Univerza v Mariboru

Fakulteta za logistiko

Doktorska disertacija

MODEL CELOVITEGA ZAUPANJA DRŽAVLJANOV V MATIČNE OBVEŠČEVALNO-VARNOSTNE SLUŽBE: LOGISTIKA APLIKACIJE

November, 2020

Gašper Hribar

Univerza v Mariboru

Fakulteta za logistiko

Doktorska disertacija

MODEL CELOVITEGA ZAUPANJA DRŽAVLJANOV V MATIČNE OBVEŠČEVALNO-VARNOSTNE SLUŽBE: LOGISTIKA APLIKACIJE

Kandidat: Gašper Hribar

Mentor: red. prof. dr. Bojan Rosi

Somentor: red. prof. dr. Iztok Podbregar

November, 2020

Doktorsko disertacijo posvečam ženi in otrokoma, ki so mi nesebično in brezpogojno stali ob strani, me podpirali in motivirali v času mojega doktorskega študija in marsikaj žrtvovali za to, da sem ga zaključil.

Iskreno se zahvaljujem mentorju **red. prof. dr. Bojanu Rosiju** in somentorju **red. prof. dr. Iztoku Podbregarju** za strokovno pomoč, nasvete, pripombe in njun čas, ko sem ju potreboval.

Hvala tudi:

- **staršem, ostalim domačim in bližnjim** za podporo, pomoč in razumevanje;
- **zasl. prof. ddr. Matjažu Muleju** za njegovo znanje, čas, predloge, usmeritve in pomoč;
- **intervjuvancem** za njihove odgovore, s katerimi so bistveno pripomogli k rezultatu doktorske disertacije;
- vsem sodelujočim v anketi leta 2016, še posebej takratnima dekanoma FL UM **red. prof. dr. Bojanu Rosiju** in FVV UM **izr. prof. dr. Andreju Sotlarju**, ki sta omogočila izvedbo ankete med študenti in zaposlenimi;
- **mag. Mariji Smolić** za lektoriranje, še posebej pa za njen čas, voljo, požrtvovalnost, pomoč in razprave;
- **(še enkrat) ženi –** za vsak slučaj, da ne bo potem kaj narobe.

Povzetek

Doktorska disertacija obravnava temo, ki je bila po naši vednosti redko obravnavana v dostopni znanstveni literaturi. Celovito opredeljuje zaupanje državljanov v matične obveščevalno-varnostne službe, dejavnike, ki vplivajo na to vrsto zaupanja ter predlaga model za vzpostavitev in vzdrževanje celostnega zaupanja. V skladu z izbranimi sistemskimi teorijami in njihovimi metodologijami za inovacije in uporabo inovacij smo razvili posebne smernice in priporočila za aplikacijo modela ter logistiko aplikacije. Opisana raziskava temelji na analizirani javno dostopni literaturi s področja zaupanja (na splošno in specifičnih vrst zaupanja), sistemskih teorij ter obveščevalno-varnostnih služb, hkrati pa ponuja svojo definicijo zaupanja (na splošno), celovitega zaupanja in celovitega zaupanja državljanov v matične obveščevalno-varnostne službe.

Ključne besede: obveščevalno-varnostne službe, zaupanje, zadostna in potrebna celovitost, model, logistika aplikacije

UDK: 005.336.6:355.40(043.3)

Holistic Model of Citizens' Trust in Domestic Intelligence and Security Services: Application Logistics

Doctoral thesis addresses a topic that has rarely been addressed in the available scientific literature, according to our knowledge. It comprehensively defines citizens' trust in the domestic intelligence and security services, identifies the factors influencing this type of trust, and proposes a model for establishing and maintaining holistic trust. Specific guidelines and recommendations for the application of the model (and application logistics) have been developed in accordance with selected system theories and their methodologies for innovation and application of innovations. The research described is based on the analysed publicly available literature in the field of trust (in general and specific types of trust), systems theories, and intelligence and security services, while offering its definition of trust (in general), holistic trust, and holistic citizen's trust in the domestic intelligence and security services.

Keywords: Intelligence and Security Services, Trust, Requisite Holism, Model, Application Logistics

UDC: 005.336.6:355.40(043.3)

Kazalo vsebine

Kazalo slik

Kazalo tabel

Seznam kratic

AH	Alkotmányvédelmi Hivatal
AISI	Agenzia Informazioni e Sicurezza Interna
BIA	Bezbednosno-informativna agencija (Безбедносно-информативна агенција)
BND	Bundesnachrichtendienst
CIA	Central Intelligence Agency
CSIS	Canadian Security Intelligence Service
DGSI	Direction générale de la sécurité intérieure
DOMR	Dialektično-omrežno razmišljanje
DP	delni program
DTS	Dialektična teorija sistemov
DZ	Državni zbor Republike Slovenije
EKČP	Evropska konvencija o človekovih pravicah (polno ime: Evropska konvencija o varstvu človekovih pravic in temeljnih svoboščin)
EQ	emotional quotient (čustvena inteligenca)
EU	Evropska unija
FBI	Federal Bureau of Investigation
FSB	Federalnaya služba bezopasnosti Rossiyskoy Federatsii (Федеральная служба безопасности Российской Федерации)
GCHQ	Government Communications Headquarters
IQ	intelligence quotient (inteligenčni količnik)
KGB	Komitet Gosudarstvenoj Bezopasnosti (Комите́т Госуда́рственной Безопа́сности)
KNOVS	Komisija za nadzor obveščevalnih in varnostnih služb
MI5	Security Service (UK)
MI6	Secret Intelligence Service (UK)
MSS	Ministry of State Security (中华人民共和国国家安全部, Ministrstvo za Nacionalno varnost Ljudske republike Kitajske)
MVS	Model viabilnih sistemov

NOVOST	Nabor in izbor teme (N), opis izbrane naloge (Op), vrednotenje, analiza podatkov (V), odločitev, preveritev (Od), sprememba dane prakse (S), trajnost, novost (T)
NSA	National Security Agency
OECD	Organizacija za gospodarsko sodelovanje in razvoj (Organisation for Economic Co-operation and Development)
OMR	omrežno razmišljanje
OOOD	opazovanje, orientiranje, odločitev, dejanje
OVS	Obveščevalno varnostna služba Ministrstva za obrambo
Sova	Slovenska obveščevalno-varnostna agencija
SNAV	Svet za nacionalno varnost
SSNAV	sekretariat Sveta za nacionalno varnost
SVR	Služba vnešney razvedki (Слýжба внéшней развéдки)
TVS	Teorija viabilnih sistemov
USOMID	Ustvarjalno sodelovanje mnogih v inovativnem delu
UVTP	Urad Vlade RS za varovanje tajnih podatkov
VKEN	vrednote, kultura, etika, norme
ZPNOVS	Zakon o parlamentarnem nadzoru obveščevalnih in varnostnih služb

Uvod

Nekdanji direktor madžarske obveščevalne službe, diplomat, politik in nekdanji nadzornik reform obveščevalno-varnostnega sistema Bosne in Hercegovine, Kálmán Kocsis, je v svoji predstavitvi na dogodku *Introductory Course on Security Sector Governance and Reform for officials from Bosnia & Herzegovina, Montenegro and Serbia* o reformi obveščevalno-varnostnih služb tranzicijskih držav dejal (Kocsis, 2007, str. 4): »*Obveščevalno-varnostne agencije ne morejo izpolniti nalog brez družbene in politične podpore. Skoraj vse službe so podedovale atmosfero nezaupanja od družbe, medijev, lastnih politikov in celo tujih partnerjev. Pridobiti zaupanje v očeh povprečnih ljudi je najtežja naloga za katerokoli mednarodno agencijo. Politiki niso kaj dosti v pomoč v tem procesu, saj je skušnjava prevelika in poskušajo pridobiti agencije za svoje politične namene. Mediji gledajo službe kot potencialne vire škandalov. In, če sem iskren, osebje služb ne sestavljajo le angeli. Med nami rečeno: angeli niso najboljša kategorija za takšno vrsto osebja. Pridobitev zaupanja je torej neizbežna, vendar zelo težka in dolgotrajna naloga službe.*« (*Bralcem sporočamo, da so vsi citati in parafraze tujih besedil v doktorski disertaciji naši prevodi oziroma prilagoditve.)* Njegove besede ne bi mogle bolje na kratko opisati glavne težave, s katero so se in se še vedno srečujejo obveščevalno-varnostne službe ne le tranzicijskih, temveč tudi post-tranzicijskih držav – s pomanjkanjem in upadom zaupanja državljanov, medijev in politikov v obveščevalno-varnostne službe. Z izrazom *obveščevalno-varnostne službe* pojmujemo obveščevalne, protiobveščevalne in varnostne službe ter njihove kombinacije (Ivanuša, Podbregar & Hribar, 2016, str. 1). Obravnavali smo le obveščevalno-varnostne službe kot organizacije, ki za potrebe države zbirajo podatke in ščitijo državo ter uresničujejo njene interese. Zasebne obveščevalno-varnostne službe zato niso predmet obravnave v doktorski disertaciji. Zaupanje državljanov v matične obveščevalno-varnostne službe se razlikuje od zaupanja v tuje obveščevalno-varnostne službe. Zaupanje v tujo službo namreč predstavlja temelj tajnega sodelovanja z njo, tega pa države opredeljujejo kot vohunstvo in je zato prepovedano in kaznivo. S težavo pomanjkanja in upada zaupanja v obveščevalno-varnostne službe se srečujejo tudi razvite države (glej npr. Baynard et al., 2013, str. 39). Medijske objave o incidentih in aferah, ki so se zgodile v zadnjih letih

in v katere so bile vpletene tuje in slovenske obveščevalno-varnostne službe, ter odziv državljanov nanje dajejo slutiti, da se je zaupanje državljanov vanje zaradi tovrstnih dogodkov zmanjšalo. Tudi vohunjenje ameriške službe National Security Agency (v nadaljevanju: NSA) za lastnimi državljani ter tujimi politiki ter predstavniki tujih držav, teroristični napadi, za katere so državljani delno krivili tudi obveščevalno-varnostne službe, češ da ne opravljajo svojega dela, razkrito nadzorovanje lastnih državljanov kljub zagotovilom pristojnih, da obveščevalno-varnostne službe delujejo zakonito (npr. MI5 in MI6 v Združenem kraljestvu Velike Britanije in Severne Irske (v nadaljevanju: Združeno kraljestvo)), pa tudi domnevno vmešavanje Ruske federacije v predsedniške volitve v Združenih državah Amerike leta 2016 preko njenih obveščevalno-varnostnih služb so le nekateri izpostavljeni primeri, ki vplivajo na upad zaupanja v takšne službe. Našteti primeri so tudi indikatorji, da je na področju obveščevalno-varnostne dejavnosti prišlo do določenih težav, s katerimi se sooča tudi razviti del družbe, ki naj bi imel svoje družbene podsisteme ustrezno organizirane, delujoče in učinkovite ter tako domnevno zakonite, etične in družbeno sprejemljive oziroma sprejete.

Zastavili smo si vprašanje: ali so se te težave pojavile zaradi morebitne in nam neznane globalne spremembe metodologije dela obveščevalno-varnostnih služb? Ponovno smo ugotovili, da ne (glej npr. Hribar, 2013), saj službe že od nekdaj delujejo enako, spreminjajo se le sredstva za izvrševanje nalog, metode se prilagajajo tehnološkemu napredku, ostalo pa je že od nekdaj nespremenjeno (z izjemo tehnoloških aktivnosti in dejavnikov, ki jih v preteklosti zaradi zastarele tehnologije ali njenega neobstoja sploh še ni bilo). Po našem prepričanju v zmanjšanje ali celo izgubo zaupanja zagotovo vodijo tudi nejasno opredeljene okoliščine in negativni vplivi, vendar pomanjkanje zaupanja državljanov v matične obveščevalno-varnostne službe na prvi pogled ne povzroča (velike) škode obveščevalno-varnostnim službam (niti nacionalni varnosti), saj naj bi imeli državljani v skladu s splošnim prepričanjem praktično zanemarljiv vpliv na njihovo delo. Podrobnejše preučevanje tovrstnega zaupanja pa nakazuje, da bi odločevalce (politiko in vodstvo obveščevalno-varnostnih služb) in državljane izguba zaupanja morala skrbeti. Zaupanje je namreč pomemben dejavnik obveščevalno-varnostne dejavnosti (Podbregar, 2016, osebni vir), ki pa mu – glede na naše predhodne poizvedbe

o obstoju znanstvenih in strokovnih prispevkov na temo – ni bilo namenjeno dovolj pozornosti.

Raziskovalci, institucije in države so k neposrednemu in posrednemu razreševanju problema upada zaupanja v praksi pristopile različno. O razreševanju problema govorimo, ker ni nujno, da se problem tudi reši, temveč se ga zgolj poskuša rešiti. Kot pravita Rosi & Rosi (2011, str. 62), je razreševanje neugodnih dogajanj odvisno od »kakovosti izbranega izhodiščnega modela, četudi njegovega nadaljnjega razvoja ne moremo povsem predvideti oz. zanj ne moremo dajati nekih splošno in še manj zanesljivo veljavnih nasvetov […],« in od »ljudi – problemskih razreševalcev, ki se obvladovanja problemov lotevajo različno in z različno uporabo razumske in čustvene inteligence.« Zato je bilo tudi pristopov k razreševanju problema (ne)zaupanja več: s spremembo zakonodaje in politik (npr. v Združenih državah Amerike po tem, ko je »žvižgač« Edward Snowden razkril obstoj in namen t.i. sistema PRISM), z reorganizacijo služb ali z menjavo njihovih kadrov (npr. Črna gora, glej Knežević, 2015), nekatere tudi z uvedbo oziroma poostritvijo nadzora obveščevalno-varnostnih služb po razkritju različnih incidentov. Vendar pa ugotavljamo, da so vse to le simptomi problema (Rosi & Rosi, 2011), ki jih pristojni z vidika dialektične teorije sistemov (v nadaljevanju: DTS) in dialektično-omrežnega razmišljanja (v nadaljevanju: DOMR) niso razreševali celovito. To lahko na kratko pojasnimo z demokratičnim nadzorom obveščevalno-varnostnih služb. Ugotavljamo, da je dokaj razširjeno prepričanje, da je demokratični nadzor najboljše (ali celo edino) zagotovilo, da bodo službe delovale demokratično in se bo povečalo zaupanje državljanov vanje – tako menijo npr. Klaus-Dieter Fritsche, nekdanji nemški komisar za obveščevalne službe na zvezni ravni (Langhorst & Nieke, 2015) ter Goldman & Rascoff (2016). Ne trdimo, da demokratični nadzor ni potreben, niti ne trdimo, da ne deluje tako, kot bi moral. Nasprotno, demokratičen nadzor služb je nujen, vendar ni (edino) zagotovilo za ustrezno, strokovno in zakonito delovanje obveščevalno-varnostnih služb. Po našem mnenju se je vzporedno s tem prepričanjem razvila miselnost, da (bolj) demokratična ureditev sistema nacionalne varnosti in s tem obveščevalno-varnostnega podsistema lahko (raz)reši problem hipotetično nezakonitega delovanja služb, ki je med drugim tudi eden od vzrokov za nezaupanje. Ne oporekamo dejstvu, da le demokratična ureditev omogoča demokratično delovanje

obveščevalno-varnostnih služb, temveč izpostavljamo in hkrati opozarjamo na zmotno prepričanje, da *le demokratična ureditev omogoča zgledno, zakonito ter etično in moralno sprejemljivo delovanje obveščevalno-varnostnih služb, zato so državljani lahko prepričani, da službe delujejo ustrezno – torej jim lahko (brezpogojno) zaupajo*. Kot smo ugotovili in tudi predstavljamo v nadaljevanju, demokratični nadzor obveščevalno-varnostnih služb predstavlja le enega izmed dejavnikov, ki vplivajo na zaupanje, zato predstavlja uvajanje strožjega nadzora le (raz)rešitev za simptom, ne pa za problem. To je tudi eno izmed izhodišč naše raziskave, ki nam preprečuje, da bi se uvodoma usmerili le na nadzor kot na domnevno najpomembnejši vpliv na zaupanje državljanov v matične obveščevalno-varnostne službe.

Navedeno in dejavniki, ki jih prepoznavamo v nadaljevanju doktorske disertacije, negativno vplivajo na zaupanje državljanov v matične obveščevalno-varnostne službe ter s tem pospešujejo njihovo naravno težnjo k propadanju – entropijo. Na podlagi ugotovljenega smo oblikovali ozadje doktorske disertacije: **dejavnik *zaupanje državljanov v matične obveščevalno-varnostne službe* prepoznavamo kot enega ključnih dejavnikov delujočega in učinkovitega obveščevalno-varnostnega sistema, ki bistveno prispeva ne le k ugledu in dolgoročni stabilnosti obveščevalno-varnostnih služb, temveč tudi k ohranjanju nacionalne varnosti, hkrati pa upočasnjuje njuno naravno težnjo k propadanju – entropijo.** Celovito zaupanje državljanov v matične obveščevalno-varnostne službe prepoznavamo kot podporni element sistema nacionalne varnosti ter njegovih podsistemov oziroma kot del strateške logistike nacionalne varnosti, kamor tudi sicer spada obveščevalno-varnostna dejavnost (glej npr. Krapež, 2015; Žirovnik, 2016).

Takšno zaupanje je – kot tudi vsako drugo zaupanje – potrebno ustvariti. Gre za netehnološki invencijsko-inovacijsko-difuzijski proces, saj gre za inovacijo vrednot, kulture, etike in norm občanov, politikov in zaposlenih v obveščevalno-varnostnih službah, o katerih državljani nimajo veliko znanja, vednosti in informacij. Ta proces mora potekati, da bi uspel, po zakonu zadostne in potrebne celovitosti (iz DTS; Mulej, 1979; Mulej et al., 2000, 2008), saj mora zajeti dialektični sistem (tj. soodvisen splet) vseh in samo bistvenih vidikov, ki dajo sinergijo (tj. součinek) vseh njih s součinkovanjem vseh

strok, štetih za bistvene po odločitvi avtorjev, določevalcev ciljev in uresničevalcev ciljev. Proces ne more potekati deterministično, tj. trdosistemsko, s popolno odvisnostjo izidov od vplivov, saj ne gre za stroje, temveč za ljudi kot posameznike in družbene skupine, ampak mehkosistemsko, s sprotnim prilagajanjem zaznanim okoliščinam, skladno z zakonom hierarhije zaporedja in soodvisnosti. Kot operativna tehnika za obvladovanje takšnih okoliščin ustvarjanja zaupanja v navedene službe niso uporabni algoritmi, tipični za trdosistemsko obravnavo, ampak *programoteka*. Bistvo te metode za operativno aplikacijo DTS je v spoznanju, da vsebinsko obstajajo razlike, glede postopkov pa je možno uporabiti izkušnje, a samo okvirno. Uporabi te metodologije lahko rečemo tudi logistika aplikacije danih izkušenj strokovnjakov, da nastanejo organizacijsko postopkovni modeli, ki so uporabni kot okvirni opomniki, ki lastne ustvarjalnosti, inventivnosti in inovativnosti uporabnikov ne nadomeščajo, sploh pa ne kot togi algoritmi, ampak jih podpirajo in spodbujajo. Ker se po nam znanih in dostopnih podatkih prvi ukvarjamo s študijo in ustvarjanjem celovitega zaupanja državljanov v matične obveščevalno-varnostne službe, smo morali poiskati ustrezen (nov) način razreševanja obravnavanega problema. Zato smo pri raziskovanju uporabili tudi metodologijo DOMR (Rosi & Mulej, 2006; Rosi & Rosi, 2011; Rosi, 2015), ki »na nov način združuje vse tiste (enkratne) uporabne značilnosti, ki jih nima nobena od nam znanih metodologij za razreševanje problemov in konfliktov, a jih tako v teoriji kot tudi v praksi stalno potrebujemo.« (Rosi & Rosi, 2011, str. 64)

Raziskovalci in uporabniki morajo v skladu z DTS najprej opredeliti svoja subjektivna (lastno znanje, vednost in vrednote) in objektivna (potrebe in možnosti izven sebe) izhodišča; pri tem uporabijo na programotečni način smernice za opredelitev izhodišč iz DTS. Potem na tej osnovi opredelijo svoj dialektični sistem vidikov, z njim spoznajo in izberejo prednostne potrebe in njim ustrezne možnosti, s sinergijo le-teh pa opredelijo svoje cilje, da ne bi bili enostranski ali celo zgolj želeni, ampak zadostno in potrebno celovito utemeljeni. Sledi priprava na uresničevanje ciljev z uporabo smernic za uresničevanje izhodišč iz DTS na programotečni način, da bi bili na koncu izidi čim bolj skladni z ustreznimi izhodišči. Ves čas potekajo povratne zanke, da se upošteva zakon hierarhije zaporedja in soodvisnosti tudi s procesnega vidika.

Izid je v tem primeru čim večje zaupanje državljanov v obravnavane službe, vmesni izid kot izid doktorske raziskave pa model, po katerem bi tako zaupanje ustvarili kot podlago za omenjeni netehnološki invencijsko-inovacijsko-difuzijski proces.

Z raziskavo smo poiskali vse dejavnike tovrstnega zaupanja in razvili v okviru našega dialektičnega sistema vidikov ustrezno celovito rešitev ali inovacijo, ki bo upočasnjevala entropijo matičnega obveščevalno-varnostnega sistema in sistema nacionalne varnosti ter omogočila razvoj in napredek matičnih obveščevalno-varnostnih služb. Tako bi državljani te službe (s)poznali toliko, kot smejo, in jih sprejeli ter jim verjeli toliko, kolikor je potrebno, se zavedali njihovega obstoja in poslanstva, jim pomagali v okviru svojih zmožnosti ter s tem posredno izboljšali nacionalno varnost države, katere državljani so. To pomeni, da bi državljani matičnim obveščevalno-varnostnim službam zaupali celovito, kolikor je to potrebno za učinkovito in zakonito delo obveščevalno-varnostnih služb ter za zagotavljanje učinkovitega delovanja sistema nacionalne varnosti in za uresničevanje nacionalnih interesov.

Če želimo raziskovati zaupanje, moramo poznati njegovo definicijo. Avtorji, ki jih postopno navajamo skozi besedilo doktorske disertacije, v svojih delih zaupanje različno opredeljujejo na več načinov ter ga delijo na več zvrsti (tipologij). Spoznali smo, da so izbrane oziroma v doktorski disertaciji obravnavane vrste zaupanja deležne različne uporabe. Ta je odvisna od vrste in števila deležnikov (tj. upnikov in zaupnikov) v odnosu ter od področja, na katerem je posamezna zvrst zaupanja obravnavana (npr. ekonomija, psihologija, menedžment, poslovanje, logistika, pravo). Za raziskovanje smo želeli uporabiti splošno definicijo zaupanja, ki ni ozko usmerjena na posamezno področje in na podlagi katere bi nato gradili naš model celovitega zaupanja državljanov v matične obveščevalno-varnostne službe. Hitro smo ugotovili, da to ni mogoče, saj je splošnih definicij več. Čeprav so si podobne, obstajajo med njimi nekatere (tudi bistvene) razlike, zato smo morali izbrati drugačen pristop. Za lažje razumevanje, kaj je zaupanje, smo v veliki množici definicij zaupanja izbrali tiste, ki jih z našega vidika obravnavanja ocenjujemo kot najbolj ustrezne za uvodno opredelitev zaupanja kot splošnega pojma (tj. ne kot zaupanja v kontekstu posameznih znanstvenih disciplin). Zaupanje bomo

kasneje predstavili in pojasnili kot celovit koncept, ki ga je zaradi odvisnosti od konteksta mogoče aplicirati na različna področja, zaenkrat pa jih bomo predstavili le nekaj:

- »Zaupanje je pripravljenost udeleženca biti ranljiv za dejanja drugega udeleženca, ki [pripravljenost biti ranljiv, op. G. H.] temelji na pričakovanjih, da bo drugi udeleženec opravil določena dejanja, pomembna za udeleženca upnika, ne glede na sposobnost spremljati ali nadzorovati drugega udeleženca.« (Mayer, Davis & Schoorman, 1995)
- »Zaupanje definiramo kot pripravljenost biti ranljiv za drugo osebo.« (Schoorman, Mayer & Davis, 2007, str. 347)
- »[Zaupanje je] trdno prepričanje v sposobnost entitete, da deluje zanesljivo, varno in verodostojno znotraj določenega konteksta.« (Grandison & Sloman, 2000 v Kovač & Trček, 2007, str. 7)
- »Zaupanje je lahko definirano kot proces, v katerem se upnik [ang. *trustor*; oseba, ki nekomu zaupa, op. G. H.] zanese na zaupnika [ang. *trustee*; oseba, ki ji je zaupano, op. G. H.] (oseba ali skupina ljudi), da bo deloval v skladu z določenimi pričakovanji, ki so za upnika pomembna, brez izkoriščanja upnikove ranljivosti.« (Martins, 2002, str. 757)
- »Ko pravimo, da nekomu zaupamo ali da je zaupanja vreden, s tem implicitno pravimo, da je verjetnost, da bo ta oseba izvajala aktivnosti, ki so za nas koristne ali ki za nas vsaj niso škodljive, dovolj visoka, da preučimo vključitev v neko obliko sodelovanja s to osebo.« (Gambetta, 1988, str. 217)
- »Zaupanje je kvaliteta socialnih odnosov in vsebuje tri elemente: soodvisnost med akterji, negotovost ali tveganje glede ravnanja drugih udeležencev v transakciji in pričakovanje, da udeleženci v transakciji naše ranljivosti ne bodo zlorabili v svojo korist.« (Lane, 1998 v Rus, 2008, str. 74)

Nekoliko drugačno opredelitev zaupanja ponuja Paliszkiewiczeva (Paliszkiewicz, 2011, str. 318):

- zaupanje je medosebno: med konkretnimi posamezniki in povezano s komunikacijo;
- zaupanje je bolj situacijsko kot pa globalno: zaupanje je dano eni določeni osebi;
- zaupanje je prostovoljno: zaupanje mora izvirati iz odločitve in ne more biti obvezno, občasno je tudi eksperimentalno;

- zaupanje pomeni zavezo, saj je vsaka oseba v odnosu zaupanja odvisna od druge osebe (brez možnosti nadzorovanja druge osebe);
- zaupanje je zavestno: vsaka oseba se zaveda zaupanja druge osebe;
- zaupanje je relevantno v smislu, da posledice zlorabe zaupanja ne morejo biti nepomembne za eno od oseb v odnosu zaupanja;
- zaupanje je dinamično ali začasno, saj se razvija s časom: zaupanje je vzpostavljeno, se povečuje, se zmanjšuje in umre [sic];
- zaupanje je usmerjeno z ukrepi, implicitno v cilje odnosa;
- zaupanje ni linearen proces: če je zaupanju povzročena škoda, bo upadlo; lahko se razvije skozi proces, vendar lahko tudi nazaduje.

V času izvajanja doktorske raziskave in pisanja doktorske disertacije enotna definicija zaupanja (še) ni obstajala. Opazili smo, da raznolikost definicij izhaja iz raznovrstnosti znanstvenih disciplin oziroma področij, v okviru katerih so raziskovalci obravnavali zaupanje. Med takšnimi področji v literaturi zasledimo tudi raziskovanje zaupanja državljanov v javni sektor oziroma v javne institucije (organe/organizacije), kamor lahko uvrstimo avtorja Salminena & Ikola-Norrbacka (2010). To področje je z našega vidika pomembno, saj obveščevalno-varnostne službe, ki jih obravnavamo v doktorski disertaciji, spadajo v javni oziroma državni sektor posamezne države. Poleg načel dobrega upravljanja države in neetičnih dejavnosti prej omenjena avtorja prepoznavata zaupanje državljanov kot enega izmed treh ključnih etičnih vprašanj, ki jih je potrebno preučevati na primeru delovanja države oziroma javne uprave (Salminen & Ikola-Norrbacka, 2010). Obravnavanje tega ni pomembno le za ohranjanje ustrezne etične kulture v javnih institucijah, temveč tudi za normalno in nemoteno delovanje državnega aparata, ki deluje v korist družbe. Temu pritrjujeta Newton & Norris (2000, str. 52), ki pravita, da je upad zaupanja v glavne družbene institucije (tudi državne institucije) veliko večja grožnja demokraciji kot pa upad zaupanja v posameznike, npr. v druge osebe ali politike. V raziskavi na primeru finske javne uprave Salminen & Ikola-Norrbacka (2010) ugotavljata, da pomanjkanje zaupanja državljanov v javno upravo ne vodi nujno v nezadovoljstvo s kakovostjo storitev, potrjujeta pa nasprotno, namreč da zadovoljstvo s storitvami državnih organov povečuje zaupanje državljanov v javne oziroma državne institucije. Ker je optimalna raven zaupanja odvisna od politične in javnoupravne

kulture, politične in državne institucije pa zaradi možnosti zlorabe moči že v izhodišču predstavljajo sistem nezaupanja, si lahko državne institucije oziroma organi pridobijo zaupanje le z dobrimi izkušnjami državljanov in njihovim spoštovanjem, ki ga izkazujejo državnim organom (ibidem). Makarovič (2004, str. 377) na primeru spornega nakupa operacijskih miz v ljubljanskem Univerzitetnem kliničnem centru ugotavlja, da zaupanje v institucijo (poleg objektivne škode) zmanjšuje predvsem subjektivna škoda, ki ima za posledico zmanjševanja zaupanja tudi razkrajanje družbe. Njegovo razmišljanje in ugotovitve zagotovo lahko preslikamo na delovanje vseh subjektov javne uprave oziroma na, kot pravi Makarovič (2004, str. 377-378), »institucije, ki so namenjene splošni družbeni koristi, vendar se z njimi okoriščajo posamezniki ter pri tem uporabljajo pollegalna ali celo izrazito nelegalna sredstva.«

Kovač & Trček (2007, str. 7) pravita, da »[p]odročje varnosti s svojimi storitvami […] še ne zagotavlja zaupanja, je torej potreben pogoj, ni pa tudi zadosten.« Zgolj izvajanje varnostnih nalog oziroma zagotavljanje varnosti tako še ne pomeni avtomatične pridobitve zaupanja od deležnikov, ki so vpleteni v zaupanje (v našem primeru: od državljanov), saj na zaupanje pomembno vplivajo tudi drugi dejavniki. Zaupanje na področju varnosti je torej potrebno obravnavati celovito. Podroben pregled dostopne literature kaže, da je literature, ki obravnava zaupanje v matične obveščevalno-varnostne službe, izjemno malo. Predpostavljamo, da je poleg kompleksnosti problema pomemben razlog za to tudi tajnost, ki, kot menita Fitsanakis & Hodges (2013, str. 18), bistveno razlikuje obveščevalno-varnostne službe od ostalih državnih funkcij oziroma institucij. Zaradi načina delovanja, ki je nujno tajno, je samo delovanje obveščevalno-varnostnih služb javnosti nedostopno in neznano. Domnevamo lahko, da se je v javnosti zaradi tega posledično izoblikovalo mišljenje, da posamezen državljan na matične obveščevalno-varnostne službe ne more vplivati. Če naša domneva drži in se državljani za obveščevalno-varnostne službe ne zanimajo, ker naj bi jim njihovo poznavanje (delovanja) služb preprečevala tajnost, so zato dovzetnejši za (tudi napačne, popačene ali zavajajoče) podatke in informacije o službah iz medijev in drugih virov, ki vplivajo na njihovo znanje in mnenje ter s tem tudi na njihovo zaupanje matičnim obveščevalno-varnostnim službam. Na to želimo navezati del pričanja Jamesa Comeya, nekdanjega direktorja ameriškega Zveznega preiskovalnega urada (*Federal Bureau of Investigation*,

v nadaljevanju: FBI), pred Odborom za obveščevalne zadeve ameriškega Predstavniškega doma dne 20. 3. 2017 o vmešavanju Ruske federacije v ameriške volitve leta 2016 (Washington Post Staff, 2017): »Upam, da boste razumeli, da obstajajo nekatere zadeve, o katerih ne morem komentirati na odprti seji niti ne morem podati specifik o določenih področjih. […] Prosim, ne delajte nikakršnih zaključkov iz dejstva, da ne morem komentirati določenih zadev. Vem, da je špekuliranje stvar človeške narave, vendar ni pravično delati zaključke preprosto zato, ker ne smem komentirati. […] Razumem človeško radovednost glede našega dela in intenziven interes ter […] pogosto špekuliranje glede tega. Vendar ga [dela, op. G. H.] ne moremo opraviti dobro in pravično do ljudi, ki jih preiskujemo, če govorimo o tem.« Comey torej pravi, da mora biti delovanje obveščevalno-varnostnih služb tajno, ne glede na človeško radovednost ali interese javnosti, ki niso upravičeni niti utemeljeni za razkritje tajnih podatkov.

»[Z]aupanje [se] oblikuje na podlagi ugleda oz. priporočil drugih,« (Kovač & Trček, 2007, str. 8) še posebej če oseba (npr. državljan) nima predhodnega znanja o zaupniku (npr. o matičnih obveščevalno-varnostnih službah). Takšno teorijo zagovarjajo tudi McKnight, Cummings & Chervany (1998, str. 478), ki pravijo, da na zaupanje med drugim vpliva tudi dostopnost informacij, ki jih osebe lahko dobijo o njihovem zaupniku: »[Č]e ni dostopnih informacij o specifični situaciji, se bo posameznik zanašal na lastna prepričanja o človeški naravi, ki se odraža kot upanje v človečnost.« Nevarnosti, ki jih prepoznavamo, je več, med večjimi pa je dokazano dejstvo, da na zaupanje v javne institucije bolj vplivajo dejavniki na družbeni ravni kot pa dejavniki na osebni ravni (Newton & Norris, 2000, str. 67). To pomeni, da največji vpliv na zaupanje državljanov v obveščevalno-varnostne službe ustvarja družba; običajnim državljanom zaradi nepoznavanja področja obveščevalno-varnostne dejavnosti navadno predstavljajo vir podatkov oziroma informacij mediji, hkrati pa državljani do služb nimajo izoblikovanega posebnega odnosa. Obenem je tudi splošno znano, da na zaupanje vplivajo pretekle izkušnje in možnosti sodelovanja med upnikom in zaupnikom (v našem primeru med državljani in matičnimi obveščevalno-varnostnimi službami, op. G. H.), kar vpliva tudi na pričakovanja upnikov o vedênju zaupnika (Bijlsma & Koopman, 2003, str. 547). Poleg tega zagotovo ovira izboljšanje zaupanja v obveščevalno-varnostne službe tudi nepoznavanje razlik med obveščevalno-varnostnimi službami (po svetu), razlik med službami nekoč in danes

(predvsem v državah, ki so nekoč imele režime, v katerih so bile sistematično kršene človekove pravice in svoboščine) ter razlik med normativno ureditvijo med državami, predvsem z vidika spoštovanja človekovih pravic in temeljnih svoboščin. Zato lahko trdimo, da na zaupanje državljanov v matične obveščevalno-varnostne službe vpliva tudi preteklost. Če državljani o obveščevalno-varnostnih služb nimajo ustreznih preverjenih, resničnih in zanesljivih znanj, s katerimi lahko samostojno in kritično pristopijo k individualni obravnavi in izgradnji zaupanja, bodo na zaupanje bistveno vplivali drugi dejavniki: priporočila drugih oseb, mediji, pretekle izkušnje (svoje izkušnje in izkušnje drugih oseb), razmerje moči, zgodovina, afere idr., kar bo ustvarilo družbeni vpliv, ki bo usmerjal zaupanje državljanov v matične obveščevalno-varnostne službe. Ocenjujemo, da se lahko v primeru negativnega družbenega vpliva razvijejo predsodki in odklonilen odnos do obveščevalno-varnostnih služb. Kasneje se lahko pojavi tudi negativno etiketiranje služb in njihovih uslužbencev. V takšnih okoliščinah (predvsem finančno in/ali politično odvisni) mediji postanejo osrednje/edino orodje za širjenje negativnega odnosa in nezaupanja v službe ter za diskreditiranje, službe pa postanejo tarče novinarskega nadzora, ki išče napake služb (vendar ne v smislu demokratičnega nadzora, ki je/naj bi bil pozitiven). To lahko producira (zelo škodljive) afere, ki zaupanje dodatno zmanjšujejo, čeprav je razlog za upad zaupanja oziroma nezaupanje izključno neznanje o obveščevalno-varnostnih službah. Službe lahko zaradi nezaupanja državljanov postanejo tarča pretiranega političnega nadzora, političnih pritiskov in vmešavanja politike v delo služb ter politično orientiranih kadrovskih menjav. Pojavi se lahko preveč političnih, predvsem pa enostranskih odločitev, zaradi česar se lahko zgodi, da rezultati služb niso več upoštevani ali cenjeni ali pa da so celo napačno interpretirani, zato se službe uporabljajo za druge namene, ki niso predpisani z zakonom. Kot posledica takšnega stanja se po našem prepričanju lahko zgodi, da lahko državljani odziv politike na zmanjšano zaupanje državljanov razumejo kot vmešavanje politike v delo obveščevalno-varnostnih služb. Da naše mnenje ni brez utemeljene podlage, verjetno nakazujejo tudi rezultati naše ankete (glej podpoglavje 7.1), v kateri je od skupaj 295 anketirancev 130 anketirancev trdilo, da ne zaupajo slovenskim obveščevalno-varnostnim službam. Od teh 130 anketirancev je 107 takšnih, ki službam ne zaupajo (tudi) zaradi vpliva politike na delo obveščevalno-varnostne službe. Na podlagi ugotovitev v tem odstavku zato predpostavljamo, da lahko obveščevalno-varnostne

službe zaradi izgube zaupanja državljanov sčasoma postanejo manj učinkovite in manj uspešne (Drucker (1967) definira učinkovitost kot »delati stvari pravilno«, uspešnost pa kot »delati prave stvari« – za slednje pravi, da je pomembnejše), v domači in tuji javnosti lahko izgubijo ugled, tuje službe z njimi ne bi več želele sodelovati, uslužbenci bi izgubili motivacijo za delo, pojavili bi se interni konflikti, ki lahko postanejo javni, v skrajnem primeru pa službe ne bi več služile svojemu namenu. Škode pa bi bil deležen celotni sistem nacionalne varnosti, ki bi bil lahko v celoti ogrožen zaradi okrnjenega ali neučinkovitega in neuspešnega delovanja enega od svojih podsistemov.

Pričakujemo, da bi se naš predlagani model lahko uporabil za izboljšanje zaupanja državljanov v matične obveščevalno-varnostne službe v katerikoli državi, saj je bil izgrajen na način, da bi ga bilo mogoče uporabiti v različnih okoljih, hkrati pa temelji na teoriji in praksi obveščevalno-varnostne dejavnosti, na splošnih oziroma generičnih modelih zaupanja ter na splošnih modelih zaupanja za posamezna področja, ki smo jih preučili: psihologija (Rotter, 1967; Mirzaie, Fesharaki & Daneshgar, 2012), ekonomija (Hart, 1988; Rus, 2008), potrošništvo (Kenning, 2008), menedžment (Hosmer, 1995; Mayer et al., 1995; Lewicki & Bunker, 1996; McKhnight et al., 1998; Brower, Schoorman & Tan, 2000; McKnight & Webster, 2001; Martins, 2002; Bijlsma & Koopman, 2003; Lucas, 2005; Burke, Sims, Lazzara & Salas, 2007; Paliszkiewicz, 2011; Rusu & Baboş, 2015), marketing (Morgan & Hunt, 1994; Arnott, 2007), poslovanje (Tan & Thoen, 2001; Mun, Shin & Jung, 2011; Martin, 2014), logistika (Križman, 2009; Laeequddin, Sahay, Sahay & Waheed, 2010), računalništvo (Kovač & Trček, 2007), pravo (Kahan, 2001), politologija (Toš, 2007; Schiffman, Thelen & Sherman, 2010), etika v kapitalizmu (Makarovič, 2004), javna uprava (Newton & Norris, 2000; Salminen & Ikola-Norrbacka, 2010), policija (Tyler & Huo, 2002; Flexon, Lurigio & Greenleaf, 2009; Jackson & Bradford, 2010).

1 Metodološki okvir

1.1 Cilja doktorske disertacije

1. Izgradnja modela celovitega zaupanja državljanov v matične obveščevalno-varnostne službe.

Takšen model je potreben za ustvarjanje in vzdrževanje ustrezne ravni zaupanja državljanov v matične obveščevalno-varnostne službe. Ocenjujemo, da je raven zaupanja v zadnjih nekaj letih nižja, kar je hkrati posledica nepoznavanja področja obveščevalno-varnostne dejavnosti in služb, negativnega vpliva medijev in drugih dejavnikov na mišljenje državljanov, pa tudi prepoznega, neučinkovitega delovanja/odzivanja ali nestrokovnega dela obveščevalno-varnostnih služb, vmešavanja politikov v delo obveščevalno-varnostnih služb, zlorabe služb za osebne ali politične namene, afer ter s tem povezanih medijskih objav, v javnosti vedno pogosteje izpostavljenih primerov nezakonitega poseganja obveščevalno-varnostnih služb v človekove pravice kot posledice širjenja pooblastil obveščevalno-varnostnih služb za učinkovitejše zagotavljanje nacionalne varnosti idr. O slednjem je dovolj zgovorna izjava red. prof. dr. Iztoka Podbregarja (2011 b, str. 15) o tem, koliko nam obveščevalno-varnostne službe nezakonito prisluškujejo v 21. stoletju: »Manj, kot si mislimo, in več, kot je dovoljeno.«

2. Opredelitev, pojasnilo in podajanje smernic za logistiko izdelave in aplikacije modela celovitega zaupanja državljanov v matične obveščevalno-varnostne službe.

Logistika izdelave in aplikacije modela celovitega zaupanja državljanov v matične obveščevalno-varnostne službe je odvisna od končne strukture modela. Smernice za logistiko aplikacije modela, ki izhajajo iz končne strukture modela, so nujno potrebne za uspešno, sistematično, sistemsko in celovito aplikacijo modela v ciljno okolje. Od izdelave in od aplikacije je odvisno, kako učinkovit bo model v praksi. Vključevati mora inoviranje in vzdrževanje modela. Z izrazom *logistika aplikacije* mislimo na zadostno in potrebno celovito podprt postopek aplikacije oziroma uvedbe izbrane rešitve v prakso v skladu s programoteko (tj. model postopkov oziroma programov, Mulej et al., 2000, str.

203). Ta (programoteka) bo nastala ob upoštevanju sistematične hevristike (Mulej, 1979), pravil DTS (Mulej, 1979; Mulej et al., 2000), pravil DOMR (Rosi, 2004) in invencijsko-inovacijskega difuzijskega managementa (Mulej et al., 2008).

1.2 Teza doktorske disertacije

Osrednje vodilo doktorske disertacije, iz katerega smo nato izpeljali tezo, je: *celovito zaupanje državljanov v matične obveščevalno-varnostne službe je pomemben zaviralec entropije obveščevalno-varnostnega sistema in sistema nacionalne varnosti.*

Gre za logistiko, zato je osrednja teza (kot koncept): **izdelava in ustrezna logistika aplikacije modela celovitega zaupanja državljanov v obveščevalno-varnostne službe omogočata upočasnitev entropije obveščevalno-varnostnega sistema in sistema nacionalne varnosti.** Trdimo, da neupoštevanje logistike aplikacije ne bo omogočalo doseganja pravih učinkov predlaganega modela. Aplikacija nečesa novega je namreč primer invencijsko-inovacijsko-difuzijskega procesa, ki nadomešča utečene navade in zato naleti na odpore, zlasti ko gre za vpliv na lastnosti ljudi, kot v našem primeru; zato je nujna ustrezna priprava, ki jo je morda – po naši hipotezi – mogoče obravnavati kot primer logistike. Da bi tak poskus uspel, mora potekati skladno z zakonom zadostne in potrebne celovitosti iz Mulejeve DTS, ki ga je treba uporabiti tudi pri modeliranju, da bo dalo uporabno, znanstveno utemeljeno podlago za prakso.

Pomožne teze ali podteze, ki izhajajo iz glavne teze in nanjo pomembno vplivajo, so naslednje:

- med državljani in matičnimi obveščevalno-varnostnimi službami ne gre za klasičen odnos zaupanja, temveč za posebno obliko, ki ni povsem primerljiva z ostalimi v obravnavani literaturi o zaupanju;
- na zaupanje državljanov v matične obveščevalno-varnostne službe vpliva več specifičnih dejavnikov (npr. politika, zgodovina, mediji, družbene razmere), kot jih prepoznava obravnavana literatura za druga sorodna področja (npr. zaupanje v javne institucije, zaupanje v policijo);

- na zaupanje državljanov v matične obveščevalno-varnostne službe pomembno vpliva politika, ki z usmerjanjem, določanjem prioritet in vplivom na izvajanje obveščevalno-varnostne dejavnosti posredno vpliva na učinkovitost, rezultate dela in javno podobo obveščevalno-varnostnih služb.

1.3 Metodologija in metode raziskovanja

1.3.1 Dialektična teorija sistemov

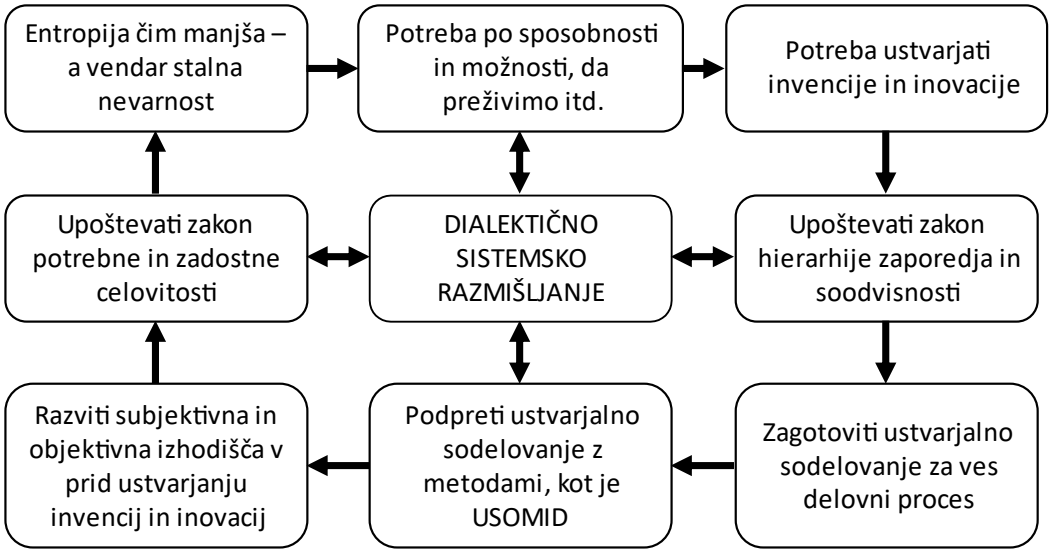
Za krovno metodologijo raziskovanja in dela smo izbrali DTS (Mulej, 1979; Mulej et al., 2000; tudi Mulej et al., 2008), ki je dialektični sistem. V literaturi je definicij izraza *sistem* veliko, z našega vidika smo izbrali kot najustreznejšo naslednjo: »*[S]istem je urejena množica, torej je sestavljen iz množice sestavin* in *množice povezav med njimi, s tem pomeni celoto*.« (Mulej et al., 2008, str. 39) V tem kontekstu je dialektični sistem »*sistem izbranih enostranskih sistemov* kot čustveno-miselnih slik, ki vsaka s svojega vidika prikazujejo neki del lastnosti obravnavanega pojava.« (ibidem, str. 53) Glavna posebnost dialektičnega sistema je, da so njegove sestavine vidiki, »s katerih bi utegnilo biti smiselno obravnavati dani/izbrani/določeni pojav/objekt,« povezave pa so »*odnosi med vidiki*, izbranimi v sistem.« (ibidem) Pri ostalih sistemih so sestavine in povezave navadno lastnosti pojava, ki ga obravnavamo (npr. skupina kot sistem, člani skupine kot posamezni elementi in odnosi ter relacije med člani skupine kot povezave), zato jih je tudi relativno lažje opredeliti, seveda pa se pri tem pojavlja dilema, ali je opredelitev oziroma opis sistema dovolj celovit. To pomeni, da čim bolj odraža celoto oziroma »*vse sestavine in vse njihove odnose (povezave, relacije) ter povezave povzročene sinergijske lastnosti*, ki označujejo obravnavani pojav.« (ibidem, str. 38) Popolna celovitost, s katero bi predstavili vse sestavine in povezave obravnavanega sistema, ni mogoča, nepopolna ali navidezna celovitost pa je osredotočena le na ožji del in izpušča ostalo, zato je takšna celovitost enostranska in omejena le na posamičen vidik (Mulej et al., 2008). Nobena od omenjenih dveh vrst celovitosti ni ustrezna, zato je potrebno uporabiti vmesno stopnjo celovitosti, ki se nahaja med totalno/popolno celovitostjo (ki je ni mogoče doseči) in navidezno celovitostjo (ki je preozka in zato nepopolna) – zadostna in potrebna celovitost. Dosežemo jo z upoštevanjem zakona zadostne in potrebne celovitosti (Mulej,

1979; Mulej & Kajzer, 1998; Mulej et al., 2000; Mulej et al., 2008) – več o tem zakonu sledi v nadaljevanju doktorske disertacije.

Dialektični sistem združuje enostranske sisteme, ki objekta ne obravnavajo celovito, ti pa se znotraj dialektičnega sistema med seboj povezujejo in dopolnjujejo ter vplivajo drug na drugega. Dialektični sistem je zato najboljši približek celovite obravnave pojava, celovitost pa je mogoča zaradi upoštevanja zakona zadostne in potrebne celovitosti. Dialektični sistem je sestavljen »*iz vseh bistvenih in samo bistvenih vidikov in iz vseh bistvenih in samo bistvenih odnosov med njimi*,« zato »ne gre niti za absolutni niti za enostranski sistem, ampak za sistem kot miselno in/ali čustveno sliko objekta, katera je v skladu z zakonom potrebne in zadostne celovitosti.« (Mulej et al., 2008, str. 54)

DTS kot dialektični sistem sestavljajo tri sestavine (smernice za opredelitev subjektivnih izhodišč, skladnih s sodobnimi razmerami, smernice za vzdrževanje ustvarjalnega sodelovanja ter **u**stvarjalno **so**delovanje **m**nogih v **i**novativnem **d**elu (v nadaljevanju: USOMID)), tri relacije med njimi (zakon hierarhije zaporedja in soodvisnosti, metode za modeliranje ustvarjalnega (so)del(ovanj)a, zakon entropije, zakon zadostne in potrebne celovitosti (Mulej et al., 2000) in druge sestavine, ki jih prikazuje slika 1.1.

Slika 1.1: Soodvisnost sestavin in povezav DTS



Vir: Mulej et al., 2008, str. 111

Izhodišča

Izhodišča so pri delovnem procesu najpomembnejša in se delijo na objektivna in subjektivna. Treba jih je oblikovati, v procesu oblikovanja pa moramo upoštevati **10 tez za oblikovanje izhodišč**, ki tvorijo naš dialektični sistem vidikov (Mulej, 1979, str. 11-12):

1. »revolucionarnost, ne konservativnost;
2. metodološko, ne le metodijsko znanje;
3. jasna opredelitev problema in preciziranje opravil;
4. razmejitev osnovnih faz dela;
5. zajetje čim številnejših možnih vidikov obravnavanja v prepletenem povezovanju;
6. sposobnost sporazumevanja specialistov;
7. omogočeno interdisciplinarno sodelovanje;
8. posodabljanje izhodišč;
9. soodvisnost vrednot, vsebinskega in metodološkega znanja;
10. posebna odvisnost metodologije za opredelitev izhodišč od vrednot in znanja.«

Ker objektivna izhodišča tvorijo okoliščine, ki so neodvisne od človeka, so z vidika vloge človeka v delovnem procesu toliko bolj pomembna subjektivna izhodišča, sestavljena iz razumskega in čustveno-vrednostnega dela človekove osebnosti. Vednost, znanje ter vrednote in čustva tvorijo sistem subjektivnih izhodišč za utemeljevanje odločitev, namen tega pa je zaznati, dojeti, razumeti ali obvladati sebe in okolje (objektivna izhodišča). Od sistema subjektivnih izhodišč je odvisna zaznava okolja, zato je pomembno, da jih znamo izoblikovati. Pri njihovem oblikovanju nam v skladu s sočasnimi razmerami pomaga **10 smernic, ki tvorijo sistem 10 povezanih vidikov** »formiranja ali razvoja subjektivnih izhodišč, tj. osebnostnih lastnosti, ki nastopajo kot splošna podlaga […],« (Mulej, 1979, str. 127) Te smernice so (ibidem):

1) »*upoštevanje razmer*: zagotovitev iznajdljivosti (= inventivnosti), celovitosti (= holizma) in koristne izrabe invencij (= inovativnosti);
2) *pristop*: metodološko (ustvarjalno), ne le metodijsko (rutinsko) znanje;
3) *kaj*: kar najbolj dognana opredelitev sistema ''problem, cilji in naloge'';
4) *kako*: kar najbolj dognana zasnova izvedbenih postopkov za vsako nalogo;
5) *upoštevanje vsega bistvenega*: dialektični sistem vidikov obravnavanja;

6) *osebna sposobnost za 5)*: dialektičen način razmišljanja (soodvisnost, med strokovno sporazumevanje, ustvarjalno sodelovanje);
7) *organizacijska možnost za 5)*: timsko delo, demokratična seja ali sestanek;
8) *sodobnost*: nenehno posodabljanje subjektivnih izhodišč;
9) *vednost, znanje in vrednote/čustva*: soodvisnost vseh treh sestavin subjektivnih izhodišč (fiziološko: leve in desne polovice človeških možganov);
10) *evolucija osebnosti*: predzgodovina trenutnih subjektivnih izhodišč.«

Smernice so med seboj povezane in tvorijo dialektični sistem, z njimi pa izoblikujemo subjektivna izhodišča, ki so pravzaprav posameznikove osebnostne lastnosti (Mulej, 1979) oziroma vednosti, znanja, vrednote in čustva ter talenti (Mulej et al., 2008). Nemogoče je, da bi kot ljudje delovali povsem objektivno kot stroji, zato je povsem normalno, da v načrtovanje in izvajanje dela vključimo subjektivne elemente. Namen smernic je torej izoblikovanje subjektivnih izhodišč, ki povzročajo najmanj enostranskosti in napak v razmišljanju in delovanju, na način, ki zagotavlja zadostno in potrebno celovitost. Da bi to dosegli, moramo svoja subjektivna izhodišča nenehno prilagajati, dopolnjevati in spreminjati v skladu s smernicami za opredelitev subjektivnih izhodišč.

