Katoliški inštitut
Fakulteta za pravo in poslovne vede

Catholic Institute
Faculty of Law and Business Studies

Magistrski študijski program Poslovne vede II

Miranda Osterc Zinrajh

EKONOMSKA OGROŽENOST GOSPODARSKIH SUBJEKTOV V LUČI GOSPODARSKEGA VOHUNJENJA

Magistrska naloga

Mentor: izr. prof. dr. Laris Gaiser

Ljubljana, 2021

Pričujoča naloga je rezultat mojih študijskih prizadevanj in pomoči spoštovanih predavateljev Fakultete za pravo in poslovne vede, predvsem mentorja, izr. prof. dr. Larisa Gaiserja, docenta dr. Simona Malmenevalla, docenta dr. Mitje Steinbacherja, prof. dr. Žige Čeparja in doc. dr. Zorana Vaupota, ki so mi nesebično pomagali s strokovnimi nasveti. Zahvala gre tudi vodstvu fakultete, saj brez pomoči fakultete pri štipendiranju moj študij v tem obdobju ne bi bil mogoč.

Posebej se moram zahvaliti tudi svojemu soprogu, ki mi je potrpežljivo in vztrajno nudil potrebno oporo.

SEZNAM UPORABLJENIH KRATIC IN OKRAJŠAV

BVT – Bundesamt für Verfassungsschutz und Terrorismusbekämpfung

CIA – Central Intelligence Agency

ECIPE – European Centre for Political Economy

EU – Evropska unija

EEA – Economic Espionage Act

FBI – Federal Bureau of Investigation

KZ – Kazenski zakonik

MAD – Militärischer Abschirmdienst

MADG – Militärischer Abschirmdienst Gesetz

OVS – Obveščevalno-varnostna služba

RS – Republika Slovenija

SOA – Sigurnosno obaveštajna agencija

SOVA – Slovenska obveščevalno-varnostna agencija

VSOA – Vojna sigurnosno obaveštajna agencija

ZDA – Združene države Amerike

ZSOVA – Zakon o slovenski obveščevalno varnostni agenciji

KAZALO

KAZALO SLIK

1. UVOD

Obveščevalna dejavnost na ekonomskem področju je zagotovo vsaj toliko stara kot prve oblike obrambno-varnostne obveščevalne dejavnosti. Družbene razmere so že pred tisočletji silile pripadnike družbenih skupin v pridobivanje podatkov o nasprotnikih in uspešnim nudile določeno prednost ter napredek. Gospodarsko vohunstvo se je usmerjalo predvsem v ugotavljanje in odkrivanje varovanih dobrin in procesov njihove izdelave. Metode obveščevalne dejavnosti so se skozi zgodovino spreminjale in posodabljale. Osnova te dejavnosti je bil človeški faktor oziroma pridobivanje informacij s pomočjo človeških virov, kar predstavlja tudi danes pomemben element. (Gaiser 2010) Ta dejavnost na ekonomskem področju je po obliki in vsebini precej široka, saj se z njo ukvarjajo tako država kakor tudi zasebne službe.[1] Oboji se osredotočajo na šibkejše gospodarske subjekte in slabo varovano tehnologijo. Kraje poslovnih skrivnosti konkurenčnih podjetij predstavljajo manjši strošek in čas, ki bi ga sicer porabili za lastne raziskave in razvoj, posledično pa se vohunjenje kljub kaznivosti izplača. Za povprečnega opazovalca so aktivnosti obveščevalnih subjektov pravzaprav težko opazne, čeprav poteka pod tančico prikritosti prava vojna[2] za poslovne in druge informacije. (Bazdan 2016, 50) Ugotavljamo torej, da v svetu že precej dolgo vlada prava obveščevalna oziroma vohunska vojna. V tej vojni praviloma zmagujejo tisti, ki so ob industrijski revoluciji pravočasno zaznali tudi obveščevalno revolucijo kot produkt gospodarskega razvoja.

1.1 Opredelitev naloge in cilji

V magistrski nalogi je opredeljeno gospodarsko vohunjenje v kontekstu negativnosti

[1] "Business Intelligence is usually defined as the ensemble of methods, systems and technologies that transform data into useful information for the economic activities of a company". (Gaiser 2016)

[2] Bazdan o tem razlaga, da gre v bistvu za revolucijo v smislu siceršnjih družbenih revolucij, poznanih iz zgodovine. Tudi nekateri drugi teoretiki lansirajo v splošno rabo izraz, da gre v navedenih primerih za vojno na področju vohunstva oziroma vohunsko vojno.

in rizika uspešnosti poslovanja gospodarskih subjektov, ki jim praviloma nezakonita dejavnost škodi. In obratno – korist imajo nasprotniki.

Na podlagi predstavitve zgodovine gospodarskega vohunjenja in tveganosti uspešnega poslovanja gospodarskih subjektov, je cilj te naloge prikazati pomembnost in soodvisnost obveščevalne dejavnosti glede na odzive gospodarskih subjektov na gospodarsko vohunjenje. V tem kontekstu pa zaznamo nekatere primere, na katere tudi opozarjajo strokovnjaki, ko poudarjajo vlogo varnostno-obveščevalnih služb v poslovnem svetu ne glede na to, ali so pogojene in vzpodbujene z državnim ali zasebnim virom. V nalogi se torej ciljno opredeljujemo do vzročnosti med gospodarsko obveščevalno dejavnostjo in gospodarskimi subjekti s poudarkom na škodljivosti vdora v poslovne sisteme podjetij. Posebej pa želimo dokazati tudi škodljivost gospodarskega vohunstva glede na poslovno uspešnost gospodarskih subjektov.

V nalogi sta razčlenjena gospodarski oziroma ekonomski del obveščevalnosti (State Economy Intelligence) in obveščevalna dejavnost zasebnega sektorja (Private Intelligence). Rdeča nit je predvsem slednje, saj se ugotovitve osredotočajo na obveščevalne dejavnosti gospodarskega področja. Naloga zajema delovanje in ustroj obveščevalne dejavnosti s poudarkom na gospodarskem področju ter celovit prikaz soodvisnosti gospodarskih subjektov in gospodarskega vohunjenja. Opredeljene so discipline in razmerja med subjekti obveščevalne dejavnosti ter z nekaj empirike prikazana njihova povezanost oziroma hotena/nehotena soodvisnost. Tudi Gaiser gospodarsko vohunstvo člení podobno, zato je v nalogi tudi na tem precejšen poudarek. (Gaiser 2016)

Naloga zajema in opredeljuje vlogo gospodarske obveščevalne dejavnosti nasploh, smisel in koristnost vdiranja v varovane podatke gospodarskih subjektov ter posledičnost tega, praviloma nezakonitega početja. Predstavljeni so nekateri akterji pričujoče problematike ter s tem zajete osnove tako državnega kakor zasebnega resorja, in sicer s ponazarjanjem nezakonitosti ravnanj, ki obstajajo vsaj tako dolgo, kot obstaja konkurenčnost.

1.2 Metode raziskave

Magistrska naloga je deskriptivno delo, zato je uporabljena metoda analize primarnih pisnih virov, metoda analize sekundarnih pisnih virov ter tudi internetnih virov. Na ta način so predstavljeni osnovni pojmi in temeljne strukture dejavnosti ter odvisnosti v obveščevalni dejavnosti, in sicer s poudarkom na gospodarskem vohunjenju. Na podlagi primarnih virov je prikazana normativna urejenost v nekaterih državah in primerjava s Slovenijo. Prav tako je uporabljen institut študije primerov, s katerimi bodo opisani posamezni konkretni primeri delovanja subjektov gospodarskega vohunjenja in protiobveščevalnih služb nasploh.

1.3 Predpostavka, hipotezi in omejitev raziskave

V nalogi je zajeta oziroma opredeljena predpostavka in dve temeljni hipotezi, ki smo jih vsebinsko argumentirali:

- predpostavka, da imajo slovenske in druge obveščevalce službe določen vpliv na gospodarske subjekte;
- hipoteza, da se gospodarsko vohunjenje intenzivira s stopnjo konkurenčnosti in vplivom določenega gospodarskega subjekta na trgu;
- hipoteza, da predstavlja gospodarsko vohunjenje gospodarskim subjektom grožnjo in oviro pri uspešnem razvoju njihove dejavnosti.

Za argumentacijo predpostave in postavljenih hipotez smo obravnavali nekaj izbranih držav območja EU ter Združenih držav Amerike v primerjavi s Slovenijo. Pri tem smo uporabili zgodovinska dejstva, posebej pa smo poudarili zadnje desetletje. V nalogi smo se omejili predvsem na škodljivost gospodarskega vohunstva.

Ob raziskavi področja gospodarskega vohunstva nas je zanimala potrditev predpostavke, da imajo slovenske in druge obveščevalce službe pomemben vpliv na gospodarske subjekte. V nalogi želimo raziskati, pojasniti in potrditi obe zadani tezi, da se gospodarsko vohunjenje intenzivira s stopnjo konkurenčnosti in vplivom

določenega gospodarskega subjekta na trgu ter da predstavlja gospodarsko vohunjenje gospodarskim subjektom grožnjo in oviro pri uspešnem razvoju svoje dejavnosti.

Z izsledki študije gradiva in praktičnih primerov, prikazanih v nalogi, želimo potrditi, da vohunjenje (s konotacijo nelegalnosti) povzroča grožnjo gospodarskim subjektom. Zato menimo, da bo naloga dodaten vir za razjasnitev in zajezitev opisane problematike ter podstat nadaljnjim raziskavam na tem področju.

S predstavljeno raziskavo izbrane problematike, želimo poleg predstavitve dosedanjega dogajanja in dejstev, v znanost pripeljati dodatne poglede na tematiko gospodarskega vohunjenja, kot enega ključnih faktorjev gospodarske uspešnosti države in gospodarskih subjektov. Magistrsko delo prinaša široko strokoven in hkrati poljuden pogled na izbrano temo, ki je zanimiva tudi iz perspektive različnih ved, saj bo nudila strokovno oporo nadaljnjim raziskovalcem.

Z navedenimi izsledki, ki potrjujejo zadani hipotezi, želimo prepričati, da pričujoča naloga prinaša pomemben znanstveni prispevek k osvetlitvi aktualnosti obravnavane teme oziroma problematike.

Čeprav strokovno, pa je pričujoče delo napisano na zadovoljivo poljuden način, dostopen in razumljiv tudi laičnemu bralcu. Prav tako ocenjujemo, da je izbrana tematika zanimiva in izjemno aktualna in bo pritegnila tudi druge raziskovalce te problematike.

Ugotavljamo, da obravnavana tema v slovenskem prostoru nima posebej širokega znanstvenega zaledja, predvsem pa pravnih virov, ki so dobra podlaga za uspešno raziskavo. Iz citiranih in zajetih virov, ki jih navajamo v samem tekstu in v kazalu, smo ugotovili, da obravnavana problematika nudi še veliko prostora za raziskavo, saj se v primeru gospodarskega vohunjenja pojavljajo vedno nove oblike oziroma modus operandi, kar ponuja še poseben izziv in aktualnost.

1.4 Struktura magistrske naloge

Magistrska naloga vsebuje šest temeljnih vsebinskih sklopov s podpoglavji. Nosilna vsebinska poglavja so štiri in zajemajo:

- zgodovinski razvoj obveščevalne dejavnosti s poudarkom na gospodarskem področju;
- pravne podlage v kontekstu dovoljevanja in omejevanja obveščevalne dejavnosti na gospodarskem področju;
- obveščevalno dejavnost na gospodarskem področju s študijami primerov;
- vsebino preventivno-zaščitnih mehanizmov različnih družbenih sistemov zoper obveščevalno dejavnost na ekonomskem področju.

V prvem sklopu je zajetih nekaj zgodovinskih dejstev kot uvod v današnjo aktualnost, saj gre za klasično kontinuiteto dejavnosti, ki bazira na tisočletni tradiciji in virih. Obveščevalna dejavnost namreč obstaja, odkar se je človek samoorganiziral v človeško skupnost. Včasih je bila to vojaška domena, sčasoma pa se je področje razširilo v vse vrste človekovih družbenih interesov. Današnja družba je potisnjena v svet interakcij in posledično so države vedno bolj odvisne od globalnega okolja. Vzporedno s tem deluje obveščevalna dejavnost ob področju politike varnosti tudi na področju ekonomskega razvoja, znanosti in tehnologije. Gre za prepletenost in soodvisnost v družbenih sistemih, kamor obveščevalna dejavnost vse bolj posega. Ključne strateške odločitve mnogokrat temeljijo na izsledkih varnostnih služb, državnih in civilnih, ki imajo svojo zgodovino. Kitajski vojaški strateg Sun Tzu je že v 6. stoletju pred našim štetjem v delu Umetnost vojne opisal pomembnost poznavanja nasprotnika in podatkov, pridobljenih z vohunstvom. Za začetek moderne obveščevalne dejavnosti v gospodarstvu pa lahko štejemo šele drugo polovico 20. stoletja. Več znanstvenikov (med njimi tudi Michael Porter) je ugotavljalo, da mora biti management gospodarskega subjekta podrobno informiran o konkurenci. Porter je poudaril, da mora biti strategija delovanja na trgu podprta z resničnimi, aktualnimi in točnimi informacijami, kar je osnova konkurenčne obveščevalne dejavnosti.

V drugem sklopu so zajeti pravni okvirji delovanja obveščevalnih služb. Za obveščevalno dejavnost (tudi na gospodarskem področju) je pravna podlaga

dejavnosti ključna, saj sicer preide v nelegalnost. Nekateri teoretiki trdijo, da je obveščevalna dejavnost na področju gospodarstva v bistvu ilegalna in kazniva. Mnenja so različna, saj ni možno absolutno trditi, da je vohunjenje oziroma zbiranje javno dostopnih podatkov, torej legalno pridobljenih virov, nezakonito. V nalogi so primerjalno prikazane posebne oblike pridobivanja podatkov na področju protiobveščevalne dejavnosti nekaterih držav Evropske unije in širše. V tem kontekstu je bila najprej pozornost usmerjena v našo državo in njeno pravno urejenost na tem področju s poudarkom na gospodarskem in industrijskem vohunjenju.

Tretji vsebinski sklop se nanaša na konkretno gospodarsko vohunjenje s prikazom nekaterih znanih primerov. Zajeti sta tudi protiobveščevalnost v kibernetskem prostoru in elementi tako imenovanega socialnega inženiringa (dve (po oceni mnogih strokovnjakov) zelo aktualni podpodročji). Prav tako je v nalogi razdelana in ponazorjena tako imenovana državna in nedržavna obveščevalna dejavnost (z vidika aktualnosti v 21. stoletju).

Zadnji (četrti) sklop tega dela naloge zajema sistem zaščitnih mehanizmov, ki jih gospodarski subjekti in države v različnih družbenih sistemih uveljavljajo za zaščito pred obveščevalno dejavnostjo predvsem na ekonomskem področju. Predstavljena so različna izhodišča ekonomske varnosti (tudi v kontekstu odnosa med trgom in državo). Podpoglavje je posebej posvečeno pomenu globalizacije kot ključnemu procesu, ki vsaj od sedemdesetih let prejšnjega stoletja zaznamuje odnos med državo in trgom. Posebej je opredeljen pomen industrijske politike ter pri tem poudarjena makroekonomska stabilnost kot nujni pogoj za gospodarsko rast. Slednje se navezuje na strateški menedžment z mrežnim organiziranjem gospodarskih subjektov, oboje pa je povezano in odvisno od družbenih norm. Vprašanje v tem kontekstu je torej odvisnost uspešnega poslovanja tudi od pozitivnih pravnih norm neke družbe/države, s katerimi le-ta pomaga preprečevati škodljivo gospodarsko vohunjenje v preventivnem in penalnem smislu. Primerjalno je omenjenih nekaj držav in njihovih sistemov kot pregled njihove skrbi za zajezitev gospodarskega in drugih vrst vohunjenja.

Zaključek naloge združuje ugotovitve zatrjevanih dejstev (posebej potrjenih postavljenih hipotez) in nakaže negativne posledice ilegalne obveščevalne dejavnosti na različnih družbenih področjih s poudarkom na gospodarskem področju.

Povzetek je strnjen prikaz obravnavane teme, ki je preveden v angleški jezik in z angleškim prevodom naslova naloge.

2. OPREDELITEV TEMELJNIH POJMOV

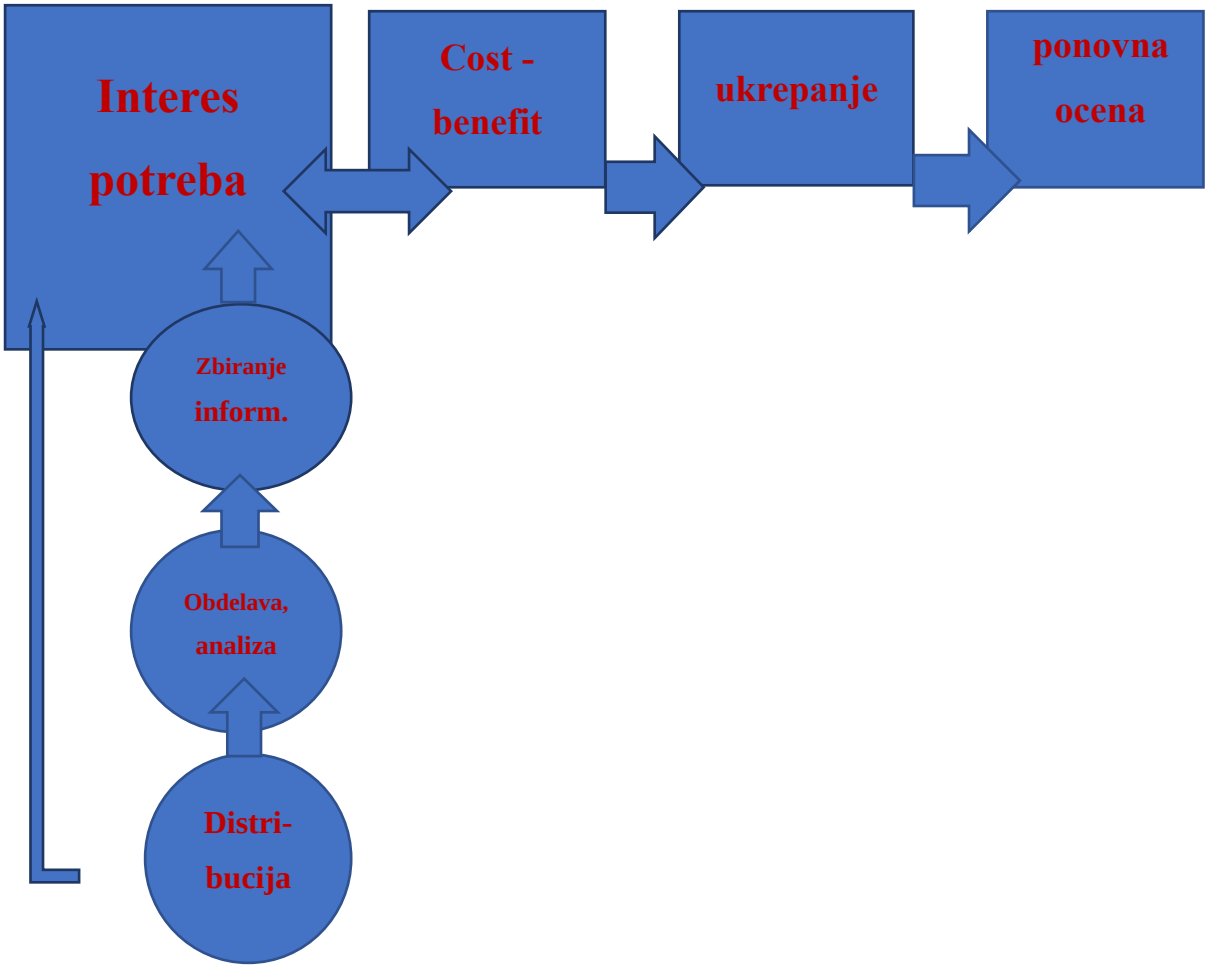
Obveščevalna dejavnost[3] je najpogosteje predmet proučevanja varnostnih študij, ki jo obravnavajo z vidika metod in sredstev obveščevalnega dela ter političnega in strokovnega nadzora nad delom obveščevalnih služb. Tovrstni pristopi z vidika državne suverenosti opredeljujejo obveščevalno dejavnost kot proces načrtovanja, zbiranja in obdelave podatkov ter analiziranja in posredovanja informacij o dogodkih na političnem, vojaškem, ekonomskem, tehnološkem in drugih področjih. Šaponja analitično razlaga vsebino več posameznih segmentov obveščevalne dejavnosti države in drugih subjektov na tem področju. (Šaponja 1999) Pri tem izpostavlja predvsem naslednja področja:

- politike držav, mednarodnih organizacij, državnih zvez in zavezništev;
- gospodarstva posameznih držav in regij v kontekstu mednarodnih gospodarskih tokov;
- znanost in tehnologijo;
- obrambno strateško področje;
- vojaško industrijo;
- jedrsko energijo.

Obveščevalni proces lahko opredelimo tudi s splošno uveljavljenim strokovnim izrazom obveščevalni ciklus, ki v vsaki fazi predvideva tudi povratni tok informacij za zagotavljanje popravkov oziroma odpravljanje potencialnih napak. (Purg 2001, 30) Obveščevalni ciklus se odvija v različnih fazah, ki so v časovni, vzročni, strokovni in uporabni soodvisnosti.

