je omejena le uporaba. Drugi omejitveni dejavnik je seveda cena. Veliko tehnične opreme je danes že neverjetno poceni, vendar pa je vedno potrebno izračunati kakšno vrednost dobiš za svoj vložek. Glede na to, da je danes večina poslovnih informacij zabeleženih v digitalni obliki, pa so tehnične naprave in metode lahko nadvse prikladna rešitev (Jelen 2009, 225).

Zgoraj omenjeno sem ugotovil tudi sam, ko sem preko pogovorov (tudi z dobaviteljem oz. prodajalcem legalne in celo prepovedane opreme) ugotovil, da danes postati »ljubiteljski James Bond« z zelo solidno opremo za vsote, ki si jih lahko privošči (skoraj) vsakdo, ni več nikakršen problem.

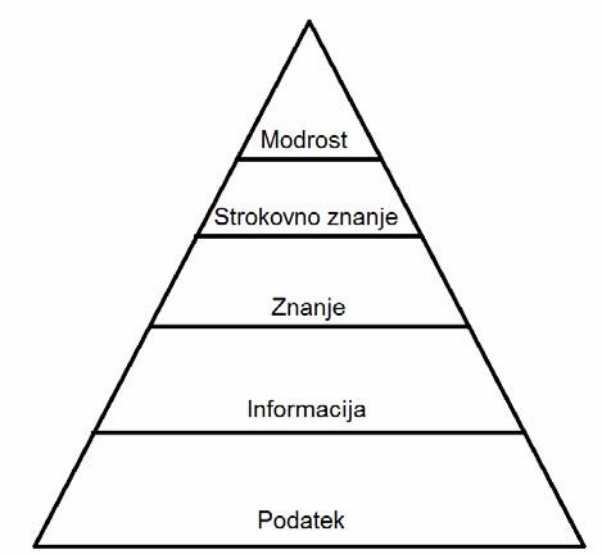
3.2 Podatek/informacija/znanje

Skoraj neverjetno se bereta naslednja citata eminentnih avtorjev iz 80 ih let 20. st. "Vpliv informacijske tehnologije je tako prodoren, da sooča vodilne s težkim problemom – preveč informacij. Ta problem ustvarja nove uporabe informacijske tehnologije za shranjevanje in analiziranje te poplave informacij, ki so na voljo vodilnim" (Porter in Millar 1985, 81). Jéquier in Dedijer (1987, 20) pa navajata, da "eden glavnih problemov, s katerim se sooča vsaka obveščevalna organizacija ni problem pridobivanja informacij ... ampak nevarnost preobilice informacij. ... Ta tendenca akumuliranja ogromnih količin, pogosto starih ali nepomembnih informacij, je eden tipičnih patoloških sindromov obveščevalnih organizacij" Če je bilo temu tako že takrat, kaj potem lahko rečemo danes?

Že v do sedaj zapisanem je moč velikokrat zaslediti termine, kot so: podatek, informacija, znanje, obveščevalni produkt… V pojasnjevalne namene je potrebno podati, kaj nekateri ti ključni termini pomenijo.

Liebowitz (2006, 7) predstavi t.i. informacijsko piramido (glej sliko 3.3), ki jo poimenuje hierarhija obveščevalnih produktov (ang. The Intelligence Hierarchy).

Slika 3.3: Hierarhija obveščevalnih produktov



Vir: Prirejeno po Liebowitz (2006, 7)

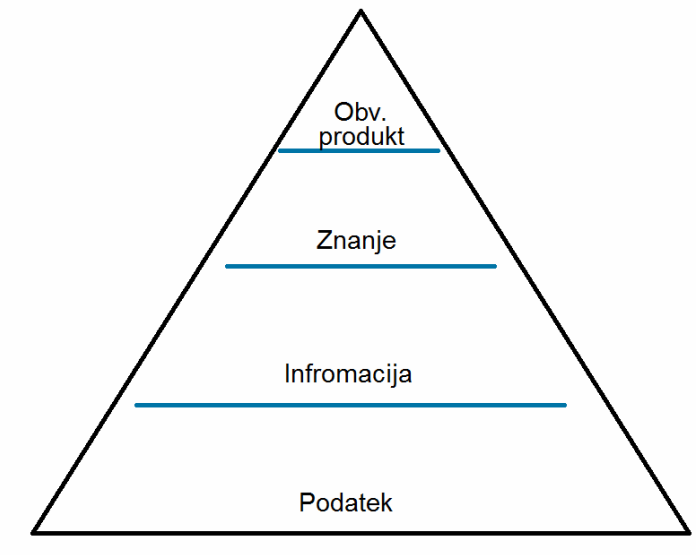
> *Podatek (ang. data op. M.A.) se nanaša na zaznane elemente. Ko je podatek na nek način strukturiran, postane informacija (ang. information op. M.A.). Informacija skupaj z razumevanjem in poznavanjem postane znanje (ang. knowledge op. M.A.). Znanje na specializiranem področju postane strokovno znanje (ang. expertise op. M.A.). Strokovno znanje se po mnogih letih izkušenj in spoznanj oblikuje v modrost (ang. wisdom op. M.A.) (Liebowitz 2006, 7).*

Global Intelligence Alliance (GIA White Paper, 2004) precej podobno predstavi, kar poimenujejo piramida obveščevalnih produktov (ang. The Intelligence Pyramid) - glej sliko 3.4.

… /K/ljub temu, da sta informacija (ang. information op. M.A.) in obveščevalni produkt (ang. intelligence op. M.A.) včasih uporabljana kot sinonima, sta na različni stopnji piramide. Ko se premikamo po piramidi navzgor, se premikamo od kvantitete (ogromne količine podatkov in informacij dostopnih vsem) do kvalitete (obveščevalni

produkt, ki vodi do specifičnih odločitev in delovanj, ki lahko omogočijo konkurenčno prednost) (GIA White Paper 2004, 3).

Slika 3.4: Piramida obveščevalnih produktov



Vir: Prirejeno po GIA White Paper (2004, 4)

Iz obeh slik in razlag je moč potegniti zaključek, da imeti podatek, informacijo ali celo znanje ni dovolj ali pač ne optimalno. Potrebno je nadgraditi znanje in iti še dlje do Liebowitzove modrosti ali kot menijo pri GIA, do obveščevalnega produkta, ki vodi do specifičnih odločitev in delovanj, ki lahko omogočijo konkurenčno prednost.

Kljub zapisanemu pa seveda velja, kar pravi Podbregar (2008, 21). "Pravočasne in dobre informacije v današnjem svetu pomenijo prednost, pa naj se to nanaša na politično, gospodarsko ali vojaško področje…", vendar le, če imamo sposobnosti in zmogljivosti, da te informacije na pravi način analiziramo in jim dodamo lastnost oz. zmožnost, da je na podlagi njih moč ukrepati. Podobno ugotavljata tudi sledeča avtorja:

> *V današnjem svetu preobilice informacij, po našem mnenju, zbiranje podatkov ali informacij ni ključna zadeva. Namesto tega je raziskovanje in vrednotenje informacij z analizo ključno za definiranje ustreznih strategij. Ta proces potrebuje veščine, čas in napor. Medtem ko večina organizacij zbira nekatere oblike konkurenčnih informacij, jih presenetljivo malo za to uporabi*

formalizirano analizo in vključi rezultate v svoje poslovne strategije (Fleisher in Bensoussan 2003, 12).

3.3 Pomen informacij za delovanje gospodarskih družb

V tem in nekaterih naslednjih poglavjih je zaradi terminološke preprostosti in uveljavljenosti terminov uporabljen termin informacije. V skladu s prejšnjim poglavjem pa moramo imeti v mislih in se zavedati, da ne gre samo za pomen informacij za delovanje gospodarskih družb, temveč za vse navedeno v prejšnjem poglavju omenjenih piramidah, saj je za (uspešno) delovanje gospodarske družbe lahko pomemben tako podatek kot informacija, znanje, modrost, obveščevalni produkt… Lahko rečemo, da višje kot je na piramidi, pomembnejše je za gospodarsko družbo.

O pomenu podatkov na splošno govori naslednji avtor:

> *Posamezniki in organizacije, tako profitne kot neprofitne, se v dinamičnem okolju v katerem živimo in ga kreiramo, srečujejo z vse večjo potrebo, ki bi jo na kratko lahko opisali s stavkom: »Potrebujem pravočasne, točne in uporabne podatke za odločanje.« Relativno preprost stavek, ki pa pred nas največkrat postavlja velike ovire, zahteva izjemno organiziranost in delovanje različnih teamov, skupin ter odlično infrastrukturo večkrat vezano na najsodobnejše informacijske tehnologije (Podbregar 2008, 13).*

Če imamo v mislih prejšnje poglavje, gre Kahaner (1996, 15) še korak dalje in v smer pomembnosti za podjetja:

> *V današnjem poslovnem okolju imeti prave informacije ni več dovolj. V svetu, kjer so konkurenti ostrejši kot kadarkoli, hitro spreminjajoče tehnologije spreminjajo pravila igre vsakodnevno in ena napačna poslovna poteza lahko uniči podjetje, menedžerji iščejo nove možnosti za odločanje. Mnogi menedžerji menijo, da so ključ informacije. Mislijo, da če imajo dovolj informacij, bodo sprejeli pravilne odločitve. Nič ni dlje od resnice. … Informacije so zgolj začetek procesa sprejemanja odločitev in ne njegov*

konec. In čeprav je kvaliteta informacij pomembna, je veliko pomembneje, kaj naredite z njimi – kako jih analizirate in nato kako jih uporabite.

Do sedaj smo ugotovili, da so podatki in informacije, ki jih pridobimo, seveda zelo pomembni, vendar je s tem, če imamo v mislih obveščevalni krog, storjen šele drugi korak in kot Kahaner zelo nazorno pojasni, to (še) ni dovolj. Potrebno je nekaj več. Po mnenju teoretikov in praktikov KOD lahko to nekaj več predstavlja KOD. "Organizacije, ki so uspele implementirati uspešne formalne in strukturirane procese KOD, ki se osredotočajo na ključne zadeve, bodo imele konkurenčno prednost pred njihovimi tekmeci. Organizacije si preprosto ne morejo več privoščiti, da ne bi imeli uspešnih KOD zmogljivosti" (Havenga in Botha 2003, 20).

Pri gospodarskih družbah je cilj doseči konkurenčno prednost pred tekmeci, ki jo Porter (1985/1998, 33) opredeli na sledeči način. "Konkurenčno prednost ne moremo razumeti z gledanjem podjetja kot celote. Izvira iz mnogih ločenih dejavnosti, ki jih podjetje izvaja z oblikovanjem, proizvodnjo, marketingom, dostavo in podporo izdelkom". Podatke in informacije lahko razumemo kot »surovine«, KOD pa na podlagi tega, »program« za oblikovanje obveščevalnega produkta, ki ima za namen uresničiti zastavljeni cilj – konkurenčno prednost, ki izhaja iz različnih področij, kot je to opredelil Porter. Vendar se je potrebno zavedati, da se v resničnem svetu vloga KOD s tem konča. Obveščevalni produkt izkoristijo ali pač ne tisti, ki odločajo v neki gospodarski družbi. Nič ne pomaga razpolaganje s prvovrstnimi obveščevalnimi produkti, če temu ne sledijo ustrezna delovanja, zato SCIP in vodilni teoretiki in praktiki KOD posebej poudarjajo ustrezen odnos odločevalcev do KOD, saj je brez tega KOD brez pomena.

3.4 Varovanje informacij

Kot smo ugotovili v prejšnjih poglavjih, so informacije izredno pomembne, v nepravih rokah lahko celo ogrozijo obstoj gospodarske družbe. Winkler (1997, 3) to predstavi še bolj dramatično. "Informacije v nepravih rokah lahko uničijo korporacije, ljudje izgubijo službe, lokalni trgovci bankrotirajo, uničene so družine delničarjev". Že na podlagi zapisanega postane očitno dejstvo, da je informacije potrebno varovati. "Informacije so poleg kapitala, ljudi, naravnih virov in znanja čedalje pomembnejši vir

podjetja, so sredstva z določeno vrednostjo, ki jih je potrebno zaščititi. Varovanje informacij le-te ščiti pred različnimi nevarnostmi, z namenom zagotoviti varno in neprekinjeno poslovanje ter omejiti poslovno škodo na najmanjšo možno raven" (Podbregar 2008, 19). In še napotek, ki je, če vsaj delno verjamemo zgoraj zapisanemu, več kot upravičen. "Program za varovanje informacij naj bo … ena glavnih prioritet poslovanja vašega podjetja" (Egan in Mather 2005, 10).

Da pa je to področje varovanja informacij hitro spreminjajoče, opozarjata naslednja avtorja. "Področje varovanja informacij je izjemno dinamično. Grožnje, ki še pred letom niso bile verjetne, so lahko resna težava že naslednji teden. Ves čas nastajajo nove nevarnosti…" (Egan in Mather 2005, 29). Ker obstajajo nevarnosti, se je razvila tudi obramba. "Glavne kategorije varnostne tehnologije sestavljajo požarni zidovi, protivirusna programska oprema, zaznavanje vdorov, upravljanje pomanjkljivosti in filtriranje vsebine" (Egan in Mather 2005, 32).

V tabeli 3.3 je povzetek glavnih vrst tehnologije za varovanje informacij, ki se danes uporabljajo in njihov namen.

Tabela 3.3: Pregled tehnologije za varovanje informacij

Varovanje poslovanja-tehnologija	**Namen**
Nadzor dostopa	Dovoli dostop do sistema samo pooblaščenim zaposlenim, strankam, ponudnikom ali partnerjem.
Požarni zidovi	Preprečuje vstop nepooblaščenega prometa v omrežje.
Protivirusna programska oprema	Sredstva informacijske tehnologije varuje pred zlonamerno kodo.
Upravljanje pomanjkljivosti	Redno preverjanje in odpravljanje mogočih varnostnih lukenj.
Zaznavanje vdorov	Odzove se na nepooblaščene dostope v omrežje.
Filtriranje vsebine	Zagotovi, da osebje nima dostopa do neprimernih vsebin v računalnikih v podjetju.
Šifriranje	Preprečuje prisluškovanje oz. prebiranje zasebnih sporočil, ščiti omrežni promet in omogoča preverjanje pristnosti.

Vir: Prirejeno po Egan in Mather (2005, 41)

Navedeno je potrebno razumeti kot varovanje digitalnih informacij, torej tistih, ki se nahajajo v digitalizirani obliki, najpogosteje na računalnikih.

4 GOSPODARSKA OBVEŠČEVALNA DEJAVNOST

Avtor v naslednjem odstavku razloži, zakaj in kako se razvije GOD:

> *Na gospodarskem področju se je obveščevalna dejavnost razvijala od prvih začetkov velikih finančnih in gospodarskih korporacij. Dominirala je v zasebnem sektorju, manj pa je bila uveljavljena na državni ravni. V zadnjem desetletju in pol sta se razvoj in uporaba te dejavnosti razširila tudi na državno raven. Razlogov za to je več. Država potrebuje dobre in pravočasne podatke za boljše pogajalske pozicije pri pogajanjih med državami ali mednarodnimi organizacijami. Za nacionalno varnost je pomembno zbiranje podatkov na gospodarskem področju, saj sta gospodarska stabilnost in napredek ključnega pomena za politično in vojaško moč neke države in s tem temelja njene nacionalne varnosti. Z obveščevalno dejavnostjo se preučuje moč drugih držav in išče njihove šibke točke, hkrati pa omogoča ustvarjalcem politike sprejeti pravočasne makroekonomske ukrepe za zaščito domačega gospodarstva. Posredno mnogo pomaga pri njegovem prilagajanju novim razmeram. Eden od razlogov, da so se obveščevalne službe usmerile tudi na to področje, je gotovo konec hladne vojne, ki je zahteval iskanje novih področij dela za obveščevalne službe (Šaponja 1999, 37).*

Angleški termin Economic Intelligence je termin, ki opisuje dejavnost, ki v svetu v zadnjih desetletjih nedvomno pridobiva na pomenu, kar se utemeljuje predvsem s prehodom iz geostrategije v geoekonomijo po koncu hladne vojne. Da je temu res tako, je vidno tudi na primeru verjetno najvplivnejše obveščevalne službe na svetu.

> *Iz tuje prakse je znan primer strateške preusmeritve ameriške centralne obveščevalne službe CIA[18] ob koncu hladne vojne. Službo so namreč preusmerili iz varnostno-političnega v gospodarski obveščevalni prostor*

[18] Ang. Central Intelligence Agency.

(v proti-terorizem šele kasneje). Za ta namen imajo, na primer ZDA, ustanovljene tudi posebne obveščevalne službe, ki so organizirane v okviru gospodarskega ministrstva (naftno področje, atomska energija) (Kastelic 2008, 65).

V slovenščino angleški termin avtorji večinoma prevajajo kot gospodarska obveščevalna dejavnost ali ekonomska[19] obveščevalna dejavnost in ju uporabljajo večinoma kot sopomenki. Nekateri avtorji celo ločijo razliko med slovenskima terminoma. Sam bom angleški termin prevajal kot gospodarska obveščevalna dejavnost (GOD). Še en pomemben vidik pa je, kako opisati in razložiti ta termin, pri čemer (ponovno) nastane precejšnja zmeda ali pač samo različno razumevanje. Nekateri razumejo to dejavnost ne glede na akterja, ki jo izvaja, spet drugi samo kot dejavnost državnih obveščevalnih služb, nekateri celo samo kot dejavnost gospodarskih družb. Področje GOD je seveda izredno obširno in bi bilo lahko samostojni predmet proučevanje takšnega dela. Sam ga bom predstavil zgolj okvirno in v toliko, kolikor je pomembno za kompleksno razumevanje KOD. Sam bom razumel to dejavnost v skladu s spodnjo definicijo, seveda pa jo je treba upoštevati z mislijo na to, da je bila pisana z mislimi na ZDA.

Gospodarska (ekonomska) obveščevalna dejavnost je eno od področij, v katera so usmerjene nacionalne obveščevalne službe. Zbiranje informacij o gospodarskih trendih in ocenjevanje njihovih implikacij na nacionalno varnost ZDA je eden od ključnih vidikov, kako lahko obveščevalna skupnost pomaga načrtovalcem politik razumeti in nato ustrezno nasloviti ključne prihajajoče zunanjepolitične in varnostne izzive. Gospodarska obveščevalna dejavnost ima dvojno poslanstvo: prvič, da zagotovi strateško opozorilo o mednarodnih gospodarskih trendih, ki lahko pomembno vplivajo na interese ZDA: in drugič, da zagotovi taktične informacije in analize za odločevalce in izvajalce politik o pomembnih mednarodnih gospodarskih vprašanjih za podporo njihovim vsakodnevnim dejavnostim doma in v stiku s tujimi partnerji (Gannon 1997 v Črnčec 2009, 119).

[19] SSKJ (1994, 250 in 190) opredeli pridevnik gospodarski kot "nanašajoč se na gospodarstvo" in pridevnik ekonomski kot "nanašajoč se na ekonomiko, gospodarski".

Za boljše razumevanje magistrskega dela želim vzpostaviti razliko glede na izvajalca obveščevalne dejavnosti. V kolikor to dejavnost izvaja državna obveščevalna služba na gospodarskem področju, gre za GOD in v kolikor jo izvajajo gospodarske družbe, za KOD. "Podatke o razmerah, vključno z gospodarskimi, o finančnih gibanjih in stabilnosti, o upoštevanju ekonomskih načel, itd. zbirajo obveščevalne službe v javnem sektorju, ki so specializirane za gospodarsko obveščevalno dejavnost" (Črnčec 2008, 126). Ta delitev se mi zdi nujna že iz razloga, ker ima obveščevalna služba neprimerno večje možnosti delovanja, ki niso omejene z legalnostjo njihovega početja.

Gannon (1997 v Črnčec 2009, 119) podrobneje opiše predmet zanimanja in delovanja GOD:

> *Obveščevalna skupnost v svojih gospodarskih analizah preučuje hitrost, obseg in smer gospodarskih reform ter spremlja izvajanje gospodarskih politik v državah in na nastajajočih trgih, pomembnih za nacionalne interese. Poseben poudarek je namenjen:*
>
> - *svarilom pred morebitnimi gospodarskimi krizami z ocenjevanjem finančnih ranljivosti, razmer v nacionalnem gospodarstvu in groženj svetovnim energetskim zalogam;*
> - *razumevanju nastajanja gospodarske politike v tujini; zaznavanju in ocenjevanju kompleksnosti razmerij med gospodarskimi, političnimi in družbenimi dejavniki, ki vplivajo na nastajanje politik in gospodarstvo na nastajajočih trgih in v državah posebnega interesa;*
> - *malopridnim državam in nezakonitim dejavnostim. Spremljanje gospodarstva v malopridnih državah in njihovih zunanjetrgovinskih povezav, učinka gospodarskih ukrepov in razvijanje pristopov za celovito sledenje finančnim mrežam, ki podpirajo trgovce z mamili, teroriste in proliferatorje (razširjevalce) orožja za množično uničevanje;*
> - *zagotavljanju enakih ekonomskih načel in enakih pogojev za vse države. Obveščevalna skupnost ni zadolžena za izvajanje ukrepov, temveč o tem le poroča pristojnim.*

Zgoraj so našteti nekateri poudarki, ki jih obveščevalne službe dajejo GOD. Da je predmet zanimanja tujih služb v takšnem kontekstu tudi Slovenija, ugotavlja Kastelic:

> *Tuje obveščevalne službe so na področju gospodarstva (v uporabi je tudi izraz gospodarsko vohunstvo)[20] usmerjene predvsem v zbiranje podatkov o strategijah in gospodarskih usmeritvah slovenskega gospodarstva. Tako so države zainteresirane za tekoče seznanjanje z vsemi odločitvami prometnega, finančnega in gospodarskega značaja (v ožjem smislu), saj je gospodarstvo temelj nacionalne neodvisnosti in varnosti. Pogosto so obveščevalne službe usmerjene tudi v zbiranje in proučevanje kapacitet strateških panog gospodarstva ali celo določenih podjetij, v cilju preverjanja primernosti sklepanja pogodb o sodelovanju, pa vse do spodkopavanja konkurenčnih podjetij ali kar celotnih gospodarskih panog določene države (Kastelic 2008, 65).*

Po mnenju strokovnjaka za obveščevalno dejavnost (intervju) bi morala biti tudi prva prioriteta SOVE gospodarsko področje. Iz njegovega mnenja sklepam, da danes temu ni tako, pa vendar, kot mi je potrdil Iztok Podbregar, SOVA seveda aktivno spremlja gospodarsko področje.

Kastelic v zgornjem odstavku razkriva tudi temnejše plati GOD, celo npr. spodkopavanje konkurenčnih podjetij, pred čemer si seveda ne smemo zatiskati oči. Menim, da je edina organizacija, ki je sposobna kaj takega zaznati in preprečevati, predvsem SOVA in njene protiobveščevalne zmogljivosti. Prepričan sem tudi, da se je s pojavom krize, ki smo ji priča, tudi gospodarski boj med državami in gospodarskimi družbami še precej okrepil in bodo države vedno več svojih obveščevalnih aktivnosti (in verjetno vedno bolj agresivnih) posvečale pridobivanju novih poslov, pridobivanju konkurenčnih prednosti idr.

V zgornjih odstavkih so že nakazane (možne) povezave oz. prepletanja med GOD in KOD, na kar opozarja Črnčec (2008, 136), kar odpira še en pomemben vidik področja. Torej, da je možno, da neka gospodarska družba nima nasproti le druge

[20] Kot že ugotovljeno, ne smemo enačiti vohunstva z obveščevalno dejavnostjo, saj vohunstvo predstavlja le (manjši) del druge stopnje obveščevalnega kroga – pridobivanja podatkov.

konkurenčne gospodarske družbe, temveč ji lahko nasproti stoji celo državna obveščevalna služba. "Ko ostane konkurenčna obveščevalna dejavnost za pol koraka prekratka pri zagotovitvi informacij naročnikom (zaradi neposluževanja nelegalnih oblik zbiranja podatkov ali pač premajhnih zmogljivosti op. M.A.), je gospodarska obveščevalna dejavnost tista, ki lahko zagotovi zgoraj predstavljene manjkajoče odstotke".[21]

Navedeno nas pripelje bližje temni plati GOD – gospodarskemu vohunstvu. "Če je gospodarska diplomacija svetla plat zbiranja podatkov, je temna plat gospodarske obveščevalne dejavnosti nezakonito pridobivanje podatkov s človeškimi viri, gospodarsko (ekonomsko) vohunstvo" (Črnčec 2009, 122).

4.1 Vohunstvo in gospodarska obveščevalna dejavnost

Ko govorimo o področju obveščevalne dejavnosti, ne moremo mimo vohunstva, saj je le ta (večinoma) inherenten tej dejavnosti in lahko celo rečemo, da mistificira to dejavnost, pa naj bo zaradi resničnih zgodb, ki pridejo v javnost, ali pa zaradi pop kulture, ki je vohunstvo v številnih knjigah in filmih močno »popularizirala«.

4.1.1 Vohunstvo – o terminu

Sloviti Sun Tzu[22] v svoji razpravi izpred pribl. 2400 let, Umetnost vojne, nameni celotno trinajsto poglavje vohunom. Sun Tzu loči pet vrst vohunov:

- krajevni: prihajajo iz vrst sovražnikovih rojakov;
- notranji: iz vrst sovražnikovih uradnikov;
- dvojni: iz vrst sovražnikovih lastnih vohunov;
- mrtvi: so tisti, za katere namenoma ustvarimo napačne informacije; oni jih potem prenesejo sovražniku;
- živi: so tisti, ki se vrnejo z informacijami.

[21] Različni avtorji ugotavljajo, da se od 1% do 20% informacij zbere na nelegalen način.
[22] Tudi Sunzi, mojster Sun, s pravim imenom Sun Wu. Rojen naj bi bil okoli leta 554 pr. n. št. O Sun Tzuju povzemam iz prevoda Johna Minforda (2003/2009).

Iz samega teksta je viden izreden pomen, ki ga Sun Tzu pripisuje pomembnosti vohunjenja oz. uporabe vohunov, kar je moč razbrati tudi iz naslednjih citatov: "V vsej vojski ne bi smel biti nihče bližji poveljniku kot njegovi vohuni, nihče deležen večjih nagrad, nihče obravnavan zaupneje"; "Premetenost vseh premetenosti! Vohuni so uporabni na nešteto načinov" in predvsem "Vohuni so ključni element v vojskovanju. Od njih je odvisna vsaka poteza vojske".

Ugotovimo lahko, da se vohunstvo uporablja »od nekdaj«. Če gremo še dlje in ponovimo rek, da je obveščevalna dejavnost druga najstarejša obrt na svetu in s precej veliko mero verjetnosti zatrdimo, da se pod pojmom obveščevalne dejavnosti v preteklosti v veliki meri razume prav vohunjenje, lahko sklepamo, da je bil pomen vohunjenja resnično ogromen.

Če preskočimo dobri dve tisočletji v prihodnost, pridemo do vohunstva v sodobnejšem pojmovanju.

> *Sodobno vohunstvo se je začelo razvijati ob koncu prejšnjega stoletja. Za njegov razvoj je najbolj zaslužna angleška obveščevalna služba, katere razmah je bil tudi tesno povezan z njeno vlogo kolonialnega imperija. V 19. stoletju je opazen razmah obveščevalnih služb, kar je bilo predvsem povezano z osvajanjem novih ozemelj, širjenjem tržišč, bojem za gospodarsko, vojaško in politično prevlado, ustvarjenjem nacionalnih držav in drugim. Vse to je vplivalo na profesionalizacijo obveščevalnih služb, poleg tega pa se je obseg obveščevalnih dejavnosti širil iz vojaške in politične sfere na ekonomsko, znanstveno, tehnično in druge. Napoleon Bonaparte je tudi vzpostavil učinkovito obveščevalno in še zlasti protiobveščevalno službo, s čimer si je med drugim zagotavljal oblast (Purg 2002, 25).*

Šaponja (1999, 59) opredeli vohunstvo kot:

> */P/repovedano zbiranje tajnih, z zakoni zaščitenih podatkov, ali pa opravljanje z zakoni prepovedanih aktivnosti, povezanih z obveščevalno dejavnostjo. Gre torej za protipravne aktivnosti, za katere določa pravni red kazenskopravne sankcije. Z obveščevalno dejavnostjo zbiramo tudi take*

podatke in opravljamo v tem smislu protipravne aktivnosti (v domači zakonodaji so take aktivnosti obveščevalne službe legalizirane s posebnimi zakoni o obveščevalni dejavnosti in službah). Zato lahko rečemo, da je vohunstvo le del in ena od metod obveščevalne dejavnosti, nikakor pa ne more biti njen sinonim.

V omenjeni opredelitvi so navedene nekatere izrazito pomembne lastnosti vohunstva. Gre sicer za prepovedano aktivnost, vendar ne iz vidika domače zakonodaje, ko vohunjenje izvajajo obveščevalne službe v skladu z njihovimi (zakonsko določenimi) pristojnostmi. Že iz tega je razvidno, da je vohunjenje kogarkoli drugega izven teh okvirov protizakonito (iz vidika lastne države seveda). K zadnjemu delu gornjega citata bi še dodal, da je vohunjenje le ena od metod druge stopnje obveščevalnega kroga – zbiranja podatkov in je tako povsem na mestu ugotovitev, da vohunjenje ni sinonim za obveščevalno dejavnost niti v primeru nacionalnih obveščevalnih služb. Pri nedržavnih obveščevalnih organizacijah pa vohunjenje sploh ne sme biti prisotno oz. del dejavnosti, če le-ta želi biti legalna, kar je razvidno tudi iz naslednjega. "Vohunstvo je ožji pojem od obveščevalne dejavnosti (predstavlja okoli 10- do 20-odstotni delež v celotni obveščevalni dejavnosti) in se lahko pravno okvalificira kot kaznivo dejanje" (Purg 2002, 16).

Ker se pojavlja cela vrsta terminov, ki podrobneje delijo vohunstvo, so v nadaljevanju predstavljeni najpomembnejši.

4.1.2 Gospodarsko in konkurenčno vohunstvo

V tem podpoglavju bom poskusil razložiti razliko med gospodarskim (ang. economic espionage) in konkurenčnim vohunstvom (ang. competitive espionage), kot ga razumem sam. Ta delitev se mi zdi zelo pomembna, saj razločuje vohunstvo glede na subjekt, ki vohunstvo izvaja. Táko razločevanje ni vsesplošno, kar je v spodnjem citatu zelo dobro vidno.