Zakon zadostne in potrebne celovitosti

Zakon zadostne in potrebne celovitosti nam pomaga pri iskanju odgovora na vprašanje: kako doseči celovitost? V skladu z DTS je celovitost opredeljena kot sistem, ki ga sestavljajo (Mulej et al., 2000, str. 283):

- »*sistemnost* (= upoštevanje globalnih, skupnih lastnosti obravnavanih pojavov, njihove sinteze, sinergije, emergence, razvoja sistema, ki presega vsoto lastnosti vseh sestavin, obravnavanih posamično), in
- *sistematičnost* (= upoštevanje podrobnih značilnosti, ki jih ima obravnavani pojav, če ga opazujemo po delih in brez sinergije, torej analitično in ne sintezno), in
- *dialektičnost* (= upoštevanje soodvisnosti med sestavinami, ki so po enem delu lastnosti enake in po drugem različne med seboj, v obravnavanem pojavu, in

upoštevanje procesov, ki jih soodvisnosti povzročajo, tako da nastanejo iz sistematičnih nove, sistemske lastnosti obravnavanega pojava) in

- *materialističnost* (= upoštevanje stvarnosti namesto metanja peska v lastne oči, ko se ukvarjajo z nekim obravnavanim pojavom).«

Če upoštevamo vse, se moramo vprašati: *katere* dejavnike (sestavine, značilnosti, lastnosti…) upoštevati in *koliko* jih upoštevati? Mulej et al. (2000) pravijo, da ne moremo upoštevati vseh popolnoma, saj popolna celovitost ni mogoča, zadostno in potrebno pa dosežemo na način, da se dela lotimo zavestno in premišljeno, predvsem pa da celovito opredelimo, katero raven celovitosti bomo šteli za ustrezno. »Ravno v nenehnem trudu, da bi bili (ravno dovolj!) celoviti in s tem dovolj uspešni, je možnost, da vsaj začasno premagamo zakon entropije – s pomočjo uporabe prvih štirih omenjenih sestavin *dialektične teorije sistemov* in povezav med njimi. Poskušamo torej iskati **srednjo pot med preveč zapletenosti in poenostavljenosti**, a glede tega ni enolične, tkim. znanstvene rešitve. V praksi se pač prepletajo znanost, institucija ter sreča (dobra in slaba).« (Mulej et al., 2000, str. 73-74) »[I]zbira manjših celot je že svojstvena redukcija; zato je važno videti in odločiti, katera raven poenostavitve je pretirana, tako da bi nadomestila sistemsko razmišljanje s tradicionalnim redukcionističnim (analitičnim).« (ibidem, str. 281)

Zadostno in potrebno celovitost lahko dosežemo z izbiro vidikov, ki jih bomo upoštevali pri obravnavi izbranega pojava. Do ustreznih vidikov pridemo s postopkom redukcije, tj. potrebne poenostavitve v prehodu od objekta na sistem ter nato na model (Mulej et al., 2000, str. 280). Ti skupaj tvorijo dialektični sistem vidikov, saj so vidiki med seboj povezani, soodvisni in usmerjeni k skupnemu cilji. Z izbiro vidikov določimo okvir dela, s tem pa postanemo odgovorni za posledice (ibidem, str. 282), ki nastanejo kot rezultat našega dela, osnovanega na dialektičnemu sistemu vidikov. Pri tem Mulej et al. (2000, str. 282) tistim, ki določajo svoj dialektični sistem vidikov, svetujejo, naj:

- »**ne pretiravajo** v smeri k *neizvedljivi celovitosti, ki bi pomenila uporabo pojma* ''*absolutni ali popolni sistem*'', ki je sistem (celota) *čisto vseh vidikov*, saj pride praktično v poštev samo teoretično; poleg tega bi tak poskus zahteval preveč napora, da bi bil smiseln (tudi če bi bil izvedljiv);

- **ne pretiravajo** v smeri k *nezadostni, navidezni celovitosti*, ki bi pomenila uporabo (zelo) reduciranega sistema (slike stvarnosti z nekega edinega vidika), ki obravnavano stvarnost poenostavlja tako, da se pretirano odmakne od vsake resničnosti; to bi namreč dalo prešibko podlago za analizo in delovanje (vodilo bi k spregledom in zato k napakam, vključno s svetovnimi vojnami, svetovnimi gospodarskimi krizami, svetovno razsežnimi ekološkimi problemi itd.);
- namesto tega dvojega upoštevajo dejansko potrebo, *da upoštevajo svojo soodvisnost, ki jo povzroča njihova nujna specializacija*, in razvijejo svoja subjektivna izhodišča v smeri k etiki in sposobnosti za medstrokovno ustvarjalno sodelovanje.«

Poleg dialektičnega sistema vidikov je ključna sestavina zakona zadostne in potrebne celovitosti tudi sodelovanje med specialisti, ki prepreči pretirano poenostavljanje. »[S]eveda [je] neka raven poenostavitve nujna, ker je zapletenosti in znanja na svetu preveč, da bi vse zmogli, toda raven poenostavitve, sprejemljiva kot način sistemskega razmišljanja, bi *ohranila zahtevo in prakso, da uporabljamo* ***transdisciplinarnost***, ki jo uresničujemo kot ***interdisciplinarno*** *sodelovanje vseh bistvenih vidikov / poklicev / partnerjev; le-ti so seveda* ***enostrokovni*** *specialisti* in hkrati sposobni in voljni tako ***sodelovati***.« (Mulej et al., 2000, str. 280-281) »[S]posobnost in voljnost sodelovati medstrokovno je tista lastnost enostrokovnih specialistov, ki je v pogledu vrednot in drugih čustev – kot sestavine njihovih subjektivnih izhodišč – izražena v njihovi **etiki soodvisnosti**; le-ta je čustveno-vrednotni odsev njihove dejanske potrebe, da priznajo svojo dejansko soodvisnost, da bi razrešili svoje lastne in skupne težave.« (ibidem)

Kaj je torej potrebno, da lahko dosegamo celovitost v skladu z zakonom zadostne in potrebne celovitosti (zadostno in potrebno celovito vedênje), na kratko povzema Ivanuša (2013, str. 10):

1. »Potrebni so tako specialisti kot generalisti (ki delajo splošne zaključke), delo v timih, ki občutijo etiko soodvisnosti in zato kreativno sodelujejo.
2. Vključujejo strokovnjake vseh bistvenih in samo bistvenih poklicev/disciplin/prednosti.
3. Njihove vrednote so izražene v etiki soodvisnosti in udejanjene v kreativnem timskem delu, uspešnem reševanju nalog, ki temelji na enakovredno zastavljenem

sodelovanju bolje kot na štabno-linijskem poveljevanju ('nihče, ki je zgoraj, ne posluša, nihče ne sliši').«

Zakon hierarhije zaporedja in soodvisnosti

Naslednja sestavina, ki jo na kratko povzemamo, je zakon hierarhije zaporedja in soodvisnosti. Ta pravi, da so spremembe v naravi in družbi posledica soodvisnosti; prvi koraki v procesih spreminjanja imajo večji vpliv kot kasnejši koraki, kar nakazuje na določeno hierarhijo zaporedja korakov. Z ukazovanjem se uresničuje hierarhija ne le zaporedja, temveč tudi soodvisnosti, kar lahko ponazorimo na primeru organizacije: višje ravni upravljajo, koordinirajo in ukazujejo (prvi koraki), nižje pa predpisano ali ukazano izvršujejo (kasnejši koraki), vendar so poleg zaporedja postopka prenosa ukaza in izvršitve dela ter prenosa povratnih informacij v nasprotno smer pomembne tudi soodvisnosti vseh vmesnih členov, ki jih ne smemo spregledati. Neupoštevanje soodvisnosti bi povzročilo odvisnosti, ki vodijo v razpad hierarhije, nato v razpad strukture sistema ter posledično v prenehanje sistema (Mulej et al., 2000).

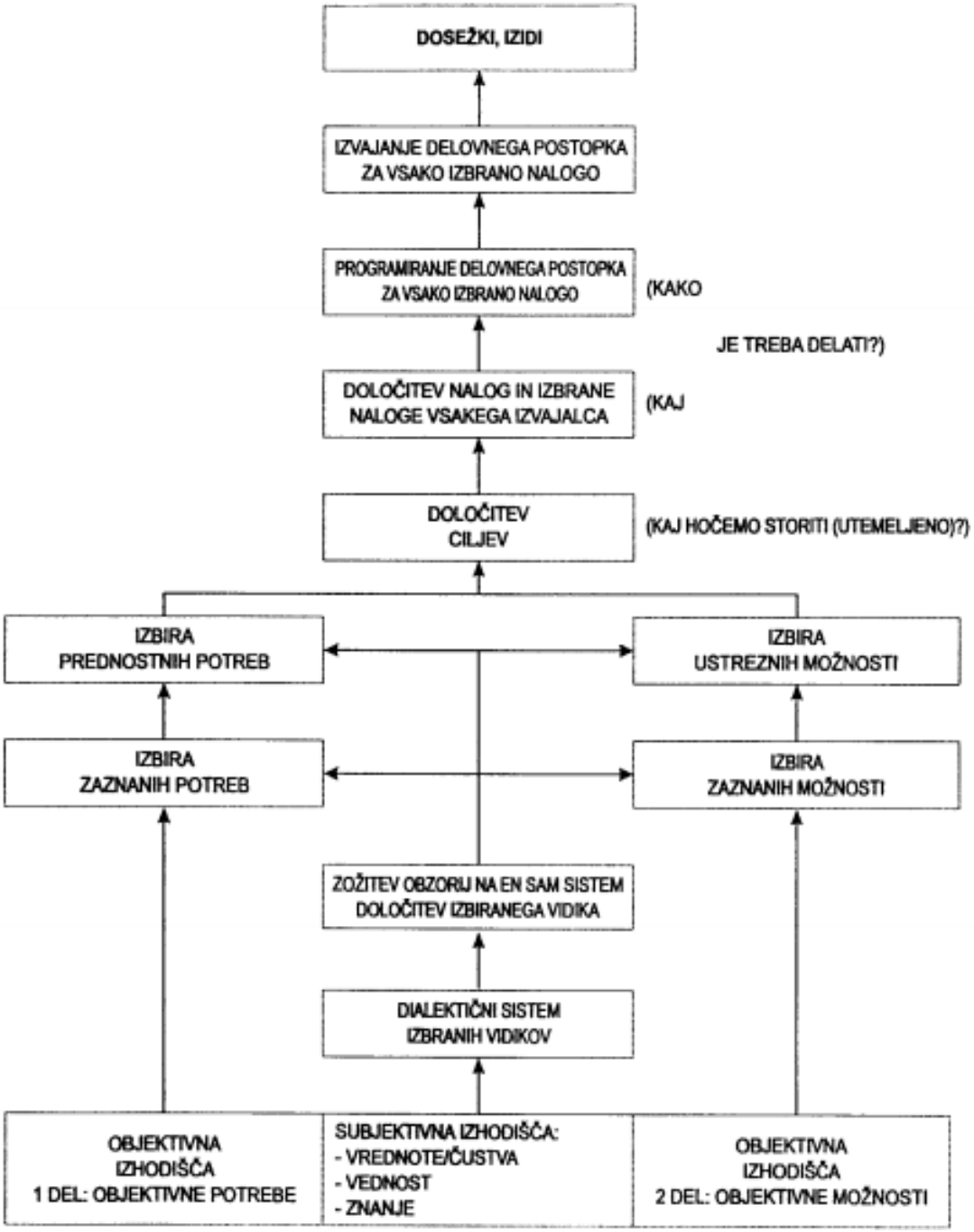
Hierarhija je različno razumljena, najpogosteje pa se zanjo uporablja tudi izraze *organizacijska hierarhija*, *ukazovalna hierarhija* in *procesna hierarhija*. Prva je razumljena kot zmanjševanje zapletenosti obvladovanja zapletenih objektov, druga kot določanje in uveljavljanje podrejenosti in nadrejenosti, tj. kdo lahko in mora opredeljevati cilje, način dela ipd. oziroma kdo ima oblast in kdo mora vse to upoštevati in izvesti, tretja pa kot opredeljevanje nujnega zaporedja dogajanja. Ukazovalna in organizacijska hierarhija imata obliko trikotnika s konico navzgor, kar pomeni, da se število tistih, ki lahko ukazujejo, manjša na poti navzgor, hkrati pa da se veča število oseb in notranjih delov organizacije na poti navzdol (npr. manj subjektov za načrtovanje na višji ravni, več za praktično izvajanje na nižji ravni). Med tema dvema vrstama hierarhije zato obstaja soodvisnost: na višjih ravneh je manj tistih, ki imajo pravico odločanja, načrtovanja in ukazovanja, na nižjih ravneh pa več tistih, ki izvajajo naloge, različna pa je tudi raven podrobnosti, s katerimi se morajo posamezne ravni ukvarjati. Na nižjih nivojih je podrobnosti več, zato je potrebno tudi večje število tistih (specialistov, op. G. H.), ki se bodo z njimi ukvarjali. Nasprotno pa ima t.i. *širina potrebnega in zadostnega*

dialektičnega sistema vidikov obliko trikotnika s konico navzdol, saj morajo imeti tisti, ki so pozicionirani višje na hierarhiji, večji dialektični sistem vidikov. Višje kot se pomikamo po organizaciji oziroma hierarhiji, več vidikov je potrebno upoštevati pri razmišljanju in delu, saj se s pomikanjem navzgor delo spreminja iz ozko specialističnega v generalistično (Mulej et al., 2008).

Zakon hierarhije zaporedja in soodvisnosti se uporablja za določanje ustreznih ciljev (družbenih/poslovnih) sistemov. Pogosto se dogaja, da organizacije najprej določijo cilje, šele nato pa postopke dela. Mulej et al. (2008) pravijo, da je takšno ravnanje napačno, saj temelji na odločitvi, ki ne upošteva soodvisnosti posameznih (objektivnih in subjektivnih) vidikov. Brez ustreznega postopka ni mogoče določiti pravih ciljev. Najprej je potrebno prepoznati želene *končne izide* vseh vpletenih, nato pripraviti delovni proces, potem opredeliti naloge ter določiti, kdo bo te naloge opravljal, nato pa upoštevati še objektivne in tudi subjektivne vidike pri določanju ciljev (Mulej et al., 2008). Mulej et al. (ibidem) poudarjajo, da je potrebno tudi zaznati dogajanje in potrebe in izbrati prednostne potrebe ter njim ustrezne možnosti. Temu sledi izbira ustreznega cilja, ki temelji na upoštevanju soodvisnosti prednostnih potreb in ustreznih možnosti. Od tega je odvisno, kako utemeljen in stvaren bo cilj (ibidem).

Kako se bodo ljudje odločili, je odvisno od njihovih objektivnih in subjektivnih izhodišč (njihovih osebnostnih lastnosti) (ibidem). Ta izhodišča se omrežno prepletajo, torej na oblikovanje ciljev ne vplivajo objektivni in subjektivni cilji posamično (ibidem). Slika 1.2 ponazarja proces hierarhije zaporedja in soodvisnosti ter kaže, da sta »organizacijska in ukazovalna hierarhija […] vsebinsko način izvedbe hierarhije in zaporedja, pri čemer proces ni enostaven in enosmeren, ampak vedno znova kaže na soodvisnosti, jih upošteva in vpliva na njih,« (ibidem, str. 58), saj se približuje stvarnosti. Soodvisnost se kaže znotraj samih faz, ki jih prikazuje slika 1.2, in fazami med seboj.

Slika 1.2: Proces hierarhije zaporedja in soodvisnosti - linearni model



Vir: Mulej et al., 2008, str. 60

Podlago za postopke na sliki 1.2 predstavlja splet objektivnih in subjektivnih izhodišč, ki se manifestira z opredeljevanjem vidika/vidikov oziroma njihovega dialektičnega sistema. Izbor vidikov, do katerih pridemo z opazovanjem okolice, je odvisen od podlage za izbor vsakega posameznika (osebnostne lastnosti v obliki dialektičnega sistema vrednot in čustev, znanja, vednosti in talentov). Ta opredeli svoje vidike, ki so navadno

drugačni od vidikov drugih oseb, kar morajo odločevalci (oziroma menedžerji) upoštevati. Več kot je različnih vidikov, bolj realno sliko dejanskega stanja je mogoče dobiti, zato je potrebno izmenjevanje različnih pogledov, mnenj ipd., da se med seboj dopolnjujejo. Vsa ta opravila se izvajajo na nižjih ravneh, njihovo prepletanje (tj. sinergije) pa tečejo navzgor po hierarhiji. Nasprotno tečejo navzdol izidi in njihovo usklajevanje. Tako je razvidno, da soodvisnost obstaja med posameznimi ravnmi (npr. med delavci in vodstvom) ter znotraj posameznih ravni (npr. med delavci, med člani vodstva) (ibidem).

Proces na sliki 1.2 je sicer prepleten s procesom ustvarjalnega dela ali sodelovanja po USOMID/NOVOST. Za podrobnejši prikaz (delovnega) procesa, ki vključuje USOMID in NOVOST, bralce usmerjamo na str. 65-66 knjige *Invencijsko-inovacijski management z uporabo dialektične teorije sistemov (podlaga za uresničitev ciljev Evropske unije glede inoviranja*) avtorjev Mulej et al. (2008).

Smernice za vzdrževanje ustvarjalnega sodelovanja

Zaradi nevarnosti, da bi specialisti ostali osredotočeni le na področja njihove specializacije in na ta način delovali preozko, obravnavali le sistema/modela ter s tem dobili zgolj delne informacije, je potrebno zagotoviti, da se pri svojem delu ne bi preveč odmaknili od celovitosti. To je mogoče doseči s **smernicami za vzdrževanje ustvarjalnega sodelovanja** (v Mulej, 1979 so predstavljene kot pravila DTS). Te so pomembne za (Mulej et al., 2008, str. 99-100):

- »[…] *opredelitev* izhodišč […] v fazi globalnega razmišljanja in kasneje, toda kasnejša specializacija na izvajanje ožjih nalog – po opredelitvi ciljev – povzroča nevarnosti, da bi jih pozabili namesto upoštevali in tako postali enostranski;
- […] *uresničevanje* izhodišč […] v fazah prevladovanja ožje specializacije, omejitve na izbrane naloge posameznikov ali ožjih skupin;
- pri običajni delitvi dela se z omenjenima skupinama opravil ukvarjajo *različni* ljudje, ki jih specializaciji na njih silita k različnim zaznavam in izbiram, kaj je prednostno in ustrezno;

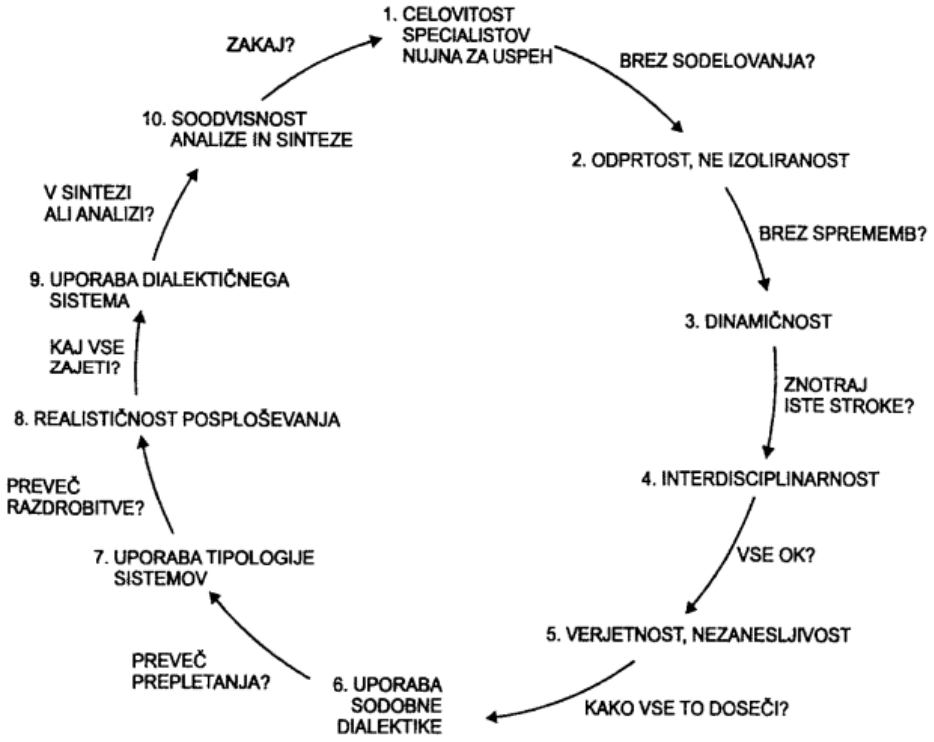
- […] da bi čim več ljudi premagalo *ozka obzorja* svoje specializacije, ne da nehajo biti specialisti za svoje delo; tako bi v družbi kot celoti […] prevladala podpora za zadostno in potrebno celovitost, ustvarjalnost, sodelovalnost, podjetnost, inventivnost in inovativnost.«

Mulej et al. (2008) opredeljujejo 10 smernic za vzdrževanje ustvarjalnega sodelovanja. Prvih pet smernic »pove, *kaj* hočemo in moramo poskušati doseči, ko uresničujemo zastavljena (globalnejša) izhodišča z delom na (ožjih) specializiranih področjih in pri (delnih) nalogah, ki jih je pri tem treba zastaviti in izvesti, pogosto vsako zase,« drugih pet pa »*kako* (naj) v splošnem ravnamo, da bi (lažje kot brez njihovega upoštevanja) uresničili, kar hočemo in moramo poskušati doseči.« (ibidem, str. 101) Te smernice so (povzeto po Mulej et al., 2008, str. 101-103):

1. *celovitost* namesto enostranskosti razmišljanja, delovanja in obnašanja;
2. *odprtost* namesto izoliranosti pri razmišljanju, delovanju in obnašanju;
3. *dinamičnost obravnavanja* namesto statičnosti razmišljanja, delovanja in obnašanja;
4. *interdisciplinarnost* namesto zaprtosti zgolj v lastno stroko;
5. *verjetnost pri obravnavanju* namesto pričakovanja deterministične zanesljivosti;
6. *uporaba materialistične dialektike* namesto srednjeveške metafizike in idealistične dialektike, ki premalo upoštevata sodobno stvarnost pri razmišljanju, delovanju in obnašanju;
7. *uporaba tipologij sistemov in modelov* omogoča upoštevanje prepletanja in povezovanja soodvisnih delov/pojavov ter njihovo razmejitev, hkrati pa omogoča tudi matematično natančnost tudi v primerih, ko ni uporabljen matematičen zapis modela;
8. *realistično posploševanje spoznanj* preprečuje odmik od stvarnosti v razmišljanju, delovanju in obnašanju;
9. *uporaba dialektičnega sistema* podpira 8. smernico ter omogoča zajemanje vseh bistvenih in samo bistvenih vidikov kot sistem;
10. *upoštevanje soodvisnosti analize in sinteze* pomeni upoštevanje zakona hierarhije zaporedja in soodvisnosti, zato mora biti prva sinteza izhodišč, druga analiza na podlagi sinteze izhodišč, tretja pa sinteza sklepov – gre za tri faze procesa razmišljanja.

Te smernice oziroma pravila metodologije DTS so pomembna tudi v postopku inoviranja oziroma invencijsko-inovacijsko difuzijskega managementa (Mulej et al., 2008). Zaporedje in medsebojni odnos smernic prikazuje slika 1.3.

Slika 1.3: Smernice za vzdrževanje ustvarjalnega sodelovanja, prikazane v krožnem vzročno-posledičnem odnosu poenostavljenega zaprtega kibernetskega kroga



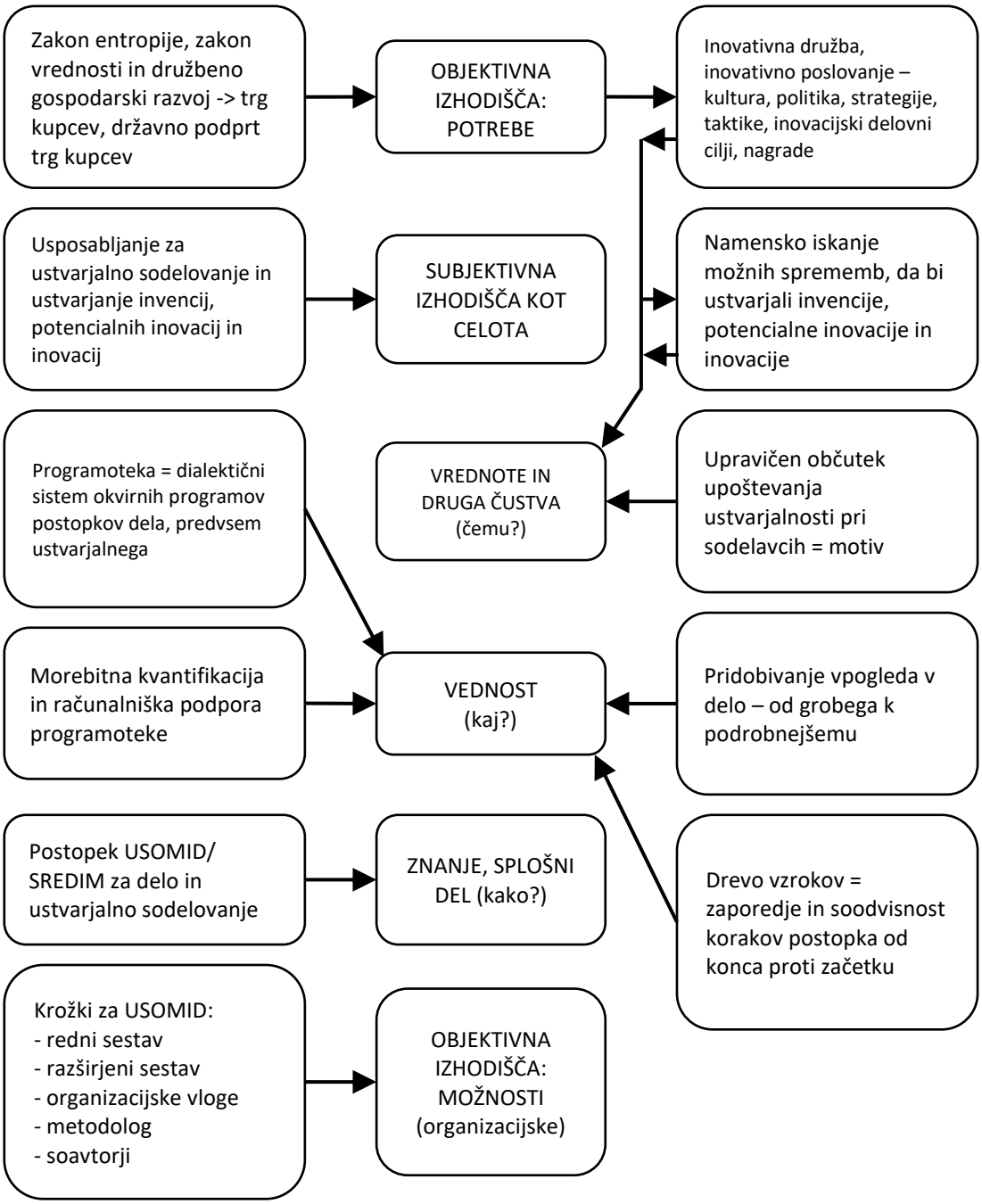
Vir: Mulej et al., 2008, str. 104

Metode za modeliranje ustvarjalnega (so)del(ovanj)a

Sodelovanje specialistov prinaša tudi nevarnost ustvarjanja procesa z deterministično natančnostjo. Takšno razmišljanje, delovanje in obnašanje zavira ustvarjalnost, saj specialiste prisili, da delajo točno po predpisih, kar vodi v rutino. V izogib temu je mogoče delati na način, da se razvije okviren model postopkov dela ali **opomnik**. Ta ni toliko osredotočen na vsebino, temveč bolj na postopke, zato je njegovo uporabo mogoče prilagoditi različnim situacijam, še posebej takrat, kadar se srečamo s problematiko, ki jo je vsaj okvirno mogoče primerjati z že obstoječimi zapisanimi izkušnjami – v takšnem primeru govorimo o **programoteki**, bazi okvirnega znanja o postopkih (Mulej et al., 2000, 2008).

Metodologija in metoda za uporabo dialektičnega sistemskega razmišljanja v ustvarjalnem sodelovanju mnogih je USOMID (Mulej et al., 2008), ki se z DTS in inovativnim poslovanjem povezuje na način, prikazanim na sliki 1.4.

Slika 1.4: Zveza med sestavnimi izhodišči (po DTS), inovativnim poslovanjem in sestavinami USOMID



Vir: Mulej et al., 2008, str. 128

Takšno povezovanje omogoča doseganje zadostne in potrebne celovitosti (Mulej et al., 2008). Za ustvarjanje v okviru USOMID se uporablja NOVOST (izhaja iz angleškega izvirnika SREDIM), ki predstavlja logiko okvirnega modelnega postopka za inoviranje (ibidem, str. 105) in je sestavljena iz šestih zaporednih faz (ibidem, str. 106), opisanih v tabeli 1.1:

- N – **N**abor in izbor teme;
- Op – **Op**is izbrane naloge;
- V – **V**rednotenje, analiza podatkov;
- Od – **Od**ločitev, preveritev;
- S – **S**prememba dane prakse;
- T – **T**rajnost, novost.

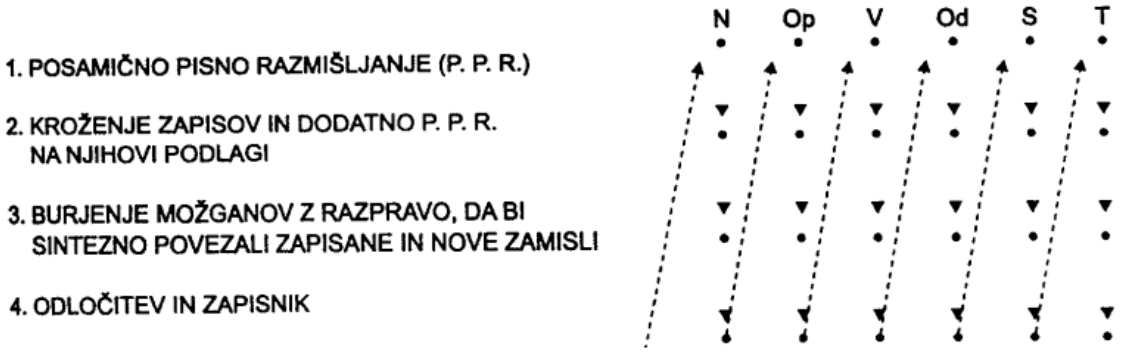
Tabela 1.1: Postopek ustvarjalnega dela NOVOST

SLOVENSKA OZNAKA	**IZVIRNA OZNAKA**	**KRATEK OPIS VSEBINE**
N nabor in izbor teme	**S** select topic	Nabor tematik, izbira teme, problematike, problema in izbrane naloge.
Op opis izbrane naloge	**R** record data	Opis dejstev o izbrani nalogi s podatki.
V vrednotenje, analiza podatkov	**E** evaluate data	Analiza (= spoznavanje skritega bistva) izbrane naloge.
Od preveritev, odločitev	**D** determine (and develop) solution	Odločitev za eno od variant možne rešitve; po preveritvi, koliko je stvarna, tudi dodelava.
S sprememba dane prakse	**I** implement the selected solution	Sprememba z uvedbo izbrane nove rešitve v prakso obvladovanja izbrane naloge.
T trajnost novosti	**M** maintain the new solution	Trajnost nove rešitve, dosežena z namenskim vzdrževanjem in prenavljanjem.

Vir: Mulej et al., 2008, str. 68

Proces NOVOST je zasl. prof. ddr. Matjaž Mulej v 80. letih prejšnjega stoletja nadgradil s postopkom USOMID (Ženko & Mulej, 2009). Tako je nastal postopek USOMID/NOVOST (slika 1.5).

Slika 1.5: Postopek ustvarjalnega sodelovanja USOMID/NOVOST



Vir: Mulej et al., 2008, str. 68

Postopek USOMID/NOVOST v praksi pomeni, da pri vsakem od faz postopka NOVOST opravimo 4 korake USOMID: 1. posamično razmišljanje, 2. kroženje zapisov in dodatno posamično pisno razmišljanje na njihovi podlagi, 3. burjenje možganov, da bi sintezno povezali zapisane in nove zamisli, ter 4. odločitev in zapisnik.

V fazi N je zelo pomembno, da izberemo bistvene vidike, vendar zgolj z enim vidikom ali več vidiki ene same osebe ne dobimo prave slike o objektu, temveč enostranski pogled nanj. »Če uvedemo **sistem vseh bistvenih vidikov**, da bi obravnavali objekt, razmišljamo s pomočjo *dialektičnega sistema*. To je komajda mogoče, razen v timskem delu. Upoštevamo zakon o potrebni in zadostni celovitosti, da bi preprečili delovanje zakona o entropiji čim bolj. Zato uporabimo tudi zakon o hierarhiji zaporedja in soodvisnosti.« (Mulej et al., 2008, str. 107)

Ključno je sodelovanje z drugimi, kar omogoča pridobitev več različnih vidikov različnih oseb in s tem izogibanje pristranskemu zaznavanju obravnavanega objekta. Vsak posameznik si namreč ustvari svojo miselno sliko o objektu, ki jo izrazi z modelom. Med objektom in modelom ter sistemom in dialektičnim sistemom obstajajo bistvene razlike (tabela 1.2).

Tabela 1.2: Odnosi med objektom, dialektičnim sistemom in modelom

STOPNJA STVARNOSTI PRI OBRAVNAVI OBJEKTA	STOPNJA POENOSTAVLJANJA PRI OPISU OBJEKTA	VIDIKI, UPOŠTEVANI V OBRAVNAVI OBJEKTA	SESTAVINE OBJEKTA, UPOŠTEVANE V OBRAVNAVANI	ODNOSI OBJEKTA, UPOŠTEVANI V OBRAVNAVI
Objekt	nič	vsi obstoječi	vse obstoječe	vsi obstoječi
Dialektični sistem	majhna	vsi bistveni za sinergijsko obravnavo	vsi bistveni vidiki	vsi bistveni med vidiki
Sistem	velika	en sam po izbiri (enostranska obravnava)	po izbranem vidiku (lastnosti)	po izbranem vidiku
Model	zelo velika	isti kot za sistem, a poenostavljen ali delen	iste kot za sistem, a poenostavljene ali samo del	isti kot za sistem, a poenostavljeni ali samo del

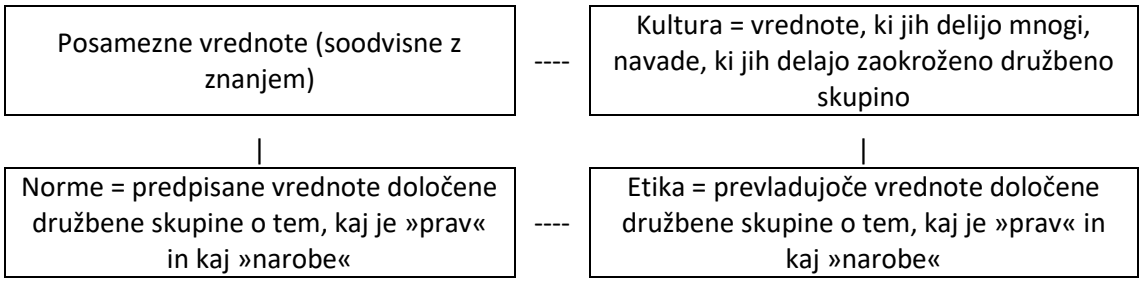
Vir: Mulej et al., 2008, str. 107

»[O]bjekt *obstaja* izven človekovih misli, sistem pa je *uveden* v človekovih mislih in/ali čustvih tako, da **izberemo**, katere od vseh lastnosti objekta bomo zajeli v obravnavo.« (Mulej et al., 2008, str. 109) Objekta ne moremo obravnavati v celoti, saj popolna celovitost pri obravnavi stvarnosti ni mogoča. Posameznik lahko opiše objekt le kot model. Če želimo višjo stopnjo stvarnosti pri obravnavi objekta, je potrebno sodelovanje z drugimi (specialisti). Takšno sodelovanje tvori sinergijo, zaradi katere nastaja sistem več (različnih) vidikov, ki jih sodelujoči določijo za bistvene in so medsebojno povezani ter prepleteni (so v soodvisnosti, dialektiki). Zato je stopnja stvarnosti pri obravnavi objekta višja, kot če bi objekt obravnavali le z vidika posameznika. Pri (invencijsko-inovacijskem) delu je potrebno sodelovanje oziroma uporaba metode za modeliranje ustvarjalnega (so)del(ovanj)a, s katerimi se upočasnjuje entropijo obravnavanega objekta.

Pomemben koncept, ki ga je potrebno upoštevati pri USOMID, je splet **v**rednot, **k**ulture, **e**tike in **n**orm (v nadaljevanju: VKEN) (Potočan & Mulej, 2006). Invencijsko-inovacijski proces namreč zahteva sodelovanje strokovnjakov z različnih področij, kultur in okolij, zato je povsem upravičeno pričakovati, da se njihove VKEN razlikujejo, kar lahko predstavlja težavo pri njihovem usklajevanju oziroma upravljanju (ibidem, str. 4).

S slike 1.6, ki prikazuje medsebojni vpliv sestavin VKEN, je razvidno, da je upravljanje razlik med posamezniki/strokovnjaki v USOMID krožku lahko kompleksno. Tisti, ki vodi oziroma usmerja USOMID krožek, mora odkriti vplivne posameznike v mreži in opredeliti, kakšne so njihove kulture (Potočan & Mulej, 2006). Nato mora odkriti povezavo med posamezniki iz vplivnih mrež, odnose med njihovimi kulturami ter kulturne razlike, na koncu pa posvetiti pozornost virom teh razlik (tabela 1.3) (ibidem).

Slika 1.6: Krožne soodvisnosti med vrednotami, kulturo, etiko in normami



Vir: Potočan & Mulej, 2006, str. 4

Tabela 1.3: Tri soodvisne skupine virov kulturnih razlik

Psihološki viri kulturnih razlik	**Sociološki viri kulturnih razlik**	**Ekonomski viri kulturnih razlik**
individualizem : kolektivizem izogibanje velikim tveganjem : izogibanje malim tveganjem velika : mala distanca moči maskulinizem : feminizem	socialna struktura družbe religija jezik izobrazba	ekonomska filozofija politična filozofija komunikacije stil menedžmenta

Vir: Potočan & Mulej, 2006, str. 5

Pri obvladovanju teh razlik je vodji oziroma usmerjevalcu USOMID krožka lahko v pomoč tabela 1.4. Čeprav se vsebina iz tabel 1.3 in 1.4 nanaša na obvladovanje kulturnih razlik na področju mednarodnih poslovnih povezav, jo lahko uporabimo tudi na primeru obvladovanja kulturnih razlik na področju celovitega zaupanja državljanov v matične obveščevalno-varnostne službe.

Tabela 1.4: Okvir za obvladovanje kulturnih razlik

Kompetence vodje za ravnanje s psihološkimi viri kulturnih razlik	Kompetence vodje za ravnanje s sociološkimi viri kulturnih razlik	Kompetence vodje za ravnanje z ekonomskimi viri kulturnih razlik
Se ne zapirati vase, temveč poslušati mnenja drugih Biti navajen drugih (empatija) Sprejeti drugačno stališče v pogovoru (svoje in od drugih) Zanimanje za druge kulture Strpnost do drugih, samokontrola, potrpljenje Sposobnost zaupati, biti iskren in biti vreden zaupanja	Sprejeti relativnost svojih vrednot, znanja in razumevanja Biti prilagodljiv Biti strpen do nejasnosti Razvijanje mostov glede jezikovnih vprašanj Reševanje konfliktov Osebni odnosi Ponovno vzpostaviti splošno kulturo narodov in podobnega Diplomatsko obravnavanje	Vsi člani skupine imajo vpliv Skupina se mora sestati na različnih mestih, ki imajo različne kulture Heterogene ideje Eksperimentiranje in napake Skupne vizije in cilji Razumevanje ciljev vseh udeležencev v procesu Pripravljenost za sodelovanje

Vir: Potočan & Mulej, 2006, str. 5

Zakon entropije

Vsak sistem je podvržen entropiji. Entropija je »večna naravna težnja k propadu, lastna vsemu, kar obstaja,« (Mulej et al., 2000, str. 72) zato je upoštevanje **zakona entropije** pomembno, če želimo, da se s celovitim in ustvarjalnim delom izogibamo propadanju oziroma ga upočasnjujemo. Hkrati nas zakon entropije opominja, da so zaprti sistemi obsojeni na propad, odprti sistemi pa ga lahko upočasnjujejo z inovativnostjo, ki pa je odvisna od predhodno opredeljenih subjektivnih izhodišč in upoštevanja zakona o hierarhiji zaporedja in soodvisnosti (Mulej et al., 2000). »V vsaki službi in fazi dela nujno prevladujejo medsebojno *različna znanja, vednosti, vrednote, čustva, talenti in objektivne možnosti/delovni pogoji in viri*. Zato je nujno, da poleg specializacije zmorejo (vsaj neformalno) sistemsko razmišljanje čim številčnejši, zlasti pa koordinatorji, ki povezuje dele procesa v celoto.« (Mulej et al., 2008, str. 79) Poleg sistemskega razmišljanja je tudi pomembno, da ne gledamo le trenutnega stanja, temveč celotni razvoj tistega, kar opazujemo, pri tem pa z uporabo zakona entropije opuščamo trditev, da je narava neskončen vir vsega, kar je potrebno, in sprejemamo razvoj v novost kot naravni proces, ki prinaša ugodne kot tudi neugodne posledice (Mulej et al., 2008).

1.3.2 Modeliranje, sistematična hevristika in programoteka

Modeliranje pomeni način za razumevanje sistemov, ki jih preučujemo (Schwaninger, 2010), torej model *predstavlja* realni sistem (ibidem) in tiste njegove značilnosti, ki jih izpostavlja izbrani vidik (Mulej, 1979). Modele se uporablja pri opisovanju, pojasnjevanju, oblikovanju, sprejemanju odločitev ali spremembah (Schwaninger, 2010). Pomembni so tudi pri razreševanju problemov, učenju, spremembi pogojev ipd., saj razkrivajo dinamiko, lastnosti, tveganja in ranljivosti sistema, kar je posledica njihovega potenciala, da pri drugih sprožijo odkritje drugih vidikov na obravnavani objekt in pridobivanje novih vpogledov (ibidem). Osnovni pogoj je, da med modelom in sistemom obstaja podobnost, z legendo, ki predstavlja sestavine in njihove odnose v modelu in sistemu, pa se omogoči prepoznavanje njune medsebojne zveze (Mulej, 1979). Model je torej predstavitev in ponazoritev sistema, ne objekta kot celote (Mulej et al., 2008, str. 99). Tu nastopi modeliranje oziroma postopek sestavljanja modelov, ki pomeni »osnovo za proces spoznavanja in obvladovanja dogajanja z uporabo zamišljanja po **analogiji** (= podobnosti),« (Mulej, 1979, str. 110) namreč smisel modeliranja je poenostavitev sistema, da bi lažje dosegli spoznanja o njem (ibidem). Modeliranje je zato pomembno predvsem pri obravnavanju objektov, ki so drugače nedostopni neposrednemu opazovanju oziroma raziskovanju (Mulej, 1979, 1994).

Pri modeliranju se išče podobnosti med različnimi sistemi (kot miselnimi slikami) in modeli, ki so izomorfni – to pomeni, da imajo izomorfizme ali »podobnosti, enake lastnosti, ki jih odkrivajo vsaka s svojega vidika različne vede in v njih najdejo medsebojne stične točke, s čimer nastane most za njihovo sodelovanje.« (Šarotar Žižek & Mulej, 2015, str. 15) »Da bi dva sistema bila izomorfna, morata imeti povsem skladni zgradbi, [sic] ali povsem skladno obnašanje.« (Mulej, 1979, str. 111) V našem primeru smo iskali izomorfnosti, saj smo, kot bomo kasneje podrobneje obrazložili, upoštevali Beerovo Teorijo viabilnih sistemov (v nadaljevanju: TVS), ki določa zgradbo viabilnih sistemov, tj. sistemov, ki niso le živi, temveč preživijo. Iskali smo torej ne le skladnost zgradbe in obnašanja med sistemom in našim modelom ter našim modelom in drugimi, obstoječimi modeli, temveč tudi med našim modelom in splošno strukturo viabilnih sistemov, ki jo je oblikoval Beer (1984). Schwaninger (2010) pravi, da je model ključen

predpogoj za viabilnost organizacije, zato je pomembno, da je dovolj kakovosten. Organizacije, ki so viabilne/sposobne preživeti, imajo boljše modele (ibidem, str. 1423). To poudarja pomembnost pravilnega modeliranja, ki v skladu s pravilno rabo DTS zmanjšuje oziroma preprečuje spreglede in napake, preprečuje preskakovanje vrstnega reda korakov delovnega procesa ter preozko ali preširoko obravnavanje izbranega problema. Kljub temu se moramo zavedati, da modeliramo v okviru zakona zadostne in potrebne celovitosti, kar pomeni, da nikoli ne bomo mogli doseči popolne celovitosti in v model vključiti čisto vseh sestavin in povezav. V zvezi s tem je Mulej (1979) določil dve osnovni zahtevi modelov: biti morajo smiselni in smotrni ter morajo ustrezati realnosti. Z upoštevanjem sestavin in povezav DTS smo, upamo, izpolnili ti dve zahtevi.

Naš model ni izpopolnitev obstoječega modela, temveč novost. Za izdelavo novega je potreben sistemski pristop, za katerega je značilno (Gigch v Mulej, 1979, str. 129-130):
»(1) Problem je opredeljen v odnosu do nadrejenega sistema ali sistemov, h katerim zadevni sistem spada in s katerim(i) je povezan s skupnimi cilji.
(2) Cilji sistema običajno ne ležijo v kontekstu podsistemov, ampak je treba gledati na njih v odnosu do nadsistemov ali celotnega sistema.
(3) Obstoječe oblike je treba ovrednotiti s stroški priložnosti ali z obsegom razhajanj med sistemom in optimalno obliko.
(4) Optimalna oblika se običajno ne da najti z naraščanjem bližnjih, obstoječih, prilagojenih oblik. Zajema planiranje, vrednotenje in uresničevanje novih alternativ, ki nudijo inovacijska in ustvarjalna izhodišča za ves sistem.
(5) Oblikovanje sistema zajema procese razmišljanja, kot sta indukcija in sinteza, ki se razlikujeta od dedukcijske in redukcijske metode, ki sta v rabi, da bi dobili izboljševalne metode.
(6) Planiranje je zamišljeno kot proces, v katerem ima planer vlogo vodje usmerjevalca, ne zgolj sledilca. Planer mora spodbujati izbiro alternativ, ki blažijo ali celo spodbijajo, ne pa krepijo želene učinke in težnje predhodnih oblik sistemov.«

Predvideni vhod pri modeliranju je navadno sistem kot miselna slika o obravnavanem objektu, uvedena z izbranega vidika znotraj dialektičnega sistema vidikov. V proces modeliranja ne vstavimo objekta, ki ga obravnavamo, saj ima preveč dejanskih lastnosti,

temveč dialektični sistem o njem, ki je poenostavljen v sistem, omejen na izbrani vidik. V modeliranje tako vstavimo sistem oziroma njegove sestavne dele in povezave, ki jih z upoštevanjem sistemskih teorij (v našem primeru DTS) zadostno in potrebno celovito poenostavimo ter oblikujemo v ustrezen poenostavljen model. V našem primeru je zato predvideni vhod v modeliranje elementarni kibernetski sistem (kot sistem z izbranega vidika obvladovanja) ali sistem, ki ga ni mogoče razstaviti na kibernetske sisteme nižjega reda, in vsebuje upravljajoče organe, izvajalne (izvršne) organe in merilne organe (Mulej, 1979). V našem primeru smo imeli dvojno modeliranje. Osnovni model smo izoblikovali s pomočjo dostopne literature, lastnega znanja, intervjujev in ustreznih sistemskih teorij, nato pa smo ga s postopkom (drugega) modeliranja preoblikovali v ustrezen model kibernetskega sistema celovitega zaupanja državljanov v matične obveščevalno-varnostne službe, ki bo omogočal celovito zaupanje.

Vhodi prvega modela so spoznanja iz literature, spoznanja praktikov, primeri dobrega in šibkega zaupanja v obveščevalno-varnostne službe – pri tem smo z metodo triangulacije soočili pozitivne in negativne izkušnje, te pa se bodo iztekle v sinergijo ali emergenco, ki »zajema nastajanje lastnosti celote, ki jih sicer spregledamo, saj jih deli nimajo. Izraža proces – nastajanje in/ali nastanek novih lastnosti pod vplivom medsebojnega učinkovanja delov, ki so v medsebojnih odnosih […].« (Šarotar Žižek & Mulej, 2015, str. 15) Drugi vhodi pa so ostali, bolj specifični dejavniki, ki vplivajo na zaupanje državljanov v matične obveščevalno-varnostne službe. Pričakovani izhod bo zaupanje v službe, vendar brez predznaka (pozitivno ali negativno). Pri drugem modeliranju pa je vhod dobljeni model-sistem osnovnega zaupanja državljanov v službe, izhod pa model celovitega zaupanja, ki ima ravno tako en sam izhod, tj. zaupanje, vendar s pozitivnim predznakom: večje zaupanje. Poudarjamo, da ne moremo zagotoviti, da bo izhod modela zaupanje s pozitivnim predznakom (večje zaupanje), čeprav je to naša želja in cilj, saj je to odvisno predvsem od upoštevanja pravil DTS pri modeliranju ter nejasno opredeljenih in spreminjajočih se dejavnikov okolja, v katerem se bo model nahajal oziroma v katerem bo uporabljen. Ker smo želeli, da bo model viabilen oziroma da bo preživel, smo morali pri modeliranju upoštevati TVS in Model viabilnih sistemov (v nadaljevanju: MVS), ki izhaja iz upoštevanja TVS.

K razreševanju nalog in problemov lahko pomembno prispeva hevristika, »nauk o metodah raziskovanja in pridobivanja novih spoznanj« (Hevristika, b. d.), ki za reševanje kompleksnih problemov ni ustrezna, saj temelji na iznajdljivosti in se osredotoča predvsem na rutinerstvo (Mulej, 1979). Temu smo se pri modeliranju želeli izogniti, zato smo namesto hevristike uporabili **sistematično hevristiko**, »ki raziskuje faze duhovnega (umskega) – ustvarjalnega dela v procesih obdelovanja problemov, daje uporabi teh procesov učinkovitejšo podobo in omogoča hitro doseganje izvirnih in vrhunskih dosežkov. Smotrno vrednoti spoznanja, pridobljena v procesih znanstveno ustvarjalnega dela, jih zbira in sistemizira in jih daje na razpolago, zato da bi nove naloge obvladovali kar se da racionalno. Gre torej za to, da bi uveljavili racionalno organizacijo umskega ustvarjalnega dela.« (Mulej, 1979, str. 155) Bistvo sistematične hevristike Mulej (ibidem, str. 134) povzema v treh točkah:

»(1) uporabna je predvsem kot **metodologija** ustvarjalnega miselnega dela, ki se ne da urediti s klasičnimi metodami organiziranja dela, ker so usmerjene na rutinsko delo;

(2) za ta namen je lahko uporabna zato, ker ne izhaja iz vsebine obravnavanih problemov, ampak iz **postopkov** za obravnavanje;

(3) teh postopkov ne oblikuje kot fiksno predpisane formule, kakor je običajno in smiselno za rutinska dela, ki se morajo urediti s preciznimi postopki, ker se tako opravijo najbolje; postopke ustvarjalnega dela oblikuje v **okvirna navodila**, ki temeljijo na bogatih in sistematično zbranih in urejenih izkušnjah in na aktivnem sodelovanju vseh sodelavcev.«

Okvirna navodila oziroma okvirni postopki za obravnavanje problemov temeljijo na sistematično zbranih in urejenih izkušnjah ter sodelovanju (ibidem), s čimer se preprečuje togost, pretirano subjektivnost, enostranskost in rutinerstvo. Sistematična hevristika se od hevristike razlikuje tudi po tem, da se (Mulej, 1979, str. 133) »naslanja na samostojno in aktivno **sodelovanje**, s tem pa omogoča ne samo upoštevanje iznajdljivosti, tudi ne samo njenega zbiranja in urejanja in s tem prenašanja iznajdljivosti v izkustvo in širše dostopno znanje, ampak še več: omogoča, da se delo okvirno normira tako, da ga v smeri pri normiranju ureja tisti, ki ga opravlja, ne pa kdo drugi […].«

Osnovne faze sistematične hevristike so opredelitev izbranega problema, nato ustvarjanje modela oziroma sinteze modela, sledi analiza problema s pomočjo modela, ki smo ga ustvarili, ter na koncu sinteza rezultatov in naših spoznanj (ibidem, str. 30). Postopek dela poteka v naslednjem vrstnem redu: analiza procesa (prikaz procesa kot sistema), optimizacija (zmanjševanje slabih delov procesa z izboljšavami) in sinteza strukture procesa (ustvarjanje novega procesa) (ibidem, str. 137).

V prvi fazi sistematične hevristike je potrebno, da na podlagi ugotovitev DTS in DOMR (Rosi, 2004) pazimo, kako se lotevamo obvladovanja in razreševanja zapletene problemske situacije. Ni najpomembneje, kako razrešiti problem, ampak je treba najprej ugotoviti, ali sploh imamo problem, nato pa kaj želimo doseči z njegovo razrešitvijo. Zato raziskujemo nastanek oziroma identifikacijo neke problemske situacije, ki ni že kar sama po sebi (bolj ali manj) zapleten problem, ampak je njena opredelitev posledica naše sposobnosti (trenutne) zaznave (tj. spleta vrednot, vednosti, izkušenj in znanj, ki jih imamo o podobni situaciji in jih pripisujemo zaznanemu (problematičnemu) pojavu). Pri tem je potrebno ločevati navidezne od resničnih problemov in iskati poti njihovega čim bolj celostnega in zato dovolj trajnega razreševanja (Rosi, 2004).