[3] Obstoj obveščevalnih in varnostnih organizacij ne sme biti samemu sebi namen in mora biti odvisen od potreb države, pri čemer obveščevalno-varnostne organizacije nudijo podporo državi oziroma odločevalcem za doseganje nacionalno varnostnih ciljev in zaščito nacionalnih interesov. Podporo nudijo z zaznavanjem, identificiranjem, spremljanjem ter ocenjevanjem tveganj in groženj, ki lahko izhajajo iz tujine ali znotraj države. (Britovšek 2012)

Klasični obveščevalni ciklus lahko ponazorimo tudi z grafičnim prikazom:



Slika 1: Obveščevalni ciklus
Vir: Lastna raziskava

O obveščevalni dejavnosti v ožjem pomenu govorimo takrat, ko je namen zbiranja in analiziranja podatkov samo oblikovanje in posredovanje obveščevalnih informacij, v širšem pomenu pa obveščevalno dejavnost sestavljata še protiobveščevalna dejavnost in tajne operacije. (Purg 2001)

Splošno sprejeta razlaga tajnih operacij je, da gre za modus operandi neposrednega izvajanja zunanje politike, ki jo opravljajo obveščevalne službe, kamor se med drugim

uvrščajo atentati, sabotaže, vzpodbujanje in vzdrževanje uporniških gibanj, sovražna propaganda, iniciacija državnih udarov, kognitivna manipulacija in drugo. Skupni imenovalec taki dejavnosti je državni interes neke vladajoče strukture, ki sicer praviloma zanika svojo vpletenost. Navedene izvedbene oblike tajnih operacij pogosto označujemo kot strategijo posrednega nastopanja med drugim tudi zato, ker so praviloma umeščene med javno diplomacijo in vojno.[4] V sodobnih mednarodnih odnosih so tajne operacije pogosto organizacijsko umeščene v sistem delovanja drugih služb predvsem zaradi civilnega nadzora ali ostalih vej oblasti lastne države in mednarodne skupnosti.[5]

Protiobveščevalna dejavnost je segment splošne varnostne dejavnosti, namenjen preprečevanju in odkrivanju delovanja tujih obveščevalnih služb ter preprečevanju in odkrivanju kaznivih dejanj, usmerjenih zoper varnost države in njeno ustavno ureditev. Protiobveščevalno in obveščevalno dejavnost praviloma opravljajo ločene službe. (Anžič 1996, 59)

V tem kontekstu razlage je potrebno razmejiti obveščevalno dejavnost in vohunstvo. (Barring 1970) Ugotovimo lahko, da je vohunstvo v bistvu vsebinsko ožja dejavnost kakor sama obveščevalna dejavnost. Da gre za vohunstvo, nas usmerja njegova kaznivost, ko se z zbiranjem informacij naklepno pristane na kaznivo dejanje, saj je storjeno po metodah ali s sredstvi za nezakonito zbiranje informacij, ki sicer imajo pravno varstvo glede na zbrane informacije. (Purg 2001, 34)

Ko je govora o državni obveščevalni službi kot obveščevalni dejavnosti v ožjem pomenu, se njena dejavnost lahko razume tudi kot servisna služba izvršne oblasti, saj za odločanje

[4] Strategija posrednega nastopanja je organizirana dejavnost, s katero država in/ali drugi subjekti na mednarodnem in/ali notranje političnem področju poskušajo uresničiti svoje politične, gospodarske, vojaške in/ali druge interese na škodo drugih subjektov, pri tem pa rešitev ne iščejo neposredno s spopadom oboroženih sil, temveč posredno, z raznovrstnimi prikritimi postopki na političnem, gospodarskem, vojaškem in/ali drugih področjih življenja in dela neke skupnosti, z izvajanjem psihološko-propagandnih akcij, ustvarjanjem in/ali kanaliziranjem družbenih kriz, ustvarjanjem in vodenjem politične agenture, izvajanjem državnih udarov itd. in v določenih primerih tudi vodenjem posredniških vojn. (Krunić 1997, 29)

[5] Obstajajo podatki o takšnem prikrivanju zadev (na primer afera Iran-Contra).

o strateških vprašanjih nujno potrebuje pravočasne in celovite informacije ter analizo dogajanj tako v matični kakor drugih državah. Temu so prirejene in na normativi podlagi dovoljene metode dela obveščevalnih služb. (Krunić 1996)

Značilnost teh služb je njihova dejavnost, ki se praviloma odraža v odkritih, prikritih in tajnih metodah dela.[6]

Šaponja izvajanje obveščevalne dejavnosti razvršča v tri skupine:

- Operativne discipline, ki jih izvajajo ljudje neposredno ali posredno in je zanje potrebno operativno delovanje. Sem prištevamo: tajno sodelovanje, tajni odkup predmetov ali podatkov, tajno sledenje in opazovanje, tajno fotografiranje in video snemanje pogovorov, tajno prisluškovanje telekomunikacijam, tajno prisluškovanje in snemanje pogovorov, kontrola računalniških sistemov bank, kontrola pisem in drugih pošiljk, delovanje pod krinko, sodelovanje s partnerskimi službami.

- Tehnične discipline za zbiranje podatkov uporabljajo različna tehnična sredstva in informacijsko tehnologijo. Gre za discipline, pri katerih so pomembna tehnična znanja in oprema. V večji meri tehnične discipline uporabljajo veliki obveščevalno-varnostni sistemi v državah, ki so ekonomsko sposobne menjati sredstva za nakup, vzdrževanje in uporabo teh sistemov. Manjše države uporabljajo le osnovne discipline ali pridobivajo tovrstne podatke na podlagi sodelovanja z večjimi službami.

  Med tehnične discipline štejejo: prisluškovanje (prisluškovanje komunikacijam, uporaba radarskih naprav, odkrivanje in zasledovanje radijskih oddajnikov in radarjev), zbiranje slikovnih podatkov in merjenje količin.

[6] Primer odkritih metod dela je zbiranje in analiziranje informacij, pridobljenih iz javnih virov. Razmejitev med prikritimi in tajnimi metodami je, da gre pri prvih za prikrit namen zbiranja informacij, ki ni nujno nezakonit. Pri tajnih metodah je namen zbiranja prav tako prikrit, a je zaradi načina zbiranja podatkov praviloma kršen pravni red države. Pri izvajanju prikritih in tajnih metod dela na področju protiobveščevalne ali varnostne dejavnosti velja, da morajo biti le-te v skladu z zakonodajo.

- Discipline zbiranja javno dostopnih podatkov, pri čemer gre za zbiranje podatkov, ki so javno dostopni in zanje ni treba uporabljati tehničnih operativnih disciplin. V to skupino prištevamo zbiranje podatkov iz sredstev javnega obveščanja, računalniških medijev in baz podatkov ter druge načine zbiranja podatkov, kot je na primer uporaba strokovne literature. (Šaponja 1999, 80−146)

Svetovna strokovna literatura deli teorijo o organizacijski delitvi zbiranja informacij na dvoje: na zbiranje s človeškimi viri (angleško Humint) in na zbiranje s tehničnimi sredstvi (Techint). Slednje pa se deli na tri segmente: fotografiranje in snemanje (Imint), prestrezanje komunikacij, telemetričnih in elektronskih signalov (Sigint) ter seizmološke, radiološke, kemične in druge meritve (Masint). (Lukanović 2017)

Glede na slovensko rabo strokovnih izrazov na področju, ki ga v nalogi obravnavamo, praviloma s terminološko opredelitvijo obveščevalne dejavnosti ni večjih težav (predvsem glede pristojnosti državnih organov). Ugotavljamo pa, da v slovenskem jeziku še ni zadovoljivega dogovora o ustreznem prevodu nekaterih pojmov in definicij iz angleške, nemške ali francoske prakse. Tak primer je beseda angleškega oziroma francoskega korena *intelligence*. Gre za pojem, ki opredeljuje zbiranje, obdelavo in posredovanje informacij, s čimer se ukvarjajo obveščevalni subjekti.[7]

Izraz ima (predvsem pri nas v laični javnosti) deloma negativno konotacijo zaradi ustvarjene javne podobe obveščevalne dejavnosti v prejšnjem družbenem sistemu.

Jelen prevaja pojem *competitive intelligence* kot konkurenčno obveščevalno dejavnost in meni, da se slovenski izraz za koncept obveščevalne dejavnosti ujema z angleškim izrazom *intelligence.* (Jelen 2008)

[7] Pri nas se je v znanstvenih krogih uveljavil termin poslovna inteligenca kot prevod *business intelligence*. Torej lahko povzamemo, da izraz opredeljuje poslovno inteligenco kot programske prijeme, ki koristnikom omogočajo dostop do podatkov, njihovo analiziranje in izmenjavo z drugimi uporabniki.

Ob zaključku tega poglavja, ki smo ga umestili v nalogo zaradi pomembnosti razumevanja strokovnih izrazov, moramo posebej poudariti, da terminološka nejasnost nekaterih strokovnih izrazov zahteva posebno skrb. Menimo, da bi strokovni in splošno uveljavljeni termini morali biti vneseni v Slovar slovenskega knjižnega jezika z ustrezno strokovno argumentacijo. S tem bi se odpravil dvom v pojmovne dileme, ki jih povzroča poljubno prevajanje strokovnih izrazov iz tujih jezikov (predvsem iz angleščine).[8] Ugotavljamo, da so tujke v našem strokovnem jeziku na različnih področjih pogoste in tudi splošno sprejete. Za naš opisani primer torej menimo, da je treba zadevo nujno ustrezno urediti.

[8] Na podlagi raziskav obravnavanega področja ugotavljamo, da se angleško besedo "intelligence" prevaja z besedo inteligenca. Široko pojmovno ta beseda ne označuje samo sposobnosti povezovanja, sklepanja, učenja, razumevanja (razlaga, zavedena v SSKJ), temveč se jo v določeni praksi uporablja kot informacijo, obvestilo ali obveščanje. Tudi pri oglaševanju računovodskih programov se pogosto pojavlja besedna zveza "poslovna inteligenca", ki pa ne pomeni umske lastnosti subjektov, temveč gre za zbiranje in prikaz podatkov.

3. VRSTE IN KLASIFIKACIJA VUHUNSTVA V GOSPODARSTVU

3.1 Gospodarsko vohunstvo

Dostopna in precej skromna literatura nudi različna pojmovanja gospodarskega vohunstva. Pojmi so sorodno definirani in podobno opisujejo specifiko gospodarskega vohunjenja. Podbregar in drugi teoretiki gospodarsko vohunstvo opisujejo kot nelegalno dejavnost tujih vlad, domačih in tujih podjetij, tujih agentov ali posameznikov, ki s krajo, nepooblaščenim fotokopiranjem, pošiljanjem, nakupom, spreminjanjem ali s prevaro nepooblaščenim osebam omogočajo dostop do poslovnih skrivnosti. Gospodarsko vohunstvo lahko definiramo kot skupek definicij industrijskega in poslovnega vohunstva. (Podbregar 2007) Oba termina pa seveda ne moremo upoštevati kot dva izraza iste dejavnosti, saj je industrijsko vohunjenje ožji in zelo specifični del gospodarskega (ekonomskega) vohunjenja.

Industrijsko vohunstvo je glede na zgoraj navedeno ozka specifična dejavnost gospodarskega vohunstva, ki je prisotna praviloma v zasebnem sektorju. Pri tem gre za kaznivo ravnanje s ciljem izgrajevanja konkurenčne prednosti ob nastanku produkta oziroma pred pričetkom proizvodnje in prodaje. Objekti vohunjenja so predvsem razvojna področja potencialnih konkurentov. Industrijskega vohunstva torej ne moremo enačiti z ekonomsko obveščevalno dejavnostjo, saj je naloga slednje pridobivanje podatkov za potrebe države oziroma njene izvršne oblasti, ki je v ozki soodvisnosti z gospodarstvom lastne države. Seveda pa se v praksi dogaja, da se obveščevalne službe vpletajo v tak način delovanja in pridobivajo podatke za zasebna podjetja, kar se prekriva s hudim navzkrižjem interesov na nacionalni in globalni ravni.

Raziskovalec Jacques Bergier navaja precej konkretnih primerov industrijskega vohunstva in ugotavlja kot skupni imenovalec nezakonite odtujitve idejnih zasnov

oziroma konceptov, procesnih postopkov ali produktov, še preden jih je podjetje uspelo patentirati ali plasirati na trg. (Bergier 2007)

Ko je govora o poslovnem vohunstvu, imamo opravka z nezakonitim odtujevanjem zaupnih podatkov s področja raziskovalne dejavnosti, financ, marketinga, kadrovske politike ter splošnega delovanja podjetij. Vohunstvo po naročilu zajema ob odkrivanju poslovnih skrivnosti tudi analiziranje in ocenjevanje konkurence. (Podbregar 2007) Različni avtorji so bolj ali manj enotni, da se gospodarsko vohunjenje v osnovi deli na dva dela, kar lahko povzamemo tudi tukaj:

1. Notranje gospodarstvo vohunstvo (prikrite metode zaposlenega v gospodarskem subjektu). Pri uporabi prikritih metod insajder zlorabi zaupanje in notranje informacije (pretveza, laž, prevara, sprenevedanje, podkupovanje, prikrivanje prave istovetnosti, prikrivanje resničnih dejstev, zvijače).

2. Zunanje gospodarsko vohunstvo, kjer prikrite metode uporablja tretja oseba (izven strukture gospodarskega subjekta), ki za pridobivanje informacij uporabi tudi tehnična sredstva (avdio-video, tokovna ali svetlobna sredstva, elektronske zapise).

3.2 Gospodarske poizvedbe

Gospodarske poizvedbe so orodje menedžmenta, ki se zaveda pomena informacij v sodobnem načinu poslovanja in gospodarjenja. Predstavljajo močna orodja uprav gospodarskih družb, ki jih le-te uporabljajo za načrtovanje posameznih poslovnih dogodkov, poslovne strategije ali onemogočanje nelojalne konkurence ter preprečevanje nezakonite proizvodnje ali kraje industrijske in intelektualne lastnine. (Dvoršek 2002) Glede dejavnosti na področju gospodarskih poizvedb, ki so nujne za odločanje v gospodarstvu, pa velja, da vohunski subjekti ne uporabljajo nelegalnih metod. Vohunstvo na tem področju lahko strnemo v štiri osnovne sklope:

- Industrijsko vohunstvo (*industrial intelligence)* lahko na kratko definiramo kot zbiranje podatkov o proizvodnji s pomočjo legalnih metod in sredstev ter z namenom ugotavljanja tehnoloških postopkov, strategije in kapacitete gospodarskega subjekta. Cilj je pogosto tudi nelegalna dejavnost preiskovanega podjetja (morebitna nelegalna proizvodnja, dumping, kršitve iz zaščite industrijske lastnine).

- Gospodarsko (ekonomsko) vohunstvo oziroma *business – economic intelligence*[9] razumemo kot zbiranje, organiziranje in uporabo poslovnih informacij na legalen in dostopen način. Gre za orodje managementa, s katerim pridobiva ključne informacije. Pri tem pa je treba razlikovati *business intelligence* od *business espionage*, saj je slednja nelegalna in kazniva zaradi uporabljenih metod in načinov ter ciljev zbiranja informacij. Ob uporabi angleških terminov obeh pojmov z razumevanjem pravzaprav ni težav. Težava nastopi, kot je že zgoraj omenjeno, ob razumevanju slovenskih terminov obeh pojmov, zaradi česar je razlaga definicij nujna.

- Konkurenčno vohunstvo oziroma *competitive intelligence* je zbiranje informacij iz javno dostopnih virov o konkurenci, njenih namerah, ciljih, trženju in drugem. Gre za pripomoček, ki naročniku omogoča lažje prilagajanje svoje strategije konkurenčnemu trgu s specifično in pravočasno informacijo o konkurenčni družbi.

- Gospodarsko protiobveščevalno vohunstvo oziroma *economic counter intelligence* se praviloma v dejavnosti, oblikah in metodah ne razlikuje od državnega, le področje delovanja je usmerjeno v zaščito ekonomskih interesov gospodarskih subjektov. O tem je več govora tudi v ostalih poglavjih te naloge.

---

[9] Laris Gaiser specificira ustroj *economic intelligence* na štiri segmente, in sicer *competitive inteligence, business intelligence, industrial intelligence* in *counter-intelligence.* (Gaiser 2016, 9−10)

Ob zaključku tega podpoglavja je treba poudariti pomembnost razumevanja koncepta obveščevalne dejavnosti. Obveščevalna služba je institucija izvršne veje oblasti in sestavina obveščevalne dejavnosti, medtem ko je v pogledih menedžmenta ekonomska obveščevalna dejavnost legalna in je ne gre enačiti z ekonomskim vohunstvom, ki spada v kriminalno sfero. (Jelen 2008) Glede terminov, o katerih je v tem delu precej govora, tudi Dvoršek priznava, da pojem *gospodarske poizvedbe* ni najbolj primeren, vendar je težko najti skupni izraz za vse vrste zbiranja in analiziranja podatkov za potrebe gospodarstva oziroma za gospodarske subjekte, ki potrebujejo informacije za odločanje o svojih poslih. (Dvoršek 2002)

3.3 Ekonomska obveščevalna in protiobveščevalna dejavnost

Nastanek obveščevalne dejavnosti na ekonomskem in industrijskem področju pogojujemo z razcvetom industrijskega in tehničnega razvoja na globalni ravni. Obveščevalna dejavnost je v najširšem pomenu dejavnost zbiranja, analiz, združevanja in interpretacije podatkov, ki zahtevajo enega ali več vidikov tuje države oziroma operativnega področja, ki je neposredno ali potencialno pomembno za načrtovanje. (Podbregar 2008) Obveščevalno dejavnost v ožjem smislu izvajajo državne institucije, ki imajo zakonska pooblastila za zbiranje tajnih podatkov za potrebe državnih organov v sklopu zagotavljanja in varovanja nacionalne varnosti. Državni organi na podlagi obveščevalnih podatkov sprejemajo pravočasne in ustrezne odločitve pri vodenju politike na političnem, gospodarskem, obrambno-varnostnem in drugih področjih. (Šaponja 2008)

Ekonomska obveščevalna dejavnost se ne ukvarja le z zbiranjem ekonomskih podatkov o drugi državi, ampak tudi z zaščito interesov lastne države pred škodo, ki bi jo lahko povzročila druga država. Zbiranje podatkov na področju gospodarstva ima velik pomen za strukture, ki sodelujejo pri zagotavljanju nacionalne varnosti, saj so ekonomski dejavniki ključnega pomena za vojaško moč neke države, njen politični razvoj ter vodenje zunanje politike. (Purg 2001)

Gospodarsko-ekonomska inteligenca[10] (kot se ta termin v praksi običajno uporablja) je v bistvu disciplina, ki preučuje informacije, ki jih država in gospodarski subjekti potrebujejo pri sprejemanju razvojne strategije in določanju ciljev s prilagoditvijo svojih kognitivnih in odločitvenih zmogljivosti v kompleksnem kontekstu konkurence. Zato je ekonomska inteligenca temeljni del ekonomske geopolitike, saj v bistvu predstavlja orodje držav, v katerih se zasebna in javna sfera tesno prepletata. (Clerc 1997)

Naloga obveščevalne dejavnosti je pridobivanje podatkov, medtem ko je naloga protiobveščevalne dejavnosti zaščita le-teh. Protiobveščevalno dejavnost pravzaprav lahko razdelimo tudi na pasivno in aktivno, kjer pasiva predstavlja klasične varnostne ukrepe za zaščito informacij (računalniška zaščita). Aktivna protiobveščevalna dejavnost pa je namenjena aktivnemu odkrivanju, dezinformiranju in tudi manipuliranju tuje obveščevalne dejavnosti. (Britovšek, Ulcej in Sotlar 2007)

3.4 Tajnost podatkov

Tajnost in skrivnost sta pojma, ki ju nemalokrat pojmovno enačimo. Anžič navaja, da je skrivnost glede na prvi pomen nekaj, česar se ne da razumeti, dojeti ali pojasniti. Za pojem tajnosti pa pravi, da ni nekaj neznanega, temveč gre pri njeni vsebini za znane stvari, ki jih posameznik, institucija ali država nočejo narediti dostopne širši javnosti. (Anžič 2000) Zanimivo je dejstvo, da se tako Brezovšek kot Črnčec z Anžičevo opredelitvijo ne strinjata v celoti, saj naj bi po njunem Slovar slovenskega knjižnega jezika pojem tajnosti izpostavil kot sinonim za skrivnost. Za Scheppela pa je tajnost družbeni mehanizem, prek katerega so interesi in nameni nekaterih družbenih akterjev, ki sprejemajo vsakodnevne odločitve, spremenjeni v neenakost v

[10] Gaiser to področje opredeli: ”Synthesizing this, we could say that we are talking about business intelligence when a company gathers and analyses information to optimize their own position on the market. When they do this on their competitors, we enter the field of competitive intelligence; while when day carry out the same activity in a covert manner against a competitor, we are talking about industrial espionage”. (Gaiser 2016)

znanju. Tajnost pojmuje kot del informacije, ki jo eden ali več družbenih akterjev namerno skriva pred drugimi družbenimi akterji. (Brezovšek in Črnčec 2007)

Zakon o tajnih podatkih[11] definira tajni podatek kot dejstvo ali sredstvo delovnega področja organa, ki se nanaša na javno varnost, obrambo, zunanje zadeve ali obveščevalno in varnostno dejavnost države, ki ga je treba zaradi razlogov, določenih v tem zakonu, zavarovati pred nepoklicanimi subjekti in je v skladu s tem zakonom določeno in označeno za tajno. Zakon v 5. členu opredeljuje tajni podatek kot pojem, s katerega razkritjem bi lahko nastale škodljive posledice za varnost države ali za njene državne, politične in gospodarske koristi.

Opredelitev tajnosti v Zakonu o tajnih podatkih razlaga Jelen kot tajne podatke, do katerih lahko gospodarske družbe dostopajo zaradi izvajanja zakonsko določenih nalog, in tajne podatke, ki so produkt in last neke konkretne gospodarske družbe in predstavljajo njeno poslovno skrivnost. Zato je bistveno za obstoj gospodarske družbe, da se podatki ustrezno zavarujejo pred nepooblaščenim razkritjem. (Jelen 2008)

3.5 Poslovna skrivnost

Odkar človek ustvarja in izumlja, svoje produkte tudi skriva. To jemlje kot poslovno skrivnost. Nič drugače ni glede države in gospodarskih subjektov. Empirika na tem področju nam nudi veliko dokazov. Razvoj na tem področju se stopnjuje premo sorazmerno glede na človekovo tehnološko kreativnost in ustvarjalnost. Kot nekoč, še toliko bolj pa danes, se pripisuje zaščiti poslovne skrivnosti velik pomen, saj interesi, razlogi in vzroki za vohunjenje ne pojenjajo.

V našem pozitivnem pravu obstaja specialni predpis iz leta 2009, Zakon o gospodarskih družbah, ki v 39. členu opredeljuje, da se za poslovno skrivnost štejejo podatki, katere določi družba s pisnim aktom. Gospodarski subjekt je dolžan seznaniti

[11] Člen 5 (Zakon o tajnih podatkih, Uradni list RS, štev. 87/1, 2006).

vse poslovne subjekte (družbeniki, delavci, člani organov družbe in druge osebe, ki so z družbo povezane) o obligacijah v podjetju, ki se nanašajo na varovanje poslovne skrivnosti. Pojem poslovne skrivnosti zajema različne podatke, ki bi ob razkritju nepooblaščenim pomenili grožnjo ali škodo podjetju. Ob tem je treba poudariti, da podjetje kot poslovno skrivnost ne sme določiti podatkov, ki so po zakonu lahko javni ali bi s tem kršilo pravni red države ali bi bili v nasprotju z veljavnimi uzanci ter dobrimi poslovnimi običaji. Omeniti velja tudi 39. in 40. člen navedenega zakona, ki opredeljujeta način in odgovorne subjekte za varovanja poslovne skrivnosti.[12]

Kot poslovna skrivnost se torej ne štejejo podatki, ki jih zakon opredeljuje kot javne. Jelen poslovno skrivnost razlaga kot informacije o gospodarski družbi, ki predstavljajo dobrino za podjetje, do katere imajo dostop z internim aktom določene (pooblaščene) osebe. Gospodarska družba sama določa način, kateri so ti poslovni podatki in način njihovega varovanja. Običajno gre za podatke o trženju, kadrih, ekonomskem potencialu in položaju družbe ter morebitno konkurenčno prednost na trgu. Zato gospodarski subjekti sprejemajo ustrezne interne akte, v katerih opredelijo področje varovanja poslovnih skrivnosti in sankcije za kršitelje. (Jelen 2008) Katalog poslovnih skrivnosti zajema določene podatke, znanja in vrednosti kot podjetniško sredstvo v konkurenčni tekmi na trgu. S poslovno skrivnostjo so zavarovana znanja o načinu in postopku organiziranja določenega dela, tehnologij, informacij o poslovnih partnerjih, finančnih podatkih ter vrsta drugih informacij, ki so se zbirale in nastajale v nekem obdobju ter so bile ali so še vedno povezane s poslovanjem in stroški. (Ivanjko 2003)

Kot je bilo v tem delu že omenjeno, se z zakonom opredeljeno varovanje poslovne skrivnosti nanaša na dve kategoriji ljudi: v prvo sodijo družbeniki, zaposleni, člani organov in druge osebe, ki znotraj družbe in za družbo opravljajo delo na podlagi

[12] Navedeni predpis obligacijo varovanja podatkov širi tudi na tretje osebe, v kolikor vedo ali bi glede na naravo podatkov morale vedeti, da so le-te poslovna skrivnost. Prav tako ni dovoljeno ravnanje, s katerim bi tretje osebe v nasprotju z zakonom in voljo družbe pridobivale podatke, ki so poslovna skrivnost.

civilnopravnih pogodb, v drugo skupino pa se razvrščajo osebe izven gospodarske družbe, ki lahko pridejo do informacij, ki jih gospodarski subjekt opredeljuje s svojimi pravili kot poslovno skrivnost, te osebe pa vedo ali pa bi glede na naravo podatka morale vedeti, da gre za poslovno skrivnost. Takšna širitev dolžnosti varovanja poslovne skrivnosti na tretje osebe oziroma osebe zunaj družbe pomaga preprečevati zlorabe poslovnih skrivnosti oziroma gospodarsko vohunstvo. (Podbregar 2008) Tako imenovane tretje osebe izgovarjanje v kazenskih postopkih na nepoznavanje internih aktov podjetja krivdno ne odvezuje, saj nepoznavanje predpisov, ki bi jih sicer glede na naravo poslovnosti morale poznati, kot rečeno, ne odvezuje krivde. Tudi po splošnem pravnem načelu *ignorantia iuris nocet*.