Gospodarsko vohunstvo ima za cilj spodkopavanje konkurenčnih podjetij ali kar vseh gospodarskih panog. Take operacije ne izvajajo le zasebne, korporacijske obveščevalne organizacije, marveč tudi državne obveščevalne

službe. Spomnimo se samo zaostritve odnosov med državama, ko je Francija obtoževala ZDA, da je CIA vohunila in izvajala tajne operacije v francoskih podjetjih (Šaponja 1999, 44).

Tudi Kop (1995, 69) ne vzpostavi razlike oz. celo menim, da ima z gospodarskim vohunstvom v mislih to, kar sam menim, da je konkurenčno vohunstvo. "Pri gospodarskem vohunstvu gre za uporabo prikritih metod pri zbiranju informacij o poslovnih skrivnostih. ... Z vso gotovostjo namreč lahko izhajamo iz tega, da nevarnost gospodarskega vohunstva obstaja in da bo tudi vedno večja; slednje velja še posebej za gospodarsko vohunstvo po naročilu". Kop (1995, 69-70) razdeli gospodarsko vohunstvo na notranje in zunanje.

O notranjem gospodarskem vohunstvu govorimo, kadar uporabi prikrite metode sodelavec v podjetju. V podjetjih, kjer sta varovanje in zaščita poslovnih skrivnosti na visoki ravni, je večja nevarnost za tovrstno pot do poslovnih skrivnosti. … Za zunanje gospodarsko vohunstvo gre, če uporabi prikrite metode nekdo, ki ni zaposlen v podjetju z želeno poslovno skrivnostjo. V primerih, ki so prišli v javnost, je šlo v veliki večini za takšno vohunstvo (Kop 1995, 69-70).

Zato pa omenjeno razliko ugotavlja Črnčec (2008, 145). "Konkurenčno vohunstvo je ožji pojem od gospodarskega vohunstva in obsega zgolj pridobivanje podatkov o konkurenci na nezakonit način znotraj zasebnega sektorja. Torej med podjetji samimi ali po naročilu določenega podjetja". Idealno tipsko bi torej lahko razdelili, da gre za konkurenčno vohunstvo, kadar gre za pridobivanje podatkov na nezakonit način znotraj zasebnega sektorja, za gospodarsko vohunstvo pa kadar ga izvajajo državne obveščevalne službe za potrebe države ali pa potrebe domačih podjetij. Schweizer (1996, 14) navaja primer, ko je francoska DGSE[23] v 70ih in 80ih letih 20. st. vrinila agente v ameriška podjetja Texas Instruments, IBM in Corning ter ukradene informacije posredovala francoskemu podjetju Compagnie des Machines Bull. Ta in še vrsta drugih primerov kažejo na uporabo državnih obveščevalnih služb za potrebe gospodarskih družb, kar je povsem v skladu z že omenjenim prehodom iz geopolitike v geoekonomijo, kjer je boj za gospodarski uspeh in naravne vire celo med političnimi

[23] Direction Générale de la Sécurité Extérieure - Francoska zunanja obveščevalna služba.

zavezniki oster, kar ugotavlja tudi Lowenthal. "Kakorkoli, v tekmi za globalne resurse, je veliko teh (zavezniških op. M.A.) držav naših tekmecev" (Lowenthal 2000, 5).

Winkler z vidika ZDA nadaljuje zgornjo misel in podaja alarmantno stanje, s katerim (naj bi) se soočale ZDA:

> *Več kot 100 držav je vključenih v dejavnost korporativnega vohunstva proti ameriškim podjetjem. Mnoge od njih se zanašajo na neposredno pomoč njihovih obveščevalnih služb. Tuje obveščevalne službe so organizacije, ki so najbolje opremljene za infiltracijo v podjetja vseh velikosti. Vlade jih financirajo in nikoli pravno ne odgovarjajo za svoja dejanja, kar jim zagotavlja ogromna sredstva in imuniteto. Edina stvar, ki jih zadržuje, je strah pred politično zadrego njihovih voditeljev (Winkler 1997, 53).*

Vendar isti avtor (po mojem mnenju precej pristransko) predstavi še, kaj v tem kontekstu počnejo ZDA. "Za razliko od večine drugih držav, ZDA uporabljajo svoje obveščevalne službe samo za zasledovanje nacionalnih interesov. Vlada ZDA ne oskrbuje ameriških podjetij z obveščevalnimi podatki. V nekaterih primerih je FBI[24] opozorila ameriška podjetja, ko so bila očitno napadena s strani drugih držav. Toda večinoma ameriške obveščevalne službe ne vstopajo na poslovno področje" (Winkler 1997, 54).

Nekoliko posmehljivo lahko zapišem, da glede na spodnje ugotovitve Bergierja (1974, 102-103), ameriška podjetja takšne pomoči sploh ne potrebujejo.

> *Za konec tega poglavja se bomo rahlo pregrešili proti časovnemu redu in objavili seznam sredstev, ki jih uporabljajo ameriški industrialci, da pridejo do informacij o konkurenci. Ta seznam je šele 23. maja 1966 objavil doktor Worth Wade v Chemical Engineering, toda vsa ta sredstva so uporabljali v času, ki ga obravnava to poglavje,[25] in pomenijo njegov odličen povzetek. Dvajset jih je. Prvih sedem je običajnih, druga pa so zahrbtna.*

[24] Federal Bureau of Investigation - Zvezni preiskovalni biro.
[25] Obdobje med obema vojnama (1919 – 1939).

1. *Objave konkurence in povzetki pravd, do katerih se pride na običajen način;*
2. *podatki, ki jih odkrito pripovedujejo prejšnji uslužbenci tekmeca;*
3. *tržne raziskave in poročila svetov inženirjev;*
4. *finančna poročila;*
5. *sejmi, razstave in brošure konkurence;*
6. *analiza konkurenčnih izdelkov;*
7. *poročila trgovskih potnikov in nabavnih služb;*
8. *poskusi, da se najamejo tehniki, zaposleni pri konkurenci, in izpolnjevanje vprašalnikov v ta namen;*
9. *obzirno zastavljena vprašanja tehnikom, zaposlenim pri konkurenci, med tehničnimi kongresi;*
10. *neposredna tajna opazovanja;*
11. *lažne ponudbe za zaposlitev uslužbencem konkurence brez namere zaposlitve, z namenom, da iz njih izvlečemo podatke;*
12. *lažna pogajanja s konkurentom pod pretvezo, da se želi dobiti licenca za enega izmed njegovih patentov;*
13. *zaposlitev poklicnih vohunov za pridobitev podatkov;*
14. *nagovarjanje uslužbencev konkurence, naj zapuste delo z namenom, da bi od njih dobili podatke;*
15. *kršenje lastnine konkurenta;*
16. *podkupovanje nabavnih služb ali uslužbencev konkurence;*
17. *vtihotapljanje agentov med uslužbence ali tehnike konkurence;*
18. *nezakonito prisluškovanje pri konkurentu;*
19. *kraja vzorcev, listin itd.;*
20. *izsiljevanje in razna sredstva prisile.*

Seveda konkurenca počne isto.

Zanimivo je tudi vrednostno mnenje Schweizerja (1996, 12) o gospodarskem vohunstvu. "Gospodarsko vohunstvo lahko skrajno oteži trgovanje in razjeda znanstveno in tehnološko osnovo države. To je parazitsko dejanje, ki se naslanja na druge, ki vlagajo veliko časa in denarja. Uničiti nagrade tega vložka pa pomeni uničiti spodbudo za inoviranje." V popolnoma drugem, lahko rečemo razvojnem kontekstu pa industrijsko vohunstvo (ki ga v skladu z napisanim lahko razumemo v okviru

gospodarskega vohunstva – več o tem v nadaljevanju) vidi Bergier (1974, 41). "Industrijsko vohunstvo, ki so ga skoraj uradno vzpodbujali industrialci in države, je postalo pomemben dejavnik tako industrijske revolucije kakor politike v prvi polovici. XIX. stoletja."

Svete poveže gospodarsko vohunjenje z uporabo IKT in spremenjenim varnostnim okoljem, kar je, kot sem poskusil nakazati že v prejšnjih poglavjih, izrazito vplivalo na to področje.

> *Gospodarsko vohunjenje je sicer staro kot sama obveščevalna dejavnost, z uporabo IKT pa je dobilo nove dimenzije, zlasti na področju zbiranja podatkov, prav tako pa so posebej ogrožena informacijsko in tehnološko razvita podjetja kot gonilna sila razvoja novih ekonomij. Zato je sodelovanje med obveščevalnimi skupnostmi ter zasebnim sektorjem nujno in v obojestransko korist (Yannuzzi, 2000), pa naj gre tako za zahodne liberalne države na eni, kot Kitajsko na drugi strani (Mulvenon in Bickford, 1999). Spremenjeno varnostno okolje pa je drugi dejavnik, ki poleg tehnologije vpliva na nove dimenzije obveščevalne dejavnosti. Medtem ko je bila ta v preteklosti usmerjena predvsem na delovanje proti antagonističnim nasprotnikom in je bila zgolj eden izmed virov družbene moči, pa z nastankom globalne družbe in trga zlasti na obveščevalnem področju vstopamo v obdobje boja vseh proti vsem, ki se še posebej odraža ravno na gospodarskem področju. Nova svetovna ureditev je tako povzročila težnje po pridobivanju prednosti na globalnem trgu, uporaba IKT pa določa nove oblike ekonomskega in industrijskega vohunjenja (omrežno vohunjenje) (Boni in Kovacich, 2000) (Svete 2005, 195).*

Za potrebe dela bom s terminom konkurenčno vohunstvo razumel »pridobivanje podatkov o konkurenci na nezakonit način, ki ga izvaja gospodarska družba«.[26]

Nekoliko cinično lahko spremenimo Clausewitzev 6. postulat,[27] da je konkurenčno vohunstvo nadaljevanje konkurenčne obveščevalne dejavnosti z drugimi sredstvi.

[26] Znani so primeri, ko neka državna obveščevalna služba ustanovi podjetje doma ali v tujini ter preko njega izvaja svoje dejavnosti (tudi vohunjenje). Tak primer seveda spada pod termin gospodarsko vohunjenje.

Jelen (2009, 226) o konkurenčnem vohunstvu, ki ga opredeli kot ekonomsko vohunstvo zapiše kar nekaj izjemno pomembnih lastnosti te dejavnosti:

> *Do uresničenja ekonomskega vohunstva pride, ko sovpadeta poslovna potreba po občutljivih informacijah in priložnost. Zaostrovanje konkurenčnega boja vpliva na rast povpraševanja po storitvah ekonomskega vohunstva. Kjer je povpraševanje, se prej ali slej pojavi tudi ponudba. Popolne varnosti in zaščite pred temi pojavi ni. Nasprotno, s hitrim razvojem se okna priložnosti samo večajo, varnostna industrija in tehnologija pa se odzivata z zamudo. Zato je zmotno pričakovati, da se bo rast ekonomskega vohunstva ustavila. Razvoj visokih tehnologij sicer omogoča hiter napredek varnostnih rešitev, vendar pa povečuje tudi ranljivost in stopnjo tveganja.*

Kot mi je v pogovoru dejal strokovnjak za obveščevalno dejavnost (intervju), grožnja vohunjenja tako obveščevalnih služb nasproti gospodarskim družbam kot gospodarskih družb nasproti drugim gospodarskim družbam tudi v Sloveniji obstaja in je realna, pa čeprav bodo gospodarske družbe to seveda kategorično zanikale, čemur pritrjuje tudi spodnji zapis:

> *Nasprotno (od obveščevalnih služb op. M.A.) pa na podjetniškem področju želijo tisti, ki se z ukvarjajo z zasebno obveščevalno dejavnostjo, prikazati, da gre za izključno zakonite in etične oblike pridobivanja podatkov, torej vohuni tu nimajo kaj iskati. Vendar je resnica nekje vmes. Zaupni viri, ki nezakonito zbirajo podatke, so lahko podaljšek obveščevalne dejavnosti, ni pa to nujen konstitutivni element zasebne obveščevalne dejavnosti (Jelen 2009, 226).*

Zakriti sledi gospodarski družbi o njeni dejavnosti vohunjenja je razmeroma enostavno. Znani so primeri, ko gospodarske družbe takšne »umazane« posle oddajo v zunanje izvajanje, ki to preda naprej v zunanje izvajanje in tako naprej. Takšnih zadev se ne zapiše na papir ali v elektronski obliki in kmalu so sledi dobro zabrisane.

---

[27] "Vojna je politično dejanje in učinkovito politično orodje, nadaljevanje političnih odnosov z drugimi sredstvi" (Časopis za kritiko znanosti 1985, 8).

4.1.3 Razno

Ne da bi se po nepotrebnem spuščali v nadaljnje delitve vohunstva, je vseeno potrebno omeniti še kar nekaj terminov, ki se pojavljajo ob vohunstvu. Slovar slovenskega knjižnega jezika (1994, 1529) pri terminu vohunstvo navaja "gospodarsko, industrijsko, vojaško, znanstveno vohunstvo". Najdemo pa še kaj drugega. Purg omenja tudi tehnološko vohunstvo in pri tem citira Richelsona (1989 v Purg 2002, 30). "Tehnološko vohunstvo se ukvarja z zbiranjem tehnoloških podatkov v civilnem sektorju, saj ima razvoj na tem področju pogosto vojaške aplikacije. Obveščevalna dejavnost na tem področju je pomembna pri ugotavljanju potencialne vojaške sposobnosti neke države, še zlasti občutljivo je področje jedrske energije". Winkler (1997, 54) govori o korporativnem vohunstvu (ang. corporate espionage) in še kakšno vohunjenje bi se našlo.

Menim, da nadaljnje delitve, obrazložitve in definicije glede omenjenih vrst vohunstva niso potrebne in je glede na proučevano problematiko zadostno razlikovanje med terminoma gospodarsko in konkurenčno vohunstvo.

5 KONKURENČNA OBVEŠČEVALNA DEJAVNOST

V delu sem že večkrat nakazal, da obveščevalno dejavnost ne moremo več pojmovati kot izključno dejavnost državnih obveščevalnih služb. Purg (2002, 17) to opredeli zelo jasno. "Obveščevalna služba ni nujno le državni organ, saj jo razvijajo tudi razna gibanja, stranke, večji gospodarski subjekti, nedržavna združenja, večje organizacije kriminalcev ipd." Tudi Shulsky (1993, 3) ugotavlja podobno. "Ne samo vlade, ampak veliko drugih vrst organizacij deluje v okolju, ki ga označuje konkurenčni boj, zato je koncept obveščevalne dejavnosti lahko apliciran tudi na njih". Avtor pronicljivo izpostavi konkurenčni boj in danes si težko predstavljamo, kje je ta boj izrazitejši kot prav med gospodarskimi družbami.

Iz do sedaj navedenega menim, da je povsem jasno, da je potrebno obveščevalno dejavnost prepoznati kot dejavnost, ki jo uporabljajo različni subjekti, med njimi tudi gospodarske družbe. Še posebej v slovenskem jeziku je terminološka nedorečenost,

neobdelanost in netočnost kako poimenovati takšno dejavnost očitna, zato bom poskusil terminološke zagate pojasniti v naslednjem poglavju.

5.1 Opredelitev pojma

Kateri je tisti termin, s katerim lahko poimenujemo obveščevalno dejavnost gospodarskih družb? Kljub ne prav veliko strokovnim člankom ali znanstvenim monografijam v Sloveniji o tem področju pa jim je vseeno pri terminologiji skupno nekaj – to, da jim ni skupno prav veliko. Seveda to področje ni edino, ki ima težave s poimenovanjem predmeta svojega proučevanja, je pa vsekakor na tem področju to zelo očitno. Da ne bo pomote, ta pojmovna nejasnost, včasih kot dvoumnost in nekonsistentnost (pogosto celo pri istem avtorju) je opazna tudi v svetovni strokovni literaturi, težav je v Sloveniji še dodatno več zaradi prevajanja.[28]

Najenostavneje bi se bilo zadeve lotiti, ko bi definicijo obveščevalne dejavnosti (oz. eno od njih) preprosto aplicirali na in združili z definicijo gospodarske družbe kot nosilca te dejavnosti. Pa vendar se tudi tokrat najenostavnejša pot izkaže za neustrezno, napačno ter predvsem neodgovarjajočo dejanskemu stanju.[29] Dejstvo je, da se je velika večina znanstvenega proučevanja obveščevalne dejavnosti dogajala z mislijo (večinoma izključno) na obveščevalno dejavnost v sklopu države, ki jo izvajajo nacionalne obveščevalne službe[30] in bo tukaj potrebno zadevo natančneje opredeliti in upoštevati posebnosti drugačnega področja.

Terminološki problemi se pojavljajo tudi s samim prevodom ang. termina »intelligence«. Ta termin v povezavi z gospodarskimi družbami večinoma prevajajo kot poizvedovanje, obveščanje ali inteligenca.[31] Da je temu tako, je verjetno krivo zelo slabo javno mnenje in prizvok (klasične) obveščevalne dejavnosti, ki jo ljudje

[28] Če vzamemo kot tak eklatanten primer angleški termin Business Intelligence, ugotovimo, da ga avtorji prevajajo kot: Poizvedbe o poslovanju (npr.: Žaže, 2007), Poslovna obveščevalna dejavnost (npr: Črnčec 2008, Gjerek 2009), Poslovna inteligenca (npr.: družba NPS d.o.o. - http://www.nps.si/), Poslovno odločanje (družba Avtenta, http://www.avtenta.si/si/podpora-poslovanju-in-poslovnemu-odlocanju/poslovna-inteligenca/), Poslovno obveščanje (družba SRC, http://www.src.si/izobrazevanje/obvescanje/default.asp). Torej, že ko bi se strinjali o angleškem izrazu dobimo pri prevodu v slovenščino celo vrsto terminov.

[29] Glede na prebrano se z menoj ne bi strinjalo kar nekaj avtorjev.

[30] Zanimivo je dejstvo, da se izredno redko nosilce obveščevalne dejavnosti v gospodarskih družbah poimenuje s tem izrazom, kar kaže na še eno razliko med podobno (enako?) dejavnostjo, ki pa jo izvajajo različni akterji.

[31] Temu ne sledijo npr. Črnčec, Vrenko, Gjerek in tudi sam.

povezujejo predvsem z dejavnostjo obveščevalnih služb in posledično na njihovo zlorabo človekovih pravic in svoboščin.

Še večja zmeda nastane, ko bi se nekako naravno pojmovanje tega, kar želimo opisati z obveščevalno dejavnostjo gospodarskih družb, imenovalo gospodarska oz. ekonomska obveščevalna dejavnost, pa temu ni tako, saj se z gospodarsko obveščevalno dejavnostjo običajno razume delovanje nacionalnih obveščevalnih služb na gospodarskem področju in ne obveščevalne dejavnosti gospodarskih družb (pa tudi tu najdemo drugačne razlage).

Sedaj lahko pogledamo, kako se s terminologijo tega področja soočajo slovenski avtorji.

Črnčec v svoji doktorski disertaciji in iz nje izhajajoči knjigi piše, da lahko obveščevalno dejavnost v zasebnem sektorju[32] opišemo s tremi termini: konkurenčna obveščevalna dejavnost, poslovna obveščevalna dejavnost (POD) ter konkurenčno vohunstvo (Črnčec 2008, 125). Zelo zanimivo je tudi dejstvo, da nadalje Črnčec v okviru obveščevalne dejavnosti zasebnega sektorja praktično ne omenja konkurenčnega vohunstva, medtem ko KOD in POD precej natančno obdela. Tudi sam razumem obveščevalno dejavnost gospodarskih družb kot legalno dejavnost iz katere je treba izločiti vsakršne nelegalne dejavnosti, torej nedvomno tudi vohunstvo.

Dvoršak[33] (2003, 1) piše o "zbiranju podatkov, potrebnih za odločanje v gospodarstvu" in jih našteva kar v njihovem angleškem izvirniku: business, competitive in industrial intelligence ter jih s skupnim imenom poimenuje z gospodarskimi poizvedbami.

Vrenkova (1998) obveščevalno dejavnost, ki jo uporabljajo podjetja, poimenuje z ekonomsko in konkurenčno obveščevalno dejavnostjo (ang. Economic and Competitive Intelligence).

[32] Črnčec uporabi tukaj termin zasebnega sektorja, nekateri uporabljajo termin obveščevalna dejavnost v podjetjih, sam uporabljam termin gospodarske družbe. Kljub različnim pojmovanjem gre za vsebinsko podobne termine in jih lahko v tem kontekstu uporabljamo kot sopomenke.

[33] Andrej Dvoršak se tako teoretično (izredni profesor na Fakulteti za varnostne vede), kot praktično (zasebni detektiv) sooča s to tematiko.

Gjerek (2009, 44-65) kot najširši pojem uporablja termin gospodarske poizvedbe in navaja naslednje zvrsti gospodarskih poizvedb: poslovna obveščevalna dejavnost (ang. Business Intelligence), konkurenčna obveščevalna dejavnost (ang. Competitive Intelligence), industrijska obveščevalna dejavnost (ang. Industrial Intelligence), skrbno preverjanje dobrega gospodarja (ang. Due Diligence), marketinška obveščevalna dejavnost (ang. Marketing Intelligence) in socialne poizvedbe (ang. Social Intelligence).

Žaže prav tako uporablja kot najširši termin gospodarsko poizvedovanje[34] in našteva naslednje vrste gospodarskega poizvedovanja (2007, 66-79): poizvedbe o poslovanju (ang. Business Intelligence), poizvedbe o konkurenci (ang. Competitor Intelligence), pregled skrbnega gospodarja (ang. Due Diligence), poizvedbe o tehnologiji, strateške in socialne poizvedbe, poizvedbe o trgu (ang. Marketing Intelligence), defenzivno gospodarsko poizvedovanje.

Iz teh primerov lahko ugotovimo, da je en termin tisti, ki ga uporablja večina avtorjev. To je konkurenčna obveščevalna dejavnost (ang. Competitive Intelligence). Poleg tega pa se pojavljajo še poslovna obveščevalna dejavnost (ang. Business Intelligence), ekonomska in konkurenčna obveščevalna dejavnost (ang. Economic and Competitive Intelligence), industrijska obveščevalna dejavnost (ang. Industrial Intelligence), konkurenčno vohunstvo (ang. Competitive Espionage), poizvedbe o konkurenci (ang. Competitor Intelligence), pregled skrbnega gospodarja (ang. Due Diligence), poizvedbe o tehnologiji, strateške in socialne poizvedbe, poizvedbe o trgu (ang. Marketing Intelligence), defenzivno gospodarsko poizvedovanje, socialne poizvedbe (ang. Social Intelligence). In primerjal sem samo pet avtorjev!

Sam se bom osredotočil predvsem na termin KOD, ki je v Sloveniji kot primarni predmet proučevanja še dodatno prezrt, kar je glede na nekatera v delu navedena dejstva nedvomno manko.

[34] Pri obeh specialističnih nalogah (Gjerek, 2009 in Žaže, 2007) je bil somentor Andrej Dvoršak, tako da je omenjeno poimenovanje skladno z njegovim. Sam se s terminom poizvedovanje namesto obveščevalna dejavnost ne strinjam, saj je bistveno preozek pojem za to, kar sam menim, da npr. KOD vsebuje.

Črnčec (2009, 145) primerja gospodarsko, konkurenčno in obveščevalno dejavnost v pregledni tabeli (glej tabelo 5.4) iz katere lahko jasno razberemo razlike in podobnosti med tremi obveščevalnimi dejavnostmi (gospodarsko, konkurenčno in poslovno).

Tabela 5.4: Primerjava gospodarske, konkurenčne in poslovne obveščevalne dejavnosti

	Gospodarska obveščevalna dejavnost	**Konkurenčna obveščevalna dejavnost**	**Poslovna obveščevalna dejavnost**
Osnovni namen	Pridobivanje **zunanjih** podatkov	Pridobivanje **zunanjih** podatkov	Podpora **notranjim** pocesom
Starost dejavnosti	Nekaj tisočletij	Nekaj desetletij	15 let
Obveščevalni krog	DA	DA	DA
Viri in zvrsti pridobivanja podatkov	Javni in tajni viri Humint (odkriti in prikriti – vohunstvo) Vse druge zvrsti	Javni viri Humint (odkriti) Imint (delno) Geospatial Intelligence (delno)	Javni viri
Velikost strukture	Velika Praviloma sestavni del večje obveščevalne službe	Majhna Specializirano podjetje, samostojni posamezniki, Posamezniki ali majhni oddelki v podjetju	Majhna Posamezniki POD 2.0 poseben oddelek
Pomen informacijske tehnologije	Majhen, narašča	Srednje velik, narašča	Ključen
Prožnost in odzivnost na spremembe v okolju	Majna	Velika	Velika

Vir: Črnčec (2009, 145)

POD in KOD ne obsegata in vključujeta nezakonitega, prikritega pridobivanja podatkov o konkurenci, črne plati gospodarske obveščevalne dejavnosti. Nedvomno je to temna plat KOD, če se v njegovem okviru pridobiva podatke tako, za GOD pa se predvideva, da se tudi izvaja s posebnimi ukrepi. Iz prakse v javnosti razkritih primerov je znano, da tudi

podjetja drugo o drugem pridobivajo podatke nezakonito. Dejavnosti te vrste ni moč umestiti ne v POD, KOD ali GOD, zato lahko govorimo o konkurenčnem vohunstvu (Črnčec 2009, 145).

Iz tabele 5.5 pa je izredno lepo vidna umestitev teh treh obveščevalnih dejavnosti v zasebni, zasebno-javni[35] in javni sektor.

Tabela 5.5: Prekrivanje obveščevalne dejavnosti v javnem in zasebnem sektorju

Zasebni sektor	Zasebni-javni sektor	Javni sektor
Konkurenčna obveščevalna dejavnost	Gospodarska obveščevalna dejavnost	
Konkurenčno vohunstvo	Mikrogospodarska obveščevalna dejavnost (prikrito izvajanje)	Makrogospodarska obveščevalna dejavnost (prikrito in odkrito)

Vir: Črnčec (2009, 146) prirejeno po Johnson (1996)

Kot že omenjeno je stanje tega področja z izjemo (pre)obilice terminologije v Sloveniji izrazito podhranjeno, česar pa ne moremo trditi za preostali svet, kjer prednjačijo predvsem avtorji iz ZDA. Eden od dodatnih razlogov, zakaj menim, da je termin KOD ustrezno in pravilno poimenovanje, je tudi v tem, da obstaja profesionalno Združenje konkurenčnih obveščevalnih strokovnjakov (Society of Competitive Intelligence Professionals – SCIP),[36] ki je globalna organizacija strokovnjakov, ki se ukvarjajo s KOD in s KOD povezanimi disciplinami ter izdaja periodične publikacije, knjige, izvaja izobraževanja, kongrese, srečanja... Združenje je bilo ustanovljeno leta 1986 in ima približno 3000 članov v več kot 60 državah sveta (povzeto po www.scip.org ter Juhari in Stephens 2006, 74-75). Glede na povedano menim, da je primerna osnova, če navedem definicijo KOD, kot jo definira SCIP (pravzaprav kar dve):

KOD je proces spremljanja konkurenčnega okolja in analiziranja ugotovitev v kontekstu notranjih dogajanj z namenom podpore odločevalskemu procesu. KOD omogoča vodilnim v podjetjih vseh velikosti sprejemati boljše odločitve npr. o marketingu, raziskavah in razvoju ter taktike investiranja za dolgoročne

[35] Prepletanje zasebnega in javnega sektorja, bo po mojem mnenju, z vidika proučevanja obveščevalne dejavnosti vse pomembnejše, saj s seboj »prinaša« mnoge dileme in vprašanja, katerim v delu sicer deloma posvečam pozornost, vendar je (bo) to področje vredno celovitejšega pristopa.

[36] Po meni znanih in dostopnih podatkih je v tem združenju kot član samo en državljan Slovenije – avtor besedila, pred časom pa je bila članica tudi mag. Ines Vrenko Peruško.

strategije. Uspešna KOD je nadaljevalni proces, ki vključuje legalno in etično zbiranje informacij in analizo, ki se ne izogiba nezaželenim zaključkom ter nadzirana distribucija obveščevalnih podatkov odločevalcem (http://www.scip.org/content.cfm?itemnumber=2214&navItemNumber=492).

Konkurenčna obveščevalna dejavnost je sistematičen in etičen program za zbiranje, analiziranje in upravljanje s podatki, informacijami in znanjem, ki zadevajo poslovno okolje v katerem gospodarska družba posluje, in prinese konkurenčno prednost ali omogoči sprejemanje osnovanih odločitev. Temeljni namen KOD je strateško zgodnje opozarjanje (http://scip.cms-plus.com/files/Prior%20Intelligence%20Glossary%2009Jan.pdf).

V vseh definicijah in opisih SCIP je podan poseben poudarek na legalnosti in etičnosti KOD,[37] saj je ena od glavnih prizadevanj združenja dokazati razliko in ločiti to dejavnost od nelegalnih in neetičnih dejavnosti, kot je npr. vohunstvo.

V nadaljevanju navajam še nekaj definicij, ki so jih zapisali vodilni (teoretični in praktični) strokovnjaki tega področja v Sloveniji in predvsem iz tujine. Tako veliko definicij KOD podajam iz razloga, ker v slovenski literaturi tega še nisem zasledil in se mi zdi pomembno predstaviti definicije termina KOD, kot to vidijo najvidnejši teoretični in praktični strokovnjaki na svetu.

"Competitive Intelligence – CI je zbiranje informacij iz javno dostopnih virov o konkurenci, njenih namerah, ciljih, njenem trženju ipd. S pomočjo teh informacij lahko naročnik prilagaja svojo strategijo in uspešno odbija poskuse konkurence, da mu zmanjša tržno nišo ali da ga v celoti izrine z določenega tržišča" (Dvoršak 2003, 8).

"Idealno je konkurenčna obveščevalna dejavnost proces, ki se ga uporablja za odločanje od največjih strateških nivojev do taktične ravni. Proces, ki je prisoten v celotnem podjetju. Osnovo konkurenčnega obveščevalnega sistema predstavlja obveščevalni krog ..., ki se sestoji iz štirih korakov: načrtovanja in usmerjanja, zbiranja, analiziranja ter posredovanja" (Črnčec 2008, 132).