Pri tem se moramo zavedati, da imajo v vseh procesih, zlasti takšnih, kot je razreševanje zapletenih problemov (npr. naš model ustvarjanja celovitega zaupanja državljanov v matične obveščevalno-varnostne službe, op. G. H.), večji vpliv (Mulej, 1994) začetni dogodki kot kasnejši. Posledični, (neposredni in posredni) vplivi vzporednih dogajanj pa se tudi prepletajo, ker so bolj ali manj odvisni drug od drugega, torej soodvisni. DOMR nam je omogočila njihovo učinkovito in uspešno sinergijsko izrabo za razreševanje zapletenih problemov (Rosi, 2004).

V nadaljevanju kreiranja modela sistematične hevristike nato z analizo prikažemo strukturo ali delovanje trenutnega sistema, postavitev novih modelov za iskanje šibkih točk obstoječega modela ter značilnosti sistema. Določiti je potrebno tudi meje analize z vidika obsega in časa. Prikaze je potrebno opisati in nato na podlagi tega prepoznati tokove, ki tečejo skozi sistem, vrstni red funkcij sistema in njihovo razporeditev po pomembnosti. Delo mora biti zaradi kompleksnosti sistema opravljeno postopno

oziroma po korakih. Sistem nato najprej prikažemo kot množico podsistemov, nato pa preučimo le strukturo bistvenih podsistemov (povzeto po Mulej, 1979, str. 137-139).

Pri tem postopku zbiramo svoje izkušnje, ki jih razvrstimo v programoteko, tj. okviren model postopkov dela oziroma bazo okvirnega dela o postopkih oziroma hevristično programsko biblioteko (Mulej, 1979; Mulej et al., 2000; Mulej et al., 2008). Če datoteka pomeni urejeno zbirko podatkov o čemerkoli, pomeni biblioteka urejeno zbirko knjig, programoteka pa urejeno zbirko modelov postopkov (Mulej et al., 2000, str. 203). Z zbiranjem in uvrščanjem znanj in izkušenj v programoteko nastane sistem programov (Mulej, 1979), ki ga s pomočjo sistematične hevristike sproti dopolnjujemo. Dopolnjujemo ga tudi tako, da pri takšnem problemu, ki je podoben kakemu že obravnavanemu, poiščemo ustrezni okvirni program ter ga dopolnimo s posebnostmi aktualnega problema (ibidem). Postopno tako nastane programski sistem sistematične hevristike, sestavljen iz osnovnega programa in pa programoteke ožje specializiranih podprogramov (ibidem). Osnovni program je mogoče primerjati s postopkom NOVOST, kot vidimo v delu avtorjev Mulej et al. (2000, str. 207).

Osnovni program daje splošni pregled nad sistematičnim načinom dela (izkušnje, že napisani programi), iz njega je razviden hierarhijski način dela ter omogoča pregled nad celoto, vendar se ne ukvarja s podrobnostmi – z njimi se ukvarja programoteka. Z osnovnim programom torej ne rešujemo konkretnih zadev, temveč se z njim uveljavlja splošni sistematični način dela glede na določene izkušnje in znanje, hkrati pa predpisuje hierarhijo (zaporedje) postopkov (ibidem).

Programoteka je sestavljena iz povezovalnih in delnih programov (Mulej et al., 2000). »***Povezovalni* program** je pri tem model splošnega, povsem okvirnega postopka ustvarjalnega miselnega dela. Povezuje delne programe. ***Delni* programi** pa so modeli poteka posamičnih korakov splošnega postopka iz povezovalnega programa.« (ibidem, str. 203) Programoteka nastaja (Mulej et al., 2008, str. 133):

- »postopno, od *grobega* pregleda k *podrobnemu* vpogledu, od globala do delnih procesov, da celovitosti ne izgubimo izpred oči, ko nas pritegne ožja specializacija;

- v sodelovanju *izkušenih in iznajdljivih* izvajalcev obravnavanih delnih procesov, ki prispevajo svojo vednost (znanje o vsebini), in *metodologov*, ki po potrebi prispevajo znanje o metodi USOMID, da izvajalci svoje znanje o metodi USOMID, da izvajalci svoje znanje in izkušnje lažje izrazijo in skupno oblikujejo;
- toliko natančno, da postane uporabna kot *okvirna* in samo okvirna rutina, ki *podpira* ustvarjalnost, ne da jo nadomešča (kot je običaj pri tehnoloških in vsaj delno pri organizacijskih predpisih).«

Shematski prikazi osnovnega/prikazovalnega programa za izdelavo in uporabo programoteke ter za posamezne naloge (podprograme) prikazujejo slike v delih Mulej (1979, str. 140, 144, 145) in Mulej et al. (2000, str. 206-208), pri čemer so slike v slednjem delu podrobno dopolnjene, dodatno pa vsebuje tudi shematski prikaz postopka podrobnega spoznavanja izbrane naloge (ibidem, str. 206) – korak N v Mulej et al., 2008 –, in shematski prikaz postopka za ugotovitev informacijskih potreb, pridobitev in ureditev informacij (ibidem, str. 209) – korak V v Mulej et al., 2008. Mulejevo delo iz leta 1979 slednjega ne vsebuje, vsebuje pa shemo pomnilnih mest hevristične programoteke (glej Mulej, 1979, str. 147). Navedene sheme smo upoštevali pri izdelavi naše programoteke, večji poudarek pa smo dali USOMID/NOVOST.

Pri ustvarjanju programoteke se upošteva postopek (Mulej et al., 2008, str. 133)

»1. korak: pogovor z izvajalci/poznavalci procesa, kako poteka od začetka proti koncu, z vprašanji: kaj, kdo, kdaj, kje, kako dela;

2. korak: pogovor z izvajalci/poznavalci procesa o zapisu iz 1. koraka, le da ga zdaj pogledujemo od konca proti začetku z vprašanji:

- Ali je zapis *popoln*?
- Ali je mogoče kakšno opravilo ali skupino opravil *opustiti*?
- Ali je predhodni korak zares *pogoj* za ta hip obravnavanega?

Pri tem postavimo vprašanje 'zakaj?' k vsakemu od prejšnjih in dobimo 'drevo vzrokov'. […] Vzroke in pogoje, ki jih ocenimo za odvečne in nekoristne ali nepotrebne, izločimo.

3. korak: pogovor z izvajalci/poznavalci procesa, a tokrat gre za *okolje* procesa:

- Od katerih dejavnosti/procesov je odvisen *vhod* v obravnavanega?

- Kateri *dokumenti* in s katerimi *informacijami* spremljajo *vpliv takih* dejavnosti/procesov in kako jih prevzemajo?

4. korak: pogovor z izvajalci/poznavalci procesa; tudi tokrat gre za okolje procesa:

- Katerim dejavnostim/procesom so *izidi* obravnavanega procesa vhod?
- Kateri *dokumenti* in s katerimi *informacijami* spremljajo *vpliv na* take dejavnosti/procesov in kako jih prevzemajo?«

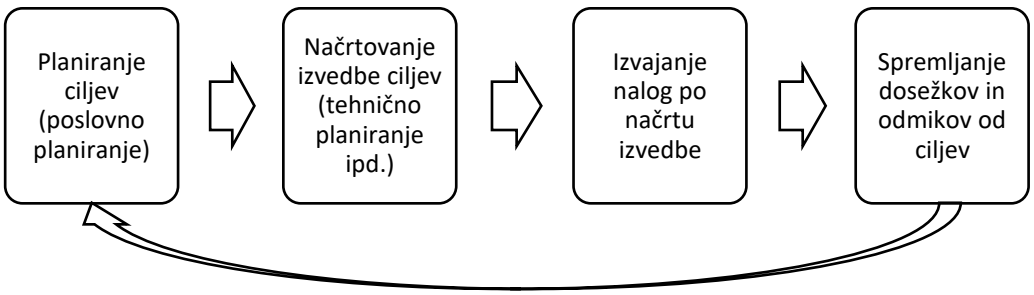
Pridobljena spoznanja nato zapišemo na programotečni list (začnemo z vrstico 4, da opravimo koraka 1 in 2, nadaljujemo z vrsticami 1-3 za korak 3, nato v vrsticah 5-7 za korak 3, a ostanemo v povezavi z vrstico 4 (Mulej et al., 2008)), ki ga prikazuje tabela 1.5. Upoštevali smo povezovalni program programoteke v najkrajši verziji (slika 1.7).

Tabela 1.5: Programski list za opis delnih procesov, vnesenih v programoteko

1. Vhodne povezave 2. Vhodni dokument in informacije	Pogoji za obravnavani proces (od kod vplivi prihajajo) Nosilec informacij
3. Vhodna informacijska dejavnost	Sprejem vpliva na proces
4. Temeljni proces obravnavanega dela celotnega procesa	Potek obravnavanega delovnega procesa
5. Izhodna informacijska dejavnost 6. Izhodni dokument in informacije	Oddaja vpliva procesa Nosilec informacij
7. Izhodne povezave	Posledice obravnavanega procesa (kam vplivi odhajajo)

Vir: Mulej et al., 2008, str. 134

Slika 1.7: Povezovalni program programoteke v najkrajši verziji



Vir: Mulej et al., 2000, str. 525; Mulej et al., 2008, str. 134

Za uporabo programoteke smo se odločili, ker nam njena izdelava »omogoča tisto uporabo *vednosti*, ki take vrednote spodbuja najmočneje in najkoristneje, ko gre za *organizacijske* inovacije, ki zmorejo aktivirati praktično vse. […] Zato kaže začeti

prenašati pozornost od samo tehnično-tehnoloških na **vse tipe invencij in inovacij** npr. z izdelavo programoteke.« (Mulej et al., 2008, str. 129) Kot pravijo Mulej et al. (ibidem, str. 132-133), nam »[u]stvarjanje *programoteke* (= baze *okvirnega znanja o postopkih*) daje ***podlago za upoštevanost*** in zapis o poteku postopkov dela in njihovih povezavah, ki je istočasno uporaben za več namenov:

1. Je priročnik (opomnik o postopkih) za vsakdanje delo, ki ne določa ničesar na pamet, ampak po preverjenih izkušnjah iznajdljivih izvajalcev obravnavanega dela. Razen tega je zapis okviren, ne zajema vseh podrobnosti, tako da hkrati *lajša* delo (v podsistemu rutinskega dela postopkov) in daje *prostor in podporo* za ustvarjalnost (v tistem podsistemu postopkov, ki se ne ponavlja).
2. Je *podlaga za invencije, potencialne inovacije in inovacije*, saj se iz programotečnega zapisa dosti lažje kot brez njega vidi, kaj je (možno) problem in/ali možna izboljšava v postopkih, v delu, z njimi opravljanjem, in v povezovanju med njimi.
3. Je *podlaga za sodelovanje*, saj daje jasno sliko odgovornosti, odvisnosti, neodvisnosti in soodvisnosti, povezav med delnimi procesi, pogojev za delo, posledic dela v drugih delnih procesih, toka informacij ipd.«

1.3.3 Dialektično omrežno razmišljanje

Kadar se želimo s teoretičnimi razrešitvami problemov resnično približati praktični poslovni stvarnosti, moramo to opraviti kar se da celostno. To nam omogočata poznavanje in uporaba teorije sistemov, ki služi za preučevanje in obvladovanje (tj. kar se da trajno razreševanje) tako teoretičnih kot tudi praktičnih problemov oziroma z njimi povzročenih problemskih situacij, ki jih obravnavamo kot sistem – splet, zapleten pojav (tudi miselna slika o njem).

Zaradi tega smo poleg DTS uporabili metodologijo DOMR (glej npr. Rosi & Mulej, 2006; Rosi & Rosi, 2011; Rosi, 2015) oziroma model sistemskega razmišljanja, ki sinergijsko združuje omrežno razmišljanje (v nadaljevanju: OMR) in DTS (Rosi & Mulej, 2006) – glej sliko 1.8. Tako DTS kot DOMR sta »namenjena povezovanju med strokovnjaki različnih specialnosti, da bi dosegli potrebno in zadostno celovitost.« (Knez & Mulej, 2011, str. 56)

Slika 1.8: Sinergijska integracija dialektične dimenzije v metodologijo OMR

Vir: Rosi, 2004

DOMR namreč temelji na prepričanju, da mora postopek razreševanja problemov vključevati soodvisno in interdisciplinarno sodelovanje vseh sodelujočih v organizacijskih ali poslovnih sistemih (Rosi, 2015), hkrati pa tudi poudarja vlogo

posameznikovih lastnosti in sposobnosti pri obvladovanju problemov (Rosi & Rosi, 2011), ki jih kot pomembno sestavino sistemskega razmišljanja upošteva že DTS.

Osrednja aktivnost DOMR je razmišljanje ali mišljenje, »usmerjen proces za odkrivanje novih odnosov med izkušnjami. Pojavi se, ko posameznik naleti na problem – na znano ali s predstavami ali simboli prikazano situacijo, ki jo skuša dojeti v novih zvezah. V tem se mišljenje razlikuje od učenja.« (Musek & Pečjak, 1988 v Rosi & Rosi, 2011, str. 65) Spremembe v okolju in nove situacije nas prisilijo, da spremenimo svoje mišljenje/razmišljanje, te pa od nas lahko tudi zahtevajo, da k razreševanju problemov pristopimo ustvarjalno (Rosi & Rosi, 2011). Poleg mišljenja poznamo tudi domišljijo. Med mišljenjem in domišljijo obstaja razlika v dojemanju odnosa do stvarnosti, zato so pri slednji v večji meri pomembna čustva (ibidem). DOMR daje poudarek predvsem interdisciplinarnemu izkoriščanju »*znanj, vednosti, talentov, vrednot, čustev in možnosti – sestavin in povezav med IQ in EQ,*« (ibidem, str. 68) saj »zaradi svojih mehkosistemskih lastnosti omogoča boljše aktiviranje in izrabo pozitivnih sinergijskih učinkov obeh, IQ in EQ.« (ibidem)

Inteligenco/inteligenčni kvocient/IQ (v nadaljevanju: IQ) je mogoče razumeti kot »hitrost in učinkovitost miselnih procesov pri uporabi znanja/sposobnosti (brainstorming) v problemskih in novonastalih situacijah.« (Mensa Slovenija, b. d.) Čustvena inteligenca (v nadaljevanju: EQ) pa je definirana kot »sposobnost spremljanja lastnih občutkov in čustev ter občutkov in čustev drugih oseb, da bi razlikovali med njimi in uporabili to informacijo kot usmeritev za lastno razmišljanje in delovanje.« (Salovey & Mayer, 1990, str. 189) EQ zato tudi odraža sposobnost vživeti se v vlogo nekoga drugega.

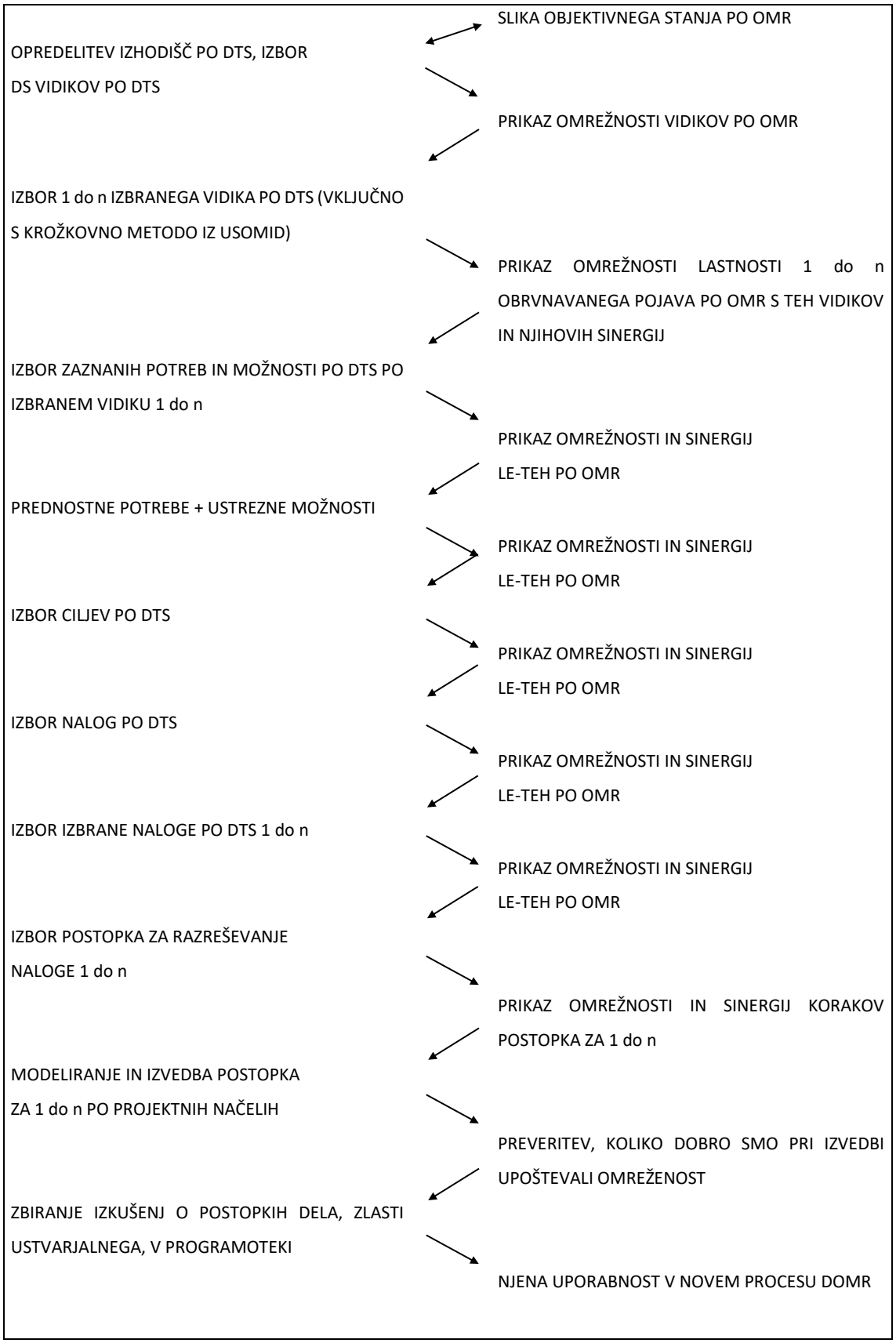
Kaufman (2017) na podlagi lastne študije in raziskav drugih namreč ugotavlja, naj bi bil IQ osebnostna lastnost, povezana z odprtostjo za izkušnje, ki bolj povezana z intelektualnim udejstvovanjem in miselno hitrostjo kot z domišljijo, iznajdljivostjo ali intelektualnostjo. Medtem pa imajo pri domišljiji večjo vlogo čustva (Rosi & Rosi, 2011), kjer pride do izraza posameznikova EQ. IQ in EQ sta zato izjemno pomembna za

delovanje v timu, kjer posameznik razmišlja samostojno in skupaj z drugimi. Iz tega posredno izhaja, da DOMR (Rosi & Mulej, 2006, str. 1171):

1) zahteva in podpira timsko delo;
2) podpira zadostno in potrebno celovito delo za razvoj organizacijskih ali poslovnih sistemov;
3) podpira organizacijo ter strukturo organizacijskih ali poslovnih sistemov, ki so osredotočeni na inovacije in razvoj;
4) prikazuje, katera vrsta organizacijskih ali poslovnih sistemov ustreza sodobnemu okolju in je zmožno uporabe DOMR;
5) poudarja soodvisnost razvoja in strukturiranja organizacijskih ali poslovnih sistemov z razvojem projektnega menedžmenta;
6) podpira spremembe menedžmenta v organizacijskih ali poslovnih sistemih;
7) olajša zaznavo potreb za prestrukturiranje organizacijskih ali poslovnih sistemov;
8) podpira pridobivanje in pozabljanje znanja v organizacijskih ali poslovnih sistemih;
9) služi kot temelj za pripravo sodobne organizacijske kulture.

Postopek DOMR kot metodologije za sistemsko razmišljanje oziroma postopek razreševanja problemov prikazuje slika 1.9. Značilnost DOMR je tudi ponavljanje oziroma iteracija procesa razreševanja problemov. »Če ugotovimo, da npr. identifikacija problema(tike) ni bila zadostna (= dovolj celovita), se vrnemo v izhodiščni korak. Od tam pa imamo dokaj odprte možnosti, saj ni vedno nujno, da ponovno preizkusimo vse korake zaporedoma, ampak lahko izbiramo (naprej in nazaj v krogotoku) za dano problemsko situacijo le najprimernejše […].« (Rosi & Rosi, 2011, str. 68) Ta fleksibilnost omogoča ukvarjanje le s tistim, kar je potrebno popraviti, spremeniti ali prilagoditi, in to takrat, ko razreševalec problema presodi, da je to potrebno. S tem se razreševalec problema bolj približa celovitosti, saj z nenehnim presojanjem različnih situacij in možnosti prihaja do novih spoznanj ter do zanj ustreznejših (raz)rešitev problema.

Slika 1.9: Potek procesa razreševanja kompleksnih problematik z uporabo DOMR



Vir: Rosi, 2004

1.3.4 Druge uporabljene znanstvene metode

Pri raziskovanju smo poleg DTS in DOMR uporabili tudi postopek kvalitativnega raziskovanja oziroma kvalitativne metode, ki so zaradi poudarjanja poglobljenega empiričnega preučevanja primerne za raziskovanje skupin, ki jih splošna javnost težje ali napačno razume (Ragin, 2007, str. 99) – v našem primeru obveščevalno-varnostne skupnosti. Metode kvalitativnega raziskovanja omogočajo celostno oziroma holistično razkrivanje subtilnih, skritih vidikov in značilnosti omenjenih skupin (Ragin, 2007).

Uporabili smo postopek analitične indukcije in postopek teoretičnega vzorčenja. Analitična indukcija je sistematično preučevanje podobnosti in nasprotovanj, ki omogoča recipročno razjasnjevanje pojmov in kategorij, cilj te metode pa je dobiti natančnejšo oziroma jasnejšo podobo o predmetu raziskovanja, kar dosežemo z iskanjem povezav in vzrokov za podobnost in razlike med posameznimi pojavi oziroma pojavnimi oblikami (Ragin, 2007, str. 99). V okviru analitične indukcije smo uporabili primerjalne metode raziskovanja, namenjene preučevanju konfiguracij, tj. specifičnih kombinacij lastnosti, ki so skupni določenemu številu obravnavanih primerov, oziroma zapletenih vzorcev podobnosti in razlik obravnavanih primerov (Ragin, 2007, str. 128) – v našem primeru modelov. Teoretično vzorčenje pomeni proces izbire novih raziskovalnih prizorišč/primerov z namenom njihove primerjave z že preučevanimi (Ragin, 2007, str. 113). Pri teoretičnem vzorčenju najprej poiščemo t.i. konstantne vidike oziroma enake značilnosti različnih obravnavanih primerov, nato poiščemo nove primere, ki ravno tako vsebujejo enake konstantne vidike kot obravnavani primer, nato pa primerjamo različne vidike obravnavanih in novih primerov. Ragin (2007, str. 114) ugotavlja, da je teoretično vzorčenje tehnika triangulacije podatkov, pri kateri uporabimo neodvisne, različne podatke, da bi bolje razumeli tisto, kar le delno oziroma manj poznamo.

Raziskovali smo v skladu z znanstveno metodo, ki povezuje dedukcijo ali deduktivno metodo, tj. »miselno dejanje, ki temelji na danem znanju,« (Ragin, 2007, str. 29) po kateri prehajamo od splošnega h konkretnemu (Ivanko, 2007; Toš & Hafner-Fink, 1997), in indukcijo ali induktivno metodo, ki pomeni oblikovanje splošnih idej z ocenjevanjem

implikacije izkustvenega, tj. novega gradiva v kombinaciji s starim gradivom (Ragin, 2007), torej prehajanje od posamičnih dejstev k splošnim dejstvom oziroma sodbi (Ivanko, 2007). Kot pravita Toš & Hafner-Fink (1997), se izraz 'izkustvo' v znanosti enači z izrazom 'empirika' (del posameznikovega spoznanja kot rezultat neposrednega zaznavanja sveta). Znanstvena metoda povezuje izkustvo in teorijo (ibidem). »[P]ri dedukciji izhajamo iz splošnih idej in jih apliciramo na izkustveno gradivo, pri indukciji pa izhajamo iz izkustvenega gradiva ter ocenjujemo implikacije tega gradiva za splošne ideje.« (Ragin, 2007, str. 30) Kot pravi Ragin (ibidem), znanstvena metoda zahteva naslednji postopek:

- »študij relevantne literature;
- formuliranje hipoteze;
- razvijanje raziskovalnega načrta (dizajna);
- zbiranje podatkov;
- analiza podatkov na način, kot zahteva hipoteza.«

Podatke smo zbirali iz javno dostopnih virov, za zbiranje podatkov pa smo uporabili tudi metodo intervjuvanja (Ivanko, 2007), natančneje metodo polstrukturiranega globinskega intervjuja. Z intervjuvanjem smo tudi izpolnjevali kriterij sodelovanja z drugimi specialisti, ki ga določa DTS oziroma USOMID/NOVOST. Globinski intervju je vrsta intervjuja, pri katerem preverjamo poglede ali mnenje posameznika ali skupine v zvezi z določeno idejo, programom ali situacijo, zato je uporaba tovrstnega intervjuja primerna, ko želimo pridobiti natančne podatke, potrebne za popolnejšo sliko o obravnavani tematiki (Boyce & Neale, 2006, str. 3). Polstrukturirani intervju pa je vrsta intervjuja, pri katerem je večina vprašanj vnaprej določenih, vendar omogoča intervjuvancu prilagodljivost in možnost, da sam oblikuje tok informacij (Wilkinson & Birmingham, 2003, str. 45). Uporaba obeh zvrsti intervjuja nam je omogočila pridobitev manjkajočih podatkov, ki niso bili dosegljivi iz javnih virov ali preko njih in so pomembni za razjasnitev skritih ozadij obravnavanega problema. Istočasno pa je ta metoda služila tudi kot orodje za preverjanje pravilnosti naših predpostavk, ugotovitev in mnenj, predvsem pa za iskanje sestavnih delov osnovnega modela, ki bi jih mi nehote spregledali, ter preverjanje ustreznosti vmesnih različic osnovnega modela pred izgraditvijo njegove končne različice. Vprašanja za intervju smo oblikovali na podlagi

spoznanj, do katerih smo prišli s sintezo starega znanja z novim znanjem, pridobljenega z raziskovanjem izbranega področja oziroma problema, vsebina vprašanj pa se nanaša na zaupanje državljanov v matične obveščevalno-varnostne službe, na domnevno soodvisnost obveščevalno-varnostih služb in zaupanja državljanov, na dejavnike učinkovitosti obveščevalno-varnostnih služb in na nekatera druga vsebinsko sorodna področja, zanimala pa so nas tudi mnenja in predlogi intervjuvancev. Za intervjuvance smo poiskali osebe, ki so bile nekoč ali v času izbire intervjuvancev zaposlene v slovenskih obveščevalno-varnostnih službah ali člani Komisije za nadzor obveščevalnih in varnostnih služb (v nadaljevanju: KNOVS). Izvedba intervjujev je podrobneje predstavljena v podpoglavju 4.1.

Razen izvedbe krajše raziskave, pri kateri nas je zanimalo mnenje, ali ljudje zaupajo slovenskim obveščevalno-varnostnim službam, zaupanja državljanov (laične javnosti) v obveščevalno-varnostne službe nismo preverjali oziroma merili. Menimo, da imajo državljani premalo (strokovnega) znanja o obveščevalno-varnostni dejavnosti in obveščevalno-varnostnih službah, zato bi bilo njihovo mnenje najverjetneje neutemeljeno, pavšalno ali napačno in preveč subjektivno. Tudi mnenje strokovnjakov, specialistov je sicer subjektivno, vendar je zaradi njihove strokovnosti o njihovem mnenju mogoče govoriti z večjo stopnjo kredibilnosti. Poleg tega smo pred izgradnjo modela predpostavljali, da je mnenje državljanov podvrženo različnim dejavnikom, med katerimi prevladujejo predvsem takšni, ki so z našega vidika obravnavanja negativni, torej pospešujejo entropijo in negativno vplivajo na povezave med elementi sistema. To smo tekom raziskave tudi potrdili, zato bi z obravnavo javnega mnenja posredno obravnavali takšne dejavnike in dobili napačne oziroma zmotne podatke/informacije ter posledično napačna spoznanja o stvarnosti. Končni model bi zato pospeševal entropijo, namesto da bi jo upočasnjeval.

Za Za analizo in interpretacijo podatkov, kasneje pa za preverjanje hipotez smo uporabili metodo deskripcije oziroma opisovanja, metodo kompilacije, komparativno oziroma primerjalno metodo in metodo sinteze oziroma združevanja (Ivanko, 2007). Ragin (2007, str. 71) opozarja, da je poleg analize pomembna in potrebna tudi sinteza oziroma

povezovanje posameznih podatkov v smiselno celoto, kar smo storili s posameznimi dejavniki, ki smo jih povezali v model.

Pri raziskovanju smo upoštevali metodološko osnovo sistemskega raziskovalnega pristopa, kar pomeni, da smo zapleteno problematiko disertacije spoznavali po delih, vendar ne da bi kakšen del razglasili za (dokončno) celoto, pač pa smo s povezovanjem takšnih delnih spoznanj v prepleteni splet (tj. sistem) želeli doseči kar se da celovito sliko in dejanje, s tem pa tudi ustvarjalnost, ki ni le navidezna, ker ni zgolj enostranska.

1.4 Predpostavke in omejitve

Izhajali smo iz predpostavke, da bodo odnosi in sinergije med splošnimi in specifični dejavniki modela, ki vplivajo na zaupanje, ter odnosi in sinergije med temi dejavniki in okoljem pokazali, da so obveščevalno-varnostne službe v večji meri odvisne od zaupanja državljanov, kot pa je to v literaturi in splošnem prepričanju veljalo doslej, in da je od tega zaupanja odvisna tudi nacionalna varnost. Pričakovali smo, da bomo dokazali tudi soodvisnost zaupanja državljanov v matične obveščevalno-varnostne službe in učinkovitosti obveščevalno-varnostnih služb, ki neposredno vpliva na nacionalno varnost. Predpostavljali smo, da obveščevalno varnostne službe že od nekdaj delujejo nespremenjeno, spreminjata se le družba in družbena ureditev, ter da bo večjo pozornost pri iskanju dejavnikov modela zato potrebno posvetiti družbenim dejavnikom/procesom in ne toliko obveščevalno-varnostnim službam. Menimo, da demokratična ureditev obveščevalno-varnostnega sistema in demokratičnega nadzora obveščevalno-varnostnih služb – v katera sicer ne dvomimo – še ne zagotavljata nujno, da bodo obveščevalno-varnostne službe vedno in dosledno upoštevale človekove pravice, zato po našem prepričanju navedena dejavnika nista glavna oziroma edina dejavnika celovitega zaupanja državljanov v matične obveščevalno-varnostne službe.

Upoštevali smo, da se modeli zaupanja z različnih področij med seboj razlikujejo, zato nekateri gradniki modela niso bili ustrezni za naš model. Kljub temu nam je analiza teh modelov in definicij zaupanja pomagala pri iskanju potrebnih dejavnikov oziroma gradnikov osnovnega modela zaupanja ter kasneje modela celovitega zaupanja

državljanov v matične obveščevalno-varnostne službe. V skladu s pričakovanju nekateri podatki iz različnih razlogov niso bili dostopni preko javnih in odprtih virov (nedostopnost podatkov). Do nekaterih podatkov nismo mogli dostopati, ker so v skladu s predpisi označeni s stopnjo tajnosti, v primeru hipotetičnega dostopa do njih pa jih ne bi smeli uporabiti in razkriti. Največjo omejitev (je) predstavlja(l) preizkus logistike aplikacije predlaganega modela, ki ga ne bomo mogli realizirati v praksi, saj nimamo niti zakonodajne niti izvršilne moči (omejitve za praktično simulacijo predlaganega modela). Logistiko aplikacije modela smo zato le teoretično simulirali. Pozorni pa smo morali biti na še eno pomembno omejitev naše doktorske disertacije: nejasno opredeljene okoliščine, ki so oteževale pojasnjevanje znotraj okvirov klasičnega razmišljanja in iskanja odgovorov.

2 Obveščevalno-varnostna dejavnost

Obveščevalno-varnostna dejavnost je proces »zajemanja, zbiranja podatkov, njihovega vrednotenja in analiziranja ter distribucije informacij do uporabnikov raznolikih obveščevalnih informacij, potrebnih pri odločanju.« (Podbregar, 2012, str. 24) Ugotovili smo (Ivanuša et al., 2016, str. 1), da uporablja »[s]lovensko znanstveno izrazoslovje (npr. v Purg, 1995; Anžič, 1997; Šaponja, 1999; Miklavčič, 2001; Podbregar, 2008, 2012; Henigman, 2008; Čaleta, 2009; Rode, 2010; Sotlar, 2012; Koren, 2012) […] skupen izraz o*bveščevalno-varnostna dejavnost,* iz katere izhajajo tri zvrsti (Podbregar, 2008): *obveščevalna, protiobveščevalna in varnostna zvrst.*« Te tri zvrsti v doktorski disertaciji imenujemo *dejavnosti* in predstavljajo svojevrstne aktivnosti v okviru obveščevalno-varnostne dejavnosti. Za potrebe doktorske disertacije je vsebina osredotočena le na obveščevalno-varnostno dejavnost, ki jo preko svojih obveščevalno-varnostnih služb izvaja država. Obveščevalno-varnostna dejavnost zasebnega sektorja in zasebnih akterjev zato v doktorski disertaciji ni obravnavana.

»Slovensko izrazoslovje in delitev se nekoliko razlikujeta od angleške, pri kateri se za obveščevalno-varnostno dejavnost uporablja izraz *Intelligence* (npr. v Rudner, 2002, 2013; Clark, 2007; Steele, 2010). Za obveščevalno zvrst se uporablja isti izraz, tj. *Intelligence* (npr. v Lowenthal, 2014), ali *Positive Intelligence* (Godson, 2011; Turner, 2014; Tromblay, 2015)*,* izraz *Intelligence* pa lahko poleg obveščevalne zvrsti pomeni tudi obveščevalni podatek ali obveščevalni izdelek, zato je pomen izraza *Intelligence* v angleškem jeziku odvisen od konteksta njegove uporabe. Za protiobveščevalno dejavnost/zvrst se uporablja izraz *Counterintelligence* (Johnson, 2009; Godson, 2011) ali *Negative Intelligence* (Kuloğlu, Gül & Erçetin, 2014), za varnostno dejavnost/zvrst pa ni podobnega izraza, kot ga poznamo v slovenščini. Ker gre za področje odkrivanja in preprečevanja posebnih oblik ogrožanja države, je tudi izrazov več: *Security* (varnost), *Homeland Security* (domovinska varnost), *Counterterrorism* (protiteroristična dejavnost) in še nekateri drugi izrazi. Te naloge izvajajo posebni policijski organi ali drugi organi s policijskimi pooblastili, zato se vsaka takšna organizacija imenuje 'varnostna služba' oziroma '*Security Service*'.« (Ivanuša et al., 2016, str. 1-2)

Obveščevalna dejavnost je (v kontekstu aktivnosti, ki jih izvaja država, op. G. H.), usmerjena na pridobivanje podatkov v tujini (oziroma v povezavi s tujino, op. G. H.) za potrebe nacionalne varnosti (Hočevar, 2011) in nacionalnih interesov. Obveščevalno-varnostno dejavnost se pogosto enači z obveščevalno dejavnostjo, čeprav je slednja le ena od sestavin obveščevalno-varnostne dejavnosti. Obveščevalna dejavnost poteka v več korakih. Nekateri avtorji sklopu teh korakov pravijo obveščevalni ciklus (npr. Šaponja, 1999; Purg, 2002; Hulnick, 2005; Johnson, 2009; Podbregar & Ivanuša, 2008; Črnčec, 2009; Phythian, 2013), drugi obveščevalni proces (npr. Taylor, 2007; Lahneman, 2010), nekateri pa uporabljajo oba izraza (npr. Gill & Phythian, 2006). Zaradi jasne vsebinske razmejitve in podrobnejšega razumevanja je prikazan potek obveščevalne dejavnosti (oziroma obveščevalnega kroga) v šestih korakih (povzeto po Dvoršek & Podbregar, 2012, str. 144-148):

1. **dodelitev naloge**: kdo je naročnik, katere informacije potrebuje, kakšne so zahteve, opredelitev področja in vprašanj, ki jih je potrebno obravnavati, določitev prednostnih nalog ipd.;
2. **načrtovanje in upravljanje**: izdelava načrta zbiranja podatkov;
3. **zbiranje podatkov**: izvedba zbiranja podatkov v skladu s predhodno pripravljenim načrtom;
4. **vrednotenje in primerjanje podatkov**: ocenjevanje izvora in kakovosti podatkov ter njihovo preoblikovanje na način, da jih lahko primerjamo z ostalimi podatki, ko je to potrebno;
5. **analiza in analitični proces**: pripisovanje pomena zbranim podatkom, ocenjevanje njihove zanesljivosti, variabilnosti in pomembnosti ter oblikovanje podatkov v obveščevalno informacijo oziroma končni izdelek (poročilo, obvestilo, ocena, mnenje ipd., op. G. H.);
6. **posredovanje končnih izdelkov**: pravočasno in ustrezno posredovanje obveščevalnih informacij naročnikom/uporabnikom ter pridobitev povratne informacije o njeni ustreznosti oziroma uporabnosti.

Zbiranje podatkov iz 3. točke se deli na več vrst. Šifrer (2008, str. 154-155) jih klasificira v tri (krovne) vrste zbiranja podatkov glede na njihovo dostopnost in glede na uporabljene metode za zbiranje:

- zbiranje javno dostopnih podatkov (mediji, novice, javno dostopni in objavljeni dokumenti, javno mnenje);
- zbiranje podatkov, do katerih je javni dostop omejen (preko diplomatsko-konzularnih in drugih predstavništev, prikritega anketiranja, prikritega znanstvenega raziskovanja);
- tajne metode zbiranja (plasiranje svojih pripadnikov obveščevalno-varnostnih služb v tuje strukture, tajno sodelovanje, tajna uporaba operativno-tehničnih sredstev).

V nekoliko ožjem smislu pa se zbiranje podatkov deli na (povzeto in združeno po Šaponja, 1999; Podbregar & Ivanuša, 2008; Črnčec, 2009; Koren, 2012; Hribar, Podbregar & Ivanuša, 2014):

- zbiranje podatkov z analiziranjem geoprostorskega slikovnega materiala – GEOINT (ang. *geospatial intelligence*);
- zbiranje podatkov s človeškimi viri (informatorji, tajni sodelavci oziroma agenti, dvojni agenti) – HUMINT (ang. *human intelligence*);
- zbiranje podatkov iz slikovnih virov – IMINT (ang. *imagery intelligence*);
- zbiranje podatkov s tehničnimi meritvami virov – MASINT (ang. *measurement and signature intelligence*), to vključuje npr. tudi pridobivanje podatkov z radarji ali RADINT (ang. *radar intelligence*);
- obveščevalna dejavnost na področju zdravstva, zbiranje podatkov o zdravju ljudi in živali – MEDINT (ang. *medical intelligence*);
- zbiranje podatkov iz javnih in odprtih virov – OSINT (ang. *open source intelligence*);
- zbiranje podatkov s prestrezanjem signalov oziroma iz elektromagnetnih emisij – SIGINT (ang. *signals intelligence*), to vključuje pridobivanje podatkov iz komunikacije, COMINT (ang. *communications intelligence*), in zbiranje podatkov iz elektronskih signalov v komunikaciji, ELINT (ang. *electronic intelligence*);
- zbiranje podatkov s preučevanjem tehničnih sredstev – TECHINT (ang. *technical intelligence*);

ter nekatere druge vrste zbiranja podatkov, ki jih nismo posebej predstavili. V okviru zbiranja podatkov je potrebno omeniti tudi pridobivanje podatkov s pomočjo mednarodnega sodelovanja, tj. s sodelovanjem z drugimi partnerskimi institucijami

(službami, agencijami, ministrstvi, mednarodnimi organizacijami ipd.). Večina, tj. okoli 80 % (Krunić, 1996 v Podbregar, 2008) oziroma 90 % (Dedijer, 2005) podatkov naj bi bilo pridobljenih z metodami OSINT, preostali delež pa je pridobljen z uporabo drugih obveščevalnih metod. Ker je večina informacij pridobljena iz odprtih virov, obstaja verjetnost, da bodo med viri tudi dezinformacije, s katerimi želijo tuje obveščevalne službe zavajati (Hribar et al., 2014). Zbrani podatki gredo nato skozi analitični postopek. Analitično delo oziroma analitiko opravljajo analitiki, ki imajo potrebna analitična znanja, znajo hitro uporabljati programsko opremo, so sposobni timskega dela, hkrati pa so zanesljivo sposobni prepoznati naročnikove zahteve v realnem času (Podbregar & Ivanuša, 2010). Johnston (2005, str. 4) definira analitični postopek kot aplikacijo posamičnih in kolektivnih kognitivnih metod obtežitve podatkov in testiranj hipotez v tajnem sociološko-kulturnem kontekstu, Podbregar (2008, str. 60) pa kot »proces urejanja, analiziranja in vrednotenja grobih oziroma neobdelanih obveščevalnih podatkov (''raw data'') in informacij iz različnih virov (''all source'') in njihovega preoblikovanja v obveščevalne informacije (''intelligence'') kot končne produkte (''final intelligence'') oziroma rezultate obveščevalne dejavnosti: opozorilna in situacijska poročila, analize, ocene, prognoze, brifinge in podobno.« Analitiki se morajo zavedati pasti pri razmišljanju (Dvoršek & Podbregar, 2012), predvsem hevristik in predsodkov (glej npr. Tversky & Kahneman, 1974), ter namernega zavajanja s plasiranimi dezinformacijami, zato morajo biti pri svojem delu previdni in natančni. Zbrani podatki so najprej ocenjeni in ovrednoteni glede na njihovo pomembnost, uporabnost, ustreznost in preverjenost oziroma verodostojnost. Z vrednotenjem analitiki preko povratne informacije sporočijo operativcem, ali so zbrali prave podatke, oziroma kaj bi še potrebovali (Podbregar & Ivanuša, 2010). Tako kot pravi tudi Podbregar (2008), so zbrani podatki nato procesirani (npr. prevajanje, interpretacija fotografij, dešifriranje) (Taylor, 2007), združeni in urejeni v ustreznejši obliko. Analitiki nato poiščejo morebitne povezave, vzorce, rešitve, pomanjkljivosti oziroma odstopanja v podatkih ter s tem poiščejo njihovo sporočilnost. Analitika je zato ključni del ne le obveščevalne, temveč tudi protiobveščevalne in varnostne dejavnosti. Vpeta je v vse korake obveščevalnega kroga (Podbregar & Ivanuša, 2010), ključni del pa je tisti, v katerem se podatki spremenijo v obveščevalno informacijo (Dvoršek & Podbregar, 2012).

Proces zbiranja, vrednotenja in analiziranja podatkov je značilen za vse tri prej omenjene dejavnosti, njihov končni produkt pa je informacija ali vplivno sporočilo, ki je razumljivo, sprejeto in povzroči akcijo (Podbregar, Mulej, Pečan, Podbregar & Ivanuša, 2010). Drugi dve opredelitvi informacije bolj poudarjata njeno vlogo v obveščevalno-varnostni dejavnosti (ibidem, str. 10):

- »Informacija je lahko (tudi, vendar ne izključno!) proizvod zavednega v imenu znanja, interpretacije podatkov, učenja ni drugih izkustev, in-determinizma in determinizma.
- […] Informacija je lahko predmet individualnega in subjektivnega razumevanja razpoložljivih podatkov ter sporočil, kar pa je odvisno od izbranega vidika obravnave.«

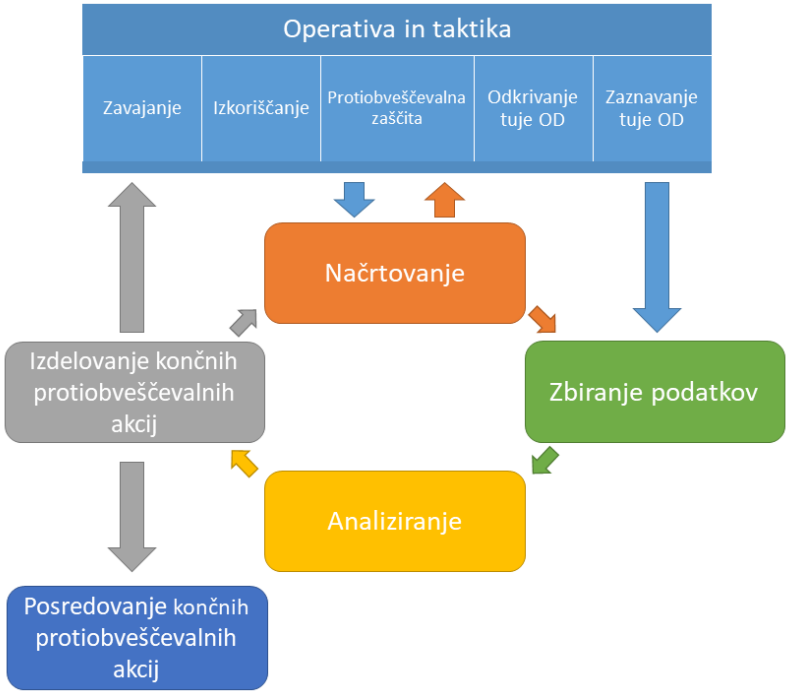
Obveščevalno-varnostne informacije v doktorski disertaciji pojmujemo kot informacije, ki so potrebne za zagotavljanje nacionalne varnosti. Nacionalna varnost lahko opredelimo kot »povezave političnih, gospodarskih, vojaških, ideoloških, pravnih, socialnih in drugih notranjih in zunanjih družbenih dejavnikov, preko katerih si države prizadevajo, da bi z različnimi sredstvi zagotovile sprejemljive razmere za ohranjanje suverenosti, ozemeljske celovitosti, za fizični obstoj in razvoj prebivalstva, ohranjanje politične neodvisnosti ter možnosti za enakopraven, uravnotežen in hiter razvoj.« (Šifrer, 2008, str. 155) Podatki, ki jih zbirajo obveščevalno-varnostne službe, so potrebni za varovanje ter uresničevanje tudi drugih nacionalnih interesov (ekonomski, gospodarski, politični, kulturni idr.). Nacionalna varnost oziroma nacionalni varnostni interesi pa so po mnenju Prezelja (2002) del nacionalnih interesov. Pridobljeni in kasneje analizirani podatki so oblikovani v informacije, namenjene odločanju na najvišji ravni. To namreč izhaja iz predpostavke, da so vlade racionalni akterji, ki se odločajo na podlagi razpoložljivih dokazov (Robinson, 2009, str. 705), teh pa vlade nimajo vedno na voljo, zato jih je potrebno pridobiti. Bistvo obveščevalno-varnostnih informacij je zaščita njihovih uporabnikov, naročnikov in nekaterih aktivnosti pred nepredvidenimi strateškimi presenečenji, obenem pa informacije služijo za vzdrževanje stabilnosti političnega sistema z varovanjem tajnih podatkov pred nepooblaščenimi osebami (Lowenthal, 2009). Johnston (2005, str. 4) obravnava obveščevalno-varnostno dejavnost kot »tajn[o] dejavnost države ali skupine, z namenom razumevanja ali vplivanja na tuje ali matične entitete,« predvsem z vidika uresničevanja interesov v mednarodnih

zadevah, kot pravi Treverton (2008). Tajnost oziroma načelo tajnosti je »legitimno sredstvo, s pomočjo katerega se ščitijo vitalni interesi države« (Brezovšek & Črnčec, 2004, str. 506) in je namenjeno »varovanju, obrambi in zaščiti obstoja države, njene ustavne ureditve ali posebnim interesom pri varovanju človekovih pravic.« (Anžič, 2000, str. 854) Tajnost je potrebna zaradi prikrivanja nacionalnih interesov in namer pred nepoklicanimi osebami, da bi država lahko zagotovila (nemoteno) uresničevanje svojih interesov.

Protiobveščevalno dejavnost, drugo sestavino obveščevalno-varnostne dejavnosti, se populistično »najpogosteje enači s protivohunstvom, v angleško govorečih državah pa tudi s protiteroristično dejavnostjo. Tudi razumevanje protiobveščevalne dejavnosti v akademski in strokovni sferi ni enotno, saj je ponekod definirana kot samostojna disciplina znotraj obveščevalnega procesa, drugod kot podporna dejavnost obveščevalni dejavnosti, spet drugod pa kot del varnostne dejavnosti. Ravno tako prihaja do razlik pri uporabi koncepta protiobveščevalne dejavnosti v praksi, kar je razvidno tudi iz delokroga služb po svetu in pa pooblastil, ki jih nekatere službe imajo, npr. pooblastilo za pridržanje osebe, za izvajanje posebnih ukrepov v domovini brez sodne odredbe, pooblastilo za aretacijo (primeri takšnih služb: FBI, FSB, BIA, Shin Bet), druge pa ne (npr. SOVA, BvF, MI5, ASIO, CSIS).« (Ivanuša et al., 2016, str. 13) V literaturi je mogoče zaslediti tudi izraz *kontraobveščevalna dejavnost*. O protiobveščevalni dejavnosti kot samostojni dejavnosti, ki se razlikuje od varnostne in obveščevalne dejavnosti, in kot področju znanstvenega raziskovanja je (še vedno pre)malo napisanega (Ivanuša et al., 2016), zato so tudi definicije v domači in tuji literaturi med seboj različne. Protiobveščevalna dejavnost zagotavlja varnost pred tujo obveščevalno dejavnostjo tako, da jo tajno zaznava, odkriva in preprečuje, izkorišča ali zavaja ter ščiti nacionalne subjekte in interese pred njenim posrednim ali neposrednim vplivom (ibidem). S tem zagotavlja varnost pred »tujimi tajnimi sodelavci in operativci, varnost pred zavajanjem, varnost pred izdajo tajnih podatkov, varnost pred tujimi škodljivimi interesi ipd. Kadar ta varnost ni zagotovljena ali kadar je pomanjkljiva, je posredno ali neposredno ogroženo delovanje celotne obveščevalno-varnostne dejavnosti ali celo sistema nacionalne varnosti.« (ibidem, str. 2) Proces protiobveščevalne dejavnosti je podoben procesu obveščevalne dejavnosti, le da je zaradi specifik nekoliko razširjen (na sliki 2.1 so predstavljeni le ključni

štirje koraki). Tudi metode protiobveščevalnega delovanja so podobne metodam obveščevalnega delovanja (Ivanuša et al., 2016), le da se jih izvaja za namene in v okviru protiobveščevalnega delovanja.

Slika 2.1: Protiobveščevalni proces



Vir: Ivanuša et al., 2016, str. 23

Tretja dejavnost, podobna obveščevalni in protiobveščevalni dejavnosti, je varnostna dejavnost in zajema »preprečevanje, preiskovanje in odpravljanje določenih oblik ogrožanja varnosti neke dobrine, v tem primeru države.« (Purg, 1995, str. 34; Purg, 2002, str. 18) Gre za dejavnost, ki je podobna protiobveščevalni, vendar pa deluje »z metodami in sredstvi, ki se razlikujejo od načina, metod in sredstev obveščevalne dejavnosti,« (ibidem, str. 35) čeprav temu ni vedno tako. Varnostna dejavnost lahko poleg nekaterih obveščevalnih metod vključuje tudi policijske metode in pooblastila, vendar se praksa po državah razlikuje. Od tod tudi zmotno razumevanje, da sta klasična policijska dejavnost in varnostna dejavnost enaki. Varnostna dejavnost deluje »proti organiziranemu kriminalu, terorizmu, nedovoljeni trgovini in proizvodnji mamil, orožja in sredstev za množično uničevanje. Namenjena je tudi za odkrivanje, preprečevanje in varovanje pred raznimi oblikami političnega ekstremizma, radikalizma, katerega cilj je

nasilno rušenje ustavne ureditve. Izvajajo jo obveščevalnovarnostne in varnostne službe, razlike se kažejo le pri pooblastilih.« (Šaponja, 1999, str. 59) Od klasičnega policijskega in kriminalističnega preiskovanja se razlikuje tudi po tem, da je odločitev o prijetju osumljencev odvisna od potrebne hitrosti hitrega odzivanja (in s tem preprečevanja potencialnih kaznivih dejanj) in odločitve, da se osumljence pusti delovati dalje, z namenom zbiranja dodatnih podatkov (Treverton, 2008). Takšno ravnanje je nujno za potrebe zagotavljanja nacionalne varnosti in ne toliko za interes poteka predkazenskega postopka, kot je značilno za klasično policijsko dejavnost.

Obveščevalna, protiobveščevalna in varnostna dejavnost so si torej podobne, med seboj so povezane, soodvisne in nujno potrebne za zagotavljanje nacionalne varnosti, hkrati pa predstavljajo tri različne ciljno usmerjene načine delovanja.