Ugotavljamo, da je odtujitev poslovne skrivnosti običajno prikrita in časovna odmaknjena ter v odvisnosti od posredovanja informacije ali produkta na tržišče. Podjetje v normativi o poslovnih skrivnostih opredeli nematerialno dobrino in dovoli seznanitev le ozkemu krogu pooblaščencev. Zato je zlorabo slednjih še posebej težko zaznati, podjetje pa svoje poslovne skrivnosti izgubi trajno, zaradi česar nastopi nepopravljiva škoda. V kolikor pa gre za materialno dobrino, je le-ta opazna običajno dokaj hitro, za podjetje pa obstaja večja možnost poprave poslovne škode. Seveda obstaja tudi pravna pot, kjer se storilca kazensko preganja in terja odškodnina. Ti postopki so običajno dolgi in v mnogih primerih podjetje pred koncem procesa več ne obstaja. Modus operandi storilcev je tudi daljše časovno odtujevanje poslovnih skrivnosti ali dobrin, saj se le-te lahko odtujujejo po delih in oškodovano podjetje tega takoj ne opazi, čeprav določena škoda v podjetju kljub nevednosti nastaja. Praksa nam ponuja še en način odtujevanja oziroma pridobivanja poslovnih skrivnosti, ko to počno znane osebe, sorodniki, vplivneži, torej ljudje, ki jih dobro poznamo in jim zaupamo.

Velja splošna in strnjena ugotovitev, da gre pri odtujitvi poslovne skrivnosti za zlorabo, izdajo in za gospodarsko vohunstvo. Pri vzpostavljanju učinkovite zaščite poslovne skrivnosti je pomembno, da poznamo razliko med poslovno skrivnostjo in patentom. Povezavo med poslovno skrivnostjo in patentom predstavlja izum. Izum lahko zaupamo zaščiti države kot patent, kar pomeni, da ga ne bo mogoče razbrati kot

skrivnost do te mere, da bi bila uporabna brez dovoljenja tretjemu. Obstaja tudi zaščita izuma kot poslovna skrivnost. (Kop 1995)

V tem poglavju smo argumentirano ugotovili, da naša zakonodaja sicer sledi svetovnim trendom na področju gospodarskega vohunjenja, vendar odzivnost ni optimalna. Posebej to velja za področje klasifikacije kaznivih dejanj in kriminalizacije pojavnih oblik, ki so ključne za dosego učinkovite pravnomočnosti obsodb na sodišču. Pojavne oblike in metode nezakonitega vohunjenja se spreminjajo tudi z razvojem tehnologije, čemur kazenskopravna stroka ne sledi dovolj učinkovito. Ker običajno nove pojavne oblike vohunjenja izvirajo pretežno iz tujine, je sinergija naših organov pregona s tujimi nujna.

Zato menimo, da bi učinkovitejši kazenskopravni postopki zoper akterje nezakonitega vohunjenja bistveno prispevali k zajezitvi tega problema tudi kot generalna prevencija. Prav tako menimo, da je širitev dolžnosti varovanja poslovne skrivnosti na tretje osebe, torej izven napadenega gospodarskega subjekta, pomembna preventivna komponenta za učinkovito preprečevanje gospodarskega vohunstva.

4. GOSPODARSKA OGROŽENOST KOT POSLEDICA VOHUNJENJA

Nekoliko globlji pogled v zgodovinskost vohunstva nam razkrije, da segajo zametki gospodarskega vohunjenja tisočletja nazaj. Menimo, da je tudi vohunstvo privedlo do prvih patentiranj človekovih iznajdb, ki so se nanašale na dobro varovane skrivnosti (upogljivo steklo, tehnike barvanja svile, način pridobivanja barv v slikarstvu, eksplozivna telesa in kemikalije ter drugo). Na splošno pa nam zgodnji zametki vohunstva dokazujejo, da gre večinoma za prepletanje političnih in vojaških interesov z ekonomskimi, skupaj pa tvorijo splet strateških interesov. (Jelen 2008) Bergier meni, da je industrijsko vohunstvo starejše od vojaškega. Kot prvi primer industrijske skrivnosti navaja iznajdbo ognja, nato način obdelovanja kremena, skrivnost pridobivanja svile.[13] (Bergier 1974) Kitajska je bila (med drugim tudi domovina svile in trdega porcelana) zelo razvita dežela in seveda logično najatraktivnejša tarča za industrijske vohune. (Dvoršek 2004)

Dvoršek meni, da primer kovača Foleya[14] ponazarja gospodarske poizvedbe, kjer se združijo interesi zasebnika z interesom države proti enakim subjektom nasprotne strani, ki imajo domnevno boljšo tehnologijo in dobro gospodarstvo. Posameznik bi imel konkurenčno prednost pred drugimi na račun poznavanja sodobne tehnologije in inovativnih idej. Za državo je skupina naprednih posameznikov zagotavljala dobro

[13] Omenjeno sega daleč v našo zgodovino in ponuja dogodek ali legendo, ko je kitajska princesa zapustila obzidje domovine in pobegnila z ljubimcem v Indijo. Na glavi naj bi nosila pokrivalo, ovenčano z rožami, v katerih je bila skrita sviloprejka, tedaj gojena samo na Kitajskem. Ob prihodu v Indijo naj bi pokrivalo s sviloprejkami izročila ljubimcu in na ta način skrivnost pridobivanja svile za vedno prenesla v drugi del sveta, Indijo. Največji uvoznik svile v tedanji evropski celini je bilo Vzhodnorimsko cesarstvo, ki jo je uvažalo s pomočjo perzijskih trgovcev. Cesar Justinijan je v 6. stoletju v kitajski del province v Indiji poslal po sviloprejke menihe, ki so ličinke prinesli skrite v votle bambusove palice in omogočili cesarju posel mimo osovražene Perzije.

[14] Velja, da je bil prvi industrijski vohun angleški kovač Foley, ki je ugotovil, da je njihovo jeklo slabo. Preoblečen v berača in godca se je potikal po celinskih kovačnicah in sledil kovanju ter obdelovanju jekla. Po vrnitvi na otok je pridobljeno znanje združil s prejšnjo prakso in uspel pridobiti za tiste čase neprekosljivo jeklo.

pozicijo na globalnem trgu, splošno pa je znano, da je moč države odvisna od njene ekonomske razvitosti. (Dvoršek 2008)

Tudi Bergier poudarja pomen in ključno pri zaščiti produktov – patentiranje iznajdb. Po njegovem mnenju se s patentiranjem počasi zaključuje tedanje obdobje industrijskega vohunjenja, ki ga sicer imenuje kot obrtniškega in poudarja prelomnico v letu 1791, ko so se v francoski zakonodaji o patentih prvič uzakonile pravice iznajditelja.

Po navedenem obdobju se je pričela prava ekspanzija gospodarskega vohunjenja, pogojena tudi z iznajdbo parnega in predilnega stroja. Predvsem iznajdba predilnega stroja (in vohunstvo v tem kontekstu) nam daje zanimiv primer gospodarskega vohunstva po naročilu in prizadevanje za zaščito ukradene skrivnosti.[15] (Kop 1995) Vojni za nove pridobitve je sledila vojna za kavčuk in s patentom za vulkanizacijo kavčuka[16] si je leta 1791 Charles Goodyear pridobil monopol. (Bergier 1974)

Očitno dejstvo je, da so vohunski uspehi pospešili potrebo po ustanovitvi organizirane industrijske zaščite. V literaturi najdemo nekaj zgodovinskih poskusov organiziranja podjetij in držav, ki so doumele, da je treba za zaščito intelektualne in poslovne lastnine najti učinkovitejšo zaščito, ki bi segala preko meja posamezne države. Med pionirji najdemo ameriško agencijo Pinkerton, imenovano po ustanovitelju Alanu Pinkertonu, ki je bil prekaljeni vodja vohunske in protivohunske mreže severnega dela Amerike. Kot trdijo viri, je ob industrijskem vohunjenju po naključju odkril politično zaroto južnjakov za umor predsednika Abrahama Lincolna. Namera je bila tedaj preprečena, a se je, kljub visoko poudarjeni obveščevalnosti, pokazalo še danes

[15] Kop opisuje podkupovanje nemškega trgovca Brugelmanna, ki je s pomočjo vohunov pridobil varovano skrivnost predilnih strojev in jo zavaroval na način, da so morali zaposleni podpisati notarsko overjeno izjavo o molčečnosti (za kršitev je bila zagrožena dosmrtna zaporna kazen). (Kop 1995)

[16] Industrija kavčuka je postala najpomembnejši cilj gospodarskih vohunov, ki so kljub vsem zaščitnim ukrepom ukradli več tajnih formul za obdelavo kavčuka. Industrijskemu vohunu Henryju Wickhamu je uspelo, da je iz Brazilije, domovine kavčuka, pretihotapil semena v Veliko Britanijo, od koder so nato sadike razposlali po vseh svojih kolonijah (Indijo, Cejlon, Borneo …). Wickhama je za njegov vohunski prispevek kraljica Viktorija povzdignila v plemiški stan. (Kop 1995)

veljavno dejstvo, da popolne varnosti ni, saj je bil predsednik Lincoln kasneje vendarle žrtev atentata.

4.1 Novejši zgodovinski razvoj obveščevalne dejavnosti in globalizacija

Če za dve stoletji preskočimo v uvodu tega poglavja omenjeno primerjalno zgodovinskost industrijskega vohunstva, se moramo ustaviti v obdobju okoli leta 1968, v trdih časih real socializma za Vzhodno Evropo in znani invaziji sovjetskih enot na Češkoslovaško ter poudariti pojav nove oblike industrijskega vohunstva. Šlo je namreč za pojav tako imenovanega intelektualnega vohunjenja oziroma za nezakonito prilaščanje podatkov s pomočjo računalniškega sistema. Kot običajno, so imeli težave tudi organi pregona, saj niso uspeli slediti napredni tehnologiji, ki je prehitevala pravno. Med izredno ogroženimi je bil tudi centralni računalnik ameriške davčne uprave, saj so na podlagi računalniških vdorov industrijski vohuni izsiljevali milijone industrialcev, trgovcev in poslovnežev. (Bergier 1974)

Globalizacija in interesne sfere so tedaj (čas tako imenovane hladne vojne in tik pred njo) potisnile dve vodilni sili v svetu, ZDA in Sovjetsko zvezo, v intenziviranje vohunske dejavnosti in posledično tudi ostali svet. Sovjetski zvezi je uspelo s pomočjo vohunske tehnologije in vohunov pridobiti najbolj varovano ameriško skrivnost – iznajdbo atomske bombe. Konec hladne vojne je pomenil nujo po sodelovanju tudi na obveščevalnem področju. Nasprotno pa je vohunstvo na gospodarskem področju tekmovalnost samo še poglobilo in zaostrilo. (Beck 2003) Čeprav zavezane k sodelovanju, so pravzaprav partnerske države ZDA, Francija, Izrael in Velika Britanija druga proti drugi izvajale močno gospodarsko vohunstvo. (Čaleta 2008) Zelo podobno se je dogajalo tudi na azijskem območju.

Ekonomska stabilnost je pravzaprav temeljni pogoj razvoja in napredka družbe, saj njena nestabilnost lahko resno ogrozi varnost v državi in posledično v svetu. Dokazov v zgodovini najdemo veliko, eden izmed njih je zagotovo recesijska kriza. Ekonomska inteligenca je temeljni del ekonomske geopolitike, saj gre za orodje, ki

ga uporabljajo države in sta javna in zasebna sfera tesno prepleteni, sta celo soodvisni. Varnost države naj bi razumeli v smislu zagotavljanja varnosti in ekonomske blaginje njenim prebivalcem. V tem okviru sta tako državna kot civilna varnostna komponenta pomembnega značaja ter v subordinaciji in medsebojno prepleteni. Če je država čezmerno agresivna, notranje represivna ali preslabotna, da bi vladala učinkovito, ogroža varnost državljanov. Skrb za varnost ljudi pa se seveda razteza čez državne meje. Za naše razumevanje je pomembno zavedanje, da je varnost ljudi v enem delu sveta pogoj za varnost ljudi drugje. Varnost držav ter ohranjanje mednarodnega miru in varnosti, kar je prvi cilj Ustanovne listine Združenih narodov, je možno uresničiti samo tam, kjer so ljudje osvobojeni strahu pred nevarnostjo umora, preganjanja, zlorabe in omejevanju ekonomske varnosti. Državna varnost nima nobene moralne legitimitete, če je vzpostavljena na račun ljudske varnosti. Vsakršno omejevanje varnostno-obveščevalnega sistema v eksluzivi države pomeni nasprotovanje ljudski iniciativi v skrbi za osebno blaginjo, kamor spada tudi sfera civilnega oziroma zasebnega varovanja ekonomskih dobrin gospodarskih subjektov in posameznika. Slehernemu človeku mora biti dovoljena in konstitualno omogočena svobodna izbira, komu in kakšni organizacijski strukturi bo zaupal svoje premoženje, varnost in eksistenco. (Zinrajh 2005)

Čeprav je imel konec hladne vojne velik vpliv na razmah aktivnosti gospodarske obveščevalne dejavnosti, metode delovanja niso novodobno orodje tržnega prostora. Kot je bilo ugotovljeno, je dejavnost prisotna že tisočletja, medtem ko pride proti koncu 20. stoletja z zmanjševanjem verjetnosti globalnih konfliktov do ekspanzije obveščevalnih aktivnosti na gospodarskem področju in s tem do neke mere izenačevanja pomembnosti obveščevalnih informacij vojaškega in ekonomskega značaja. V obdobju hladne vojne sta se tako obveščevalna kot protiobveščevalna dejavnost osredotočali predvsem na vojaško in politično področje, medtem ko so v novodobnem trenutku ločnice med zasebnim in javnim sektorjem zabrisane, številna podjetja so vsaj posredno v državni lasti, posebnost pa je, da se vse pogosteje tudi gospodarstveniki pojavljajo kot politiki in delujejo celo v upravnih in nadzornih odborih multinacionalk. Gospodarska moč in prevlada sta postali prav tako pomembni kot vojaška moč, obe pa sta v subordinaciji, ustroj obveščevalne dejavnosti pa se je preoblikoval.

Razmah obveščevalne dejavnosti na ekonomskem področju ni pogojen samo z usahnitvijo hladne vojne, temveč časovno sovpada z razcvetom razvoja sodobne elektronike in računalništva. Oboje je generiralo gospodarski razvoj, ki je postal eden ključnih strateških ciljev vseh držav. Hkrati pa so bili tudi dani pogoji razcvetu obveščevalne dejavnosti.

Kot smo v raziskavi ugotovili, se postavlja gospodarsko vohunstvo kot vodilno po vsebini in pomenu v primerjavi z drugimi vohunskimi dejavnostmi, ker je v zadnjih desetletjih doživelo velik razmah. Vzroke za razmah pripisuje Čaleta tudi internetni tehnologiji in političnim spremembam, ki so v svetu globalne tehnologije spremenile metode nedovoljenih posegov v poslovne skrivnosti in vrednote, katerim je botrovala visoka mobilnost zaposlenih. Zvestoba posameznika enemu podjetju pa je zdrsnila z vrednostne lestvice. (Čaleta 2008)

Ocenjuje se, da v moderni globalni ekonomiji ni več realnih razlikovanj med nacionalnimi in mednarodnimi gospodarskimi odnosi. Nacionalna gospodarstva, razen redkih izjem, niso nič več izolirana okolja, v katerih bi zgolj domače razmere vplivale na končne rezultate. (Gregory 1977) Tudi po ocenah kitajskih oblasti predstavljata prvi dve dekadi enaindvajsetega stoletja strateške možnosti za osredotočanje držav na zagotavljanje gospodarske rasti, neodvisne inovacije, znanstveni in tehnološki napredek ter razvoj na področju obnovljivih virov energije. V svetovni gospodarski prostor se umeščajo dejavniki, ki bodo na področju informacijskih in komunikacijskih tehnologij onesposabljali varnostne mehanizme in omogočali nadaljnje zbiranje občutljivih informacij gospodarskega in tehnološkega značaja.[17] Naraščanje kompleksnosti in nasičenosti kibernetskega prostora nudi vse večje možnosti prikrivanja in otežuje pregon storilcev. Število telekomunikacijskih in multimedijskih naprav, ki je že do 2015 naraslo na več kot petindvajset milijard in skorajda nekontrolirano raste, bo rezultiralo s povečanjem ciljnih tarč pridobivanja informacij. Pričakuje se, da bo tak ekonomski premik povzročil premik korporacij in državnih organizacij v kontekstu uporabe lastnih računalniških oziroma aplikacijskih

[17] Ugotovitve so bile predmet razprave predstavnikov podjetja Cisco Systems na konferenci NCIX-a novembra 2010.

resursov. Prehod na tako imenovano Cloudy Computing oziroma oblačno računalništvo predstavlja ceneno alternativo klasičnemu delovanju s strežniki in ponuja varnostne rešitve ter hkrati nevarnost povečanja priložnosti za krajo in manipulacijo s podatki.

Za naš primer obdelave gospodarskega in tudi siceršnjega vohunstva se velja dotakniti tudi kulturnih sprememb. Ocenjuje se, da zahodna delovna sila stremi k zmanjševanju razlikovanja med zasebnostjo in delovnimi obveznostmi, kar terja dostop do sistemov in informacij od koderkoli. Tudi geopolitični premiki predstavljajo nadaljnjo globalizacijo političnih, vojaških in predvsem gospodarskih ukrepov, saj državne meje in kontinenti ne predstavljajo posebnih ovir, razen tehnične nedostopnosti do svetovnega spleta.[18] Gaiser ocenjuje, da Slovenci nismo znali unovčiti dejanske prednosti naše zemljepisne lege, saj se očitno dojema, da so pogledi na geopolitiko še vedno obremenjeni in pod vplivom polpretekle zgodovine. (Gaiser 2010) To velja tudi za področje ekonomije.

Aktualnost današnjega časa je tudi dejstvo, da je vedno več nekoč skrbno varovanih skrivnosti industrije in države pravzaprav dostopnih vsakomur, saj so na voljo celo v strokovnih revijah in drugih publikacijah ter na spletu. Imamo opravka z OSINT metodo, s katero se informacije pridobivajo iz javno dostopnih virov. (Dvoršek 2004) Treba pa je dodati, da se vse bolj aktualno globalno vohunjenje izvaja s pomočjo visokotehnoloških opazovalnih in prisluškovalnih sistemov ter s pomočjo ustrezno razvejane satelitske mreže.[19] (Jelen 2008)

Ko v kontekstu vohunjenja omenjamo globalizacijo ter vpliv na ekonomske tokove in interesne sfere v svetu, ne moremo mimo ameriške politične vohunske afere Watergate. Afera je izbruhnila v sedemdesetih letih 20. stoletja, ko so neznanci 17. junija 1972 vlomili v prostore poslovne stavbe Watergate, kjer je bil sedež Demokratske stranke v Washingtonu. Afera je bila razkrita šele z informacijo o

[18] Več o tem v gradivu The Office of the National Counterintelligence Executive, 2011.

[19] Naj omenimo sistem Echelon, ki ga je razvila ameriška NSA. Ima nevojaške naloge in pokriva območje celotnega planeta.

denarnem toku med storilci in republikansko komisijo za ponovno izvolitev Richarda Nixona, ki je bil v času afere republikanski predsednik ZDA. Glavni operativni cilj Nixonove administracije je bilo vohunjenje za tedanjo opozicijo, torej demokrati. Vlomilci so prejeli navodila, da je treba fotografirati načrte Demokratske stranke za prihodnje volitve in namestiti prisluškovalne naprave v telefone njihovih vodilnih članov. Naprave so nekaj časa delovale brezhibno, nato pa je prišlo do okvare in odločevalci so se odločili za ponovni vlom, pri čemer pa jih je zalotil oskrbnik stavbe, ki je obvestil lokalno policijo. Policija je storilce prijela in flagrante, sodišče pa jih je obsodilo zaradi storitve kaznivih dejanj vloma, zarote in kršenje zveznih predpisov o prisluškovanju. Preiskovalci FBI so kasneje ugotovili, da je bil eden od prijetih vlomilcev neposredno povezan s predsednikovo administracijo, ostali pa so bili nekdanji agentje obveščevalnih služb. Denar, ki so ga storilci prejeli za izvedbo akcije, pa je bil del črnega fonda komisije za ponovno izvolitev Richarda Nixona. Ker bi razkritja lahko vplivala na ponovno Nixonovo izvolitev, je CIA prejela navodila predsednikovega kabineta, kako naj ovira preiskavo FBI. Šlo je za hud konflikt interesov in vmešavanje CIA v pristojnosti zvezne policije FBI (ki je bila v Hooverjevih časih neodvisna organizacija), kar je pri uslužbencih FBI vzbudilo nestrinjanje, še posebej pri posebnem agentu Marku Feltu[20], ki je bil evidentiran kot potencialni kandidat za direktorja FBI. Felt je kritično ocenjeval aktualnega direktorja FBI L. Patricka Grayja, ki je osebno posredoval informacije o preiskavi Watergate Nixonovi administraciji ter s tem aktivno posegel v afero in prikrivanje dokazov. Prav slednje naj bi vzpodbudilo posebnega agenta Felta h kontaktiranju novinarjev časopisa The Washington Post Boba Woodwarda in kasneje še Carla Bernsteina, kar je imelo za posledico uvedbo uradne preiskave. Preiskovalci in tožilci so ugotovili, da

[20] Mark Felt se je rodil leta 1913 v zvezni državi Idaho. Leta 1942 je vstopil v vrste FBI in se vztrajno vzpenjal po birokratski lestvici. Tik pred smrtjo direktorja FBI J. Edgarja Hooverja leta 1972 je bil tretji človek FBI. Po Hooverjevi smrti je bil manj kot dve leti namestnik direktorja FBI, potem pa je odstopil. Felt je bil glavni vir preiskovalnih novinarjev, ki sta razkrinkala afero Watergate, kar je pripeljalo leta 1974 do odstopa tedanjega ameriškega predsednika Richarda Nixona. Predsednik Nixon in njegovi svetovalci so domnevali, da je bil Felt vir, ki je Nixonovo administracijo neposredno povezal z vdorom v prostore ameriške Demokratske stranke v pisarniškem kompleksu Watergate leta 1972. Vir informacij sta bila novinarja časopisa The Washington Post Bob Woodward in Carl Bernstein, kar je posledično spodneslo Nixona s predsedniškega položaja, Felt pa je priznal šele maja 2005.

je v Beli hiši nov snemalni sistem in so magnetne trakove, razen tistih, ki jih do leta 1974 Nixon ni hotel izročiti, zasegli. S trakov je bilo jasno razvidno, da je Nixon ne samo vedel, ampak tudi ukazal prisluškovanje in oviranje preiskave. To je imelo za posledico njegov odstop avgusta 1974.