[37] Področje etičnosti in legalnosti KOD in podobnih dejavnosti v gospodarskih družbah je nedvomno predmet proučevanja, ki bi ga bilo koristno in potrebno natančno obdelati, pa zaradi omejenega prostora v pričujočem delu to puščam za druge priložnosti in/ali druge avtorje.

"KOD je sistematičen program zbiranja in analiziranja informacij o dejavnostih konkurentov in o splošnih poslovnih trendih z namenom podpirati cilje lastne družbe" (Kahaner 1996, 16).

"KOD je podobno kot gledanje ven iz vašega okna v pisarni. … S KOD prvenstveno »strmite« in delate pregled okolja, da bi ugotovili kaj dela konkurenca" (Liebowitz 2006, 53).

"KOD je tako preprosta – zbirajte, analizirajte, razvijajte in upravljajte; zbirajte ustrezne informacije in znanje, analizirajte informacije in znanje, razvijajte pristop, ki temelji na sintezi rezultatov, in upravljajte vaša pričakovanja in strategijo ter jih ustrezno prilagajajte" (Liebowitz 2006, 58).

"KOD je definirana s preoblikovanjem surovih informacij glede zunanjega konkurenčnega okolja v obveščevalne produkte, da bi s tem podpirala poslovne odločitve" (Hughes 2005, 5).

"KOD je sistematičen proces s katerim organizacije etično zbirajo in analizirajo relevantne informacije o konkurentih in konkurenčnem okolju z namenom uporabe pri odločanju in načrtovanju s ciljem izboljšati učinek. Sistematičen proces uporabljen za razvoj KOD produktov je splošno znan kot obveščevalni krog in se izvaja kot načrtovanje, zbiranje podatkov, analiza in posredovanje" (Fleisher 2004, 56).

"KOD – analiziranje informacij, ki vam omogočijo vpogled in konkurenčno prednost – je disciplina, ki se jo je moč naučiti" (Fuld 2006, 4). In še praktični nasvet za izvajalce. "Poimenujte to kakorkoli hočete, toda naredite to. Delajte pravilno in delajte dobro. To je vse, kar je v resnici pomembno. V idealnem svetu bi bil proces obveščevalne dejavnosti del in zadolžitev vsakega delovnega mesta" (Fuld 2006, 274).

"Če želijo organizacije ostati konkurenčne v svetovnem merilu, so potrebna nova orodja za odločevalski proces. Eno teh orodij, ki je kot tako mednarodno prepoznano, je KOD, ki hitro postaja bolj merilo kot izjema pri pomoči menedžmentu pri odločanju v moderni, na znanju temelječi organizaciji. Namen KOD v organizaciji je torej

podpora in svetovanje pri odločanju in dejanjih menedžmenta" (Havenga in Botha 2003, 2).

Iz te množice definicij bom oblikoval svojo definicijo, ki po mojem mnenju najceloviteje in najustrezneje opredeljuje konkurenčno obveščevalno dejavnost, kot jo razumem sam:

> *Konkurenčna obveščevalna dejavnost je legalni in etični sistematični proces spremljanja poslovnega okolja (s poudarkom na konkurentih in konkurenčnem okolju), ki kot svoje orodje uporablja obveščevalni krog in katerega končni izdelki, na podlagi katerih je mogoče sprejemati osnovane odločitve, imajo namen pridobiti konkurenčno prednost gospodarski družbi, na taktičnem ali strateškem nivoju.*

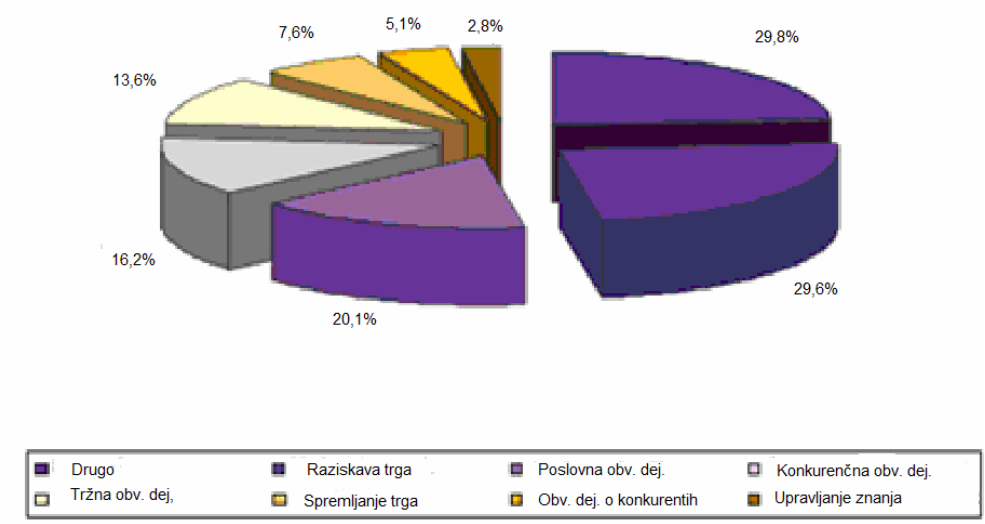
Ugotavljam precejšnje pomanjkanje empiričnih študij glede KOD v različnih državah. Eno svetlih izjem predstavlja študija »KOD v velikih družbah – globalna študija«, ki jo je spomladi leta 2005 izvedla GIA[38] v 18 državah - Avstralija, Brazilija, Kanada, Kitajska, Finska, Nemčija, Hong Kong, Indija, Japonska, Koreja, Malezija, Mehika, Nizozemska, Norveška, Singapur, Tajvan, Tajska in Švica. Študija je bila izvedena tako, da so v vseh omenjenih državah intervjuvali najvišje odgovorne za KOD v nekaterih izmed 100 največjih podjetij v posamezni državi. Tako je nastal vzorec, ki predstavlja 287 velikih podjetij (GIA White Paper 2005), kar je po mojem vedenju največji vzorec kakšne od študij glede KOD.

Zelo zanimivo z vidika terminološke opredelitve je pogledati, kako so intervjuvanci odgovarjali na sledeči dve vprašanji. Na vprašanje "Ali imate sistematično organizirano aktivnost zbiranja in analize informacij o zunanjem okolju vašega podjetja?" jih je pritrdilno odgovorilo 87% od vzorca 287 velikih podjetij. Nato je ob pritrditvi na zgornje vprašanje sledilo vprašanje, ki je ključno za poimenovanje tega področja. Vprašanje se je glasilo "kako imenujete to aktivnost?" Odgovori so bili: 29,6% raziskava trga (ang. Market Research); 20,1% poslovna obveščevalna dejavnost (ang. Business Intelligence); 16,2% konkurenčna obveščevalna dejavnost (ang. Competitive Intelligence) 13,6% tržna obveščevalna dejavnost (ang. Market

[38] Global Intelligence Alliance

Intelligence); 7,6% spremljanje trga (ang. Market Monitoring), 5,1% obveščevalna dejavnost o konkurentih (ang. Competitor Intelligence) in 2,8% upravljanje znanja (ang. Knowledge Management), kar 29,8% pa je to aktivnost poimenovalo s kakšnim drugim terminom (odgovor je bil lahko več kot en, zato je skupno več kot 100%) (GIA White Paper 2005, 7). Grafično so odgovori predstavljeni na sliki 5.5.

Slika 5.5: Terminologija konkurenčne obveščevalne dejavnosti



Vir: Prirejeno po GIA White Paper (4/2005, 7).

Pomembno je poudariti, da obstajajo glede uporabe terminologije pomembne razlike tudi med državami in regijami. V Azijsko-pacifiški regiji je najpogosteje izbran termin raziskava trga, medtem ko se na Finskem ta termin pojavi v le 8%. V Kanadi je to področje opredelilo kot KOD 50%, na Finskem le 8% (GIA White Paper 2005, 7). Zakaj je temu tako, je razvidno iz naslednjega. "Na Finskem koncept KOD v večji meri kot POD vsebuje negativno konotacijo, ki se jo celo povezuje z vohunjenjem" (Hirvensalo 2004 in Wright 2005 v Pirttimäki 2007, 146). Poslovna obveščevalna dejavnost je najpogostejši termin na Finskem 67% in na Nizozemskem (58%) (GIA White Paper 2005, 7).

Kar je delno razvidno iz zgoraj napisanega, pojasnjuje Buchda (2007, 25). "V anglosaksonski literaturi je termin KOD široko uporabljan in je pogostejši kot POD" za razliko od evropske znanstvene skupnosti.

Iz vsega navedenega postane tudi v praksi jasno, kar je moč razbrati iz zgornjih teoretičnih razprav - KOD ni splošno in globalno sprejet termin. Pojasnilo raziskovalcev omenjene študije, da so se odločili prav za ta termin pa je - "/l/ahko zaključimo, da univerzalna terminologija KOD ne obstaja in očitno prihaja do razlik med različnimi državami. Kot termin je bil KOD za potrebe te raziskave izbran, ker glede na razumevanje raziskovalcev, najbolje opisuje aktivnost, ki se je proučevala v tej študiji" (GIA White Paper 2005, 7) in podobno velja tudi v mojem primeru.

Z obrazložitvijo termina KOD, kot ga razumejo v svetu in pri nas, pa se postavlja temeljno vprašanje: zakaj bi neka gospodarska družba sploh uporabljala KOD in v razvoj lastnih KOD sposobnosti oz. za njeno zunanje izvajanje sploh investirala?

Za začetek si poglejmo, kako na to vprašanje odgovarjajo vodilni strokovnjaki KOD. Hughes (2005, 4) pri KOD izpostavlja razvoj uspešne strategije in posledično trajne konkurenčne prednosti.

> *Ključ do katerekoli uspešne strategije je zmožnost identificirati, razviti in vzdrževati konkurenčno prednost naproti konkurentom. Lahko trdimo, da je KOD vir trajne konkurenčne prednosti za podjetja, ki razvijajo te zmožnosti na dva načina. Prvi je v tem, da KOD prispeva pravočasne, relevantne in analizirane (obveščevalne) produkte, ki lahko pozitivno vplivajo na različnih stopnjah procesa oblikovanja strategije. Kot drugo, specifično znanje KOD strokovnjakov lahko pozitivno vpliva na proces razvoja strategije z zagotovitvijo, da odločevalci dobijo obveščevalne produkte in jih upoštevajo v vseh fazah procesa upravljanja strategije.*

Bernhardt (1994 v GIA White Paper 2004, 3), ki imenuje obveščevalno dejavnost »življenjska sila« strategije gre še korak naprej, ko pravi, da "strategija brez uporabe obveščevalne dejavnosti sploh ni strategija, temveč le ugibanje". Medtem, ko gre pri obveščevalni dejavnosti za »ugibati pravilno«.

Hulnick (2002, 70) izpostavlja KOD kot pomoč biti boljši od konkurenta. "Če je trg bojišče, kot trdijo nekateri teoretiki, potem bi morala KOD imeti enako vlogo v poslu,

kot jo ima v bojevanju. Morala bi biti uporabljena za spoznavanje sovražnika oz. konkurenta in biti v pomoč pri njegovem porazu."

Fuld (2006, 5) vidi KOD predvsem kot spremljanje in predvidevanje tekmecev. "KOD kot sredstvo videti preko in vnaprej hitro spreminjajočih se tekmecev je postala kritična komponenta poslovnega nabora. Moral bi biti del vsakega delovnega mesta". Podobnega mnenja je tudi Črnčec (2008, 135). "... /P/rava vrednost KOD leži v tem, da omogoči podjetju za katerega dela informacije, s pomočjo katerih lahko le-to »anticipira in prevara konkurenco« ter tako prihrani ogromno denarja."

Črnčec (2008,134) gre pri razlagi še dlje in pojasni strateško in taktično vlogo KOD:

> *V procesu konkurenčne obveščevalne dejavnosti ... se išče odgovore na strateška in taktična vprašanja. Strateška v smislu: kakšni so globalni trendi v gospodarstvu, na določenem geografskem območju, v določeni panogi? Katera podjetja so najpomembnejša za državno gospodarstvo, ali za določeno panogo ipd. Taktična vprašanja so povezana z neposrednimi interesi naročnika informacij. Iščejo se konkretne informacije o ključnih kadrih v določenih podjetjih, o njihovih prednostih in slabostih, kapitalskih in poslovnih povezavah itd.*

Strateško vlogo KOD prepoznavata tudi Fleisher in Bensoussan (2003, 4). "KOD bi morala pomagati organizaciji sprejemati uspešnejše strateške odločitve".

Kahaner (1996, 23-28) navaja, kaj lahko zmore formaliziran program KOD:

- Predvideti spremembe na trgu;
- Predvideti dejanja konkurentov;
- Odkriti nove ali potencialne konkurente;
- Učiti se iz uspehov in neuspehov drugih;
- Izboljšati prevzeme;
- Učiti se o novih tehnologijah, produktih in procesih, ki vplivajo na posel;
- Učiti se o političnih, zakonodajnih ali regulatornih spremembah, ki vplivajo na posel;
- Omogočiti vstop na nov trg;

- Omogočiti vpogled na lasten posel z »odprtim umom«;
- Pomagati implementirati nova menedžerska orodja.

Kahaner (1996, 28-31) nadaljuje še z odgovori na vprašanje, zakaj podjetja potrebujejo KOD sedaj bolj kot kadarkoli prej.[39]

- Hitrost sprememb v poslovnem svetu se vse hitreje povečuje;
- Preobilica informacij;
- Povečana globalna konkurenca;
- Obstoječa konkurenca postaja vse bolj agresivna;
- Politične spremembe ki močno in hitro vplivajo na posel;
- Hitre tehnološke spremembe.

McGonagle in Vella (2004, 68) navajata, da v primeru, da je KOD dobro uporabljena, omogoči boljše delovanje na treh področjih:

1. Pridobivanje novih poslov
2. Ohranitev obstoječih poslov
3. Izboljšanje prodajnih rezultatov in morale

Ista avtorja (prav tam) nadaljujeta, da je KOD več kot le ena izmed menedžerskih ved ali disciplin. "Je praktična, uporabna in spreminjajoča se metoda ugotavljanja kje podjetje je v poslovnem svetu in kako lahko uspešneje ter bolje obveščeno konkurira na trgu. KOD postaja vse bolj nujna, ne samo za uspeh, temveč tudi za preživetje".

5.2 Zgodovinski pregled KOD

"Obveščevalna dejavnost je stara toliko kot človeštvo …, državna obveščevalna dejavnost pa vsaj nekaj tisoč let. O začetkih sodobnih nacionalnih obveščevalnih sistemov govorimo od šestnajstega stoletja naprej, obveščevalna dejavnost v zasebnem sektorju pa je stara šele nekaj desetletij" (Črnčec 2009, 12).

[39] Čeprav gre za zapis star 14 let, menim, da zapisano še vedno velja.

Črnčec obveščevalno dejavnost v zasebnem sektorju vidi kot dejavnost staro le nekaj desetletij, nekateri drugi pa vidijo zgodovinske korenine nekaj stoletij ali celo tisočletij nazaj.

Tao in Prescott (2000 v Juhari in Stephens 2006, 65) tako celo pravita, da je KOD obveščevalna dejavnost, ki izhaja iz vojaške, gospodarske, trgovske in/ali politične obveščevalne dejavnosti, ki na Kitajskem obstaja že več kot 5.000 let.

Carr (2003, 2-3) meni, da prvi potencialni primer uporabe KOD izhaja iz 15. in 16. st. med vzponom družine Fugger, mogočne nemške trgovske in bančne družine, ki je prevladovala v takratnem evropskem poslovnem prostoru. Časopisi družine Fugger so sledili lokalne poslovne dejavnosti, poslovne rezultate, ekonomske in politične trende, ki so jih opazovali njihovi poročevalci. Te informacije so objavljali in jih pošiljali vodilnim v bankah in drugih podjetjih, ki so s temi informacijami sklepali posle, prevzemali šibke banke, vplivali na politiko in se odločali za strateške poteze. Carr (2003, 3) nadalje navaja Edwarda Lloyda, ki je ugotovil pomen čenč v kavnih hišah v Londonu. Lloyd je ustanovil časnik Lloyds List leta 1696, v katerem je zapisoval informacije o prihodih in odhodih ladij te pomembne informacije o položaju na tujem in doma. Naslednji primer avtorica (Carr 2003, 4) vidi v primeru družinske dinastije Rothschild, k je v prvi polovici 19. st. uporabljala mreže agentov in informacij pri ustvarjanju svojega imperija.

Glede starosti KOD imajo prav vsi navedeni avtorji ali pač nobeden. V modernem smislu KOD se povsem strinjam s Črnčecem, da je dejavnost stara nekaj desetletij, je pa po drugi strani tudi res, da so nekateri vidiki današnje KOD vidni že v tisočletjih prej, kar ugotavljata tudi Juhari in Stephens (2006, 76). "Glede na časovnico ima sodobna KOD, kot jo poznamo, svoj izvor v daljni preteklosti. Njena zapletena zgodovina in razvoj si je sposodila elemente in procese mnogih disciplin. Tako so lahko raziskave KOD sestavljene iz številnih zornih kotov in različnih intenzivnosti".

Ker bi podrobnejše navajanje in iskanje izvora, iz katerega jemlje sodobna KOD, bila lahko monografija sama zase in ker v tem pregledu ni možno brez poglobljene analize ugotavljati vzrokov in posledic ter ugotavljati, ali gre npr. pri nekaterih primerih za zgodovino (predvsem gospodarske) obveščevalne dejavnosti, vohunjenja

ali česa drugega, se bom raje posvetil razvoju moderne/sodobne KOD, kar ima tudi pomembnejše implikacije za sedanjost in prihodnost.

John Prescott, ki je eden najpomembnejših predstavnikov, ki tudi akademsko proučujejo KOD ter obenem eden od ustanoviteljev SCIP, razdeli razvoj KOD na tri oz. štiri faze.[40] Avtor (1999, 39-42) opisuje, da se je prva faza, ki jo poimenuje zbiranje konkurenčnih podatkov (ang. Competitive Intelligence Gathering) zgodila v 60ih in 70ih letih 20. st. in je zajemala predvsem zbiranje podatkov o konkurenci oz. konkurenčnih podatkov. Drugo fazo, ki se začne v 80ih, poimenuje analiza industrije in konkurentov (ang. Industry and Competitor Analysis). V tem obdobju se je KOD razvijala iz novo nastalega in pojavljajočega področja v hitro rastoče področje. V tem obdobju je bil močan poudarek na analizi strukture industrije in konkurentov (ang. Analysis of Industry Structure and Competitors). Tretja faza, ki se začne ob koncu 80ih let in jo poimenuje KOD v namene strateškega odločanja (ang. Competitive Intelligence for Strategic Decision Making) ima poudarek na strateških implikacijah KOD. Prihodnost oz. kot že omenjeno 4. fazo poimenuje KOD kot jedrna zmogljivost (ang. Competitive Intelligence as a Core Capability) in je opredeljena z razumevanjem KOD kot konkurenčne prednosti. Omenjene štiri faze in drugi pomembni vidiki teh obdobij so prikazani v tabeli 5.6.

Tabela 5.6: Evolucija konkurenčne obveščevalne dejavnosti

EVOLUCIJA KOD				
Obdobje	Pred 1980	1980-1987	1988-dalje	Sedanjost/prihodnost
Stopnje	Zbiranje konkurenčnih podatkov	Analiza industrije in konkurentov	KOD v namene strateškega odločanja	KOD kot jedrna zmogljivost
Ključne prelomnice	Porterjeva knjiga Competitive Strategy	Ustanovitev SCIP	Začetek izdajanja revije Competitive Intelligence Review	KOD kot predmet na poslovnih šolah po celem svetu
Lastnosti				
Stopnja formalnosti	Neformalno	Vzpostavljanje formalnih enot	Formalno	Združitev formalnega in neformalnega
Usmerjenost	Taktična	Taktična	Mešana	Strateška

[40] Članek je bil napisan leta 1999 in kar on opisuje kot stanje sedaj, lahko razumemo kot tretjo fazo, kar piše o prihodnosti lahko glede na razvoj, ki se je zgodil, pojmujemo kot sedanjost oz. 4. fazo.

Analiza	Malo ali nič	Omejeno kvantitativna	Kvantitativna in kvalitativna	Poudarek na kvalitativni
Pozornost vodilnih	Majhna	Omejena	Zmerna	Visoka
Vez z odločevalskim procesom	Majhna	Šibka	Močna	Neposreden doprinos
Položaj				
Umeščenost KOD osebja	Knjižnica / marketing	Načrtovanje / marketing	Marketing / načrtovanje / KOD enota	KOD enote /marketing / načrtovanje
Ključna vprašanja				
	Razvoj veščin za pridobivanje informacij	Ustvarjanje potrebe za KOD Videz vohunstva Razvoj analitičnih veščin	KOD na podlagi ponudbe ali povpraševanja Protiobveščevalna dejavnost Mednarodna KOD KOD tehnologija Vloga IT	Upravljanje paralelnih procesov Obveščevalna infrastruktura za multinacionalke KOD kot učenje Analiza mrež

Vir: Prirejeno po Prescott (1999, 39)

Pomembna ugotovitev avtorja je tudi, da so te faze tudi zaporedne faze sofisticiranosti KOD v današnjem času, saj večina podjetij tudi danes (torej 1999) ni prestopila druge faze razvoja tj. analize industrije in konkurentov.

Avtor navaja, kako imajo KOD organizirano vodilna podjetja tega področja in kot lahko ugotovimo, gre v tem primeru že za nekatere elemente 4. faze razvoja KOD.

> *Enota KOD je dobro razvita s formaliziranim procesom in mreženjem. Obstaja močna povezava z uporabniki obveščevalnih produktov, ki prvenstveno določajo smernice in omogočajo financiranje. Pogosto obstajajo sofisticirane metode tako kvantitativne kot kvalitativne analize. Pomemben del projektov je usmerjen v strateške odločitve. Top menedžment jasno prepoznava vrednost KOD in jo direktno povezuje v proces odločanja (Prescott 1999, 42).*

Lahko rečemo, da je bila tretja faza odločilna v razvoju KOD, kar je lepo prikazano tudi v sledečem odstavku:

Rast KOD v 90ih letih je bila hitra. Vedno več konferenc, delavnic in univerzitetnih programov namenjenih upravljanju KOD so ponujali posamezniki s pomembnim ozadjem v raziskavah in praksi KOD po celem svetu. Raziskave tega področja so postale izdatnejše in zrelejše, kar je razvidno iz izvirnih člankov, ki so se pojavljali v publikacijah kot Competitive Intelligence Review, Competitive Intelligence Magazine, AGSI Journal in Long Range Planning. Objavljenih pa je bilo tudi vedno več knjig… (Fleisher in Bensoussan 2003, xvii).

Za zgoraj zapisano Fuld (2006, 5) navaja podatek, da je bilo o KOD in/ali obveščevalni dejavnosti o konkurentih leta 1990 objavljenih 69, leta 1994 157, leta 1998 751 ter leta 2003 9.574 člankov.

Fleisher in Bensoussan (2003, 5) navajata, da je KOD prišla v ospredje približno leta 1980 in se je »napajala« iz razvoja v ekonomiji, marketingu, vojaški teoriji in strateškem menedžmentu in nadaljuje s svojim razvojem iz teh korenin v ločeno funkcijo znotraj organizacij. Nadalje trdita, da ima KOD sedaj dovolj praktične, zgodovinske in empirične podpore, da je lahko samostojna dejavnost.

KOD kot samostojno in različno disciplino vidita tudi Juhari in Stephens (2006, 78). To obrazložita s tem, da ima KOD lastno literaturo, celo vrsto različnih svetovalnih podjetij in močno profesionalno združenje – SCIP. Ugotavljata tudi, da vedno večje število univerz in drugih akademskih institucij vključuje KOD v svoje programe in raziskave.

V že omenjeni študiji GIA je bilo ugotovljeno, "da imajo velika podjetja v povprečju sistematično organizirano KOD 7 do 8 let." Povprečno je bil torej KOD vpeljan v velika podjetja z globalnim tržiščem v letih 1997 oz. 1998 (GIA White Paper 2005, 8).

Za konec tega poglavja se mi zdi poučno navesti še razmišljanje Juhari in Stephens (2006, 63), ko pravita:

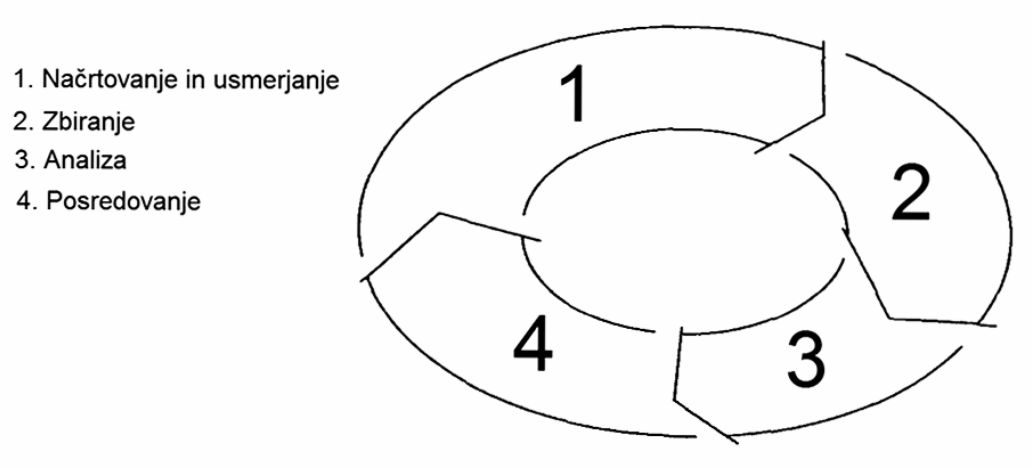
V sledenju izvora KOD je sedaj jasno, da koncept KOD ni nenadoma prišel kot učinkovito sodobno orodje strateškega delovanja organizacij. Ideja in

terminologija KOD, kot to kažejo zgodovinski pojavi po celem svetu, je prisotna veliko dlje, kot to kaže sam pojav termina, ki je bil razumljen kot obvezno delovanje ameriških organizacij, ki so želele uspeti na njihovem poslovnem področju ali v njihovih odnosih z vlado. Prvenstveno je tehnološka eksplozija 90ih let verjetno vzpodbudila, da je pojem KOD nekaj povsem novega ali celo revolucionarnega.

5.3 Obveščevalni krog KOD

V poglavju 2.2. je bil predstavljen »klasični« obveščevalni krog, ki je dodobra obdelan v literaturi, ki se ukvarja s »klasično« obveščevalno dejavnostjo. V tem poglavju pa bom predstavil poglede avtorjev KOD na obveščevalni krog, ki svoje korenine, ki jih niti ne skriva, dolguje »klasičnemu« obveščevalnemu krogu, kar ugotavlja tudi Kahaner (1996, 44) "Osnovna enota sistema KOD je obveščevalni krog. To je proces s katerim so surove informacije oblikovane v končne obveščevalne produkte. Ta proces, ki ga uporabljajo podjetja, je podoben temu, kar uporablja CIA in drugi v obveščevalni skupnosti po celem svetu". Glede na zapisano ni presenetljivo, da Kahaner kot obveščevalni krog KOD (glej sliko 5.6), dobesedno prekopira klasični štiri stopenjski obveščevalni krog; načrtovanje in usmerjanje (ang. Planning and Direction), zbiranje (ang. Collection), analiza (ang. Analysis) in posredovanje (ang. Dissemination) (Kahaner 1996, 44). Vsebina pa je seveda prilagojena področju KOD.

Slika 5.6: Obveščevalni krog KOD



Vir: Prirejeno po Kahaner (1996, 44)

1. Načrtovanje in usmerjanje

Načrtovanje in usmerjanje Kahaner (1996, 43-44) opredeli kot korak v katerem je vključen menedžment, ki odloči kakšne obveščevalne produkte potrebuje, izvajalec KOD pa se odloči po kakšni poti bo izpolnil naročeno. Obenem pa lahko razumemo ta korak tudi kot zadnji korak, saj bo končni obveščevalni produkt spodbudil nove obveščevalne potrebe.

2. Zbiranje

Ta korak vsebuje dejansko zbiranje surovih informacij[41] iz katerih bo nastal končni obveščevalni produkt. Ogromna večina je zbranega iz javnih virov, kar pomeni, da so dostopni vsem, ki vedo, kje jih iskati. Avtor nadalje navaja zelo pomembno dejstvo in sicer, da lahko kreativni posamezniki, ki zbirajo potrebne informacije le-te najdejo legalno in etično. Ta korak vključuje tudi procesiranje teh informacij z namenom, da se jih lahko prenaša in shranjuje v digitalni obliki, kar omogoči, da se jih oblikuje v obliko, ki je primerna za analizo (Kahaner 1996, 44).

3. Analiza

Običajno je ta korak najtežji del obveščevalnega kroga. Za analizo se potrebuje izjemne veščine in odločnost, saj od analitika zahteva, da tehta informacije, išče vzorce in pride do različnih scenarijev, glede na to, kaj se je naučil. Pomembna je tudi ugotovitev, da kljub temu, da je analiza postavljena na logiki in trdnih informacijah, mora analitik včasih zapolniti vrzeli in utemeljeno ugibati o mogočih rezultatih (Kahaner 1996, 44-45).

4. Posredovanje

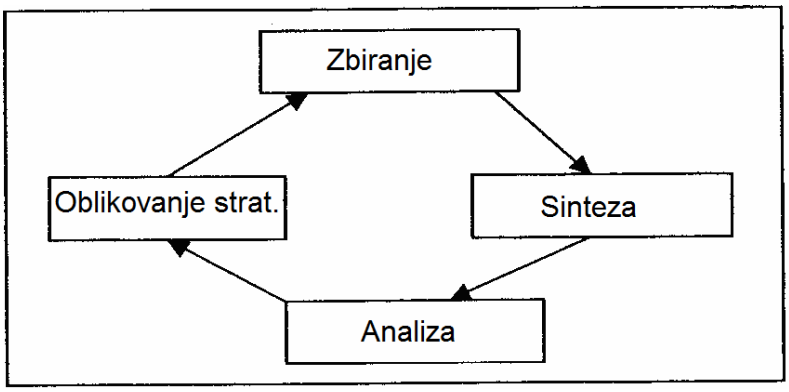
Posredovanje je tako zadnji kot tudi prvi korak in vsebuje posredovanje končnih obveščevalnih produktov tistim, ki so jih zahtevali. V tem koraku analitik tudi predlaga mogoča ukrepanja, glede na delo, ki ga je opravil prej. Mora biti sposoben artikulirati svoje predloge in jih braniti z logičnimi argumenti (Kahaner 1996, 45).