2.1 Obveščevalno-varnostni sistem

Obveščevalno-varnostni sistem je podsistem sistema nacionalne varnosti (Šaponja, 1999, str. 57). Slednjega sestavljajo varnostna politika, varnostna struktura in varnostno samoorganiziranje civilne družbe (Grizold, 1992, 2000 v Črnčec, 2009, str. 27-28). »Obveščevalnovarnostni sistem je vsota vseh obveščevalnih in protiobveščevalnih služb ter služb za varstvo ustavne ureditve.« (Šaponja, 1999, str. 57) Warner (2009, str. 15-16) pojmuje obveščevalno-varnostni sistem kot kolektiv organov, sredstev, nadzora in nalog, dodeljenih vpletenim, ki so uradno združeni z namenom izvajanja dolžnosti s področja obveščevalno-varnostne dejavnosti. Zaradi naloge pridobivanja podatkov in oblikovanja obveščevalnih informacij ga opredeljuje tudi kot sistem, ki odločevalcem zagotavlja informacije (ibidem, str. 23). Obveščevalno-varnostne službe so »organizirane in oblikovane v obveščevalno-varnostni sistem ali skupnost, ki obsega predvsem obliko in način organiziranja, usklajevanje, usmerjanje in nadzorovanje obveščevalnih služb.« (Črnčec, 2009, str. 39) Za obveščevalno-varnostni sistem se zato uporablja tudi izraz *obveščevalno-varnostna skupnost*, v angleško govorečih državah pa *obveščevalna skupnost* (ang. *intelligence community*). V ožjem smislu obveščevalna skupnost zajema »nacionalni obveščevalni sistem oziroma s predpisi določeno področje dela in medsebojnih odnosov vseh obveščevalnih organizacij in drugih ustanov države

(profesionalne državne in paradržavne institucije), ki zbirajo ocenjujejo in posredujejo obveščevalne podatke ter informacije, opravljajo pa tudi druge naloge.« (Đorđević, 1978 v Purg, 2002, str. 19) Ob tem je potrebno poudariti, da je obveščevalna skupnost lahko razumljena kot sistem obveščevalnih služb (brez protiobveščevalnih in varnostnih služb, tj. obveščevalna skupnost v ožjem smislu) (ibidem), ali pa kot sistem obveščevalno-varnostnih služb (obveščevalna skupnost v širšem smislu), npr. »obveščevalno-varnostno skupnost tvorijo državne ustanove, ki z namenom zaščite ustavne ureditve in temeljnih človekovih pravic in svoboščin izvajajo oz. sodelujejo pri izvajanju obveščevalne, protiobveščevalne ali varnostne dejavnosti, bodisi v funkciji usmerjanja, nadzora ali koordinacije.« (Črnčec, 2003, str. 2) »Značilnost vseh obveščevalno(-varnostnih) skupnosti – sistemov je, da imajo ustrezno vodstveno strukturo, ki je glede na tip političnega sistema skoncentrirana pri predsedniku države ali vlade in je zadolžena na ustrezen nadzor, usmerjanje in usklajevanje« (Črnčec, 2009, str. 40), njegove sestavine pa povezuje skupno usmerjevalno in koordinacijsko telo (Šaponja, 1999, str. 28). Cilj obveščevalno-varnostnega sistema je zaščita temeljnih in splošnih družbenih vrednot (Đorđević, 1978 v Purg, 2002, str. 19). Te so pomembne za delovanje sistema nacionalne varnosti, saj posameznika lahko motivirajo in usmerijo v ustvarjalno dejavnost ali pa ga pri tem zavirajo, zaradi česar lahko postane odklonilen do družbe in posledično tudi destruktiven (Anžič, 1997). Tudi vrednote predstavljajo pomemben dejavnik sistema nacionalne varnosti, saj »na eni strani povezuje subjekte ter na drugi strani predstavlja temeljna načela, ki izhajajo iz družbe in političnega sistema, za podporo katerega je namenjen.« (Črnčec, 2009, str. 29-30)

Šaponja (1999, str. 55) deli obveščevalno-varnostne sisteme na centralizirane, decentralizirane in integrirane:

- *centralizirani obveščevalno-varnostni sistemi*: sestavljeni so iz enotne obveščevalne službe, ki opravlja obveščevalne naloge za vse državne organe, in enotne protiobveščevalna oziroma varnostna služba, ki izvaja naloge za potrebe različnih resorjev;
- *decentralizirani obveščevalno-varnostni sistemi*: obveščevalne, protiobveščevalne in varnostne službe so organizirane po različnih resorjih, vendar so med seboj povezane;

- *integrirani obveščevalno-varnostni sistemi*: gre za decentralizirane sisteme, ki imajo eno centralizirano službo za obveščevalno ali protiobveščevalno oziroma varnostno službo ter več ostalih služb. Njihovo delo koordinirajo organi pri svetih za nacionalno varnost oziroma drugih podobnih organih.

Na oblikovanje in delovanje obveščevalno-varnostnega sistema vplivajo trije dejavniki, ki se odražajo v strukturi in delovanju obveščevalno-varnostnega sistema. Prvi dejavnik je strategija oblasti, s katero je določena politika (oziroma cilji), s tem pa oblast preko strategije narekuje tudi tarče in tempo obveščevalno-varnostnih služb. Drugi dejavnik je režim, od katerega je odvisna strategija, preko nje pa režim posredno (in neposredno) vpliva na obveščevalno-varnostni sistem. Na režim vpliva struktura oziroma tip vladavine, oblika vlade, vrsta nadzora, struktura resorjev in notranji izzivi. Režim vpliva tudi na tretji dejavnik: tehnologijo. Z njo si obveščevalno-varnostna skupnost pomaga določati cilje in objekte, obenem pa predstavlja sredstva, ki jih obveščevalno-varnostne službe uporabljajo pri svojem delu. V tem kontekstu tehnologijo sestavljajo informacije in informacijska tehnologija, tip produkcije (kapitalistični ali kolektivistični), razpoložljivi viri (naravni viri, človeški viri, izobrazba idr.) in pa družbene formacije. S tehnologijo oblast dosega svoje cilje v skladu s strategijo (Warner, 2009).

Spremembe strategije, režima ali tehnologije se lahko odražajo kot spremembe naslednjih značilnosti obveščevalno-varnostnega sistema: struktura in podrejenost agencij, proračun, fizična velikost in tloris, tarče in zahteve, tehnološke zmožnosti, narava in obseg povezav s tujimi službami, dostop do uporabnikov in kakovost odnosa, kakovost in vizija vodstva, profesionalnost delovne sile, menedžerske veščine, kakovost interne komunikacije in konzultacij, kakovost varnostnih postopkov in opreme, prisotnost ali odsotnost korupcije ter sankcije za neprimerno vedênje (Warner, 2009, str. 35). Na obveščevalno-varnostni sistem vplivajo tudi velikost države, stopnja ogroženosti in razpoložljivi (finančni) viri (Podbregar, 2008, str. 27). Vse to tudi nakazuje, da je obveščevalno-varnostni (pod)sistem dinamičen, saj se nenehno spreminja in razvija tako v organizacijskem kot tudi v vsebinskem smislu (Purg, 2002).

Pregled državnih obveščevalno-varnostnih sistemov po vsem svetu kaže, da so ti različno strukturirani. Čeprav vsi opravljajo enake funkcije in naloge, med njimi obstajajo razlike v številu in vrstah subjektov (agencije, službe, uradi, direktorati, ministrstva, zveze ipd.) ter s tem povezane razlike v številu osebja, pooblastilih, pristojnostih in nalogah, dodeljenih finančnih sredstvih, hierarhiji idr. Primerjava dostopne literature, ki je zaradi velike količine ne navajamo posebej, in različnih obveščevalno-varnostnih sistemov po svetu kaže, da je splošno razumevanje obveščevalno-varnostnih sistemov takšno: *obveščevalno-varnostni sistem je struktura vseh državnih in nedržavnih organizacij oziroma služb, ki izvajajo obveščevalno, protiobveščevalno ali varnostno dejavnost ter jih usmerja, koordinira in nadzira država skupaj z drugimi organi(zacijami)*. Takšno razumevanje se ujema z opredelitvijo *sistema* avtorjev Mulej et al. (2008, str. 39), po kateri je sistem »urejena množica, torej je sestavljen iz množice sestavin in množice povezav med njimi, s tem pomeni celoto.« Obveščevalno-varnostni sistemi naj bi bili v teoriji enako zasnovani in naj bi delovali na enak ali podoben način. Ocenjujemo, da preveč ohlapna definicija obveščevalno-varnostnega sistema dopušča, da v praksi prihaja do razlik med obveščevalno-varnostnimi sistemi. Ugotovili smo, da le redki strokovni in znanstveni prispevki (glej npr. Frankovič & Preston, 1993) podrobneje obravnavajo in opredeljujejo obveščevalno-varnostni sistem s sistemskega vidika. Zaradi odsotnost ustrezne obravnave obveščevalno-varnostnega sistema z vidika izbrane teorije sistemov smo obveščevalno-varnostni sistem zato opredelili sami, pri tem pa smo se odločili za uporabo Teorije viabilnih sistemov (TVS) avtorja Stafforda Beera (1984). Izbiro TVS utemeljujemo s pojasnilom, da je TVS zanesljivo orodje za vzpostavitev viabilne strukture organizacije (Schwaninger & Pérez Ríos, 2008) in s tem za izboljšanje njene vitalnosti, odpornosti in razvoja (Schwaninger & Scheef, 2016). Obveščevalno-varnostni sistem ne sme biti tog, odporen mora biti na vse vrste groženj, nestabilnosti in negotovosti, hkrati pa se mora nenehno posodabljati in razvijati skupaj z družbo, tehnologijo, varnostnim okoljem idr. Obveščevalno-varnostni sistem, ki ni viabilen, na prvi pogled nima večjih težav, zaradi katerih bi bil lahko podvržen hitrejši entropiji ali bil eksistencialno ogrožen. Pri obveščevalno-varnostnih sistemih se znaki neviabilnosti in entropije kažejo kot slabše sodelovanje in slabša komunikacija subjektov, slaba in nepravočasna izmenjava podatkov med subjekti znotraj istega obveščevalno-varnostnega sistema, podvajanje nalog, neustrezne relacije, zapletenost organizacije,

togost, slabo odzivanje na grožnje in dogodke, tveganja in nevarnosti, slaba koordinacija, počasno usklajevanje idr. Ti znaki morda ne kažejo na propad služb/-e, vendar vsekakor vodijo k temu, saj dolgoročno zmanjšujejo učinkovitost, ker sistem ni več kos nalogam in tako postopoma izgublja svojo identiteto. To posledično in posredno vodi tudi v izgubo zaupanja državljanov v matične obveščevalno-varnostne službe.

Zato ugotavljamo, da je struktura pomemben dejavnik obveščevalno-varnostnega sistema, saj vpliva tudi na njegovo delovanje. Vendar ta ugotovitev ni novo odkritje. Uporabljamo jo kot dokaz, da ni vseeno, kako si raziskovalci, politiki, akademiki in drugi predstavljajo obveščevalno-varnostni sistem kot *sistem*. Učinkovit in viabilen obveščevalno-varnostni sistem je mogoče doseči oziroma vzpostaviti le, če ga oblikujemo v skladu s katero od izbranih teorij sistemov. Zaradi ugotovitve, da je viabilnost obveščevalno-varnostnih sistemov ključnega pomena za celovito zaupanje državljanov v matične obveščevalno-varnostne službe, smo viabilni obveščevalno-varnostni sistem najprej izoblikovali, nato pa ga uporabili pri izgradnji modela celovitega zaupanja državljanov v matične obveščevalno-varnostne službe. Postopek izgradnje viabilnega obveščevalnega sistema je predstavljen v enem od kasnejših poglavij doktorske disertacije.

2.2 Obveščevalno-varnostne službe

»Vohuni so prisotni že stoletja, obveščevalne službe pa so nove.«
(Knightley, 1986, str. 5)

Uvodni citat pojasnjuje, da je vohunstvo oziroma obveščevalna dejavnost prisotna v družbenem življenju že zelo dolgo časa – nekateri (med njimi tudi uvodoma citirani Knightley) jo celo omenjajo kot drugo najstarejšo obrt. O prvem pojavu institucionalizirane obveščevalno-varnostni dejavnosti obstaja več mnenj in teorij. Nekateri avtorji (npr. Trigger, Kemp, O'Connor & Lloyd, 2001) menijo, da so obveščevalno-varnostne organizacije v institucionalni obliki obstajale že v času starega Egipta. Drugi menijo, da so obstajale že v času indijskega vladarja Chandragupte Maurya (npr. Mookerji, 1988), tretji pa, da že v času antičnega Rima (npr. Sinnigen, 1962), itd. Za

začetek sodobnih obveščevalno-varnostnih službah naj bi šteli 15. oziroma 16. stoletje, ko sta v Angliji nastali prva notranja policija in prva obveščevalna služba, nastanek sodobnejših oblik institucionaliziranih obveščevalno-varnostnih struktur (služb) pa postavljamo v konec 18. stoletja ter 19. in 20. stoletje (Purg, 2002). Močnejše sodobne evropske obveščevalno-varnostne službe so pojavile v prvih treh desetletjih 20. stoletja, ameriške pa šele po koncu 2. svetovne vojne (Taylor, 2007).

V doktorski disertaciji uporabljamo izraz *službe*, s katerim zajemamo vse različne oblike organizacij in organizacijskih enot (npr. službe, agencije, uradi, direktorati, sektorji, ministrstva, oddelki, odseki), ki izvajajo obveščevalno-varnostno dejavnost. Vendar ob tem ponovno pojasnjujemo, da z izrazom *obveščevalno-varnostne službe* v doktorski disertaciji pojmujemo »obveščevalne, protiobveščevalne in varnostne službe ter njihove kombinacije« (Ivanuša et al., 2016, str. 1) in hkrati »organizacije, ki za potrebe države, posebej njenega političnega in vojaškega vodstva, z namenom uresničitve političnih ciljev in zunanjepolitičnih interesov države zbirajo in analizirajo podatke o možnostih, namenih in dejavnostih tujih sil in drugih obveščevalno in varnostno zanimivih subjektih ter varujejo pred njihovimi obveščevalnimi in drugimi dejavnostmi, izvzemivši [sic] odkrito oboroženo agresijo, ki lahko ogrozi nacionalno varnost.« (Žunec & Domišljanović, 2000 v Črnčec, 2009, str. 38) Zasebnih in drugih nedržavnih obveščevalno-varnostnih služb, kot jih npr. omenja Purg (2002), v doktorski disertacij torej ne obravnavamo.

Obveščevalno-varnostne službe so »pomemben del nacionalnovarnostnega in političnega delovanja, in sicer tako v pozitivnem kot negativnem smislu.« (Purg, 2002, str. 7) Njihovo pomembno vlogo prepoznavata tudi Anžič & Golobinek (2003), ki pravita, da so te službe najbolj aktivni in hkrati najbolj odgovorni nosilci varnostnih prizadevanj demokratične družbe. Glede na območje delovanja se službe delijo na več segmentov. Ehrman (2009, str. 7-8) jih deli na:

- *eksterne* ali *zunanje službe*, ki se osredotočajo na tarče in operacije zunaj matične države (npr. britanska MI6 in GCHQ, ameriški CIA in NSA, nemška BND, ruska SVR, op. G. H.);

- *interne* ali *notranje službe* (zanje se uporablja tudi angleški izraz *domače*: *domestic service*, op. G. H.), ki znotraj matične države delujejo proti tarčam, ki predstavljajo nevarnost državi ali entiteti (npr. ameriški FBI, britanski MI5, italijanska AISI, madžarska AH, op. G. H.);
- *unitarne službe*, ki združujejo funkcije eksterne in interne službe v eno službo. Te so obstajale predvsem v totalitarnih režimih, obstajajo pa tudi še danes (npr. kanadska CSIS, nekdanja sovjetska KGB, kitajsko ministrstvo MSS, srbska BIA, v Sloveniji pa Slovenska obveščevalno-varnostna agencija (v nadaljevanju: Sova) in Obveščevalno varnostna služba Ministrstva za obrambo (v nadaljevanju: OVS), op. G. H.).

Purg (2002, str. 17) jih deli glede na različne kriterije, in sicer glede na:

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

Born & Leigh (2007) prepoznavata dva vzorca organizacije služb: enotne službe, ki izvajajo notranjo in zunanjo obveščevalno dejavnost, ter različne službe, ki posebej izvajajo notranjo ali zunanjo obveščevalno dejavnost, njihove teritorialne pristojnosti pa se prekrivajo. Šaponja (1999) jih deli na strateške in taktične ter centralizirane in decentralizirane, Taylor (2007, str. 251) pa na:

- nadzorne pisarne ali skupine pisarn, ki so zadolžene za koordinacijo celotne obveščevalne skupnosti;
- službe, zadolžene za zbiranje, analiziranje in oblikovanje obveščevalnih informacij iz podatkov iz tujih držav ter drugih zunanjih virov;
- službe, zadolžene za zbiranje, analiziranje in oblikovanje obveščevalnih informacij o *domačih* oziroma notranjih grožnjah (ang. *domestic threats*) državi;

- službe, zadolžene za zbiranje in distribucijo SIGINT;
- službe, ki delajo po navodilih vojaškega oddelka ali oddelkov vlade za pridobivanje obveščevalnih informacij, ki jih potrebujejo vojaške sile;
- službe, ki se ukvarjajo s protiterorizmom, razvojem, operacijo in izkoriščanjem satelitskih fotografiranj, protiobveščevalno dejavnostjo, varovanjem državne meje in drugimi posebnimi funkcijami.

Večini predstavljenih delitev je skupna klasifikacija služb na obveščevalne, protiobveščevalne in varnostne službe, službe zadolžene za notranjo varnost ali domovinsko varnost in službe zadolžene za zunanjo varnost. Obveščevalne službe so zadolžene za »zbiranje, analiziranje in ocenjevanje obveščevalnih podatkov in spoznanj o drugih državah, njihovem vojaškem in ekonomskem potencialu, političnem stanju in namerah ter znanstvenih dognanjih. […] [P]oleg posebnih metod in sredstev dela uporablja tudi številne legalne možnosti za pridobivanje podatkov. Cilji in metode dela obveščevalne službe so praviloma determinirane s političnimi cilji in načini vodenja vladne politike. Poleg zbiranja podatkov ščiti lastne interese, zaupne podatke in dokumente pred nasprotnikom ter opravlja še druge naloge, ki so pomembne pri realizaciji določenih (tudi političnih) ciljev, pri čemer uporablja specifične (posebne) metode in sredstva. Ponekod opravlja tudi 'umazane posle', katerih cilj je, da s pritiskom (vojaškim, ekonomskim, političnim) vplivajo na politiko določene države.« (Purg, 1995, str. 32-33) Za t.i. umazane posle se uporablja tudi izraz *neobveščevalna dejavnost*, ki zajema druge naloge, neobveščevalne naloge za uresničevanje nacionalnih interesov s psihološkim in subverzivnim delovanjem ter s specialnimi operacijami (Podbregar, 2008). Notranje obveščevalne službe (ang. *domestic intelligence service*) so v slovenski literaturi (npr. Purg, 1995, 2002) enačene z varnostnimi službami, ki so namenjene predvsem notranji varnosti pred notranjim sovražnikom. Notranje obveščevalne službe delujejo tudi na področju zaznavanja in preprečevanja vohunstva oziroma tajnega sodelovanja matičnih državljanov s tujimi službami. Ko govorimo o notranjih obveščevalnih službah, je potrebno poudariti, da se kljub povezovanju protiobveščevalne in varnostne dejavnosti protiobveščevalne službe ločijo od varnostnih služb. V teoriji naj bi bile protiobveščevalne službe usmerjene le na izvajanje protiobveščevalne dejavnosti, varnostne službe pa izključno na izvajanje varnostne

dejavnosti. V praksi je seveda drugače, saj po svetu obstaja več varnostnih služb, ki izvajajo kombinacijo varnostne in protiobveščevalne dejavnost (npr. ameriški FBI, britanska MI5, ruska FSB, francoski DGSI; op. G. H.), npr. delo na področju ekstremizma, protivohunstva, terorizma, posebnih oblik organiziranega kriminala, rušenja državne/ustavne ureditve (Šaponja, 1999). Takšne službe so pogosto organizirane kot službe za varstvo ustavne ureditve (za več o tem glej Šaponja, 1999, str. 46-48). Znova poudarjamo (glej Hribar, 2016), da protiobveščevalna dejavnost ni del varnostne dejavnosti, čeprav sta v praksi pogosto izvajani v okviru ene organizacije. Službe, ki opravljajo varnostno dejavnost, delujejo proti npr. terorizmu, političnemu, rasnemu in verskemu ekstremizmu ter izvajajo različne naloge za zaznavanje aktivnosti takšnih skupin in posameznikov, preprečujejo pa tudi izvrševanje subverzivnih, protiustavnih ali drugačnih protidržavnih dejavnosti (glej npr. Purg, 2002). Varnostne službe pri svojem delu zato potrebujejo policijska pooblastila (npr. legitimacija, pripor, aretacija, hišna preiskava), kot jih imajo policijske organizacije, medtem ko protiobveščevalne službe teh pooblastil nimajo. Tako kot protiobveščevalne tudi obveščevalne službe navadno nimajo represivne funkcije (Šifrer, 2008). Varnostne službe pri svojem delu uporabljajo obveščevalno dejavnost za izvajanje varnostne dejavnosti v državi, zato so pogosto del policijskih organizacij ali ministrstev, pristojnih za notranje zadeve ali pravosodje (Šaponja, 1999).

Obveščevalno-varnostne službe morajo zaradi izvrševanja nalog tudi posegati v človekove pravice in svoboščine. Na drugi strani pa so službe te pravice in svoboščine tudi dolžne spoštovati tako v domovini kot v tujini (Raab, 2017), vendar je spoštovanje pravic v tujini »sekundarnega pomena«, saj je delo služb podrejeno zagotavljanju nacionalne varnosti in interesov – ne glede na to, ali bodo pravice kršene ali ne. Pravice na področju posameznikove zasebnosti določa Splošna deklaracija o človekovih pravicah (Organizacija združenih narodov, 1948, 12. člen): »Nikogar se ne sme nadlegovati s samovoljnim vmešavanjem v njegovo zasebno življenje, v njegovo družino, v njegovo stanovanje ali njegovo dopisovanje in tudi ne z napadi na njegovo čast in ugled. Vsakdo ima pravico do zakonskega varstva pred takšnim vmešavanjem ali takšnimi napadi.« V Evropi človekove pravice ureja tudi Evropska konvencija o varstvu človekovih pravic in temeljnih svoboščin (Svet Evrope, 1950; v nadaljevanju: EKČP), ki v 8. členu določa:

»1. Vsakdo ima pravico do spoštovanja njegovega zasebnega in družinskega življenja, doma in dopisovanja. 2. Javna oblast se ne sme vmešavati v izvrševanje te pravice, razen, če je to določeno z zakonom in nujno v demokratični družbi zaradi državne varnosti, javne varnosti ali ekonomske blaginje države, zato, da se prepreči nered ali kaznivo dejanje, da se zavaruje zdravje ali morala, ali da se zavarujejo pravice in svoboščine drugih ljudi.« To sta dva ključna dokumenta, ki v Evropi zagotavljata varovanje človekovih pravic pred nepooblaščenim posegom. Torej je poseganje v človekove pravice v evropskem prostoru dopustno le, če so izpolnjeni pogoji iz 2. točke EKČP. Ker obveščevalno-varnostne službe delujejo za potrebe nacionalne varnosti in (tudi ekonomske) blaginje države, je poseganje v človekove pravice nujno. Anžič (1996, str. 205) hudomušno pravi: »Brez poseganja v človekove pravice varnostne in obveščevalne službe ne bi bile v funkciji institucionaliziranega državnega nadzorstva, temveč bi bile kvečjemu društva ali klubi ljubiteljev lepega vedenja.« Pomembno vlogo ima pri tem tudi tajnost. Obveščevalno-varnostne službe so od nekdaj delovale v tajnosti (Born & Leigh, 2007), zato od njih ni mogoče pričakovati odprtosti za širšo družbo. Z našega vidika obravnavanja je tajnost pomemben dejavnik, saj, kot pravita Lester & Jackson (2009), vpliva na javno zaznavanje in mnenje o službah ter na (zaznavanje) transparentnost(i) njihovega delovanja. Tajnost pa žal tudi omogoča krinko za etično nesprejemljive prakse delovanja ter zlorabo služb za politične namene (Born & Leigh, 2007). Obveščevalno-varnostne službe so tesno povezane s politiko, ker izhajajo njihove temeljne funkcije iz političnega sistema, ta pa »določa vrsto, obseg in ofenzivnost nalog, ki naj bi jih službe izvajale. Od tega sta odvisna tudi velikost in ustroj obveščevalno varnostnega sistema.« (Šifrer, 2008, str. 153) Svet Evrope (2009) je z namenom preprečevanja zlorabe služb za zasebne ali politične namene oblasti sprejel stališče/smernice, naj službe ne bodo »politizirane«. Kljub temu pa je politizacijo obveščevalno-varnostnih služb težko popolnoma preprečiti, saj so glavni uporabniki njihovih storitev ravno politiki (Fitsanakis & Hodges, 2013).

Dejavnika, ki jima je potrebno nameniti več pozornosti, sta vloga in uporabnost obveščevalno-varnostnih informacij v obliki dokazov, ki jih je mogoče uporabiti pred sodiščem. To je odvisno od pooblastil obveščevalno-varnostnih služb in pravne ureditve države, predvsem pa od ureditve nacionalnega pravosodnega sistema. Parlamentarna

skupščina Sveta Evrope (2005, str. 16) je ugotovila: »Nekatere države so nazadovale na področju osnovnih človekovih pravic, predvsem pri pravici do poštenega sojenja, saj je bilo na podlagi zakonodaje mogoče osebo zapreti tudi na podlagi dokazov, ki so jih zbrale tajne službe […].« Navedeno dokazuje pomembnost ločevanja obveščevalno-varnostnih služb s pooblastili od tistih brez pooblastil, predvsem pa izpostavlja potrebo po pravni ureditvi vprašanja obveščevalno-varnostnih informacij kot dokazov, ki jih je mogoče uporabiti pred sodiščem (za več o tem glej v npr. Žirovnik, 2016). V zvezi s tem je Parlamentarna skupščina Sveta Evrope (Parlamentarna skupščina Sveta Evrope, 2005, str. 18) poudarila, da mora zakonodaja določati mandat oziroma pristojnost obveščevalno-varnostnih služb le za varovanje nacionalne varnosti ter opredelitev nacionalne varnosti, sicer je lahko ta razumljena kot preširok pojem in posledično omogoča delovanje obveščevalno-varnostnih služb tudi na drugih področjih. To je v skladu s priporočili Sveta Evrope št. 1402 (Svet Evrope, 1999, str. 2, odstavek A, 2. točka), ki za službe notranje varnosti določa: »Edina naloga služb notranje varnosti mora biti varovanje nacionalne varnosti. Varovanje nacionalne varnosti je definirano kot boj proti jasnim in prisotnim nevarnostim demokratični ureditvi države in njeni družbi. Ekonomski cilji oziroma boj proti organiziranemu kriminalu, *per se*, ne bi smeli spadati pod pristojnost služb notranje varnosti.« Tej definiciji bi bilo potrebno dodati tudi nejasne nevarnosti, ki izvirajo iz nejasno opredeljenih groženj. Ker varnost ni stoodstotna, tudi obveščevalno-varnostne službe ne morejo biti stoodstotne pri svojem delu. Ne morejo predvideti vseh varnostnih dogodkov in jih preprečiti, njihovi neuspehi pa lahko vodijo v spremembe v delovanju ali organizaciji služb. Službe so bile od 11. 9. 2001 dalje pogosto tarča kritik ob terorističnih napadih, zato so bile z namenom izboljšanja njihove koordinacije in njihovega delovanja izvedene reforme. Za reforme je (bilo) značilno predvsem (Parlamentarna skupščina Sveta Evrope, 2005, str. 16):

- »povečano sodelovanje obveščevalnih služb in deljenja podatkov znotraj države;
- povečano sodelovanje s tujimi obveščevalno-varnostnimi službami, mejnimi stražami, carinskimi organi in službami za imigrante na nacionalni ravni;
- vključitev zasebnih organizacij za boj proti terorizmu, npr. obvezno posredovanje telekomunikacijskih prometnih podatkov obveščevalno-varnostnim službam;
- sprejetje in uskladitev zakonodaje med evropskimi državami na področju pranja denarja, evropskega naloga za prijetje in širjenja definicije terorizma;

- varovanje človekovih pravic in svoboščin z namenom večje osredotočenosti na varnost.«

Nekatere reforme so vodile tudi v povečanje pooblastil in pristojnosti obveščevalno-varnostnih služb, kar jim je omogočila sprememba zakonodaje. S tem se ponovno vračamo k državni ureditvi oziroma politiki, ki določa temelje obveščevalno-varnostnega sistema in služb (glej npr. Purg, 2002, str. 40). Seveda pa razlike v položaju služb niso odvisne le od politike, temveč »tudi od varnostno-političnega položaja, procesov, dogodkov v neposredni bližini, od stopnje ogrožanja varnosti, ustavne ureditve in drugega.« (ibidem, str. 37) Potrebno je poudariti, da je za ureditev in spremembe, posredno pa tudi za delovanje obveščevalno-varnostnega sistema, odgovorna predvsem politika oziroma oblast.

2.3 Demokratični nadzor obveščevalno-varnostnih služb

Možnost uporabe posebnih metod in sredstev dopušča zlorabe pooblastil ali službe za lastne ali politične interese. Te je mogoče preprečiti z nadzorom, ki se v demokratično urejenih državah zaradi upoštevanja demokratičnih načel imenuje *demokratični nadzor*. V okviru demokratičnega nadzora delujeta institucionalni (npr. nadzor vlade, parlamenta, ombudsmana) in neinstitucionalni nadzor (npr. javnost, mediji, državljani) (Črnčec, 2009). V nedemokratičnih sistemih neformalni nadzor ni dopusten, v nekaterih takšnih sistemih pa se ga celo kazensko ali neformalno preganja (predvsem v diktaturah, totalitarnih/avtoritarnih državah). Zloraba pooblastil in moči obveščevalno-varnostnih služb omogoča nedovoljen poseg v človekove pravice, zato je demokratičen nadzor nujno potreben (Svet Evrope, 2009). Enako trdita Fitsanakis & Hodges (2013), namreč če nadzora ni, obstaja tveganje demokratični ureditvi, kar bi zahtevalo hitre in bistvene spremembe takšne ureditve. Demokratični nadzor obveščevalno-varnostnih služb je relativno nov pojav (Svet Evrope, 2009) iz sredine 70. let prejšnjega stoletja (Born & Leigh, 2007). Države so ga uvedle zaradi škandalov, kršenja človekovih pravic, ustavnih sprememb, tranzicije k demokratični ureditvi države, zakonskih sprememb, ki so jih zahtevali državljani (ibidem), ali prekoračitve pooblastil pri preprečevanju notranjega

terorizma (Wills, Born, Scheinin, Wiebusch & Thornton, 2011). Po 11. 9. 2001 je bil nadzor v nekaterih državah poostren ali spremenjen zaradi domnevne pomanjkljive strokovnosti in vplivanja politike na delo obveščevalno-varnostnih služb, v drugih pa zaradi nezaupanja internemu nadzoru v službah (ibidem). Razlogov za nadzor obveščevalno-varnostnih služb je tako več, poleg naštetih so tudi npr. zagotavljanje učinkovitosti ter zakonitosti in ustavnosti njihovega delovanja (Raab, 2017), preprečevanje zlorabe pooblastil, zagotavljanje primerne in učinkovite porabe denarja ter zagotavljanje legitimnosti dela služb (Bochel & Defty, 2017), nadzorovanje izvajanja strateških usmeritev dela (Šaponja, 1999). S tem se zagotavlja tudi demokratično odgovornost obveščevalno-varnostnih služb, ki hkrati preprečuje njihovo politizacijo (Born & Leigh, 2007). Pomembno vlogo pri nadzoru ima politična kultura, ki se odraža skozi zakonodajo (in obratno, op. G. H.) in (naj bi) temelji(la) na načelih politične odgovornosti (transparentnost, dolžnost, odgovornost, participacija in odzivnost) (Born & Leigh, 2005).

Zakonodaja mora natančno določati, kdo usmerja delo obveščevalno-varnostnih služb, kdo je njihov naročnik, kdo so uporabniki njihovih izdelkov (Šaponja, 1999). Hkrati mora zakonodaja upoštevati ustrezne mednarodne akte, še posebej Splošno deklaracijo o človekovih pravicah, v evropskem prostoru pa tudi EKČP. Priporočljivo je, da zakonodaja kljub relativni zaprtosti obveščevalno-varnostnega področja spodbuja kulturo odprtosti, predvsem pa spoštovanja človekovih pravic (Born & Leigh, 2005).

Med državami obstajajo manjše in večje razlike pri organizaciji in izvajanju nadzora (Wills et al., 2011). Tudi po evropskih državah so se uveljavili različni sistemi demokratičnega nadzora, kar je rezultat različnih zakonskih ureditev in vpletenih organov (Svet Evrope, 2009). Vrste nadzora se delijo na izvršilni nadzor, parlamentarni nadzor in nadzor neodvisnih teles, sodni nadzor, interni nadzor, strokovni nadzor (zunanji in notranji), finančni nadzor ter nadzor ombudsmana, informacijskega pooblaščenca, računskega sodišča, interesnih skupin, akademikov, raziskovalcev, javnosti in državljanov (Anžič & Golobinek, 2003; Born & Leigh, 2005, 2007; Črnčec, 2009; Sotlar, 2012). Ob tem velja omeniti tudi dve dimenziji nadzora, ki delita nadzorne organe glede na vsebino nadzora: 1) nadzor nad posegi v zasebnost in druge človekove pravice ter temeljne svoboščine, 2)

nadzor nad porabo finančnih in posebnih sredstev (Črnčec, 2009, str. 99). Ker so imele oziroma še vedno imajo na obliko in izvajanje nadzora največji vpliv preteklost, ustavna/državna ureditev in pa politična kultura (Bochel & Defty, 2017, str. 105), ne preseneča, da so si delitve med seboj podobne, saj vse izhajajo iz demokratičnih načel in demokratične ureditve.

Notranji ali **interni nadzor** je vrsta nadzora obveščevalno-varnostne službe, ki ga izvaja njena lastna organizacijska enota. S tem se zagotavljajo demokratični standardi, saj preprečuje zlorabo obveščevalno-varnostnih služb (Born & Leigh, 2005) od znotraj. Naloga notranjega nadzora je preverjanje zakonitosti, strokovnosti, obsega in pravočasnosti izvajanja nalog ter uskladitve dela službe s politiko s področja nacionalne varnosti (Sotlar, 2012). Takšen nadzor se zato imenuje tudi strokovno nadzorstvo in ga izvajajo različne institucije v okviru izvršilne oblasti, deli pa se na nadzor znotraj obveščevalno-varnostne službe (interni nadzor, op. G. H.) in nadzor znotraj resorja (inšpekcija, notranja revizija) (Črnčec, 2009). Nadzoruje in išče odgovornost uslužbencev pri izvajanju pooblastil, (prioritetnih) nalog in drugih relevantnih aktivnosti (Born & Geisler Mesevage, 2012). S to vrsto nadzora služba nadzoruje sama sebe. V vseh ostalih primerih službo nadzorujejo zunanji nadzorniki (posamezniki ali organizacije), ki niso del nadzorovane službe. Notranji nadzor določajo in urejajo zakonodaja ter notranji akti (Sotlar, 2012). Ti predpisi naj bi tudi sicer preprečevali oziroma prepovedovali vsako neetično in nelegitimno ravnanje uslužbencev. Dodatno naj bi uslužbence pred zlorabo pooblastil varovali tudi notranji predpisi in različni kodeksi, vsak posameznik pa naj bi bil poučen in usposobljen za ukrepanje v primeru, ko nadrejeni želi izvajati nedovoljene ukrepe (samostojno ali preko podrejenih) (Born & Leigh, 2005). Dodatno naj bi jih od neetičnega in nezakonitega ravnanja odvračali stimulativni delovni odnos in ustrezne usmeritve za delovanje (ibidem). Vključuje tudi nadzor finančnega poslovanja oziroma izvajanje revidiranja (Born & Geisler Mesevage, 2012; Sotlar, 2012).

Pomembna oblika nadzora služb je **politični ali parlamentarni nadzor**. Pojavlja se v več različnih oblikah: splošni parlamentarni odbori, specializirana parlamentarna telesa ali specializirana neparlamentarna telesa, ki jih imenuje parlament (Sotlar, 2012, str. 461). Parlamentarni nadzor lahko izvajajo tudi posamezni poslanci, saj imajo možnost, da na

sejah parlamenta ali posameznih delovnih teles vodji službe ali predstavnikom vlade (kadar služba spada pod okrilje vlade) postavijo vprašanja v zvezi z delovanjem služb. Države imajo različno urejen parlamentarni nadzor, zato se tudi mandat, struktura in drugi pomembni elementi parlamentarnega nadzora (npr. dostop do tajnih podatkov, varnostno preverjanje članov teles, proračun) razlikujejo po državah. Tako lahko parlament izvaja nadzor nad strokovnostjo in zakonitostjo, finančnim poslovanjem, administrativnim poslovanjem, izvajanjem pooblastil, poseganjem v človekove pravice in svoboščine, uresničevanjem politike/vladnih prioritet/letnega načrta dela, izvajanjem operacij idr. (Born & Leigh, 2005). Parlament sme nadzorovati uporabo pooblastil in finančnih sredstev služb le *ex post facto* (ibidem, str. 55), ne pa tudi za trenutno obdobje oziroma za tekoče zadeve. S tem se zagotavlja operativno varnost in hkrati nemoteno tekoče delo služb. Politično nadzorstvo vzpodbuja možnost zaupanja javnosti v delo služb in v delo nadzornega telesa (Anžič & Golobinek, 2003), kljub temu pa vedno obstaja tveganje, da se bo tovrstni nadzor zlorabilo za politične razloge, kar lahko vpliva na javno podobo služb in tudi na javno (ne)zaupanje službam (Born & Leigh, 2005). Ključno je, da tisti del parlamenta, ki ne izvaja nadzora, in javnost vseeno zaupata parlamentarnemu nadzoru ter da službe delujejo ustrezno (ibidem).

In čeprav je parlamentarni nadzor tisti, ki ga v imenu ljudstva izvajajo izvoljeni predstavniki, je zaradi praktičnih razlogov in tajnosti z vidika učinkovitosti še bolj pomemben **izvršilni ali vladni nadzor** (Born & Leigh, 2005, str. 55). Ta izvaja nadzor na vseh področjih obveščevalno-varnostnih služb, še posebej pa na področju strokovnosti in učinkovitosti (Šaponja, 1999). V okviru vlade so izvrševalci takšnega nadzora osebe, ki so na čelu vlade (predsednik vlade, v predsedniških sistemih pa predsednik države, op. G. H.), in ministri, kadar je obveščevalno-varnostna služba del njihovega resorja (Born & Leigh, 2005). Za razliko od parlamentarnega oziroma zakonodajnega nadzora izvršilni spremlja in nadzoruje delovanje služb v realnem času (ibidem). Nadzora ne izvaja na enak način kot zakonodajna veja oblasti, temveč se ta realizira v obliki zahtev za pridobitev informacij (npr. o sprotnem delovanju služb, o realiziranih nalogah in prioritetah, o organizacijskem in finančnem stanju), v obliki četrt- ali polletnih in letnih poročil o delu služb in drugih podobnih oblikah poročanja. Takšen nadzor ne sme biti vmešavanje v delo služb, temveč dajanje usmeritev in preverjanje njihovega

uresničevanja ter strokovnega delovanja. Neposredna vključenost v aktivnosti takšnih služb bi namreč pomenila njihovo politiziranje, s tem pa uporabo/zlorab služb za ozke politične interese (Sotlar, 2012).

Sodni nadzor bdi nad uporabo posebnih ukrepov (Born & Leigh, 2005). Izvajajo ga splošna in ustavna sodišča (Črnčec, 2009), ki so zadolžena predvsem za nadzor (ustavnosti in) zakonitosti dela obveščevalno-varnostnih služb (Šaponja, 1999). Lahko se uporablja kot predhodni ali naknadni nadzor (Sotlar, 2012). Prvi predstavlja »varovalko«, da mora obveščevalno-varnostna služba pred izvajanjem ukrepa zaprositi sodišče za dovoljenje za poseg v določene človekove pravice, drugi pa pomeni, da ima državljan možnost poiskati pravico na sodišču, če meni, da je prišlo do domnevnih kršitev njegovih pravic s strani obveščevalno-varnostnih služb (ibidem).

Finančni nadzor je zadolžen za revizijo poslovanja obveščevalno-varnostnih služb in pregled porabe finančnih sredstev (Črnčec, 2009). V nekaterih državah ga izvajajo računska sodišča, ponekod revizorji za nadzor proračuna, drugod s posebnimi finančnimi inšpektorji ipd. (Sotlar, 2012). S finančnim nadzorom se zagotavlja pregled nad porabo javnih sredstev in vpogled v delovanje in učinkovitost obveščevalno-varnostnih služb, kar tudi omogoča preprečevanje in odkrivanje finančnih tveganj (Wills, 2012), npr. neupravičene porabe, prilaščanja javnih sredstev, korupcije, davčne utaje. Pri tem se ugotavlja tudi smotrnost in doseganje ciljev službe s porabo (javnih) finančnih sredstev (Sotlar, 2012). Izvaja se *ex post*, torej za nazaj (ibidem).

Ombudsman izvaja posebno oblika nepolitičnega in neodvisnega nadzora in je še posebej pomemben takrat, kadar posameznik meni, da mu je matična obveščevalno-varnostna služba kršila človekove pravice. S tem se uresničuje načelo transparentnosti delovanja obveščevalno-varnostnih služb (Born & Leigh, 2005). Ombudsman lahko od služb na podlagi pritožb državljanov zahteva podatke in pojasnila v zvezi z domnevnimi kršitvami (Črnčec, 2009), ne glede na to, ali so podatki označeni s stopnjo tajnosti in ali so del tekočih ali končanih postopkov. Pomembno vlogo ima pri tem tudi **informacijski pooblaščenec**, ki izvaja nadzor nad izvedbo postopka odobritve ali zavrnitve dostopa do tajnih podatkov, osebnih podatkov (Črnčec, 2009) in informacij javnega značaja, kadar

državljani ali organizacije zahtevajo umik stopnje tajnosti ali pridobiti določene podatke, za katere menijo, da bi morali biti dostopni javnosti.

V tem pogledu je posebnega pomena **nadzor javnosti**, ki se od ostalih vrst nadzora razlikuje predvsem po tem, da je javnosti onemogočen dostop do tajnih podatkov o delu obveščevalno-varnostnih služb. Zaprtost služb zaradi tajnosti otežuje vpogled v delo služb, zato se mora javnost bolj zanašati na druge subjekte demokratičnega nadzora (Wills et al., 2011). Kljub temu se nadzor javnosti izraža v obliki medijskih prispevkov in javnega mnenja o delovanju služb (Sotlar, 2012). Ima tudi vpliv, da zadrži oziroma omeji delovanje služb z objavljanjem alternativnih pogledov javnosti, z medijskim razkrivanjem škandalov in kriz ter s pritožbami v zvezi z nepravilnostmi v službah (Born & Leigh, 2005, str. 15). Mediji so namreč tisti, ki prenašajo informacije od oblasti javnosti in oblikujejo svoje informacije, zato imajo tako neposredni kot posredni vpliv na oblikovanje javnega mnenja (ibidem). Državljani, ki nimajo dovolj znanja ali informacij o obveščevalno-varnostnih službah (tudi zaradi tajnosti), **so dovzetnejši za podatke in informacije** (tudi napačne, popačene ali zavajajoče) o službah iz medijev in drugih virov, ki vplivajo na njihovo znanje in mnenje. Težko je sicer pričakovati, da bodo obveščevalno-varnostne službe redno posredovale določene informacije o svojem delu in s tem komentirale svoje delovanje v javnosti, saj je njihova molčečnost »njihova največja vrlina in hkrati tudi pomanjkljivost. […] To je njihov obrambni mehanizem, ki jih ohranja pred entropijo. Nobena obveščevalno-varnostna služba si ne more privoščiti, da bi bila nenehno v izložbi, na televiziji, v etru ali v časopisih.« (Sotlar, 2012, str. 484) Relevantne informacije zato javnosti posredujejo oblast in nadzorni organi, s čimer uresničujejo načelo javnosti in transparentnosti, vendar javnosti posredujejo le tisto, kar sme vedeti. Fitsanakis & Hodges (2013) ugotavljata, da literatura obravnava medije kot »institucije za potrjevanje legitimnosti« (delovanja) obveščevalno-varnostnih služb, s tem pa mediji obveščajo javnost o uspešnosti služb in počasi brišejo »skrivnostnost«, ki je (bila) značilna za službe. Na takšen način se tudi izboljšuje ugled služb v očeh javnosti (ibidem).

K nadzoru pomembno prispevajo tudi javne razprave. Te predstavljajo možnost za izboljšanje nadzora ter zaupanja v obveščevalno-varnostne službe (Goldman & Rascoff, 2016, str. xxix), saj izpostavljajo ključne elemente, ki jih javnost prepoznava kot kritične.

Na takšen način se nenehno oblikuje in spreminja **javno mnenje**, ki predstavlja pomemben del zaupanja državljanov v matične obveščevalno-varnostne službe. Z njim lahko družba doseže določene akcije, vplive ali spremembe v delovanju države. Najpomembnejši vpliv javnega mnenja izpostavlja Sotlar (2012, str. 483): »Pametna vlada bo torej poskušala spoštovati prevladujoče javno mnenje v družbi, saj je od tega odvisna njena legitimnost, brez nje pa nobena družba ne bo pripravljena podaljšati ''pogodbe'', sklenjene med vlado in družbo.« Če javnost z izvajanjem nadzora izraža nezaupanje obveščevalno-varnostnim službam, bo morala oblast poskusiti umiriti pritiske javnosti in nezadovoljstvo, sicer javnost ne bo zaupala niti oblasti/vladi. To lahko privede do družbenih nemirov, demonstracij in izgredov, v skrajnih primerih pa tudi do spopadov in nasilne ali nenasilne menjave oblasti. Menimo, da je to dodaten argument, zakaj je zaupanje v matične obveščevalno-varnostne službe pomembno ne le za službe, temveč za celotno nacionalno varnost, ki jo preko državnih institucij upravlja oblast oziroma vlada. »Zaupanje je verjetno najpomembnejša determinanta, kako dobro bo šlo obveščevalno-varnostnim službam v liberalnih demokracijah. […] Učinkoviti nadzor je kritičen za gojenje in vzdrževanje zaupanja v institucije, ki izvajajo obveščevalno-varnostne funkcije, predvsem zato, ker je veliko orodij, ki so razvita za sprejemanje odgovornosti javnih institucij v zahodnih demokracijah, jih ni mogoče uporabiti na obveščevalno-varnostnem področju.« (Goldman & Rascoff, 2016, str. xxix) S tem potrjujemo, da je nadzor pomemben dejavnik zaupanja, o čemer govori tudi Purg (2002, str. 71): »Vprašanje nadzora nad delovanjem obveščevalnih oziroma varnostno-obveščevalnih služb je v neposredni in tesni zvezi z legitimnostjo političnega sistema, pa tudi z **zaupanjem javnosti v njihovo delo**. **Obstaja teza, da bolj kot so obveščevalne službe nadzorovane, in manj je odkritih napak, večje je zaupanje javnosti v zakonitost njihovega dela** [poudaril G. H.].«

Gill (2007) pravi, da ima pri določanju uspešnosti organa nadzora ključno vlogo šest spremenljivk: oblika (parlamentarni, izvršilni, sodni itd.), mandat (pristojnosti, pooblastila, omejitve), članstvo (kdo je član skupine – predvsem v smislu strankarske pripadnosti), viri (kadrovski, materialni, finančni, prostori), dostop do informacij (dostop do vseh vrst podatkov, tudi tajnih, stopnja zagotovljenega pritoka informacij iz nadzorovanih služb in drugih organov) in poročanje (matičnemu, nadrejenemu oziroma

pristojnemu organu). Ob tem je potrebno upoštevati, da ima vsaka vrsta nadzora svojo funkcijo in svoje področje, ki ga pokriva (Born & Leigh, 2005), zato je težko govoriti o enotnih kriterijih ugotavljanja uspešnosti nadzora. Uspeh in učinkovitost izvršilnega nadzornega mehanizma je težko ocenjevati tudi zaradi tajnosti, saj je ta potrebna za zagotavljanje zaščite aktivnostim obveščevalno-varnostnih služb. Ker vpogled javnosti v delo nadzornikov ni mogoč, jim morajo zaupati, da svoje delo opravljajo dosledno. Zaupanje vanje oziroma v nadzor (in posledično v službe, op. G. H.) pa se lahko izboljša, če se na položaje nadzornikov imenuje kompetentne in izkušene strokovnjake, njim pa se dodeli mandat, neodvisnost in močna pooblastila (Hardy & Williams, 2016). Šaponja (1999, str. 51) opozarja, da lahko pri tem pride do težav, saj nadzorniki pogosto nimajo znanja s področja obveščevalno-varnostne dejavnosti, zato pri nadzorovanju težko ocenijo upravičenost in smotrnost določenega ukrepa.

Nadzorstvo mora biti **uravnoteženo** (Podbregar, 2017, osebni vir). To pomeni, da nadzora ne izvajajo vsi organi hkrati niti da posamični organi z izvajanjem nadzora ne preobremenijo izvajanje temeljnih funkcij oziroma dela obveščevalno-varnostnih služb (ibidem). Ob tem moramo razumeti, da si »[n]adzorstvo in strokovne potrebe praviloma nikoli niso povsem v sozvočju. Potrebe nadzorstva velikokrat omejujejo stroko in zmanjšujejo njeno učinkovitost. Pomembno je izoblikovati tak sistem nadzorstva, ki ta nasprotja čim bolj ublaži.« (Šaponja, 1999, str. 53) Črnčec (2009, str. 101) celo pravi, da sta navzočnost in razpršenost »jasna kazalca demokratičnosti nekega sistema.« Posledica nadzora naj ne bi bila le kritika, temveč, kot trdi Anžič (1996, str. 197), mora biti posledica nadzora nagrada ali sankcija: »Nagrajevanje je tista oblika izražanja priznanja in zahvale za opravljeno delo, ki ima za posledico finančne, moralne ali statusne učinke ter je usmerjena v perspektivo tako za nagrajence kakor tudi za druge udeležence nadzorovalnega procesa. Sankcionirajo pa se tista ravnanja, ki so v nasprotju s postavljenimi pravnimi ali moralnimi normami in trčijo na načela njihovega varstva. Toda sankcionirajo se lahko le posamezniki skladno s titularjem svoje funkcije, nikoli ustanova.« Pomemben je tudi odziv nadzorovanih subjektov. Njihove pozitivne reakcije lahko okrepijo zaupanje javnosti tako v izvajalca nadzora kot tudi v subjekt nadzora ter izboljša odnos med javnostjo, izvajalcem nadzora in subjektom nadzora, medtem ko negativne reakcije povzročajo ravno obratno (Anžič, 1996).

Prepričani smo, da zaupanje v obveščevalno-varnostne službe ni vezano izključno na demokratični nadzor teh služb, kot velja splošno prepričanje. To med drugim potrjuje primer Združenega kraljestva iz leta 2014, ko so ljudje manj zaupali matičnim obveščevalno-varnostnim službam kot nekoč, čeprav imajo verjetno enega najboljših sistemov demokratičnega nadzora obveščevalno-varnostnih služb na svetu. Razlog za manjše zaupanje so bila med drugim širša pooblastila, ki so jih službe dobile z novo zakonodajo (*Investigatory Powers Act*) in jim omogoča množičen nadzor elektronskih komunikacij. Podobno je bilo v Franciji leta 2015, ko so obveščevalno-varnostne službe dobila širša pooblastila kot odgovor na teroristični napad, in kasneje leta 2016, ko sta francoski parlament in senat potrdila zakonodajo o širših pooblastilih policijskih in varnostnih organov. Menimo, da je zato nesmiselno zagovarjati tezo, da dobro vzpostavljen in učinkovit sistem demokratičnega nadzora obveščevalno-varnostnih služb zagotavlja zaupanje državljanov v matične obveščevalno-varnostne službe. Ugotavljamo, da je demokratični nadzor sicer pomemben dejavnik zaupanja, ni pa edini, hkrati pa lahko tudi demokratični nadzor zaradi neustreznega nadzora postane pospeševalec nezaupanja namesto zaupanja.

3 Zaupanje

O zaupanju nikoli ali redko razmišljamo kot o znanstveni disciplini, saj je del vsakdanjega življenja. Ker je poznavanje zaupanja kot znanstvene discipline in raziskovalnega področja ključno za razumevanje vsebine doktorske disertacije, predvsem pa za kasnejše modeliranje oziroma izgradnjo modela celovitega zaupanja državljanov v matične obveščevalno-varnostne službe, ga podrobneje obravnavamo v tem poglavju.

V doktorski disertaciji smo se izognili opredelitvi nezaupanja. Schoorman et al. (2007, str. 350) ugotavljajo, da se večina teoretikov, ki se ukvarjajo z zaupanjem, strinja, da sta zaupanje in nezaupanje nasprotna si in ločena konstrukta. Poleg tega je zaupanje kot pozitivna stran človeške narave tisto, ki domneva in pričakuje od ljudi najboljše (McKnight & Chervany, 2001). To tudi odraža našo željo: z doktorsko disertacijo želimo izgraditi model, ki bo državljane vzpodbudil k večjemu, tj. celovitem zaupanju v matične obveščevalno-varnostne službe.

3.1 Izbor ustrezne tuje terminologije

Na začetku raziskovanja zaupanja smo upoštevali dejavnik, ki ga pri obravnavi tuje literature nismo mogli niti smeli spregledati – jezikovna raznolikost. Slovar slovenskega knjižnega jezika (Zaupanje, b. d.) slovenski izraz *zaupanje* definira kot »[…] *prepričanje, da je kdo sposoben, voljen narediti, kar se pričakuje:* z delom upravičiti zaupanje koga; delavci so izkušeni, zato uživajo zaupanje; poln zaupanja prositi koga za pomoč / imeti zaupanje vase // *prepričanje, da je kdo pošten, iskren:* zlorabiti zaupanje koga; ekspr. v slepem zaupanju mu je verjela // *prepričanje, da je kaj dobro in da bo dobro vplivalo na uresničitev določenih pričakovanj:* zaupanje lastni moči / zaupanje v razum ● publ. večina volivcev mu je izrazila zaupanje *je glasovala zanj*; knjiž. podarjati komu zaupanje *zaupati vanj* ♪.« Izraz ***prepričanje***, ki ga v definiciji zaupanja uporablja Slovar slovenskega knjižnega jezika (glej Zaupanje, b. d.), lahko definiramo kot občutek, ko vemo, da nekdo/nekaj ne bo neuspešen/neuspešno pri svojem delovanju (Hart, 1988), zato je prepričanje osnovni gradnik zaupanja. Iz definicije Slovarja slovenskega

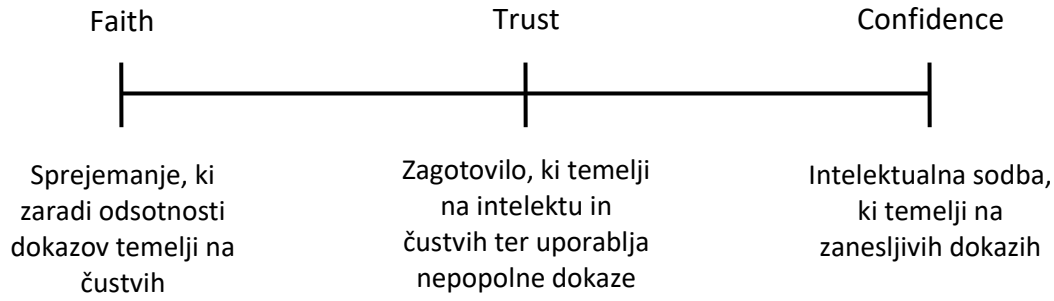
knjižnega jezika je razvidno, da ima slovenski izraz *zaupanje* več sorodnih pomenov, vendar se v vseh primerih uporablja isti izraz – *zaupanje*. V slovenskem jeziku tako ne poznamo drugih izrazov, ki pomenijo zaupanje, medtem ko v npr. angleškem jeziku za izraz zaupanje, kot ga pojmujemo in razumemo v slovenskem jeziku, obstajata vsaj dva različna, vendar pomensko sorodna izraza: *trust* in *confidence*. Nekateri tuji avtorji poleg teh dveh angleških izrazov prištevajo tudi druge, npr. *faith* (Hart, 1988; Gambetta, 1988) oziroma vera/verovanje, *cooperation* (Mayer et al., 1995) oziroma sodelovanje in *predictability* (ibidem) oziroma predvidljivost. Izrazom *trust*, *confidence* in *faith* je skupno, da izražajo prepričanje, verovanje oziroma zaverovanost (v nekaj *verjeti*), imeti nekaj za resnično, hkrati pa odražajo različne stopnje njihove dokazljivosti z dokazi, ki jih pridobimo s čutili (Hart, 1988).