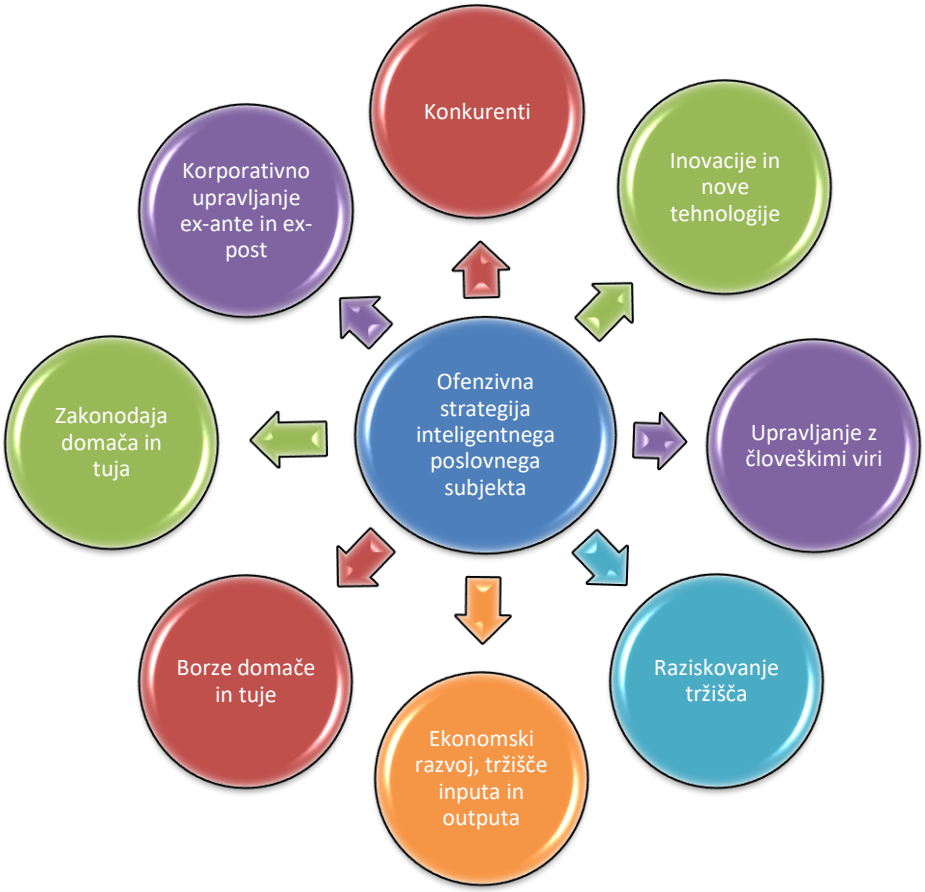
4.2 Obveščevalna dejavnost na gospodarskem področju

Na splošno lahko navedemo, da so akterji oziroma subjekti, ki delujejo na področju gospodarskega vohunstva, nacionalne obveščevalne službe, zasebno obveščevalne službe oziroma podjetja, interesna združenja in posamezniki, gospodarske korporacije in tudi drugi gospodarski subjekti. Za zaščito svojih nacionalnih gospodarskih interesov sprejema sleherna država ustrezno nacionalno strategijo. Osnovne dejavnike, ki vplivajo na uspešnost strategije, lahko ponazorimo tudi s shemo:

Slika 2: Vpliv dejavnikov na strategijo gospodarske varnosti
Vir: Lastna raziskava

Za uspešno zavarovanje svojih ekonomskih interesov bi moral sleherni gospodarski subjekt imeti tudi svojo (tako imenovano ofenzivno) politiko, s katero bi strateško učinkovito obvladoval informativno obveščevalno dejavnost za prestrezanje podatkov

o konkurenci in za lastno zaščito. Takšna strategija bi morala vsebovati ustrezni operativni načrt in vsaj (kot v spodnji shemi) navedene dejavnike:



Slika 3: Ofenzivna strategija zoper poslovno vohunstvo
Vir: Lastna raziskava

Kot je bilo že omenjeno, imajo pri nas pristojnosti za legalno delovanje in pravno podlago za uporabo posebnih metod in sredstev pri pridobivanju tajnih podatkov trije obveščevalni subjekti: SOVA, OVS in policija. Iz tega izhaja, da drugi subjekti ki pri zbiranju podatkov uporabljajo prikrite metode in sredstva, torej to počnejo nezakonito, kar konkretneje raziskujemo tudi v tej nalogi. Omeniti je treba, da so običajno žrtve gospodarskega vohunstva perspektivni in inovativni gospodarski subjekti, ki imajo sicer konkurenco na trgu. Ugotovimo lahko, da se naša podjetja na

mednarodnih trgih spopadajo z močno konkurenco tudi zato, ker so glede na velikost tržišča v Sloveniji relativno majhna. A vendarle opozarjajo nase s svojo kvaliteto in prodornostjo.[21] Seveda Slovenija ni nedotakljiva oaza, ki gospodarskega vohunjenja ne bi poznala ali se ji ta vrsta kriminalitete ne bi dogajala.[22]

V bistvu so lahko gospodarski vohuni vsi subjekti, ki želijo priti do pomembnih poslovnih skrivnosti ne glede na to, ali so del sistema, v katerem delujejo, ali izven njega. Običajno so za vohunjene posameznikov pomembni predvsem trije motivi: lasten pohlep, sovražnost, ki eskalira z maščevanjem, in posledica prisile (izsiljevanje) tretjega. V teh primerih lahko rečemo, da potencialno grožnjo predstavljajo tudi zaposleni, ki poznajo ustroj in delovanje podjetja ter so kot taki dober vir informacij zunanjim interesentom in konkurentom. V neredkih primerih gre za tako imenovane vgrajene oziroma vrinjene vohune, ki se jih rekrutira iz kvot študentov, pripravnikov, ki so zaposleni na izmenjavi iz sorodnih družb, ter predstavnikov zunanjih podjetij, ki izvajajo različne dejavnosti, svetovanja in revizije v ciljnem podjetju. (Podbregar in Slapar 2007) Prav zato se vse več podjetij zaveda pomembnosti sistema zaščite informacij in potrebe, da tudi sama ravnajo na podoben način v odnosu do svoje konkurence. V bistvu začaran krog, ki mu Američani popularno pravijo »never ending story«.

[21] Eno takih podjetij je Gorenje, ki je svoj tržni potencial gradilo na lastnem intelektualnem kapitalu, ter znani in uspešni slovenski gospodarski subjekti Seaway, Akrapović, Pipistrel ter verjetno naši največji potencialni tarči ekonomskega vohunstva – farmacevtski podjetji Lek in Krka.

[22] Omenimo lahko zadevo Peklar iz leta 2005, ko je ta poslovnež opravljal finančne posle s švicarskim podjetjem Bados Consulting, Navedeno podjetje iz Züricha je po podatkih France Finance podjetju Mobitel prodajalo podatke, pridobljene s pomočjo in na način, ki je značilen za poslovno vohunjenje (*business intelligence*), s čimer so pridobili konkurenčno prednost v odnosu do podjetja Simobil. (Jelen 2008) Drugi tak zanimiv in poučen primer je rop banke SKB oziroma njenih sefov. Preiskovalci so ugotovili, da je šlo v zadevi za gospodarsko vohunjenje s pridobivanjem insajderskih podatkov, saj so roparji do varovanih podatkov, znanih samo bančnemu osebju, lahko prišli le preko notranjih informatorjev (bančnega osebja in pripadnikov varnostne službe). (Jelen 2008)

Kot smo že ugotovili, gospodarski poizvedovalci pri svojem delu uporabljajo metode in sredstva, katerih uporaba je sicer izključno vezana na legalnost oziroma pozitivno pravno zakonodajo posamezne države. Zato bi se delo zasebnih poizvedovalcev od obveščevalnih služb moralo razlikovati po tem, da je njihovo delo v bistvu javno. Gospodarski poizvedovalci, ki uporabljajo metode in tehnike v nasprotju z zakonodajo, seveda storijo kaznivo dejanje in v teh primerih je govora o gospodarskem vohunjenju. (Dvoršek 2004)

Praviloma obveščevalne službe pri zbiranju podatkov uporabijo naslednje metode in sredstva: zbiranje podatkov s pomočjo človeških virov (v strokovnih krogih gre za izraz HUMINAT), tehničnih sredstev (TECHINT) in zbiranje javno dostopnih podatkov (OSINT) (Podbregar in Slapar, 2007). Kot trdi Pottter, se obveščevalna dejavnost na gospodarskem področju izvaja na medsebojno povezanih ravneh, ki jih deli na štiri osnovne ravni:

- primarna raven v podjetju,
- vmesna raven mrež, ki se medsebojno povezujejo v strateška zavezništva,
- nacionalna raven,
- transnacionalna raven na bilateralni oziroma multilateralni ravni (Potter 1988)

Čaleta ugotavlja, da sta najbolj uporabljani metodi pridobivanja informacij, ki jih storilci uporabljajo pri svojem delu: izraba podatkov iz javno dostopnih virov ter pregledovanje odpadne dokumentacije, ki je podjetje ustrezno ne uniči. V nelegalni coni se v te namene uporabljajo aktivnosti organiziranega kriminala, notranjih sodelavcev, vrivanje ustreznih oseb v sistem organizacije, vdiranje v informacijsko komunikacijski sistem, kraje in vlomi ter različne oblike elektronskega nadzora. (Čaleta, 2008)

4.3 Metode v sistemu gospodarskega vohunjenja

Različni teoretiki klasificirajo metode delovanja obveščevalnih služb načeloma podobno in jih delijo po načinu zbiranja podatkov praviloma v tri sklope, ki so lahko učinkoviti ločeno ali kombinirano. Za naš primer predstavimo tri sprejemljive načine oziroma metode delovanja obveščevalnih služb. (Bazdan 2016, 39–69)

1. Metoda poslovno obveščevalne službe

Pri tej metodi gre za strokovno premišljen standardizirani način zbiranja podatkov s pomočjo človeškega faktorja in tehničnih sredstev. V tem primeru delujejo strokovnjaki na posameznem področju, kjer ob zbiranju podatkov le-te tudi analizirajo in ovrednotijo. V tem primeru se uporabijo torej izkušeni visoko izobraženi strokovni kadri.

2. Metoda industrijskega vohunjenja

Ta metoda vsebuje načine in postopke, ki zanesljivo pripeljejo do željenih podatkov na tem področju. Koristijo tako imenovane klasične postopke (prisluškovanje, sledenje, fotografiranje, snemanje) in moderne postopke, ki se spreminjajo glede na tehnološki razvoj. Tudi zaradi koriščenja računalniške tehnike se tak nezakoniti način pridobivanja podatkov razume kot računalniška kriminaliteta.[23] Pojavne oblike računalniške kriminalitete so predvsem: odkrivanje poslovnih skrivnosti, softversko piratstvo, nelegalni prenos tehnologije in drugi. Torej gre za nezakonito vdiranje v računalniške sisteme z namero pridobivanja zaupnih poslovnih podatkov.

3. Metoda gospodarskega vohunjenja

Pod metodo gospodarskega vohunjenja razumemo nezakoniti način pridobivanja podatkov države in njenih organov. Pri tem mislimo na tajne operacije državnih obveščevalnih služb doma in v tujini. V angleščini to pojmujejo kot Covert Operation, zato se tudi službe praviloma imenujejo Human Intelligence, saj so akterji plačani in dobro izurjeni državni uslužbenci ali tuji plačanci. Zanje se praviloma uporablja

[23] Prevedeno iz angleščine *Computer Crime* (računalniško vohunjenje) oziroma *Computer Espionage*.

ljudski naziv vohuni, ki jih od znane ameriške afere Watergate v zahodnem svetu poznajo kot globoko grlo. Pri tem koristijo ob modernih kemičnih resursih tudi podkupovanja in druge oblike koruptivnih prijemov, prav tako pa tudi plasiranje dezinformacij in diskriminacij.

Ob raziskovanju določenega področja v tej nalogi smo trčili v teoretičnih razpravah na različne definicije in razlage pojma gospodarskega vohunstva. Nekateri ta pojem prevajajo tako, kot je naveden zgoraj, drugi kot gospodarsko-ekonomsko inteligenco. Pravzaprav lahko ugotovimo, da gre za disciplino, ki preučuje informacije, nujne državi in gospodarskim subjektom za sprejem razvojnih odločitev, s ciljem prilagoditve svojih kognitivnih zmogljivosti v zelo kompleksnem kontekstu svetovne konkurence. S tem postane ekonomska inteligenca temeljni del ekonomske geopolitike, saj postane orodje, ki ga uporabljajo države. Pri tem se javna in zasebna sfera tesno prepletata, sta celo soodvisni. (Kramar 2014)

V obveščevalni dejavnosti na ekonomskem področju se srečujeta dve vrsti gospodarskih družb. Nekatera podjetja se zavedajo pomembnosti lastne obveščevalne dejavnosti kot funkcije svojega managementa, lastnih obveščevalnih oddelkov ali pa najemajo tovrstne storitve pri zunanjih izvajalcih (oziroma outsourcing). Na drugi strani pa se pojavljajo gospodarske družbe, ki tovrstne storitve nudijo trgu. Potrebno je poudariti, da je za podjetja pomembno tudi upravljanje tveganj in zaščita pred obveščevalnimi vdori konkurenčnih podjetij ali tujih obveščevalnih služb. (Jelen 2008)

Gospodarski subjekti do željenih informacij prihajajo na različne načine. Pogosto ne gre za primere vohunjenja ali vdorov v informacijske sisteme, saj si lahko večina konkurentov pridobi informacije o novih izdelkih in tehnologijah na različnih sejmih in oglaševanjih za kupce, za katere se včasih izdelajo tudi predrazvojni projekti. To je praksa, ki jo lahko zazna tudi laik. Kot smo že ugotovili v prejšnjih poglavjih, zajema področje gospodarskega vohunstva dokaj širok spekter dejavnosti, zato je razumevanje pravne ureditve na tem področju zelo pomembno. Gre za Zakon o gospodarskih družbah (kjer 5. poglavje zajema poslovno skrivnost in prepoved

konkurence), Zakon o industrijski lastnini (15. člen opisuje industrijsko uporabljivost izuma) in 17. člen (ta se nanaša na zaupne izume, pomembne za obrambo in varnost države). (Podbregar in Slapar 2007)

Za učinkovito preprečevanje gospodarskega vohunstva so poleg zakonodaje, ki ustrezno inkriminira dejanja, potrebni tudi drugi varnostni, kadrovski, finančni, informacijski in organizacijski ukrepi. Nekateri teoretiki so mnenja, da bi bilo treba naše kazenskopravno področje preoblikovati. Razlog za spremembo zakonodaje je v spreminjanju razvojnih in gospodarskih trendov ter v novih prefinjenih oblikah izvrševanja kaznivih dejanj. V primerjavi z ostalimi evropskimi državami so kazni na področju gospodarske kriminalitete prenizke in bi bilo treba (morda po zgledu ZDA) pripraviti ustrezen področni lex specialis, ki bi enotno in na enem mestu urejal področje gospodarskega vohunstva. (Podbregar in Slapar 2007) Kljub vsemu pa lahko ugotovimo, da naša kazenskopravna in druga zakonodaja na obravnavanem področju nima večjih pravnih praznin. Tako je na primer vohunstvo kot splošno kaznivo dejanje opredeljeno v 33. poglavju, členu 358 Kazenskega zakonika (KZ-1-UPB2), ki zajema kazniva dejanja zoper varnost in njeno ustavno ureditev. Vohunstvo in metode, ki jih vohuni uporabljajo, so v tesni povezanosti varstvom človekovih pravic in svoboščin, gospodarstvom in poslovnimi skrivnostmi. V navedenem zakonu pa so konkretno opisani v naslednjih členih: neupravičeno prisluškovanje in zvočno snemanje (137. člen), neupravičeno slikovno snemanje (138. člen), kršitev tajnosti občil (139. člen), neupravičena izdaja poklicne skrivnosti (142. člen) in zloraba osebnih podatkov (143. člen). V 23. poglavju Kazenskega zakonika, ki se nanaša na kazniva dejanja zoper premoženje, pa lahko na gospodarsko vohunstvo navežemo tudi 221. člen, ki določa kot kaznivo dejanje napad na informacijski sistem. V 24. poglavju KZ, ki se nanaša na kazniva dejanja zoper gospodarstvo, lahko v razmerju do gospodarskega vohunstva izpostavimo naslednje člene: neupravičena uporaba tuje oznake ali modela (233. člen), neupravičena uporaba tujega izuma ali topografije (234. člen), ponareditev ali uničenje poslovnih listin (235. člen), izdaja in neupravičena pridobitev poslovne skrivnosti (236. člen), zloraba informacijskega sistema (237. člen) in zloraba notranje informacije (238. člen).

Na univerzi v Tilburgu so leta 2015 opravili študijo vpliva industrijskega vohunjenja na gospodarstvo in pri tem dali največ poudarka uporabi kibernetske tehnologije, ki je tudi na tem področju vse bolj prisotna. V študiji je ocenjeno, da je bilo približno dvajset odstotkov evropskih podjetij tarča kibernetskih napadov oziroma kršitev zakonodaje s tega področja. Evropska podjetja so zaradi te vrste groženj še posebej izpostavljena, predvsem pa njihovo napredno znanje in razvoj proizvodnje. Izpostavlja se predvsem naslednje države in njihov odstotkovni delež pri industrijskem vohunjenju, kjer je bila uporabljena kibernetska tehnologija:

- Italija (36 %),
- Francija (24 %),
- Nemčija (20 %),
- Nizozemska (17 %),
- Slovenija (teh podatkov žal ne klasificira).

Ocenjuje se, da so na območju večine držav Evropske unije proizvodnja, informacijske in komunikacijske tehnologije, finance, zdravstvo in medicina največje tarče za kibernetsko prisvajanje poslovnih skrivnosti. Zato menimo, da bi bilo treba osrednjo strateško gospodarsko proizvodnjo sistemsko povezati v smislu spodbujanja pridobivanja sredstev in tehnologije za skupno preprečevanje kibernetskih vdorov. Ocene o gospodarskem učinku kibernetske kraje poslovnih skrivnosti so negativne tako za gospodarske subjekte kot tudi celotno družbo. Evropski center za mednarodno politično ekonomijo (ECIPE) kot možganski trust s sedežem v Bruslju v poročilu o kibernetski kriminaliteti opisuje gospodarski vpliv kibernetskih kraj in ocenjuje škodo v zadnjih petih letih na 60 milijard EUR v smislu gospodarske rasti v EU in posledično izgubo približno 289.000 delovnih mest. Prav zato je nujna učinkovitejša strategija proti industrijsko kibernetskemu vohunjenju, ki mora vsebovati multidisciplinarni pristop z usklajenim sodelovanjem držav EU, gospodarskih subjektov in ponudnikov storitev kibernetske varnosti. (Publications Office of the EU 2018)

Kibernetskemu kriminalu ob rob je treba dodati, da se te resurse vse pogosteje koristi tudi za trgovanje z notranjimi informacijami, kar je seveda kaznivo dejanje v vseh državah in pomeni enega izmed značilnih modus operandi poslovnega vohunjenja v gospodarstvu. Tarča so tako gospodarski subjekti neposredno na trgu kot tudi borzne

hiše. Nezakonito trgovanje z notranjimi informaciji močno vpliva na stabilnost gospodarskih subjektov in lahko povzroči tudi njihov zlom ali celo uniči konkurenčne trge.[24] Trgovanje z notranjimi informacijami v primeru poslovanja z delnicami podjetij ali drugimi vrednostnimi papirji vključuje seveda tudi negativno konotacijo oziroma zlorabe, saj se pri trženju in vrednotenju koristijo prednosti kot posledica uporabe notranjih informacij oziroma Insider Trading.

4.4 Zaščitni mehanizmi za preprečevanje industrijskega vohunjenja

Gospodarske družbe so v tudi današnjem času ranljive za osebne, tehnične oziroma kibernetske napade od znotraj in od zunaj. Ocenjuje se, da je največja grožnja za krajo pomembnih in skrivnostnih informacij s strani osebja oziroma zaposlenih, ki si lahko neopazno prisvojijo pomembne informacije. V ta koncept sodijo tudi bivši delavci, partnerji, svetovalci, dobavitelji (o čemer je bilo v nalogi že govora). Večina informacij se torej pridobi brez uporabe tehnične opreme, vendar pa je uporaba informacijske tehnologije kljub temu vse pogostejša. (Podbregar 2006, 57−58)

Poslovne skrivnosti so tako ogrožene iz različnih virov, izpostavili pa bi dva:

- človeško mentaliteto,
- razlike v dosežkih posameznih gospodarskih subjektov, ki zagotavljajo uspešnejšim podjetjem prednost na trgu.[25]

[24] Trgovanje z notranjimi informacijami je pogost pojav v poslovnem svetu. Tak vzorčni primer je tudi primer Martha Steward Insider Trade case. Martha Steward se je namreč z uporabo internih (notranjih) informacij družbe ImClone, kjer je bila zaposlena, nezakonito okoristila. V lasti je imela delnice navedenega podjetja in pri svojem delu prišla do informacije možnega padca vrednosti zalog njihovih produktov ter zato delnice prodala na borzi. Po dveh dneh je vrednost produktov na zalogi dejansko padla za 16 %. S prodajo delnic se je Stewardova na tak način izognila izgubi v višini 45.673 ameriških dolarjev. (Moffat 2020)

[25] Premosorazmernost se torej kaže v tem: večja je prednost pred konkurenco, večja je ogroženost poslovne skrivnosti. (Kop 1995) To pa potrjuje tudi eno izmed naših tukajšnjih tez.