Obveščevalni krog KOD Liebowitz (2006, 60) poimenuje življenjski krog KOD in je prav tako štiri stopenjski, vendar z različnim poimenovanjem stopenj – glej sliko 5.7.

[41] V skladu z že napisanim bi bil verjetno ustreznejši termin surov podatek, saj je informacija že »obdelana« do določene mere.

Avtor (prav tam) meni, da je zbiranje[42] eden izmed pomembnih začetnih korakov v izvajanju KOD. Običajno zbiranje primarnih ali sekundarnih virov informacij izvaja strokovnjak KOD. Druga stopnja je sinteza (ang. synthesize), ki zbrane informacije »prečisti« v obvladljive dele in povzetke, vendar avtor opozarja, da to ni analiza, ki je bolj proaktivna in naprej usmerjena. Namen analize je ustvariti končne obveščevalne produkte, na podlagi katerih je moč izboljšati odločanje, kar vodi v zadnji korak – oblikovanje strategije (ang. strategize). Končni produkt KOD lahko vpliva na poslovno strategijo (tako kratko kot dolgoročno) organizacije. Ko se strategija izvaja, prihaja do novih potreb po informacijah za podporo, izboljšanje ali prilagoditev strategije organizacije s čimer se krog KOD začne znova (Liebowitz 2006, 60).

Slika 5.7: Življenjski krog KOD

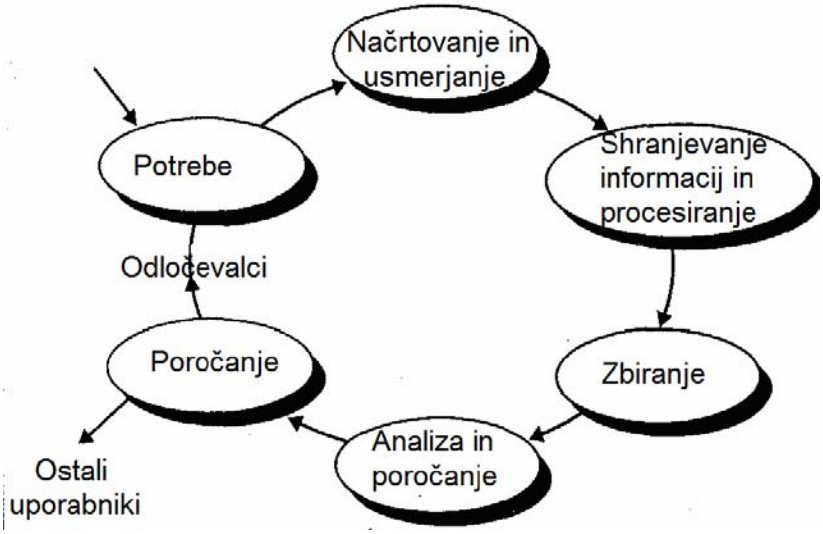


Vir: Prirejeno po Liebowitz (2006, 63).

Fleisher in Bensoussan (2003, 6) predstavljata šest stopenjski »sistematični proces oz. krog« (glej sliko 5.8). KOD obsega možne učinke (npr. nevarnosti in priložnosti), ki jih ponujajo zunanji elementi poslovnega okolja, ki vplivajo na trenutno konkurenčnost in prihodnje konkurenčne zmogljivosti organizacije. To je sistematičen proces oz. krog za zbiranje in analiziranje informacij o konkurentovih dejavnostih, poslovnem okolju in poslovnih trendih s ciljem izboljšati uspešnost organizacije.

[42] Zbiranje se nanaša na zbiranje podatkov in informacij.

Slika 5.8: Sistematični proces oz. krog KOD



Vir: Fleisher in Bensoussan 2003, 6

Kar osem stopenjski obveščevalni krog KOD pa je predstavljen pri GIA (GIA White Paper 2004, 9), a na žalost ga ne pojasnijo podrobneje ali navedejo prednosti takšne podrobnejše členitve. V zaporedju si stopnje sledijo: analiza potreb, opazovanje in spremljanje, zbiranje iz zunanjih in notranjih virov, vzpostavljanje in izločanje, analiza, posredovanje, shranjevanje, koriščenje in povratna informacija, kar je vidno tudi iz slike 5.9. Glede na navedeno lahko ugotovimo, da gre zgolj za podrobnejšo členitev nekaterih faz, kar pa za večjo jasnost samega kroga morebiti sploh ni napačno.

Slika 5.9: Osem stopenjski krog KOD

Vir: GIA White Paper (2004, 11)

Seveda ni bistvo v tem koliko stopenjski obveščevalni krog KOD kateri izmed avtorjev predstavi ali kako ta krog poimenuje, saj je v ozadju različnih prikazov in imen večinoma zelo podobna vsebina. Pomembneje je, da so te faze dobro in strokovno izpeljane, predvsem pa da je smer pravilno začrtana!

5.4 Zunanje izvajanje

Friedman (2005/2008) v svoji knjigi Izravnavanje sveta vidi oz. razlaga zunanje izvajanje kot enega izmed desetih ravnalcev sveta in povsem na mestu se postavlja vprašanje, ali je moč tudi dejavnost kot je KOD oddati v zunanje izvajanje, ali pa je potrebno zaradi specifike področja to dejavnost zagotavljati izključno znotraj gospodarske družbe.

> *Podjetja pri spremljanju informacij o konkurenci imajo na voljo dve možnosti. Lahko se odločijo, da sama zgradijo interne oddelke, ki bodo sistematično spremljali in analizirali informacije ter jih v obliki managerskih poročil ali povzetkov pošiljali avtoriziranim prejemnikom znotraj podjetij. Takšen pristop je primeren zlasti za velike organizacije, kjer so na voljo precejšnji človeški in finančni viri za vzpostavitev lastnega Business intelligence[43] oddelka ali funkcije. Izkušnje iz tujine so tudi pokazale, da takšen pristop potrebuje dalj časa preden polno zaživi, saj morajo preteči določene faze izobraževanja in urjenja uslužbencev (Vrenko Peruško 2004b).*

Črnčec (2008, 148) o dilemi zunanje izvajanje ali vzpostavitev lastnih zmogljivosti KOD pravi: "Mnenje o tem, kaj je bolje, lastna konkurenčna obveščevalna dejavnost ali zunanje pridobivanje, so deljena. Kakor so tudi argumenti za in proti" (Črnčec 2008, 148). Argumente za podaja Fiora (2002 v Črnčec 2008, 148).

> *Argumenti za zunanje pridobivanje konkurenčno obveščevalnih storitev:*
>
> - *pomanjkanje lastnega osebja;*

[43] Avtorica uporablja termina Business Intelligence in Competitive Intelligence kot sopomenki.

- *zunanje pridobivanje je bolj učinkovito pri razreševanju dveh ključnih izzivov, soočanju s prevelikim številom taktičnih ad hoc zahtev in pri lažjem komuniciranju z najvišjimi menedžerji (niso del strukture);*
- *zunanje ekipe so tudi bolj fleksibilne, prilagajajo lahko število izvajalcev neposrednim potrebam;*
- *specializirana KOD podjetja zaposlujejo vrhunske lastne strokovnjake;*
- *vzpostavitev lastne KOD ekipe v podjetju traja vsaj tri do pet let ter*
- *ekipa od zunaj lažje pridobiva informacije o neposredni konkurenci in o drugih občutljivih zadevah, ker ima zadostno distanco, prav tako se pri svojem delu sklicuje na varovanje podatkov o naročniku.*

Tudi Vrenko Peruško (2004b) opisuje primer zunanjega izvajanja zelo pozitivno.

> *V primeru outsourcinga naročnik dobi storitev izkušenega raziskovalca z dodano vrednostjo v obliki priporočil zunanjega svetovalca. Mnogokrat se takšno sodelovanje razvije po nekaj uspešnih ad hoc Business Intelligence projektih, ko naročnik pri zunanjem izvajalcu naroči raziskavo ozko definiranega vprašanja, ki se nanaša na konkurenco. Različica z outsourcingom se je v mnogih primerih pokazala kot optimalna pot za podjetja, ki jim je čas ključnega pomena ter ki ne želijo investirati v področja, ki ne sodijo v njihovo temeljno dejavnost.*

Sodba o zunanjem izvajanju KOD je prepuščena vsaki gospodarski družbi, ki želi izvajati to dejavnost, strinjati pa se je potrebno z načelnim mnenjem Črnčeca. "Samo po sebi je razumljivo in logično, da podjetja ne razvijajo lastnih zmogljivosti te vrste, če lahko po potrebi na trgu kupijo ustrezno storitev. In konkurenčna (obveščevalna op. M.A.) dejavnost ni pri tem nobena izjema" (Črnčec 2008, 149). Dodal pa bi še eno zelo pomembno dejstvo. Tudi če se neka gospodarska družba na podlagi tehtanja razlogov za in proti odloči za zunanje izvajanje KOD, je potrebno imeti vsaj do neke mere vzpostavljene zmogljivosti KOD, ki bodo spremljale področje, imele znanje, katere zunanje organizacije so sposobne zagotavljati ustrezno kakovost KOD, in predvsem bile ustrezen sogovornik znotraj družbe do zunanjega izvajalca. Sam sem glede na povedano mnenja, da v kolikor želi družba aktivno in v celoti

koristiti »ugodnosti«, ki jih (lahko) prinese KOD in tudi v primeru, da se odloči za zunanje izvajanje teh storitev, mora vseeno, vsaj do določene mere, razviti tudi notranje zmogljivosti KOD.[44]

5.5 Vohunjenje gospodarskih družb

Vohunjenje gospodarskih družb oz. konkurenčno vohunstvo[45] je bilo, je in bo predstavljajo grožnjo gospodarskim družbam. Splošno mnenje o tem, da so žrtve konkurenčnega vohunstva le velike korporacije in visokotehnološke gospodarske družbe, zanika naslednji avtor.

> *V resnici so majhna podjetja pogosteje tarča kot velike korporacije, preprosto zato, ker imajo več konkurentov. Študije kažejo, da so podjetja vseh velikosti, od več milijardnih korporacij do manjših družinskih podjetij, žrtve industrijskega vohunjenja. Nobeno podjetje ali organizacija ni imuna, da postane tarča napada, in za majhno podjetje je lahko izguba nekaj tisoč dolarjev bolj uničujoča kot izguba milijard za velika podjetja (Winkler 1997, xv).*

Zanimiva je sledeča ugotovitev. "Da postavimo stvari na svoje mesto, potrebno je poudariti da vohunjenje, ki ga lahko definiramo kot pridobivanje tajnih informacij z nelegalnimi sredstvi, predstavlja samo zelo majhen del celotnih aktivnosti zbiranja informacij korporacije, nacionalne obveščevalne službe ali države" (Jéquier in Dedijer 1987, 18). Glavna zanimivost napisanega ni v majhnem deležu, ki ga zajema vohunjenje kot aktivnost zbiranja informacij, temveč sámo dejstvo, da to počno (tudi oz. navedeno celo na prvem mestu) korporacije. Sam dodajam, da se te dejavnosti (nekatere in občasno) poslužujejo ne le korporacije, temveč tudi gospodarske družbe vseh velikosti. Kahaner (1996, 16) meni, da večina podjetij ne vstopi v ta nelegalni svet in da v resnici to niti ni potrebno, saj se da z drugimi legalnimi metodami (avtor navaja od uporabe najnovejše tehnologije, uporabe baz podatkov pa do najetja

[44] Študija takega primera, ki podpira moja razmišljanja, je podrobno opisana v Liebowitz (2006, 129-138). Na poslovnem področju, ki je zelo specifično in na njem nastopajo kot zunanji izvajalci zelo redki vrhunski strokovnjaki pa opažam še en problem – konflikt interesov. Ker je vrhunski zunanji izvajalec samo eden le-ta dela analize in svetuje konkurenčnim podjetjem celo v medsebojnih sporih.

[45] Terminologija nekaterih navajanih avtorjev v skladu z že napisanim ni enaka, vendar je vsebinsko ustrezna.

psihiatrov za izdelavo profila vodilnih) pridobiti informacije, ki se jih potrebuje. Z avtorjem se strinjam, da večina tega ne počne, pa vseeno je v javnost prišlo veliko primerov, ko se je izkazalo, da se to dogaja, kar zapiše tudi Kahaner (prav tam), ko ugotavlja, da obstajajo odkriti primeri družb, ki so prestopile mejo legalnega s krajo informacij, prisluškovanjem telefonov in vlomi v pisarne. Winkler (1997, xvi) piše da "glede na ugotovitve FBI in podobnih organizacij industrijsko vohunstvo stane družbe v ZDA od 24 do 100 milijard dolarjev letno".

Zelo odmeven primer se je zgodil v aferi med družbama Procter & Gamble (P&G) in Unilever. Jordan in Finklestein (2005) opisujeta ta primer v delu, ki nosi zelo pomenljiv naslov – Etika KOD (ang. The Ethics of Competitive Intelligence). Spomladi 2001 je John Pepper, ki je predsednik družbe P&G, razkril, da so bili člani KOD oddelka podjetja udeleženi v dejanja korporativnega vohunstva proti njihovemu glavnemu konkurentu, družbi Unilever. Ta »vohunska operacija« je zbrala okoli 80 dokumentov z načrti Unileverjevega posla s produkti za nego las. Zanimivo je predvsem, kako so prišli do teh dokumentov. P&G je najel zunanje podjetje, ki je izvajalo to operacijo.[46] Za pridobivanje dokumentov so uporabljali npr. brskanje po smeteh družbe Unilever,[47] v stikih z uslužbenci Unileverja pa so se predstavljali kot novinarji, študenti ali raziskovalci trga. Pepper in drugi vodilni so poudarjali, da njihove metode niso kršile zakonodaje ZDA, temveč so kršile njihova stroga merila poslovnega delovanja.

Posledice tega primera opisuje Boatright (2003 v Hočevar 2007, 65).

> *Aprila 2001 je podjetje Procter & Gamble odpustilo tri izvršne delavce, odgovorne za projekt, predsednik korporacije John Pepper pa je zagotovil, da informacije, pridobljene v zgoraj opisanem projektu, ne bodo uporabljene. V*

[46] Prav zanimivo, kako ta opisani primer spada v naslednje besede Winklerja (1997, 52). "Nekatere družbe se poslužujejo vprašljivih metod plačevanja zasebnih posameznikov za pridobivanje podatkov o njihovih konkurentih. Glede na besede ruskega bivšega pripadnika obveščevalne službe precej ameriških družb uporablja storitve zasebnih preiskovalcev preko tretjih oseb. Najamejo ljudi, ki najamejo ljudi, ki najamejo ljudi, ki pridobijo informacije o konkurentu na nezakonit način. Njihov namen je ločiti nelegalne dejavnosti od končnega prejemnika teh informacij. Ta Rus mi je povedal, da se takega početja poslužujejo mnoge korporacije pa tudi manjša podjetja."

[47] Varnostni menedžer, ki je bil zaposlen v eni največjih slovenskih podjetij mi je povedal, da je naročil, da mora imeti čistilka, ko čisti prostore vodilnih v družbi, ob sebi vedno varnostnika in glede na njegovo siceršnjo izredno strokovnost in izkušnje menim, da to ni počel brez razloga. Poznam tudi primer, ko je neka slovenska gospodarska družba najela detektivsko agencijo, ki je prav z brskanjem po smeteh ugotovila (oz. dokazala) nedovoljeno početje druge gospodarske družbe s katero je poslovno sodelovala.

pogajanjih, ki so sledila, je Unilever zahteval med 10 milijonov ter 20 milijonov dolarjev odškodnine zaradi morebitnih izgub, ki bi nastale zaradi neetičnega pridobivanja informacij, ter premestitev osebja z oddelka za lasno kozmetiko v korporaciji, ki bi potencialno lahko prebralo pridobljene dokumente, na takšne položaje, kjer ne bi mogli uporabiti pridobljenih informacij. Oškodovano podjetje je prav tako podalo zahtevo o oblikovanju skupine neodvisnih preiskovalcev, ki bi preučevali poslovanje oddelkov za lasno kozmetiko Procter & Gamble naslednjih nekaj let ter opozorili Unilever na vsakršno situacijo, kjer bi lahko bile uporabljene sporno pridobljene informacije.

Pomenljiva je tudi izjava Charlesa B. Straussa, direktorja Unilever ZDA, ki je izjavil: "Dosegli smo dogovor, ki zagotavlja, da so naše zaupne informacije zaščitene. S tem dogovorom smo prepričani, da P&G ne bo oviral nadaljnje rasti naših blagovnih znamk. S tem dogovorom se zaključuje ta nesrečni incident" (http://findarticles.com/p/articles/mi_m0DQA/is_2001_Sept_27/ai_79196013/).

Verjetno ni treba posebej pisati, da podrobnosti dogovora niso bile razkrite javnosti.

Opisani primer se mi zdi izredno poučen in reprezentativen, saj vključuje veliko elementov, ki sem jih opisal v prejšnjih poglavjih, kako se izvaja vohunstvo in kako se to poskuša zakriti.

Primerov konkurenčnega vohunstva je še veliko, vendar bi nadaljnje navajanje primerov preseglo namen naloge, zelo zanimiv primer pa predstavlja poskus »nekonkurenčnega vohunstva«, kot je to poimenoval Črnčec (2009, 136).

Agenti FBI so julija 2006 aretirali tri ljudi, ker so hoteli prodati poslovne skrivnosti podjetja Coke podjetju Pepsi. Ena od prijetih je administrativna pomočnica znotraj podjetja Coke. FBI se je lotil raziskave pod krinko, potem ko je podjetje Pepsi obvestilo Coke, da je dobilo pismo od nekoga znotraj podjetja Coke, ki je ponujal zelo podrobne in zaupne informacije o njihovih izdelkih v prihodnje. Podjetje Pepsi je sodelovalo pri preiskavi s kon-kurentom, saj menijo, da je konkurenca včasih neusmiljena, biti pa mora tudi

pravična in legalna (FBI: aretacije zaradi izdaje skrivnosti Coca Cole, 6. 7. 2006, siol.net v Črnčec 2009, 136).

Težko bi rekel, da je to praksa, ki se je poslužujejo družbe v takšnih primerih, vseeno pa je pokazatelj, da je tudi to možno.

5.6 Pregled KOD po izbranih državah

V tem poglavju bom na kratko predstavil stanje KOD v nekaterih vodilnih državah tega področja. Poskusil se bom omejiti zgolj na KOD v smislu moje definicije in se ne bom (pretirano) spuščal v druge dejavnosti, ki pa se jih včasih enači s KOD (npr. vohunstvo).

Skoraj kot teorija zarote se bere spodnji odstavek v katerem avtor ugotavlja, da ima

danes vsako vodilno podjetje strukture, ki so sposobne zamenjati državne institucije. Nekatere od njih, denimo Coca-Cola, Ford ali Nissan, imajo svoje podružnice v več kot 200 državah po svetu – toliko diplomatskih predstavništev nimajo niti najbogatejše države. Veliki koncerni imajo lastne socialne programe, pokojninske sklade in velikanske kadrovske službe, ki skrbijo za ustrezne življenjske razmere zaposlenih. Imajo lastne paravojaške enote za varovanje objektov, pa tudi obveščevalne službe. Po analizi ameriškega podjetja The Futures Group imajo najbolj profesionalne vohunske in protiobveščevalne strukture Microsoft, IBM, Motorola, General Electric in Coca-Cola. Na nevarnost prevlade koncernov je opozorila korejska kriza. V Južni Koreji je dejanska oblast v rokah vodij štirih velikih družb: Hyundai, Daewoo, Kia in Samsung. Ko so delovanje državnih organov podredile svojim interesom, so se te družbe rešile zunanje konkurence in tako izgubile stik s trgom, kar jih je pripeljalo do bankrota, državo pa na rob prepada (Marinković 2001, 5).

Zgornji odstavek nisem navedel zaradi poudarjanja strahu pred korporacijami in njihove moči, temveč zaradi navedbe katera podjetja imajo najbolj profesionalne

vohunske in protiobveščevalne strukture, in ni presenetljivo, da so navedene severnoameriške družbe.

Glede na proučeno literaturo in spremljanje področja KOD lahko sklepam, da je ta dejavnost najširše uporabljana v ZDA, večina vodilnih strokovnjakov KOD prihaja iz ZDA, tam pa je bilo tudi ustanovljeno združenje SCIP.

Spletna stran Marketwire (2007, http://www.marketwire.com/press-release/Corporate-Spending-on-Competitive-Intelligence-Projected-Rise-Ten-Fold-10-Billion-743788.htm) poroča,[48] da namerava 1.000 največjih ameriških družb povečati stroške namenjene (samo) za zaposlene in aktivnosti KOD na najmanj 10 milijard dolarjev do leta 2012. Leta 2007 pa je teh 1.000 družb samo za kadre znotraj podjetja, ki izvajajo KOD, namenilo 1 milijardo dolarjev. Farmacevtska panoga je tista, ki vlaga največ v KOD.

Če lahko verjamemo navedbam družbe Fuld & Company,[49] bo vsako izmed 1.000 največjih ameriških družb samo za lastno izvajanje KOD povprečno namenila 10 milijonov dolarjev (in to brez zunanjega izvajanja, naročnin na podatkovne baze...) na leto, kar ni več zanemarljiva številka in pomeni proračun, ki ga tudi nekatere obveščevalne službe manjših držav nimajo na voljo (če govorimo samo o stroških za zaposlene in aktivnosti).

Da je KOD dejavnost, ki se v ZDA hitro razvija, je razvidno tudi iz podatka, da je še leta 1997 imelo polno razvite zmogljivosti KOD manj kot 7% velikih ameriških družb (Kahaner 1996, 16), leta 2001 pa je delež med 500 največjimi družbami v ZDA, ki uporabljajo KOD, Miller (2001, www.infotoday.com/it2001/presentations/jmiller.ppt) ocenil na 90%.

Sheila Wright (2005, 20-27) je v svojem članku povzela in primerjala stanje KOD v sedmih evropskih državah (Finska, Nemčija, Litva, Rusija, Španija, Švedska in Velika

[48] Pri tem povzemajo študijo družbe Fuld & Company, ki so jo izvedli na vzorcu 141 korporacij.
[49] Ob tem je treba poudariti, da gre za družbo, ki je bila ob ustanovitvi leta 1979 pravzaprav prva družba namenjena KOD, njen ustanovitelj Leonard Fuld pa velja za »očeta« KOD. Družba še danes velja za eno najeminentnejših tovrstnih družb.

Britanija).[50] Izpostavil bom nekaj posebnosti KOD v navedenih državah. Na Finskem tako KOD izvajajo že od začetka 60ih let 20 st., do leta 1995 pa niso poznali družb, ki bi se ukvarjale s KOD za zunanje naročnike, kar je sedaj pogost pojav. Družba z najbolj razvito KOD je seveda Nokia. Terminološko to dejavnost opisujejo kot POD, saj ima termin KOD preveč agresiven prizvok. Tudi v Nemčiji termin KOD ni ravno priljubljen, tisk pa KOD navaja kot »nov fenomen« in »ameriško verzijo korporativnega vohunjenja«, kar pa ne pomeni, da te dejavnosti nemška podjetja ne uporabljajo, saj ima uporaba informacij o konkurenci s ciljem doseganja konkurenčne prednosti v Nemčiji dolgo tradicijo. Za Litvo je pomenila priključitev EU ugodne pogoje za razvoj KOD, saj je mednarodna konkurenca velika, negativna konotacija termina oz. dejavnosti glede na sistem, v katerem so bili dolga desetletja pa seveda ne preseneča. Formalizirani programi izobraževanja KOD so se v Litvi začeli leta 2000. Za Rusijo ni presenetljivo, da imajo skoraj vsi profesionalci, ki izvajajo KOD vojaško, obveščevalno ali policijsko preteklost. KOD sedaj uporablja širok spekter družb in zavzema svoje mesto ob bolj tradicionalnih funkcijah, kot so računovodstvo in proizvodnja. Velika podjetja prepoznavajo KOD kot nekaj več kot le poslovno vohunjenje. V Španiji KOD zavzema bolj strateško vlogo od leta 2001 naprej, številne univerze pa nudijo programe KOD, ponavadi v povezavi z marketingom in tehnologijo. Švedska je evropska država, ki ima najbolj razvito KOD, katere razvoj lahko razdelimo na naslednje faze. Pred letom 1980 je bila KOD prisotna pri večjih izvozno naravnanih podjetjih, ki so jo izvajale občasno in nestrukturirano. Podjetja, kot so Volvo, Ericsson in Tetra Pak, pa so že začela uvajati interne in centralizirane oddelke KOD. V 90ih letih se je KOD počasi širila v švedskih podjetjih in je začela biti prepoznavna kot prava profesija. V začetku 21. st. je KOD zaradi slabše ekonomske situacije nekoliko nazadovala. Kot začetnika KOD se izpostavlja že omenjenega Stevana Dedijerja, ki je v 70ih letih začel predavati obveščevalno dejavnost v poslovnem sektorju na univerzi Lund. KOD je sedaj kot predmet proučevanja prisotna na devetih švedskih univerzah, petih visokih šolah, štirih zasebnih družbah in petih vladnih institucijah. Švedsko lahko v KOD terminologiji poimenujemo »zrela« država z mnogimi izobraževanimi programi, globalnimi podjetji in kakovostnimi zunanjimi izvajalci. V Veliki Britaniji je KOD aktivno prisotna od leta 1985 in kot posebna disciplina nadaljuje z rastjo. Kar 16.500 menedžerjev je bilo prisotnih na

[50] Članek povzema študije posameznih držav objavljenih v reviji Journal of Competitive Intelligence & Management leta 2004.

izobraževanjih KOD, čeprav je tudi res, da je KOD v britanskih podjetjih prisotna predvsem na taktičnem nivoju.

Wrightova (2005, 27) o stanju KOD zaključi s sledečim:

> *Umetnost KOD ima veliko prihodnost v Evropi, čeprav pod različnimi imeni. Pravzaprav sploh ni pomembno, kako se poimenuje, samo da ima svoje mesto. Uspeh izvajalcev KOD bo prišel, ko se bodo veščine teh izvajalcev v velikih multinacionalkah širile v podjetja usmerjena na domači trg. To bi služilo kot izhodišče za nadaljnji razvoj in večje sprejemanje KOD, katere prave koristi bi bile vidne odločevalcem in delničarjem.*

Kahaner (1996, 16-17) navaja, da je imela Japonska dobro osnovane sisteme KOD od konca 2. sv. vojne dalje. Njihova sedanja infrastruktura KOD pa vključuje trgovske družbe in vladne agencije, ki imajo ljudi nastavljene po celem svetu, ki zbirajo informacije in jih posredujejo v ogromna »skladišča« na Japonsko, kjer so potem na voljo odločevalcem v družbah.

Da je zamenjavanje in/ali enačenje KOD s kakšno drugo dejavnostjo pogosto, je razvidno iz spodnjega odstavka, ki po mojem mnenju ustrezneje opredeli Japonsko po 2. sv. vojni.

> *Spomnimo se samo na Japonsko v obdobju po 2. svetovni vojni, ko je stopila na pot izjemne gospodarske moči. Ta je v veliki meri temeljila na agresivnem pridobivanju tehnološkega znanja od dotedanjih industrijskih sil. Temu bi danes lahko rekli kar ofenzivno ekonomsko vohunjenje. A v tistem času so bile obveščevalne in protiobveščevalne strukture občutljive le na vprašanja hladne vojne in se s tem problemom niso posebej ukvarjale. Japonske organizacije pa so pridobile vrhunsko organizacijsko in tehnološko znanje, ki jim ga danes zavidajo tudi najbolj razviti (Jelen 2009, 213).*

Vohunjenje japonskih družb ugotavlja tudi Winkler (1997, 66), ko pravi, da "verjetno ni države, ki bi integrirala industrijsko vohunstvo v svojo kulturo do večje mere kot Japonska".

KOD v pravem (legalnem in etičnem) smislu,[51] na primeru japonskih multinacionalk, prepoznavam v sledečem. "Na primer, Mitshubishi ima približno 13.000 zaposlenih v več kot dvesto poslovalnicah po svetu. Zberejo več kot trideset tisoč poslovnih in konkurenčnih informacij dnevno. Ti podatki so prečiščeni, analizirani in posredovani družbam v okviru podjetij Mitshubishi, ki jih uporabljajo kot strelivo v nadaljujoči globalni vojni proti konkurentom" (Kahaner 1996, 17). Navedeno je primer multinacionalke, ki se očitno izredno dobro zaveda pomena celotnega (konkurenčnega) obveščevalnega kroga in koristi, ki jih lahko prinese. Menim, da je navedeni primer v svetu velikih multinacionalnih družb bolj pravilo kot izjema.

Winkler (1997, 66) o velikih japonskih družbah pravi, da imajo celotne enote namenjene KOD, ki so odgovorne za predvidevanja o namerah konkurentov, njihovih zmogljivosti, dobičkonosnosti, proizvodnih zmožnosti, v kakšne nove smeri se podajajo in kakšne edinstvene procese so iznašli. Proučujejo vsak javno dostopen dokument o konkurentih, kar vključuje časnike, revije, letna poročila in vladne dokumente. Redno spremljajo patentne vloge in registracije blagovnih znamk. "Japonske družbe hočejo vedeti vse o svojih konkurentih" (prav tam). Zapisano bi po mojem mnenju morala upoštevati vsaka odgovorna družba, ki želi obstati na konkurenčnem trgu, paziti pa je potrebno, da se ne prestopa vsaj meje legalnosti, po možnosti tudi etičnosti.

Prostor in namen dela ne dopuščata podrobnejšega spuščanja v podrobnosti ter širjenja kroga držav, kjer je KOD razvita ali se razvija kot pomembna disciplina ali celo že kot profesija. V tem poglavju sem le zelo na kratko izpostavil nekatere države in stanje KOD v njej. Vsekakor menim, da če bi želeli proučiti najnovejše in najbolj razvito stanje KOD na svetu, bi se bilo potrebno osredotočiti na ZDA, Japonsko in Švedsko.

[51] Čeprav je glede na zgornje navedbe to težko trditi.