Obravnavali smo tujo literaturo o zaupanju v angleškem jeziku, zato je za ustrezno in pravilno rabo ter kasnejšo aplikacijo teoretičnih spoznanj o zaupanju iz tuje literature v slovenski jezik potrebno poznati razlike angleških različic slovenskega izraza *zaupanje*. Poznavanje teh razlik je izrednega pomena zaradi pravilne opredelitve odnosa posameznika do okoliščin, predmeta ali osebe, ki se odraža kot zaupanje v nekaj/nekoga. Zato je pri analizi literature v angleškem jeziku potrebno biti pozoren na raznolikost posameznih izrazov, pri uporabi slovenskega izraza *zaupanje* pa je zato nujno potrebno opredeliti tudi kontekst uporabe, saj je zaupanje, kot trdijo mnogi avtorji (npr. Olmedilla, Rana, Matthews & Nejdl, 2006; Kovač & Trček, 2007; Little, Marsh & Briggs, 2007; Martin, 2014), **odvisno od konteksta**, znotraj katerega obravnavamo zaupanje. Prepričani smo, da takšne jezikovne razlike ne pomenijo, da je slovenski jezik zaradi skromnejšega izrazoslovja na tem področju v slabšem položaju niti da je uporabnik slovenskega jezika pri izražanju misli, mnenj o zaupanju ali zaupanja omejen.

V nadaljevanju pojasnjujemo angleške izraze *faith*, *trust* in *confidence*. Zadnja sta si vsebinsko podobna, saj oba izražata določeno stopnjo pozitivnega odnosa do človeka, oba lahko preideta oziroma vodita v razočaranje, oba sta lahko del normalnega vedênja in rutine (Luhmann, 1988, str. 97) ter oba izražata neko vrsto prepričanja (Hart, 1988), tako kot tudi angleški izraz *faith*. *Faith* in *confidence* izhajata iz latinskega izraza *fides* (Hart, 1988, str. 187), v glagolski obliki *fidere*, kar pomeni *zaupati* (Faith, b. d.). Podobno

kot slovenski izraz *zaupanje* je tudi izbrane tri angleške izraze mogoče uporabiti ne le za poimenovanje prepričanja v osebo, temveč tudi prepričanja v predmete, okoliščine ali abstraktne reči (npr. zamisli, ideje, vero). Tako meni tudi Hart (1988), ki pravi, da se angleški izraz *trust* z enakim pomenom nanaša na osebe, ideje ali predmete, zato je meja med razlikovanjem prepričanja v oziroma odnosa do oseb in vsega ostalega zabrisana. V teoriji (v angleškem jeziku) pa med *faith*, *trust* in *confidence* obstajajo pomembne vsebinske razlike. Ključni dejavniki, ki ločujejo te tri različne angleške izraze zaupanja, so *čustva* in *dokazi*. Glavne razlike med *faith, confidence* in *trust* ponazarja slika 3.1.

Slika 3.1: Razlika med *faith*, *trust* in *confidence*



Vir: Judge, 1999, str. 150

Beseda *faith* v angleški terminologiji pomeni *zaupanje* (zaupati v nekaj/nekoga) ali *vero*, *verovanje*, *verovati*, kadar dokazi niso potrebni, zato *faith* kot zaupanje pomeni čustveno in brezpogojno sprejemanje, da bo nekaj/nekdo bo uspešno/uspešen pri svojem delovanju (Hart, 1988). Od tod tudi izvira poimenovanje tovrstnega zaupanja kot *slepo zaupanje*. V slovenskem prostoru je izraz *verovati* bolj prepoznan v kontekstu religije (Verovati, b. d.): »*[I]meti zavest o obstoju boga, nadnaravnih sil* […], *biti prepričan o obstoju, resničnosti česa, kar uči vera* […], *biti prepričan o obstoju česa skrivnostnega, umišljenega; verjeti*.« Isti izraz hkrati pomeni tudi zvrst *zaupanja* kot *prepričanja*, npr. »*biti prepričan o obstoju, možnosti nastopa, uresničitve zlasti česa zaželenega:* verovati v prijateljstvo, resnico, srečo / verovali so, da bodo zmagali […], *biti prepričan o uspešnosti, učinkovitosti koga ali česa:* verovati v ljudi; verovali so v delavski razred / veruje v njihovo nadarjenost […], *biti prepričan o poštenosti, iskrenosti koga; verjeti:* mladina jim več ne veruje / ne veruje tem besedam.« (ibidem)

Nasprotno od *faith* je *confidence* – zaupanje, ki je odvisno od dokazov. *Confidence* je tista oblika prepričanja ali zaupanja, ki je v tuji literaturi (Luhmann, 1988, str. 97) opredeljeno kot odnos, ki je v manjši meri odvisen od naših dejanj in odločitev, povezan pa je s prepričanji in pričakovanji ter izhaja iz željá in zmanjševanja kognitivne disonance (miselne razglašenosti, miselnih neskladij, op. G. H.). Iz tega razloga je bolj podobna upanju kot pa zaupanju. Hart (1988) pravi, da je *confidence* mogoče razumeti kot močno prepričanje ali sodbo, ki temelji na zanesljivih dokazih ali logični dedukciji. S preučevanjem okoliščin in preverjanjem dokazov namreč posameznik ugotovi, da zaradi (dokazljive, op. G. H.) izredno majhne verjetnosti, da do razočaranja sploh pride, in ker mu ne preostane nobena druga možnost, kot pa da zaupa v situacijo in v za posameznika pričakovan izid, možnost razočaranja enostavno zanemari (Luhmann, 1988). V obeh primerih je izraženo upanje oziroma želja, ki je zaradi miselnih procesov in dokazov, da naše vedênje in dejanja nimajo pomembnega ali večjega vpliva na dogajanje oziroma situacijo, postalo/-a prepričanje, da se nam nekaj ne more zgoditi. Ker obstajajo trdni dokazi, v katere je posameznik lahko prepričan, je čustvena vpetost posameznika v okoliščine zato manjša (Hart, 1988). *Confidence* od posameznika ne zahteva, da se aktivno vključi v situacijo in sprejme tveganje, saj je iz okoliščin oziroma dokazov razvidno, da nanje nima vpliva, zato tudi ne bo sprejel nobenih tveganj, ker to ni potrebno. Te dokaze posameznik spremeni v informacije. O pomembnosti informacij pri odločanju, ali zaupati ali ne zaupati, govori tudi Rus (2008, str. 75): »Čeprav je zaupanje vselej slepo, pa *odločitev* o tem, komu bomo zaupali, še zdaleč ni sprejeta na slepo, temveč temelji na izčrpnih informacijah,« in nadaljuje, da »[z]aupanje namreč namenjamo samo tistim, ki so po našem mnenju tega vredni. Zato vsako dejanje slepega zaupanja vselej gradi na predhodnem socialnem odnosu, prek katerega smo preverjali in utrjevali vtis o tem, ali in koliko je partner vreden zaupanja. Odločitev o tem, komu bomo zaupali, je vselej utemeljena na ekstenzivnih informacijah o transakcijskih partnerjih.« (ibidem)

Med slepim (*faith*) in previdnim (*confidence*) zaupanjem se nahaja *trust*: pričakovanje ali prepričanje, ki temelji na intelektu in čustvih (Judge, 1999) ter nepopolnih oziroma nepojasnjenih dokazih (Hart, 1988). Ker je prepričanje občutek, ko vemo, da nekdo/nekaj ne bo neuspešen/neuspešno pri svojem delovanju, ti občutki pa se obratno

spreminjajo z dokazi, pomeni *trust* v tem smislu tudi globino in zagotavljanje takšnih občutkov z neprepričljivimi dokazi (ibidem). Zaradi slednjih se mora posameznik odločiti na podlagi tistega, kar ima na takrat na razpolago, tudi če ti dokazi niso povsem utemeljeni, dovolj jasni, številčni ali zanesljivi, da bi lahko z njihovo analizo prišel do prepričljivih zaključkov, ali nekomu/nečemu zaupati ali ne. Pomanjkanje dokazov in s tem nejasne okoliščine posameznika prisilijo, da tvega. Posameznik namreč predpostavlja, prepozna in sprejme oziroma mora sprejeti tveganje v določeni situaciji (Luhmann, 1988, str. 97). Do tega pri *faith* in *confidence* sploh ne pride, zato lahko v kontekstu izraza *trust* govorimo o aktivnejši vlogi posameznika, ki je zaradi prepoznane verjetnosti, da pride do razočaranja, prisiljen ukrepati. Poudarjamo, da zaupanje v obliki *trust* ne pomeni *tvegati*, temveč ***biti pripravljen tvegati*** (Mayer et al., 1995).

Tveganje je opredeljeno kot učinek negotovosti na cilje, pri čemer učinek pomeni pozitiven ali negativen odklon od pričakovanega (International Organization for Standardization, 2009). Tveganje vedno obstaja, ne glede na naše želje ali vplive, njihovih razsežnosti pa ne moremo predvideti v celoti. Vnaprej jih lahko le deloma predvidimo, vendar se lahko zaradi majhne spremembe v izhodišču tveganje manifestira na popolnoma drugačen način in v drugačnih razsežnostih, kot smo sami predvideli. Biti pripravljen tvegati izraža pripravljenost tvegati, čeprav upnik še ni vstopili v situacijo, ko bi tudi dejansko tvegal (Mayer et al., 1995). Biti pripravljen tvegati je zato mogoče razumeti kot zavestno sprejemanje tveganja, biti pripravljen izpostaviti se tveganju in hkrati pričakovati, da bo nekdo/nekaj uresničil/a/o upnikova pričakovanja – kljub tveganju. Pri tem je bistveno, koliko smo pri obvladovanju tveganj pripravljeni tvegati glede na subjektivno zaznano, ki pa ni nujno identično realni obstoječi stopnji ali vrsti tveganja. Dojemanje tveganja je namreč stvar percepcije, zato Luhmann (1988) pravi, da je zaupanje (*trust*) odvisno od posameznikove percepcije in atribucije. Atribucija je »[k]ognitivna teorija motivacije, ki pojasnjuje oblikovanje različnih atribucij oziroma atribucijskih stilov posameznikov; preučuje načine, na katere posamezniki pripisujemo vzroke dogodkom, s preučevanjem razlogov, zakaj in kako to počnemo, in pogojev, v katerih to počnemo ali ne počnemo ter kako vse to vpliva na motivacijo.« (Atribucija, b. d.) Kadar pa upnik vstopi v situacijo, ko dejansko tvega, pa gre za vedênjsko manifestacijo pripravljenosti tvegati (Mayer et al., 1995) oziroma ***zaupljivo vedênje***, kot

temu pravimo avtorji doktorske disertacije. Razlika med zaupanjem in zaupljivim vedênjem je torej v tem, da je pri zaupanju upnik zaenkrat le pripravljen tvegati, vendar ne vstopi situacijo, za katero meni, da bi tvegal, pri zaupljivem vedênju pa upnik *vstopi v situacijo* in po njegovem prepričanju *že tvega*. Ponovno poudarjamo: zaupanje ni vezano na (dejansko) tveganje, temveč na pripravljenost tvegati. S tveganjem je posameznik tudi ranljiv, zato lahko zaupanje definiramo tudi kot »pripravljenost udeleženca biti ranljiv za dejanja drugega udeleženca, ki [pripravljenost biti ranljiv, op. G. H.] temelji na pričakovanjih, da bo drugi udeleženec opravil določena dejanja, pomembna za udeleženca upnika, ne glede na sposobnost spremljati ali nadzorovati drugega udeleženca,« (Mayer et al., 1995, str. 712) saj obstaja svobodna volja zaupnika, da stori, kar mu je bilo zaupano, ali pa upniku namerno ali nenamerno škoduje (Little et al., 2007). Podobno Arnott (2007, str. 981) razume zaupanje kot prepričanje v zanesljivost tretje osebe, še posebej ko je prisoten dejavnik osebnega tveganja.

Deutsch (1958, str. 266-267) pravi, da se izraz *trust* navezuje na kontekst pričakovanja, ko želeni dogodek oziroma izid za posameznika ni škodljiv. To je popolnoma razumljivo in skladno z naravo človeka, ki ga v podzavesti žene boj za preživetje, zato išče njemu najbolj ugodne in najmanj škodljive rešitve za dane probleme in situacije. Pri tem posameznik (miselno) tehta ali preračunava, kakšne so možnosti, da pride do zanj pozitivnega (pričakovanega) izida. Po mnenju Luhmanna (1988) takšna logika pri zaupanju ne pride v poštev, saj bi v primeru zaznanega prevelikega tveganja, ki temelji na takšnem preračunavanju, enostavno odstopili od namenov ali želja in se s tem izognili doseganju koristi in morebitni razočaranju, ker je zaznana škoda večja od pričakovane ali želene koristi. Takšno mnenje izhaja iz trditve (Deutsch, 1958, str. 266), da je zaupanje mogoče le v okoliščinah, ko so negativne motivacijske posledice večje od pozitivnih motivacijskih posledic. Podobno pravi tudi Hosmer (1995), in sicer da sta pričakovanje, da bo razočaranje ob izgubi zaupanja večje od koristi ob vzdrževanju zaupanja, in prepričanje, da posameznik ne more vedeti ter obvladovati verjetnosti izgube zaupanja, pomemben del definicije zaupanja. Tako Deutsch (1958) kot Hosmer (1995) menita, da bi bilo vprašanje zaupanja brez tega le stvar preprostega verjetnostnega izračuna, ki bi nam s številkami povedal, ali glede na verjetnost razočaranja zaupati ali ne. Če posameznik zaradi rezultata izračuna, da bi več izgubil kot pridobil, ne bi zavestno vstopil

v situacijo tveganja, potem tudi ne bi potreboval nekoga/nekaj, komur/čemur bi lahko zaupal, da bi prišlo do realizacije pričakovanj. V praksi bi to pomenilo, da zaradi »računsko dokazljivega« neuspeha in bojazni pred neuspehom npr. ne bi sprejemali hitrih, pomembnih, odločilnih ali drznih odločitev v trenutkih, ko nismo povsem prepričani o uspehu. Da pa bi posameznik kljub večjim možnostim neuspeha vseeno poskušal doseči pričakovano, je potrebno, da nekomu/nečemu (npr. varni prometni ureditvi, napravi, čeladi) zaupa. Iz tega izhaja, da je zaupanje potrebno v situacijah, ko *obstaja verjetnost*, da bo posameznik zaradi dejanj ali okoliščin na koncu *razočarani* (Luhmann, 1988, str. 98), hkrati pa *nima druge izbire*, kot da zaupa (Hosmer, 1995).

V posamezni življenjski situaciji lahko posameznik uporablja vse tri vrste zaupanja, nič nenavadnega pa ni, če jih uporabi tudi v enakem okolju ali situaciji. Primer: nekdo zaupa (*confidence*) v organizacijo zaradi trdnih dokazov, npr. pozitivni poslovni rezultati in zadovoljni zaposleni, in hkrati v svoje sodelavce (*trust*) zaradi mešanice lastnih prepričanj in čustev ter nekaterih dokazov. Ta primer kaže dvoje:

1. slovensko izrazoslovje ne pozna razlik med različnimi vrstami zaupanja, še posebej ne v smislu razmerja čustva-dokazi;
2. dve različni angleški izrazoslovni obliki zaupanja se nanašata na različne objekte/subjekte, vendar v istih okoliščinah, medtem ko v slovenskem izrazoslovju za vse okoliščine uporabljamo enak izraz in pristop.

Luhmann (1988, str. 99) pravi, da za uporabo različnih angleških izrazov v istih okoliščinah prihaja zaradi različnih alternativ, ki so na voljo, hkrati pa lahko ti dve vrsti zaupanja pozitivno ali negativno vplivata ena na drugo, npr. izguba zaupanja v sodelavce (*trust*) lahko zamaje zaupanje v organizacijo (*confidence*) – in obratno. S tem želimo poudariti, da v praksi uporabljamo več različnih oblik zaupanja, ne glede na jezik, in da izbira ene oblike zaupanja pomeni ignoriranje drugih oblik. Nekaterim osebam zaupamo bolj zaradi čustev, drugim zaradi dokazov, tretjim zaradi vmesne kombinacije obojega ipd., v slovenskem jeziku pa takšnemu prepričanju vedno pravimo *zaupanje*.

Vsa naša dosedanja spoznanja o zaupanju so bila za nas pomembna iz razloga, da:

- zaupanja nismo obravnavali enostransko, npr. kot en sam izraz z enim pomenom;

- zaupanja nismo obravnavali preveč široko in preveč splošno;
- smo znali razlikovati oblike zaupanja v angleškem jeziku;
- smo znali upoštevati vlogo in težo čustev ter dokazov, ki oblikujejo zaupanje;
- smo se lažje odločili, kateremu angleškemu izrazu/obliki zaupanja nameniti več pozornosti in ga/jo izbrati za nadaljnje raziskovanje.

V zvezi z zadnjo alinejo smo ugotovili, da je *trust* edina zvrst zaupanja, ki :

1. od posameznika zahteva, da je pripravljen sprejeti tveganja in biti ranljiv;
2. posameznika prisili v razmislek o izbiri izmed različnih alternativ;
3. temelji na čustvih in hkrati (pomanjkljivih) dokazih, obenem pa je potrebno upoštevati, da je zaupanje – kar zaradi vpletenosti čustev še posebej velja za angleški izraz *trust* – odvisno tudi od konteksta oziroma situacije, v kateri obravnavamo pojav zaupanja (enako ugotavljajo tudi Little et al., 2007)

Ker iz lastnih izkušenj vemo, da se v kontekstu obveščevalno-varnostnih služb ne odločamo le na podlagi dokazov ali čustev, ocenjujemo, da je *trust* najustreznejši angleški izraz za zaupanje, kakršno obravnavamo v našem kontekstu, zato smo se pri obravnavi literature v angleškem jeziku osredotočili le na tisto literaturo, ki obravnava obliko zaupanja *trust*.

3.2 Opredelitev zaupanja

Enotna definicija zaupanja v času pisanja doktorske disertacije ni obstajala, zato je veliko različnih, vendar v določeni meri podobnih si definicij, kar ugotavljajo tudi Laeequddin et al. (2010, str. 55-56), ki so jih v metaanalizi obravnavali preko 40, McKnight & Chervany (2001) pa kar 65. Za takšno raznolikost in številčnost definicij obstaja več razlogov, vendar bomo našteli le tiste, ki so pomembni za naš sistemski vidik obravnavanja. Prvi razlog je dejstvo, da so zaupanje kot ključni element prepoznale različne znanstvene discipline (ekonomija, psihologija, menedžment, marketing, področje informacijske tehnologije idr.), zato so definicije področno usmerjene. Iz tega izvira naslednji razlog: raziskovalci so isti pojem obravnavali z različnih vidikov, zaupanje

pa so predstavili izključno s svojega vidika (McKnight & Chervany, 2001). S tem je povezan tudi naslednji razlog, in sicer *kontekst*, znotraj katerega obravnavamo zaupanje (npr. Olmedilla et al., 2006; Kovač & Trček, 2007; Little et al., 2007; Martin, 2014). Ta je namreč odvisen ne le od področja in vidikov, temveč tudi od okoliščin, ki so lahko – kljub enakemu področju in enakim vidikom – vsakokrat drugačne. Naslednji razlog so različni pogledi na pričakovanja (Mirzaie et al., 2012), ki pomembno vplivajo na zaupanje.

Našteli smo le nekaj razlogov, ki po našem mnenju predstavljajo temelj raznolikosti definicij, zagotovo pa obstajajo tudi drugi. Kot pravi Martins (2002), raznolikost definicij kaže, da gre za dinamičen pojav oziroma fenomen, ki je odvisen od različnih dejavnikov, ki vplivajo na strukturo modela zaupanja. Sam namreč trdi (ibidem), da je definicija zaupanja odvisna od obstoječih modelov in drugih definicij, ki se osredotočajo predvsem na gradnike oziroma sestavine dele zaupanja, kot so npr. integriteta, kompetentnost, odprtost, ranljivost, zanesljivost in pričakovanja ter na vlogo upnika in zaupnika. Zato predlaga svojo definicijo zaupanja: »Zaupanje je lahko definirano kot proces, v katerem se upnik zanaša na zaupnika (osebo ali skupino ljudi), ki deluje v skladu s specifičnimi pričakovanji, ki so pomembna za upnika, ne da bi (zaupnik, op. G. H.) izkoristil upnikovo ranljivost.« (Martins, 2002, str. 757) Zaupnik namreč ni nujno oseba, temveč je lahko kompetenca, sposobnost, oprema, tehnologija, izračun, družbeni sistem, varnost ipd. (Laeequddin et al., 2010). »Zaupanje je vselej povezano z nekim 'objektom', neko osebo (prijateljem, neko skupino, npr. kolegi), neko institucijo […] ali pa nekim sistemom […] kot kolektivnim subjektom.« (Toš, 2007, str. 369) Zaupamo lahko meteorologom, da so pravilno napovedali sončno vreme in da zato ne bomo mokri, če ne vzamemo dežnika, ko se odpravimo od doma. Zaupamo lahko zračni blazini v avtomobilu, da nas bo obvarovala v primeru prometne nesreče. Zaupamo lahko državi, da bo ustrezno skrbela za državljane in da jim ne bo škodovala. Zaupamo pa lahko tudi verjetnostnemu izračunu, da bomo z vplačilom izbranih loto številk zadeli glavni dobitek. Za namene raziskovanja našega izbranega problema smo se osredotočili le na zaupanje med eno in drugo osebo oziroma med osebo in organizacijo, zato smo zaupanje v objekte, procese, izračune, pojave in drugo izpustili iz obravnave.

Zaupanje je pomembna sestavina vseh družbenih procesov (Paliszkiewicz, 2011, str. 316) in vseh faz človeških odnosov (vzpostavljanja, vzdrževanja in razširjanja) tako med

posamezniki kot posamezniki in organizacijami (Kaptein, 1998). Burke et al. (2007, str. 609) so zaupanje razdelili na več vidikov, ki so odvisni od namena raziskovalca. Od teh vidikov (oziroma konteksta) je odvisno, kako posameznik obravnava zaupanje (ibidem):

- *kot osebno lastnost*: v vsakem posamezniku sta splošna težnja k pozitivni atribuciji dejanj drugih oseb in osnovna raven zaupanja, ki ga je posameznik pripravljen deliti s tistimi, s katerimi je v interakcijah;
- *kot nastajajoče stanje*: to stanje se nanaša na kognitivna, motivacijska in druga dinamična stanja ter deluje kot funkcija različnih dejavnikov (sistema, dodal G. H.), npr. vhodi, izhodi in procesi. Zaupanje v tem kontekstu je mogoče obravnavati kot odnos, ki se počasi ali pa hitro spreminja v odvisnosti od takratnih kontekstualnih dejavnikov in potreb. Zato lahko zaupanje prevzame vlogo vhoda ali izhoda;
- *kot proces*: zaupanje lahko razumemo kot proces, ki okrepi ali oslabi določena pomembna vedênja in odnose do nekoga/nečesa drugega.

Ne glede na kontekst so osrednji del zaupanja kot elementa človeških odnosov **pričakovanja.** Mayer et al. (1995) pravijo, da so za obstoj zaupanja med drugim ključna tudi lastna pričakovanja, ali kot pravijo Rousseau, Sitkin, Burt & Camerer (1998, str. 394): »Samozavestna pričakovanja in pripravljenost biti ranljiv sta kritični komponenti vseh definicij zaupanja.« Da je pričakovanje pomemben element zaupanja, je povsem logično, ni pa povsem samoumevno, o kakšnem pričakovanju govorimo. Tako Fukuyama (1995, str. 27) pravi, da je zaupanje pričakovanje, ki znotraj določene skupnosti izhaja iz navadnega in iskrenega sodelovalnega vedênja, ki temelji na skupnih normah pripadnikov skupnosti, Boon & Holmes (1991, str. 194) pa pravita, da je zaupanje stanje, ki vključuje pozitivna pričakovanja o motivih druge osebe glede na situacije, ki zasledujejo tveganja. Tudi Gambetta (1988, str. 217) pravi, da je zaupanje določeno pričakovanje, ki ga imamo glede na verjetno, torej pričakovano vedênje drugih. Hosmer (1995) zato govori o pričakovanjih ene osebe, skupine ali podjetja o etično upravičenem vedênju ali sprejemanju moralno pravih odločitev in dejanj na račun drugih oseb, skupin ali podjetij, zato je zaupanje pomemben dejavnik prepoznavanja in varovanja pravic in interesov članov družbe. Seveda ni nujno, da gre za etično in/ali moralno upravičeno vedênje in prave odločitve. Npr. načrtovalec terorističnega napada zaupa napadalcu, da bo ta zares izvedel napad. Za civilizirano družbo teroristični napad ni etično niti moralno

upravičeno vedênje oziroma prava odločitev, je pa moralno upravičeno vedênje z vidika (interne) morale teroristične organizacije in etično prava odločitev z vidika načrtovalca in napadalca. Ker na razumevanje, kaj je etično in kaj moralno, vplivajo individualni in družbeni dejavniki, ti pa so si med seboj različni (še posebej med različnimi kulturnimi okolji), menimo, da uporaba besednih zvez *etično upravičeno vedênje* in *sprejemanje moralno pravih odločitev* v prej navedeni definiciji lahko vodi v napačno razumevanje, če pri tem hkrati ne upoštevamo dejstva, da ne obstaja samo ena »prava« etika oziroma ena »prava« morala. Strinjamo se z bistvom definicije, in sicer da gre za dejanja, ki so za nekoga pomembna in v skladu z notranjimi prepričanji osebe, ta pa so lahko enaka, podobna ali popolnoma različna prepričanjem družbe, v kateri upnik deluje. Ker je pričakovanje za upnika nekaj pozitivnega, tudi če je sámo dejanje za ostale ljudi z moralnega ali etičnega vidika negativno, se lahko strinjamo s Hosmerjem (1995), da je zaupanje optimistično pričakovanje pozitivnega izida dogodka ali vedênja neke druge osebe (zaupnika). Pri tem kot alternativno razmišljanje Hosmer navaja Barberja (1983, v Hosmer, 1995, str. 282-283), ki namesto optimističnega pričakovanja pozitivnih izidov v nekem nepredvidljivem dogodku poudarja vlogo pogojev in predvidevanj, ki vplivajo na končni izid (navedli smo le bistveno, op. G. H.):

1. pričakovanje vztrajnosti in izpolnitve naravnega in obstoječega družbenega reda, v katerem se posameznik/posameznica nahaja;
2. pričakovanje tehnično kompetentnega izvrševanje vlog drugih oseb, povezanih s posameznikom/posameznico;
3. pričakovanje moralno korektnega izvrševanja vlog drugih oseb, povezanih s posameznikom/posameznico.

Pričakovanja, ki jih ima upnik do zaupnika, so torej različna od primera do primera, vsem primerom pa je skupno, da se od zaupnika pričakuje izpolnitev upnikovih pričakovanj ali želja v okviru določenih norm, predpisov, pravil znotraj določenega okolja ipd. V primeru nerealiziranih pričakovanj posameznik doživi **razočaranje**, ki s seboj prinaša določeno škodo za upnika. Ko ta *post festum* spozna, da je bodisi napačno presodil ali zanemaril dokaze ali pa čustva, prične z iskanjem razlogov, zakaj je prišlo do razočaranja. Če je posameznik razočaran (v primeru oblike zaupanja *trust*), nastopi notranja ali interna atribucije, saj mora razloge za negativne posledice poiskati v sebi – v svoji odločitvi za

eno od alternativ (Luhmann, 1988), ki je nastala kot rezultat presoje stanja lastnih čustev in misli ter nepopolnih dokazov. Navadno mislimo ali vsaj pričakujemo, da se zaupnik zaveda dejstva, da ravnanje v nasprotju z našimi pričakovanji nam povzroča razočaranje in škodo (Deutsch, 1958). Upnik ne samo da zaupa zaupniku, temveč do neke mere tudi misli, da je zaupnik dolžan izpolniti njegovo zaupanje (ibidem) oziroma da se upnik tega zaveda in da sprejema dolžnost varovanja upnikovih interesov (Hosmer, 1995). Na drugi strani pa ima zaupnik določeno svobodo in možnost, da razočara upnika in ne izpolni njegovih pričakovanj (Gambetta, 1988). Pojavita se dve zanimivi (retorični) vprašanji: je torej zaupnik »določen za prostovoljca«, da uresniči upnikova pričakovanja? Je takšno razmišljanje upnika upravičeno? Z izpostavljanjem razočaranju in s tem škodi je upnik **ranljiv**, odprt za negativne vplive ali posledice. Drugo vprašanje zato nasprotuje definiciji, da je zaupanje pripravljenost biti ranljiv (npr. Schoorman et al., 2007), saj pripravljenost biti ranljiv temelji na upnikovih pričakovanjih, da bo zaupnik izvedel ali opravil določena dejanja ali naloge, pomembna za upnika, *ne glede na upnikovo zmožnost nadzorovanja zaupnika* (Lane & Bachman, 1999, v Mun et al., 2011, str. 346). Tej definiciji po naši oceni manjka to, da mora upnik dopuščati obstoj razočaranja in od zaupnika ne sme in ne more zahtevati zgolj izpolnitev pričakovanj v smislu: »Druge možnosti dovoljenega končnega izida ni,« lahko pa si to želi. Potrebno je razumeti, da je z vidika obravnave zaupanja kot teoretičnega diskurza *pripravljenost biti ranljiv* bolj pomemben element od same ranljivosti. *Pripravljenost biti ranljiv* odraža posameznikovo soočenje in sprejetje dejstva, da bo ranljiv (za razočaranje). Če ga ne sprejme, ne bo tvegal in če ne bo tvegal, obstaja majhna verjetnost (ali pa ta verjetnost sploh ne obstaja), da se bodo njegova pričakovanja uresničila. Ne smemo pozabiti, da je posameznik »prisiljen« zaupati drugi osebi, ker sam ne more izpolniti pričakovanj. V tem kontekstu je zaupanje opredeljeno tudi kot »psihološko stanje, ki vsebuje namen sprejeti ranljivost, ki temelji na pozitivnih pričakovanjih o namenih ali vedênju drugega.« (Rousseau et al., 1998, str. 395) Tudi Fink Hafner, Krašovec & Kustec Lipicer (2002, str. 5) ugotavljajo, da naj bi bilo zaupanje »psihološki pojav prepričanosti v nekaj.«

Hosmer (1995) ugotavlja, da do zaupanja pride v situacijah, ko sta prisotna ranljivost zaradi interesov posameznika ter odvisnost od vedênja drugih ljudi. V običajni situaciji zaupanja bi na prvi pogled lahko ocenili, da pri zaupanju prihaja le do odvisnost upnika

od zaupnika, saj upnik potrebuje zaupnika za uresničitev pričakovanj, zaupnik pa od upnika ni odvisen. Kljub temu menimo, da do neke mere *lahko* pride tudi do soodvisnosti upnika in zaupnika. Upnik potrebuje zaupnika za uresničitev upnikove želje, zahteve oziroma pričakovanja (Rousseau et al., 1989). Do zadnjega trenutka ne ve, ali bodo njegova pričakovanja realizirana ali ne, zato vedno obstaja **tveganje**, da bo razočaran. Kot ugotavljajo Rousseau et al. (1998), je v večini definicij zaupanja z različnih področij ravno tveganje prvi pogoj, da lahko govorimo o obstoju zaupanja. Kot smo že ugotovili, zaupanje ne pomeni *tvegati*, temveč ***biti pripravljen tvegati*** (Mayer et al., 1995). V odnosu do pripravljenosti tvegati se zaupanje odraža kot pokazatelj, koliko tveganja je posameznik pripravljen sprejeti (Schoorman et al., 2007, str. 346). S tem posameznik oziroma upnik (sebi in drugim) ne priznava zgolj to, da potrebuje nekoga drugega, ki bo uresničil njegova pričakovanja, temveč tudi, da je pri tem pripravljen tvegati, da pričakovanja ne bodo uresničena.

Tveganje in ranljivost v zvezi z zaupanjem sta močno povezana z **negotovostjo**. Od sprejemanja negotovosti glede rezultatov pričakovanj je odvisno, koliko posameznik potrebuje drugo osebo, ki ji lahko zaupa. Za zaupanje je torej značilna negotovost, na drugi strani pa je pomemben del zaupanja tudi gotovost. Iskanje gotovosti ne pomeni, da je nekdo zainteresiran za zmanjševanje tveganj v zaupanju ali da želi prepoznati izide zaupanja (kot rezultat pričakovanj, op. G. H.). Pomeni, da bo posameznik iskal tista zagotovila, ki delajo določen izid, pričakovanja ali okoliščine zanesljive, npr. večji vložek na eno samo številko na ruleti sicer pomeni veliko tveganje in s tem negotovost, po drugi strani pa gotovost, da večji vložek prinaša tudi večji dobiček. Pri iskanju gotovosti si posameznik pomaga z lastnim znanjem in sposobnostmi, z mehanizmi, ki delajo zanesljive rezultate verjetnejše, ter s sposobnostmi in prizadevanji zaupnika (Kaptein, 1998).

»[P]ri zaupanju nikdar ne gre za to, da bi se negotovost operacionalizirala kot tveganje, kot po našem [avtor prispevka je Andrej Rus, op. G. H.] mnenju zmotno trdi Luhmann (1988). Tveganje zahteva informacijo, kalkulacijo, presojo, nadzorovanje, vodenje in upravljanje. V odnosu zaupanja, [sic] se izogibamo vsem tem korakom racionalnega upravljanja transakcij. […] Zaupanje pomeni, da akterji preprosto sprejmejo negotovost

[…] in z njo ne upravljajo neposredno, pač pa skušajo upravljati socialne odnose […]. Posebnost zaupanja je prav v tem, da negotovost ni racionalizirana v zbir ciljev, pogojev in procesov, ki bi skušali obvladati tveganje […].« (Rus, 2008, str. 74) Enako kot v podpoglavju 3.1 ponovno ugotavljamo, da procesov odločanja, ki se skrivajo v ozadju zaupanja (med njimi tudi proces zmanjševanja negotovosti in iskanja gotovosti), ne poganja matematika, temveč t.i. strategije za soočanje s tveganji v družbenih odnosih, ki temeljijo na podlagi tehtanja med racionalno izpeljanimi stroški in koristmi (Laeequddin et al., 2010).

Spoznali smo, da lahko govorimo o obstoju zaupanja, kadar so izpolnjeni določeni pogoji. Poleg pričakovanj, tveganj, ranljivosti, negotovosti in pripravljenosti sprejeti tveganja, ranljivost ter negotovost navajajo nekateri avtorji tudi druge pogoje; npr. Lucas (2005, str. 89-90) prepoznava štiri pogoje za obstoj zaupanja:

1. Zaupanje lahko obstaja le, če obstaja element negotovosti – če nekomu zaupaš, si pripravljen biti ranljiv.
2. Obstajati morajo pričakovanja o konkretnem rezultatu zaupanja – zaupnik bo deloval v skladu s pričakovanji upnika.
3. Upnik zaznava, da je zaupnik motiviran za delovanje v skladu z upnikovimi pričakovanji – zaupnik ima interese za uresničevanje upnikovih pričakovanj.
4. Obe strani (upnik in zaupnik) imata motive za uresničevanje pričakovanj nasprotne strani.

Na podlagi do sedaj obravnavane literature o zaupanju menimo, da lahko govorimo o obstoju zaupanja, kadar:

1. ima upnik **pričakovanja**, za katera želi, da so izpolnjena;
2. obstaja **negotovost**, zaradi katere je upnik prisiljen zaupati drugi osebi;
3. obstaja **tveganje**, da bo upnik **razočaran**, ker pričakovanja ne bodo izpolnjena, zaradi česar je **ranljiv**;
4. je posameznik zavestno **pripravljen tvegati**, da bo razočaran, je **pripravljen biti ranljiv** in je **pripravljen sprejeti negotovost**.

Za zaupanje naj bi bilo potrebno sodelovanje oziroma zaupanje naj bi bilo posledica uspešnega sodelovanja. Vendar obstaja tudi obratno stališče, in sicer da je zaupanje pogoj za sodelovanje. Zagovornik tega je tudi Gambetta (1988, str. 224-229), ki svoje mnenje med drugim utemeljuje z vojaki v jarkih med prvo svetovno vojno. Ti na sovražne vojake iz nasprotnih jarkov iz različnih razlogov (strah, namerno streljanje mimo nasprotnika, čas kosila, prazniki ipd.) niso vedno streljali, torej so med seboj sodelovali (ibidem). Kako je prišlo do takšnega sodelovanja, čeprav so nasprotniki in si zato ne morejo zaupati? Gambetta (1988) meni, da je do sodelovanja prišlo zaradi pravega zaporedja *korakov sodelovanja*, ki spominjajo na vedênje, kot da bi si vojaki med seboj zaupali. Ti koraki izhajajo iz pripravljenosti zaupati in osebnega prepričanja, da bo nasprotna stran sodelovala, na korake pa do neke mere vplivajo tudi skupna preteklost osebe z nasprotno stranjo, okoliščine in naključje (povzeto po Gambetta, 1988). Če strnemo bistvo avtorjeve razprave, kot jo razumemo mi: na sodelovanje (in začetek sodelovanja) bo vplivalo zaupanje ali vedênje, ki spominja na zaupanje, saj ima podobne znake. Kljub temu ugotavlja (ibidem, str. 226), da je zaupanje lahko tudi posledica sodelovanja, vendar le v primeru, ko se obe strani zavedata pritiska (za sodelovanje, op. G. H.) in obstaja motivacija za sodelovanje. Mayer et al. (1995) se ne strinjajo s stališčem, da je zaupanje nujen pogoj, da pride do sodelovanja. Menijo (ibidem), da je mogoče sodelovanje brez zaupanja, kadar ni nadzornih mehanizmov za kaznovanje neprimernega vedênja zaupnika, kadar upnik v situaciji sodelovanja ni ranljiv in kadar je jasno, da se upnikovi motivi za sodelovanje ne ujemajo z željami zaupnika. V takšnih situacijah je tveganje za upnika minimalno, zanemarljivo ali pa ga sploh ni, pri zaupanju pa je obstoj tveganja pogoj, da sploh lahko govorimo o zaupanju (ibidem). To je dodaten argument, zakaj sodelovanja ne moremo in ne smemo enačiti z zaupanjem. Sodelovanje niti ne pomeni obojestransko zaupanje, npr. nadrejeni zaupa delavcu, delavec pa ne zaupa nadrejenemu (Brower et al., 2000), vendar kljub temu sodelujeta. Cilj zaupanja je v večini primerov izboljšanje sodelovanja in s tem pridobivanjem (skupnih) koristi, pri čemer mora biti takšno sodelovanje prostovoljno (Hosmer, 1995), enostranskost in enostransko zaupanje pa ne omogoča pridobivanja vseh koristi. Zato je obojestransko zaupanje nujno potrebno, če želita obe strani doseči želeno (pričakovanja/cilji sodelovanja). Bolj kot si upnik in zaupnik zaupata, bolj bosta pripravljena sodelovati, s

tem pa bosta okrepila medsebojno zaupanje (Fukuyama, 1995). Zaupanje in sodelovanje sta torej sorodna pojma, vendar različna v svojem bistvu (Mayer et al., 1995).

Razmišljanje o vlogi sodelovanja v zaupanju nas je pripeljalo do pomembnega vprašanja, kako zaupati nekomu (posamezniku ali organizaciji), s katerim nismo sodelovali, ne sodelujemo in ne bomo sodelovali ali pa ne moremo sodelovati? Zastavljeno vprašanje postavlja pod vprašaj sodelovanje kot dejavnik, ki tvori situacijo, ko lahko govorimo o zaupanju. Poglejmo primer zaupanja v matične obveščevalno-varnostne službe: nekateri ljudje jim zaupajo, čeprav z njimi nikoli niso neposredno ali posredno sodelovali. V takšnem primeru ni bi mogli govoriti o zaupanju, če bi sodelovanje uvrščali med elemente zaupanja. Po našem mnenju kljub temu lahko govorimo o zaupanju, saj so prisotni drugi elementi: pričakovanja, tveganje, verjetnost razočaranja, ranljivost, negotovost, pripravljenost tvegati, pripravljenost biti ranljiv in sprejemanje negotovosti. Podobno se lahko enako vprašamo tudi glede zaupanja v organe pregona, v sodstvo, v politiko in politične stranke, v športnike itd. Tudi v teh primerih ni nujno, da je posameznik z njimi predhodno sodeloval, da jim lahko zaupa. V povezavi s sodelovanjem izpostavljamo posebej zanimivo definicijo zaupanja avtorjev Schlenker, Helm & Tedeschi (1973, str. 419), ki pravijo, da je zaupanje zanašanje na informacije, ki jih prejmemo od drugih oseb in se nanašajo na negotovosti ter izide negotovosti v tveganih situacijah. Podobno definicijo imata tudi Kovač & Trček (2007, str. 8): »[Z]aupanje [se] oblikuje na podlagi ugleda oz. priporočil drugih.« Obe definiciji dajeta odgovor na vprašanje, kaj lahko upnik stori, če nima lastnih izkušenj z zaupnikom. Upnik takrat težko presodil, ali zaupniku lahko zaupa, zato se zanese na podatke oziroma informacije drugih oseb, ki te izkušnje imajo oziroma *naj bi jih imeli*. Ni pa nujno, da bo upnik na podlagi informacij drugih oseb zaupal zaupniku v takšni meri, kot mu drugi. S tem in z argumentom Mayerja et al. (1995), da sodelovanja ne moremo enačiti z zaupanjem, ker pri sodelovanju ni vedno prisotno tveganje, okvirno utemeljujemo, da sodelovanje ni element, ki mora biti obvezno prisoten, da lahko govorimo obstoju zaupanja. Tudi sicer v obravnavani literaturi o zaupanju nismo zasledili, da bi avtorji (npr. Zucker, 1986; Hosmer, 1995; Kahan, 2001; Schoorman et al., 2007) uvrstili sodelovanje med elemente zaupanja, ga pa omenjajo v povezavi z zaupanjem.

Na podlagi obravnavane literature in naših argumentov smo za potrebe raziskovanja izoblikovali lastno delovno definicijo zaupanja, hkrati pa se strinjamo z avtorjema McKnight & Chervany (2001), ki menita, da je zaupanje zaradi njegove narave, širokega pomena in vsakdanje rabe težko strniti v eno samo definicijo. Naša definicija opredeljuje zaupanje v družboslovnem kontekstu (vidiku) in opredeljuje zaupanje upnika (posameznika) v zaupnika, tj. v drugo osebo, skupino ali organizacijo. Zavedamo se in hkrati bralce opozarjamo, da naša definicija ni edina oziroma »najbolj« pravilna, saj je nastala tako kot ostale definicije na področju zaupanja, pri katerih vsak avtor definicije meni, da se je najbolj približal celoviti definiciji zaupanja. Po našem prepričanju naša definicija ni primerna za področja, kjer je predmet preučevanja zaupanje posameznika v objekt, neživo strukturo, proces ali situacijo (npr. ekonomija, organizacija in menedžment, elektronsko poslovanje, bančništvo, informacijski sistemi), zato je potrebno biti previden, v kakšnem kontekstu se jo uporablja. Predlagana definicija zaupanja, ki je hkrati tudi naša delovna definicija zaupanja, se glasi:

*Zaupanje je **psihološko stanje** oziroma **prepričanje upnika**,*
*da bo zaupnik **izpolnil upnikova pričakovanja,***
*zato je **pripravljen sprejeti tveganja in biti ranljiv,***
*saj je zaupnika **ocenil kot ustrezno entiteto**, ki je to pripravljena in sposobna storiti.*

Osrednji element naše definicije je **upnikovo stanje** oziroma **prepričanje** in ne odnos med upnikom in zaupnikom (kar je npr. v Lane, 1998; Paliszkiewicz, 2011). Izhajamo iz stališča, da »[z]aupanje ni vedênje ali izbira, temveč psihološko stanje, ki lahko povzroči ali postane rezultat takšnih dejanj« (Rousseau et al., 1998, str. 395) ter da »temelji na osebnem in subjektivnem odnosu do ciljne entitete.« (Kovač & Trček, 2007, str. 8) Zato se ne strinjamo s tistimi avtorji (npr. Burke et al., 2007; Rus, 2008), ki pravijo, da je zaupanje odnos med upnikom in zaupnikom. Če naše stališče nekoliko drugače ponazorimo in argumentiramo:

zaupanje = psihološko stanje oziroma prepričanje posameznika

psihološko stanje posameznika ≠ (dvostranski) odnos med dvema subjektoma

torej

zaupanje ≠ (dvostranski) odnos med dvema subjektoma

V samem bistvu zaupanje razumemo in opredeljujemo kot **enostranski odnos**. Zaupnik sprva ne more vedeti, ali mu zaupamo, dokler mu tega ne pokažemo z **zaupljivim vedênjem** (razen če ima zaupnik sposobnost branja misli). Zaupljivo vedênje pojmujemo kot vsako ravnanje, ki izhaja iz upnikovega psihološkega stanja oziroma prepričanja, da bo zaupnik izpolnil njegova pričakovanja, ne glede na to, v koga je takšno vedênje usmerjeno (v zaupnika ali v druge osebe, procese, okoliščine ipd.). Z njim upnik kaže, da zaupniku zaupa. Do trenutka, dokler zaupnik ne bo zaznal in hkrati odgovoril na upnikovo zaupljivo vedênje, je zaupanje še vedno *enostranski* odnos. In tudi takrat, ko bo zaupnik odgovoril na takšno vedênje, še ne moremo vedno govoriti o soodvisnosti, temveč le o dvostranskem odnosu. »Kvantitativno« gre morda res za soodvisnost, saj sta za to potrebna dva subjekta, sicer pa ne, saj zaupnik ne izkazuje svoje odvisnosti do upnika, kadar od njega ni odvisen. Poleg tega moramo tudi upoštevati, da zaupnik morda ne zaupa upniku. Zato trdimo, da je koncept zaupanja, po katerem je mogoče zaupanje opredeliti kot stopnjo soodvisnost med upnikom in zaupnikom (tega je v literaturi zasledil Lane (1998)), pravilen le takrat, kadar gre dejansko za njuno soodvisnost in si obojestransko zaupata. Tudi sicer odvisnost še ne pomeni zaupanje. Za lažje razumevanje s tabelo 3.1 prikazujemo, kdaj v zaupanju prihaja do enostranskega ali dvostranskega zaupanja in odvisnosti ali soodvisnosti, kadar upnik zaupa zaupniku.

Tabela 3.1: Tip odvisnosti in smer zaupanja, kadar upnik zaupa zaupniku

	ZAUPNIK			
	ni odvisen od upnika in mu **ne zaupa (1)**	**je odvisen** od upnika in mu **ne zaupa (2)**	**je odvisen** od upnika in mu **zaupa (3)**	**ni odvisen** od upnika in mu **zaupa (4)**
tip odvisnosti	odvisnost (upnika)	soodvisnost	soodvisnost	odvisnost (upnika)
smer zaupanja	enostransko zaupanje (upnik)	enostransko zaupanje (upnik)	obojestransko zaupanje	obojestransko zaupanje

Vir: Osebni vir

O zaupanju lahko govorimo le takrat, ko potrebujemo drugi subjekt, da bi uresničil naša pričakovanja v določenih okoliščinah. Za to smo tudi pripravljeni tvegati in biti ranljivi. **Vendar to velja le za okoliščine, v okviru katerih pričakujemo izpolnitev naših pričakovanj** (določen čas, določen kraj, določene osebe, določene okoliščine itd.), ne pa tudi za druge okoliščine. Trditev, da nekdo na splošno zaupa nekomu drugemu sicer kaže, da je oseba pripravljena biti ranljiva in tvegati za namene uresničitve pričakovanj v kateremkoli kontekstu, vendar tega ne moremo posploševati na takšen način, saj bi to pomenilo, da je oseba v kateremkoli kontekstu odvisna od druge osebe. Navadno se zaupanje vzpostavi takrat, ko sami nečesa ne zmoremo storiti, kar pomeni, da o zaupanju lahko govorimo takrat, ko potrebujemo pomoč in smo prepričani, da nam lahko druga oseba pri tem pomaga. Če se nekoliko drugače izrazimo: odvisni smo (od drugih) le takrat, ko potrebujemo pomoč, ne pa tudi takrat, ko je ne potrebujemo. Za lažje razumevanje tega odstavka in tabele 3.1 navajamo nekaj situacij, v katerih oseba A (upnik) zaupa osebi B (zaupnik), da bo proti plačilu temeljito očistila kuhinjo (številka v oklepaju se nanaša na zaupnikovo stanje v tabeli 3.1):

- **Odvisnost osebe A od osebe B in enostransko zaupanje (1)**: oseba B ni odvisna od denarja osebe A niti ne zaupa osebi A.
- **Soodvisnost in enostransko zaupanje (2)**: oseba B je odvisna od denarja osebe A, ki ga lahko dobi le s čiščenjem kuhinje, vendar osebi A ne zaupa, ker dvomi, da ji bo plačala za čiščenje. Zato se oseba B odloči, da ne bo očistila kuhinje, čeprav je finančno odvisna od osebe A.
- **Soodvisnost in dvostransko zaupanje (3)**: oseba B je odvisna od denarja osebe A, ki ga lahko dobi le s čiščenjem kuhinje, zato jo bo očistila, ker osebi A zaupa, da ji bo plačala.
- **Odvisnost osebe A od osebe B in dvostransko zaupanje (4)**: oseba B ni odvisna od denarja osebe A, saj je finančno dobro preskrbljena, vendar zaupa osebi A, da ji bo plačala.

Enostransko zaupanje ni napačno, potrebno pa je vedeti, da zaupanje kot enostransko dejanje, odnos ali proces v družbenih sistemih navadno ne vodi k sodelovanju in k uresničitvi želenih ciljev upnika (Gambetta, 1988), zato ne prispeva h krepitvi socialnih/družbenih vezi. Rus (2008, str. 74) pravi, da je »[z]aupanje […] kvaliteta

socialnih odnosov.« Več kot je zaupanja, bolj kakovostni so lahko ti odnosi, bolj trdne so družbene vezi. Te so zagotovo pomembne za trajnostni razvoj družbe, kar še posebej velja za delovanje države kot entitete. Na področju nacionalnih interesov in nacionalne varnosti si škodljivih posledic ne moremo in ne smemo privoščiti. Pomembno je, da je zaupanje obojestransko in odnos soodvisen, kar vzpostavlja in krepi zaupanje. To velja tudi za odnos med državljani in matičnimi obveščevalno-varnostnimi službami, ki je bil po naši oceni, do katere smo prišli z opazovanjem in analizo aktualnih dogodkov na področju obveščevalno-varnostne dejavnosti v Sloveniji in po svetu v zadnjih nekaj letih, do sedaj obravnavan na enostranski način: na način, kot da med državljani in obveščevalno-varnostnimi službami sploh ni povezav, sodelovanja niti soodvisnosti. Dokazali pa smo, da bi med državljani in matičnimi obveščevalno-varnostnimi službami **morala obstajati** soodvisnost, poleg katere je potrebno tudi vzpostaviti obojestransko zaupanje.

3.3 Vrste zaupanja

Različni avtorji, ki jih obravnavamo v nadaljevanju, poznajo več vrst oziroma tipov zaupanja. Delitev izhaja iz analize zaupanja na individualni, medosebni/medskupinski in institucionalni/kulturni ravni (McKnight & Webster, 2001). V doktorski disertaciji smo obravnavali dve tipologiji. Prva razlikuje vrste zaupanja glede na t.i. konceptualni tip zaupanja (McKnight & Chervany, 2001). Ta zajema tri vrste zaupanja: **dispozicijsko**, **institucionalno** in **medosebno zaupanje** (ibidem). Druga tipologija zaupanja pa loči **kognitivno** in **afektivno zaupanje** (McAllister, 1995). Obstajajo tudi druge tipologije, ki pa se od tiste, ki smo jo uporabili mi, razlikujejo po tem, da vrste zaupanja razlikuje glede na različne dejavnike, npr. glede na način nastanka zaupanja (Lewicki & Bunker, 1996), glede na njegove temelje oziroma vire pričakovanj (zaupanje, ki temelji na procesih, na značilnostih ali na instituciji) (Zucker, 1985), glede na vire informacij (Rus, 2008), glede na vrsto zaupnika (Mirzaie et al., 2012) idr. Zaupanje, ki temelji na znanju, je vrsta zaupanja, ki je nismo obravnavali kot relevantno. Razlog za to so nasprotujoča si mnenja v literaturi, kaj takšna vrsta zaupanja predstavlja (npr. razlike med avtorji McKnight et al., 1998; Lewicki, Tomlinson & Gillespie, 2006; Paliszkiewicz, 2011). S tem ne bomo ničesar izpustili, saj uporabljena tipologija avtorjev McKnight & Chervany (2001) zajema

področji definiciji zaupanja, ki temeljita na znanju, vendar ju umešča v drugačen sklop oziroma komponente te tipologije. Med vrstami zaupanja, ki jih bomo predstavili, obstajajo nekatere razlike zaradi drugačnih subjektov/objektov, ki jim upnik zaupa, sicer pa so dejavniki, ki jih upnik presoja pri zaupniku, pri vseh vrstah podobni ali enaki, kar ugotavljajo tudi Laeequddin et al. (2010).