Zato ugotavljamo, da je gospodarsko vohunjenje za državne obveščevalne službe težavno in zahtevno področje, kar pa za protiobveščevalne službe pravzaprav ne velja. Obveščevalne službe so zoperstavljanju gospodarskemu vohunstvu v zadnjem obdobju primorane namenjati izjemno veliko pozornosti, saj trendi kažejo na konstanten porast vohunstva na gospodarskem področju. Države, ki so zaveznice v političnih in vojaških prizadevanjih ter v boju zoper mednarodni terorizem in kriminal, so v primežu hude dinamike gospodarskih konkurentov, ki so pripravljeni uporabljati tudi nezakonita sredstva. (Jelen 2008)

Poslovno okolje in razvoj tehnologije dvigata verjetnost za gospodarsko obveščevalno dejavnost in industrijsko vohunjenje, saj omogočata dostop do intelektualne lastnine. Kot primer navajamo splošno uporabo elektronskih naprav sodobnega tipa Apple iPod, katerih sestavne komponente proizvajajo na Japonskem, Filipinih, Koreji, Kitajskem in Tajvanu. Takšen outsourcing je sicer stroškovno cenen, pušča pa matičnega proizvajalca ranljivega pred industrijskim vohunstvom. (Rishikof 2009). Varovanje lastne inovativne tehnologije je nuja že v procesu razvoja, saj postaja celo vprašanje nacionalne varnosti. Rishikof opozarja, da podjetja ne sledijo rada vmešavanju državnih regulatorjev, saj bi le-ti utegnili ovirati razvoj in odprtost družb. (Rishikof 2009)

Pravzaprav morajo gospodarske družbe same vzpostaviti mehanizme, s katerimi bodo uspešno zaznale izgube informacij in ostalih oblik intelektualne lastnine, predvsem pa v okviru možnosti zajezitve notranjega odliva poslovnih skrivnosti. Na podlagi priporočil inštituta Software Engineering Institute z univerze Carnegie Mellon v Pittsburghu bi morali gospodarski subjekti uvesti evidenco dostopov do pomembnih poslovnih informacij. Raziskave navedenega inštituta so namreč pokazale, da kraje intelektualne lastnine in drugih podatkov pogosto izvršujejo odhajajoči insajderji, zato mora management uvesti sistem nadzora vračanja opreme in zadolžitev, še preden zapustijo podjetje. To je seveda zahtevno, saj insajderji koristijo sofisticirano elektronsko tehnologijo. Indic, na katerega naj bi naj bila podjetja še posebej pozorna, je povečana frekvenca in kopiranje dokumentov, kar se sicer lahko učinkovito prepreči že z omejevanjem dostopa do pomembnih resursov. Omejeni in nadzirani dostopi so velika ovira odhajajočim zaposlenim, ki imajo vohunske pretenzije,

pogojene iz različnih vzgibov.[26] Varnostni mehanizmi, ki jih podjetja uporabljajo, so še vedno vse preveč klasični oziroma tradicionalni v odnosu na problematiko, ki v tem času ne pripomore k lastnemu preprečevanju gospodarskega in industrijskega vohunjenja. Očitno je, da se odgovorni v nekaterih podjetjih še vedno ne zavedajo posredne škode, nastale z vdorom konkurenčnega podjetja, oziroma se tuje obveščevalne službe z lahkoto dokopljejo do poslovnih skrivnosti, saj posledice običajno niso takoj vidne. Še vedno pa je marsikje prisotna miselnost, da se tak kriminal ne da učinkovito preprečiti ter da je preventiva predraga. Iz zatrjevanega torej izhaja, da so za varnost v zasebnem sektorju odgovorne predvsem gospodarske družbe same, ki za zagotavljanje varnosti posegajo po storitvah zasebnih ponudnikov varnostnih storitev. Ob tem pa se pojavi možnost vohunskih aktivnosti tega istega ponudnika, ki lahko hkrati opravlja dejavnost poizvedovanja za konkurenčno družbo.

Gospodarski subjekt lahko gradi svojo varnost tudi na temelju varnostne kulture, saj je le-ta proizvod individualnih in skupnih vrednot, nazorov, percepcij, kompetenc in vedenjskih vzorcev, ki opredeljujejo zavezanost, način in sposobnost organizacijskega upravljanja zdravja in varnosti. (Jelen 2008) Pri tem pa se je treba zavedati tveganj, o katerih je sicer že precej govora v tem poglavju, zaradi česar je treba vzpostaviti adekvatne protiukrepe in tako zaščititi najbolj dragocene informacije.

Glede na dostopne podatke in prakso lahko ugotovimo, da Slovenija na področju protiobveščevalne dejavnosti na gospodarskem področju nekoliko zaostaja, saj bi že pred leti morala država ustrezno umestiti strategijo oziroma usmeritve v boju zoper gospodarsko vohunstvo. Ob že navedeni potrebi po modernizaciji kazenskopravnega področja zaradi novih gospodarskih trendov je nujen sprejem nacionalne strategije na tem področju, ki bi zajel tudi varnostno-obveščevalni sistem. Podbregar meni, da gre tudi za kadrovsko podhranjenost struktur, katerih naloga je odkrivanje in preiskovanje tovrstnih dogajanj. (Podbregar in Slapar 2007)

[26] Več o tem v študiji inštituta Insider Threat Center at CERT, 2009.

Slovenska obveščevalna dejavnost na ekonomskem področju se je pravzaprav pričela intenzivirati predvsem v zadnjih dvajsetih letih. Po novem ustroju delovanja in kadrovskih rošadah je SOVA na ekonomskem področju pričela s prioriteto izvajati ukrepe iz svoje pristojnosti. Gričar ocenjuje, da je pri preoblikovanju te službe prišlo do zastojev za učinkovito zoperstavljanje škodljivim ekonomskih trendom, kar naj bi bila posledica predolge tranzicije obveščevalne skupnosti in oblikovanja primerne zakonodaje. Razlog za manj agresivno obveščevalno dejavnost v zadnjih letih na gospodarskem področju bi lahko iskali tudi v prilagojenosti služb glede na slovenske integracije v EU in NATO, kar je posledično prineslo manj agresivnosti in obveščevalnih aktivnosti SOVE. (Gričar 2006)

Do neke mere je razumljivo, da je vlaganja slovenskih podjetij v varnostne ukrepe pogojevalo tudi usihanje gospodarske konjunkture in nekajletna recesija, saj se gospodarski subjekti niso tako intenzivno ukvarjali z vprašanjem vdorov konkurenčnih podjetij in so se zato vlaganja na tem področju minimalizirala. Domača podjetja, ki želijo uspešno delovati na tujih trgih, enostavno ne morejo zanemarjati dejstev in ignorirati pomembnosti gospodarske obveščevalne dejavnosti, pa naj gre za aktivno zbiranje podatkov in poizvedovanje o konkurenci oziroma za namen oblikovanja ustreznih obrambnih strategij pred odtekanjem informacij, razkrivanja poslovnih skrivnosti in posledičnega izgubljanja tržnega položaja na račun prizadevanj konkurenčnih družb. Razlogov za slabšo raziskanost je več, v glavnem pa se z njimi srečujejo po vsem svetu. Podjetja, ki so žrtve vohunstva, se tega velikokrat niti ne zavedajo zaradi pomanjkljive varnostne kulture v samih podjetjih ali pa gre slednje na račun varnostnih mehanizmov, ki ne uspejo zaznati in preprečevati vohunskih vdorov. Po drugi strani pa prizadeta podjetja v primeru zaznanih vohunskih aktivnosti slednjih ne želijo razkrivati in prijaviti organom pregona, saj ob dodatni izpostavljenosti podjetja v javnosti ne verjamejo v uspeh kazenskega pregona. Obstaja bojazen, da razkritja ne utegnejo slabo vplivati samo na javno podobo prizadetih podjetij, temveč bi lahko vplivala tudi na sodelovanje in zaupanje poslovnih partnerjev. (Jelen 2008)

Ocenjuje se, da naša obveščevalna skupnost še ni povsem na nivoju družbenih integracij drugih zahodnih služb, saj so pojavne oblike gospodarske obveščevalne

dejavnosti slabo raziskane, znanstveno šibko obdelane in kot subjekt nezadostno zastopane v strokovnih razpravah.

Občutljivosti slovenskega trga za napade in industrijsko vohunjenje tujih podjetij ne gre minimalizirati zaradi relativno majhne tržnosti, saj se interesenti na kvantitativne karakteristike trgov, opredeljene na geografske ravni ali področja poslovanja, veliko ne ozirajo.[27] Pri nas delujejo manjša in srednje velika podjetja, ki so v zaostreni konkurenci slabših gospodarskih razmer primorana vlagati več konkurenčnega truda in marketinških tveganj. Ob tipu navedenih podjetjih pa pri nas obstajajo seveda tudi večja podjetja. Mnoga od njih uspešno in prepoznavno poslujejo in so s svojimi inovativnostmi pridobila svetovno prepoznavnost, s tem pa seveda pozornost tujih konkurentov. Jelen ocenjuje, da se slovenska podjetja zavedajo rizičnosti gospodarskega in industrijskega vohunjenja, vendar pa se tega problema lotevajo preveč pasivno. (Jelen 2008)

Občutljivosti slovenskega trga za napade in industrijsko vohunjenje tujih podjetij ne gre minimalizirati zaradi relativno majhne tržnosti, saj se interesenti na kvantitativne karakteristike trgov, opredeljene na geografske ravni ali področja poslovanja, veliko ne ozirajo. Dejavnost zasebnega konkurenčnega svetovanja in poizvedovanja je pri nas v domeni zasebne sfere. Gre za delovanje na področju zbiranja in vrednotenja podatkov na gospodarskem področju zasebnih detektivskih agencij, pri čemer je nujna specializiranost zasebnih detektivov, saj izvajajo poizvedbe z zbiranjem in analiziranjem javno dostopnih podatkov, ne da bi pri tem zašli v nelegalnost. Kot je

[27] Gaiser poudarja tudi pomembnost nacionalnega interesa na v nalogi obravnavanem področju, in sicer: »The establishment of the most appropriate information exchange system among the key economic actors is indispensable for: the further development of the economy and the protection of its interests, the strengthening of the presence of Slovenian entrepreneurship worldwide and the reduction of threats to its interests on foreign markets, the increase of attractiveness of the country's investment environment, the strengthening of the geo-economic projection of the Slovenian national interest around the world, increasing the employment rate, improving the collection of information from foreign environments, better planning of state's tax and legal efficiency, and increasing general welfare.« (Gajser 2019)

že zgoraj omenjeno, lahko zasebni sektor na tem področju deluje v smislu svetovalnih subjektov, saj zasebni detektivi svojim naročnikom posredujejo spoznanja o najučinkovitejših ukrepih zaščite zoper obveščevalne aktivnosti konkurenčnih družb. (Dvoršek 2002)

Ko se na tem mestu dotikamo detektivske dejavnosti za koristi gospodarskih subjektov, je treba omeniti njihovo pomembno dejavnost, ki se kaže v zbiranju podatkov in preverjanju kandidatov za posamezna delovna mesta in tudi zaposlenih. Predvsem v zahodnih državah EU je to dolgoletna praksa, saj naročniki uporabljajo manj preverjanj podatkov in primernosti kadrov s pomočjo zasebnih detektivskih in drugih zasebnih obveščevalnih agencij. Takšna praksa se že nekaj let uveljavlja tudi pri nas, saj predstavlja delodajalcem pomemben vir informacij. (Dvoršek 2002) Morda je prav dodati, da so osnovna preverjanja pri nas prisotna že dolgo, vendar so bila izvajana brez ustrezne profesionalne sistematike in v domeni kadrovskih služb ter posameznih agencij za zaposlovanje.

4.5 Pravna podlaga za delovanje obveščevalnih služb

Varnostno-obveščevalni sistem praviloma sestavlja več med seboj sorodnih in povezanih služb, ki so po naravi obveščevalnega tipa, in služb, ki so protiobveščevalnega značaja, z nalogo preprečevanja obveščevalnih dejavnosti tujih služb in za zaščito ustavne ureditve. Civilna in vojaška sfera zbirata informacije, pomembne za odločevalce na mednarodnih, političnih in drugih interesnih področjih. Te službe so praviloma umeščene v državno upravo kot posebne vladne službe – agencije in v strukturo različnih ministrstev, predvsem treh: ministrstva za notranje zadeve, zunanjega ministrstva in ministrstva za obrambo. (Purg 2001)

Ob obravnavi organizacijskih shem in metod delovanja pa se je v tej nalogi pomembno in nujno dotakniti tudi področja pravne ureditve kot legalne osnove za delovanja vseh vrst obveščevalnih subjektov. Interes služb je seveda fleksibilnost pravnega reda na tem področju, interes civilne družbe pa ravno nasprotno. Nekatera področja delovanja obveščevalnih služb so pravno zadovoljivo urejena, problem pa običajno nastopi ob naglici tehnološkega razvoja, ki prehiteva pravni ustroj v

posameznih državah in skupnostih. Očitne normativne pomanjkljivosti, s katerimi se srečujejo organi pregona, se nanašajo tudi na necelovito kazenskopravno urejenost na področju kibernetike.

Ugotavlja se, da nekatere države temu področju ne posvečajo posebne pozornosti, nekatere pa so kazniva ravnanja inkorporirale kot delno modifikacijo obstoječe zakonodaje, čeprav bi bil sprejem lex specialis za to področje nujen in v smislu generalne prevencije veliko bolj učinkovit. Sprejetje in implementacija v pravni red namreč storitve kaznivih dejanj ne preprečujeta samoumevno. Države se morajo ravnati v smislu transnacionalnosti te vrste kriminala, saj lahko kriminal izhaja iz ene države, posledice pa so evidentne tudi v drugih.

Ko je govora o zakonitosti ravnanj obveščevalnih služb, je vsaj na gospodarskem področju dopustnost in kaznivost jasno normativno razmejena. Lahko ocenimo, da je ločnica med etičnim in neetičnim ravnanjem teh služb velikokrat nejasna. Predvsem je na tem mestu treba omeniti način pridobivanja informacij na neetičen način, kar je lahko tudi njihov namen in njihova uporaba. Različne taktike, ki se ne spogledujejo z moralnimi načeli in veljavnimi kodeksi, zlahka izkrivijo meje etične in zakonite poslovne prakse, saj se kažejo kot kraje informacij, nameščanje prisluškovalnih avdio in video naprav, zavajanje poslovnih partnerjev ter zbiranje zavrženih materialov ali odpadkov konkurentov.[28] Ob nezakonitosti je kot neetično opredeljeno tudi pridobivanje informacij zaupne in zasebne narave. V to sfero spadajo digitalne informacije. Običajno gre v teh primerih za krajo in poseg v zaščiteno intelektualno lastnino visokotehnoloških podjetij ali zasebnikov neposlovne narave. Nezakonito je tudi pridobivanje informacij z namenom delovanja zoper javni interes, saj v nasprotju z zakonodajo vpliva na konkurenčna podjetja ali je zaradi zlorabljenih informacij ogrožena nacionalna gospodarska strategija ter nacionalna varnost.

[28] Vzorčni primer industrijskega vohunstva iz leta 2004 je lahko tudi vpletenost multinacionalk P&G (Procter&Gamble) in Unilever, ko je P&G najela neodvisne pogodbenike za pridobivanje podatkov o izdelkih za nego las konkurenčnih družb (tudi britansko-nizozemskega giganta Unilever). Do obsežne količine podatkov so prišli tudi s preiskovanjem vsebine kontejnerjev za odpadke ter s ponarejenimi identifikacijami tržnih analitikov in novinarjev.

ZDA so leta 1996 v odgovor na vse bolj uveljavljeno grožnjo vohunskih aktivnosti sprejele Zakon o gospodarskem vohunstvu oziroma Economic Espionage Act (EEA).[29] Navedeni zakon je obligatorno opredelil varovanje poslovnih skrivnosti, saj so postajale vse pogosteje tarča tujih konkurenčnih podjetij in obveščevalnih služb drugih držav. (Gregory 1997)

V enem od podpoglavij omenjamo tudi terminološke zaplete glede na pojmovno razumevanje posameznih strokovnih terminov in njihovo prevajanje v slovenski jezik. Na tem mestu pa osvetljujemo kot težavo pri preiskovanju obravnavanega področja neenotnost glede tehnološke opredelitve na normativni osnovi. Omeniti velja delno zavajajoče poimenovanje prej omenjenega zakona EEA, ker v njem gospodarsko vohunstvo na makro nivoju ni zajeto. Gospodarsko vohunstvo predstavlja ustaljeno prakso v okviru pridobivanja pomembnih podatkov državnih služb, kar velja seveda tudi za ZDA. Zakon sicer razumljivo opredeljuje znake industrijskega vohunjenja in dejavnost na tej osnovi kot nelegalen del obveščevalne dejavnosti, vendar pa gospodarsko vohunjenje v ZDA ni zvezno kaznivo dejanje (ki bi veljalo na celotnem ozemlju ZDA), industrijsko vohunjenje kot ena od njegovih kategorij, pa je, kar je res težko razumljiva ureditev tega kazenskega področja. V praksi ne najdemo podobnega primera, torej tako definirane zakonodaje. Morda je problem v različnem pristopu posameznih zveznih držav ZDA do te problematike. Kritiki zakonske ureditve vidijo problem predvsem v ozki opredelitvi 1831. člena EEA, ki otežuje sprejem večjega števila obsodilnih sodb, slednje pa tožilce odvrača od vztrajanja pri pregonu gospodarskega in industrijskega vohunjenja. (Gregory 1997)

Naša zakonodaja gospodarskega in industrijskega vohunstva posebej ne opredeljuje. V 358. členu Kazenskega zakonika Republike Slovenije (v nadaljevanju: KZ) je sicer

[29] Zakon uveljavlja celovit pristop za zajezitev vohunstva na gospodarskem področju s pospeševanjem preiskav organov pregona in hitrejšim zaključkom sodnih postopkov. Za zakon so značilne strožje kazenske sankcije za odtujitev poslovnih skrivnosti v primerjavi z drugimi kršitvami pravic o zaščiti intelektualne lastnine.

vohunstvo opredeljeno z znaki kaznivosti in predpisano kazensko sankcijo. V prvem odstavku navedenega člena je določba, da vsakogar, ki služi tuji državi ali organizaciji z zbiranjem zaupnih vojaških ali gospodarskih uradnih podatkov ali dokumentov, izroči ali omogoči, da se do njih pride, kaznuje z zaporom od enega do osmih let. (Kazenski zakonik RS 2008) V členu je torej govora o samo enem segmentu obveščevalne dejavnosti na gospodarskem področju, in sicer gospodarskem vohunjenju. Vendar pa nas empirika opomni, da se pri izvajanju gospodarskega in industrijskega vohunjenja izvršujejo tudi druge oblike kaznivosti, s katerimi se posega v pravice gospodarskih družb in posameznikov: nezakonito prisluškovanje, zvočno in slikovno snemanje, kršitve tajnosti občil, neupravičen vdor v informacijski sistem, neupravičena uporaba tujega izuma ali topografije, izdaja in neupravičena pridobitev poslovne tajnosti, zloraba notranje informacije ter izdaja uradne in državne tajnosti. (Jelen, 2008) V triindvajsetem poglavju navedenega zakona so opredeljena kazniva dejanja s področja gospodarstva tudi v členih 236., 237. in 238., ki kot kaznivo določajo izdajo in neupravičeno pridobivanje poslovnih skrivnosti, vdore v poslovne informacijske sisteme in zlorabo notranjih informacij.

Nezakonito trgovanje s poslovnimi skrivnostmi predstavlja modus operandi pridobivanja zaupnih poslovnih informacij konkurenčnih gospodarskih subjektov. Naš pravni red na tem področju vsebuje Zakon o gospodarskih družbah, ki v 40. členu kot kaznivo ureja ravnanje oseb izven družbe, ki v nasprotju z zakonom in voljo družbe pridobivajo podatke iz kataloga poslovnih skrivnosti družbe. (Zakon o gospodarskih družbah 2006)

Kot protipravno določa Zakon o varstvu konkurence (13. člen) pridobivanje poslovnih tajnosti drugega podjetja ali neupravičeno izkoriščanje zaupanih poslovnih tajnosti kot enega od segmentov nelojalne konkurence.[30]

Obveščevalne dejavnosti na ekonomskem področju se dotikajo tudi predpisi s področja informacijske varnosti, zasebnega varovanja, tajnih podatkov[31] in drugi, ki

[30] Zakon o varstvu konkurence (1999).

[31] Tudi Zakon o tajnih podatkih (2001).

urejajo delovanje sistema notranje varnosti. (Jelen 2008) Ta normativa je v bistvu velik korak v smeri, da bi se lahko predpisi istega področja spravili na skupini imenovalec. Razpršenost istovrstnih kaznivih dejanj po različnih predpisih za uspešen pregon ni optimalna rešitev. Na splošno pa lahko ocenimo, da je slovenska zakonodaja na navedenem področju dokaj primerljiva z evropsko prakso in normativo. Empirika in sodni judikati potrjujejo, da je obravnava v tem delu obravnavanih kaznivih ravnanj izjemno zahtevna in težko dokazljiva.

Slovenska obveščevalno-varnostna agencija (v nadaljevanju: SOVA) je edina civilna obveščevalno-varnostna služba v naši državi. Naloge ima določene v 2. členu Zakona o Slovenski obveščevalno-varnostni agenciji (v nadaljevanju: ZSOVA). Navedeni zakon področja gospodarstva eksplicitno ne zajema, vendar pa je v drugem členu določba, ki agenciji omogoča zakonito pridobivati in vrednotiti podatke tudi v navezi s tujino, pomembne za zagotavljanje varnostnih, političnih in gospodarskih interesov držav.[32]

V ZSOVA so posebne oblike pridobivanja podatkov zajete v 5. poglavju od 19. do 25. člena. Na podlagi 24. člena lahko predsednik Vrhovnega sodišča Republike Slovenije dovoli tudi nadzorovanje telekomunikacij z izpisom telekomunikacijskega zapisa, in sicer na podlagi 24. člena za največ šest mesecev. Za obravnavo našega področja je pomemben tudi 25. člen, ki daje pooblastilo direktorju SOVE za odreditev uporabe uradnih listin s prirejenimi identifikacijskimi podatki in uporabo prirejenih identifikacijskih oznak.[33] Sova po naši pravni ureditvi nima policijskih pooblastil in ne sodeluje v pregonu storilcev kaznivih dejanj.
Obveščevalno-varnostna služba (v nadaljevanju: OVS) je notranja organizacijska enota oziroma organ v sestavi Ministrstva za obrambo (v nadaljevanju: MORS) in spada med obrambne obveščevalne službe. Njene naloge, pristojnosti in pooblastila

[32] Zakon o Slovenski obveščevalno-varnostni agenciji (2006).

[33] Sova lahko na podlagi navedenega zakona (20. člen) pridobiva podatke tudi s tajnim delovanjem in posebnimi oblikami pridobivanja podatkov: spremljanjem mednarodnih sistemov zvez, tajnim nakupom dokumentov in predmetov, tajnim opazovanjem in sledenjem na odprtih ali javnih prostorih z uporabo tehničnih sredstev za dokumentiranje.

določata Zakon o obrambi in Uredba o obveščevalno-varnostni službi Ministrstva za obrambo. Na podlagi določb 34. člena navedenega zakona imajo delavci OVS, ki opravljajo protiobveščevalne naloge, enaka pooblastila kot uslužbenci SOVE in dovoljeno uporabo posebnih metod in sredstev za pridobivanje obveščevalnih podatkov. OVS opravlja obveščevalne, protiobveščevalne in varnostne naloge na obrambnem področju, protiobveščevalne naloge pa izvaja le za MORS in Slovensko vojsko ter za varovanje podatkov v obrambnem sistemu. Slovenska vojska nima pooblastil za protiobveščevalno delovanje.

Slovenska policija (kriminalistična) pri pridobivanju podatkov in informacij prav tako uporablja z zakonom določene prikrite metode in sredstva. Kot organ v sestavi Ministrstva za notranje zadeve lahko pridobiva podatke na podlagi odredbe sodišča v skladu s pravno podlago v Zakonu o Policiji (ZPol) in Zakonu o kazenskem postopku (ZKP). Za zakonitost na ta način pridobljenih podatkov je pomembno, da obstaja utemeljeni sum, da se pripravlja ali je bilo storjeno kaznivo dejanje. Praviloma pa zadostuje utemeljeni razlog za sum (na podlagi členov 156, 148 in 149b ZKP).

4.6 Pridobivanje podatkov na področju obveščevalne dejavnosti – primerjava izbranih držav

V pravnih sistemih držav so civilne obveščevalne službe lahko samostojne ali pa sestavni del ministrstev. Za v nalogi primerjalno obravnavane države Slovenijo, Hrvaško in v Italijo velja, da so samostojne, v Avstriji in Nemčiji pa so civilne obveščevalne službe podrejene notranjim ministrstvom oziroma so njihov sestavni del.