6 MOŽNE ZLORABE KOD S STRANI GOSPODARSKIH DRUŽB IN NADZOR NAD NJIHOVIM DELOVANJEM

Pomemben vidik proučevanja KOD predstavlja (ali bi moralo predstavljati) ugotavljanje in predstavitev možnih zlorab s strani gospodarskih družb. Ta problem sta nakazala že Šaponja (1999, 35), ki pravi "/d/andanes je pravzaprav dokaj lahko nadzirati državne obveščevalne službe. Vse težje pa bo obvladovati številne zasebne obveščevalne organizacije, v katerih so zaposleni nekdanji uslužbenci državnih obveščevalnih služb. Teh služb namreč nihče ne nadzoruje" in Črnčec (2008, 271) - "/t/rdim, da je v informacijski dobi potrebno vzpostaviti učinkovitejši sistem nadzora nad posegi v človekove pravice v zasebnem sektorju" ter še enkrat isti avtor (2009, 9), ki se mu zdi "največji izziv, s katerim se bo treba spopasti, kako nadzorovati obveščevalno dejavnost v zasebnem sektorju". Avtorja sta nedvoumno nakazala velik potencialni problem, ki je vsekakor vreden razprave. Z nakazanim pridemo do temne strani konkurenčne obveščevalne dejavnosti – uporabe oz. zlorabe KOD, ki prestopi »Rubikon« in se poda v svet vohunjenja in s tem povezanih kaznivih dejanj, ter kako, in ali sploh izvajati nadzor nad tem.

6.1 Nevarnosti in zlorabe

Pravzaprav je težko najti članek o KOD, ki ne bi izpostavljal tudi razmerja med legalno in etično (konkurenčno) obveščevalno dejavnostjo ter temno stranjo obveščevalne dejavnosti – vohunjenjem. Velikokrat se v časnikih (manj v strokovni literaturi) termina vohunjenje in KOD prepletata tako močno, da je moč ugotoviti, da ju avtorji navajajo kot sopomenki. Proti takšnemu pojmovanju KOD zelo aktivno nastopa SCIP in strokovnjaki KOD, ki ne poudarjajo samo legalnosti te dejavnosti, temveč tudi etičnost. Zavedati pa se je potrebno, da konkurenčno vohunjenje obstaja, da je poleg tega veliko sivo območje ter da obstajajo vedno večji pritiski za uspešnost gospodarskih družb, kar ob veliki konkurenci odpira vrata še malo bolj na stežaj za stranpoti KOD.

Kot zanimivost izpostavljam razpis za delovno mesto menedžerja KOD (ang. CI manager), ki ga je 13.08.2009 na spletni strani SCIP

(http://jobs.scip.org/c/job.cfm?site_id=296&jb=5828667) objavila družba Ansaldo STS USA, Inc.[52] Zahteve, ki jih je družba postavila za to delovno mesto so zelo visoke in zahtevne, izpostavljam najzanimivejše:

- minimalno 10-15 let izkušenj v korporativnih ali drugih okoljih KOD;
- dokazljivi uspehi pri izvabljanju nejavnih informacij in sposobnost vpogleda v še ne objavljene javne vire;
- izkušnje v profiliranju vodilnih;
- izkušnje v protiobveščevalni dejavnosti;
- pretekle izkušnje iz vojaških ali vladnih obveščevalnih služb visoko zaželene.

Glede na zahteve, ki jih je družba navedla pri iskanju menedžerja KOD, se berejo skoraj kot vohunski roman. Verjetno je, da se ta družba sooča z okoljem, kjer so ta znanja nujno potrebna, saj je vohunjenje prisotno, ali pa želi družba sama nastopati bolj agresivno. V kolikor bi bil sam vodilni v konkurenčni družbi, bi vsekakor bil pozoren na konkurenta, ki išče tak profil kadra, ki je (očitno) vešč (tudi) dejavnosti, ki segajo v polje nelegalnosti. Da se to tudi v resnici dogaja, ugotavlja naslednji avtor:

> *Predstavljali bi si, da prikrito delovanje nima mesta v zasebnem sektorju, saj taka dejanja niso le nelegalna, temveč tudi zavržna. Toda pojavljajo se dokazi, ki kažejo na to, da je prikrito delovanje uporabljano v zasebnem sektorju, ko želijo podjetja oslabiti svoje konkurente. Obstaja kar nekaj področij, kjer so bile uporabljene klasične metode prikritega delovanja v zasebnem sektorju (Hulnick 2002, 72).*

Avtor med temi spornimi metodami izpostavlja črno propagando, ki jo pogosto uporabljajo lobistične skupine ali združenja, katere vezi z njihovim naročnikom so lahko skrite; uporabo prevare, s katero se skrijejo lastne poslovne aktivnosti in se tako ukani konkurenta; dezinformacije, s katerimi se diskreditira konkurenčno podjetje ali njegove izdelke in celo sabotaže, s katerimi se poskuša onemogočiti konkurenčno podjetje. Pa četudi neka družba ne uporablja nelegalnih aktivnosti, so na voljo tehnologije, s katerimi je korak v »sivo« ali »črno« območje zelo majhen in enostaven. "Kljub temu, da izvajalci obveščevalne dejavnosti zasebnega sektorja ne smejo izvajati vohunjenja, pa imajo dostop do visokotehnoloških metod, ki so bile še

[52] Glavna dejavnost družbe je na področju železnic in množičnih prevoznih sistemov.

pred nekaj leti nedostopne. To je še posebno resnično na takšnih področjih kot je rudarjenje podatkov (ang. data mining)… Včasih strogo tajno poizvedovanje z uporabo satelitov je sedaj javno dostopno" (Hulnick 2002, 69).

Spiegel je 06.09.2008 objavil zelo zanimiv članek s pomenljivim naslovom - Temna stran moči (ang. The Dark Side of Power - German Corporate Spying Scandal Widens) avtorjev Balzli in dr. v katerem je zapisanih nekaj zanimivosti.

Avtorji trdijo, da varnostna industrija[53] (ang. security industry) še vedno deluje brez direktnega nadzora, kar se izkazuje v načinu njenega delovanja. Ugotavljajo, da npr. detektivske agencije poleg legalnih sredstev uporabljajo tudi sredstva, ki so nelegalna, kot npr. video nadzor in prisluškovanje. Navajajo primer Münchenske svetovalne družbe Corporate Trust, ki je organizirala seminarje in delavnice na teme, kot so »Uporaba prikritih preiskovalcev«,[54] »Preiskovanje zasebne sfere«, »IT forenzika za odkritje in preprečevanje nepravilnosti«, na katerih je predaval Christian Schaaf z 19-letnimi policijskimi izkušnjami. Nadalje navajajo izpostavo družbe Control Risks v Nemčiji, katere izvršni direktor je priznal, da najemajo novinarje, katerih naloga je razkriti kolege novinarje, ki pišejo kritične članke o določenih družbah[55] ali odkriti ljudi, ki v teh družbah izdajajo podatke novinarjem.

Navedeni primeri so namenjeni ilustraciji, kaj se tudi dogaja in kakšne so mogoče zlorabe in nevarnosti, ko se legalna KOD nadaljuje z nelegalnimi in/ali neetičnimi sredstvi oz. načini delovanja.

Če torej obstaja zavedanje o problemu, bi moralo to sprožiti tudi reakcijo, kot to ugotavlja Jelen (2009, 242).

> *Naša domneva je, da je prav na področju ekonomskega vohunstva sivo območje, torej delež neodkritih primerov, še posebej obsežno. Drznimo si tudi trditev, da se ta oblika obveščevalne dejavnosti širi eksponentno, tako pri naraščanju števila pojavnosti, kot tudi povzročene škode (slednje morda še*

[53] Glede na vsebino članka je jasno, da gre (tudi) za področje proučevanja pričujočega dela.
[54] Ali je moč, glede na naslov delavnice, razumeti to delavnico kaj drugače, kot da gre za »učenje« nelegalnih načinov zbiranja podatkov?
[55] Seveda tistih, ki so za to najela podjetje Control Risk.

bolj). Na določeni stopnji postanejo posledice tako očitne, da sprožijo zavedanje problema, na podlagi tega pa tudi ustrezno akcijo, ki naj bi ta trend zajezila.

Ugotavljam, da posledice niso tako očitne, saj ustrezne akcije, ki bi zajezila trende zlorab (skoraj) nisem zasledil. Za tak odziv lahko štejemo sprejetje Economic Espionage Act iz leta 1996 v ZDA. "Podpis predsednika Clintona za sprejetje Economic Espionage Act je pomenil vrhunec skoraj dveletnih prizadevanj FBI in predstavnikov industrijskih združenj, zagotoviti nova pravna sredstva za preganjanje tistih, ki izvajajo gospodarsko vohunstvo s krajo poslovnih skrivnosti" (http://www.da.usda.gov/pdsd/Security%20Guide/T1threat/Legal.htm). V tem primeru je jasno, da sta tako zasebni sektor (industrijska združenja) kot organ javnega sektorja (FBI) zaznala problem, ki ga predstavlja predvsem kraja poslovnih skrivnosti, kar se je odrazilo v sprejetju zakona, ki bi tako dejavnost preprečeval, odkrival in sankcioniral. Glede na prebrano literaturo in nekatere primere pa trdim, da je bil ta odziv pozen.

Na spletni strani FBI (http://www.fbi.gov/hq/ci/economic.htm) je zapisano sledeče:

Hladne vojne ni konec, samo premaknila se je v novo območje – globalni trg. FBI ocenjuje, da so vsako leto izgubljene milijarde dolarjev, ki jih pridobijo tuji konkurenti, ki namenoma uporabljajo gospodarsko obveščevalno dejavnost v cvetočih industrijah in tehnologijah ZDA in »nabirajo« obveščevalne podatke o tehnologijah z uporabo javnih virov in tajnih podatkov, poznanih kot poslovne skrivnosti. Tuji konkurenti, ki nelegalno iščejo gospodarske obveščevalne podatke običajno delujejo na tri načine pri ustvarjanju svojih vohunskih mrež:

- *Agresivno ciljajo in rekrutirajo dovzetne ljudi (pogosto enakega nacionalnega porekla), ki delajo za ameriške družbe in raziskovalne inštitute;*
- *Rekrutirajo ljudi, ki iščejo gospodarske obveščevalne podatke preko dejavnosti, kot so podkupnine, diskretne kraje, brskanje po smeteh (v iskanju zavrženih poslovnih skrivnosti) in prisluškovanje ter*

- *Ustanovijo na prvi pogled nedolžne poslovne vezi med tujimi in ameriškimi družbami z namenom zbiranja gospodarskih obveščevalnih podatkov, ki vključujejo zaupne informacije.*

Na isti spletni strani (prav tam) nadaljujejo, da je direktor FBI Robert Mueller določil vohunjenje kot drugo prioriteto FBI (prva je seveda terorizem). Ustanovljena je tudi enota za gospodarsko vohunjenje, ki je zadolžena za zoperstavljanje grožnji gospodarskemu vohunjenju, kar vključuje razvoj izobraževanja in gradiv, sodelovanja na konferencah, obiski zasebnih družb, sodelovanje z organi pregona in obveščevalno skupnostjo ter zagotavljanja določenih tajnih in javnih predstavitev.

Leta 2006 je zanimiv članek objavil Press Millen, ki se kot odvetnik sooča s primeri, ki so predmet Economic Espionage Act - EEA. Avtor navaja, da je bilo v obdobju od 2000 do konca leta 2005 pred sodišči 34 primerov, ki so bili v sklopu EEA, od tega kar 15 v območju, ki pokriva Silikonsko dolino. Trije zanimivi primeri obsodb so bili npr., ko je bivši zaposleni prodal poslovne skrivnosti južnoafriškemu konkurentu; neki človek je bil obsojen na dve leti zapora, ker je ukradel skrivnosti podjetju Microsoft in jih poskušal prodati na internetu; vodilni v nekem kalifornijskem podjetju pa je priznal, da je iz bivše službe vzel inženirske zapiske z namenom, da mu bo to izboljšalo uspeh v novi službi. Ne glede na navedeno pa avtor navaja celo vrsto razlogov, zakaj je primerov tako malo.[56] Avtor zaključuje, da je EEA sicer močno orodje in potencialno veliko darilo za družbe, ki imajo poslovne skrivnosti, vendar še zdaleč ni v celoti izkoriščeno.

6.2 Primerjava nadzora nad obveščevalno dejavnostjo javnega sektorja in gospodarskih družb

Čeprav je naslov poglavja primerjava nadzora…, je naslov nekoliko zavajajoč, saj ugotavljam, da nadzora nad obveščevalno dejavnostjo gospodarskih družb praktično ni. Če bi izhajali iz zgoraj navedenega, očitno ta problem (še) ni tako očiten, da bi bilo potrebno izvajati nadzor nad obveščevalno dejavnostjo gospodarskih družb. Vendar

[56] Eden glavnih razlogov, kot jih navaja avtor, in sem ga prepoznal v pogovorih s strokovnjaki tudi sam, je zaskrbljenost družb, da če naznanijo krajo poslovne skrivnosti, bo ta poslovna skrivnost razkrita med raziskovanjem ali med sojenjem, seveda pa bo padla tudi »slaba luč« na takšno družbo.

si vseeno na kratko poglejmo nadzor nad obveščevalno dejavnostjo v javnem sektorju, iz česar bomo lahko podali nekatere smernice za razmišljanje tudi o nadzoru obveščevalne dejavnosti gospodarskih družb. Opozarjam pa še na protislovnost nadzora obveščevalne dejavnosti gospodarskih družb. V kolikor je izvajanje v skladu s teorijo, potrebe nadzora ni, ker gre za legalno in tudi etično dejavnost. Potreba po nadzoru se pojavi, če se zave(da)mo, da je to dejavnost pri kateri je »korak vstran« relativno enostaven, pogosto pa tudi zelo mamljiv in predvsem, da se to tudi v resnici dogaja.

Anžič (1996, 57) o nadzoru oz. nadzorstveni dejavnosti v kontekstu varnostnih služb (vendar lahko to posplošimo tudi na proučevano dejavnost) zapiše. "Nadzorstvena dejavnost je izrazita oblika državne intervencije, s katero poskuša država vzpostaviti svoj stik in vpliv na varnostne službe." Vendar je nadzorstvo lahko tudi širše, ne samo državno. Črnčec (2009, 100-101) nadzorstvo obveščevalne dejavnosti deli na institucionalno in neinstitucionalno:

> *Pomembno je poudariti razliko med institucionalnim in neinstitucionalnim nadzorstvom. V kategorijo institucionalnega nadzorstva uvrščamo:*
>
> - *politično ali parlamentarno nadzorstvo obsega od celotnega parlamenta kot institucije do specializiranih odborov in komisij za vprašanja nadzora nad službami, obrambno področje, nadzor javnih financ, itn. do preiskovalnih komisij;*
> - *strokovno nadzorstvo, različne institucije znotraj izvršne veje oblasti. Obsega več ravni intra agencijsko/službeno (notranji nadzor), intra resorno (inšpekcija, notranja revizija) ipd.;*
> - *sodno nadzorstvo (ustavna sodišča, vrhovna sodišča, preiskovalni sodnik), vključno s tožilstvom kot institucijo »nekje vmes«;*
> - *nadzor neodvisnih institucij. V posameznih državah so močne in samostojne neodvisne institucije (predstojnike ponavadi imenuje parlament), ki lahko v okviru svojih pristojnosti izvajajo nadzor nad določenimi nalogami oziroma področji dela obveščevalnih služb. Nekatere najbolj prepoznavne in s precejšnjimi pooblastili so: informacijski pooblaščenci, ki imajo možnost, da se vključijo v upravičenost zavračanja dostopa do tajnih podatkov in/ali varstva*

osebnih podatkov; ombudsmani lahko v primeru pritožb državljanov zahtevajo od obveščevalnih služb natančna pojasnila; računsko sodišče ali primerljiva institucija opravi pregled porabe finančnih sredstev obveščevalnih služb, vključno s porabo posebnih sredstev.

Neinstitucionalno nadzorstvo pa lahko razdelimo na dve skupini:

- *nadzor javnosti. Od medijev do državljanov, posebej je treba poudariti možnost uporabe instrumenta dostopa do informacij javnega značaja.*
- *državljanski nadzor. O njem govorimo takrat, ko so državljani, največkrat so to prepoznavne javne osebnosti, varnostni strokovnjaki in ljudje, ki se ukvarjajo z varovanjem človekovih pravic, imenovani v posebno telo, ki neposredno nadzoruje posege v človekove pravice državljanov ter je po svoji pojavnosti dejansko formaliziran nadzor javnosti.*

Glede položaja v Sloveniji pri nadzoru obveščevalnih služb, Črnčec (2009, 102) ugotavlja. "Kot eno od večjih demokratičnih pridobitev lahko omenimo, da ima demokratična Slovenija danes vzpostavljene vse oblike nadzora nad obveščevalnimi službami", javnega sektorja, seveda. Za izvajalce obveščevalne dejavnosti v zasebnem sektorju pa lahko le pritrdimo misli, ki jo zapiše Črnčec (2009, 103). "Način izvajanja nadzora, kot ga pozna javni[57] sektor, pa je tudi tabula rasa za obveščevalno dejavnost v zasebnem sektorju (Črnčec 2009, 103).

Institucionalni okvir formalnega nadzorstva nad ekonomskim vohunjenjem v Sloveniji obrazloži in grafično (glej tabelo 6.7) prikaže Jelen (2009, 266):

Neposredne pristojnosti za varnostno-obveščevalno delo imajo predvsem Slovenska obveščevalno-varnostna agencija in Obveščevalno-varnostna služba Ministrstva za obrambo (OVS MO), le deloma policija, eksplicitno pa ima pristojnosti na ekonomskem področju le SOVA. Vendar so njene pristojnosti v skladu z zakonodajo omejene izključno na delovanje v tujini oz. dejavnikov iz tujine (Podbregar, 2002). Z drugimi besedami to pomeni, da obveščevalno praviloma ne deluje v slovenskem poslovnem prostoru.

[57] Avtor sicer tu uporabi termin zasebni, vendar sem prepričan da gre zgolj za tiskarsko napako, saj bi bilo to vsebinsko povsem nesmiselno.

Pristojna pa je za protiobveščevalno delo. Podobne pristojnosti kot SOVA ima tudi OVS MO, vendar le v zvezi z obrambnimi vprašanji in interesi. Kadar pa gre za sum kaznivega dejanja vohunstva (in sorodnih dejanj), ki se preganjajo po uradni dolžnosti, pa gre za pristojnost Policije in sodne veje oblasti.

Tabela 6.7: Institucionalni okvir formalnega nadzorstva nad ekonomskim vohunjenjem v Sloveniji

Zakonodajna oblast	**Izvršna oblast**	**Pravosodna oblast**
Državni zbor	**Vlada RS**	**Sodišča**
Delovna telesa ▪ Komisija za nadzor nad delom varnostnih in obveščevalnih služb...	Ministrstva	Državna tožilstva
	Agencije in službe ▪ SOVA ▪ OVS MO ▪ Policija ▪ drugo	

Vir: Prirejeno po Jelen (2009, 266)

Podbregarjem (intervju) je postavil retorično vprašanje "ali je nadzor nad obveščevalno dejavnostjo gospodarskih družb sploh potreben?" in obenem dodal še eno takšno vprašanje "ali je sploh mogoče ne posegati v človekove pravice pri takšni dejavnosti?", ki implicira pritrdilni odgovor na prvo vprašanje. Na drugo vprašanje Podbregar meni, da je sicer le to možno, vendar težko in le do neke mere. Tudi neki drugi strokovnjak za obveščevalno dejavnost mi je v pogovoru izpostavil, da se bo (in se že) kot velik problem pojavlja potencialno in že obstoječe prestopanje meja legalnosti s strani gospodarskih družb. Zavedati se je v tem kontekstu potrebno, da je tehnologija danes izredno napredovala, resursi ki jih imajo na voljo npr. multinacionalke pa so v primerjavi z obveščevalnimi službami manjših držav neverjetne. Ugotovim lahko, da tehnologija obstaja in je naprodaj, nezadovoljni ali preprosto »odvečni« obveščevalci na voljo[58] za nove (bolje plačane) »izzive«, manjka torej le še namen gospodarske družbe, da se poda v kaj takega, možnost da se jih pri tem odkrije pa je po vsesplošni oceni zelo majhna. Ugotovim lahko le, da je torej verjetnost, da se kaj takega dogaja velika, torej obstaja potreba tudi po vzpostavitvi nadzorstva.

[58] "Prav tako je treba upoštevati, da se je v Sloveniji po letu 1991 upokojilo veliko število razmeroma mladih pripadnikov varnostnih in obveščevalnih služb, ki so se v pomembnem deležu vključili v hitro razvijajočo se zasebno varnostno industrijo" (Jelen 2009, 268).

Podbregar (intervju) meni, da je potrebno za funkcijo nadzorstva nad obveščevalno dejavnostjo gospodarskih družb usposobiti obstoječe mehanizme, ki že obstajajo. V ta namen bi lahko več poudarka zlorabam KOD[59] namenile institucije, ki so že tako ali tako pristojne za kaj takega – policija, obveščevalne službe, inšpekcijske službe, pooblaščenka za dostop do informacij javnega značaja, komisija za preprečevanje korupcije, detektivska zbornica… Vendar menim, da se temu področju pravzaprav sploh ne posveča pozornosti. Težko pa je trditi, da to tudi v resnici pomeni velik problem in je sploh potrebno kaj takega. Po drugi strani pa si zatiskanje oči, da se npr. vohunjenje proti slovenskim družbam s strani njihovih slovenskih in tujih konkurentov ali obveščevalnih služb tujih držav ne dogaja, bi bilo v današnjem globaliziranem in visoko konkurenčnem okolju nekoliko naivno.

Menim, da je potrebno, da se navedenim potencialnim problemom začne posvečati nekoliko več pozornosti, saj je le tako moč ugotoviti kakšno je stanje tega področja. V kolikor je stanje slabo, so potrebni seveda tudi institucionalni in zakonski odgovori. Mnenja pa sem, da zakonodaja v smislu ameriškega EEA ne bi škodila.

7 ŠTUDIJA PRIMERA – SLOVENIJA

V tem poglavju se bom posvetil Sloveniji. Na kratko o normativnem okviru in bolj podrobno o razvoju in stanju KOD v Sloveniji ter še o pridobivanju in varovanju podatkov/informacij/znanja… Še eden izmed paradoksov, ki se jim ni moč izogniti, je da pri normativnem okviru obravnavam le stranpoti KOD, medtem ko se bom pri razvoju in stanju KOD usmerjal predvsem v dejavnost, ki je tako legalna kot etična.

7.1 Normativni okvir

Kot že omenjeno, bo to poglavje namenjeno normativnemu okviru, ki »pokriva« področje nelegalnih dejavnosti, ki po mojem mnenju pri zlorabah KOD zajemajo dve glavni kategoriji, to sta vohunjenje in posegi v človekove pravice.

[59] Po mojem mnenju sta glavni dve skupini v tem kontekstu, posegi v človekove pravice in vohunjenje.

V kazenskem zakoniku (KZ-1-NPB1, v nadaljevanju KZ) najdemo termin vohunstvo v 358. členu, kjer je določeno kot:
(1) Kdor služi tuji državi ali tuji organizaciji ali njunemu agentu, tako da zbira zaupne vojaške, gospodarske ali uradne podatke ali dokumente ali ji jih sporoči ali izroči ali ji omogoči, da pride do njih, se kaznuje z zaporom od enega do osmih let.
(2) Kdor v škodo Republike Slovenije ustvari za tujo državo ali tujo organizacijo obveščevalno službo ali jo vodi, se kaznuje z zaporom od treh do petnajstih let.
(3) Kdor se vključi v tujo obveščevalno službo iz prejšnjega odstavka ali podpira njeno delo, se kaznuje z zaporom od šestih mesecev do petih let.

> *Kot vidimo, mora biti izpolnjena vrsta pogojev, da zakon prepozna v dejanju znake vohunstva. Predvsem gre za utrjeno in zelo tradicionalno pojmovanje dejanja, kjer praviloma nastopa tuja obveščevalna služba s svojo agenturo. Njegov cilj in obenem predmet kaznivega dejanja pa so zaupni vojaški, gospodarski ali uradni podatki oziroma dokumenti in njihovo razkritje ogroža nacionalnovarnostne interese Republike Slovenije. Zanimivo je, da v primeru izdaje državne tajne storilec ni kaznovan za vohunstvo, temveč za izdajo državne tajne. Obvezni konstitutivni element kaznivega dejanja vohunstva je naklep. Gre tudi za klasično obliko hudodelstva zoper državo, zato so tudi predvidene hude kazni (zapor od enega do osmih let za prvo obliko, tri leta za drugo in šest mesecev do petih let za tretjo obliko) (Jelen 2009, 208).*

Po mojem vedenju v samostojni državi Sloveniji še ni bilo primera, da bi bil kdo obsojen za kaznivo dejanje vohunstva. Kot mi je v pogovoru dejal strokovnjak za obveščevalno dejavnost (tako iz prakse kot iz teorije), odsotnost sodne prakse glede vohunjenja izhaja iz dejstva, da sta se obveščevalni službi (ki sta v realnosti edini sposobni odkriti takšno kaznivo dejanje) odločili, da bosta na svoj način reševali takšne primere. Opozarja pa na problem, ki se pojavi ob takšni praksi. V Sloveniji je uradna oseba, ki zazna kaznivo dejanje (in vohunjenje to je) dolžna naznaniti le-to organom pregona. Znašli smo se torej v situaciji, ko sta si praksa in teorija v očitni koliziji in to zakonsko pomanjkanje, ki takšne prakse v zakonih ne dopušča, v bistvu kriminalizira pripadnike obveščevalnih služb, ki delajo v interesu svoje države. Ta primer, ko sta si praksa obveščevalnih služb, ki stremi za učinkovitostjo in zakonodajne rešitve nedosledni, je še nekaj. Sklepam, da si v takšnem in podobnih

primerih vsi malo zatiskamo oči, vendar se je potrebno zavedati, da ob neurejenosti takšnih nedoslednosti lahko pride do afer in (ponovne) oslabitve zmožnosti obveščevalnih služb, ki so oz. bodo morale biti pomemben »igralec« na gospodarskem področju (tudi) Slovenije. Drugi razlog po mojem mnenju leži v dejstvu, da bi bila npr. pridobitev poslovne skrivnosti, pa čeprav pridobljena z vohunsko dejavnostjo, obravnavana npr. po 236. členu - Izdaja in neupravičena pridobitev poslovne skrivnosti.

V KZju je zgoraj navedeni člen sicer edini, ki se navezuje na termin vohunstvo, pa vendar KZ navaja še kar nekaj členov, ki jih lahko povežemo z vohunstvom in s kršitvami človekovih pravic.[60] Spodaj navedene člene sem izbral na podlagi razmisleka in proučene literature, kakšnih kaznivih dejanj bi se lahko (in za večino je tudi dokazano, da se je kaj takega že zgodilo) poslužila neka obveščevalna organizacija v gospodarski družbi:

- 137. člen: Neupravičeno prisluškovanje in zvočno snemanje;
- 138. člen: Neupravičeno slikovno snemanje;
- 139. člen: Kršitev tajnosti občil;
- 141. člen: Kršitev nedotakljivosti stanovanja;
- 143. člen: Zloraba osebnih podatkov;
- 209. člen: Poneverba in neupravičena uporaba tujega premoženja;
- 211. člen: Goljufija;
- 213. člen: Izsiljevanje;
- 221. člen: Napad na informacijski sistem;
- 228. člen: Poslovna goljufija;
- 235. člen: Ponareditev ali uničenje poslovnih listin;
- 236. člen: Izdaja in neupravičena pridobitev poslovne skrivnosti;
- 237. člen: Vdor v poslovni informacijski sistem;
- 238. člen: Zloraba notranje informacije;
- 242. člen: Nedovoljeno dajanje daril;
- 248. člen: Izdelava, pridobitev in odtujitev pripomočkov za ponarejanje;
- 251. člen: Ponarejanje listin;
- 252. člen: Posebni primeri ponarejanja listin;

[60] Pri tem se seveda osredotočam na tista kazniva dejanja, za katera menim, da so relevantna za proučevano področje.

- 259. člen: Ponareditev ali uničenje uradne listine, knjige, spisa ali arhivskega gradiva;
- 260. člen: Izdaja tajnih podatkov;
- 262. člen: Dajanje podkupnine;
- 264. člen: Dajanje daril za nezakonito posredovanje.

V ZGDju je najpomembnejše peto poglavje: Poslovna skrivnost in prepoved konkurence:

- 39. člen (pojem poslovne skrivnosti)
- 40. člen (varstvo poslovne skrivnosti)
- 41. člen (prepoved konkurence)
- 42. člen (kršitev prepovedi konkurence)

Nadaljnje naštevanje zakonov in njihovih členov, ki so relevantni, bi preseglo okvir, zato navajam sledečega avtorja, ki je za področje ekonomskega vohunstva na sledeč način združil skupine pravnih aktov:

> *Naloga, da bi na tem mestu oblikovali spisek vseh pravnih aktov, ki kakorkoli zadevajo področje ekonomskega vohunjenja, bi presegala naš namen in cilje, še zlasti, ker gre za razmeroma novo, a hitro razvijajoče področje, kjer se normativni akti hitro spreminjajo in razvijajo. Opozorili bi le na skupine pravnih aktov, ki tvorijo pravno podlago in okvir:*
>
> - *zakonski akti, ki urejujejo delovanje sistema notranje varnosti, kot ga opredeljuje Resolucija[61] (Zakon o policiji, Zakon o Slovenski obveščevalno-varnostni agenciji in podobno);*
> - *zakoni, ki urejujejo področje zasebnega varovanja;*
> - *zakoni, ki urejujejo področje informacijske varnosti;*
> - *zakonski akti, ki urejujejo poslovno skrivnost in tajne podatke (npr. Zakon o tajnih podatkih);*
> - *zakoni, ki sankcionirajo dejanja, ki jih po širšem pojmovanju povezujemo z ekonomskim vohunjenjem (v prvi vrsti Kazenski zakonik);*
> - *zakon o gospodarskih družbah in drugi zakoni;*

[61] Resolucija o strategiji nacionalne varnosti Republike Slovenije (ReSNV).