3.3.1 Dispozicijsko zaupanje

Dispozicijsko zaupanje temelji na (pre)dispoziciji oziroma težnji posameznika, da zaupa drugim (ne glede na osebo ali okoliščine) oziroma da ima splošno težnjo, da je pripravljen biti odvisen od drugih. Kljub temu ne pomeni, da bo oseba zaradi težnje zaupala tudi točno določenemu posamezniku, izkazuje le *težnjo* zaupanja ljudem *na splošno*. Dispozicijsko zaupanje oziroma stopnja dispozicijskega zaupanja se razvija in oblikuje z odraščanjem in izkušnjami. Ta vrsta zaupanja igra pomembno vlogo takrat, ko se oseba znajde v novi situaciji ali spozna nove ljudi (McKnight & Chervany, 2001).

Tvorita ga dve komponenti: *(za)upanje v človeštvo* in *naravnanost k zaupanju* (ibidem). Prva komponenta izkazuje stopnjo domnevanja ali prepričanja, da so druge osebe iskrene, dobronamerne, predvidljive ipd. (torej »dobre« z etičnega in moralnega vidika, op. G. H.) (ibidem), druga pa izkazuje domnevo, da lahko z drugimi osebami dosežemo boljše rezultate (ibidem), neodvisno od tega, ali so te osebe zanesljive ali nezanesljive (McKnight et al., 1998). Bolj kot bodo posamezniki zaupali drugim osebam, višja bo njihova raven dispozicijskega zaupanja (Lewin, 2003). Na obe navedeni komponenti vplivajo izkušnje z drugimi ljudmi (Rotter, 1967), zato se lahko sčasoma spremenita, kar se odraža kot manjše dispozicijsko zaupanje.

3.3.2 Institucionalno zaupanje

Institucionalno zaupanje odraža zaupanje v ugodne pogoje, ki omogočajo uspeh v tveganih situacijah in pri ljudeh ustvarja občutek relativne varnosti (McKnight & Chervany, 2001). Razlog za to so zagotovila, predpisi, varnostni mehanizmi, pogodbe, dogovori, situacije, vloge, strukture in drugi neosebni objekti (tj. objekti, na katere se

navezuje zaupanje, vendar to niso ljudje kot posamezniki, op. G. H.), ki ustvarjajo ali vplivajo na pogoje oziroma okolje (Laeequddin et al., 2010; McKnight et al., 1998; McKnight & Chervany, 2001;). »Institucionalno zaupanje namreč ne temelji […] na neposrednih ali posrednih odnosih med akterji, temveč je od teh odnosov neodvisno. […] [Z]ajema vse sedanje in prihodnje transakcije, hkrati pa nima moči, da bi neposredno izvajalo pritisk na vedênje partnerjev v konkretnih, partikularnih situacijah,« zato deluje kot »povezovalni mehanizem, ki negotovost iz medosebnih odnosov prenese na institucionalno raven in s tem med akterji vzbudi občutek gotovosti, kar predstavlja močno spodbudo za participacijo […].« (Rus, 2008, str. 84) Z ustvarjanjem ugodnih okoliščin pripomore, da posamezniki lažje zaupajo drugim (McKnight & Chervany, 2001). V tem smislu je institucionalno zaupanje definirano tudi kot *prepričanje*, da potrebne neosebne strukture posameznikom omogočajo delovanje v pričakovanju uspešnih prihodnjih prizadevanj (McKnight et al., 1998, str. 478). Motivacija za takšno zaupanje torej izhaja iz racionalne kalkulacije prihodnjih donosov (Rus, 2008, str. 87).

Institucionalno zaupanje ne odraža zaupanja v posameznike, temveč v ustanove (Rus, 2008) oziroma neosebne strukture, organizacije, okolja. Nekateri avtorji (npr. Paliszkiewicz, 2011; Rusu & Baboş, 2015) ga omenjajo kot *organizacijsko zaupanje*, ki opredeljuje zaupanje v organizacije na podoben način kot v osebe, vendar obstajajo različni pogledi na to, kdaj organizacijo prepoznati kot del institucionalnega zaupanja in kdaj kot del organizacijskega zaupanja. Za potrebe doktorske disertacije smo se odločili obravnavati organizacije kot del *institucionalnega* zaupanja, saj je ta raba bolj razširjena in se nam zdi tudi bolj smiselna, hkrati pa bi težko določili mejo, kdaj je organizacija kot »objekt« oziroma okolje in kdaj kot »subjekt« zaupanja. Zaupamo tudi drugim osebam znotraj takšnih neosebnih struktur, in sicer zaradi pričakovanja, da se bodo te osebe vedle in delovale enako, ker so del tega okolja (Rusu & Baboş, 2015). Ni nujno, da te osebe predhodno poznamo, da jim zaupamo. Vse to nakazuje na obstoj povezave med institucionalnim in medosebnim zaupanjem. Da je v praksi res tako, kaže primer, ki smo si ga izmislili, temelji pa na primeru letalske družbe in njenih uslužbencev, ki ga opisuje Sztompka (1999, v Rusu & Baboş, 2015, str. 177): Iz različnih virov smo izvedeli, da je določena banka zanesljiva in varna ter da svojim klientom omogoča kakovostne storitve. Na podlagi teh informacij se zato odločimo, da bomo banki zaupali svoj denar in da bomo

uporabljali njene storitve. Uslužbenke na bančnem okencu ne poznamo, vendar ji vseeno izročimo svoj denar in jo prosimo za izvedbo naročenih storitev. Zakaj smo ji izročili denar in jo prosili za izvedbo storitev, čeprav je nikoli prej nismo videli in ne moremo vedeti, ali ji lahko zaupamo? Razlog sedaj že poznamo: ker zaupamo banki, zaupamo tudi njenim zaposlenim, za tem pa se skriva princip vpliva institucionalnega zaupanja (zaupamo banki) na medosebno zaupanje (zaupamo bančni uslužbenki). Institucionalno zaupanje torej **ne sili posameznika**, da zaupa drugemu posamezniku, temveč le **ustvarja ugodne pogoje** oziroma **pripomore k temu**, da (laže) zaupa drugim. Ali kot pravi Rus (2008, str. 76): »O vedenju akterjev samo sklepamo na podlagi kakovosti institucionalnega okolja, pri čemer pričakujemo, da se bodo vsi akterji znotraj danega okolja vedli približno enako. Institucionalno zaupanje je torej zelo univerzalistično, saj lahko vsakdo na podlagi poznavanja sistema oblikuje enaka pričakovanja glede kateregakoli akterja v sistemu.« Obstaja pa tudi obratni vpliv: s tem, ko se krepi medosebno zaupanje, se krepi tudi zaupanje v institucijo, vendar »[k]dor zaupa posameznim osebam (npr. nosilcem funkcij), še ne zaupa nujno v institucije.« (Toš, 2007, str. 269)

Raven institucionalnega zaupanja je odvisna od posameznikovega zaznavanja institucionalnih (kontrolnih) mehanizmov kot tveganj (je tvegano/ni tvegano/se splača tvegati) (Laeequddin et al., 2010), predpogoj pa je, **da oseba institucijo sploh zazna** (Toš, 2007). Za zaupanje je potrebna vez, ki je lahko zgolj simbolična (članstvo v organizaciji/strukturi, registracije, prevzemanje standardov) (Rus, 2008). Za razliko od medosebnega zaupanja, kot bomo pojasnili kasneje, pri institucionalnem zaupanju niso potrebne vezi, saj je zaupanje utemeljeno na informacijah, ki prihajajo od institucij (ibidem) in od zaupanja vrednih posredovalcev (Toš, 2007). Zato upnik išče zaupnika na podlagi takšnih informacij, katerih verodostojnost se veča z zaupanjem v institucijo (Rus, 2008).

Tako kot dispozicijsko zaupanje tudi institucionalno zaupanje tvorita dve komponenti: ***strukturna zagotovila*** in ***običajnost situacije***. *Strukturna zagotovila* so prepričanja osebe v uspeh v določeni situaciji zaradi ugodne strukture okolja, ki je sestavljena iz obljub, pogodb, pravil/predpisov, zagotovil ipd. Ta vpliva na posameznika, da se je

pripravljen zanesti na organizacijo, saj (struktura) temelji na postopkih in procesih, ki delajo zadeve znotraj strukture varne in pravične glede na njene značilnosti in izhodišča. Druga komponenta, *običajnost situacije*, pa pomeni prepričanje v uspeh v tvegani situaciji, ker je situacija običajna oziroma ugodna in tako tudi vpliva na uspeh (McKnight et al., 1998; McKnight & Chervany, 2001). Prepričanje posameznika, da je situacija običajna, povzroči, da se posameznik udobneje počuti, zato tudi lažje zaupa drugim v tej situaciji (McKnight et al., 1998; McKnight & Chervany, 2001). Posameznik v negotovosti išče gotovost, ki pozitivno vpliva na stopnjo zaupanja (Rus, 2008). Vloga institucije (strukture, organizacije ipd.) je, da z institucionalnim zaupanjem poveča gotovost, ki jo bo zaznal posameznik. »Gotovost […] akterjem omogoča, da jim ni treba pridobivati zasebnih informacij o vsakem partnerju neposredno v osebnem stiku z njimi ali prek poizvedovanja v omrežju, temveč lahko relevantne informacije pridobijo iz javnih virov, saj jih zbirajo zanesljive, nepristranske in neodvisne ustanove.« (Rus, 2008, str. 77) Luhmann (1988) je zato institucionalno zaupanje poimenoval gotovost, Lane (1998) pa *sistemsko zaupanje*. Institucija je namreč sistem, s poznavanjem sistema in njegovih značilnosti pa ima posameznik možnost, da si sam izoblikuje mnenje, kaj lahko pričakuje od udeležencev oziroma akterjev sistema (Rus, 2008).

Goldsteen, Schorr & Goldsteen (1989) so na primeru nesreče v jedrski elektrarni Three Mile Island v ZDA dokazali, da na institucionalno zaupanje pomembno vpliva tudi dispozicijsko zaupanje. Tamkajšnji okoliški prebivalci niso zaupali uslužbencem jedrske elektrarne zaradi slabega dispozicijskega zaupanja, ki je vplival na njihovo razmišljanje in s tem dojemanje uslužbencev. Med drugim so ugotovili, da navedeno bistveno vpliva na dojemanje stresnih okoliščin in nesreč (ibidem). Primer kaže tudi na to, da prebivalci niso imeli informacij, zaradi katerih bi lahko (bolj) zaupali zaposlenim. Iz tega izhaja spoznanje, da se posamezniki v specifičnih situacijah, ko nimajo informacij (povezanih z institucionalnim zaupanjem), ki jih omenja Rus (2008), zanašajo na lastna prepričanja o svetu, kar se odraža kot (za)upanje v človeštvo (McKnight et al., 1998). V kolikor pa posameznik ima informacije, vendar ne od institucij ali od njihovih članov, pa so to navadno informacije, ki jih dobi od družbe.

3.3.3 Medosebno zaupanje

»Medosebno zaupanje je najpogosteje definirano kot pozitivno pričakovanje do vedenja drugih akterjev,« (Rus, 2008, str. 83) da se lahko zanesemo na njihove besede, obljube ter ustne ali pisne izjave (Rotter, 1967, str. 651). Opredelimo ga lahko tudi kot zaupanje v zaupnikove atribute, ki ga delajo vrednega zaupanja (McKnight & Chervany, 2001).

Medosebno zaupanje temelji na medosebnih odnosih, ki nastanejo z dolgotrajnimi interakcijami, zato deluje tudi kot vezni mehanizem za povezovanje skupnosti. S tem ustvarja trden normativni red, ki se ga vzdržuje s sistemom socialne kontrole in neformalnih sankcij. Medosebno zaupanje je odvisno od informacij o udeležencih, ki prihajajo preko močnih osebnih stikov z njimi. Ti stiki so nastali zaradi pozitivnih izkušenj (preteklost), vendar ne zaradi akumulacije več posameznih pozitivnih transakcij, temveč zaradi preteklosti specifičnega odnosa s transakcijskim partnerjem (tj. zaupnikom, op. G. H.), zato medosebni odnos vsebuje kakovost medosebnega odnosa. Iz tega izhaja, da upnika za zaupanje ne motivira presoja zmožnosti zaupnika in možnih koristi, ki bi jih imel od tega odnosa, temveč splošna naklonjenost in pozitivna naravnanost do zaupnika. Zato je medosebno zaupanje obravnavano tudi kot pozitivno pričakovanje do vedênja drugih (povzeto po Rus, 2008).

Na ravni posameznikov lahko pride do t.i. ***mrežnega zaupanja***, ki »temelji na šibkih vezeh in posrednih stikih med akterji. Deluje prek tretjih oseb, ki imajo svoje osebne zaveze zgolj do mediatorja, med samimi pogodbenimi strankami pa niso nujne.« (Rus, 2008, str. 83) Tovrstnega zaupanja ne smemo enačiti z medosebnim zaupanjem, saj je glavna razlika med njima ta, »da gre pri mrežnem zaupanju za socializacijo odnosa med akterjem [upnikom, op. G. H.] in partnerjem, saj poteka prek nekoga tretjega, vpleten je torej 'tertius'. […] Akter [upnik, op. G. H.] namreč do svojega partnerja [zaupnika, op. G. H.] vzpostavlja odnos zaupanja na podlagi informacij, ki jih ne dobi v neposrednih izkušnjah z njim, temveč se v celoti opre na informacije in priporočila tertiusa, ki ju povezuje. Zato tertius ali mediator ni samo tisti, ki daje priporočila in prenaša informacije, temveč hkrati ponuja poroštvo za verodostojnost partnerja.« (Rus, 2008, str. 79)

Medosebno zaupanje sestavljajo tri komponente, ki jih bomo na kratko povzeli glede na obrazložitev, ki jo podajata McKnight & Chervany (2001, str. 34-37):

1. ***Prepričanja glede zaupanja***: izraža obseg upnikovega prepričanja, da je konkretna oseba vredna zaupanja. Takšno prepričanje je povezano z občutkom relativne varnosti, da ima potencialni zaupnik ustrezne značilnosti, ki upniku lahko koristijo. Sestavljeno je iz štirih sub-komponent, pri katerih upnik presoja značilnosti določene osebne značilnosti:
   a. ***Prepričanje o kompetentnosti***: upnikovo prepričanje o sposobnostih ali močeh druge osebe, da uresniči upnikova pričakovanja.
   b. ***Prepričanje o benevolenci***: upnikovo prepričanje, da drugi osebi ni vseeno za ostale in da je motivirana za delovanje v skladu z interesi drugih.
   c. ***Prepričanje o integriteti***: upnikovo prepričanje, da druga oseba dela dogovore v dobri veri, govori resnico in izpolnjuje obljube.
   d. ***Prepričanje o predvidljivosti***: upnikovo prepričanje o predvidljivosti vedênja druge osebe oziroma o konsistentnosti pozitivnih ali negativnih dejanj osebe, ki omogoča napovedovanje dejanj te osebe v drugih situacijah.
2. ***Nameni za zaupanje***: izraža posameznikovo pripravljenost biti odvisen od druge osebe kljub odsotnosti nadzornih mehanizmov in možnosti negativnih posledic. Ta komponenta je sestavljena iz dveh sub-komponent:
   a. ***Pripravljenost biti odvisen***: oseba je rade volje pripravljena postati ranljiva za drugo osebo, ko se nanjo zanese, in ima hkrati občutek relativne varnosti.
   b. ***Subjektivna verjetnost odvisnosti***: izraža obseg, koliko oseba lahko predvidi ali napove njeno odvisnost od druge osebe in ima hkrati občutek relativne varnosti. Izraža bolj konkretno in trdno zavezo ter pripravljenost, da bo upnik odvisen od druge osebe.
3. ***Zaupljivo vedênje***: oseba je prostovoljno odvisna od druge osebe in ima kljub možnim negativnim posledicam hkrati občutek relativne varnosti. Odvisnost osebe se od tiste pri sub-komponentah *pripravljenost biti odvisen* in *subjektivna verjetnost odvisnosti* razlikuje v tem, da je pri sub-komponentah izražena *pripravljenost biti odvisen*, pri zaupljivem vedênju pa ne gre več le za pripravljenost, temveč za konkretno vedênje, ki izraža zaupljivost. S tem oseba pokaže, da je pripravljena

sprejeti tveganje (oziroma ga že sprejme, op. G. H.). Zaupljivo vedênje tvorijo naslednje sub-komponente:

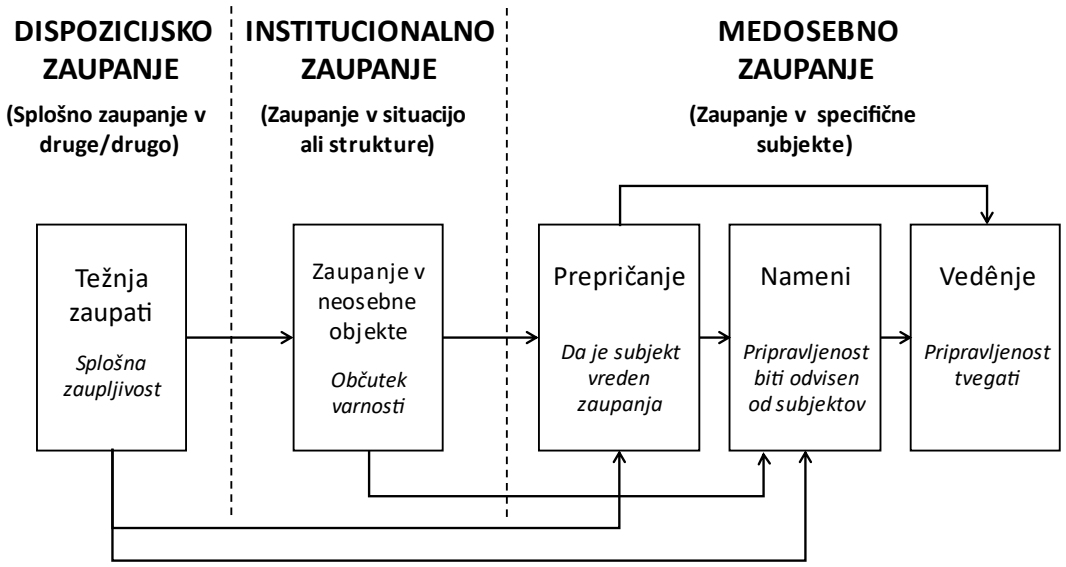
a. ***Sodelovanje***.
b. ***Deljenje informacij***: z deljenjem informacij upnik postane ranljiv, od zaupnika pa pričakuje, da jih bo varoval.
c. ***Neformalni dogovor***: dogovor o sodelovanju in zaupanju brez pogodbe.
d. ***Zmanjševanje nadzora***: s tem, ko oseba popušča pri nadzoru druge osebe (zaupnika), povečuje tveganje in ranljivost.
e. ***Sprejemanje vpliva***: upnik pusti, da zaupnik vpliva nanj, ker upa in verjame, da bo zaupnikovo mnenje pravilno (sicer bi v nasprotnem primeru tvegal negativne posledice).
f. ***Podeljevanje avtonomije***: upnik drugi osebi, ki ji zaupa, podeli (delegira, op. G. H.) moč odločanja, ki jo je prej imel sam. Upa, da se bo zaupnik prav odločil namesto njega.
a. ***Transakcija posla***: pri transakciji posla je upnik odvisen od zaupnika z dveh vidikov: 1) ali bo zaupnik uresničil upnikova pričakovanja in 2) ali bo zaupnik še naprej varoval upnikove informacije.

Vsaka od predstavljenih glavnih treh komponent (*prepričanja glede zaupanja*, *nameni za zaupanje* in *zaupljivo vedênje*) zavzema v konkretni situaciji določeno vrednost. Od njihove sinergije, ki nastaja kot posledica soodvisnosti, pa je odvisno, kako močno bo medosebno zaupanje kot končni rezultat.

3.3.4 Povezovanje dispozicijskega, institucionalnega in medosebnega zaupanja

Vrste/tipi zaupanja, ki smo jih obravnavali v okviru tipologije avtorjev McKnight & Chervany (2001), lahko med seboj povežemo, kar smo nakazali že med opisom posameznih vrst zaupanja. Njihove medsebojne povezave oziroma vplive prikazuje slika 3.2.

Slika 3.2: Interdisciplinarni model konstruktov zaupanja

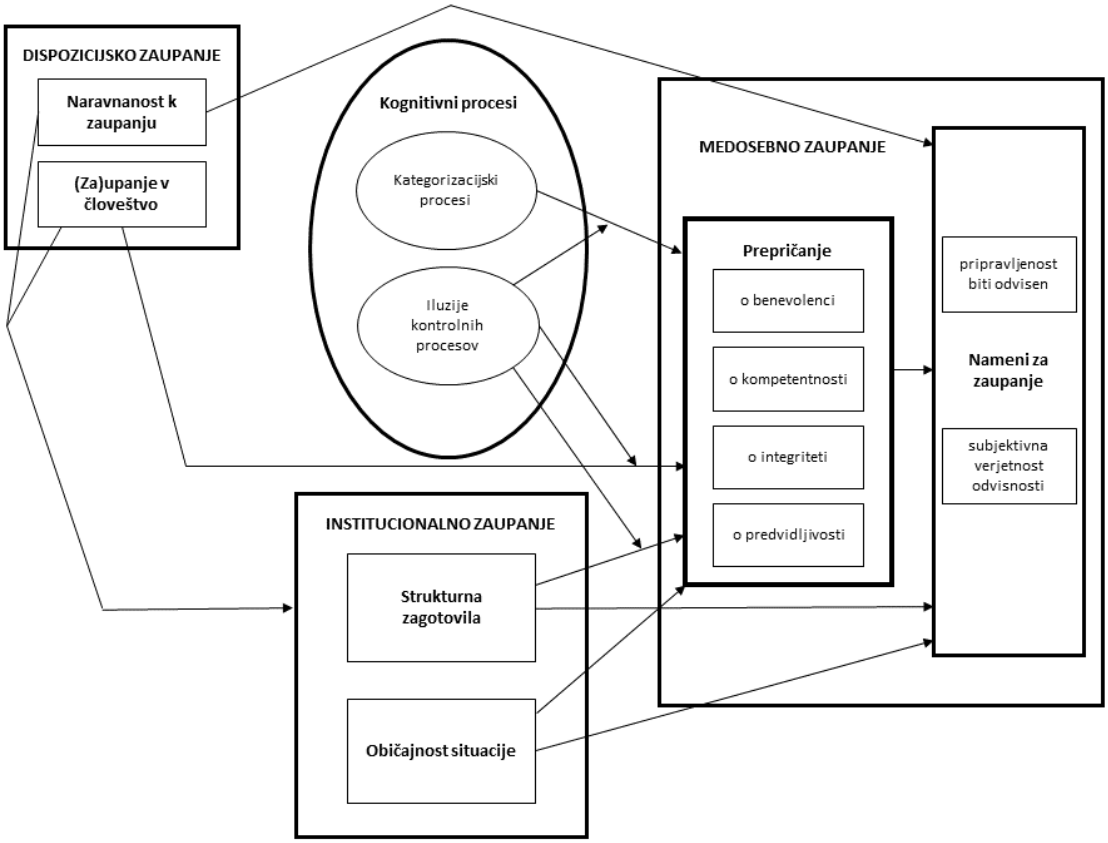


Vir: Prirejeno po McKnight & Chervany, 2001, str. 33

Kot prikazuje slika 3.2, se zaupanje razvije zaradi dispozicijskega zaupanja in institucionalnega zaupanja. Ni pa razvidno, kako posamezne komponente vplivajo na druge komponente in vrste zaupanja, zato predstavljamo drugačno shemo (slika 3.3). Ta je, kronološko gledano, predhodnica sheme na sliki 3.2, vendar prikazuje tudi posamezne komponente in njihove vplive ter vpliv kognitivnih procesov, ki jih na sliki 3.2 ni. Koncept avtorjev McKnight et al. (1998, str. 476) smo preoblikovali tako, da smo namesto *o integriteti* napisali *o iskrenosti*, saj je iskrenost del integritete, kot sta kasneje napisala McKnight & Chervany (2001), dva od treh avtorjev prvotnega koncepta (McKnight et al., 1998). V desni, večji okvir smo namesto *Zaupanje*, kot je napisano v izvirniku (tj. McKnight et al., 1998), napisali *Medosebno zaupanje* (glej sliko 3.3). Avtorji (ibidem) so model začetne izgradnje zaupanja namreč razvili za potrebe vzpostavitve zaupanja in za razvoja obstoječega zaupanja. Čeprav se strinjamo, da je *Zaupanje* končni rezultat celotnega procesa izgradnje (medosebnega) zaupanja, je *Zaupanje* preveč splošen izraz, desni, večji okvir pa očitno prikazuje komponente medosebnega zaupanja. Po do sedaj analizirani literaturi menimo, da je zaupanje lahko rezultat institucionalnega zaupanja ali dispozicijskega zaupanja, ne le medosebnega zaupanja, zato smo *Zaupanje* spremenili v *Medosebno zaupanje*. Če izhajamo iz uporabljene tipologije, je zaupanje

nenazadnje rezultat medsebojnih vplivov dispozicijskega, institucionalnega in medosebnega zaupanja.

Slika 3.3: Model začetne izgradnje zaupanja



Vir: Osebni vir (koncept je povzet po McKnight et al., 1998, str. 476 ter dopolnjen z McKnight & Chervany, 2001 in z lastnimi dopolnitvami)

Pomembna komponenta koncepta na sliki 3.3, ki je ne najdemo na sliki 3.2, so ***kognitivni procesi***. Ti so sestavljeni iz *kategorizacijskih procesov* in *iluzij kontrolnih mehanizmov*. Pred nadaljnjim branjem o kognitivnih procesih je potrebno upoštevati, da so ti težje določljivi (Toš, 2007). *Kategorizacijski procesi* vplivajo na prepričanja o zaupniku, koliko mu lahko zaupamo. Ti procesi so (McKnight et al., 1998, str. 480-481):

1. *Uvrščanje v skupine*: procesi, s katerimi upnik umešča zaupnika v isto skupino, v kateri je tudi sam (npr. interesna področja, delo, znanje, sposobnosti). S tem, ko so zaupniki v isti skupini kot upniki, jim upniki hitreje in bolj zaupajo.

2. *Kategorizacija glede na ugled*: upnik dodeli zaupniku atribute glede na informacije o zaupniku iz »druge roke«. Večji ugled kot ima zaupnik, hitreje in bolj mu bo upnik zaupal.
3. *Stereotipiziranje*: umeščanje zaupnika v določeno kategorijo ljudi glede na stereotipe. Zaradi pozitivnih stereotipov, ki jih upnik pripiše zaupniku, lahko upnik tvori pozitivna prepričanja v upnika.

Na prepričanje, koliko upnik lahko zaupa zaupniku, vpliva tudi napačna ali pretirana upnikova percepcija, da ima kontrolo nad negotovo situacijo, čemur Langer (1975, v McKnight et al., 1998, str. 481) pravi *iluzije kontrolnih mehanizmov*. Te so lahko nevarne, saj upnik zaradi zmotne zaznave prične iskati potrditve za svoja prepričanja, ki mu dvignejo samozavest, s tem pa postanejo prepričanja, koliko lahko zaupamo zaupniku, zelo visoka (McKnight et al., 1998). V praksi se bo pokazalo kot zmotna percepcija o zaupnikovi benevolenci, kompetentnosti, integriteti in predvidljivosti. Upnik lahko doseže takšno prepričanje s preverjanjem, koliko lahko vpliva na zaupnika (v izvirniku: *token control efforts*), npr. pripravi zaupnika, da se nasmeje (ibidem). To upnik uporabi, ko ne ve, ali je zaupnik vreden zaupanja, nato pa si ustvari neutemeljeno lastno prepričanje o pozitivni kategorizaciji in strukturnih zagotovilih (ibidem).

V obravnavanem konceptu manjka komponenta *zaupljivo vedênje* (in njene sub-komponente), ki sta jo v model povezovanj različnih vrst zaupanja vključila McKnight & Chervany (2001). Te po našem mnenju manjkajo, ker so avtorji modela iz leta 1998 (McKnight et al., 1998) pripravili model za začetek izgradnje zaupanja, ko zaupljivega vedênja do subjekta/objekta še ni, saj mora posameznik najprej priti do odločitve, ali zaupa ali ne, šele nato pa pride do vedênj in dejanj. To lahko razumemo na način, da zaupljivo vedênje ni pogoj, da zaupanje obstaja, saj lahko zaupanje obstaja zgolj v obliki misli ali mnenja; nekomu lahko zaupamo, tudi če mu tega ne pokažemo s svojim vedênjem (sodelovanje, deljenje informacij, neformalni dogovori idr.). Kljub temu zagovarjamo stališče, da zaupanje vpliva na naše razmišljanje ***in*** na naše vedênje, če ne drugače pa vsaj tako, da smo zaupniku bolj naklonjeni in sprejemamo njegove vplive (tudi če zaupnik tega ne more opaziti ali ne opazi). Zato menimo, da je v splošni model

zaupanja potrebno vključiti tudi vedênje posameznika, kot sta to naredila McKnight & Chervany (2001).

3.3.5 Kognitivno in afektivno zaupanje

Kognitivno zaupanje temelji na prepričanjih upnika o zanesljivosti (McAllister, 1995) ter kompetentnosti upnika, torej prihaja »iz glave« (Chua, Ingram & Morris, 2008), iz razuma. Vzpostavljeno je na podlagi znanja, ki ga posameznik pridobi z opazovanjem druge osebe in iz zaznanega ugleda druge osebe (Johnson & Grayson, 2005). S kognitivnim zaupanjem se povečuje tudi afektivno zaupanje (ibidem). Primerjava nekaterih dejavnikov kognitivnega zaupanja in dejavnikov medosebnega zaupanja na sliki 3.3 razkriva, da gre za podobne oziroma enake dejavnike. Ne moremo trditi, da so McKnight et al. (1998) pri medosebnem zaupanju (namerno) spregledali afektivnost oziroma čustveno komponento zaupanja, lahko pa trdimo, da je ta komponenta vplivna in nujna, vendar v njihovem modelu manjka (izvirnik modela je predstavljen v poglavju 3.4).

Druga vrsta zaupanja je ***afektivno zaupanje***, ki prihaja »iz srca« (Chua et al., 2008) in temelji na medsebojni skrbi (McAllister, 1995), čustvih, občutjih in motivih, povezanih z drugo osebo (Chua et al., 2008). Nanj vplivajo tudi prijateljstvo (ibidem), upnikov altruizem, število interakcij med upnikom in zaupnikom (McAllister, 1995), občutek varnosti v odnosu, zaznana moč odnosa, izkušnje in tudi zaupnikov ugled (Johnson & Grayson, 2005). Afektivno zaupanje povečuje upnikovo percepcijo, da je zaupnik motiviran za izvedbo dejanj (ibidem), ki lahko upniku koristijo. Odraža na čustvih temelječe zanašanje na partnerja, zato ne potrebuje dokazov, saj predstavlja tisto vrsto zaupanja, ki ji z angleškim izrazom pravimo *faith* (verovanje). Sedaj lahko ponovno pojasnimo izbiro angleškega izraza *trust* za namene našega raziskovanja: izraz *trust* pomeni pričakovanje ali prepričanje, ki temelji na **intelektu** in **čustvih** (Judge, 1999) ter nepopolnih oziroma nepojasnjenih dokazih (Hart, 1988). **Kognitivno** zaupanje je tisto, ki izhaja iz upnikovega ***intelekta***, **afektivno** pa tisto, ki izhaja iz upnikovih ***čustev***, torej lahko potrdimo, da izbrani tipologiji skupaj tvorita koncept *trust,* tj. razmerje med dokazi in čustvi – ljudje nismo stroji brez čustev, vendar smo kljub temu razumska bitja. S tem

tudi dokončno dokazujemo ustreznost izbire z našega vidika relevantnih tipologij zaupanja.

3.4 Izbrani splošni in specifični modeli zaupanja

Obravnava različnih definicij in vrst zaupanja je bila potrebna za izoblikovanje delovne definicije zaupanja ter za izbiro splošnih (generičnih) in področno-specifičnih modelov zaupanja izmed preučevanih modelov. S preučevanjem izbranih modelov smo iskali dejavnike, s katerimi smo kasneje izgradili model zaupanja državljanov v matične obveščevalno-varnostne službe. Analizirali smo različne modele (Brower et al., 2000; Burke et al., 2007; Corritore, Kracher & Wiedenbeck, 2003; Doney, Cannon & Mullen, 1998; Fink Hafner et al., 2002; Hoffman, Lawson-Jenkins & Blum, 2006; Hurley, 2006; Jackson & Bradford, 2010; Kenning, 2008; Kovač & Trček, 2007; Križman, 2009; Martin, 2014; Martins, 2002; Mayer et al., 1995; McKnight & Chervany, 2001; McKnight et al., 1998; McKnight & Webster, 2001; Mirzaie, Fesharaki & Daneshgar, 2011; Morgan & Hunt, 1994; Mun et al., 2011; Rousseau et al., 1998; Salminen & Ikola-Norrbacka, 2010; Salo & Karjaluoto, 2007; Schiffman et al., 2010; Tan & Thoen, 2001; Van de Walle, 2007; Zand, 1972), ki smo jih našli v javno dostopni literaturi. Med njimi ni takšnega, ki bi obravnaval zaupanje v obveščevalno-varnostne službe. Po analizi modelov zaupanja smo ugotovili, da so obravnavani avtorji različno strukturirali splošne in specifične modele zaupanja ter da različno vrednotijo in vanje uvrščajo posamezne sestavine. Za nadaljnje raziskovanje smo zato izbrali tiste, ki so z našega vidika sistemskega obravnavanja relevantni (niso tehnični, niso matematični, so razumljivi, smiselni in znanstveno utemeljeni, vsebujejo elemente, ki se pojavljajo tudi pri drugih modelih, smiselno dopolnjujejo druge modele).

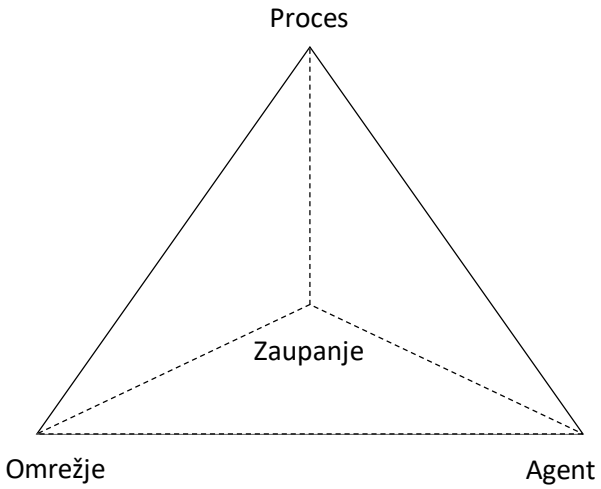
Obravnavo izbranih modelov pričenjamo s Capra kognitivnim ogrodjem. Temelji na biološki definiciji kognicije: poznavanje/védenje v življenju, kako in katere zmogljivosti živi organizmi uporabljajo za preživetje (Mirzaie et al., 2012, str. 198) oziroma kako ti uporabljajo kognicijo za življenje (Mirzaie et al., 2011). Orodje je uporabljeno za razumevanje bioloških in družbenih pojavov s štirih vidikov (ibidem):

1. *vzorec*: odnosi med sestavnimi deli sistema;

2. *struktura*: materialno utelešenje vzorca sistema. Ta se pri živih organizmih razvije z njihovo interakcijo z okoljem;
3. *življenjski procesi*: integracija perspektiv vzorcev in strukture;
4. *pomen*: ko so življenjski procesi umeščeni v družbeno okolje, pridobijo prvi trije vidiki pomen.

Capra kognitivno ogrodje naj bi omogočalo raziskovanje kateregakoli kompleksnega družbenega pojava (tudi zaupanja) z vseh štirih vidikov (ibidem). Mirzaie et al. (2012) so za modeliranje zaupanja izraz *vzorec* nadomestili z izrazom *omrežje*, ker človeški odnosi, ki so podobni vzorcem, tvorijo omrežje, izraz *struktura* pa z izrazom *agent*. »Agent je subjekt, ki lahko v kompleksnem modeliranju sistema predstavlja celico, človeka ali katerekoli žive organizme,« (Mirzaie et al., 2011, str. 182) torej živo strukturo, ki ima svoje lastnosti, ki se razvijajo skozi življenje (Mirzaie et al., 2012). Bistvo modeliranja zaupanja predstavlja zaupanje (ibidem), ki lahko v osnovni obliki Capra kognitivnega ogrodja nadomesti izraz *pomen*.

Slika 3.4: Štiri perspektive Capra kognitivnega ogrodja



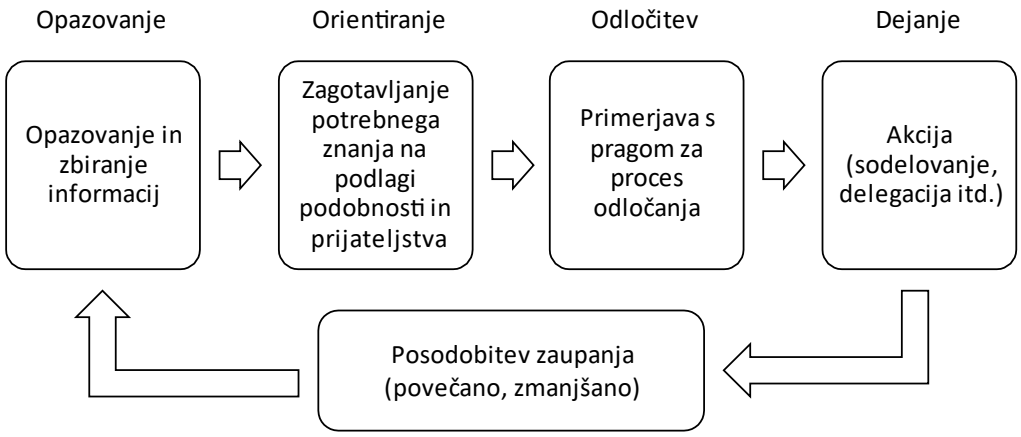
Vir: Mirzaie et al., 2012, str. 199

Njihov predlagani okvir kognitivnega orodja, ki ga lahko obravnavamo kot model zaupanja (slika 3.4), prikazuje, da zaupanje temelji na treh vidikih – agentu, omrežju in procesu:

a) *Agenti* predstavljajo ljudi v družbi, zato ima vsak agent tri parametre oziroma lastnosti: *specialnost*, *odgovornost* in *osebnost* (Mirzaie et al., 2012). Avtorji (ibidem, str. 202) predlaganega modela so s pomočjo računalniške simulacije npr. ugotovili, da specialnost in odgovornost oseb (zaupnikov, op. G. H.) vodita k povečanju zaupanja, hkrati pa zaupanje ne more biti razvito, če osebe niso odgovorne.
b) *Omrežje* sestavljajo med seboj povezani agenti (ljudje). Ko posameznik nekaj potrebuje, pošlje prošnjo/zahtevo ostalim prijateljem ali znancem, ki so člani omrežja. S tem se utrdijo določene povezave, zato takšno omrežje predstavlja matriko z obteženimi vrednostmi, kar omogoča merjenje zaupanja enega agenta v drugega (Mirzaie et al., 2012). Večje kot je zaupanje, večja je verjetnost, da bo agent drugemu agentu delegiral izpolnitev svoje potrebe (ibidem).
c) Glavni *proces* zaupanja je sprejemanje odločitev, komu (ne moremo) zaupati in zakaj (ne). V tem procesu se ocenjuje drugo osebo, rezultate pa se primerja s pragom, ki ga ima upnik ponotranjenega. Če rezultat presega prag, osebi lahko zaupamo, v nasprotnem primeru pa ne. Na določitev praga vpliva tip sprejemanja odločitev oziroma odločevalca (npr. če je prag višji, je oseba pesimistična, če pa je nižji, pa je oseba optimistična) (Mirzaie et al., 2012).

Capra model uporablja OODA zanko (ang. *Observe, Orient, Decision, Act*), po slovensko OOOD zanko (*Opazovanje, Orientiranje, Odločitev, Dejanje*; v nadaljevanju: OOOD). Slika 3.5 prikazuje, kako agent z opazovanjem okolja (*Opazovanje*) ustvari znanje (*Orientiranje*), se na podlagi znanja odloči (*Odločitev*) in izvede svojo odločitev (*Dejanje*). Dejanja vplivajo na trenutno stanje zaupanja, ki se lahko poveča ali zmanjša (Mirzaie et al., 2012). V izvirniku je v spodnjem okviru OOOD zanke (*Posodobitev zaupanja*) uporabljen izraz *katastrofalno* (ang. *catastrophic*), ki pa se nam ni zdel ustrezen, saj deluje nekoliko pretirano, zato smo ga nadomestili z izrazom *zmanjšano*.

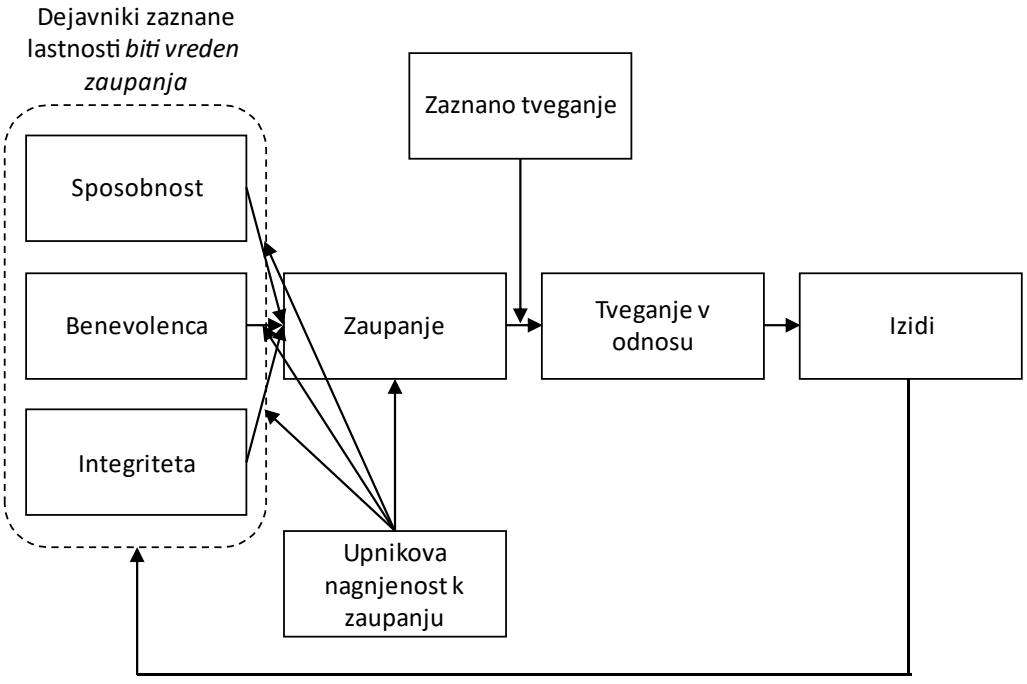
Slika 3.5: Proces OOOD



Vir: Mirzaie et al., 2012, str. 201

Naslednji model zaupanja, ki smo ga obravnavali, so razvili Mayer et al. (1995). Je prvi model, ki je predlagal preučevanje značilnosti upnika in zaupnika (ibidem). Njegovo strukturo prikazuje slika 3.6.

Slika 3.6: Model zaupanja (Mayer et al., 1995)



Vir: Mayer et al., 1995, str. 715

Na skrajni levi strani modela so prikazani trije dejavniki, ki skupaj tvorijo skupino 'zaznane lastnosti *biti vreden zaupanja*'. V izvirniku in tudi v drugi literaturi so avtorji za te tri dejavnike uporabili izraz *predhodniki zaupanja*, saj predstavljajo elemente, ki so predhodno potrebni za zaupanje. Namesto izraza *predhodniki zaupanja* smo uporabili splošen izraz *dejavniki zaupanja*, ki je bil uporabljen tudi za preostale dejavnike. Ti trije dejavniki, ki jih upnik presoja pri zaupniku glede na zaznane zaupnikove lastnosti, so ***sposobnost, benevolenca*** in ***integriteta***. Avtorji modela (ibidem) ugotavljajo, da se v literaturi o zaupanju najpogosteje pojavljajo ravno ti dejavniki. ***Sposobnost*** predstavlja skupino veščin, kompetenc in drugih značilnosti, ki osebi omogočajo imeti vpliv na določenem področju (ibidem, str. 717), na modelu pa označuje upnikovo zaznavo zaupnikovih sposobnosti. Vpliv zaupnik dosega in uveljavlja z delom, ki je specifično zaradi področja. Zato je sposobnost vezana točno na določeno področje in je ni mogoče generalizirati za vsa področja. Primer: mehaniku zaupamo, ker je sposoben popraviti avto, vendar to ne pomeni, da mu zaupamo katerokoli delo (npr. popravilo vodovodne napeljave). ***Benevolenca*** pomeni dobrohotnost, naklonjenost (Benevolenca, b. d.), v modelu pa označuje percepcijo pozitivne naravnanosti zaupnika do upnika (Mayer et al., 1995). Enako kot sposobnost in benevolenca je tudi ***integriteta*** dejavnik, ki odraža upnikovo percepcijo, koliko se zaupnik drži določenih načel in koliko so ta načela sprejemljiva za upnika (ibidem). Izpolnjena morata biti oba pogoja, da je zaupnik zaznan kot nekdo z integriteto. Če se zaupnik drži določenih načel, ima osebno integriteto (McFall, 1987 v Mayer et al., 1995), vendar če ta načela upniku niso všeč, zaupnik po njegovem mnenju nima integritete.

Upnikova percepcija ni zagotovilo, da je zaupnik dejansko takšen, kot ga upnik zaznava, temveč zgolj pomeni, da obstaja verjetnost, da je zaupnik takšen. To velja za obe možnosti: kadar upnik pozitivno in kadar negativno oceni zaupnika. Zato je priporočljivo, da se lastnost *biti vreden zaupanja* obravnava kot kontinuum, v katerem se obravnavani trije dejavniki spreminjajo, in ne samo z dvema možnostma: je vreden zaupanja ali ni vreden zaupanja (Mayer et al., 1995).

Na zaznano zaupnikovo sposobnost, benevolenco in integriteto vpliva tudi *upnikova nagnjenost k zaupanju*. Izraža splošno pripravljenost upnika, da zaupa drugim osebam,

in stopnjo pričakovanja, da so te osebe vredne zaupanja (ibidem). Ljudje smo različno nagnjeni k zaupanju, saj na nagnjenost vplivajo različni dejavniki, npr. kultura, okolje, izkušnje, osebnost (ibidem).

Brower et al. (2000) so izdelali podoben model kot Mayer et al. (1995), a so namesto *nagnjenost k zaupanju* uporabili dejavnik *nagnjenost k povezovanju/poistovetenju*. Njihov model je predstavljen kasneje, vendar jih tem mestu omenjamo zaradi njihovega mnenja, da je *nagnjenost k zaupanju* oziroma k *povezovanju/poistovetenju* dinamičen koncept (to pa zaradi odvisnosti od kulture, izkušenj, osebnosti idr.), ker se spreminja z doživetji. To je tudi glavni razlog, zakaj se ljudje različno odzovejo na isto osebo ali organizacijo, ko se je potrebno odločiti, ali zaupati ali ne. Zaradi tega je nagnjenost k zaupanju razumljena tudi kot temelj odnosa (Brower et al., 2000). Ključna lastnost modela na sliki 3.6 je, da lahko na podlagi nagnjenosti k zaupanju pojasni zaupanje, še *preden* upnik in zaupnik razvijeta odnos. Kljub temu je potrebno upoštevati, da upnik z vzpostavljanjem odnosa z zaupnikom pride do novih podatkov in informacij, ki lahko spremenijo njegovo mišljenje o zaupniku. Preden in medtem ko upnik vzpostavlja zaupanje (ter tudi kasneje, op. G. H.), pridobiva podatke o zaupniku predvsem iz drugih virov in (navadno) ne neposredno od zaupnika. Težje je pridobiti podatke o zaupnikovi benevolenci, zato je v zgodnejših stopnjah tvorjenja zaupanja večji del presoje osredotočen na podatke o zaupnikovi integriteti. Z razvojem zaupanja upnik pride do novih podatkov o zaupnikovi benevolenci (pa tudi o integriteti in sposobnosti). Ti lahko povečajo ali pa zmanjšajo zaupanje, zato lahko razvoj odnosa spremeni pomembnost dejavnikov, ki vplivajo na presojo, ali je oseba vredna zaupanja (ibidem).

Ugotovili smo, da je definicija zaupanja odvisna od konteksta, iz česar sledi, da je presoja sposobnosti, benevolence in integritete odvisna od konteksta, kar ugotavljajo tudi Mayer et al. (1995). Percepcija in kontekst imata največji vpliv na presojo, ali je nekdo vreden zaupanja, zato je zaupanje dinamično in se nenehno spreminja, saj se spreminja tudi kontekst, ki ga upnik zaznava in razlaga po svoje. Potrebno je tudi upoštevati, da sta upnikova percepcija, koliko je zaupnik vreden zaupanja, in nagnjenost k zaupanju dva različna dejavnika. Slednji ne pomeni nagnjenost k točno določeni osebi, organizaciji ali

stvari, temveč na splošno. Le takrat, ko navedena dejavnika združimo, dobimo obseg, koliko je upnik pripravljen zaupati točno določenemu zaupniku (ibidem).

Slika 3.6 tudi prikazuje, da zaznana tveganja vstopijo v proces ***po*** formiranju zaupanja. Ta del modela v izogib napačni interpretaciji potrebuje podrobno pojasnilo. Mayer et al. (1995) pravijo, da o pripravljenosti tvegati lahko govorimo, ko upnik še ni vstopili v situacijo, ko bi po njegovem prepričanju tudi dejansko tvegal. Ker je zaupanje enako kot biti pripravljen tvegati (ibidem), izraža pravokotnik *Zaupanje* ***pripravljenost tvegati***, puščica, ki izhaja iz pravokotnika v naslednji korak, pa vstop upnika v tvegano situacijo. Vmesna puščica izhaja iz pravokotnika *Zaznano tveganje*, pri čemer se zastavlja vprašanje, zakaj namesto tega ne piše *Tveganje*. Za odgovor je potrebno analizirati naslednji korak procesa – *Tveganje v odnosu*. To tveganje je po mnenju Mayerja et al. (ibidem) izhod oziroma rezultat zaupanja, pri čemer je stopnja zaupanja dejavnik, ki vpliva na upnikovo pripravljenost tvegati v odnosu. *Tveganje v odnosu* izraža upnikovo pripravljenost, da je ranjen, in razočaran (ibidem). V tem smislu je tveganje v odnosu tisti korak v modelu, ki označuje realizacijo pripravljenosti tvegati v specifičnem kontekstu. Pred realizacijo je seveda potrebno, da upnik zazna in interpretira tveganja. Na njegovo zaznavo in interpretacijo vplivajo potencialne koristi in izgube v določeni situaciji, poznavanje problema, kontrolni mehanizmi organizacije, družbeni vplivi idr. (ibidem).

Vrnimo se k vprašanju, zakaj namesto *Tveganje* piše *Zaznano tveganje*. Mayer et al. (1995) ugotavljajo, da se je v literaturi izoblikovala teorija, da so tveganja, ki izhajajo iz odnosa med upnikom in zaupnikom (v fazi *Tveganje v zaupanju*, op. G. H.), združena z zaznanimi tveganji, ki jih upnik zazna, preden gre v odnos z zaupnikom (v fazi *Zaupanje*, op. G. H.). Trdijo (ibidem), da takšen pristop ni ustrezen, saj ne omogoča pogleda na to, kako se zaupanje odraža na vedênju oziroma kako zaznana tveganja vplivajo na vedênje. Zato predlagajo (ibidem), da se loči zaznana tveganja, ki izhajajo iz situacije, preden upnik formira odnos z zaupnikom, in tveganja, ki jih je upnik deležen v situaciji, ko manifestira svoje zaupljivo vedênje. To so storili tudi sami, zato namesto izraza *Tveganje*, ki ga v svoje bistvo vključuje pravokotnik *Tveganje v odnosu*, uporabljajo izraz *Zaznano tveganje*.

Nadalje avtorji (Mayer et al., 1995) predlagajo, da se raven zaupanja oziroma njeno vrednost (pravokotnik *Zaupanje* na sliki 3.6) primerja z vrednostjo zaznanih tveganj (pravokotnik *Zaznano tveganje* na sliki 3.6) in nato ugotovi, ali vrednost zaupanja presega vrednost zaznanih tveganj. Če je vrednost zaupanja višja, potem bo upnik vstopil v odnos z zaupnikom oziroma bo tvegal v odnosu. Podoben mehanizem vsebuje tudi že predstavljeni model avtorjev Mirzaie et al. (2012), pri katerem mora biti ocena o zaupniku višja od upnikovega praga.

Kljub temu Mayer et al. (1995) pravijo, da lahko na zaupanje poleg sposobnosti, benevolence, integritete in nagnjenja k zaupanju vplivajo tudi specifične posledice zaupanja, ki jih določajo kontekstualni dejavniki, npr. vložki, ki so v igri, razmerje moči v odnosu, zaznavanje stopnje tveganja in alternative, ki jih lahko izbere upnik. Z drugimi besedami, kontekst lahko vpliva na upnikovo percepcijo in s tem spremeni njegovo zaznavanje zaupnikove sposobnosti, benevolence, integritete in nagnjenja k zaupanju. Percepcija in interpretacija sta tista dejavnika, ki vplivata na upnikovo potrebo po zaupanju in presojo, ali oziroma koliko je zaupnik vreden zaupanja (ibidem). Da je obravnavani model dinamičen, dokazuje povratna zanka *Izidi*, ki je rezultat tveganja v odnosu in posredno pozitivno ali negativno vpliva na zaupanje preko percepcije o zaupnikovi sposobnosti, benevolenci, integriteti in nagnjenju k zaupanju (ibidem).