Avstrijska vojaška protiobveščevalna služba se nahaja v okviru obrambnega ministrstva, podobno velja za sorodne službe na Hrvaškem, Madžarskem, Nizozemskem in v Nemčiji. Italija nima specifično oblikovane posebne vojaške obveščevalne ali protiobveščevalne službe, pač pa ima samo zunanjo in notranjo obveščevalno službo, pri čemer slednja primarno opravlja protiobveščevalne naloge. Med obravnavanimi državami sta civilna in vojaška protiobveščevalna služba v

ločenih zakonih urejeni v Avstriji in Nemčiji, pri čemer delovanja avstrijskega BVT (Zvezni urad za zaščito ustave in boj proti terorizmu) ne ureja poseben zakon, pač pa je njegovo delovanje, tako kot velja tudi za druge varnostne organe, urejeno v Zakonu o varnostni policiji. (Vodovnik 2011) Nemški MADG (Vojaška obveščevalna služba) se glede posebnih ukrepov v precejšnji meri sklicuje na civilni BVerfSchG (Zvezni zakon o ustavni zaščiti). Podobno se v Sloveniji ZSOVA uporablja tudi za OVS, ki se nahaja v okviru Ministrstva za obrambo RS.

4.6.1 Avstrija

Avstrijsko zvezno notranje ministrstvo ima v svoji strukturi Zvezni urad za zaščito ustave in boj proti terorizmu (Bundesamt für Verfassungsschutz und Terrorismusbekämpfung – BVT) kot civilno obveščevalno službo. Delovanje je regulirano na podlagi Zakona o varnostni policiji (Sicherheitspolizeigesetz – SPG) in pri izvajanju kazenskopravnih nalog na podlagi Zakona o kazenskem postopku (Strafprozessordnung – StPO), poleg tega pa predstavljajo podlago za delovanje urada tudi nekateri drugi zakoni. BVT je varnostni organ (Sicherheitsbehörde) s pristojnostmi sodelovanja s tujimi varnostnimi in obveščevalnimi službami ter organizacijsko spada pod Generalno direkcijo za javno varnost (Generaldirektion für die öffentliche Sicherheit) Zveznega notranjega ministrstva. Pristojnosti ima predvsem na področju preprečevanja ekstremizma in terorizma, vohunstva, trgovine z orožjem in jedrskim materialom ter organiziranega kriminala. BVT na zvezni ravni daje pobude in koordinira ukrepe vseh devetih deželnih uradov predvsem glede zaščite oseb, objektov, predstavnikov tujih držav in mednarodnih organizacij. Avstrijska civilna obveščevalna služba je drugače umeščena, kot je to pri nas, saj nima posebnega zakona (kot je pri nas ZSOVA), ki bi celovito urejal položaj in vlogo civilne obveščevalne službe. (Blažič 2010)

4.6.2 Hrvaška

Naša južna soseda ima področje dela obveščevalnih služb urejeno v Zakonu o varnostno-obveščevalnem sistemu Republike Hrvaške (Zakon o sigurnosno-

obavještajnom sustavu Republike Hrvatske), ki je bil sprejet leta 2006. V sistemu delujeta dve ločeni obveščevalni strukturi: na civilnem področju deluje Varnostno-obveščevalna agencija (Sigurnosno-obavještajna agencija – SOA), na vojaškem pa Vojaška varnostno-obveščevalna agencija (Vojna sigurnosno-obavještajna agencija – VSOA).

SOA ima pristojnosti na področju preprečevanja ogrožanja ustavnega reda, nacionalnih interesov, državnih organov in državljanov. Svoje zakonite pristojnosti (23. člen navedenega zakona) izvajajo za zajezitev terorizma in ekstremizma ter obveščevalne dejavnosti tujih obveščevalnih služb, organizacij in posameznikov, nepooblaščenega vstopanja v zaščitene informacijske in komunikacijske sisteme državnih organov, pridobivanja tajnih podatkov od funkcionarjev ter zaposlenih v državnih organih in znanstvenih institucijah ali v pravnih osebah z javnimi pooblastili. V ta namen lahko pridobivajo, analizirajo, obdelujejo in vrednotijo različne podatke o tujih državah, organizacijah, političnih in gospodarskih zvezah, skupinah in posameznikih.

VSOA je organizacijska enota obrambnega ministrstva za načrtovanje in izvajanje podpore ministrstvu ter oboroženim silam pri izvrševanju nalog obrambe, državne suverenosti in neodvisnosti ter teritorialne nedotakljivosti države. Krajevne in stvarne pristojnosti so teritorialno omejene na območje Republike Hrvaške. Na podlagi 24. člena navedenega zakona pa VSOA lahko pridobiva, obdeluje, vrednoti in analizira podatke o nezakonitih naklepih ter delovanju oseb, skupin in organizacij v državi, ki imajo za cilj ogrožanje obrambne moči države. (Blažič 2010)

4.6.3 Italija

Italija ima dolgo tradicijo delovanja obveščevalne dejavnosti, ki se je skozi zgodovino in varnostne prioritete vladarjev stalno spreminjala. Obveščevalne službe so normativno regulirane v Zakonu o obveščevalnem sistemu za varnost države in o novi ureditvi tajnosti. (Sistema di informazione per la sicurezza della Repubblica e nuova disciplina del segreto, 2007) Zanimiva je neposredna podrejenost vladi oziroma predsedniku vlade kot šefu izvršne oblasti v državi. Pristojnost premiera je tudi

imenovanje generalnega direktorja in namestnikov obeh obveščevalnih služb ter koordinacijske skupine, ki pa lahko v skladu z zakonom te pristojnosti prenese na pooblaščenca. Italijanski obveščevalni sistem sestavljajo še različna z zakonom določena telesa, obveščevalni službi pa sta: Agencija za zunanjo obveščevalno dejavnost in varnost (l'Agenzia informazioni e sicurezza esterna – AISE) ter Agencija za notranjo obveščevalno dejavnost in varnost (l'Agenzia informazioni e sicurezza interna – AISI, kar opredeljujejo členi od 1 do 3 navedenega zakona.

Navedeni zakon v 4. členu opredeljuje delovanje prej omenjene koordinacijske strukture oziroma Oddelka za obveščevalno dejavnost in varnost (Dipartimento delle informazioni per la sicurezza – DIS), ki deluje v okviru predsedstva vlade (Presidenza del Consiglio dei ministri) in zagotavlja skupno kontinuiteto načrtovanja, zbiranja in analiziranja obveščevalnih podatkov. Oddelek koordinira, nadzira ter usklajuje delo obeh navedenih obveščevalnih služb (torej civilne in vojaške obveščevalne komponente). Pristojnosti za samostojno posredovanje tako zbranih podatkov nima, ozirati se mora na odločitev vsakokratnega predsednika vlade. Zunanja obveščevalna dejavnost je opredeljena v 6. členu prej omenjenega zakona, s katerim je ta dejavnost regulirana z Agencijo za zunanjo obveščevalno dejavnost in varnost (AISE). Slednja ima pristojnost zbiranja in vrednotenja podatkov tujini in tudi v tujini. Zanimiva pa je teritorialna pristojnost, saj AISE lahko aktivnosti izvaja tudi doma, a omejeno in izključno v sodelovanju z AISI.

Če ugotovitve in podatke strnemo, v Italiji izvaja protiobveščevalno dejavnost samo AISI, saj tako eksplicitno določa 7. člen prej omenjenega zakona. Agencija ima pooblastila za zbiranje, obdelavo in distribucijo obveščevalnih podatkov, navedena zakonska določba pa njeno področje strne na varovanje ustavnega sistema (subverzivnost, terorizem in drugo). Lahko pa preiskuje tudi delovanje obveščevalnih služb tujih držav na ozemlju Italije. (Blažič 2010)

4.6.4 Nemčija

Kot v večini evropskih držav tudi v Nemčiji delujeta na državnem nivoju dve osnovni obveščevalni službi:

- Zvezni urad za varstvo ustavne ureditve (Bundesamt für Verfassungsschutz – BfV), ki je podrejen zveznemu notranjemu ministrstvu. Njegova osnovna krajevna pristojnost je vezana na delovanje znotraj države, stvarna pristojnost pa zajema vsestransko ogrožanje ustavne ureditve, varnost države ter vohunsko aktivnost tujih služb v ZRN.[34]
- Vojaška protiobveščevalna služba (Militärische Abschirmdienst – MAD), ki se ukvarja z zadevami na področju obrambe in sovražnosti zoper nemško vojsko. MAD je sistemsko umeščena in podrejena obrambnemu ministrstvu ter svoje naloge izvaja izključno v tej področni pristojnosti.

Nemčija je svoj obveščevalni sistem sestavila hierarhično in teritorialno v kontekstu deželnega sistema ustroja države. V sleherni zvezni deželi je ustanovljen Urad za varstvo ustavne ureditve (Landesämter für Verfassungsschutz – LfV), ki hierarhično in strokovno tesno sodeluje z Zveznim uradom za varstvo ustavne ureditve (Blažič 2010). Nemčija ima na zvezni ravni za nadzor nad delom teh služb ustanovljeni dve telesi:

- Parlamentarni nadzorni gremij (Das Parlamentarische Kontrollgremium – PKGr),
- Komisija G 10 (G-10 Kommission).[35]

Stvarne pristojnosti BfV oziroma nemške civilne protiobveščevalne službe ureja Zvezni zakon o varstvu ustavne ureditve (Bundesverfassungsschutzgesetz – BVerfSchG)). Zakon v drugem odstavku 8. člena določa pristojnosti BfV za: pridobivanje, obdelavo in analizo osebnih podatkov v skladu z normativo o varstvu

[34] Nemška tajna služba je Zvezna obveščevalna služba (Bundesnachrichtendienst – BND). Podrejena je neposredno zvezni izvršni oblasti, konkretneje predstojniku Urada zveznega kanclerja. Gre za tako imenovano zunanjo obveščevalno službo, ki v tujini pridobiva podatke, pomembne za zunanjo in varnostno politiko države.

[35] Komisija je bila ustanovljena na podlagi 10. člena nemške ustave. Njeni člani ne smejo biti poslanci Bundestaga oziroma nemškega parlamenta. Brez soglasja Komisije se posamezni ukrep praviloma ne more izvesti, razen v nekaterih nujnih primerih.

osebnih podatkov, pri čemer uporablja različne metode, ki so konkretizirane v podzakonskem aktu, ki praviloma ni javen in ga odobri zvezni notranji minister. V 8. členu je eksplicitno določeno, da BfV nima policijskih pooblastil. (Blažič 2010)

4.7 Primerjalni pregled delovanja obveščevalnih služb na gospodarskem področju

V prejšnjih poglavjih je bilo precej govora o temi, ki zajema miselnost, da se obveščevalne službe ob ukvarjanju z ekonomskim področjem ukvarjajo tudi z industrijskim vohunstvom predvsem takrat, ko državni odločevalci tako ocenijo in odločijo ali to predstavijo kot nacionalni interes. Nekateri opisani primeri nam to sicer tudi dokazujejo, toda treba bi bilo ubežati logiki, da se za takšno odločitvijo skrivajo enaki vzroki po načelu, da cilj opravičuje sredstva. Da to nekoliko podrobneje osvetlimo, sta v nalogi primeroma zajeti dve državi: Francija kot ena izmed držav EU ter ZDA kot primerljivo zanimiva država, katere vloga ameriških obveščevalnih služb je izjemno pomembna za svetovno ravnovesje na tem področju.

Za navedeni državi lahko ugotovimo, da se je ekonomska obveščevalna dejavnost razvila v okviru različnih diskurzov. Za ZDA velja, da je na podlagi relacije države in trga predvsem varnost njihove ekonomije pogoj za morebitne državne intervencije na trgu, kar je rezultiralo s tem, da je ekonomska varnost postala kriterij delovanja obveščevalnih služb. V drugi obravnavani državi, Franciji, je uveljavljanju te dejavnosti botrovala državna birokracija s tako imenovano geo-ekonomsko argumentacijo. V Franciji se je predvsem širilo pristojnosti za obravnavano področje dela obveščevalnih služb, medtem ko sta bila v ZDA zaradi zapletene strukture obveščevalne skupnosti na novo ustanovljena Podporni center (posredovanje informacij podjetjem) in Nacionalni ekonomski svet (politično odločanje). Za združene države lahko velja ocena, da je pri njih največji uporabnik obveščevalnih informacij vojaško-industrijski sistem.

Kot primer sta torej izbrani državi, kjer so finančne oziroma materialne omejitve glede obravnavane tematike bistveno manj vplivale na razvoj obveščevalnega sistema za razliko od nekaterih drugih držav, kjer finančne omejitve močno kreirajo in posegajo v razvoj in vzdrževanje globalnega varnostnega sistema.

4.7.1 Združene države Amerike

Združene države imajo zelo dolgo tradicijo razvejanih služb za zaščito svojih ekonomskih interesov. Že med drugo svetovno vojno sta na ekonomskem področju delovala Odbor za ekonomsko bojevanje in Urad za strateške cilje, vendar pa je kmalu po vojni ključno področje zbiranja ekonomskih informacijo prešlo pod okrilje Osrednje obveščevalne agencije (CIA). Po nastanku obdobja hladne vojne je bila večina aktivnosti CIA povezana z ocenjevanjem gospodarskih sposobnosti tedanje kontra supersile Sovjetske zveze, in sicer do druge polovice sedemdesetih let. Zaradi globalizacijskih sprememb in nove porazdeljenosti gospodarske moči je bila obveščevalna pozornost ZDA preusmerjena h gospodarski rasti evropskih držav, Japonski in v zadnjih letih Kitajski ter spremljanju trgov strateških surovin.[36]

Združene države imajo dobro in široko razvejano obveščevalno dejavnost, kjer se akterji delijo glede na metode dela ter območno in področno naravo. Pobliže si oglejmo strukturo delovanja ekonomske obveščevalne dejavnosti:

- CIA: Osrednja obveščevalna agencija s pristojnostmi zbiranja obveščevalnih informacij na vseh področjih, njena dejavnost pa je usmerjena v tujino.
- NSA: Nacionalna varnostna agencija, ki je pristojna za obveščevalne naloge na področju kripto zaščite, dešifriranja in varovanja ameriških komunikacij.
- FBI: Zvezni preiskovalni urad, pristojen za področje protiobveščevalnega dela in je krajevno omejen na državno območje.
- Urad za obveščevalno dejavnost in raziskave ima pristojnosti na področju zunanjih zadev in je strukturno umeščen v zunanje ministrstvo.

[36] S predsedniško direktivo nacionalne varnosti številka 67 iz leta 1992 so se določile njihove prioritete in so v ta namen ustanovili tri institucije: Nacionalni ekonomski svet, Odbor za koordinacijo in pospeševanje trgovine ter Podporni center (Advocacy Center) kot koordinacijsko telo.

- Na področju nadzora in finančne discipline deluje oddelek, ki se ukvarja z zbiranjem in obdelavo javnih virov ter s finančnimi politikami tujih držav.
- Urad za raziskovanje in razvoj v ministrstvu za energetiko, ki je zadolžen za ocenjevanje energetskih kapacitet in jedrsko energijo.
- V resor za zunanjo trgovino so umeščeni Urad za obveščevalne zveze, Obveščevalni urad za izvoz in Urad za oskrbo obveščevalnih.

Ugotovimo lahko, da združene države pravzaprav javno ne negirajo koriščenja tajnih metod in sredstev za zbiranje ekonomskih informacij. V ta namen zagovarjajo doktrino o upravičenosti in zaščiti njihovih nacionalnih interesov ter konkurenčnosti na tujih trgih. Tako pridobljene informacije sistemsko uporabijo kot informacijsko podporo svoji diplomaciji. Za razumevanje ameriške doktrine o siceršnji in ekonomski obveščevalni dejavnosti je torej treba imeti v vidu diskurz o ekonomski varnosti, saj kot močna gospodarska sila na eni strani obsojajo ekonomsko vohunstvo za večjo konkurenčnost podjetij, po drugi strani pa zanikajo ali pa opravičujejo lastno izvajanje takšne dejavnosti. Del že omenjene doktrine je zagotovo prevzem njihovih stališč s strani drugih držav kot sprejemljive norme v mednarodni skupnosti. V tem kontekstu mora takšna politično in ekonomsko dominantna sila tolerirati *free riding* drugih držav in se vsaj začasno distancirati od reciprocitete ukrepov. (Andolšek 2003)

4.7.2 Francija

Francija ima enega najstarejših evropskih obveščevalnih sistemov in zato bogato tradicijo tudi na ekonomskem področju. Francoske obveščevalne službe imajo skozi dolgo tradicijo različnih družbenih sistemov pridobljene resurse, ki presegajo državne okvirje, saj je bila Francija kolonizacijska država, ki je stoletja s pridom koristila izsledke službe na področju ekonomske obveščevalne dejavnosti. Po obeh svetovnih vojnah, predvsem pa po obdobju tako imenovane hladne vojne, je ta dejavnost postala predmet državnega strateškega načrtovanja in se je na ravni birokracije transformirala v eno izmed pomembnih javnih politik ter bila predmet ekonomsko-teoretskega pristopa. Kot je bilo v gradivu že omenjeno, je francoska moderna osnovna doktrina o ekonomski obveščevalni dejavnosti utemeljena na tako imenovani geo-ekonomiji. Iz tega koncepta se je po evropskih političnih spremembah leta 1990 razvil tako

imenovani nov strateški koncept ekonomska vojna (guerre économique), kar v bistvu pomeni ekonomsko bojevanje, v katerem je osnovni vir moči v mednarodnih odnosih ekonomska moč države. (Lucas 2001)

Omeniti je treba tudi delovanje francoskega sistema ekonomske obveščevalne dejavnosti, v katerem so najpomembnejši naslednji organi: Splošni komisariat za načrtovanje, Komite za konkurenčnost in ekonomsko varnost, Medresorski komite za obveščevalno dejavnost, Generalna direkcija za zunanjo varnost (DGSE), Direkcija za nadzor območja (DST), Osrednja direkcija za splošno informativno dejavnost in Center za analize in prognoze v Ministrstvu za zunanje zadeve. Čeprav so pristojnosti ustrezno zakonsko razmejene, službe znotraj sistema med seboj strokovno sodelujejo.

Ob navedenem je treba poudariti združitev služb pod okrilje ministrstva za ekonomijo, in sicer kot Varnostni oddelek za gospodarske strateške informacije (SISSE), ki sodeluje z ustreznimi ministrstvi, ključnimi za varovanje francoskega gospodarstva ter njihovih specifičnih industrijskih in znanstvenih interesov. SISSE je ključni faktor pri pripravi uradnih stališč do tujih naložb, prav tako pa je njegova prioriteta obveščanje državnih organov, gospodarskih subjektov in organizacij glede na možen obstoj groženj francoskim strateškim interesom.

Francoski Splošni komisariat za načrtovanje je že leta 1994 objavil splošno sprejeto študijo o tveganjih v informacijski družbi, na podlagi katere je bilo sprejetih pet strateških oziroma ključnih elementov na področju delovanja ekonomske obveščevalne skupnosti v državi:

- pomen organizacije pretoka in uporabe ekonomskih informacij za mednarodno konkurenčnost,
- razvoj konkurenčne obveščevalne dejavnosti kot poslovne storitve na trgu informacij,
- aktivna vloga države v razvoju ekonomsko obveščevalne dejavnosti,
- poslovna obveščevalna dejavnost kot dodana vrednost gospodarskih subjektov,
- poslovna obveščevalna dejavnosti kot del sistema nacionalne varnosti.

Na podlagi navedenih izsledkov in sprejete strategije delovanja obveščevalne gospodarske dejavnosti Francije je bil po ameriškem vzorcu ustanovljen Komite za konkurenčnost in ekonomsko varnost.

Ugotovimo lahko, da je sistem francoske obveščevalne dejavnosti med drugim usmerjen tudi v vzpostavljanje ravnotežja z ZDA in k stremljenju oziroma težnji po tesnejšem in skupnem sistemskem obveščevalnem sodelovanju na ravni Evropske unije.[37]

4.8 Kazniva dejanja na področju gospodarskega vohunstva – primer ZDA

Mnoge države posebej ne opredeljujejo, klasificirajo ali evidentirajo storitev kaznivih dejanj s področja gospodarske kriminalitete glede na njihovo specifiko. Še posebej to velja za primere gospodarskega vohunjenja, kjer so pojavne oblike zelo različne. Slovenija to ozko področje statistično zajame kar v področje gospodarske kriminalitete. Na tak način je seveda težko pripraviti ustrezno strategijo boja zoper vse bolj razširjeno kriminaliteto s področja gospodarskega vohunstva.[38] Kot je bilo v nalogi že omenjeno, bi bilo treba specificirati pojavne oblike gospodarskega vohunjenja in jih tudi ustrezno klasificirati v slovenskih področnih zakonih – KZ in ZKP. Za slednje pa bo treba nekaj več posluha politike in stroke. Manko smo zaznali

[37] Evropska unija ima težave z razvojem skupnega koncepta na področju obveščevalne dejavnosti kot dela skupne zunanje in varnostne politike. Države članice imajo glede sodelovanja na tem področju različna stališča, Francija pa daje prioriteto razvoju in dvigu skupne evropske obveščevalne sposobnosti.