- *podzakonski akti in interne določbe o varovanju poslovnih skrivnosti (Jelen 2009, 265).*

7.2 Razvoj in praksa KOD v Sloveniji

Kot že večkrat omenjeno je proučevanje KOD (ne glede na to kako posamezen avtor poimenuje to dejavnost in ali ima v mislih celoto KOD, kot to dejavnost razumem v magistrskem delu) v Sloveniji zelo redko, pa vendar najdemo nekaj zapisov. Eden najstarejših (po mojem vedenju) je iz leta 1993:

> *Poizvedovanje za koristi podjetja je legitimni, včasih pa tudi nelegitimni (nelegalni) del iskanja inovacijskih informacij. Pri tem poslu so naša podjetja šibka. V razvitih državah nekatera podjetja najamejo posebne agencije, ki profesionalno pristopijo k pridobivanju inovacijskih informacij za interesenta. Pri nas se je ta, za podjetja koristna dejavnost, skromno (pa vendarle) začela razvijati v začetku leta 1993, ko sta se dve zasebni varnostni firmi začeli profesionalno ukvarjati s poizvedovalno dejavnostjo. Tovrstna dejavnost se v svetu kar hitro razvija, saj je znano, da so se zadnja leta celo sodobne obveščevalne in protiobveščevalne službe začele intenzivno ukvarjati z ekonomskim vohunjenjem in komercialnim poizvedovanjem za koristi nekaterih korporacij. Tudi naša podjetja se bodo morala prilagoditi tem trendom in spremljati svojo branžo in razvojno ter tržno strategijo konkurenčnih podjetij, če želijo pospešiti tehnično-tehnološki razvoj, vzpostaviti sodobni menedžment, organizacijo, logistiko in marketing. To kar nudijo razni sejmi, razstave, simpoziji, posvetovanja ipd. je vse premalo za sodobni razvoj podjetja. Ob intenzivnejšem razvoju lastnega znanja je pač nujno tudi brskanje za inovacijskimi informacijami pri nas in v tujini. Tudi tu se mora podjetje držati dopustnega tveganja, pri čemer menedžerji in poslovneži - skupaj z varnostno službo - presodijo in določijo strategijo in taktiko, tovrstnega nastopanja na trgu. Pri tem opravilu je smotrno, da pokličejo na pomoč zunanjega strokovnjaka, ki jim pomaga sestaviti ekonomsko, pravno in varnostno sprejemljiv pristop k problemu. Zunanja pomoč je potrebna zlasti takrat, ko namerava podjetje pri urejanju in vodenju intelektualne in industrijske lastnine ter poslovnih skrivnosti uporabiti*

računalniško tehnologijo in ko gre za obsežne in programsko zahtevne obdelave zbranih podatkov, informacij in dokumentov. Vendar pa je treba pri uporabi zunanje pomoči računati na tveganje, da kak del poslovne skrivnosti, skupaj z nosilcem pomoči, odide iz podjetja (Vršec 1993, 132-133).

Avtorju je treba priznati pronicljivost in zavedanje, čeprav je pričujoč odstavek nastal že pred davnimi 17 leti (seveda gledano s slovenskega vidika). Poudaril bi nekaj vidikov, ki so še posebej izstopajoči in na katere bom poskušal podati komentarje oz. odgovore v nadaljevanju z vidika današnjega časa. "Pri tem poslu so naša podjetja šibka" - če je temu še vedno tako, bom preverjal tako na podlagi treh kvantitativnih raziskav kot s pogovori z ljudmi, ki dobro poznajo to področje. "Pri nas se je ta, za podjetja koristna dejavnost, skromno (pa vendarle) začela razvijati v začetku leta 1993, ko sta se dve zasebni varnostni firmi začeli profesionalno ukvarjati s poizvedovalno dejavnostjo" - po avtorjevem mnenju, ki sicer imensko ne navaja omenjenih podjetij, so torej nekatera podjetja že leta 1993 spoznala, da je to dejavnost, ki ima tržni potencial, in jo je moč tržiti kot zunanje izvajanje. "Tudi naša podjetja se bodo morala prilagoditi tem trendom in spremljati svojo branžo in razvojno ter tržno strategijo konkurenčnih podjetij, če želijo pospešiti tehnično-tehnološki razvoj, vzpostaviti sodobni menedžment, organizacijo, logistiko in marketing". To je napotek, ki ga je (že davno) osvojila praktično vsaka večja multinacionalka in uspešno podjetje, ki deluje na trgu z močno konkurenco, ne velja pa to v enaki meri za slovenska podjetja, vsaj kolikor sem uspel pridobiti vpogled preko proučevanja literature, nekaterih raziskav in pogovorov z ljudmi, ki to področje v Sloveniji dobro poznajo tudi iz prakse.

Ines Vrenko (1998) je v svoji diplomski nalogi kot prva meni znana oseba v Sloveniji izvedla empirično raziskavo področja (poimenuje ga ekonomska in konkurenčna obveščevalna dejavnost), ki ga tudi sam proučujem v pričujočem delu. Avtorica se je odločila za vzorec 90 podjetij, ki jih je izbrala na podlagi klasifikacije iz revije Gospodarski vestnik, kjer so bili objavljeni seznami najhitreje rastočih podjetij, podjetij z največjim dobičkom in največjih izvoznikov v Sloveniji (vsi podatki so za leto 1996). Iz vsakega izmed navedenih seznamov je izbrala prvih 30 podjetij. Ker so se nekatera podjetja podvajala, je bil njen vprašalnik poslan na 85 podjetij, vrnjenih in pravilno izpolnjenih pa je bilo 30 vprašalnikov. Avtorica o raziskavi povzema sledeče:

Če na kratko povzamem v skladu z izsledki ankete se uspešna slovenska podjetja zavedajo nevarnosti konkurentov na globalizirajočem se trgu, ne zavedajo pa se (ali vsaj ne v zadostni meri), da je prav ekonomska in konkurenčna obveščevalna dejavnost način, kako izboljšati kakovost in količino informacij o okolju ter sočasno zaščititi strateške informacije podjetja pred konkurenti. Če na splošni, formalni ravni lahko govorimo vsaj o minimalni stopnji zavesti o pomenu ekonomske in konkurenčne obveščevalne dejavnosti, pa je nedvomno šibka točka podjetij iz vzorca praksa. Izkazalo se je namreč, da podjetja ne nastopajo dovolj agresivno ter da postopkov, značilnih za ekonomsko in konkurenčno obveščevalno dejavnost, ne izvajajo organizirano in dosledno, ampak v najboljšem primeru le občasno in selektivno. Nasvet, ki ga praksa in teorija ekonomske in konkurenčne obveščevalne dejavnosti podeljujeta vsem, ki želijo uspeti v vedno ostrejši konkurenci, velja tudi za slovenska podjetja. Ozaveščanje vseh zaposlenih v podjetjih in sprememba (tako organizacijska kot v obliki načina razmišljanja) njihovega odnosa do informacij o konkurentih, novih poslovnih priložnostih ali tveganjih za podjetje, postajata vedno bolj pomembni orodji za doseganje uspešnosti podjetij (Vrenko 1998, 88).

Naslednjo empirično raziskavo z naslovom »Zaščita pred business intelligence[62] v Republiki Sloveniji« tega (ali temu podobnega/sorodnega) področja je izvedel Bernardin Gjerek v svoji specialistični nalogi.

Anketa je potekala od 07.04.2008 do 07.07.2008. Vprašalnike so avtor in ostali poslali 657 podjetjem. Odgovorilo je 105 podjetij od tega 104 (15,8%) pravilno. Sodelovali so direktorji, predsedniki uprav, člani uprav ter direktorji ali vodje oddelkov. Za selekcijo podjetij so z argumentom - »/n/ajostrejši konkurenčni boji so prav v mednarodni menjavi«, uporabili podatkovno bazo slovenskih izvoznikov – SLOEXPORT. Tako so pripravili spisek in izbrali vzorec slovenskih izvoznikov (dne

[62] Avtor je resda naredil raziskavo o POD (ki tako tudi prevede ang. termin Business Intelligence, pa vendar v nadaljevanju uporablja večinoma kar angleški termin, za strokovnjaka POD pa uporabi termin gospodarski poizvedovalec - glej npr. Gjerek (2009, 121)), vendar je moč ugotoviti, da iz same definicije in uporabe termina POD v njegovem delu izhaja ugotovitev, ki velja kar za večinoma objavljenih del v Sloveniji na to oz. podobno, sorodno ali povezano tematiko, da se včasih bistveno podoben ali celo enak predmet proučevanja poimenuje različno, bistveno različen predmet proučevanja pa enako! Ker menim, da je anketa v nekaterih delih koristna za pregled stanja KOD v Sloveniji, jo tudi navajam.

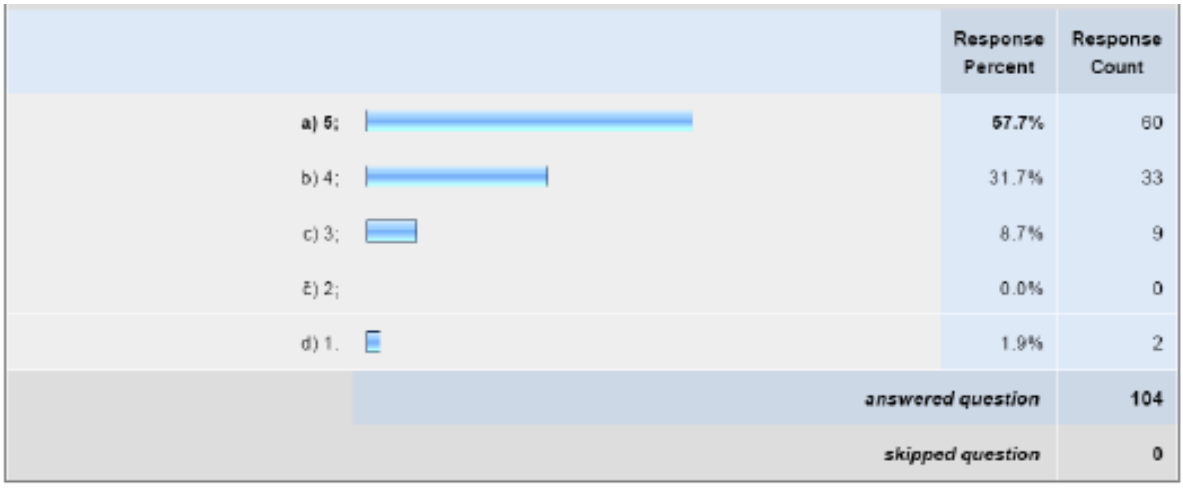
17.01.2008) po kriterijih glede na delež izvoza na celotne prihodke (51% in več) ter glede na izvor kapitala – domač (Gjerek 2009, 119-120).

Gjerek (2009, 120) ugotavlja:

> *Nastali vzorec podjetij je tako dovolj velik in raznolik: zajema namreč 104 slovenskih izvoznih podjetij različnih velikosti, osnovnih dejavnosti, prihodkov od izvoza, števila zaposlenih, let obstoja idr. … Kljub anonimnosti ankete pa obstaja potencialna nevarnost v morebitni odvisnosti odgovorov od tega, kdo od zaposlenih (direktor, drugi vodilni) je izpolnjeval vprašalnik. Velikokrat namreč vodilni v podjetju (in drugi zaposleni) ali težko priznajo pomanjkljivosti ali pa se niti ne zavedajo svoje neozaveščenosti na varnostnem področju!*

Poleg nekaterih drugih terminoloških in definicijskih zagat, pri katerih se z omenjenim avtorjem precej razlikujeva, me je pri anketi zmotilo nekaj vprašanj. Vprašanje (Gjerek 2009, 121), ki se glasi »Ali veste, kaj je poslovna špijonaža (business intelligence)?«. Iz navedenega vprašanja v anketi je namreč moč sklepati, da avtor (anketar) razume POD kot vohunstvo! Takšno sklepanje podkrepijo tudi naslednja vprašanja. Naslednje vprašanje se tako glasi »Ali je lahko nevarna?« (Gjerek 2009, 121) in še »Ali ste v podjetju sploh kdaj zaznali BI (npr. zlorabo podatkov, izdajo poslovne tajnosti)?« (Gjerek 2009, 122), ki prav tako implicirajo POD kot na nekaj nedovoljenega in v nasprotju z zakonom, čeprav avtor (Gjerek 2009, 48) pri poglavju poslovna obveščevalna dejavnost (Busines Intelligence - BI) povzema Dvoršaka (2003, 7-8) – "Razlika med business intelligence ter business espionage je v metodah, načinih in ciljih zbiranja informacij. **Prvo je zakonito, drugo pa nelegalno** (poudaril M.A.)". Na tako zastavljena vprašanja, ki sama po sebi implicirajo in navajajo na vohunstvo, so rezultati ankete, da je POD zelo nevarna, odgovori tako kar 57,7% anketirancev in da je nevarna, 31,7% anketirancev – (glej sliko 7.10). Na vprašanje »Ali veste, kaj je poslovna špijonaža (business intelligence)?«, kar 94,2% odgovorov z odgovorom DA (glej sliko 7.11), torej ogromna večina ve, kaj je poslovna špijonaža (business intelligence)?!? Možno je torej, da (skoraj) nihče ne ve kaj je POD oz. poslovna špijonaža (vohunstvo), vendar menim, da ob tako neposrečeno zastavljenem vprašanju analiza odgovorov ni smiselna.

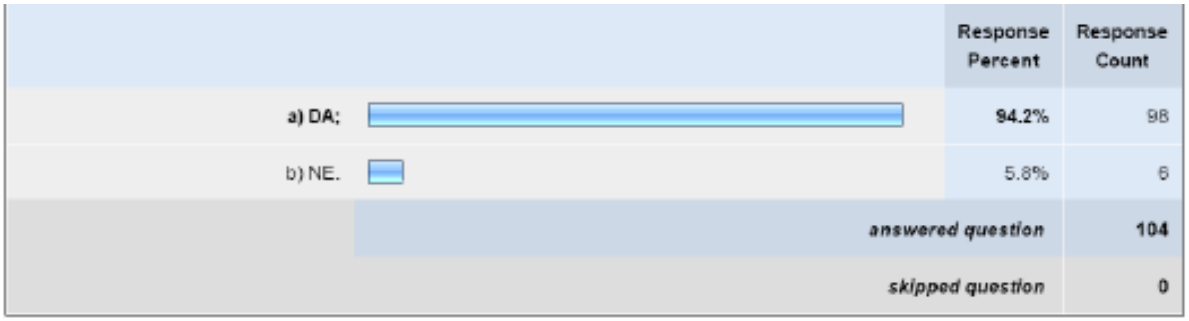
Slika 7.10: Ali je POD lahko nevarna?



	Response Percent	Response Count
a) 5;	57.7%	60
b) 4;	31.7%	33
c) 3;	8.7%	9
č) 2;	0.0%	0
d) 1.	1.9%	2
answered question		104
skipped question		0

Vir: Gjerek (2009, 149)

Slika 7.11: Ali veste kaj je poslovna špijonaža (business intelligence)?



	Response Percent	Response Count
a) DA;	94.2%	98
b) NE.	5.8%	6
answered question		104
skipped question		0

Vir: Gjerek (2009, 149)

Nekatera druga vprašanja in odgovore te raziskave predstavljam v nadaljevanju

Tretja empirična raziskava – pilotska raziskava, ki jo je izvedla družba GfK Gral-Iteo in katere ugotovitve so bile objavljene v elektronskem časopisu Relacije v članku z naslovom »Business Intelligence: oči in ušesa uspešnih podjetij« izpod peresa Ines Vrenko Peruško (Vrenko Peruško 2004a). Raziskava je potekala "preko interneta, in sicer na priložnostnem vzorcu 39 podjetij, v raziskavi pa so sodelovali vodilni kadri (direktorji, predsedniki uprav, člani uprav ter direktorji ali vodje oddelkov za marketing ali prodajo), ki naj bi imeli najboljši vpogled v dejavnosti, ki jih pri spremljanju konkurence izvajajo v podjetjih" (Vrenko Peruško 2004a).

Tudi v tej raziskavi je osrednji termin Business Intelligence, ki ga definirajo na sledeč način:

> *Na kratko lahko »business intelligence« (BI) opredelimo kot redno in sistematično zbiranje informacij o konkurenci in o poslovnem okolju, analiziranje le-teh in preoblikovanje v znanje. Na drugi, višji ravni pa je BI menedžersko orodje, ki pomaga odločevalcem sprejemati tehtne in manj tvegane odločitve. Ker najbolj prodornim podjetjem ne zadostuje le vedenje o tem, kdo so tekmeci in kaj počno danes, pač pa morajo vedeti ali vsaj predvidevati, kje bodo čez šest mesecev in kje čez pet let, je torej vloga BI še bolj strateška (Vrenko Peruško 2004a).*

Ponovno lahko ugotovimo, da je definicija POD v tem primeru v veliki meri podobna nekaterim definicijam KOD, kot sem jih navedel v poglavju 5.1.[63] Ista avtorica pa v nekem drugem članku zapiše sledeče "Business intelligence (nekateri uporabljajo tudi ime Competitive intelligence)…" (Vrenko Peruško 2004b), iz česar je razvidno zgoraj omenjeno. Nekatere ugotovitve raziskave bodo predstavljene v naslednjih poglavjih, kamor tematsko ustrezno spadajo.

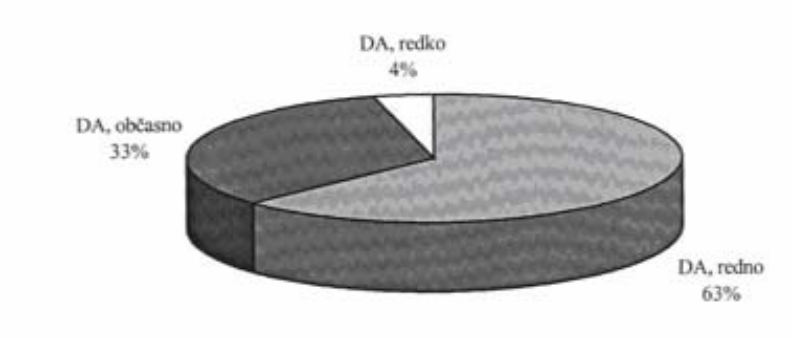
7.3 Pridobivanje

Iz zgoraj predstavljenih raziskav lahko potegnemo nekatere zaključke o tem, ali slovenska podjetja sploh pridobivajo podatke o konkurentih, poslovnem okolju, konkurenčnih priložnostih idr., ali to pridobivanje izvajajo sami ter kateri so najpogostejši in najpomembnejši viri pridobivanja podatkov.

V raziskavi Vrenkove (1998) je v kontekstu tega poglavja zelo pomembno vprašanje »Zbiranje informacij o konkurentih, poslovnih tveganjih in priložnostih za podjetje« (glej sliko 7.12).

[63] Glej npr. definicije KOD, Kahanerja, SCIP…

Slika 7.12: Zbiranje informacij o konkurentih, poslovnih tveganjih in priložnostih za podjetje



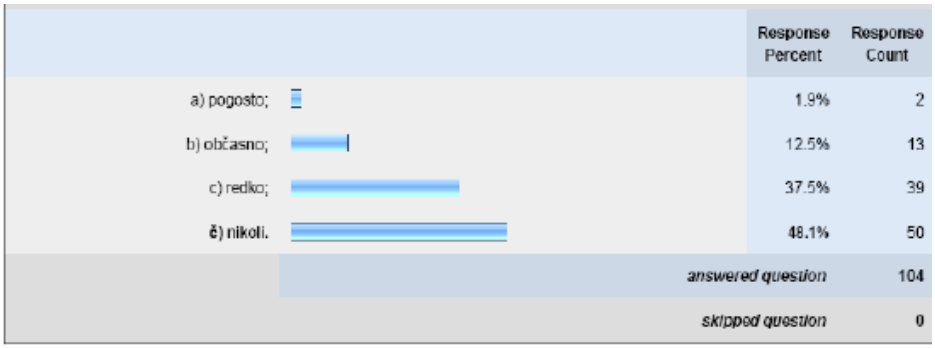
Vir: Vrenko (1998, 91)

Vrenkova (1998, 91) ugotavlja:

> *Čeprav razmeroma visok delež podjetij (63 %) iz vzorca redno zbira informacije o konkurentih, je skrb zbujajoč podatek, da takšne informacije le občasno zbira kar tretjina podjetij, 4 % podjetij pa le redko. Če omenjene podatke gledamo še v luči dejstev, da kar 70 % podjetij iz vzorca izvaža več kot 60 % izdelkov in/ali storitev … ter da so vsa podjetja ocenila, da imajo konkurente, se zdi delež tistih, ki informacije o njih zbirajo redno, še manj spodbuden.*

Iz raziskave Gjereka (2009) so pomembna predvsem sledeča vprašanja. Na vprašanje »Kako pogosto ste koristili storitve strokovnjaka za gospodarske poizvedbe?« so odgovori sledeči (glej sliko 7.13).

Slika 7.13: Kako pogosto ste koristili storitve strokovnjaka za gospodarske poizvedbe?

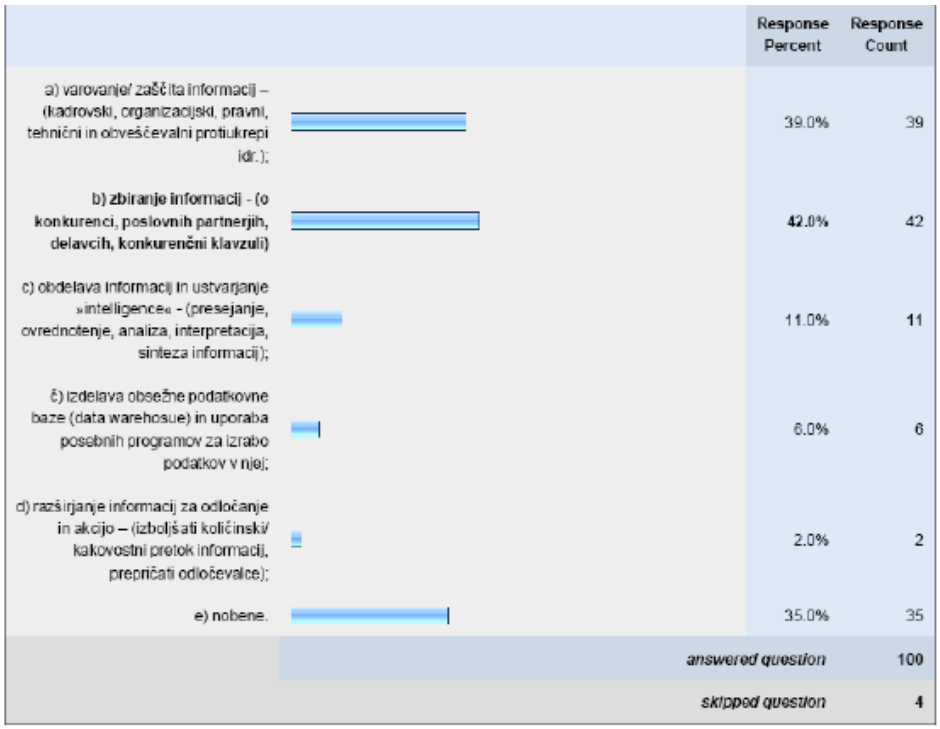


	Response Percent	Response Count
a) pogosto;	1.9%	2
b) občasno;	12.5%	13
c) redko;	37.5%	39
č) nikoli.	48.1%	50
answered question		104
skipped question		0

Vir: Gjerek (2009, 155)

Na vprašanje »Katere storitve (taktike, metodike, ukrepe) gospodarskih poizvedovalcev ste že koristili?«, ki se navezuje na zgornjega, so odgovori sledeči (glej sliko 7.14):

Slika 7.14: Katere storitve (taktike, metodike, ukrepe) gospodarskih poizvedovalcev ste že koristili?



	Response Percent	Response Count
a) varovanje/ zaščita informacij – (kadrovski, organizacijski, pravni, tehnični in obveščevalni protiukrepi idr.);	39.0%	39
b) zbiranje informacij - (o konkurenci, poslovnih partnerjih, delavcih, konkurenčni klavzuli)	42.0%	42
c) obdelava informacij in ustvarjanje »intelligence« - (presejanje, ovrednotenje, analiza, interpretacija, sinteza informacij);	11.0%	11
č) izdelava obsežne podatkovne baze (data warehosue) in uporaba posebnih programov za izrabo podatkov v njej;	6.0%	6
d) razširjanje informacij za odločanje in akcijo – (izboljšati količinski/ kakovostni pretok informacij, prepričati odločevalce);	2.0%	2
e) nobene.	35.0%	35
	answered question	100
	skipped question	4

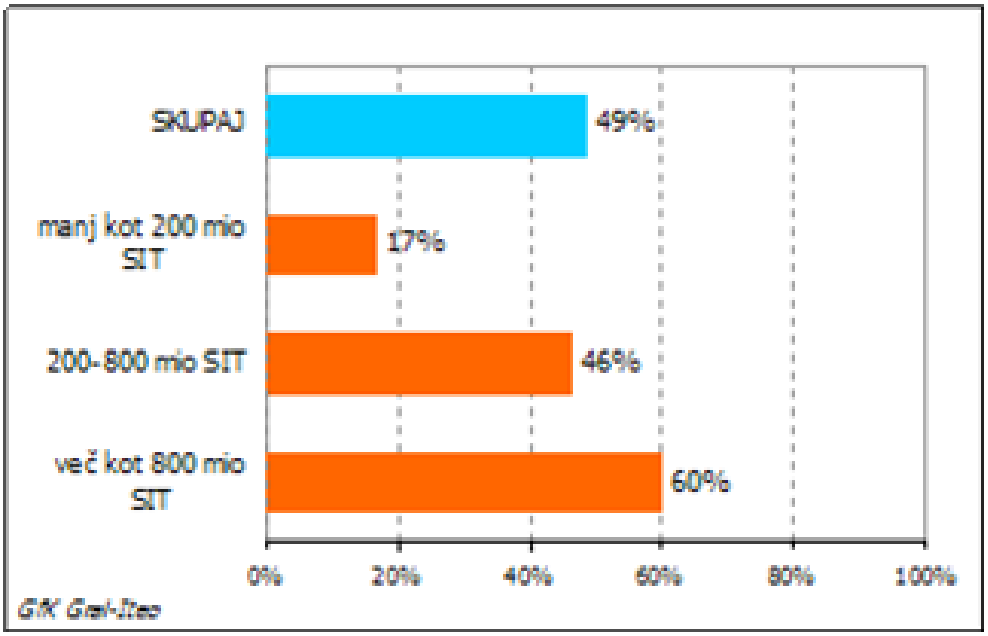
Vir: Gjerek (2009, 156)

Zgornji dve vprašanji seveda implicirata na zunanje izvajanje te dejavnosti, pa vendar sta koristni tudi v luči tega podpoglavja. Ugotovimo lahko, da zelo malo podjetij (zgolj 1,9 %) pogosto ter le 12,5 % podjetij občasno koristi storitve strokovnjaka za gospodarske poizvedbe. Naslednje vprašanje pa poda odgovore na to, katere storitve teh strokovnjakov so uporabili. Ni presenečenje, da je najpogostejši odgovor z 42 % zbiranje informacij (o konkurenci, poslovnih partnerjih, delavcih, konkurenčni klavzuli), čemur sledijo še - varovanje/zaščita informacij – (kadrovski, organizacijski, pravni, tehnični in obveščevalni protiukrepi idr.) 39 %. Drugi odgovori so bistveno manj pogosti.

Najcelovitejša raziskava, relevantna za to poglavje, je raziskava GfK (Vrenko Peruško 2004a). Najpomembnejše ugotovitve so:

Rezultati raziskave nakazujejo, da v Sloveniji po stopnji osveščenosti o potrebi po spremljanju konkurence in poslovnega okolja izstopajo večja podjetja (in sicer tako po prihodkih kot po številu zaposlenih). Kot je razvidno (glej sliko 7.15 – op. M.A.), med podjetji z več kot 800 milijoni tolarjev[64] *prihodkov v letu 2003 kar 60 odstotkov redno zbira informacije o konkurenci in o poslovnem okolju, pri podjetjih z 200*[65] *do 800 milijoni tolarjev prihodkov v letu 2003 ta delež pade na 46 %, medtem ko je v skupini podjetij z do 200 milijoni tolarjev letnih prihodkov ta delež le 17-odstoten.*

Slika 7.15: Delež podjetij, ki redno zbirajo informacije o konkurenci, glede na prihodek organizacije v letu 2003.



Vir: Vrenko Peruško (2004a)

Logično sklepanje o tem, da velikost podjetja (merjeno s prihodki) seveda vpliva na pogostost rednega zbiranja informacij o konkurenci, je z zgoraj predstavljenimi podatki potrjena. Pa vendar menim, da je odstotek (pre)nizek pri vseh treh kategorijah podjetij.

Raziskava tudi poda odgovor, kje takšne informacije zbirajo in analizirajo ter kdo so prejemniki teh informacij.

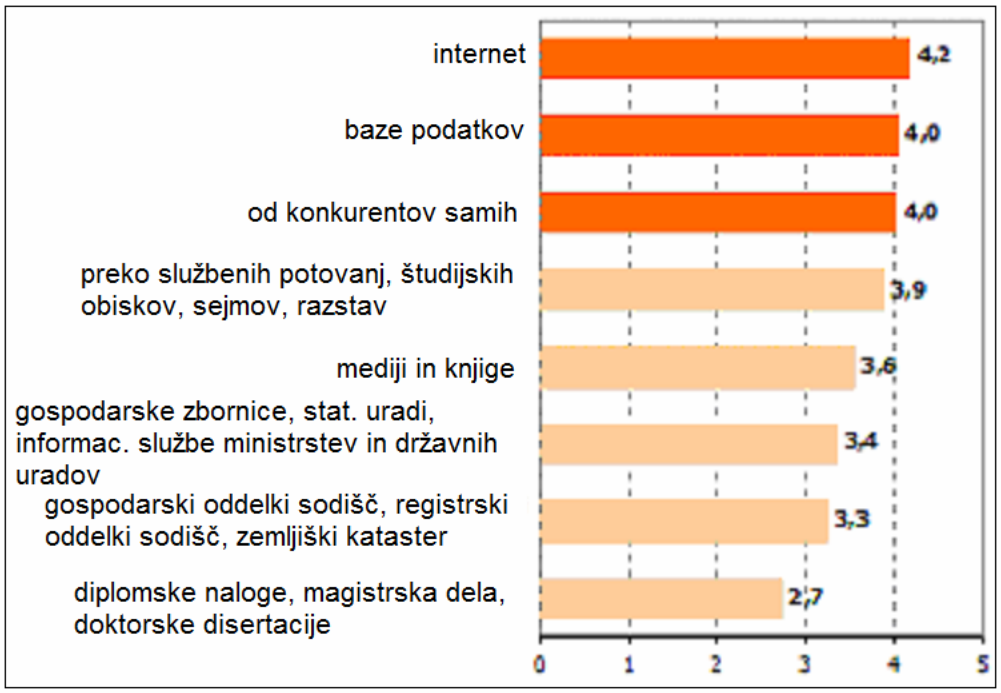
[64] 3.338.341€.
[65] 834.585€.