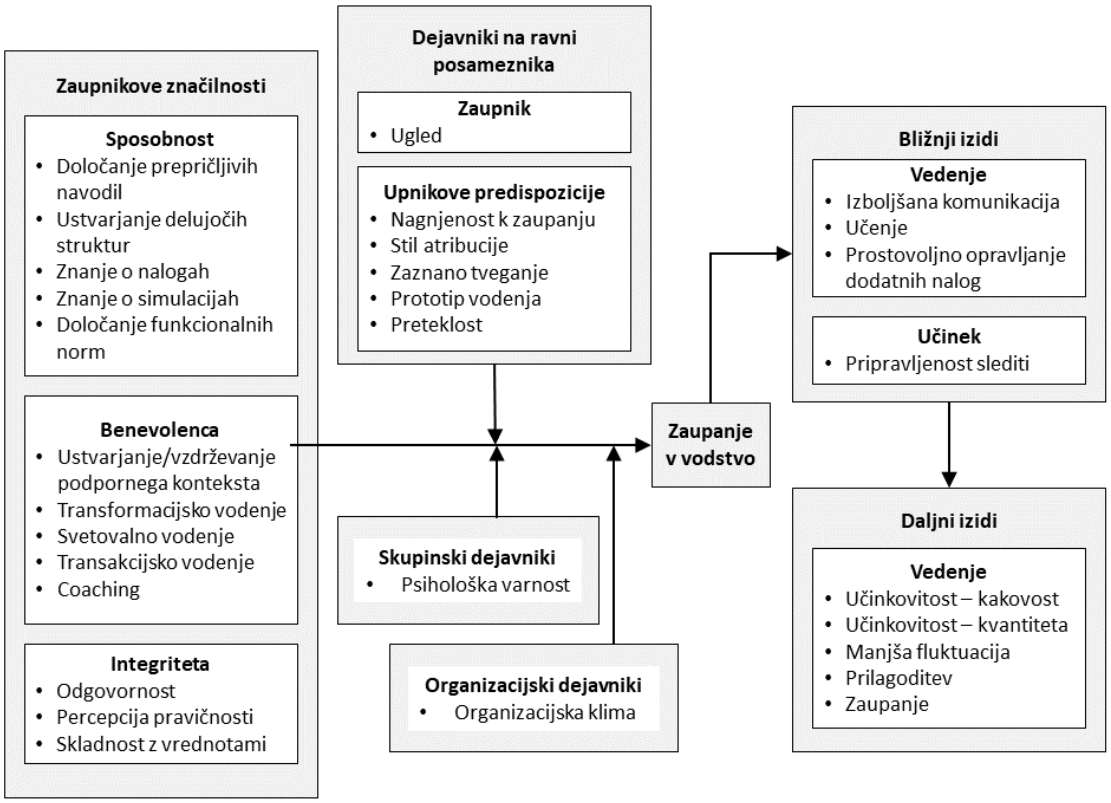
Model ima tudi nekaj omejitev (Mayer et al., 1995, str. 729-730):

1. obravnava le zaupanje določenega upnika v določenega zaupnika;
2. zaupanje je obravnavano le enosmerno (upnik zaupa zaupniku), zato model ni ustvarjen za obravnavanje vzajemnega zaupanja;
3. model se osredotoča na zaupanje v organizacijskih odnosih, zato ni uporaben za odnose v drugih kontekstih;
4. sestavine modela so bile izbrane izmed različnih možnosti iz analizirane literature, ki se med seboj razlikujejo.

Burke et al. (2007, str. 610) ugotavljajo, da ima model avtorjev Mayer et al. (1995) nekaj prednosti, vendar da je njegova slabost slaba specifikacija rezultatov zaupanja. Burke et al. (2007) so analizirali velik del pomembnejše literature na področju zaupanja in

izoblikovali model zaupanja v vodstvo (področje menedžmenta, op. G. H.). Model temelji na modelu avtorjev Mayer et al (1995), ki so ga nekoliko spremenili in dopolnili (slika 3.7).

Slika 3.7: Integrirano večstopenjsko ogrodje za razumevanje zaupanja v vodstvo



Vir: Burke et al., 2007, str. 613

Tudi model na sliki 3.7 obravnava značilnosti zaupnika, kot jih zaznava upnik: *sposobnost*, *benevolenca* in *integriteta*. Vsaka od značilnosti je podrobneje razdeljena na posamezne dejavnike, ki vplivajo na to značilnost. Opazili smo, da je model na sliki 3.7 razširjen z dvema dodatnima sestavinama, ki vplivata na zaupanje (*Skupinski dejavniki* in *Organizacijski dejavniki*), sestavina *Nagnjenost k zaupanju* s slike 3.6 pa je umeščena v novo, razširjeno sestavino (*Dejavniki na ravni posameznika*). V slednjo je umeščeno tudi *Zaznano tveganje*. Čeprav Burke et al. (2007) ne povzemajo ali komentirajo stališča avtorjev Mayer et al. (1995) glede vloge in umestitve zaznanih tveganj ter tveganj v odnosu v modelu zaupanja, je mogoče razbrati, da imajo drugačno mnenje: zaznano tveganje uravnava odnos med zaupnikovimi značilnostmi (sposobnost,

benevolenca, integriteta) in zaupanjem v vodstvo. Ko se poveča stopnja zaznave tveganja, se upnik bolj opre na zaupnikove značilnosti in tako lažje odloči glede zaupanja (ibidem). Med ostale dejavnike na ravni posameznika (v organizaciji, op. G. H.) oziroma upnika avtorji modela na sliki 3.7 uvrščajo (ibidem) *zaupnikov ugled* (kot ga zazna upnik) ter upnikovo *nagnjenost k zaupanju*, njegov *stil atribucije*, *mentalni model prototipa učinkovitega vodenja/vodje* in pa njegovo *preteklost z zaupnikom*.

Med skupinske dejavnike, ki vplivajo na zaupanje, spada *psihološka varnost*. Ta odraža skupinsko vzdušje, v katerem medosebno zaupanje in spoštovanje zagotavljata, da dobronamerna dejanja ne bodo vodila h kaznovanju (ibidem, str. 622). Takšno vzdušje vzpodbudi osebe, da (kritično, op. G. H.) podvomijo v predloge in odločitve vodstva (ibidem), torej zaupnika, prispeva pa tudi k motiviranju skupine in k poudarjanju pomembnosti vseh članov skupine (Edmondson, 2003 v Burke et al., 2007, str. 622). Vodjo, ki ustvarja psihološko varnost, bo upnik zato ocenil kot bolj benevolentno in sposobno (Burke et al., 2007, str. 622).

Organizacijska klima je kontekst, ki vpliva na zaupanje preko upnikove zaznave vrednot organizacije. Na dobro organizacijsko klimo vpliva več dejavnikov, med pomembnejšimi pa je odnos vodstva do politik in postopkov v organizaciji. Vodstvo s tem pokaže, koliko izpolnjuje napovedi, načrte in cilje ter v kolikšni meri se drži postopkov in koliko je vodstvo pravično v teh postopkih. Ta odnos vpliva na zaupanje zaposlenega (upnika, op. G. H.) v vodstvo (zaupnika, op. G. H.). Na zaupanje pozitivno vplivata tudi podpora in spoštovanje zaposlenih ter spodbujanje k razpravljanju o storjenih napakah, pri čemer ni cilj iskanje krivca in označevanje zaposlenih za »grešne kozle« (Burke et al., 2007).

Burke et al. (ibidem) izhajajo iz perspektive, da rezultat procesa ni zaupanje, temveč vedênje, na katerega zaupanje vpliva. Takšno vedênje se odraža na izidih, ki so na sliki 3.7 razdeljeni na bližnje in daljne. S tem so avtorji (ibidem) podrobneje konkretizirali izide zaupanja, kar po njihovem mnenju manjka modelu avtorjev Mayer et al. (1995). Zaupanje naj bi olajšalo in odprlo komunikacijo glede procesov v organizaciji, spodbudilo opravljanje dodatnih nalog, ki jih oseba sicer ni dolžna opravljati, vendar jih je kljub temu pripravljena opravljati, spodbudilo učenje, izboljšalo delo (kakovost in kvantiteto),

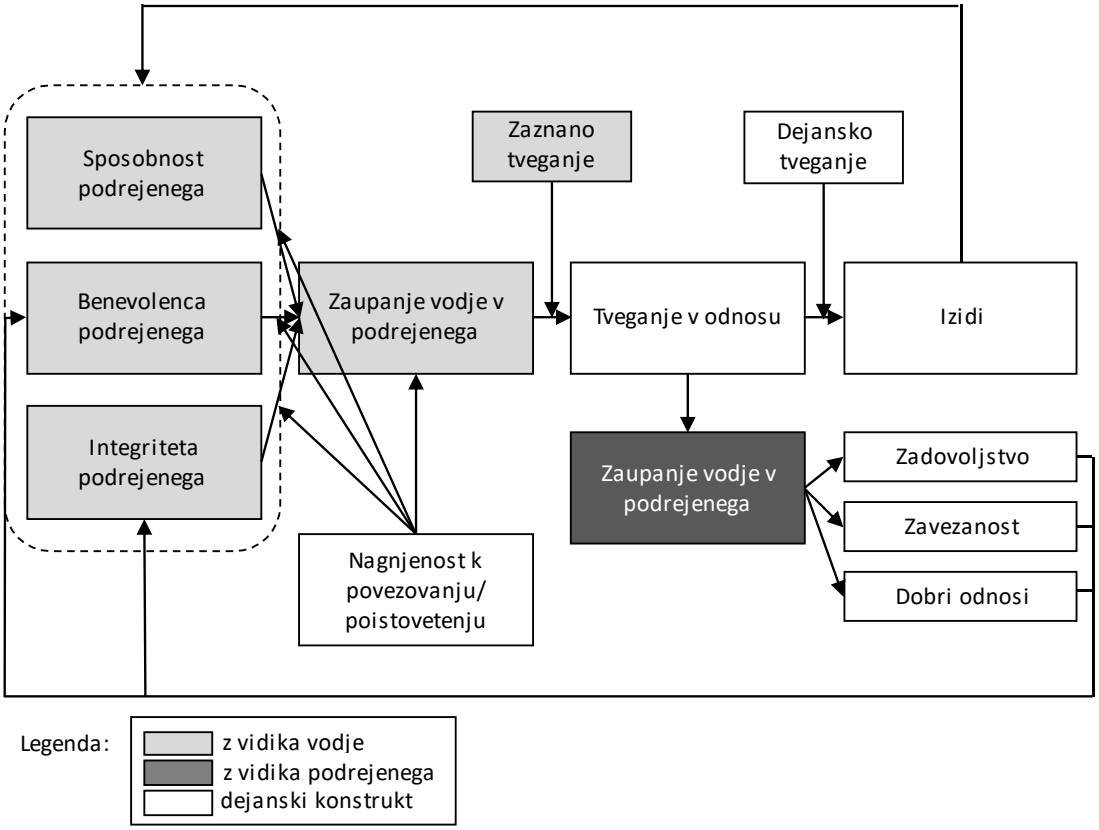
zmanjšalo fluktuacijo, izboljšalo sposobnost prilagajanja na različne situacije, povečalo pripravljenost oseb slediti vodstvu, obenem pa naj bi tudi povečalo zaupanje (Burke et al., 2007). Model na sliki 3.7 se od modela na sliki 3.6 razlikuje tudi po tem, da nima povratne zanke, ne vemo pa, ali so avtorji (Burke et al., 2007) povratno zanko namerno izpustili iz modela ali ne.

Podoben model kot Mayer et al. (1995) so predlagali tudi že omenjeni Brower et al. (2000). Njihov model se nanaša na relacijski pristop k vodenju (slika 3.8) in prikazuje model zaupanja vodje v podrejene. Model je nastal na podlagi integracije dveh teorij oziroma teoretičnih perspektiv: teorije vodenja in teorije zaupanja. Tega modela nismo podrobneje predstavljali, saj je z vsebinske perspektive osredotočen predvsem v menedžment oziroma vodenje in odnos med vodjo ter zaposlenimi (podobno kot model na sliki 3.7, le da z vidika vodje), zato smo predstavili le tiste sestavine, ki se razlikujejo od modela avtorjev Mayer et al. (1995), iz katerega izhajajo (glej sliko 3.6). Namesto sestavine *Nagnjenost k zaupanju* ima model na sliki 3.8 sestavino *Nagnjenost k povezovanju/poistovetenju*, ki pomeni »zaupati hierarhičnim odnosom. Za vsakega posameznika bo temeljna vrednost nagnjenosti k zaupanju novemu podrejenemu najverjetneje drugačna od splošne nagnjenosti k zaupanju.« (Brower et al., 2000, str. 236) Izraz *povezovanje/poistovetenje* so uporabili zaradi razlikovanja splošne nagnjenosti od specifične nagnjenosti. Splošna nagnjenost k zaupanju je tista, ki jo McKnight et al. (1998) umeščajo v dispozicijsko zaupanje ter odraža splošno pripravljenost zaupati drugemu človeku. V modelu avtorjev Mayer et al. (1995) sestavina *Nagnjenost k zaupanju* ravno tako odraža splošno nagnjenost k zaupanju, ne glede na to, za katero osebo gre. V tem smislu se strinjamo z Brower et al. (2000), ki trdijo, da je npr. upnikova raven nagnjenosti k zaupanju na splošno visoka, medtem ko je raven nagnjenosti k zaupanju določeni osebi nizka, zato je tudi sestavina smiselno nadomeščena z ustreznejšo.

Svetlo siva polja na sliki 3.8 ponazarjajo sestavine, ki jih zaznava vodja, in odražajo njegove presojo o določenem dejavniku, temno sivo polje pa ponazarja sestavino, ki jo zaznava podrejeni. Z belo barvo so označeni t.i. *dejanski konstrukti*, ki predstavljajo

(objektivno) dejansko stanje ali rezultat (npr. kakšni so dejanski izidi, kakšna so dejanska tveganja, koliko oseba resnično tvega v odnosu).

Slika 3.8: Relacijski pristop k vodenju

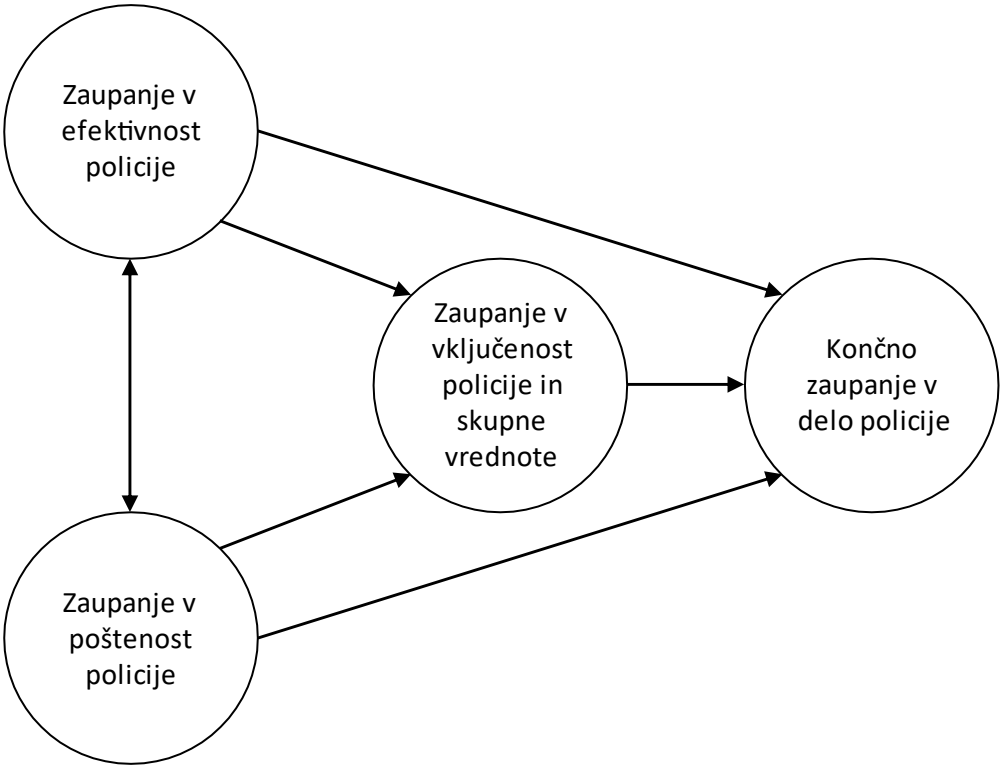


Vir: Brower et al., 2000, str. 233

Na področju zaupanja v državne organe, natančneje v policijo in delo policistov, sta Jackson & Bradford (2010, str. 5) prepoznala tri dimenzije zaupanja: efektivnost (tehnične kompetence), poštenost (poštenost v postopkih) in vključenost v skupnost (skupne vrednote). Njun model prikazuje slika 3.9. Tudi pri tem modelu zasledimo, da so izkušnje in percepcija državljanov dejavniki, ki vplivajo na njihova čustva v zvezi s policijo in zaupanje vanjo (ibidem). Avtorja (ibidem) ugotavljata, da ima največji vpliv na zaupanje vključenost policije v skupnost in pa vrednote, ki si jih delijo (skupne vrednote), takšno zaupanje pa izvira iz zaznane poštenosti policije. Pri tem dopuščata in upoštevata vpliv stereotipov na percepcijo javnosti, ki izhajajo iz vloge policije v družbenem, kulturnem in političnem življenju (ibidem). To znova dokazuje, da je zaupanje v državni organ odvisno ne le od njega samega, temveč tudi od vpliva drugih – predvsem v smislu

vplivanja na (medijsko) podobo organa v javnosti glede na njegovo vpetost v posamezno področje družbenega življenja.

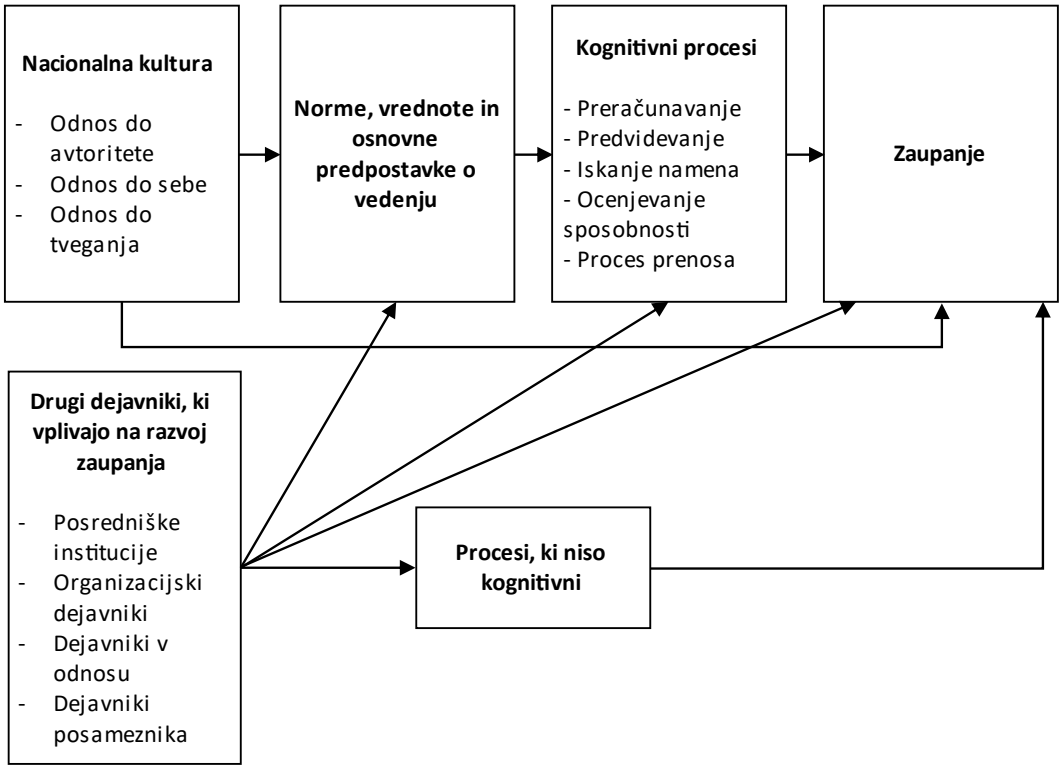
Slika 3.9: Model zaupanja v policijo



Vir: Prirejeno po Jackson & Bradford, 2010, str. 6

Pri ocenjevanju dela državnih organov oziroma zaupanju vanje ne smemo pozabiti vpliv kulture. Doney et al. (1998) so razvili model (slika 3.10), ki prepoznava in opisuje pet kognitivnih procesov (*preračunavanje*, *predvidevanje*, *namernost*, *sposobnost*, *prenos*) izgradnje zaupanja, na katere pomembno vpliva nacionalna kultura. Izraz *nacionalna* so avtorji dodali zgolj zaradi razlikovanja od korporativne kulture in drugih podobnih zvrsti, zajema pa splošno kulturo določene države; kulturo definirajo enako kot Hill (1997 v Doney et al., 1998, str. 607): »Sistem vrednot in norm, ki si jih delijo člani skupine in ki skupaj tvorijo način življenja teh članov.« Doney et al. (1998) so raziskovali vpliv nacionalne kulture na prej omenjenih pet kognitivnih procesov z vidika izgradnje zaupanja.

Slika 3.10: Model nacionalne kulture in razvoja zaupanja



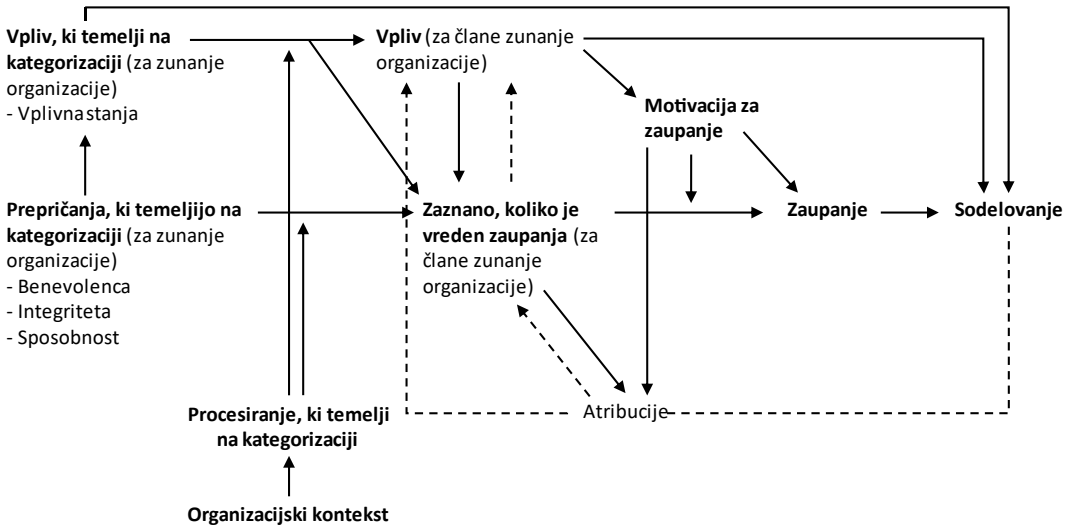
Vir: Doney et al., 1998, str. 602

Z našega vidika obravnavanja je pomembna ugotovitev, da kadar upnik in zaupnik izhajata iz iste kulture (tj. si delita enake norme in vrednote), obstaja večja verjetnost, da se bo med njima oblikovalo zaupanje, saj je smer, po kateri upnik ugotavlja, koliko je zaupnik vreden zaupanja, enaka smeri, po kateri zaupnik išče, kako pridobiti zaupanje od upnika (ibidem). Na zaupanje in pred tem na kognitivne procese ter pred tem na norme, vrednote in osnovne predpostavke o vedênju posredno vpliva kultura. Če se kultura kot izhodišče (upnika – kultura, ki vpliva na norme in vrednote, te pa na njegove kognitivne procese in ti »potujejo« proti zaupanju) ali kot končna točka (zaupnika – po postopku obratnega inženiringa išče, kako do zaupanja priti preko vplivanja na upnikove kognitivne procese in tako »potuje« proti kulturi) razlikuje od nasprotne osebe, potem bo zaupanje težje vzpostavljeno. S tem modelom lahko do neke mere tudi pojasnimo povezavo med zaupanjem, kontekstom in sposobnostmi zaupnika. Zaupanje se prične kot sodba ali mnenje o zaupnikovih zmogljivostih, da opravi določeno nalogo, pri tem pa se ocenjuje tudi njegovo pripravljenost in iskrenost za opravljanje naloge (Martin, 2014).

Ker določene naloge lahko opravijo le določeni ljudje, je nabor potencialnih oseb specifičen in tako odvisen od konteksta oziroma okoliščin. *Kontekst* je opredeljen kot povezave oziroma okolje, s katerim je vsebina povezana (Oxford English Dictionary, 1996, v Schwaninger & Ríos, 2008, str. 146), ali »kar z določeno stvarjo nastopa, je z njo povezano.« (Kontekst, b. d.) Zato Martin (2014) in njegovi predhodniki (npr. Kovač & Trček, 2007; Little et al., 2007; Olmedilla et al., 2006) ugotavljajo, da je zaupanje odvisno od konteksta. Če se vrnemo k avtorjem Doney et al. (1998) in njihovemu modelu zaupanja: tudi sami so ugotovili, da kontekst oziroma situacijski dejavniki in pripadnost določeni kulturi (npr. dve osebi izhajata vsaka iz svoje kulture) vplivajo na odnos med kulturo in kognitivnimi procesi, torej na zaupanje kot končni rezultat celotnega procesa.

Z vprašanjem oblikovanja zaupanja pri osebah, ki izhajajo iz različnih družbenih skupin, se je ukvarjala Williamsova (2001). Njen model (slika 3.11) temelji na vplivu percepcije, motivacije in pro-družbenega vedênja osebe na zaupanje v člane drugih, zunanjih organizacij, v katere oseba ni vključena (ibidem, str. 385).

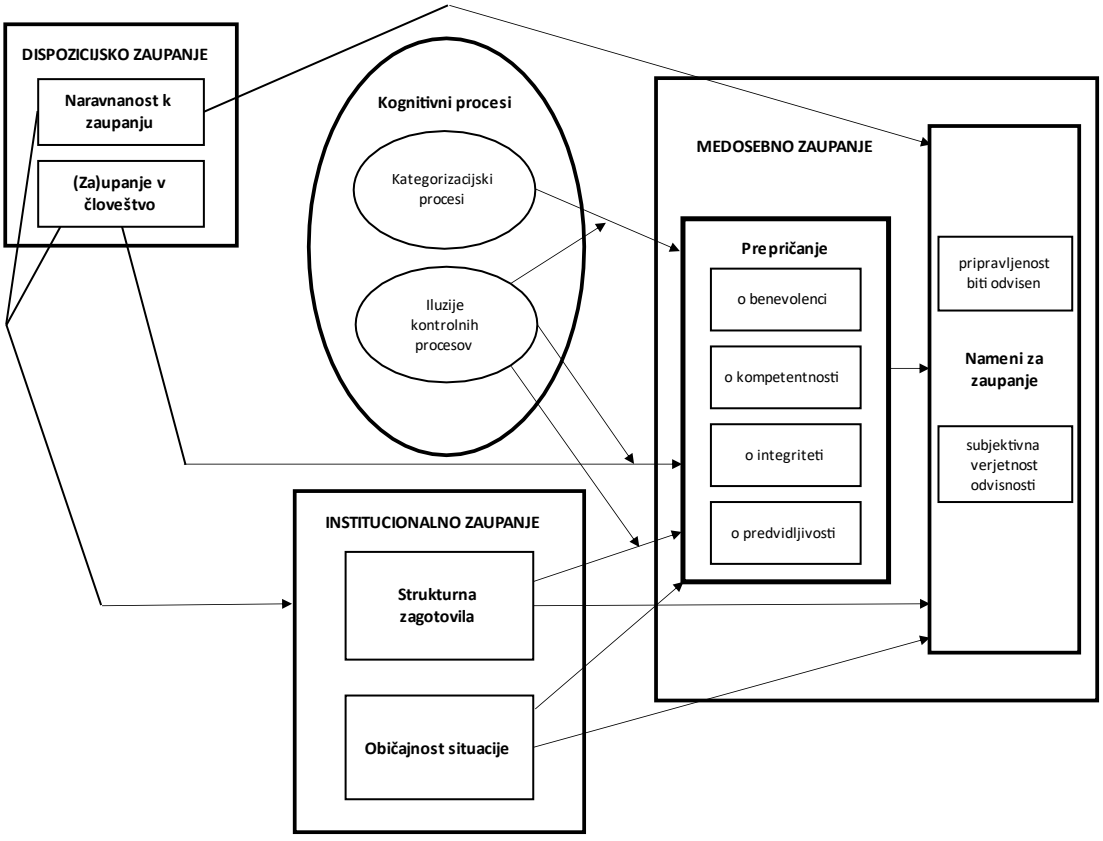
Slika 3.11: Afektivno-kognitivni model članstva v različnih družbenih skupinah in začetnega zaupanja



Vir: Williams, 2001, str. 385

Model Williamsove (2001) lahko primerjamo z enim segmentom modela McKnight et al. (1998), ki smo ga v večji meri že obravnavali v podpoglavju 3.3.4, saj oba modela prepoznavata vpliv organizacije oziroma institucije na zaznavanje določenih značilnosti članov organizacij (tj. potencialnih zaupnikov) in s tem na morebitno zaupanje. McKnight et al. (ibidem) ugotavljajo, da do začetnega zaupanja pride naravno, brez predhodnih izkušenj ali znanja o drugi osebi. Kot prikazuje model (slika 3.12), se začetno zaupanje razvije na podlagi posameznikovega dispozicijskega zaupanja, institucionalnega zaupanja in dveh kognitivnih procesov, zato se nanaša le na situacije, ko upnik prvič sreča potencialnega zaupnika (McKnight et al., 1998).

Slika 3.12: Model začetne izgradnje zaupanja



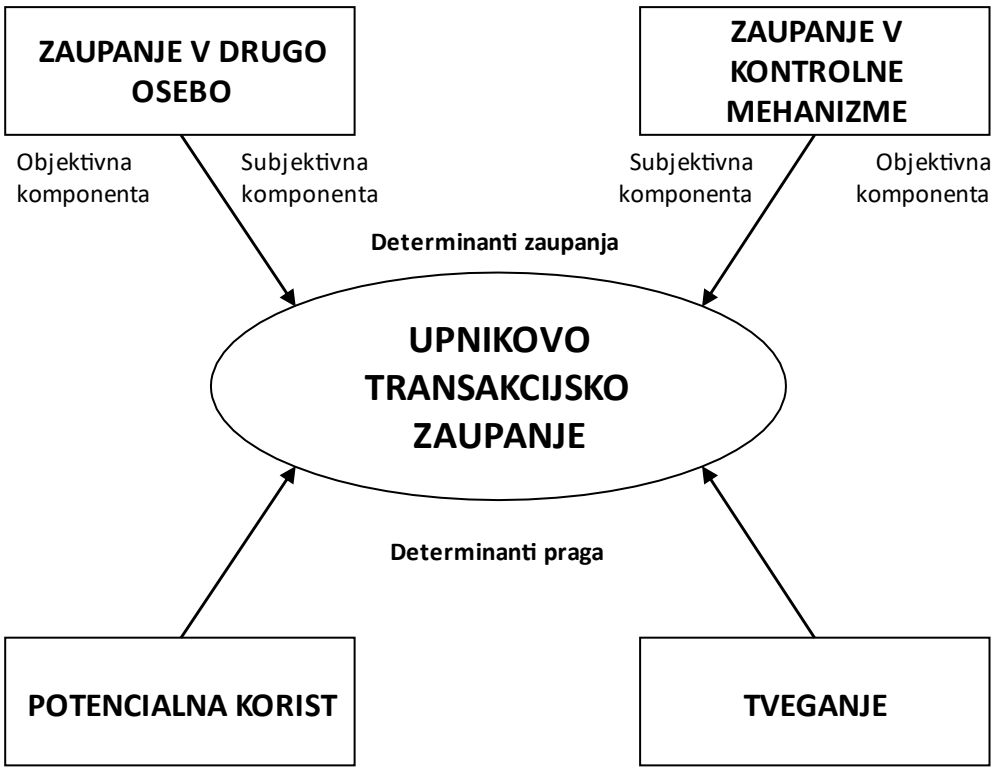
Vir: McKnight et al., 1998, str. 476 (ter dopolnjen z McKnight & Chervany, 2001 in z lastnimi dopolnitvami)

Ključno pri tem modelu je, da dispozicijsko zaupanje vpliva na institucionalno zaupanje, kasnejepa na prepričanja in upnikove namene za zaupanje. Model nakazuje, da je vsaka kasnejša oblika oziroma vrsta zaupanja odvisna od dispozicijskega zaupanja. Pomembno

vlogo namenja zadnji sestavini modela – *namenom za zaupanje*. Ta komponenta je lahko krhka (tj. kadar se nameni za zaupanje v določenem časovnem obdobju nenadno in bistveno spremenijo v pozitivnem ali negativnem smislu) ali robustna (tj. kadar se nameni za zaupanje v določenem časovnem obdobju ne spremenijo bistveno). Ti nameni so krhki, 1) kadar ni zadostne podpore prepričanj o zaupanju, 2) zaradi začasne oziroma neodločne narave dejavnikov prepričanja o zaupanju ali pa 3) zaradi zaznanega velikega tveganja; krhki nameni za zaupanje so zato nestabilni, hitro se spreminjajo, poleg tega pa je nanje mogoče vplivati. Nasprotno pa so nameni robustni, 1) kadar je dovolj podpore prepričanj o zaupanju, 2) zaradi kognitivnih mehanizmov, ki potrjujejo prepričanja ter 3) zaradi socialnih mehanizmov (npr. dobri medsebojni odnosi, pozitivno sodelovanje, negativni dogodki težje zmanjšajo zaupanje, če ima oseba dober ugled). Nameni bodo zato najverjetneje robustni, ko imata upnik in zaupnik osebno komunikacijo in kadar ima zaupnik široko razširjen dober ugled (McKnight et al., 1998).

Naslednji model je generični model zaupanja (slika 3.13) avtorjev Tan & Thoen (2001), ki sta ga razvila za področje elektronskega poslovanja. Model temelji na modelu zaupanja avtorjev Castelfranchi & Falcone (1998, v Tan & Thoen, 2001, str. 6), ki pa ga zaradi nedostopnosti članka omenjenih avtorjev žal nismo mogli obravnavati. Kot navajata Tan & Thoen (ibidem), naj bi na zaupanje vplivale štiri vrste prepričanja: prepričanje o kompetencah (ali je druga oseba sposobna doseči pričakovani rezultat), prepričanje o odvisnosti (upnik potrebuje drugo osebo za uresničitev cilja oziroma se je bolje zanesti na drugega, kot pa na nikogar), prepričanje o dispoziciji (druga oseba ni le sposobna opraviti nalogo, temveč je to tudi pripravljena storiti) ter prepričanje o izpolnitvi (prepričanje, da bo cilj po zaslugi druge osebe dosežen). Prepričanje o odvisnosti naj bi bil po mnenju avtorjev (ibidem) nujen pogoj za zaupanje v drugo osebo, vendar ne zadosten. Ugotavljata (ibidem), da kompetentnost, dispozicija za zaupanje in odvisnost ne zadostujejo za obstoj zaupanja, saj je potrebna tudi manifestacija zaupanja (tisto, čemur mi pravimo *zaupljivo vedênje*, op. G. H.).

Slika 3.13: Generični model zaupanja (Tan & Thoen, 2001)



Vir: Tan & Thoen, 2001, str. 2

V sredini modela na sliki 3.13 je upnikovo transakcijsko zaupanje, tj. mentalno stanje upnika, ki določa, ali ima dovolj zaupanja, da se vključi v transakcijo. Prag je določen s potencialno koristjo, (prepoznanim, op. G. H.) tveganjem in upnikovim odnosom do tveganja (pripravljenost tvegati), kontrolni mehanizmi (postopki in protokoli za nadzorovanje in kontrolo uspešne izvedbe transakcije) in zaupanje v osebo pa determinirata »vrednost« oziroma »količino« zaupanja. Glavna domneva modela je, da se zaupanje v drugo osebo in zaupanje v kontrolne mehanizme medsebojno dopolnjujeta. Kadar je zaupanja v drugo osebo malo, mora biti več zaupanja v kontrolne mehanizme, ki bo nadomestilo manjše zaupanje v drugo osebo – in obratno. Ko »vrednost« zaupanja preseže determinirani prag zaupanja, bo oseba zaupala drugi osebi, v nasprotnem primeru pa ne (Tan & Thoen, 2001).

Zanimiv model je razvil Robert F. Hurley, profesor na Fordham University v New Yorku. Ustvarjen je bil za menedžerje, da bi lahko pomagali zaposlenim pri razvoju osebnostnih zmogljivosti za zaupanje in razvoj zaupanja. Z njegovim modelom lahko predvidimo, ali

bo posameznik zaupal drugim v določeni situaciji ali ne. Določil je 10 dejavnikov, ki vplivajo na upnikovo odločitev (povzeto po Hurley, 2006, str. 56-59):

- *tolerantnost do tveganj*: koliko je posameznik pripravljen tvegati (vpliv kulture);
- *stopnja prilagajanja*: odraža posameznikovo sposobnost prilagajanja;
- *moč*: posameznikova pozicija moči;
- *varnost*: varnost v določeni situaciji oziroma okolju;
- *število/stopnja podobnosti*: ujemanje dveh oseb, tudi osebe s skupino ali z organizacijo (vpliv delovne etike, članstev, ambicij itd.);
- *ujemanje interesov*: koliko je delavec pripravljen slediti interesom vodje oziroma organizacije;
- *sposobnost*: vodja ocenjuje kompetentnost zaposlenega za delo;
- *benevolentno izkazovanje skrbi*: koliko vodja izkazuje skrb za zaposlene;
- *predvidljivost in integriteta*: kako predvidljiv je zaposleni in koliko integritete ima;
- *stopnja komunikacije*: ali je oziroma koliko je komunikacija dobra, iskrena in odprta.

Prvi trije dejavniki (*tolerantnost do tveganj*, *stopnja prilagajanja*, *moč*) so mešanica osebnosti, kulture in izkušenj in odražajo upnikove osebnostne karakteristike, medtem ko so preostali dejavniki situacijski dejavniki in dejavniki v odnosu (Hurley, 2006). Hurley (2012) je do dejavnikov prišel s pomočjo analize in združevanja različnih dejavnikov zaupanja iz dostopne literature o zaupanju (tabela 3.2).

Tabela 3.2: Umestitev dejavnikov zaupanja iz druge literature v dejavnike zaupanje po Hurley (2012)

Dejavniki po Hurley, 2012	**Dejavniki iz druge literature**
toleranca tveganja	*toleranca tveganja*
	previdnost
prilagajanje	*prilagajanje*
	dispozicija, osebnost za zaupanje
moč	*moč, zastraševanje*
	avtonomnost
podobnosti	*skupne vrednote, skladnost vrednot*
	skupna identiteta
	pristranskost znotraj skupine
Tabela se nadaljuje na drugi strani	

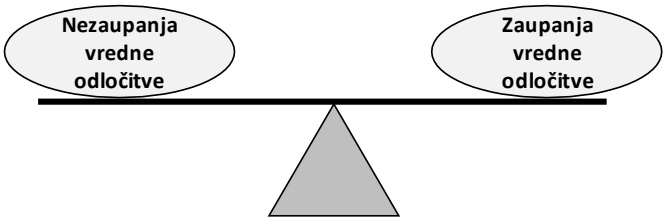
Dejavniki po Hurley, 2012	Dejavniki iz druge literature
(podobnosti)	*učinki mrežnega zaupanja*
	skupinske norme
	skupinski cilji
	osebna privlačnost
	ugled, mnenja drugih
interesi	*interesi, motivi*
	spodbude
	sodelovanje
	skupinski cilji
	pravičnost
	namen proizvajati ali podpirati
benevolenca	*benevolenca*
	altruizem
	zvestoba
	imeti skrb za druge
	ustrežljivost
sposobnost	*kompetenca, specialnost, strokovnost*
	sposobnost
	presoja
	nadzor
predvidljivost in integriteta	*pretekle interakcije, izidi in eksperimenti*
	kredibilnost obljub
	zanesljivost, konsistentnost
	integriteta, moralna integriteta
komunikacija	*komunikacija*
	diskretnost, ohranjanje skrivnosti
	odprtost, sprejemanje
	zanesljivost kot vir informacij
	zaupnikove trditve, kako se bo vedel

Vir: Hurley, 2012, str. 199-200

Model uporabnike (menedžerje) spodbuja k sprejemanju ustreznih odločitev in ukrepanju za povečanje posameznih dejavnikov oziroma njihov premik na pozitivno stran (*Zaupanja vredne odločitve*). Ozadje modela je princip tehtnice, na kateri se ves čas tehta med zaupanja in nezaupanja vrednimi odločitvami, prikazuje slika 3.14.

Slika 3.14: Model nezaupanja in zaupanja vrednih odločitev

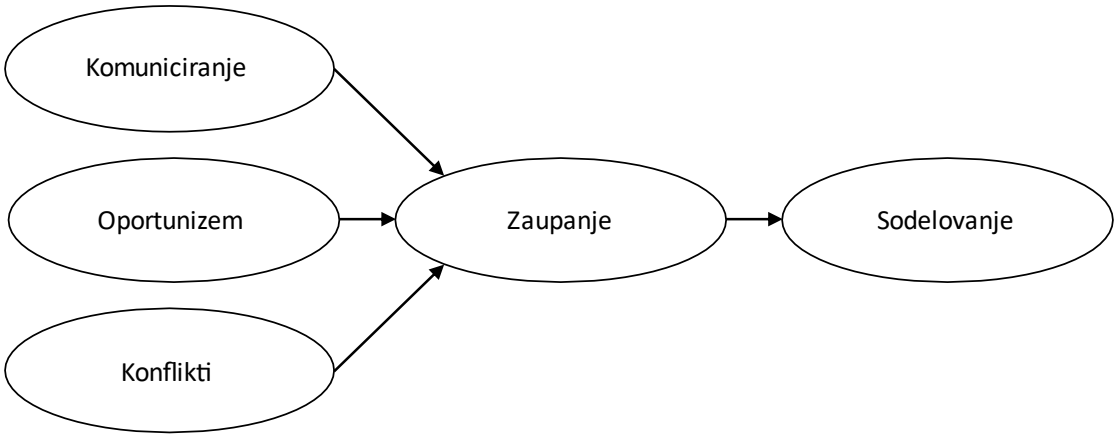
Majhna	Tolerantnost do tveganj	*Velika*
Majhna	Prilagodljivost	*Velika*
Majhna	Moč	*Velika*
Visoko	Situacijsko tveganje	*Nizko*
Niso očitne	Podobnosti	*So očitne*
Konflikti	Interesi	*Ujemanje*
Ni izkazano	Benevolentno izkazovanje skrbi	*Izkazano*
Nizka	Zmogljivost	*Visoka*
Nizka	Predvidljivost in integriteta	*Visoka*
Slaba	Komunikacija	*Dobra*



Vir: Prirejeno po Hurley, b. d., str. 4

Tudi za potrebe raziskovanja zaupanja na področju logistike je bil izoblikovan konceptualni model vplivov na zaupanje (Križman, 2009), prikazan na sliki 3.15.

Slika 3.15: Konceptualni model

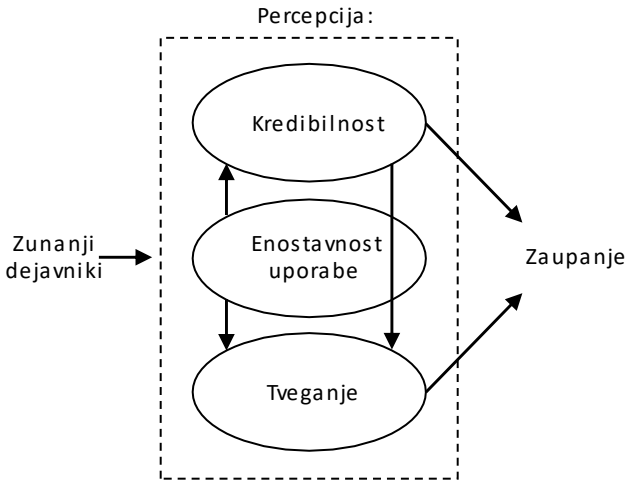


Vir: Križman, 2009, str. 335

Med dejavniki obravnavanih modelov še nismo zasledili vpliva oportunizma in konflikta na zaupanje, ki ju je v svoj konceptualni model umestila Križmanova (2009) na podlagi

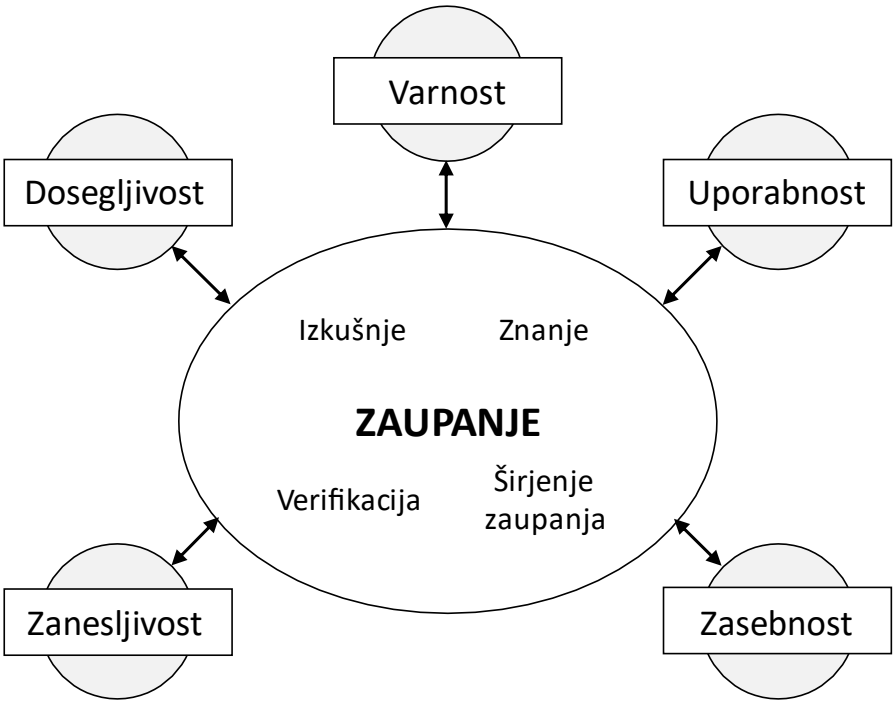
analizirane literature. Na slikah 3.16, 3.17 in 3.18 prikazujemo še nekaj ostalih modelov zaupanja.

Slika 3.16: Model spletnega zaupanja



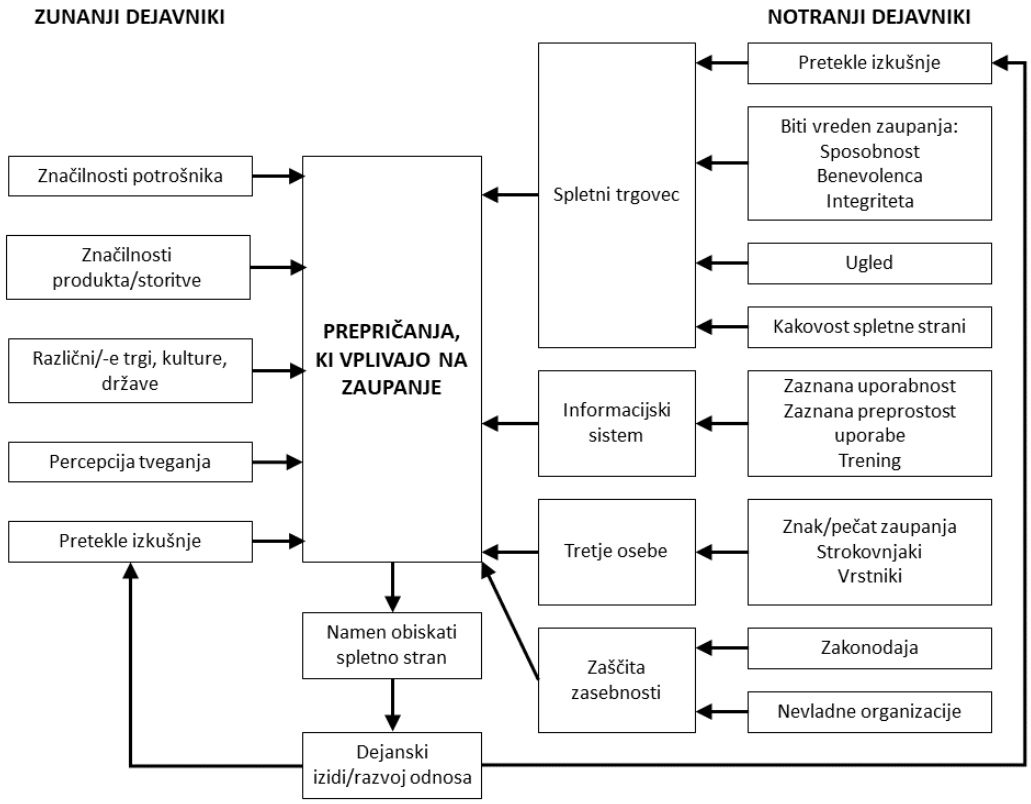
Vir: Corritore et al., 2003, str. 749

Slika 3.17: Splošni model zaupanja s povratnim mehanizmom k drugim funkcionalnim modelom



Vir: Hoffman et al., 2006, str. 8

Slika 3.18: Razviti raziskovalni model za preiskovanje spletnega zaupanja



Vir: Salo & Karjaluoto, 2007, str. 616

Modeli na slikah 3.16, 3.17 in 3.18 so področno-specifični in v primerjavi z modeli, ki smo jih obravnavali doslej, ne vsebujejo elementov, ki jih še nismo zasledili. Obravnavali smo jih, ker vsebujejo naslednje dejavnike, ki so bili v definicijah ali modelih, predstavljenih v doktorski disertaciji, prikazani kot vpliv na zaupanje ali kot sestavni del modela zaupanja. S tega vidika izpostavljamo naslednje sestavne dele modelov na slikah 3.16, 3.17 in 3.18: *zasebnost* (slika 3.17 in slika 3.18), *pretekle izkušnje* (slika 3.18), *percepcija* (slika 3.16 in 3.17), *znanje* (slika 3.17) ter *razlike* med trgi, kulturami in državami (slika 3.18).

3.5 Zaupanje in nadzor

Kadar nekomu brezpogojno zaupamo, zaupnika ne nadziramo, saj smo v njegov uspeh trdno prepričani. Kadar pa nekomu ne zaupamo brezpogojno, se pojavijo manjši ali večji dvomi o uspešnosti zaupnika pri uresničevanju naših pričakovanj. Ti lahko vodijo v

nadziranje zaupnika. Slovita reka »*zaupanje je dobro, nadzor pa še boljši*« (Vladimir Iljič Uljanov – Lenin) in »*zaupaj, vendar preveri*« (ruski pregovor, ki ga je uporabljal tudi nekdanji predsednik ZDA, Ronald W. Reagan: »*Trust, but verify*.«) odpirata široko razpravo o zaupanju in nadzoru, vendar se bomo omejili le na z našega vidika celovito obravnavo vloge nadzora v zaupanju. Začeli bomo z vprašanjem, ali lahko v primeru nadzora še vedno govorimo o zaupanju? Schoorman et al. (2007) menijo, da tistega, ki mu zaupaš, ni potrebno preverjati in nadzorovati, saj bi v nasprotnem primeru pomenilo, da mu ne zaupaš. Podobno pravita tudi Tan & Thoen (2001), in sicer da se nadzor uporabi takrat, kadar nekomu ne zaupamo. Na tem mestu želimo opozoriti, da je zadnjo poved potrebno razumeti v smislu, da se nadzor takrat uporabi kot nadomestek za manjkajoči del zaupanja. Gambetta (1988, str. 217) pravi, da zaupanje obstaja takrat, ko zaupnik opravi določeno dejanje, preden ga upnik lahko nadzoruje, in v kontekstu, v katerem zaupnikova dejanja vplivajo na upnikova dejanja. Njegova definicija izključuje uporabo nadzora in za zaupanje (kot prepričanje, op. G. H.) predvideva obstoj tiste ravni zaupanja, ko upnik ne želi niti mu ni treba nadzorovati zaupnika. V nekaterih primerih to iz različnih razlogov ni mogoče (npr. upnik ima majhno stopnjo predispozicijskega zaupanja, ne zaupa določenim okoliščinam ali organizaciji, osebe ne zaznava kot popolnoma vredne zaupanja), zato si pomaga z nadzornimi mehanizmi oziroma sredstvi, ki nadomestijo zaupanje. Majhno zaupanje naj bi zato vodilo v nadzor (Mayer et al., 1995). Podobno ugotavljata Tan & Thoen (2001, str. 4): več kot je zaupanja, manj nadzora je potrebnega – in obratno. To nakazuje na komplementarnost zaupanja in nadzora (ibidem), na katero smo opozorili malo prej. To tudi pomeni, da zaupanja in nadzora ne moremo razumeti kot dve absolutni opciji, temveč kot konstrukt, ki lahko zavzame eno izmed več različnih vrednosti. V tem smislu uporaba nadzora še ne pomeni, da osebi sploh ne zaupamo, temveč da ji zaupamo manj, kot bi ji, če nadzor ne bi bil potreben. Kadar raven zaupanja ne presega določenega praga, takrat sta potrebna nadzor in **zaupanje v nadzor**; slednji kot substitut nadomesti manjkajoče zaupanje ter preseže prag (Tan & Thoen, 2001; kot smo že navedli v enem od prejšnjih podpoglavij, so o takšnem pragu pisali tudi Mirzaie et al., 2012). Takšno stališče bi lahko izpodbijali Burke et al. (2007), ki na podlagi rezultatov nekaterih študij o obstoju tveganja ugotavljajo, da se zaupanje zmanjša takrat, kadar oseba *mora* nadzorovati posameznika.

Nadzor po mnenju Mayerja et al. (1995) nakazuje, da upnik ni toliko pripravljen tvegati. Avtorji trdijo (ibidem), da je to mogoče izboljšati z ocenjevanjem zaznanega tveganja s pomočjo anket ali z nadziranjem upnika v simulacijah, v katerim ima upnik omejeno število odzivov na tveganje, ki ga simulirajo. Kljub temu upnik ne bo zaupal drugi osebi, če zaupanje ne bo preseglo praga, ko bo pripravljen tvegati. Odloči se lahko med nezaupanjem in nadzorom. Če izbere nadzor, mu mora zaupati, torej ga mora dobro poznati. »Če popolnoma razumeš sredstvo nadzora, potem lahko sam oceniš njegovo učinkovitost. V takšnem primeru lahko dosežeš višjo raven zaupanja kot pa če ne moreš sam oceniti njegove učinkovitosti, ker ga ne razumeš.« (Tan & Thoen, 2001, str. 5) Transakcijsko zaupanje, ki pomeni stopnjo zaupanja, ko je posameznik pripravljen stopiti v transakcijo z zaupnikom (ta se kaže kot zaupljivo vedênje, op. G. H.), je zato definirano kot (ibidem):

transakcijsko zaupanje = zaupanje osebi + zaupanje nadzornim sredstvom

Na zaupanje osebi vplivajo *objektivni vidiki* oziroma družbeni znaki, ki jih zazna upnik, npr. uniforme, pozitivna energija, ki jo oddaja oseba, izkušnje in mnenje skupnosti. Na zaupanje sredstvom nadzora ravno tako vplivajo *objektivni vidiki*, in sicer ocena nadzora, ki jo izdela zaupnik, vplivajo pa tudi *subjektivni vidiki*, ki se kažejo kot razumevanje (delovanja) nadzornih sredstev in mnenje skupnosti (ibidem, str. 5-6).