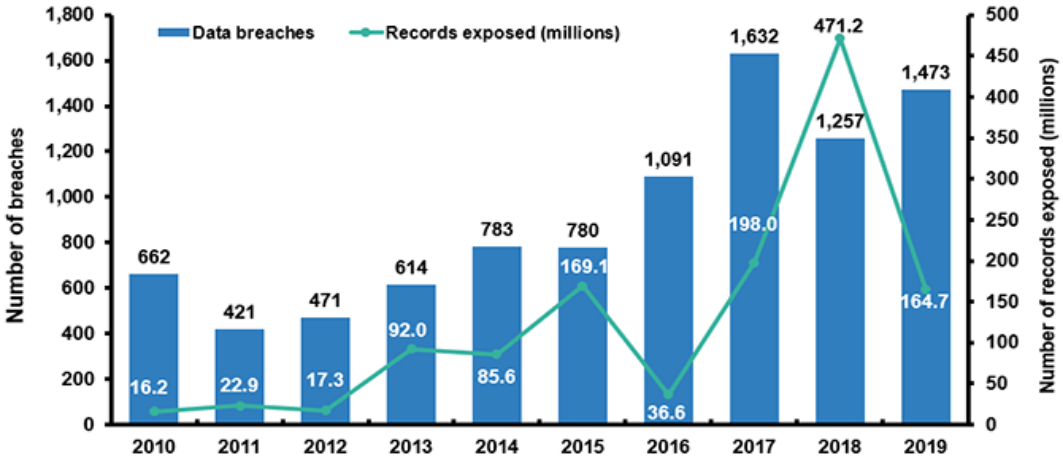
[38] Slovenska sistemska ureditev tega področja se je pričela v letih 2016 in 2017, in sicer z vladno Strategijo kibernetske varnosti in Sklepom o ustanovitvi, nalogah in organizaciji Urada Vlade RS za varovanje tajnih podatkov (UVTP), kar pomeni, da je UVTP pristojni organ nacionalnega sistema informacijske varnosti. Na operativni ravni pa delujeta dve instituciji, in sicer SI-CERT ter CSIRT. Slovenija je realizirala prenos Direktive 2016/1148/ES, Evropskega parlamenta in Sveta z dne 6. julija 2016 o ukrepih za visoko skupno raven varnosti omrežij in informacijskih sistemov v naš pravni red, in sicer z Zakonom o informacijski varnosti (ZInfV).

tudi v nekonkretizirani klasifikaciji modus operandi tipa kibernetičnega kriminala v slovenski kazenskopravni zakonodaji. (Kekec 2017)

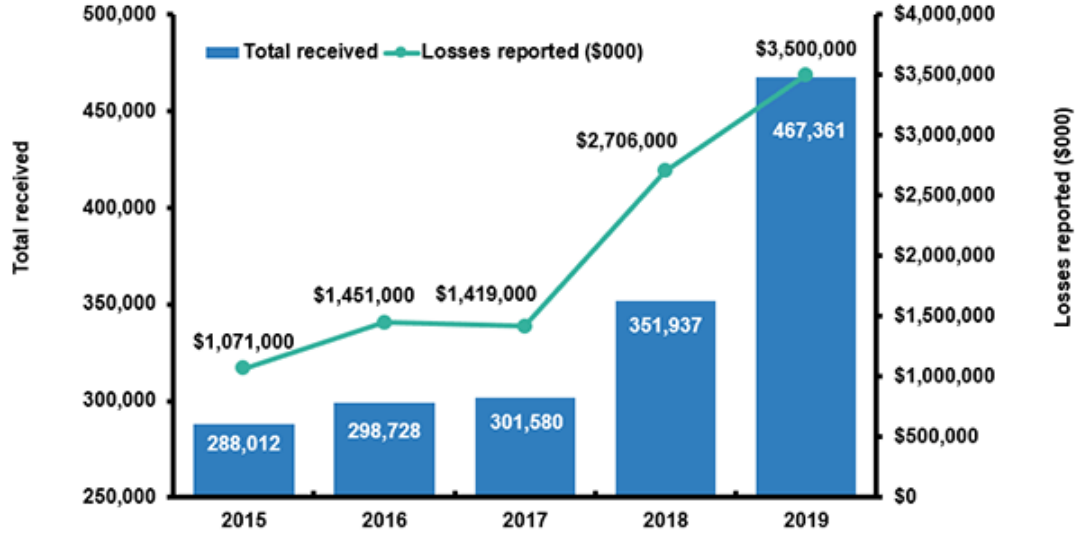
Na podlagi izsledkov študije ameriškega instituta Insurance Information Institute – III se ugotavlja, da kibernetsko kriminalno ogrožanje še naprej narašča, predvsem zaradi kršitev pridobivanja podatkov v prepogosti izpostavljenosti podjetij. Zanimiv je podatek, da je na primer v letu 2017 največji ameriški kreditni urad Equifax Inc utrpel vdor v sicer zaščiteno tajno datoteko, ki je razkril osebne podatke kar stopetinštirideset milijonov ljudi. V letu 2019 se je število nezakonitih kibernetskih vdorov glede na predhodno leto podvojilo. V navedenem letu je bilo zaznano enormno število kaznivih dejanj z uporabo kibernetskih znanj in tehnike, med njimi izstopata oškodovana gospodarska subjekta Capital One Financial Corp (s približno sto milijoni razkritih tajnih poslovnih zapisov) in Adobe Creative Cloud (s približno sedmimi milijoni nedovoljenih posegov). V povprečju so bili v ZDA gospodarski subjekti v letu 2019 žrtev kriminalnih napadov na navedenem področju s pomočjo kibernetske programske opreme vsakih 14 sekund. Zaskrbljujoč je podatek, da medtem ko več organizacij kupuje zavarovanje za zaščito pred tveganjem, zahteve po odkupnini naraščajo, saj napadalci običajno vnaprej poznajo vrednost gospodarskega subjekta in tako ocenijo, ali je podjetje sposobno izpolniti njihove izsiljevalske zahteve.

Z navedeno študijo je bilo ugotovljeno, da je bilo v letu 2019 zaznanih 1.473 kršitev, kar je 17 odstotkov več kot v letu 2018, vendar še vedno pod rekordnim številom kršitev iz leta 2017, ko jih je bilo 1.632. Zaradi tega je bilo v letu 2019 prizadetih 163,7 milijona občutljivih oziroma tajnih osebnih podatkov, kar je sicer za 65 odstotkov manj kot leta 2018, ko je bilo z nezakonitimi hekerskimi vdori odkritih kar 471,2 milijona podatkov.

V letu 2019 predstavlja poslovni sektor 44 odstotkov vseh kršitev; na področju zdravstva 39,4 milijona občutljivih zapisov in na področje izobraževanja 2,3 milijona občutljivih zapisov. Bančništvo je bilo tedaj oškodovano za približno 108 milijonov ameriških dolarjev. Za primerjavo predstavljamo grafična prikaza trenda razkritih podatkov za obdobje 2010–2019 in kazenski pregon storilcev kibernetskega kriminala (Cyber Crime) v obdobju 2015–2019.



Slika 4: Statistični prikaz kibernetskih vdorov
Vir: Publications Office of the EU (2019)



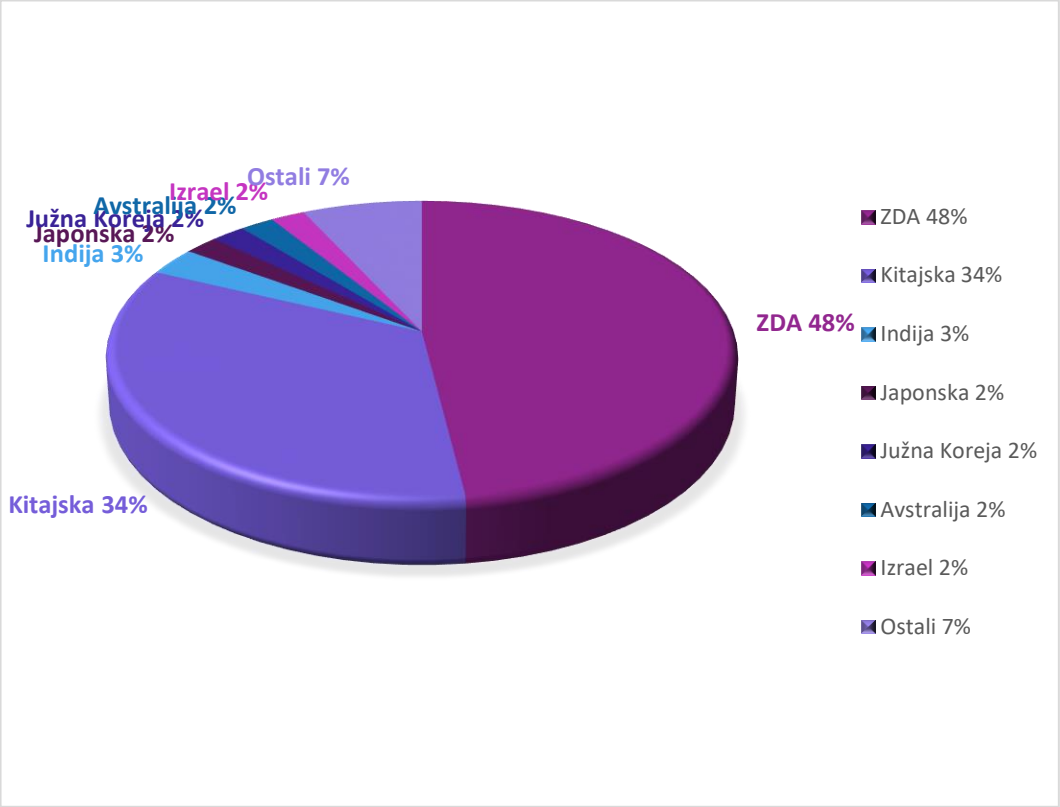
Slika 5: Statistični prikaz odkritih storilcev
Vir: Publications Office of the EU (2019)

Navedena študija zajema tudi klasifikacijo podatkov pravosodnega ministrstva DOJ (Department of Justice), ki so jih pridobili na podlagi kazenske evidence. Iz prve tabele je razviden trend gospodarske kriminalitete s pomočjo vohunstva (kršitev določb EEA – Economic Espionage Akt oziroma Zakona o ekonomskem vohunjenju) glede na nacionalnost storilcev, v naslednji tabeli pa so zajeti statistični podatki in trend storilcev po rasni pripadnosti. Slednje zahteva naš posebni komentar oziroma opazko, saj je na podlagi splošno priznanih standardov človekovih pravic sporno, če

ne celo nezakonito klasificiranje podatkov po spolu in narodni pripadnosti, še posebej glede na pozitivno pravno regulativo v Sloveniji in v ostalih državah EU .

Z navedeno študijo se je ugotovilo, da je šlo v 48 % zaznanih kriminalnih primerih kraje poslovne skrivnosti za oškodovane ameriške korporacije in druge gospodarske subjekte. V 34 % primerov so imele ameriške oškodovane družbe sedež na Kitajskem, ostali delež pa pripada družbam s sedežem v Indiji, Južni Koreji, Avstraliji, Izraelu in na Japonskem.

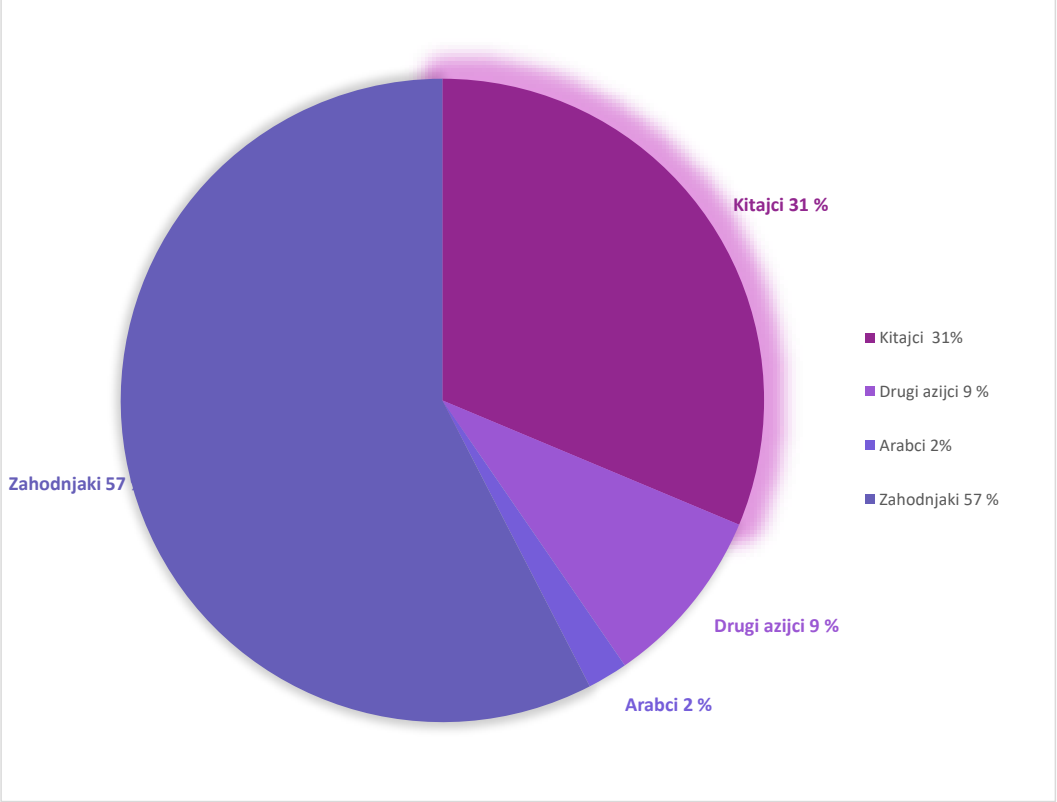
Za lažjo predstavitev trendov sta bila na podlagi podatkov navedene študije pripravljena tudi tortna diagrama.



Slika 6: Prikaz oškodovanih gospodarskih subjektov glede na njihov sedež
Vir: Kim, Andrew Chongseh (2018)

Posebej bi se dotaknili izsledkov v drugem diagramu, kjer je prikazan trend zastopanosti storilcev kibernetskih kaznivih dejanj po rasni pripadnosti, o čemer je bilo govora že v enem od prejšnjih odstavkov.

Študija zajema ločeno statistiko storilcev ter deli na: kitajsko narodnost in ostalo Azijo, arabski svet in zahodnjake. K slednjim so zajeli državljane ZDA, Avstralije, Velike Britanije, Nove Zelandije in držav EU.



Slika 7: Statistični prikaz storilcev glede na rasno in nacionalno pripadnost
Vir: Kim, Andrew Chongseh (2018)

Ob zaključku tega poglavja lahko ugotovimo, da države k obravnavanemu področju pristopajo z različno stopnjo pozornosti. Medtem ko nekatere kot kazniva ravnanja zelo precizno opredeljujejo vohunstvo nasploh, nekatere pri tem zamujajo. Ugotovili smo, da pri tem tudi naša država ni izjema in bi bil sprejem lex specialis za to področje pravzaprav nujen.

Ugotovili smo, da sprejetje in implementacija v pravni red sicer sami po sebi ne preprečujeta kaznivih dejanj, vendar je ustrezna pravna podlaga temelj, na katerem se gradi zaupanje v trdnost gospodarskega sistema neke države. Glede zakonitosti delovanj obveščevalnih subjektov pa smo ugotovili, da sta na gospodarskem področju dopustnost in kaznivost zelo jasno normativno razmejena.

5. ZAKLJUČEK

Zgodovinski pregled obveščevalne dejavnosti je identificiral nadzorovanje kot osnovno funkcijo obveščevalne dejavnosti, ki se ohranja vse do danes. Namen teoretične razprave o sami dejavnosti je bil opozoriti na odnos med obveščevalnimi službami kot subjekti proučevanja mednarodnega okolja in opredeliti njihovo vlogo pri spreminjanju tega okolja neposredno ali posredno s posredovanjem informacij za politično odločanje. Izpostavili smo, da gre tudi pri načrtovanju dela obveščevalnih služb za politiko (policy), ki je odvisna od družbenega konteksta, identitete in interesov. Uvajanje pojma obveščevalne politike ima za cilj veliko bolj jasno poudariti vlogo naročnika in obveščevalnih služb v obveščevalnem ciklusu. Prikazali smo razlike v obveščevalnih politikah, oblikovanih na različnih konceptualnih opredelitvah ekonomske obveščevalne dejavnosti, ki jo mnogi avtorji utemeljujejo s podobnimi ekonomsko teoretskimi pristopi.

Z vidika ene naših tez, da je ekonomska obveščevalna dejavnost lahko vzvod in ovira gospodarskega razvojnega dohitevanja, je težko ex ante opredeliti konkretno merljivi dejanski razvojni učinek informacij na gospodarstvo. Pri tem imata pomembno vlogo tudi interpretacija informacije in njena uporabnost. Ugotavljamo, da zgodovinski zgled v nalogi obravnavanih držav potrjuje tezo, da se gospodarsko vohunjenje intenzivira s stopnjo konkurenčnosti in vplivom določenega gospodarskega subjekta na trgu. S tem pa omogoča konkretni lokalni ekonomiji razvojno dohitevanje pod pogojem, da je sistem ekonomske obveščevalne dejavnosti dobro organiziran in delujoč. Doseženi pa morajo biti še nekateri drugi pogoji, med njimi pa najpomembnejša: kooperativni odnos med državo in ekonomskimi subjekti ter učinkovita organizacijska struktura hitrega pretoka informacij, sposobna ustvarjati pozitivne sinergične učinke glede na zunanje ekonomije. Pridobljene informacije o zunanjem okolju države in tujih podjetij vplivajo na večjo fleksibilnost in odzivnost pri oblikovanju ekonomskih politik glede na spremembe v okolju. Te trditve smo argumentirano omenili v več poglavjih pričujoče naloge.

Ekonomska doktrina nas uči, da nove informacije zmanjšujejo tveganja, ki so lahko kritična ali celo usodna za razvoj podjetja, saj med drugim omogočajo bolj učinkovito rabo resursov. Gre torej za pomoč pri uveljavljanju sprememb, ki sledijo preoblikovanju ekonomske politike, saj je le-ta med najpomembnejšimi uporabniki informacij in ima vlogo posrednega organa med obveščevalnimi službami in gospodarskimi subjekti pri nastopanju na mednarodnem trgu. Obveščevalne službe praviloma posedujejo bogata specifična strokovna in organizacijska znanja na področju zbiranja, obdelave in analiziranja informacij. Prav zaradi tega so se tudi nekatere (v tej nalogi obravnavane) države odločile za organizacijo ločenih specializiranih obveščevalnih služb v okviru državne uprave. To je zagotovo rezultiralo intenziviranje zbiranja informacij z namenom posredovanja podjetjem in drugim v luči krepitve njihovih konkurenčnih pozicij. Na podlagi teh naših ugotovitev lahko potrdimo kot koristno in uporabno pri raziskavi tudi našo predpostavko, da imajo tako slovenske kakor tudi druge obveščevalce službe določen vpliv na gospodarske subjekte. To trditev zagovarja več teoretikov. (Fujs 2011)

Ko je govora o ekonomskem vohunjenju in ekonomski obveščevalni dejavnosti nasploh, je treba poudariti, da gre za državno podpiranje povsem konkretnih gospodarskih subjektov, ki so strateškega pomena za gospodarstvo. Glede na intenzivnost in ekonomsko upravičenost vohunjenja smo ugotovili, da so glede tega prakse držav različne, saj je od slednjih odvisno, ali so ob zavedanju cost-benefita pripravljene sprejeti tveganja, povezana z ekonomskim vohunjenjem. Ob tem pa je treba povedati, da kljub civilnemu in državnemu nadzorstvu delovanja obveščevalne dejavnosti še vedno obstaja nadzorna potreba glede spoštovanja človekovih pravic.

Ekonomska obveščevalna dejavnost bi morala prvenstveno služiti obvladovanju zunanjega ekonomskega okolja držav in v kontekstu oblikovanja razvojno naravnanih politik, čeprav se ugotavlja, da daje tudi možnost razvojne vrzeli z nadziranjem in omejevanjem pretoka informacij in znanj.

Splošna ugotovitev je, da je obveščevalna dejavnost v zadnjih dveh desetletjih doživela temeljito preobrazbo, saj ni več v izključni domeni državnih organov, kar je med drugim posledica naglega razvoja informacijske tehnologije in vpliva globalizacije. Na ekonomskem področju nudi pomemben temelj stabilnosti držav in konkurenčni napredek gospodarskih družb.

Kot smo že ugotovili v prejšnjih poglavjih, temelji del obveščevalnih aktivnosti na področju gospodarstva, na legalnem pridobivanju, vrednotenju, analiziranju in distribuciji podatkov. Del obveščevalne dejavnosti pa seveda pripada tako imenovanemu gospodarskem vohunjenju, ki ima ilegalno oziroma kaznivo konotacijo. Tudi v procesu globalizacije ima skrb za varovanje poslovnih skrivnosti in tržnih prednosti vse večjo vrednost, saj so se gospodarski subjekti znašli v položaju, ko morajo svojo eksistenco graditi v razvojnem sorazmerju s konkurenco ali pa se gospodarsko vohunjenje intenzivira s stopnjo konkurenčnosti gospodarskega subjekta na trgu. Tudi zato je tolikšen interes po spremljanju razvojnih in prodajno poslovnih dejavnosti konkurenčnih družb, kar je rezultiralo s težnjami po izvajanju ukrepov za pridobivanje informacij o poslovanju konkurenčnih družb, kadrovskih potencialih konkurenčnih gospodarskih družb, tržnih študijah in svetovalnih storitvah. Posledično so zasebne svetovalne agencije, ki so se v zadnjih dvajsetih letih pojavile tudi v nezahodnih državah EU, svojo dejavnost močno razširile. Tako lahko potrdimo tudi našo tezo, da se gospodarsko vohunjenje intenzivira s stopnjo konkurenčnosti in vplivom določenega gospodarskega subjekta na trgu.

Lahko ugotovimo, da sistemsko obravnavanje obveščevalne dejavnosti na ekonomskem področju v naši državi le počasi lovi povezavo predvsem glede na zahodnoevropske države. O specifiki je govora v prejšnjih poglavjih, tukaj pa velja omeniti relativno majhnost našega trga, ki nekako v kvalitetni premo sorazmernosti glede obveščevalnega interesa drugih držav bdi nad vdori tujih služb in gospodarskih subjektov v naš gospodarski prostor. K temu je treba dodati, da naša (predvsem izvozno naravnana) podjetja dajejo zaščiti lastnih poslovnih skrivnosti vse večji poudarek, k čemur jih seveda silijo razmere na trgu, ki zahtevajo vlaganja v celovitost varnostnih sistemov v podjetjih.

Ugotavljamo, da se trendi informacijske varnosti spreminjajo zelo hitro, kar pomeni izziv gospodarskim subjektom glede odločitev varovanja svojih podatkov. Kot že omenjeno, obstaja mnogo različnih metod upravljanja informacijske varnosti, hkrati pa se ponuja možnost certificiranja in sistematičnega preverjanja varnosti. Porajajo se nova vprašanja o uporabi storitev v tako imenovanem oblaku in zagotavljanju varnosti informacij na oddaljenih strežnikih. Podjetja morajo zagotoviti zadostno varnost svojih informacijskih sistemov, da lahko ostanejo konkurenčna na trgu. Ugotovili smo, da se na področju informacijske varnosti pojavlja tako imenovani »etični heking«[39], ki ga naš pravni red eksplicitno ne definira, temveč ga umešča v splošnem pojmu napada na informacijski sistem. V primeru hekinga modus operandi ni drugačen kot pri ostalih oblikah vohunjenja. Razlika je le v obliki odnosov strank, saj gre pri etičnem hekingu za pogodbeni dogovor med dvema strankama.

Ob raziskavi področja gospodarskega vohunstva, ki je temeljna poanta pričujoče naloge, smo dobili pritrdilen odgovor na glede predpostavko, da imajo slovenske in druge obveščevalne službe pomemben vpliv na gospodarske subjekte in uspeli raziskati, pojasniti in potrditi tezi, da se gospodarsko vohunjenje intenzivira s stopnjo konkurenčnosti in vplivom določenega gospodarskega subjekta na trgu ter da predstavlja gospodarsko vohunjenje gospodarskim subjektom grožnjo in oviro pri uspešnem razvoju svoje dejavnosti. Ugotovili smo, da imajo tako slovenske kot tudi druge navedene službe izjemno pomembno vlogo in vpliv na obstoj, razvoj in dinamiko poslovanja gospodarskih subjektov.

Prav tako smo ugotovili, da se gospodarsko vohunjenje premo sorazmerno intenzivira glede na konkurenčnost gospodarskih subjektov in obratno. Gospodarski subjekti spremljajo konkurenco in glede na izsledke intenzivirajo svoj interes tudi na področju gospodarskega vohunjenja, saj je cilj prehiteti konkurenco.

[39] Gre za tujko, ki pomeni vdor v informacijski sistem, kot obliko nedovoljenega zbiranja podatkov v računalniških sistemih.

Izsledki študije gradiva oziroma literature in v nalogi obdelani praktični primeri potrjujejo, da vohunjenje s konotacijo nelegalnosti povzroča grožnjo gospodarskim subjektom, ki se najdejo v enaki ali podobni poslovno-konkurenčni interesni sferi. Ugotovili smo, da gospodarsko vohunjenje ni le grožnja konkurenčnim podjetjem, temveč povzroča posredno ali neposredno škodo.