Rezultati raziskave kažejo, da informacije o konkurentih, poslovnem okolju ter priložnostih in tveganjih za podjetje najpogosteje zbirajo in analizirajo v oddelkih ali službah za prodajo in v marketinških oddelkih. Sledijo oddelki za tržne raziskave in službe za strateško načrtovanje ter zunanja podjetja. Vsi sodelujoči, ki so navedli, da tovrstne informacije zanje zbira zunanje podjetje, so odgovorili, da gre za tržno raziskovalno podjetje. »Business intelligence« je tudi menedžersko orodje, ki zmanjšuje tveganja odločevalcev. Podjetja, ki so sodelovala v raziskavi, so kot glavne prejemnike tovrstnih informacij navedla direktorja podjetja ali predsednika uprave, sledijo člani uprave in nato prodajni ter trženjski oddelki (Vrenko Peruško 2004a).

V prejšnjih poglavjih sem nakazal veliko pomembnost javno dostopnih podatkov za KOD in zato je zelo zanimivo pogledati, iz katerih virov podjetja pridobivajo podatke in kako pomembni za podjetje so ti viri (glej sliko 7.16):

Med javno dostopnimi viri informacij je največ podjetij navedlo, da informacije o konkurenci in poslovnem okolju dobijo iz medijev in knjig (84 %), od konkurentov samih, torej preko njihovega marketinga ali finančnih poročil, pa tudi preko dneva odprtih vrat, obiskih pri konkurentu in podobno (76 %) ali preko interneta (74 %). Sledijo različne baze podatkov, službena potovanja, študijski obiski, sejmi in razstave ter gospodarska zbornica, statistični uradi in informacijske službe državnih ustanov. Kljub temu, da so med javno dostopnimi viri informacij mediji na prvem mestu, pa je pri oceni pomembnosti posameznih virov na prvem mestu internet. Sodelujoča podjetja so ga ocenila s povprečno oceno 4,2 (na lestvici od 1 do 5, kjer 1 pomeni »sploh ni pomemben«, 5 pa »zelo pomemben vir informacij«). Po mnenju anketirancev po pomembnosti sledijo različne baze podatkov ter informacije, pridobljene od konkurentov samih.

Slika 7.16: Ocene pomembnosti javno dostopnih virov informacij o konkurenci



Vir: Vrenko Peruško (2004a)

Avtorji raziskave so ugotovili še eno zelo pomembno dejstvo:

> *Ne glede na to, ali podjetje izvaja BI ali ne, ima nedvomno neformalne poti, po katerih v podjetje pritekajo informacije o konkurenci. Zato smo sodelujoče v raziskavi vprašali, iz katerih drugih virov dobijo informacije o konkurenci in poslovnem okolju. Na prvo mesto so se uvrstili poslovni partnerji, zatem kupci in dobavitelji, nato še zaposleni v podjetju, zunanji ponudniki storitev ter zaupni viri. Čeprav podjetja največ informacij o konkurenci iz drugih virov dobijo od poslovnih partnerjev, pa so se po oceni pomembnosti posameznega vira na prvo mesto uvrstili kupci oziroma stranke, poslovni partnerji so na drugem mestu, sledijo pa zaupni viri, dobavitelji in različni zunanji ponudniki takšnih storitev.*

Iz zapisanega ugotavljam, da podjetja pridobivajo informacije tudi iz drugih virov, kot so javno dostopni viri, kar je za učinkovitost in uspešnost takšnega početja praktično nujno, vendar je potrebno paziti, da se ne prekorači legalne meje (kar bi lahko

predstavljali zaupni viri), za strokovnjaka KOD pa tudi, da ne prekorači etične in moralne meje.[66]

Vrenko Peruško (2004a) zaključi, da "/r/ezultati pilotske raziskave … kažejo, da se večja slovenska podjetja zavedajo potrebe po rednem spremljanju konkurence in poslovnega okolja" pa vendar dodaja:

> *Bolj poglobljena ocena stanja te dejavnosti v Sloveniji pa bo zahtevala še več odgovorov, in sicer na vprašanja, kako podjetja sistematično spremljajo konkurenco, ali pri tem uporabljajo uveljavljene metodologije, ali je dejavnost podprta z ustreznimi programskimi rešitvami in nenazadnje, ali se dodatno znanje in predvidevanja, ki naj bi bila rezultat sistematične dejavnosti BI, zares vpletajo v sprejete odločitve.*

Črnčec (2008, 143) navaja, da prihaja do zunanjega izvajanja KOD pri širitvi na nove trge, kar je povsem razumljivo. "V Sloveniji gospodarski subjekti največkrat pred širitvijo na nove trge zahtevajo zunanjo analizo trga ali globalno analizo. Analize izdelajo domači ali tuji strokovnjaki oz. specializirane institucije iz tujine, ki se ukvarjajo z izdelki te vrste. V praksi se tega poslužujejo na način, da pridobijo vsaj dve analizi s strani različnih institucij." Črnčec (prav tam) navaja primer podjetja Mobitel d.d. in podjetja Bados Consulting, ki je v preteklosti »buril duhove« v Sloveniji.

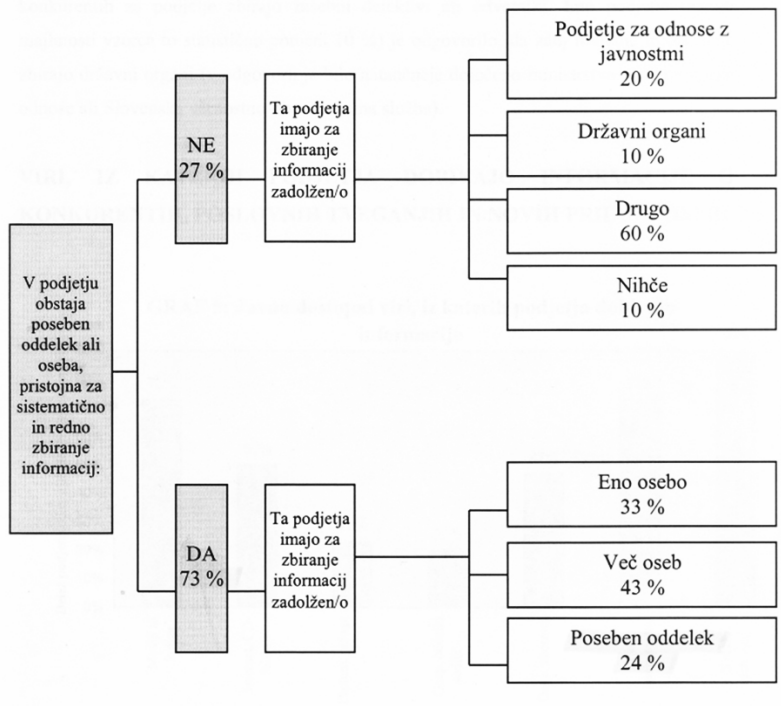
Pri vprašanju - »Organiziranost služb za sistematično in redno zbiranje informacij« (glej sliko 7.17), avtorica ugotavlja:

> *73 % podjetij iz vzorca ima poseben oddelek, osebe ali osebo, pristojno, za sistematično in redno zbiranje informacij o konkurentih. Od teh jih ima le 24 % poseben oddelek, 43 % več oseb, vendar pa je treba poudariti, da je iz natančnejših odgovorov (ki niso statistično obdelani) pri tem vprašanju razvidno, da gre večinoma za 2 ali 3 osebe. Če upoštevamo, da gre v vzorcu za kar 60 % podjetij z več kot 1000 zaposlenimi … se zdijo podatki o številu zaposlenih na področju ekonomske in konkurenčne obveščevalne dejavnosti*

[66] Verjetno nekoliko iluzorna pripomba, vendar v skladu z usmeritvami etičnega kodeksa SCIP.

še manj spodbudni. Med podjetji, ki nimajo posebnega oddelka, oseb ali osebe za zbiranje tovrstnih informacij, je kar 60 % podjetij izbralo odgovor »DRUGO«. V tej skupini pa je mogoče najti najrazličnejše odgovore, od tega, da informacije o konkurentih zbira direktor podjetja sam, pa do sodelavcev na trgih, zbiranja informacij od kupcev itd. (Vrenko 1998, 92).

Slika 7.17: Organiziranost služb za sistematično in redno zbiranje informacij



Vir: Vrenko (1998, 92)

V povezavi z zunanjim izvajanjem pa ugotavlja:

Med podjetji, ki nimajo zaposlenih za zbiranje informacij, je tudi 20 % takšnih, ki za tovrstne naloge najemajo zunanje ponudnike - tj. podjetja za odnose z javnostmi. Nobeno izmed podjetij pa se ni odločilo za ponujena odgovora, da informacije o konkurentih za podjetje zbirajo zasebni detektivi ali odvetniki. Eno podjetje (zaradi majhnosti vzorca to statistično pomeni 10 %) je odgovorilo, da zanj tovrstne informacije zbirajo državni organi (v odgovoru je bilo natančneje določeno ministrstvo za ekonomske odnose ali Slovenska varnostno-obveščevalna služba) (Vrenko 1998, 93).

Podbregar (intervju) meni, da je v Sloveniji zelo malo »resnih« zasebnih izvajalcev obveščevalne dejavnosti, pa vendar tudi obstajajo. Najpogosteje podjetja za kaj takega uporabljajo zunanje izvajanje. Kot primer, kjer prihaja do možnega vpletanja takšnih in drugačnih izvajalcev, ki pa tudi prestopajo mejo legalnega so npr. gradbeni razpisi. Podbregar tudi meni, da detektivi niso pomembnejši igralec na takšnem trgu.

> *Podjetja, ki se odločajo za drugo možnost (torej ne za razvijanje lastnih KOD zmogljivosti), storitve Business Intelligence naročajo pri zunanjih izvajalcih. Pogosto gre za svetovalna ali raziskovalna podjetja, s katerimi dolgoročno in dobro sodelujejo že na drugih področjih. V temu primeru gre lahko za strateško dolgoročno sodelovanje, ko zunanji izvajalec v sodelovanju z naročnikom identificira konkurenco ter jo zanj redno spremlja in analizira. Na osnovi analiz nato naročniku pošilja poročila, lahko pa tudi priporočila in akcijski načrt. (Vrenko Peruško 2004b).*

7.4 Varovanje

V prejšnjem poglavju sem izpostavil nekatere vidike pridobivanja informacij s strani gospodarskih družb. Očitno pa je, da če gospodarske družbe pridobivajo podatke/informacije o drugih gospodarskih družbah, je gospodarska družba tudi predmet zbiranja takšnih informacij s strani druge oz. drugih gospodarskih družb ali celo koga drugega.

Izpostaviti želim izjemno pomembno stvar. Varovanje, ki je zelo širok pojem, v tem podpoglavju uporabljam v kontekstu varovanja tistih informacij, za katere gospodarske družbe iz raznoraznih razlogov ne želijo, da bi jih izvedeli drugi, kar pa ne pomeni, da gre samo za poslovne skrivnosti. Varovanje se sooča z dilemo, ki je posledica (zaželene) odprtosti podjetja do svojih strank, dobaviteljev, lastnikov, javnosti idr., saj na ta način npr. pridobiva nove delničarje podjetja, in »zaprtostjo« kako onemogočiti, da bi konkurenti o gospodarski družbi izvedeli stvari, ki jim lahko pomagajo v konkurenčnem boju proti tej gospodarski družbi, predvsem pa preprečiti vohunjenje. Lepo je del zgoraj zapisanega vidno v spodnjem citatu:

Podjetje kot poslovni sistem je v svojem obstoju, delovanju in razvoju vseskozi podvrženo raznim oblikam zunanjih in notranjih nevarnosti. Le-te materialno in moralno neugodno vplivajo na proizvodni, tehnološki in poslovni proces v podjetju, s tem pa tudi na poslovne izide (rezultate) podjetja. V širšem pomenu pa grozeče ali dejanske nevarnosti neugodno vplivajo tudi na zaposlene in na ugled podjetja (Vršec 1993, 34).

Tukaj vidimo tudi posledice teh nevarnosti, glavna od njih je seveda neugodni vpliv na poslovne rezultate podjetja. Isti avtor izpostavlja še nekaj vidikov, ki so tudi izjemno pomembni:

Ključno vprašanje varnosti podjetja je, kako vzpostaviti zaščitno in hkrati ekonomsko, poslovno in moralno učinkovito varnostno delovanje v podjetju. Zanima nas torej varnostno delovanje, ki bo finančno znosno - na daljši rok pa donosno – in ki bo opravilo svojo preventivno in (če je treba) represivno nalogo. Finančna znosnost se na eni strani nanaša na finančno ovrednotenje škod in izgub, na drugi strani pa na finančni vložek (stroške) varnostnega sistema. Obvladovanje ogroženosti, poslovnega in varnostnega tveganja daje možnost, da se v podjetju čim bolj približajo teoretično zasnovanemu finančnemu ravnovesju (ravnotežju) med finančno ovrednotenimi škodami/izgubami ter stroški zaščite in finančnimi ter drugimi koristmi varnostnega sistema … Novi varnostni koncepti podjetij temeljijo torej na prvinah ekonomike in poslovnosti podjetja, zatem pa še na pozitivnih prvinah vedenja lastnikov, menedžmenta in zaposlenih, kar sestavlja kulturo posameznega podjetja (Vršec 1993, 25).

Avtor ima v mislih seveda bistveno širše pojmovanje varovanja podjetja, kot želim to tematiko predstaviti v tem poglavju, vendar je za izhodišče dober začetek.

Problem ogrožanja poslovnih skrivnosti[67] izpostavlja Kop (1995, 52-53). "Obstoječa ali prihodnja podjetja ogrožajo poslovne skrivnosti bodisi neposredno ali pa posredno. O neposrednem ogrožanju govorimo takrat, ko si podjetje samo brez

[67] Kraja poslovne skrivnosti se lahko izkaže za pogubno za podjetje in prav zato si varovanje poslovnih skrivnosti v gospodarski družbi zasluži osrednjo pozornost.

pomoči posrednikov prizadeva, da bi se dokopalo do poslovnih skrivnosti. Na podlagi znanih primerov lahko sklepamo, da gre v večini primerov za neposredno ogrožanje". Avtor nadaljuje zgornjo misel z naslednjim:

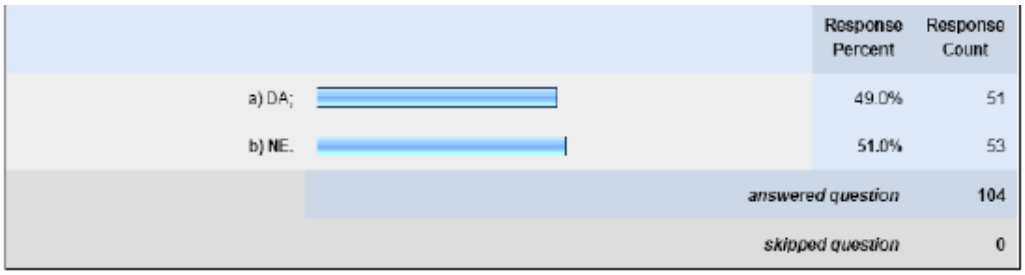
> *Najbrž pa tudi z domnevo, da posredno ogrožanje dobiva vedno večji pomen, nismo daleč od resnice. Bistvo tega posrednega ogrožanja je v tem, da se interesent za neko poslovno skrivnost dogovori s posrednikom, da mu za dobro plačilo priskrbi skrivnost sedanjega ali prihodnjega tekmeca na trgu. Ti posredniki so največkrat zasebna »svetovalna« podjetja, ki se poleg drugega ukvarjajo tudi z gospodarskim vohunstvom in prodajo poslovnih skrivnosti. Takšna podjetja so postala nekaj vsakdanjega predvsem na Japonskem in v ZDA, v zadnjem času pa tudi v Zahodni Evropi. Spremembe na politični karti Evrope pa so podrle tudi meje, ki bi takšna podjetja omejevale le na del Evrope zahodno od nas. Z veliko zanesljivostjo lahko iz tega sklenemo, da se je področje dela takšnih podjetij že razširilo na vso Evropo in seveda tudi na našo državo. Celo domneve, da se s temi posli skrivaj ukvarja tudi že katero od domačih podjetij, najbrž niso preveč predrzne in bodo prej ali kasneje dobile javno potrditev (Kop 1995, 53).*

Kop (1995, 53) omenja poleg svetovalnih podjetij še zasebne detektive. "Svetovalna podjetja pa niso edina, ki se ukvarjajo s takšnim nečednim poslom. Tudi nekateri t. i. zasebni detektivi niso nepristopni, če so le dobro plačani; odkriti primeri drugod po svetu dokazujejo, da je res tako …" in nadaljuje, da ni prav nobenega razloga, da bi bilo v Sloveniji drugače. S tema dvema kategorijama subjektov pa se seznam ne konča. "Med posredniki pri zagotovitvi poslovnih skrivnosti pa moramo omeniti tudi državne ustanove. Izrazit primer za to je v sklopu velikih političnih sprememb vzhodno od nas tudi doživel določeno preobrazbo, vendar ni izginil. Tudi edini ni bil. S to vrsto posrednega ogrožanja moramo računati tudi v prihodnje" (Kop 1995, 53-54). Menim, da ima avtor v mislih predvsem obveščevalne službe, ki so bile, so in bodo aktivne tudi v taki vlogi.

Poglejmo še, ali se slovenske gospodarske družbe zavedajo problema varovanja z omenjenega vidika.

Gjerek (2009) v svoji raziskavi nameni nekaj vprašanj tej tematiki. Med podjetji, ki so odgovorila, da so v preteklosti že zaznala BI (npr. zlorabo podatkov, izdajo poslovne tajnosti) – glej sliko 7.18 in teh je bilo 49 %, je iz vprašanja »Katere informacije so doslej že bile tarče/žrtve napadov BI?« (glej sliko 7.19) razvidno, da so »tarča« najpogosteje informacije: o kupcih, dobaviteljih, podjetjih, s katerimi podjetje sodeluje, 75,9 %; o novih izdelkih/storitvah, ki jih namerava podjetje lansirati na trg 44,4 %; o R&R,[68] proizvodnih, industrijskih in tehnoloških procesih 35,2 %.

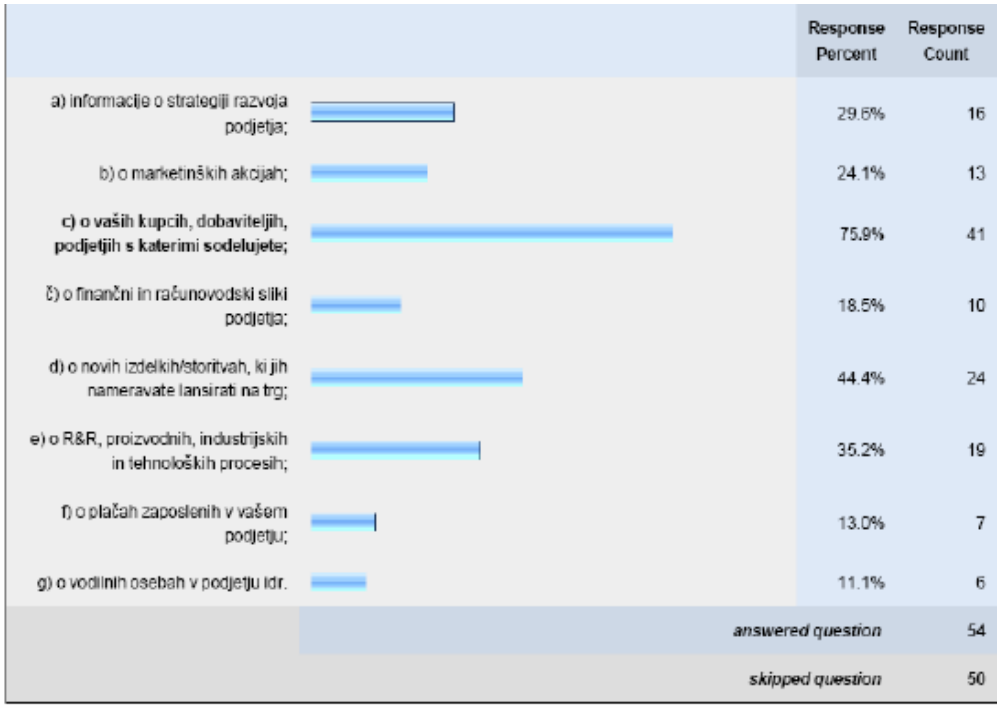
Slika 7.18: Ali ste v podjetju sploh kdaj zaznali BI (npr. zlorabo podatkov, izdajo poslovne tajnosti)?



	Response Percent	Response Count
a) DA;	49.0%	51
b) NE.	51.0%	53
answered question		104
skipped question		0

Vir: Gjerek (2009, 150)

Slika 7.19: Katere informacije so doslej že bile tarče/žrtve napadov BI?



	Response Percent	Response Count
a) informacije o strategiji razvoja podjetja;	29.6%	16
b) o marketinških akcijah;	24.1%	13
c) o vaših kupcih, dobaviteljih, podjetjih s katerimi sodelujete;	75.9%	41
č) o finančni in računovodski sliki podjetja;	18.5%	10
d) o novih izdelkih/storitvah, ki jih nameravate lansirati na trg;	44.4%	24
e) o R&R, proizvodnih, industrijskih in tehnoloških procesih;	35.2%	19
f) o plačah zaposlenih v vašem podjetju;	13.0%	7
g) o vodilnih osebah v podjetju idr.	11.1%	6
answered question		54
skipped question		50

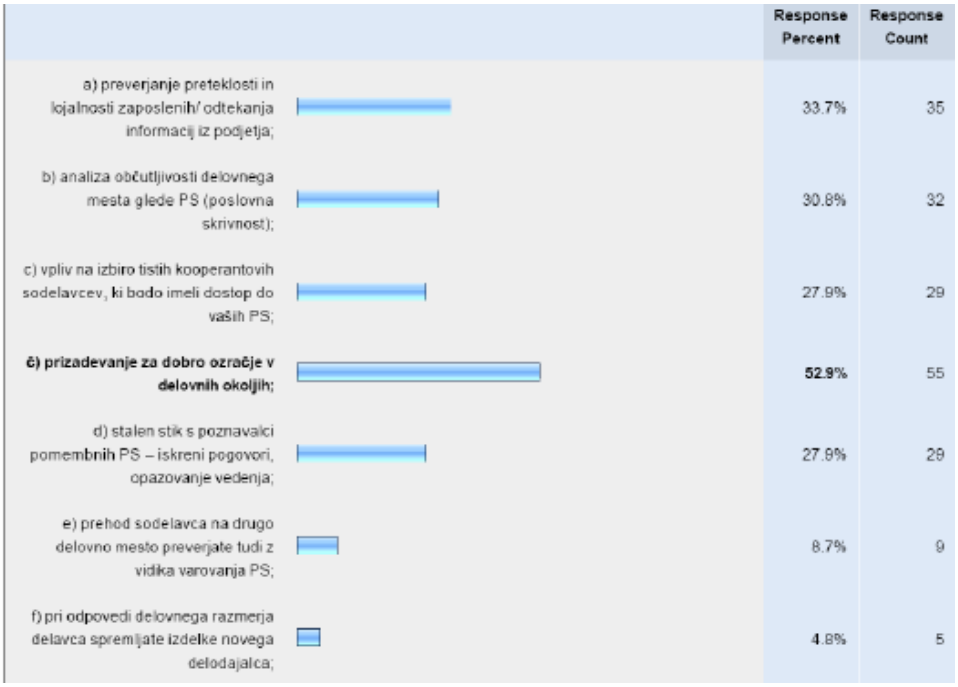
Vir: Gjerek (2009, 150)

[68] Raziskave in razvoj.

Sklop vprašanj, ki sledi prejšnjim, je namenjen ugotavljanju, kako se podjetja tem očitno zaznanim grožnjam zoperstavljajo.

Vprašanja si sledijo - s katerimi organizacijskimi/kadrovskimi/tehničnimi in pravnimi ukrepi so podjetja poskrbela za varovanje/zaščito informacij. Iz slik 7.20, 7.21, 7.22 in 7.23 je razvidno, da so v izredno visokem odstotku podjetja uporabljala organizacijske ukrepe, medtem ko druge ukrepe uporabljajo v prav neverjetno nizkem odstotku. Preobsežno bi se bilo poglabljati v vsak odgovor in odstotke, naj omenim le en primer za katerega menim, da je dober prikaz varnostnega delovanja slovenskih podjetij. Kot tehnični ukrep zaščite notesnikov proti kraji in nepravilni uporabi (v takšnih primerih gre npr. za kodiranje notesnika, ki je brez varnostnega gesla neuporaben, trdi disk nedostopen) je navedlo le 12,4 % podjetij. Poznam primer podjetja, ki je takšno kodiranje izvedlo na vseh službenih notesnikih, po nekaj primerih kraje notesnikov.[69] Menim, da se večina podjetij z varnostnimi grožnjami sooča reaktivno, torej se večinoma soočajo in preprečujejo grožnje, po tem, ko so se te že zgodile.

Slika 7.20: S katerimi kadrovskimi ukrepi ste poskrbeli za varovanje/zaščito zaupnih podatkov?



[69] Vsekakor ni moč trditi, da je v teh primerih šlo za kaj več kot slučaj in da je bila tarča kraja poslovnih skrivnosti ali drugi zanimivi podatki, vendar tega tudi ni mogoče v celoti izključiti.

g) pravilno poimenovanje delovnih mest – da ni zavajanja kandidatov zaradi večje privlačnosti dela;	8.7%	9
h) angažiranje zunanjega strokovnjaka za informacijsko varnost;	15.4%	16
i) drugo (opišite)	8.7%	9
	answered question	104
	skipped question	0

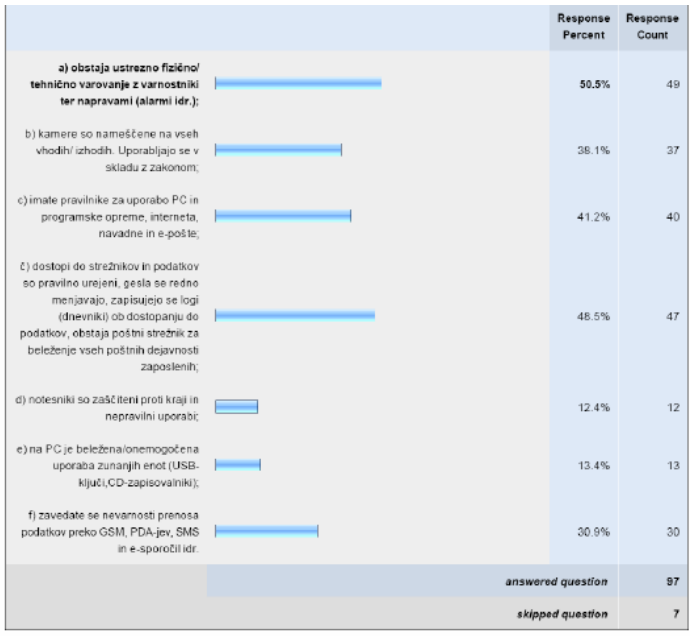
Vir: Gjerek (2009, 151-152)

Slika 7.21: S katerimi organizacijskimi ukrepi ste poskrbeli za varovanje/zaščito zaupnih podatkov?

	DA	NE	Response Count
a) osebni pogovor z delavci – kaj sploh je PS, načela varovanja;	**97.4% (75)**	2.6% (2)	77
b) izdelava katalogizacije in klasifikacije podatkov v podjetju za določitev stopnje tajnosti in dostopnosti do posameznega podatka;	**92.1% (35)**	7.9% (3)	38
c) preventivna predavanja o PS - vsaj 2 x letno (npr. kaj je SOCIALNI INŽENIRING in zaščita pred njim, kako KLASIFICIRATI PODATKE itd.);	**63.6% (7)**	36.4% (4)	11
č) članki o varovanju PS v internih glasilih, plakati za osveščanje, knjižica s priporočili;	**83.3% (5)**	16.7% (1)	6
d) pri vodenju obiskovalcev po obratih in pisarnah ste preprečili možnosti razkritja PS;	**95.3% (41)**	4.7% (2)	43
e) na sejmih ter pri objavi strokovnih člankov ste previdni pri dajanju navidezno nepomembnih informacij;	**100.0% (37)**	0.0% (0)	37
f) v prostorih občutljivega področja (npr. laboratoriji) ni fotokopirnih strojev, velja striktna prepoved vnosa fotokamer in telefonov s fotokamero ipd.;	**88.9% (8)**	11.1% (1)	9
g) o xpomembnejših PS se po telefonu/ telefaksu ne pogovarjate. Če pa že, jih prej šifrirate/dešifrirate	**100.0% (17)**	0.0% (0)	17
idr.			
		answered question	102
		skipped question	2

Vir: Gjerek (2009, 152-153)

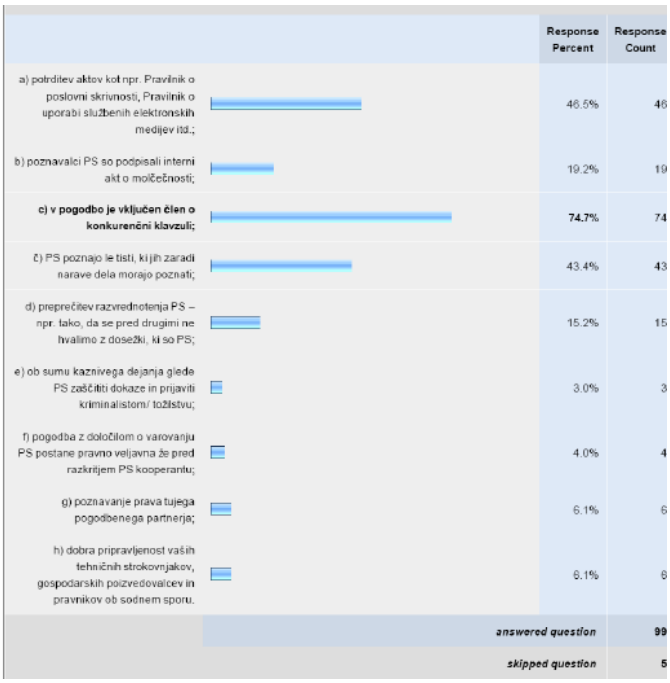
Slika 7.22: S katerimi tehničnimi ukrepi ste poskrbeli za varovanje/zaščito zaupnih podatkov?