V nalogi smo sledili zadanim ciljem in glede na predpostavko ter hipotezi dokazali, da relativna majhnost našega trga ne vpliva na intenziteto gospodarskega vohunjenja, temveč je le-to odvisno predvsem od uspešnosti kotiranja nekega gospodarskega subjekta na trgu. Do enakega zaključka smo prišli tudi v primeru obravnavanih držav. Analiza obravnavanih primerov nas prepriča, da je za zajezitev obravnavane problematike nujna varnostno-zaščitna odzivnost gospodarskih subjektov ter države. Slednja je dolžna vzpostaviti učinkovite mehanizme, ki so eden izmed predpogojev uspešnega tržnega gospodarstva. Kot smo ugotovili, med te državne mehanizme sodi tudi ustrezna zakonodaja in učinkovita obravnava kaznivih ravnanj s strani organov pregona. Ob upoštevanju v nalogi določene predpostavke in analitičnem razčlenjevanju hipotez smo prišli do sklepa, da pravna praznina, teoretično šibka obdelanost in slabi nadzorni mehanizmi v veliki meri omogočajo zlorabe in uspešnejše gospodarsko vohunjenje.

Na podlagi analize v nalogi obravnavanih primerov in drugega zbranega gradiva smo ugotovili, da se tudi slovenske gospodarske družbe zavedajo pomena konkurenčne obveščevalne dejavnosti na gospodarskem področju, saj jo uporabljajo tudi kot orodje za pridobivanje konkurenčne prednosti na trgu. Prav tako smo ugotovili, da je nelegalno gospodarsko vohunjenje neločljiv del konkurenčne obveščevalne dejavnosti, kar nujno ne pogojuje uspešnosti gospodarskega vohunjenja. Menimo, da se podatke v veliki meri lahko pridobi tudi po legalni poti, ki pa je običajno nekoliko zahtevnejša in časovno daljša.

Na podlagi navedenih izsledkov, argumentacije in predvsem potrjenih hipotez smo prepričani, da pričujoča naloga prinaša pomemben znanstveni prispevek k osvetlitvi aktualnosti obravnavane teme oziroma problematike.

Naloga vsebuje strokovno argumentiran in jasen pregled odzivnosti naše države in v nalogi obravnavanih držav ter gospodarskih subjektov, kar je lahko učinkovita podlaga za uresničevanje kvalitetnejšega pristopa k zajezitvi obravnavane problematike. S potrjenima hipotezama smo jasno predstavili šibko odzivnost nekaterih gospodarskih subjektov na izzive agresivnih konkurentov in prepočasen odziv države/državnih organov na nove pojavne oblike tega dela področja gospodarske kriminalitete v Sloveniji. Prepričani smo, da izsledki naloge prinašajo pomembno dodano vrednost k osvetlitve pomembnosti obravnavane problematike.

Ob zaključku naloge pa lahko obravnavanim trem temeljnim ugotovitvam glede na naše izsledke dodamo tudi pozitivni vidik, saj gospodarsko vohunjenje sili prizadete gospodarske subjekte k ustreznejši zaščiti notranjih informacij in k intenzivnejšemu ter inovativnejšemu razvoju. Glede na slednje torej ugotavljamo, da ima gospodarsko vohunjenje ob negativni konotaciji lahko tudi pozitivni učinek.

Menimo, da izsledki naloge in potrjeni hipotezi prinašajo kvaliteten kritični pogled na obravnavano problematiko in so lahko podlaga nadaljnjih študij ter ukrepanj. Nenazadnje tudi sugestij zakonodajalcu.

6. REFERENCE

Andolšek, Matej. 2003. Teorija hegemonske stabilnosti: racionalnosti versus konstruktivisti. Teorija in praksa 40, št. 4: 6−21.

Anžič, Andrej. 1996. Vloga varnostnih služb v sodobnih parlamentarnih sistemih – nadzorstvo. Ljubljana: Enotnost.

Anžič, Andrej. 1999. Obveščevalne službe – legalni in legitimni labirinti in izhodi. Revija za teorijo in prakso varstvoslovja 1, št. 1: 5−12.

Anžič, Marko. 2006. Obveščevalno-varnostni vidiki ogrožanj pomembnih gospodarsko poslovnih subjektov. UL, Fakulteta za policijsko-varnostne vede. http://dk.fdv.uni-lj.si/magistrska/pdfs/mag_anzic-marko.pdf (pridobljeno 5. 8. 2020).

Barring, Ludwig. 1970. Vohuni in obveščevalci – od antike do danes. Ljubljana: Mladinska knjiga.

Bazdan, Zdravko. 2016. Poslovno-obavještajne službe, industrijska i gospodarska špijunaža u međunarodnoj ekonomiji. Hrčak, 6. april. https://hrcak.srce.hr/index.php?show=clanak&id_clanak_jezik=250727 (pridobljeno 25 .8. 2020).

Beck, Urlich. 2003. Kaj je globalizacija? Zmote globalizma – odgovori na globalizacijo. Ljubljana: Krtina.

Bergier, Jacques. 1974. Vohunstvo v industriji in znanosti. Ljubljana: Mladinska knjiga.

Blažič, Janez. 2014. PP – primerjalni pregled. Posebne oblike pridobivanja podatkov v okviru protiobveščevalne dejavnosti. Državni zbor RS, 12. junij.

https://fotogalerija.dz-rs.si/datoteke/Publikacije/Zborniki_RN/2014/Posebne_oblike_pridobivanja_podatkov_v_okviru_protiobvescevalne_dejavnosti.pdf (pridobljeno 2. 11. 2010).

Brezovšek, Marjan; Črnčec, Damir. 2007. Demokratična uprava in tajnost podatkov. Ljubljana: Knjigarna FDV.

Britovšek, Jaroš; Ulcej, Dejan; Sotlar, Andrej. 2012. Privatizacija obveščevalne dejavnosti v sodobnem varnostnem okolju. DKUM, 4. junij. http://www.fvv.uni-mb.si/dv2009/zbornik/clanki/britovsek.pdf (pridobljeno 2. 11. 2020).

Britovšek, Jaroš. 2007. Protiobveščevalna dejavnost v sodobni državi. Repozitorij Univerze v Ljubljani, 20. november. https://repozitorij.uni-lj.si/IzpisGradiva.php?id=9216&lang=slv&prip=dkum:15127:d4 (pridobljeno 5. 8. 2020).

Clerc, Philipe. 1997. Economic Intelligence. World information report 89, štev.16: 304.

Črnčec, Damir. 2009. Obveščevalna dejavnost v informacijski dobi. Ljubljana: Defensor.

Črnčec, Damir. 2005. Spremembe v načinu delovanja obveščevalno-varnostnih služb, imperativ uspešnega soočanja s sodobnimi varnostnimi izzivi. 6. slovenski dnevi varstvoslovja, 1-7.

Dvoršek, Anton. 2002. Detektiv – taktika in metodika poizvedovanja & primeri. Ljubljana: SAD.

ECG. 2012. Obveščevalna dejavnost v gospodarstvu. ECG, 20. avgust. http://ecg.si/clanki/obvescevalna-dejavnost-v-gospodarstvu/ (pridobljeno 25. 8. 2020).

Evropska socialna listina. 1999. Uradni list Republike Slovenije št. 7. https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina?urlmpid=199920 (pridobljeno 5. 8. 2020).

Evropska Konvencija o varstvu človekovih pravic in temeljnih svoboščin. 1994. Uradni list Republike Slovenije št. 7 https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/1994-02-0041?sop=1994-02-0041 (pridobljeno 5. 5. 2020).

Fujs, Darjan. 2011. Obveščevalna dejavnost in vpliv na gospodarske službe. DKUM, 20. maj. https://dk.um.si/Brskanje.php?id=57&chkZDat=on&page=66&lang=slv (pridobljeno 5. 8. 2020).

Gaiser, Laris. 2010. Geopolitika, Dinamika mednarodne politike v XXI. stoletju. Radovljica: Didakta.

Gaiser, Laris. 2016. Economic intelligence and world governance, Reinventing States for a New World Order. Il Cerchio SRL. Sistema di informazione per la sicurezza dellla repubblica, 12. julij. https://www.sicurezzanazionale.gov.it/sisr.nsf/approfondimenti/intelligence-economica-per-un-nuovo-ordine-mondiale.html (pridobljeno 5. 8. 2020).

Gaiser, Laris. 2016. Economic intelligence for a new order. Rimini: Il cerchio iniziative editoriali.

Gaiser, Laris. 2019. Economic intelligence in the Slowenian environment. Res novae 4, štev. 1: 93.

Gregory, Sean. 1997. Economic Intelligence in the Post-Cold Was era. Issues of Reform. FAS, 10. februar. https://fas.org/irp/eprint/snyder/economic.htm (pridobljeno 5. 8. 2020).

Gričar, Vitja. 2006. Državna ekonomsko obveščevalna dejavnost. Fakulteta za družbene vede. Repozitorij Univerze v Ljubljani. https://repozitorij.uni-lj.si/IzpisGradiva.php?id=8478&lang=slv&prip=dkum:8726755:d1 (pridobljeno 5. 8. 2020).

Hribar, Gašper; Podbregar, Iztok; Ivanuša, Teodora. 2012. Protiobveščevalna dejavnost - znano, neznano. DKUM. https://www.fvv.um.si/dv2012/zbornik/varnostno_obvescevalna_dejavnost/hribar_podbregar_ivanusa.pdf (pridobljeno 10. 5. 2020).

Insurance Information Institute – III. 2019. Facts + Statistics: Identity theft and cybercrime. https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime (pridobljeno 12. 12. 2020).

Izvedbeni sklep Komisije EU. 2017. Uradni list Evropske unije št.: 2320. https://www.a-tvp.si/storage/app/media/Documents/zakonodaja/predpisi-eu/MiFID/62_izvedbeni_sklep2017_2320.pdf (pridobljeno 5. 11. 2020).

Jelen, Ladislav. 2006. Ekonomsko vohunstvo in upravljanje tveganj. DKUM. https://dk.um.si/IzpisGradiva.php?id=29457&lang=eng (pridobljeno 5. 8. 2020).

Kazenski zakonik. 2011. Uradni list RS, štev. 91. https://www.uradni-list.si/glasilo-uradni-list-rs/celotno-kazalo/201191 (pridobljeno 5. 11. 2020).

Kim, Andrew Chongseh. 2018. Prosecuting Chinese “Spies”: An Empirical Analysis of the Economic Espionage Act. Cardozo law review 40, št. 2. http://cardozolawreview.com/prosecuting-chinese-spies-an-empirical-analysis-of-the-economic-espionage-act/ (pridobljeno 12. 12. 2020).

Kramar, Nina. 2014. Gospodarsko vohunstvo – upravljanje s tveganji. DKUM. https://dk.um.si/IzpisGradiva.php?id=43443&lang=slv&prip=rup:10943901:d5 (pridobljeno 20. 8. 2020).

Kekec, Danilo. 2017. Kibernetske grožnje in odzivanje nanje v logističnih sistemih. Ljubljana: FL.

Kop, Ivo. 2019. Varovanje in zaščita poslovnih skrivnosti. Ljubljana: Gospodarski vestnik.

Krunić, Zoran. 1996. Metode dela obveščevalnih služb – poskus klasifikacije in pomen agenturne metode. Zbornik strokovno znanstvenih razprav, št. 10: 143−154.

Lukanović, Lea. 2017. Računalniška kriminaliteta in varstvo osebnih podatkov. UP – Fakulteta za management. http://www.ediplome.fm-kp.si/Lukanovic_Lea_20171017.pdf https://books.google.si/books/about/Ra%C4%8Dunalni%C5%A1ka_kriminaliteta_in_varstvo.html?id=xjAEtAEACAAJ&redir_esc=y (pridobljeno 20. 8. 2020).

Lucas, Didier. 2001. BdD des Sciences d'Information Introduction à l'intelligence économique et stratégique: Vers un nouveau paradigme de l'interaction concurrentielle http://www.cndwebzine.hcp.ma/spip.php/dist/ecrire/spip.php?article770 (pridobljeno 22. 12. 2020).

Mednarodni pakt o državljanskih in političnih pravicah. 1995. ALAGRAF Ljubljana. https://www.varuh-rs.si/pravni-temelji-cp/ozn-organizacija-zdruzenih-narodov/mednarodni-pakt-o-drzavljanskih-in-politicnih-pravicah/ (pridobljeno 5. 11. 2020).

Moffat, Mike. 2020. Martha Stewart's Insider Trading Case. ThoughtCo , 30. januar. https://www.thoughtco.com/martha-stewarts-insider-trading-case-1146196 (pridobljeno 25. 8. 2020).

Nasheri, Hedieh. 2005. Economic Espionage and Industrial Spying. Cambridge: Cambridge University Press.

Odločba št. U-I.132/15-14. 2018. Ustavno sodišče RS. http://www.us-rs.si/documents/f7/c9/u-i-132-152.pdf (pridobljeno 5. 5. 2020).

Podbregar, Iztok. 2008. Vohunska dejavnost in gospodarstvo. Ljubljana: FVV 2008.

Podgornik, Jernej. 2013. Obveščevalna dejavnost na ekonomskem področju. DKUM. https://dk.um.si/IzpisGradiva.php?id=41136 (pridobljeno 10. 5. 2020).

Potter, Evan. 1998. Economic Inteligence and national security. Ottawa Carleton University press, 1. marec. https://www.cambridge.org/core/journals/canadian-journal-of-political-science-revue-canadienne-de-science-politique/article/economic-intelligence-and-national-securityevan-h-potter-ed-ottawa-carleton-university-press-1998-pp-xii-217/31D3E8632F1406C83D238FB130E88FE9 (pridobljeno 5. 11. 2020).

Pricewaterhouse Coopers Advisory EU Services EESV. 2019. The scale and impact of industrial espionage and theft of trade secrets through cyber. Publications Office of the EU. https://op.europa.eu/en/publication-detail/-/publication/4eae21b2-4547-11e9-a8ed-01aa75ed71a1/language-en (pridobljeno 20. 12. 2020).

Purg, Adam. 2001. Obveščevalne službe. Povezave med obveščevalnimi službami, političnimi sistemi in državno suverenostjo v luči iskanja modela sodobnega obveščevalnega sistema Republike Slovenije. Teorija in praksa 38, št.1: 103−118.

Rishikof, Harwey. 2009. Economic and Industrial Espionage: A Question of Counterintelligence or Law Enforcement? Washington: NSF.

Sicherl, Pavle; Svetličič, Marjan. 2004. Slovensko dohitevanje razvitih: kdaj in kako? Teorija in praksa 2004, št. 41: 418−439.

Sun, Tsu. 1998. Umetnost vojne. Ljubljana: Amileti.

Šaponja, Vladimir. 1999. Taktika dela obveščevalno varnostnih služb. Ljubljana: VPVŠ.

The Office of the National Counterintelligence Executive, 2011. Security Clearance Reform - Current Status. https://www.dni.gov/index.php/ncsc-features/203-about/organization/national-counterintelligence-and-security-center?start=12 (pridobljeno. 20. 8. 2020).

Ustava RS. Uradni list RS št. 33/91-I, 42/97 – UZS68, 66/00 – UZ80, 24/03 – UZ3a, 47, 68, 69/04 – UZ14, 69/04 – UZ43, 69/04 – UZ50, 68/06 – UZ121,140,143, 47/13 – UZ148, 47/13 – UZ90,97,99 in 75/16 – UZ70a). http://pisrs.si/Pis.web/pregledPredpisa?id=USTA1 (pridobljeno 5. 5. 2020).

Vodovnik, Andraž. 2011. Priprava sistemske urejenosti boja zoper terorizem v Avstriji, Hrvaški, Nemčiji, Nizozemski, Veliki Britaniji in Sloveniji. UL FDV, 14. september. http://dk.fdv.uni-lj.si/magistrska/pdfs/mag_vodovnik-andraz.pdf http://dk.fdv.uni-lj.si/magistrska/pdfs/mag.vodovnik-andrsz.pdf (pridobljeno 2. 11. 2020).

Zinrajh, Zvonko. 2005. Demokracija in človekove pravice v postsovjetskih državah Centralne Azije. Dignitas 05, št. 26/27: 79–107.

Zakon o gospodarskih družbah. 2006. Uradni list RS št. 42. https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina?urlurid=20061799 (pridobljeno 5. 5. 2020).

Zakon o industrijski lastnini. 2001. Uradni list RS št. 45. http://www.pisrs.si/Pis.web/pregledPredpisa?id=ZAKO1668 (pridobljeno 5. 11. 2020).

Zakon o obrambi. 2014. Uradni list RS št.103. http://www.pisrs.si/Pis.web/pregledPredpisa?id=ZAKO532 (pridobljeno 5. 11. 2020).

Zakon o parlamentarnem nadzoru obveščevalnih in varnostnih služb. 2003. Uradni list RS št. 26. http://www.pisrs.si/Pis.web/pregledPredpisa?id=ZAKO3455 (pridobljeno 5. 11. 2020).

Zakon o Slovenski obveščevalno-varnostni agenciji. 2004. Uradni list RS št. 20. http://www.pisrs.si/Pis.web/pregledPredpisa?id=ZAKO1884 (pridobljeno 5. 11. 2020).

Zakon o Slovenski obveščevalno-varnostni službi. 2014. Uradni list RS št. 81. http://www.pisrs.si/Pis.web/pregledPredpisa?id=ZAKO1884 (pridobljeno 5. 11. 2020).

Zakon o tajnih podatkih. 2001. Uradni list RS št. 87. http://www.pisrs.si/Pis.web/pregledPredpisa?id=ZAKO2133 (pridobljeno 5. 11. 2020).

7. POVZETEK

Gospodarska obveščevalna dejavnost pridobiva vedno večji pomen na področju ekonomske globalizacije, saj so tarče obveščevalne dejavnosti predvsem uspešni gospodarski subjekti, ki se vse bolj zavedajo pomembnosti varovanja notranjih informacij. Naraščanje gospodarskega vohunjenja in rast zasebnih varnostnih služb nakazujeta, da trend potreb po učinkoviti zaščiti narašča premo sorazmerno z novimi pojavnimi oblikami gospodarskega vohunjenja, čeprav se je za kvalitetno analizo do natančnih podatkov težko dokopati. Oškodovani gospodarski subjekti namreč te podatke prikrivajo, saj za njih to posledično predstavlja zunanji dvom o ugledu organizacije.

Ugotovili smo, da se predvsem ob gospodarski in politični globalizaciji objekti zanimanja obveščevalnih subjektov fokusirajo na ekonomsko področje. Menimo, da je ekonomska obveščevalna dejavnost lahko vzvod in tudi ovira gospodarskega razvojnega dohitevanja najuspešnejših na tem področju, čeprav je konkretni dejanski razvojni učinek informacij na gospodarstvo kratko časovno težko merljiv. V nalogi smo učinkovito potrdili zadano tezo, da se gospodarsko vohunjenje intenzivira s stopnjo konkurenčnosti in vplivom določenega gospodarskega subjekta na trgu, ker omogoča ekonomiji razvojno dohitevanje. Ob slednjem pa mora biti sistem ekonomske obveščevalne dejavnosti dobro organiziran in delujoč (predvsem v smislu kooperativnega odnosa med državo in ekonomskimi subjekti), pretok informacij pa ekspliciten in časovno optimalen, da bo njegova distribucija zainteresiranim gospodarskim subjektom zmožna omogočiti pozitivne sinergične učinke.

Nekatere v tej nalogi obravnavane države so se odločile za sistemsko uzakonjeno organiziranost ločenih specializiranih obveščevalnih služb v okviru državne uprave. To je zagotovo rezultiralo z intenziviranjem dejavnosti in posredovanjem podatkov podjetjem ter drugim za krepitev njihovih konkurenčnih pozicij na trgu. Ugotavljamo, da imajo tako slovenske kakor tudi druge obveščevalce službe določen vpliv na gospodarske subjekte. Lahko ocenimo, da vpliv nikakor ni nepomemben, saj ima tudi v procesu globalizacije skrb za varovanje poslovnih skrivnosti in tržnih prednosti vse

večjo vrednost. Gospodarski subjekti so se namreč znašli v položaju, ko morajo svojo eksistenco graditi v razvojnem sorazmerju s konkurenco oziroma se gospodarsko vohunjenje intenzivira s stopnjo konkurenčnosti gospodarskega subjekta na trgu. Tudi zato je takšen interes po spremljanju razvojno poslovnih dejavnosti konkurenčnih družb. Ugotovili smo, da je s tem tudi ena naših tez, da se gospodarsko vohunjenje intenzivira s stopnjo konkurenčnosti in vplivom določenega gospodarskega subjekta na trgu, z zadovoljivo argumentacijo potrjena.

Gospodarski subjekti so v obveščevalnem krogu torej lahko prejemnik ali naročnik vohunskih storitev, lahko so žrtev ali storilec vohunske dejavnosti, odvisno od položaja, v katerem se na zahtevnem trgu ekonomskih vojn znajdejo. V pričujoči magistrski nalogi smo vse te segmente zajeli in razčlenili. Tudi v upanju, da zainteresiranemu bralcu ponudijo kaj koristnega.

Ključne besede: gospodarski subjekti, poslovna skrivnost, obveščevalni ciklus, gospodarsko vohunstvo, industrijsko vohunstvo, konkurenčno vohunstvo, gospodarsko protiobveščevalno vohunstvo, kibernetsko vohunstvo, etični heking.

8. ABSTRACT

Economic risk to business subjects in aspect of economic espionage

Economic intelligence is gaining more and more importance in the field of economic globalization as the targets of intelligence are primarily successful economic entities that are increasingly aware of the importance of protecting inside information. The growth of economic espionage and the growth of private security services suggest that the trend of needs for effective protection is growing in direct proportion to new forms of economic espionage, although it is difficult to obtain accurate data for quality analysis. The aggrieved economic conceal this information as it consequently represents an external doubt for the reputation of the organization.

We found that especially in the context of economic and political globalization, the objects of interest of intelligence entities focus on the economic field. We believe that economic intelligence can be both a lever and an obstacle to the economic development catching up with the most successful in this field, although the actual development impact of information on the economy is difficult to measure in the short term. In this master's thesis, we have effectively confirmed the thesis that economic espionage intensifies with the level of competitiveness and the influence of a certain economic entity on the market, mainly because it enables the economy to catch up. At the latter, the system of economic intelligence must be well organized and functioning, especially in terms of the cooperative relationship between the state and economic subjects, and the flow of information must be explicit and time-optimal so that its distribution can provide positive economic synergies.

Some of the countries discussed in this thesis have opted for the systemic legalization of separate specialized intelligence services within the state administration. This has certainly resulted in the intensification of activities and the provision of data to companies and others to strengthen their competitive position in the market. This refers to the finding that both Slovenian and other intelligence subjects have certain influence on economic entities.

We can say that the impact is by no means insignificant, as even in the process of globalization, the concern for the protection of business secrets and market advantages is of increasing value. Namely, an economic subject has found itself in a situation where it has to build its existence in a developmental proportion to the competition, or economic espionage intensifies with the level of competitiveness of the economic entity on the market. This is one of the reasons why there is so much interest in monitoring the development business activities of competing companies. Therefore, we can say that one of our theses that economic intelligence (espionage) intensifies with the level of competitiveness and the influence of a certain economic entity on the market is confirmed by satisfactory argumentation.

Therefore, economic subjects (companies) can be the recipients or subscribers of espionage services in the intelligence circle, they can be also the victims or perpetrators of espionage activity, given the role in which they find themselves in the demanding market of economic wars. In the present master's thesis, we have covered and analyzed all these segments. Nevertheless, in hope of offering something useful to the interested reader.

Keywords: economic subjects, trade secret, intelligence cycle, economic intelligence, industrial intelligence, competitive intelligence, economic counter intelligence espionage, cyber intelligence.