	Response Percent	Response Count
a) obstaja ustrezno fizično/ tehnično varovanje z varnostniki ter napravami (alarmi idr.);	**50.5%**	49
b) kamere so nameščene na vseh vhodih/ izhodih. Uporabljajo se v skladu z zakonom;	38.1%	37
c) imate pravilnike za uporabo PC in programske opreme, interneta, navadne in e-pošte;	41.2%	40
č) dostopi do strežnikov in podatkov so pravilno urejeni, gesla se redno menjavajo, zapisujejo se logi (dnevniki) ob dostopanju do podatkov, obstaja poštni strežnik za beleženje vseh poštnih dejavnosti zaposlenih;	48.5%	47
d) notesniki so zaščiteni proti kraji in nepravilni uporabi;	12.4%	12
e) na PC je beležena/onemogočena uporaba zunanjih enot (USB-ključi,CD-zapisovalniki);	13.4%	13
f) zavedate se nevarnosti prenosa podatkov preko GSM, PDA-jev, SMS in e-sporočil idr.	30.9%	30
	answered question	**97**
	skipped question	**7**

Vir: Gjerek (2009, 153)

Slika 7.23: S katerimi pravnimi ukrepi ste poskrbeli za varovanje/zaščito zaupnih podatkov?



	Response Percent	Response Count
a) potrditev aktov kot npr. Pravilnik o poslovni skrivnosti, Pravilnik o uporabi službenih elektronskih medijev itd.;	46.5%	46
b) poznavalci PS so podpisali interni akt o molčečnosti;	19.2%	19
c) v pogodbo je vključen člen o konkurenčni klavzuli;	**74.7%**	74
č) PS poznajo le tisti, ki jih zaradi narave dela morajo poznati;	43.4%	43
d) preprečitev razvrednotenja PS – npr. tako, da se pred drugimi ne hvalimo z dosežki, ki so PS;	15.2%	15
e) ob sumu kaznivega dejanja glede PS zaščititi dokaze in prijaviti kriminalistom/ tožilstvu;	3.0%	3
f) pogodba z določilom o varovanju PS postane pravno veljavna že pred razkritjem PS kooperantu;	4.0%	4
g) poznavanje prava tujega pogodbenega partnerja;	6.1%	6
h) dobra pripravljenost vaših tehničnih strokovnjakov, gospodarskih poizvedovalcev in pravnikov ob sodnem sporu.	6.1%	6
	answered question	**99**
	skipped question	**5**

Vir: Gjerek (2009, 154)

Iz zgornjih štirih grafov razberemo, da so kot najpogostejši ukrepi za varovanje/zaščito informacij uporabljeni: prizadevanje za dobro ozračje v delovnih okoljih; o pomembnejših poslovnih skrivnostih se po telefonu in telefaksu ne pogovarja; fizično/tehnično varovanje z varnostniki in napravami ter vključitev konkurenčne klavzule v pogodbo o zaposlitvi. Vidimo tudi, da podjetja v največji meri uporabljajo organizacijske ukrepe.

Naj navedem še praktični napotek, ki ga Vršeč (1993, 132-133) podaja visokotehnološkim podjetjem in/ali podjetjem s prodornim inovacijskim razvojem:

> *V podjetjih z visoko tehnologijo in/ali s prodornim inovacijskim razvojem bi morale varnostne službe temeljiteje spoznati (profesionalno) zaščito poslovnih skrivnosti pred ekonomskim vohunjenjem ter podjetniško strategijo, taktiko, tehniko in metodiko podjetniškega vidika poizvedovanja. Pri tem bi morale seči po dodatni literaturi, ki obravnava to področje, in poiskati dodatno specializirano izpopolnjevanje za tistega strokovnjaka za varnost, ki bo skrbel za to področje.*

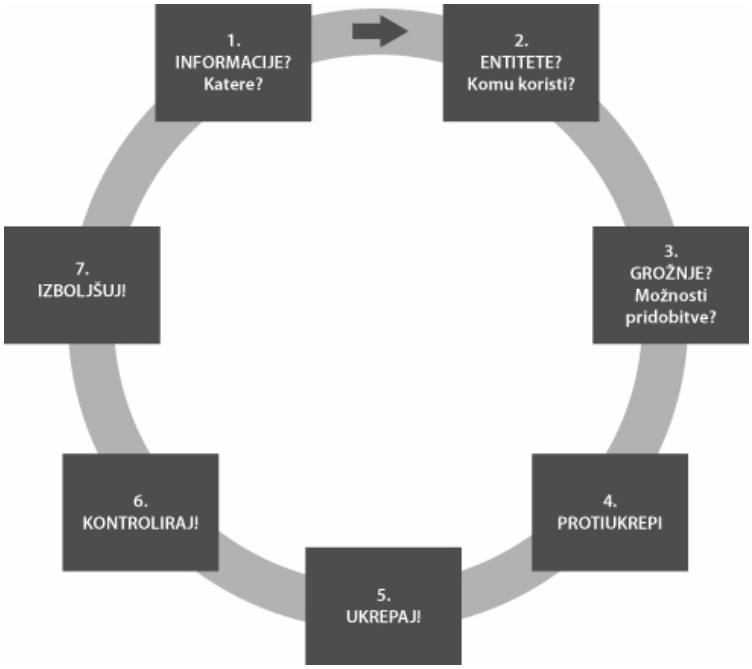
Jelen je s sodelavci razvil lastni model za upravljanje s tveganji, ki predstavlja zanimiv poskus in čeprav ne preizkušen v praksi, po mojem mnenju predstavlja dobro osnovo, ki so jo razvili slovenski strokovnjaki. "Na temelju znanja, ki smo ga zbrali do te točke in izkušenj, poskušamo v nadaljevanju razviti lastni model (pravzaprav točneje, elemente zanj) oziroma okvir za upravljanje s tveganji pred ekonomskim vohunstvom" (Jelen 2009, 271).

> *Naš model povezuje ugotovljene ključne elemente, ki opredeljujejo tovrstna tveganja ter osnovne managerske pristope. Razvit je kot proces, ki ga predstavlja niz zapovrstnih aktivnosti (korakov), ki pripeljejo do celovitega prepoznavanja oziroma zaznavanja tveganj ter vrednotenja; najprimernejših in stroškovno upravičenih ukrepov za njihovo preprečevanje, odvračanje, ali zmanjševanje negativnih posledic ter obenem zagotavljajo (s povratno zanko) stalno izboljševanje tega procesa. Model ponuja možnost, da se vpelje v obliki projekta ali pa izvaja kot stalna aktivnost (Jelen 2009, 272).*

Pomembno popotnico k uspešnosti in učinkovitosti modela vidimo v tem, da je postavljen v managerske funkcijo in ne zgolj prepuščen oddelku, ki skrbi za varnost v podjetju. To je mogoče zagotoviti na več načinov. Najučinkovitejša rešitev pa je, da je nekdo v top managementu neposredno odgovoren za protiobveščevalno varnost in, da je v nadzorno funkcijo v modelu vključena tudi enota ali kompetentni delavec zunaj varnostnega oddelka (denimo, v strateškem controllingu), Okvirni model ima naslednjih sedem korakov (glej sliko 7.24 op. M.A.):

1. *Identificiranje občutljivih informacij;*
2. *Ocena groženj;*
3. *Ocena ranljivosti;*
4. *Načrtovanje protiukrepov;*
5. *Udejanjanje (načrtov in protiukrepov);*
6. *Kontrola (izvajanja in učinkov);*
7. *izboljševanje (načrtov in izvajanja) (Jelen 2009, 272).*

Slika 7.24: Model sedmih korakov prikazan v ciklični obliki



Vir: Prirejeno po Jelen 2009, 273

Zavedati se je seveda potrebno, "da ne obstaja popolna varnost. Vsaka organizacija je in bo vedno ranljiva do določene mere. Toda to ne pomeni, da bi prenehali z

varovanjem lastnih pomembnih informacij. Kar morate storiti, je vzpostaviti razumne varnostne ukrepe, ki minimizirajo tveganja; to je nekaj, kar lahko doseže vsaka organizacija" (Winkler 1997, xviii).

8 SKLEP

V pričujočem magistrskem delu sem v prvi monografiji, posvečeni primarno konkurenčni obveščevalni dejavnosti, poskusil predstaviti to področje na nadaljevalni in razvojni način, s katerim sem predstavil to področje preko klasične (gospodarske) obveščevalne dejavnosti, iz katere sodobna KOD črpa tako terminologijo kot tudi del metod in taktik dela ter iz katerih vrst prihaja veliko današnjih teoretikov in praktikov KOD. Ker je vsakdanje, tako laično kot deloma tudi strokovno, razumevanje KOD povezano z dejavnostmi, ki se dotikajo sive cone ali tudi že izven zakonsko dovoljenega območja, sem velik del namenil tudi vohunstvu. Poskusil sem tudi osvetliti pogled na možne zlorabe in nadzor nad to dejavnostjo, na koncu pa še proučiti stanje KOD v Sloveniji. Velik del prostora sem porabil tudi za predstavitev obveščevalne dejavnosti kot dejavnosti, ki jo izvajajo številni akterji (predvsem gospodarske družbe) in ne zgolj državni organi, kar odlično predstavi tudi Črnčec, in v povezavi s še tremi pojavi, ki so za razumevanje tega področja zelo pomembni – globalizacija, informacijska tehnologija in sodobne varnostne grožnje, čemur sem v večji ali manjši meri tudi namenil prostor v delu. "Globalizacija, pospešen razvoj informacijske tehnologije in sodobne varnostne grožnje so obveščevalno dejavnost v javnem in zasebnem sektorju postavili pred številne zahteve in pričakovanja. Obveščevalna dejavnost v zasebnem sektorju je dobila in dobiva zagon, nove možnosti in priložnosti" (Črnčec 2009, 15).

V delu sem si zastavil tri hipoteze. Prva se glasi - »Slovenske gospodarske družbe se zavedajo pomena konkurenčne obveščevalne dejavnosti in jo uporabljajo kot orodje, ki jim omogoča konkurenčno prednost na trgu«. To hipoteze sem preverjal s proučevanjem literature, proučitvijo treh empiričnih raziskav, s pogovori s strokovnjaki, s spremljanjem tega področja v medijih, zaposlitvijo v dveh izmed petih največjih IKT družbah v Sloveniji, stiki z ljudmi idr. Na podlagi navedenega to hipotezo zgolj deloma potrjujem, saj menim da se v (vsaj zadovoljivi meri) KOD zavedajo in jo v polni meri sistematično uporabljajo zelo redke slovenske gospodarske družbe. Na podlagi nekaterih indicev bi lahko kot take prepoznali predvsem družbi Krka d.d. in Telekom Slovenije d.d. Prepričan pa sem, da se te dejavnosti (pa kakorkoli jo že poimenujejo) vsaj deloma poslužujejo vse največje

slovenske družbe, še posebej, če delujejo v okolju mednarodne konkurence in v panogah, v katerih je KOD v svetu tradicionalno najmočnejša – farmacevtika, telekomunikacije, energetika.

Drugo hipotezo – »Nelegalna dejanja, predvsem vohunjenje, so neločljiv del konkurenčne obveščevalne dejavnosti, brez katerih le-ta ne more biti uspešna«, zavračam. Na podlagi številne literature in pogovorov se zavedam, da se prestopanje v sivo ali celo nelegalno območje dogaja pogosto, pa vendar trdim, da je KOD lahko uspešna tudi brez posluževanja nelegalnih metod in sredstev, pa še sramota in ponižanje ob razkritju takih dejanj je preprečena. Vseeno imejmo v mislih sledeče:

> *V primeru, ko govorimo o obveščevalni dejavnosti obveščevalne službe, se pri tem torej misli običajno na dejavnost s tistim presežnim pomenom, ki vsebuje vohunjenje (a ostaja pogosto neizrečeno). Ko pa govorimo o obveščevalni dejavnosti v podjetniški sferi, se na vsa usta poudarja zakonitost in etičnost delovanja. Torej, le legalno zbiranje in analiziranje podatkov in informacij, brez prepovedanih oblik, brez omenjenega presežka. Ampak, ali je res (vedno) tako? Morda, ali pa tudi ne. Ali ne govorimo pri poslih o mejnem območju, zoni somraka (»twilight zone«)? To je najbrž podobno kot pri (nekaterih) masažnih salonih, za katere se ve, da ponujajo »nekaj več« (a ostaja neizrečeno) (Jelen 2009, 301).*

Z navedenim pridemo tudi do nadzora nad to dejavnostjo, ki je predmet zadnje hipoteze, ki se glasi – »Pravna praznina, teoretična neobdelanost in odsotnost mehanizmov nadzora omogočajo oz. ne preprečujejo zlorabe, sicer legalne konkurenčne obveščevalne dejavnosti v nelegalne namene«. To zadnjo hipotezo deloma potrjujem. Deloma zaradi tega, ker ne moremo trditi o popolni teoretični neobdelanosti ter o popolni odsotnosti mehanizmov, ki pa resda niso primarno usmerjeni na to področje, temveč zgolj posredno. Ne glede na zapisano pa je prav področje nadzora, po mojem mnenju področje, ki mu je potrebno nameniti veliko večjo pozornost, saj do zlorab prihaja, kar se da prepoznati že iz spremljanja dnevnega tiska, še veliko večjo pa je področje zlorab, ki ali niso zaznana ali pa niso sporočena javnosti. Jasno je seveda tudi, da npr. država, kot je Slovenija, ne bo razvijala posebnih mehanizmov nadzora »samo« zaradi KOD oz. zlorab, ki so lahko s

to dejavnostjo povezana, pa vendar je napotek o večji pozornosti organov tudi na to področje povsem na mestu. Moj predlog bi bil, kar je razvidno, da se dogaja, iz nekaterih primerov iz sveta, da se tudi obveščevalne in varnostne službe aktivneje vključijo v preventivno (aktivno?) vlogo za potrebe domačih gospodarskih družb.

Poleg treh predstavljenih hipotez se pri KOD odpira še cela vrsta vprašanj in področij, ki bi jih bilo koristno tudi (ali predvsem) v slovenskem prostoru temeljiteje obdelati. Ena izmed teh je nedvomno tudi bolj praktično naravnano proučevanje tega področja in vprašanje etike KOD, ki je v samem jedru razprav, saj je to področje (nelegalnost in neetičnost) tisto, na katerem se sliši največ očitkov KOD. Zanimivo bi bilo tudi proučevanje zasebno-javnega sektorja, kjer se prepletata državni in zasebni interes, kar ima lahko zanimive implikacije na področju KOD.

Za konec citiram Sun Tzuja, v čigar zapisu prepoznavam tisočletno resnico in iz katerega prepoznavam potencialno korist KOD v današnjem konkurenčnem boju:

Poznaj sovražnika,
poznaj sebe,
pa ne bo zmaga
nikoli vprašljiva,
niti v stotih bitkah ne.

Kdor pozna sebe,
a ne pozna sovražnika,
bo utrpel en poraz
za vsako zmago.

Kdor ne pozna
ne sebe
ne sovražnika,
mu bo spodletelo v vsaki bitki.

9 LITERATURA

1. Agrell, Wilhelm. 1987. The Changing role of National Intelligence Services. V *Intelligence for Economic Development. An Inquiry into the Role of the Knowledge Industry*, ur. Stevan Dedijer in Nicolas Jéquier, 31-40. Oxford: Berg Publishers Limited.
2. Anžič, Andrej. 1996. *Vloga varnostnih služb v sodobnih parlamentarnih sistemih – nadzorstvo*. Ljubljana: ČZP Enotnost.
3. Balzli, Beat, Dinah Deckstein, Frank Dohmen, Isabell Hülsen, Marcel Rosenbach, Jörg Schmitt, Holger Stark, Thomas Tuma. 2008. The Dark Side of Power – German Corporate Spying Scandal Widens. *Spiegel*, 6. september 2008. dostopno prek: http://www.spiegel.de/international/business/0,1518,558510,00.html (4. april 2010).
4. Bergier, Jacques. 1974. *Vohunstvo v industriji in znanosti.* Ljubljana: Mladinska knjiga.
5. Brody, Roberta. 2008. Issues in Defining Competitive Intelligence: An Exploration. *Journal of Competitive Intelligence and Management* 4 (3): 3-16.
6. Buchda, Sascha. 2007. Rulers for Business Intelligence and Competitive Intelligence: An Overview and Evaluation of Measurement Approaches. *Journal of Competitive Intelligence and Management* 4 (2): 23-54.
7. Carr, Margaret Metcalf. 2003. *Super Searchers on Competitive Intelligence. The Online and Offline Secrets of Top CI Researchers*. New Jersey: Cyber Age Books.
8. China bugs and burgles Britain. *Times,* 31. januar 2010. Dostopno prek: http://www.timesonline.co.uk/tol/news/uk/crime/article7009749.ece (4. april 2010).
9. *Corporate Spending on Competitive Intelligence Projected to Rise Ten-Fold, to $10 Billion, in Five Years*. Dostopno prek: http://www.marketwire.com/press-release/Corporate-Spending-on-Competitive-Intelligence-Projected-Rise-Ten-Fold-10-Billion-743788.htm (4. april 2010).
10. Časopis za kritiko znanosti 75/76. 1985. *Clausewitz*. Ljubljana: Univerzitetna konferenca Zveze socialistične mladine Slovenije Maribor in Ljubljana.

11. Črnčec, Damir. 2008. *Obveščevalna dejavnost v javnem in zasebnem sektorju (gospodarska vs. konkurenčna obveščevalna dejavnost).* Doktorska disertacija. Ljubljana: FDV.
12. Črnčec, Damir. 2009. *Obveščevalna dejavnost v informacijski dobi*. Ljubljana: Defensor.
13. Dvoršak, Andrej. 2003. Zbiranje relevantnih podatkov o proizvodnji, konkurenci in poslovanju/Industrial Intelligence & Competitive Intelligence & Business Intelligence/. V *IV. Slovenski dnevi varstvoslovja.* Ljubljana: Visoka policijsko-varnostna šola.
14. *Economic Espionage Act of 1996*. Dostopno prek: http://www.da.usda.gov/pdsd/Security%20Guide/T1threat/Legal.htm (4. april 2010).
15. Egan, Mark in Tim Mather. 2005. *Varnost informacij. Vodnik za podjetja.* Ljubljana: Pasadena.
16. Fleisher, Craig S. 2004. Competitive Intelligence Education: Competencies, Sources, and Trends. *The Information Management Journal* March/April 2004: 56-62.
17. Fleisher, Craig S. in Babette Bensoussan. 2003. *Strategic and competitive analysis: methods and techniques for analyzing business competition.* New Jersey: Prentice Hall, Upper Saddle River.
18. Friedman, Thomas L. 2005/2008. *Izravnavanje sveta*. Tržič: Učila International.
19. Fuld, Leonard M. 2006. *The Secret Language of Competitive Intelligence*. New York: Crown Business.
20. Gjerek, Bernardin. 2009. *Taktika in metodika dela gospodarskih poizvedovalcev*. Specialistična naloga. Ljubljana: Fakulteta za varnostne vede.
21. Global Intelligence Alliance. 2004. *Introduction to Competitive Intelligence.* Dostopno prek: http://www.globalintelligence.com/insights-analysis/white-papers/introduction-to-competitive-intelligence (4. april 2010).
22. Global Intelligence Alliance. 2005. *Competitive Intelligence in Large Companies – Global Study.* Dostopno prek: http://www.globalintelligence.com/ insights-analysis/white-papers/ci-in-large-companies-global-study (4. april 2010).

23. *Glossary of terms used in competitive intelligence and knowledge management*. Dostopno prek: http://scip.cmsplus.com/files/Prior%20Intelligence%20Glossary%2009Jan.pdf (4. april 2010).
24. Havenga, Johan in Deonie Botha. 2003. *Developing competitive intelligence in the knowledge-based organisation*. Dostopno prek: http://www.saoug.org.za/archive/2003/0312a.pdf (4. april 2010).
25. Hočevar, Barbara. 2007. *Gospodarska obveščevalna dejavnost*. Diplomsko delo. Ljubljana: Fakulteta za družbene vede.
26. Hughes, Stephanie. 2005. Competitive intelligence as competitive advantage. The Theoretical Link Between Competitive Intelligence, Strategy and Firm Performance. *Journal of competitive intelligence and management* 3 (3): 61-82.
27. Hulnick, Arthur S. 2002. Risky business. Private Sector Intelligence in the United States. *Harvard International Review*. Fall 2002: 68-72.
28. International Telecommunication Union. 2009. *Measuring the Information Society - The ICT Development Index*. Dostopno prek: http://www.itu.int/ITU-D/ict/publications/idi/2009/material/IDI2009_w5.pdf (4. april 2010).
29. *Investigative Programs - Counterintelligence Division: Focus on Economic Espionage.* Dostopno prek: http://www.fbi.gov/hq/ci/economic.htm (4. april 2010).
30. Jelen, Ladislav. 2008. Ekonomsko vohunstvo in upravljanje tveganj. V *Vohunska dejavnost in gospodarstvo*, ur. Iztok Podbregar, 185-302. Ljubljana: FVV.
31. Jéquier, Nicolas in Stevan Dedijer. 1987. Information, Knowledge and Intelligence: A Generala Overview. V *Intelligence for Economic Development. An Inquiry into the Role of the Knowledge Industry*, ur. Stevan Dedijer in Nicolas Jéquier, 1-24. Oxford: Berg Publishers Limited.
32. Jordan Jennifer in Finklestein Sydney. 2005. *The Ethics of Competitive Intelligence*. Dostopno prek: http://mba.tuck.dartmouth.edu/pdf/2005-1-0095.pdf (4. april 2010).
33. Juhari, Arrif S. in Derek Stephens. 2006. Tracing the Origins of Competitive Intelligence Throughout History. *Journal of Competitive Intelligence and Management* 3 (4): 61-82.

34. Kahaner, Larry. 1997. *Competitive Intelligence. How to Gather, Analyze, and Use Information to Move your Business to the Top*. New York: Touchstone.
35. Kastelic, Marko. 2008. *Protiobveščevalna dejavnost kot vidik zagotavljanja nacionalne varnosti Republike Slovenije*. Magistrsko delo. Nova Gorica: Evropska pravna fakulteta v Novi Gorici.
36. *Kazenski zakonik* (KZ-1-NPB1). Dostopno prek: http://www.dz-rs.si/index.php?id=101&sm=k&q=kazenski+zakonik&mandate=1&unid=UPB|1B04368E4254FD4BC12575C40026DF98&showdoc=1 (4. april 2010).
37. Kop, Ivo. 1995. *Varovanje in zaščita poslovnih skrivnosti*. Ljubljana: Gospodarski vestnik.
38. Liebowitz, Jay. 2006. *Strategic Intelligence: Business Intelligence, Competitive Intelligence and Knowledge Management.* Boca Raton: Auerbach Publications.
39. Lowenthal, Mark M. 2000. *Intelligence. From Secrets to Policy*. Washington: CQ Press.
40. *Manager of Competitive Intelligence.* Dostopno prek: http://jobs.scip.org/c/job.cfm?site_id=296&jb=5828667 (13. september 2009).
41. Marinković, Ilija. 2001. Od povezovanja do globalizacije. *Delo,* (19. aprila 2001).
42. Mazzeti, Mark. 2009: Global Economy Top Threat to U.S., Spy Chief Says. *The New York Times*, (12. februarja 2009). Dostopno prek: http://www.nytimes.com/2009/02/13/washington/13intel.html?_r=1 (16. maj 2010).
43. McGonagle, John J. in Caroline M. Vella. 2004. Competitive intelligence in action. *The Information Management Journal* March/April 2004: 64-68.
44. Millen, Press. 2006. *The Economic Espionage Act - is it finally catching on?* Dostopno prek: http://findarticles.com/p/articles/mi_qn4185/is_20060319/ai_n16143091/pg_3/?tag=content;col1 (4. april 2010).
45. Miller, Jerry P. 2001. *Competitive Intelligence: What is IT & It's Status.* Dostopno prek: www.infotoday.com/it2001/presentations/jmiller.ppt (4. april 2010).
46. Minforda, John. 2003/2009. *Sunzi – Umetnost vojne*. Ljubljana: Mladinska knjiga Založba.
47. *NPS poslovne rešitve*. Dostopno prek: http://www.nps.si/ (4. april 2010).

48. Nye, Joseph S. Jr. 2004. *Soft Power: The means to Success in World Politics.* New York: PublicAffairs.
49. Pirttimäki, Virpi. 2007. Comparative Study and Analysis of the Intelligence Activities of Large Finnish Companies. *Journal of Competitive Intelligence and Management* 4 (1): 132-155.
50. Podbregar, Iztok, ur. 2008. *Vohunska dejavnost in gospodarstvo*. Ljubljana: FVV.
51. Podbregar, Iztok. 2010. Intervju z avtorjem. Ljubljana, 23 februar.
52. *Podpora poslovnemu odločanju*. Dostopno prek: http://www.avtenta.si/si/podpora-poslovanju-in-poslovnemuodlocanju/poslovna-inteligenca/ (4. april 2010).
53. Porter, Michael E in Victor E. Millar. 1985. How Information Gives You Competitive Advantage. V *On Competition*, ur. Michael E. Porter, 73-96. Harvard: A Harvard Business Review Book.
54. Porter, Michael E. 1985/1998. *Competitive Advantage. Creating and Sustaining Superior Performance.* New York: Free Press.
55. *Poslovno obveščanje*. Dostopno prek: http://www.src.si/izobrazevanje/obvescanje/default.asp (4. april 2010).
56. Prescott, John. 1999. The Evolution of Competitive Intelligence. *APMP Journal*, Spring 1999. Dostopno prek: www.apmp.org/fv-154.aspx (4. april 2010).
57. Purg, Adam. 1995. *Obveščevalne službe*. Ljubljana: Enotnost.
58. Purg, Adam. 2002. *Primerjalni obveščevalni sistemi*. Ljubljana: Visoka policijsko-varnostna šola.
59. Raščan, Stanislav. 2005. *Spremembe varnostne politike ZDA po 11. septembru 2001*. Ljubljana: Fakulteta za družbene vede.
60. Schweizer, Peter. 1996. The Growth of Economic Espionage. America is Target Number One. *Foreign Affairs* 75 (1): 9-14.
61. *Scientia potentia est.* Dostopno prek: http://en.wikipedia.org/wiki/Knowledge_is_power (4. april 2010).
62. Shulsky, Abram N. 1993. *Silent Warfare. Understanding the World of Intelligence.* Brassey's.
63. *Slovar slovenskega knjižnega jezika*. 1994. Ljubljana: DZS.

64. *Society of Competitive Intelligence Professionals*. Dostopno prek: http://www.scip.org (4. april 2010).
65. Strokovnjak za obveščevalno dejavnost. 2010. Intervju z avtorjem. Ljubljana 25. februar.
66. Svete, Uroš. 2005. *Varnost v informacijski družbi*. Ljubljana: Fakulteta za družbene vede.
67. Šaponja, Vladimir. 1999. *Taktika dela obveščevalnovarnostnih služb.* Ljubljana: Visoka policijsko-varnostna šola.
68. Španinger, Vili. 2008. Varovanje poslovnih skrivnosti v gospodarskih družbah. V *Vohunska dejavnost in gospodarstvo*, ur. Iztok Podbregar, 425-530. Ljubljana: Fakulteta za varnostne vede.
69. *Unilever and P&G announce agreement*. Dostopno prek: http://findarticles.com/p/articles/mi_m0DQA/is_2001_Sept_27/ai_79196013/ (4. april 2010).
70. Van der Kraats, Barend. 2009. Applying Competitive Intelligence in the Public Sector. *Competitive Intelligence* 12 (2): 20-23.
71. Varnostni menedžer. 2008. Intervju z avtorjem. Ljubljana. 15. maj.
72. Vrenko Peruško, Ines. 2004b *Business intelligence kot nadgradnja klasičnih sekundarnih raziskav.* Dostopno prek: http://gfk.si/4_2_lclank.php?cid=983 (17. februar 2009).
73. Vrenko Peruško, Ines: 2004a. *Business intelligence: oči in ušesa uspešnih podjetij.* Dostopno prek: http://www.relacije.com/clanek.php?niceid=business-intelligence-oci-in-usesa-uspesnih-podjetij (4. april 2010).
74. Vrenko, Ines. 1998. *Ekonomska in konkurenčna obveščevalna dejavnost.* Diplomsko delo. Ljubljana: Fakulteta za družbene vede.
75. Vršec, Milan. 1993. *Varnost podjetja – tokrat drugače*. Ljubljana: Viharnik.
76. *What is competitive intelligence?* Dostopno prek: http://www.scip.org/content.cfm?itemnumber=2214&navItemNumber=492 (4. april 2010).
77. Winkler, Ira. 1997. *Corporate espionage. What it is, why it is happening in your company, what you must do about it.* Rocklin: Prima Publishing.
78. Wright, Sheila. 2005. *Seven European Nations: A Profile of Current CI Practice.* Dostopno prek: http://www.scip.org/files/secure/index.cfm?FileID=6413 (4. april 2010).

79. *Zakon o gospodarskih družbah* (ZGD-1-UPB3). Ur. L. RS 65/09. Dostopno prek: http://www.uradni-list.si/1/objava.jsp?urlid=200965&stevilka=3036 (04.04.2010).
80. Žaže, Simona. 2007. *Nedovoljenosti gospodarskega poizvedovanja. Specialistična naloga.* Ljubljana: Fakulteta za varnostne vede.
81. Žirovnik, Janez in Iztok Podbregar. 2006. Obveščevalno-varnostni vidiki ogrožanj pomembnih gospodarsko poslovnih subjektov. V *Kriminalni napadi na premoženje gospodarskih subjektov (varnostni, pravni in zavarovalni vidiki),* ur. Anton Dvoršek in Liljana Selinšek, 47-66. Ljubljana: Pravna fakulteta in Fakulteta za policijsko-varnostne vede.