Spoznali smo, da nas lahko napačno ali pomanjkljivo razumevanje nadzora zavede, zaradi česar lahko napačno presodimo, da je zaupnik vreden zaupanja. Lahko se celo zgodi, da uporabimo nadzor, ne da bi presodili svojo obstoječo stopnjo zaupanja, kar lahko rezultira v zaupanju osebi, četudi ji sploh ne zaupamo (Tan & Thoen, 2001). Nadzor zato ne sme biti nadomestek ali dopolnilo za zaupanje, kadar ne vemo, koliko imamo zaupanja (ibidem). Zaupanje, ki deluje zgolj zaradi nadzora, po našem prepričanju ni zaupanje, zato upamo, da bo naš model spodbudil državljane, da zaupajo matičnim obveščevalno-varnostnim službam tudi v primeru, če bi bile te zaradi izrednih okoliščin določeno časovno obdobje brez ustreznega nadzora.

Nadzora ne smemo enačiti s sumničavostjo, čeprav je ta lahko razlog za nadzor. Sumničavost vodi v prikrivanje upnikovega zavedanja zaupnikovih motivov in zaupnikovega zavedanja upnikovih motivov, zaupanje pa v upnikovo in zaupnikovo komunikacijo (Deutsch, 1958, str. 6). To potrjuje, da se nadzor in zaupanje dopolnjujeta, medtem ko se sumničavost in zaupanje izključujeta. Kako torej vedeti, kakšno je pravo razmerje med zaupanjem in nadzorom? Analizirana literatura o tem ne govori, glede na prebrano pa menimo, da je pravo razmerje med zaupanjem in nadzorom odvisno od *namena* izvajanja nadzora oziroma uporabe nadzornih sredstev, *konteksta* in *vidika obravnavanja*. Izraz *sredstva* v našem primeru vključuje materialna (npr. video kamere, sledilne naprave, čitalec kartic, terminal za beleženje prisotnosti na delovnem mestu) in nematerialna sredstva nadzora (npr. predpisani postopki poročanja, zakonodaja oziroma predpisi, opazovanje, organizacijska kultura). Nadzor je koristen, ker naj bi zaznal ali preprečil oportunistično vedênje in (nenamerne) napake zaupnika, ne da bi vplivali na zaupanje, s njim pa se povečuje tudi (upnikova zaznava) predvidljivost(i) zaupnikovega vedênja (Tan & Thoen, 2001). Nadzor oziroma sredstva nadzora so lahko uporabljena tudi kot orodje za utrjevanje zaupanja.

3.6 Zaupanje v državo in javni sektor

»[…] če ljudje ne morejo zaupati svoji vladi,
da bo opravila nalogo, za katero obstaja – da jih ščiti in
spodbuja skupno dobrobit –, je vse drugo izgubljeno.«
Barack Obama, 44. predsednik ZDA

Zaupanje je »ključno za vzdrževanje sodelovanja v družbi in nujno kot temelj tudi za povsem rutinske, vsakodnevne interakcije,« (Zucker, 1985, str. 56) zato politični sistem brez zaupanja ne more preživeti (Miller, 1974). Brez medsebojnega sodelovanja ne more biti političnega (so)delovanja. Ko govorimo o zaupanju v politični sistem oziroma politiko, govorimo tudi o zaupanju v državo in njene institucije. V tem okviru obravnavamo zaupanje državljanov v matične državne obveščevalno-varnostne službe, saj so del javnega sektorja (oziroma državne uprave). Kasneje podrobneje pojasnjujemo in dokazujemo, da politika vpliva na delovanje obveščevalno-varnostnih služb. Tako smo

uvodoma domnevali in tudi navedli v tretji podtezi: *na zaupanje državljanov v matične obveščevalno-varnostne službe pomembno vpliva politika.*

Zaupanje državljanov je mogoče razumeti kot najpomembnejši del javnega sektorja (Heintzman & Marson, 2005) in ključni dejavnik delovanja političnega sistema (Makarovič, 2004). Državljani imajo morda kljub temu občutek, da se politika (občasno ali pogosto, odvisno od mnenja posameznika) požvižga na njihove interese in da njihovo zaupanje ne igra nobene vloge. Enako domnevamo tudi o zaupanju v politiko, javni sektor, državo ipd.

Ignoriranje (ne)zaupanja državljanov v državo in javne institucije je lahko nevarno. Newton & Norris (2000) trdita, da je izguba zaupanja v ključne institucije družbe in demokracije veliko bolj resna grožnja kot pa izguba zaupanja v posamezne državljane ali politike, upad zaupanja tudi v ostale (zasebne) institucije in medije pa naj bi bil odraz, ki presega politično življenje in nakazuje tudi na šibkost družbe. Da s konkretnim primerom podpremo njune besede, izpostavljamo dejstvo, da je Evropsko komisijo leta 2014 skrbelo zabrisovanje države in vladnih strank, ki je načelo zaupanje makedonskih državljanov v javne institucije (Evropska komisija, 2014, str. 35). Izkazalo se je, da pomanjkanje zaupanja vpliva na politično in ekonomsko stabilnost države. Tudi v *Beli knjigi o prihodnosti Evrope* je Evropska komisija (2017) ugotavljala, da spremembe v svetu in občutek negotovosti, ki so ga prinesle spremembe, povzročajo nezadovoljstvo ljudi s politiko in institucijami na vseh nivojih. Posledično se je zmanjšalo tudi zaupanje v Evropsko unijo (v nadaljevanju: EU), za nastale probleme pa naj bi ljudje krivili Bruselj (ibidem). Nekateri razlogi za upad zaupanja, ki jih je mogoče razbrati iz bele knjige s pomočjo znanja, pridobljenega z obravnavo definicij in modelov zaupanja, naj bi bili neustrezna komunikacija, napačne informacije, pomanjkanje znanja o EU in aktivnostih EU na lokalnem/državnem nivoju, napačna predstava o zmogljivostih EU ter preveliko prepričanje, da bo EU uresničila pričakovanja državljanov. Evropska komisija je namreč ugotovila (ibidem, str. 12), da je med razlogi za manjše zaupanje tudi razkorak med *pričakovanji* ljudi in *zmogljivostmi* EU, da jih uresniči. Podoben razlog za upad zaupanja v politiko je najbrž tudi, da politika ne odraža prepričanj in vrednot posameznikov (Burke et al., 2007, str. 619). Makarovič (2004, str. 385) meni, da »[v]se večje globalno

ekonomsko, politično in ideološko odpiranje vodi, paradoksalno, k psihološkemu *zapiranju*, h krizi zaupanja,« Newton & Norris (2000) pa, da je upad zaupanja indikator javnega nezadovoljstva s sodobnim svetom. Razloge utemeljujeta s tremi šolami (povzeto po Newton & Norris, 2000, str. 58-62):

1) *Družbeno-psihološke razlage*. Osredotočajo se na družbeno-psihološke dejavnike v posameznikih. Zaupanje, nezaupanje in pomanjkanje zaupanja obravnavajo kot del tipov osebnosti. Vsi ljudje naj bi se rodili z nagnjenostjo k zaupanju, nato pa naj bi na vsakega posameznika vplivala njihova psihološka zgodovina in izkušnje. Zaupanje je s tega vidika obravnavano kot afektivna orientacija, ki oblikuje del človekove osebnosti in je odvisna od izkušenj ter zunanjega političnega sveta. Ljudje smo nosilci politične percepcije, brez povezave z učinkovitostjo političnega sistema ali njegovega vodstva, zato naj bi naši odzivi odražali naš odnos, ne pa sveta, v katerem živimo.
2) *Družbeni in kulturni model*. Osredotoča se na kulturno okolje posameznikov, skupin in skupnosti. Ta model predstavlja stališče, da življenjski dogodki in izkušnje posameznika (predvsem višja izobrazba, sodelovanje v skupnosti in dobrodelnost) ustvarjajo družbeno zaupanje, sodelovanje, delovanje v dobro družbe in recipročnost med posamezniki. S tem krepijo družbene organizacije (vključno s političnimi organizacijami), ki jim lahko ljudje zaupajo in v zameno ljudem pomagajo graditi zaupanje, sodelovanje in recipročnost ter zaupanje v druge institucije. To bi pomenilo, da ljudje, ki bolj zaupajo drugim, bolj zaupajo tudi javnim institucijam in so bolj vključeni v prostovoljne in družbene dejavnosti.
3) *Model institucionalne učinkovitosti*. Osredotoča se na učinkovitost vlade in nakazuje na tri stvari:
    1. ustrezno zastavljene in izvedene ankete so lahko dober pokazatelj učinkovitosti političnega sistema, vprašanja o zaupanju pa pokažejo stanje družbenega življenja;
    2. kadar je zaupanje državljanov v politične institucije majhno, mora politika ali znižati javna pričakovanja o učinkovitosti političnega sistema (politiki lahko obljubijo manj) ali pa izboljšati svojo institucionalno učinkovitost (politiki lahko dajo več);
    3. zaupanje v politične institucije je rezultat učinkovitosti vlade, saj presoja, koliko je oseba vredna zaupanja, in pripravljenost zaupati drugim na enak

način temeljita na izkušnjah, kako se drugi vedejo. Učinkovitost vlade vpliva na vse posameznike (npr. z inflacijo, korupcijo in ekonomsko rastjo) ne glede na njihovo osebnost ali družbeni status, vendar je (ne)zaupanje državljanov v politiko naključno porazdeljeno glede na različne dejavnike (izobrazba, dohodek, starost, spol idr.). Obstaja tudi povezava med družbenim zaupanjem in zaupanjem v politične institucije. Družbeno zaupanje pomaga graditi družbeni kapital, ki krepi politične institucije, zato se izboljšata učinkovitost vlade in zaupanje državljanov vanjo. Kadar pa se družbeno zaupanje zmanjša, se zmanjša tudi družbeni kapital, zato bodo politične institucije in vlada manj učinkovite, zaupanje pa se bo še bolj zmanjšalo.

Newton & Norris (2000) sta pred skoraj 20 leti opravila raziskavo o korelaciji med družbenim zaupanjem, zaupanjem v politične institucije in prostovoljstvom. S primerjavo sta izračunala šibko korelacijo med družbenim zaupanjem in zaupanjem v politične institucije na individualni ravni ter ugotovila, da je korelacija med aktivnostjo državljanov v prostovoljstvu, prispevanju k družbi in zaupanju v javne institucije sicer statistično značilna, vendar zelo majhna (ibidem). S tem sta dokazala, da **družbeno zaupanje in zaupanje v institucije delujeta v večji meri na ravni družbe in ne toliko na ravni posameznika** (ibidem, str. 67), žal pa nista odkrila razlogov, zakaj je temu tako.

Pomanjkanje zaupanja ali nizko zaupanje državljanov pogosto sproži dvome o pravilnosti in transparentnosti delovanja države. Različni avtorji (Heintzman & Marson, 2005; Rosario, Hartlyn & Morgan, 2006; Salminen & Ikola-Norrbacka, 2010; Van de Walle et all., 2008; idr.) ugotavljajo, da na zaupanje vpliva več dejavnikov, v literaturi pa so najpogosteje omenjeni: učinkovitost vlade (izvršilne veje oblasti, op. G. H.), učinkovitost javnega sektorja, pričakovanja državljanov in njihova percepcija izpolnjevanja pričakovanj, ekonomska blaginja, varnost, (ne)etično vedênje, stopnja korupcije, obstoj protikorupcijske zakonodaje in etičnih kodeksov ali standardov idr. Salminen & Ikola-Norrbacka (2010) sta preučevala etiko in integriteto javne uprave na primeru finske javne uprave. Določila in analizirala sta tri dejavnike, ki imajo pomemben vpliv na etiko in integriteto javne uprave: *zaupanje državljanov*, *načela dobrega vodenja* in *neetična dejanja* (ibidem). Podobno kot Salminen & Ikola-Norrbacka sta v okviru študije vplivov

na vrednostno verigo javnega sektorja raziskovala zaupanje tudi Heintzman & Marson (2005). V raziskavi sta analizirala študijo dejavnikov v Združenem kraljestvu, ki vplivajo na zaupanje v javne institucije. Teh je šest (MORI Social Research Institute, 2003 v Heintzman & Marson, str. 556):

- izpolnjevanje obljub;
- učenje iz napak;
- mnenje družine in prijateljev o storitvi;
- odnos zaposlenih do strank;
- zanimanje zaposlenih za človeške poglede;
- kakovost vodij in menedžerjev.

Večino navedenih dejavnikov in ugotovitve ostalih podobnih raziskav sta vključila v svoj predlog za izvedbo prihodnjih raziskav, s katerimi bi se preverjalo naslednja področja dejavnikov zaupanja v javni sektor (ti odražajo percepcijo državljanov, op. G. H.) (Heintzman & Marson, 2005):

- kako etični so javni uslužbenci;
- koliko vpliva imajo državljani na odločitev vlade in javnih organizacij;
- ali in kako se vlada odziva na potrebe državljanov;
- učinkovitost ekonomske in socialne politike;
- kako vlada izpolnjuje obljube, prizna napake in se iz njih uči;
- učinkovitost upravljanja z viri, kateri projekti in ukrepi so upravičili porabo denarja;
- kakovost storitev organov in vlade.

Pri tem ugotavljata (ibidem), da je zaupanje v vlado produkt zadovoljstva z zaznano učinkovitostjo politike in izvajanja storitev, izvajanje storitev pa naj bi imelo večji vpliv na zaupanje v vlado. Tako sta dokazala, da je zadovoljstvo s storitvami institucij javnega sektorja povezano z zaupanjem v vlado oziroma državo, ki preko institucij zagotavlja javne storitve in interese. Ob tem prihaja do prehajanja zaupanja, saj zaupanje eni javni instituciji povečuje možnost zaupanja tudi drugi instituciji javnega sektorja (Salminen & Ikola-Norrbacka, 2010). Kljub temu Van der Walle (2007) opozarja, da sta ocenjevanje izkušenj in mnenja, torej zaupanja, določenih služb (mikro raven) in ocenjevanje istega

celotnega javnega sektorja (makro raven) dve različni zadevi. Fink Hafner et al. (2002) so opravile študijo nezaupanja državljanov v Državni zbor Republike Slovenije (v nadaljevanju: DZ). V končnem poročilu so določile tri grozde dejavnikov, ki vplivajo na (ne)zaupanje: 1) *makroekonomski*, 2) *mikrosocialni in mikroekonomski* ter 3) *politični*. Na vprašanje, kakšno povezavo imata politična in ekonomska plat države z zaupanjem, pojasnjuje Rus (2008, str. 76): »Makro pristop k zaupanju skuša določiti zvezo med stopnjo zaupanja v dani družbi in ravnijo njene ekonomske razvitosti. […] Makro pristop k zaupanju je še zlasti uveljavljen med politologi, ki societalno zaupanje povezujejo z uspešnostjo političnih in ekonomskih institucij (Putnam, 1993; Norris, 2002). V tem kontekstu najdemo razlago za zvezo med ekonomsko uspešnostjo in zaupanjem v tem, da zaupanje vselej nastopa kot javna dobrina, ki je dostopna vsem posameznikom v družbi in ki s tem vpliva na individualno vedenje.« Povezavo med politiko, ekonomijo in zaupanjem je potrdil tudi Makarovič (2004). Pri ocenjevanju nezaupanja v DZ so avtorice prej omenjene študije (Fink Hafner et al., 2002) upoštevale naslednje vidike: učinkovitost delovanja parlamenta, informacijska sredstva in tokovi, ki vplivajo na zaznavo državljanov o delovanju parlamenta, učinki javnih politik ter pričakovanja in kriteriji vrednotenja, ki jih državljani upoštevajo pri ocenjevanju dela parlamenta in oblikovanju izjav o zaupanju vanje (ibidem). Njihova analiza odgovorov intervjujev s strokovnjaki je pokazala, da so tuji in slovenski strokovnjaki prepoznali podobne dejavnike, zakaj Slovenci niso zaupali Državnemu zboru: zaradi poročanja in delovanja medijev, negativnega odnosa ljudi do politike in do politikov, razkoraka med pričakovanji ljudi in dejanskim stanjem (razočaranje, op. G. H.), nepoznavanja parlamentarnega sistema (neznanje, nevednost, op. G. H.), negativnega vrednotenja konfliktov v parlamentu ter neprimernega načina delovanja poslancev (ibidem, str. 35). Na podlagi končne analize so zato določile štiri dejavnike, ki vplivajo na (ne)zaupanje v parlament: 1) *informacije* (sredstva in tokovi, ki vplivajo na zaznavo državljanov o delovanju DZ), 2) *učinki javnih politik* (te oblikuje parlament), 3) *pričakovanja in merila za vrednotenje* (državljani in njihova percepcija) ter 4) *delovanje parlamenta*. Tudi ta študija prepoznava učinkovitost (četrti dejavnik) in (ne)skladnost pričakovanj državljanov (tretji dejavnik) kot pomembna dejavnika, ki vplivata na zaupanje državljanov v javno institucijo. Schiffman et al. (2010) so obravnavali tri zanje pomembna področja zaupanja v politiko: zaupanje v obliko vladavine, politični cinizem in zaupanje v uslužbenca. Prvo področje odraža zaupanje

posameznika v obliko vladavine zaradi njenih značilnosti, delovanja idr., ne glede na to, kdo vodi državo. Politični cinizem je kompleksen in nejasno opredeljen pojav, priznavajo Schiffman et al. (2010), in se ga povezuje z nezaupanjem, nezadovoljstvom, prezirom, dvomom, razočaranjem. Čeprav naj bi izražal nezaupanje v politiko v negativnem smislu, se v pozitivnem smislu odraža kot gonilo vključevanja državljanov v politiko in udejstvovanja v politiki, vendar z nizkimi pričakovanji, da bodo zadovoljni, oziroma s pričakovanji, da bodo nezadovoljni (ibidem). Zaupanje v uslužbenca, tj. tretje področje obravnave, pa je odvisno od dejanj uslužbenca. Povsem normalno je, da se zaupanje v politiko sčasoma poveča, zaupanje v uslužbenca pa poveča ali zmanjša (ibidem). S tem se vračamo k obstoju povezav med institucionalnim in medosebnim zaupanjem, npr. majhno zaupanje organizaciji vpliva na zaupanje osebam, zaposlenim v organizaciji. Te povezave se kažejo tudi na področju javnega sektorja, kjer je zaupanje v posameznika veliko bolj dovzetno za večji in kratkotrajni upad kot pa zaupanje v institucijo, saj so te večje, splošne in neosebne, zato jih osebe težje ocenijo pravilno (Newton & Norris, 2000). Razlog za tako majhen vpliv na zaupanje v institucijo bi lahko pripisali tudi ugotovitvi, da ljudje v sodobnem času zaradi vedno bolj neosebnega modernega sveta bolj zaupajo institucijam kot pa posameznikom (ibidem).

Krajši pregled nekaterih študij in prispevkov, ki definirajo relevantne dejavnike zaupanja v politiko in javne institucije, prikazuje, kako različni avtorji prepoznavajo različne dejavnike. Katere dejavnike posamezni avtor izbere, je stvar njegovih vidikov obravnavanja ter stopnje zavednega ali nezavednega upoštevanja DTS. Ne glede na različne poglede in dejavnike je temeljno, da si lahko javni sektor pridobi zaupanje s pozitivnimi izkušnjami državljanov in njihovim spoštovanjem (Salminen & Ikola-Norrbacka, 2010). Storitve javnih institucij so posredni ali neposredni odraz države, (ne)zaupanje pa je odraz (ne)zadovoljstva državljanov s storitvami javnih institucij oziroma z državo. Kadar pride do nizkega zaupanja državljanov v institucije javnega sektorja, se pogosto pokaže potreba državljanov po kontroli (Makarovič, 2004) in uvedbi podrobnih aktov s konkretnimi določili (Camén, Gottfridsson & Rundh, 2011), ki bi uredili pomanjkljivosti in s tem dvignili zaupanje. Vendar ni vsako nezaupanje škodljivo (Salminen & Ikola-Norrbacka, 2010), tudi na nizko zaupanje ali nezaupanje v politiko, javno/državno upravo in državne organe ne smemo vedno gledati kot na nekaj

negativnega. Toš (2007, str. 368, opomba 2) namreč pravi, da je »v razvitih demokracijah […] nezaupanje predpostavka oz. nekaj normalnega in pričakovanega.« Tako menijo tudi tuji strokovnjaki, ki so ocenjevali nezadovoljstvo Slovencev z DZ (Fink Hafner et al., 2002). Določena raven nezaupanja je zdrava in učinkovita, saj je potrebna za vzdrževanje odgovornosti javnega sektorja (Salminen & Ikola-Norrbacka, 2010). Pomanjkanje zaupanja ne vodi vedno v nezadovoljstvo z javnimi storitvami, nasprotno pa zadovoljstvo s temi storitvami vpliva na izboljšanje zaupanja v javne institucije (ibidem). Kljub temu je težko pričakovati trden odnos med zaupanjem in politično dejavnostjo, saj se napajata iz različnih virov: zaupanje se napaja iz enakih mnenj, politična dejavnost pa iz nezaupanja v avtoriteto (Uslaner, 2004). Ker imajo politiki avtoriteto in skušnjavo, da avtoriteto zlorabijo, je vsak politični sistem postal sistem nezaupanja (Salminen & Ikola-Norrbacka, 2010).

Analiza zaupanja Slovencev v DZ (Fink Hafner et al., 2002) je pokazala, da ima zelo velik vpliv na zaupanje **(ne)znanje** o subjektu, ki mu oseba (ne) zaupa oziroma ga ocenjuje. Iz pomanjkanja znanja izhaja druga pomanjkljivost – napačno ocenjevanje dejanj drugih oseb (Tyler & Huo, 2002). Pomanjkljivo znanje javnosti o institucijah je razlog, zakaj javnost ne more izvajati strokovnega in učinkovitega nadzora institucij (ibidem), saj ne ve, kaj institucije smejo in česa ne smejo početi ter kaj bi morale in česa ne bi smele storiti niti kakšne ukrepe lahko javnost ali druge institucije sprejmejo v primeru neustreznega delovanja institucij. S takšnim problemom se srečuje tudi slovensko sodstvo. Med glavnimi razlogi za upad zaupanja je namreč »nerazumevanja funkcije sodišč v splošni javnosti,« (Igličar, 2012, str. 99) kar se kaže tudi v rezultatih raziskav javnega mnenja. Pri tem se moramo vprašati, kakšno in kolikšno znanje o slovenskem pravosodnem sistemu ima javnost ter od kod ji znanje in informacije.

Posebno dilemo v tem kontekstu predstavlja dejstvo, da nekateri poklici zahtevajo posebno znanje, ki ga javnost ne more imeti in ji ga ni mogoče na kratko pojasniti (Tyler & Huo, 2002). Tu ločimo znanja, ki jih javnost *ne more* imeti zaradi strokovne prezahtevnosti (npr. poznavanje dela kirurgov, kontrolorjev v kontroli zračnega prometa, strokovnjakov za delo s hadronskim trkalnikom), in znanja, ki jih javnost *ne sme* imeti. Dilema v zvezi s slednjim ni, ali je to dopustno ali ne, temveč kako lahko

javnost pozna institucije in njihovo delo, če je znanje nedostopno ali pa je dostop do znanja zelo omejen. Takšno znanje je javnosti navadno nedostopno zaradi nerazkrivanja metod dela, varnosti ali interesov, zaščite poslovnih interesov in poslovanja, (zagotavljanja) tajnosti ali pa zaradi drugih podobnih razlogov. Tajnost oziroma načelo tajnosti je »legitimno sredstvo, s pomočjo katerega se ščitijo vitalni interesi države« (Brezovšek & Črnčec, 2004, str. 506) in je namenjena »varovanju, obrambi in zaščiti obstoja države, njene ustavne ureditve ali posebnim interesom pri varovanju človekovih pravic.« (Anžič, 2000, str. 854) Zaradi tajnosti je npr. omejen dostop do določenega znanja, ki ga imajo pripadniki obveščevalno-varnostnih služb. Zato je povsem razumljivo in upravičeno, da javnost ne more in ne sme vedeti vsega o obveščevalno-varnostnih službah. Kljub temu je priporočljivo, po našem mnenju pa tudi nujno, da ima javnost vsaj osnovno znanje, ki ga je mogoče dobiti z javno dostopno literaturo. Z osnovnim znanjem bodo državljani vedeli, s čim se institucija ukvarja in kaj je njen namen, najpomembnejše pa je, da bodo znali ustrezno oceniti institucije in njihovo delo ter da se bodo znali zaščititi pred nepravilnostmi in zlorabami. Pri tem je ključno razločevanje med situacijami sodelovanja in situacijami zlorabe (Tyler & Huo, 2002). Javnost bi postala bolj seznanjena z motivi institucij in bi posledično lažje presojala, ali institucijam zaupati ali ne. Tyler & Huo (ibidem) namreč ugotavljata, da je poznavanje motivov ključ do ustrezne presoje dela institucij, kar jim omogoča pravilno presojo zaupanja v institucije. S tem, ko javnost zaupa njihovim motivom, je tudi bolj pripravljena sprejeti sporne odločitve ali konfliktne situacije, hkrati pa je tudi pripravljena sodelovati z institucijami – ne glede na odločitve institucije (ibidem).

Pripravljenost državljanov za sodelovanje je pomembno predvsem za tiste institucije, katerih delo je odvisno (tudi) od državljanov. Primer takšnih institucij so policijski organi. Kadar ljudje ne zaupajo policiji, ne upajo prijaviti kaznivih dejanj, prositi policijo za pomoč niti pomagati policistom, zato so policisti pri svojem delu manj uspešni (Flexon, Lurigio & Greenleaf, 2009). Opisano situacijo lahko primerjamo z nezaupanjem ali s pomanjkanjem zaupanja v varnostne in protiobveščevalne službe, ki delujejo predvsem na ozemlju države in so odvisne tudi od državljanov (npr. informacije, sodelovanje). To seveda ne pomeni, da bi morali z namenom izboljšanja zaupanja državljanov v matične obveščevalno-varnostne službe razkriti identiteto operativcev in jih npr. poslati na

obhode po ulicah, da bi jih ljudje opazili, saj bi s tem ogrozili svoje delo in delo službe, svoje življenje, življenja drugih ter nacionalno varnost in nacionalne interese. Bistvo ravnanja, kot je npr. napotitev policistov na patruljiranje, je opominjanje prebivalstva, da je institucija vključena v življenje državljanov, kar seveda ne odraža nujno učinkovitost, vsekakor pa kaže na aktivnost, povezanost z državljani in do neke mere tudi dostopnost za državljane. Čeprav obstajajo nekatere razlike med dejavniki zaupanja v javne institucije na splošno in v konkretne institucije, ugotavljamo, da imajo naslednje skupne dejavnike: percepcija strokovnosti in učinkovitosti institucij, poznavanje njihovega dela in njihovih motivov, zadovoljstvo z rezultati dela institucij ter njihovo ujemanje s pričakovanji.

Pomemben dejavnik je tudi etika javnega sektorja. Ta naj bi bila zagotovljena z zakonodajo in s krepitvijo etičnih vrednot v organizaciji, vendar zaradi vedno bolj kompleksnih problemov in pogostega preoblikovanja organizacij to dvoje ni vedno zagotovilo za izboljšanje etike. Do kršitev in spornega vedênja pride zaradi neustrezne uporabe ali zlorabe moči, kar vodi v slabo presojo, ki ustvarja pogoje za napačno ravnanje. S povečevanjem števila nepravilnosti in kršitev se povečuje možnost za pojav korupcije, kar vpliva na zaupanje državljanov. Te možnosti je mogoče zmanjšati s povečevanjem odgovornosti in z upoštevanjem pravil (Salminen & Ikola-Norrbacka, 2010).

Podpoglavje zaključujemo z ugotovitvijo, da je zaupanje v politiko oziroma državo in javno upravo ter njene institucije obsežna in kompleksna tema, ki smo jo morali obravnavati v ozkem, za naš vidik obravnavanja bistvenem segmentu, saj bi njeno širše obravnavanje presegalo zastavljene okvire doktorske disertacije. Kljub temu smo prišli do nekaterih pomembnih ugotovitev in dejavnikov, ki po naši presoji vplivajo na zaupanje državljanov v matične obveščevalno-varnostne službe.

4 Pomembnost zaupanja državljanov v matične obveščevalno-varnostne službe

Pregled dostopne literature je pokazal, da se z vprašanjem celovitega zaupanja državljanov v matične obveščevalno-varnostne službe še ni ukvarjal nihče, nekaj malega pa je različnih raziskav oziroma prispevkov, v katerih se avtorji bežno ukvarjajo z vprašanjem, *zakaj* državljani matičnim obveščevalno-varnostnim službam ne zaupajo. Splošnih razlogov, zakaj je temu tako, v dostopni literaturi nismo našli, obstaja pa literatura, ki ugotavlja upad ali izgubo tovrstnega zaupanja v določeni državi (glej npr. Phythian, 2005). V zvezi z obravnavano tematiko smo našli predvsem sporočila za javnost ali primere iz medijev, v katerih je bilo izpostavljeno zaupanje v obveščevalno-varnostne službe ali pa je bilo zaupanje obravnavano kot dejavnik z vplivom na delovanje teh služb. Tematika je v manjši meri obravnavana tudi v dokumentih, ki se nanašajo na reformo varnostnih sektorjev tranzicijskih in nekaterih drugih držav. Raziskovalci, akademiki, politiki in mednarodne organizacije ugotavljajo, da je bila v tranzicijskih ali post-konfliktnih državah za ponovno vzpostavitev javnega zaupanja v varnostni sistem potrebna reforma varnostnega sektorja (glej npr. Organizacija za gospodarsko sodelovanje in razvoj, 2007; Ebo, 2008). Obveščevalno-varnostne službe teh držav so bile v času njihovih nekdanjih režimov zlorabljene ter so sistematično kršile človekove pravice in svoboščine, zato ne uživajo oziroma niso uživale zaupanja državljanov (Organizacija za gospodarsko sodelovanje in razvoj, 2007). Te službe so bile pogosto vpletene v paralelne obveščevalne in varnostne strukture, ki so bile vpete v politične spletke in organizirani kriminal ter so izvajale (z današnjega vidika za Zahodni svet nelegitimen in ilegalen, op. G. H.) družbeni nadzor (ibidem).

Za vzpostavitev zaupanja v službe tranzicijskih držav je po priporočilih Organizacije za gospodarsko sodelovanje in razvoj (v nadaljevanju: OECD) potrebno ugotoviti legitimnost služb, racionalizirati njihove aktivnosti, odstraniti nezakonite operacije, po možnosti pa tudi združiti različne službe v eno novo organizacijo (Organizacija za gospodarsko sodelovanje in razvoj, 2007). Vendar pa to utegne povzročiti, da bo nova organizacija toga in da ji državljani ne bodo zaupali, kar lahko prepreči vzpostavitev

kompetentne in zaupanja vredne službe (ibidem). Nekatere nove službe so ob »preobrazbi« iz starih obveščevalno-varnostnih služb komunističnih režimov obdržale večino zaposlenih, opreme, nalog ipd. (Fitsanakis & Hodges, 2013), ugled novih služb pa je ostal enak prejšnjim službam – negativen. Državljani morajo pri spremembi stare ureditve obveščevalno-varnostnih služb tranzicijskih držav v novo ureditev zaznati spremembe v delovanju službe (Organizacija za gospodarsko sodelovanje in razvoj, 2007). Potrebno je tudi zagovarjati politiko ničelne tolerance do takšnih zlorab, kaznovati kršitelje in pa prepričati državljane, naj nimajo strahu pred obveščevalno-varnostnimi službami (ibidem).

Do sedaj navedeno naj bi pretežno veljalo za tranzicijske in post-tranzicijske države, nas pa je tudi zanimalo, kako je z zaupanjem v ostalih, »razvitih« državah. Ko ugotavljamo pomembnost zaupanja državljanov v matične obveščevalno-varnostne službe, lahko takšno zaupanje primerjamo z zaupanjem državljanov v druge (pod)sisteme javne uprave. Takšen primer je npr. zaupanje v javni zdravstveni (pod)sistem (Rădoi & Lupu, 2017, str. 12-13): »Zaupanje v zdravnike, medicinske strokovnjake, medicinske institucije in zdravstveni sistem je v zadnjem času pritegnilo pozornost raziskovalcev, pri čemer so obravnavali upad zaupanja […]. Upad zaupanja so povzročile tudi spremembe odnosa, vrednot in pričakovanj javnosti glede zdravstvenega sistema, pojav zasebnih zdravstvenih zavarovanj in zasebnih institucij, ekonomska kriza […]. Posledice takšnega vedenja je dvom javnosti v medicinsko znanosti in ljudi, ki sestavljajo zdravstveni sistem.« S podobnimi težavami se (je) sooča(lo) tudi slovensko sodstvo (Igličar, 2012, str. 99): »K zmanjšanju zaupanja v delovanje sodstva je pripomoglo več dejavnikov, od pojavljanja sodnih zaostankov in nepredvidljivosti sodnih rešitev prek aferaškega ter negativnega prikazovanja sodstva v medijih in nerazumevanja funkcije sodišč v splošni javnosti do tako imenovane sodniške stavke ter neustrezne in nepopolne zasedenosti sistemiziranih sodniških mest.« Če si izposodimo zadnje besede in jih nekoliko priredimo, ugotovimo, da je pomembnosti zaupanja v prej obravnavana (pod)sistema javne uprave primerljiva z obveščevalno-varnostnim področjem: *k zmanjšanju zaupanja v delovanje* ***obveščevalno-varnostnih služb*** *je pripomoglo več dejavnikov, od pojavljanja* ***domnevne nestrokovnosti*** *in* ***domnevne neučinkovitosti*** *prek aferaškega ter negativnega prikazovanja* ***obveščevalno-varnostnih služb*** *v medijih in nerazumevanja*

*funkcije **obveščevalno-varnostnih služb** v splošni javnosti.* S pomočjo pridobljene dostopne literature, intervjujev ter lastnega znanja in razmisleka smo poskušali bolj podrobno ugotoviti, zakaj je zaupanje državljanov v matične obveščevalno-varnostne službe tako pomembno. Izhajali smo iz domneve, da je takšno zaupanje pomemben zaviralec entropije obveščevalno-varnostnega sistema in sistema nacionalne varnosti.

Nekatere ključne segmente zaupanja v obveščevalno-varnostne službe je leta 2007 v javnem govoru izpostavil Jonathan Evans, nekdanji generalni direktor MI5. Spregovoril je o vlogi zaupanja javnosti in medijev v obveščevalno-varnostne službe, zato smo zaradi pomembnosti vsebine, ki se navezuje na predmet doktorske disertacije, citirali večji del govora (Security Service - MI5, 2007): »*[V]prašanje zaupanja je zelo pomembno za svet obveščevalno-varnostne dejavnosti.* […] *Javno zaupanje postaja vse pomembnejše vprašanje za številne organizacije, za javne in zasebne.* [MI5] *ni izjema, zato moramo zagotoviti, da je naše delo dovolj razumljivo. Čeprav morajo naše operacije ostati tajne, če želimo, da so uspešne, imamo odgovornost, da javnost obveščamo o grožnjah, s katerimi se sooča, in kaj počnemo, da bi jih odpravili.* […] *Javnost ima pravico razumeti način našega dela in naše razmišljanje o širši protiteroristični strategiji. In tukaj imate vi, mediji, ključno vlogo.* […] *Vendar moramo biti previdni, kjer obstaja potencial za kompromitacijo operacije ali, huje, javno varnost. Ko se to zgodi, predvsem zaradi odtekanja* [informacij, op. G. H.]*, je ključen premislek o posledicah. Prvo vprašanje mora biti, ali je javni interes objavljanja večji od morebitnih posledic* […]*. In ko se zahteva po novicah povečuje, si ne moremo privoščiti, da bi takšno razumevanje izginilo. Ne obstaja pogodba med obveščevalno-varnostnimi agencijami in mediji. Ne obstaja memorandum o medsebojnem razumevanju. To je stvar zaupanja.* […] *Stvar zaupanja ni nič novega v naši službi. Že skoraj 100 let tajno zbiramo podatke in vedno smo se zanašali na pripravljenost drugih, da nam dajo sledi, ki lahko rešijo življenja.* […] *In, seveda, zaupanje si je potrebno prislužiti.*«

O odnosu med obveščevalno-varnostnimi službami in mediji sta leto pred tem pisala red. prof. dr. Iztok Podbregar, takratni direktor Sove, in Jana Hibler, takratna in aktualna predstavnica Sove za odnose z javnostmi. Komuniciranje obveščevalno-varnostnih služb z javnostmi je namreč postalo del njihovega delovanja šele v prejšnjem desetletju.

Avtorja ugotavljata, da je na takšne spremembe vplivalo drugačno dojemanje demokracije, človekovih pravic in temeljnih svoboščin, zaradi teh vplivov pa je tudi prišlo do uvedbe nadzora obveščevalno-varnostnih služb. S tem je bila poudarjena pravica državljanov do informiranosti in seznanjenosti o delovanju tovrstnih služb, ki so morale sprejeti odgovornosti za informiranje javnosti. Avtorja tudi pravita, da je obveščanje javnosti (postalo) pomemben element pri razvijanju splošne varnostne kulture in učinkovitega kriznega komuniciranja, pripomoglo pa je k poznavanju, demistifikaciji, strokovnosti in transparentnosti služb. Te so bile postavljene pred nove izzive: o čem obveščati javnost in na kakšen način, predvsem pa kako ohraniti tajnost, vendar hkrati delovati javno? Svoje tajnosti ne smejo žrtvovati za pozitivno medijsko podobo, kljub temu pa je javnost potrebno seznaniti z vsemi grožnjami in nevarnosti, s katerimi se država sooča. Dodatno pa na njihov odnos z javnostmi vplivajo tudi sistema nacionalne varnosti, preteklost službe in pa negotovost pri vzpostavljanju oziroma razvijanju odnosa. Varnostne službe naj bi imele s komunikacijo manj zadržkov kot obveščevalne službe, namreč njihovo poročanje javnosti ne bi ogrozilo dela, saj delujejo v domovini. Nasprotno pa je z obveščevalnimi službami, ki delujejo v tujini, saj bi lahko njihovo razkritje imelo hude posledice za službo ali nacionalne interese (Podbregar & Hibler, 2006).

Več primerov poročanja javnosti zato najdemo na področju protiobveščevalne in varnostne dejavnosti. Npr. v Rusiji je od eksplozije stanovanjske stavbe v Moskvi leta 1999 dalje takratni direktor FSB, Nikolaj Patrušev, javnosti leta poročal o zadevah, ki so se nanašale na terorizem in na preiskave terorističnih napadov (npr. »Аслан Масхадов скорее жив, чем мёртв«, 2002) ter na končane protiobveščevalne operacije (npr. »ФСБ предотвратила антироссийские действия ЦРУ«, 2003). Državljani, ki zaupajo službam, jim bodo pripravljeni pomagati pri njihovem izvajanju protiobveščevalne in varnostne dejavnosti. Vpliv je obojestranski: služba s poročanjem obvešča, s čim se ukvarja in zakaj, zaradi česar so državljani seznanjeni s tekočimi zadevami, zaupajo službam in se počutijo (bolj) varne. Državljani pa so zato bolj pozorni na vsebino, ki jo izvejo od služb, in tudi bolj pripravljeni sodelovati na teh področij.

Morda je sedaj nekoliko lažje razumeti vpliv zaupanja državljanov v matične protiobveščevalne in varnostne službe, še vedno pa je zagotovo težje razumeti vpliv zaupanja v matične *obveščevalne* službe. Protiobveščevalne in varnostne službe delujejo predvsem v domovini in v povezavi z domovino, kjer je ključno pridobivanje podatkov in namigov tudi od matičnih državljanov, obveščevalne službe pa (praviloma) ne. Slednje namreč zbirajo podatke v tujini oziroma v povezavi s tujino. Običajen državljan bo zato težje videl pomembnost povezave med njim in matično obveščevalno službo. Kljub temu državljanov ne moremo obravnavati zgolj kot vir podatkov, temveč tudi kot podporni element. Ta podpora se izkazuje posredno, predvsem na področju podpiranja vodstva države, politike, subjekta, ki je zadolžen za menedžment nacionalnega obveščevalno-varnostnega sistema, ali izvajalca demokratičnega nadzora. Lahko bi rekli, da so obveščevalno-varnostne službe kot podporni servis vodstva države z vidika javnega mnenja in zaupanja povezane z javnim mnenjem in zaupanjem v vodstvo države: kdor podpira državo/politiko, podpira tudi politične odločitve, ki se sprejemajo na najvišji ravni. Nekatere odločitve temeljijo na obveščevalnih izdelkih obveščevalno-varnostnih služb, ki delujejo v skladu s predpisi in usmeritvami, ki jih je sprejela politika. A žal se državljani tega žal ne zavedajo zaradi pomanjkanja znanja o funkcijah obveščevalnih služb.

Če državljani ne zaupajo službam, hkrati pa ne zaupajo niti njihovim informacijam, ki jih uporablja politika, ne zaupajo nekaterim političnim odločitvam. Kljub povezanosti s politiko je potrebno obravnavati tudi samostojno vlogo služb. »Ena glavnih funkcij liberalne demokracije je, da so se posamezniki odpovedali nekaterim pravicam in svoboščinam v zameno za kolektivno varnost, ki jo zagotavljajo avtoritete. […] Zanaša se na pripravljenost državljanov, da zaupajo državi avtoriteto, ki ji je bila dana, kot tudi zagotovila, da država teh moči ne bo zlorabila proti državljanom. V trenutku, ko je zaupanje porušeno, državljani pričnejo iskati ukrepe, da bi si pridobili nazaj moč, ki so jo delegirali državi. […] Če je zaupanje zmanjšano ali postavljeno v dvom, bodo državljani pričeli izvajati aktivnosti, da dobijo nazaj kontrolo nad vlado. To vodi v razdor družbene pogodbe, v zavračanje sodelovanja državljanov z varnostnimi in obveščevalnimi službami ter v spremembo vlade ali, v najhujšem primeru, v revolucijo proti vladi.« (Lépine, 2014, str. 37, 38) Dogodkov, ki potrjujejo povezavo med družbeno pogodbo (v

tem primeru med državo in njenimi obveščevalno-varnostnimi službami ter državljani), je bilo v zadnjih nekaj letih več; omenimo npr. odziv ameriške in britanske javnosti na razkritje Edwarda Snowdena o ravnanju ameriških in britanskih obveščevalnih služb glede masovnega zbiranja podatkov ter na upor državljanov Severne Makedonije proti nekdanji vladi Nikole Gruevskega zaradi izkoriščanja služb za prisluškovanje državljanom.

Ti in tudi drugih primeri so prišli v javnost preko medijev. Ob tem velja omeniti, da od nekdaj obstajajo napetosti med demokratičnimi normami in prakso obveščevalno-varnostnih služb v demokratičnih ureditvah (Fitsanakis & Hodges, 2013), zato vsakršno spreminjanje zakonodaje, ki omeji delovanje obveščevalno-varnostnih služb, lahko povzroči nezadovoljstvo uslužbencev obveščevalno-varnostnih služb. Na drugi strani pa so lahko predpisi, ki urejajo delovanje obveščevalno-varnostnih služb, ravno zaradi afer, terorističnih napadov ali drugih razlogov spremenjeni brez podpore javnosti. Takšna primera sta že omenjeni širitvi pooblastil obveščevalno-varnostnih služb Združenega kraljestva ter francoskih policijskih in varnostnih organov v zadnjih nekaj letih. To med drugim tudi načelno dokazuje, da afere vplivajo na proces sprejemanja oziroma spreminjanja zakonodaje na področju obveščevalno-varnostne dejavnosti. Zaradi nezadovoljstva javnosti s sprejemanjem zakonodaje, ki izhaja iz afer, je zaupanje v matične obveščevalno-varnostne službe upadlo. Takšno vzročno-posledično zvezo lahko povežemo s prispevkom McKnighta & Websterja (2001), v katerem avtorja ugotavljata, da zavedanje, da smo pod nadzorom, lahko povzroči neprijetno počutje in tudi nezaupanje. Nekateri državljani se namreč bojijo, da bi službe brez posebnega razloga vdirale v njihovo zasebnost. Delovanja služb ne smemo razumeti kot »vohunjenje iz radovednosti«, vendar pa je zavedanje njihovega obstoja in delovanja tudi neke vrste preventivni mehanizem ali *sistem zavedanja*, kot ga imenujeta McKnight & Webster (2001), ki preprečuje ali zmanjšuje morebitno nezakonito delovanje državljanov. Če pa je takšen sistem zavedanja zlorabljen za vohunjenje in državljani to zaznajo, se bo pričela odvijati spirala kontrole in nezaupanja, ki bo zmanjšala medosebno in institucionalno zaupanje (ibidem). Zato je potrebno poskrbeti, da je vsakršno ravnanje in delovanje služb najprej zakonito, potrebno/nujno in upravičeno, nato pa da se ga ne zazna zaradi morebitne bojazni tistih državljanov, ki menijo, da obveščevalno-varnostne službe (ali policija) spremljajo vsakogar. Hkrati pa je priporočljivo državljane izobraziti, da je delo

obveščevalno-varnostnih služb nujno potrebno, vendar dopustno le, kadar je upravičeno, nujno potrebno in zakonito.

Pomanjkljivo znanje se povezuje z ugotovitvijo o močnem vplivu medijev na javno mnenje: če državljani nimajo dovolj znanja o obveščevalno-varnostnih službah (tudi zaradi tajnosti), so dovzetnejši za (tudi napačne, popačene ali zavajajoče) podatke in informacije o službah iz medijev in drugih virov, ki vplivajo na njihovo znanje in mnenje. S tem vplivajo tudi na njihovo zaupanje matičnim obveščevalno-varnostnim službam. Kadar je znanje državljanov o službah pomanjkljivo, bodisi zaradi pridobljenega znanja bodisi zaradi podatkov/informacij od drugih, je lahko ocena delovanja in organizacije obveščevalno-varnostnih služb pristranska, nekritična in neutemeljena, kar vpliva na zaupanje. V najhujšem primeru to lahko pomeni, da bodo nekritični državljani oziroma tisti državljani, ki nimajo ustreznega znanja, razmišljali v skladu z vsebino in usmeritvijo medijskih sporočil in javnega mnenja. V tem prepoznavamo **tveganje**, da se **neznanje državljanov** s pomočjo **medijske manipulacije** lahko izkoristi za korenite spremembe na tem področju. Obenem poudarjamo, da ne oporekamo opozarjanju medijev in javnosti, kadar so odkrite nepravilnosti obveščevalno-varnostnih služb očitne in utemeljene.

Kot zanimivost povzemamo nekatere rezultate raziskave o tem, koliko Britanci poznajo britanske obveščevalne službe (Faulkner Rogers, 2013). Rezultate je leta 2013 objavilo mednarodno podjetje YouGov, sodelovalo pa je 1.948 anketirancev starejših od 18 let. Raziskava je bila osredotočena na javno mnenje o tej temi in na primerjavo rezultatov z rezultati predhodno izvedenih raziskav o kršenju zakonodaje s strani britanskih obveščevalnih služb, o »žvižgačih« in o (preiskovalnih) pooblastilih služb za boj proti terorizmu. Hiter pregled rezultatov kaže, da naj bi anketiranci večinoma vedeli, kaj njihove službe lahko počnejo, pri odgovoru, kaj naj bi jim bilo dovoljeno, pa se niso strinjali le s prestrezanjem komunikacij. Na rezultat je najverjetneje vplivalo takratno razkritje »žvižgača« Edwarda Snowdena, da ameriške in britanske službe sodelujejo pri vohunjenju za lastnimi državljani (kar je protizakonito tako v ZDA kot v Veliki Britaniji). Anketiranci so zato imeli v zvezi s službami več znanja le o prestrezanju v telekomunikacije, o ostalih aktivnostih pa ne toliko. 51 % anketirancev je trdilo, da službam ne bi smelo biti dovoljeno kršenje zakonov v tujini, 35 % pa jih je trdilo, da jim

ne bi smelo biti dovoljeno vdiranje v tujo posest (ostalih 31 % je odgovorilo »Nič od tega/Ne vem«, 33 % pa se s tem strinja). Avtorji raziskave ugotavljajo, da so bili Britanci takrat bolj seznanjeni z delom obveščevalnih služb le zato, ker so dobili z aferami in razkritji drugačen vpogled v delo obveščevalnih služb, kot pa jih prikazujejo filmi o Jamesu Bondu (Faulkner Rogers, 2013).

Posebno zaskrbljujoče pa je pomanjkljivo znanje o obveščevalno-varnostnem področju tistih, ki se s to dejavnostjo pogosto srečujejo, so z njo povezani ali pa so od nje odvisni. Ko je bil Donald Trump kandidat za predsednika ZDA, je na vprašanje novinarke, ali zaupa obveščevalnim informacijam ameriških obveščevalnih služb, odvrnil: »Ne toliko [obveščevalnim informacijam] od ljudi, ki delajo to za našo državo. Poglejte, kaj se je zgodilo v zadnjih 10 letih. Bilo je katastrofalno. Ne bom uporabil tistih ljudi [tj. zaposlenih v obveščevalnih službah, op. G. H.], […] ker so naredili toliko napačnih odločitev.« Če sodimo po medijskih objavah in njegovih izjavah, ko je že bil predsednik, se njegov odnos do obveščevalno-varnostnih služb tekom njegovega predsedniškega mandata ni bistveno spremenil. Spomnimo se tudi zlorabe služb v ZDA in Združenem kraljestvu za dokazovanje obstoja orožja za množično uničevanje v Iraku, čeprav ga tam kasneje niso našli. S tem je bil, kot ugotavlja Phythian (2005), izgubljen velik del zaupanja Britancev v njihove matične obveščevalno-varnostne službe. Upad zaupanja v obveščevalne službe so ZDA doživele že prej, ugotavlja Gentry (2008), predvsem takrat, ko so javnost in politiki menili, da so bile službe presenečene in s tem nepripravljene. To se navezuje na teroristični napad 11. 9. 2001 v ZDA. Avtor (ibidem) prepoznava, da so bila neprimerna pričakovanja javnosti in politike do ameriških obveščevalnih služb glavni razlog za takšno mnenje. In če je temu res tako, potem je večina kritik na račun nekompetentnosti in večina predlogov za reforme napačnih (ibidem). Napačna ravnanja predvsem oseb, ki so na visokih položajih v državi in s svojim delovanjem vplivajo na obveščevalno-varnostno skupnost, lahko v samem bistvu izhajajo iz nevednosti oziroma pomanjkanja znanja o tem področju. Že omenjeni Jonathan Evans, nekdanji direktor MI5, je dejal (Security Service - MI5, 2007): »Dokler predajamo obveščevalne informacije drugim v uporabo, jim zaupamo, da jih bodo uporabili odgovorno.« Da vsi ne znajo ravnati z obveščevalnimi informacijami in s tajnimi podatki (kar je, domnevamo, posledica neznanja in slabe varnostne kulture), je po našem mnenju zagotovo dokazuje tudi primer, ko je Donald

Trump ruskemu zunanjemu ministru Sergeju Lavrovu na srečanju v Beli hiši leta 2017 razkril tajne podatke, ki so jih ameriške obveščevalne službe pridobile od tujih služb (domnevno od izraelskih). S tem je ogrozil ameriške in tuje obveščevalne vire ter posledično najverjetneje povzročil, da so ZDA izgubile zaupanje ali pa del zaupanja tujih obveščevalnih služb, hkrati pa da so ameriške obveščevalne službe težje zaupale predsedniku Trumpu. »Nobena obveščevalna služba ne tvega razkritja svojih virov. Zato imamo princip kontrole – služba, ki prva dobi informacijo, ima pravico nad kontrolo, kdo jo uporablja, s kom jo deli in kako ukrepati na podlagi informacije. […] Kadar so obveščevalne informacije razkrite, poskušajo ostali najti njihov vir. Agenti so lahko identificirani, aretirani, mučeni ali celo ubiti s strani iste organizacije, ki deluje proti nam. Če princip kontrole ni spoštovan, obveščevalni viri usahnejo,« je dejal Sawers (2010). Brez zaupanja lahko posredno na dolgi rok upade število tajnih sodelavcev – bodisi zaradi težjega pridobivanja le-teh bodisi zaradi njihovega nezadovoljstva ali občutka ogroženosti. Premalo zaupanja ali nezaupanje lahko zaradi javne podobe odbije potencialne kandidate, ki bi lahko postali njihovi uslužbenci. V obeh primerih pa se lahko zmanjša število pridobljenih podatkov, ki jih obveščevalno-varnostne službe zbirajo.

Pomembnost zaupanja prepoznava tudi Resolucija o strategiji nacionalne varnosti Republike Slovenije (Ur. l. RS, št. 27/2010, ReSNV-1): »V zapletenih razmerah finančne, gospodarske in socialne krize se lahko ogrožanje javne varnosti pojavlja v obliki povečanega obsega napadov na življenje in premoženje ljudi, gospodarske kriminalitete, korupcije, finančnih prevar, ponarejanje listin, denarja in blaga, kibernetske in okoljske kriminalitete ter množičnih kršitev javnega reda in miru. Ti pojavi lahko med prebivalstvom okrepijo **nezadovoljstvo z delovanjem ali vsaj nezaupanje v učinkovitost delovanja institucij nacionalnega varnostnega sistema** in države nasploh, **kar je dodaten element slabitve** posameznikove ter **nacionalne varnosti** [poudaril G. H.].«

4.1 Polstrukturirani intervjuji

Za pridobivanje podatkov, ki so pomembni za razjasnitev skritih ozadij obravnavanega problema, in za preverjanje pomembnosti zaupanja državljanov v matične obveščevalno-varnostne službe ter naših ugotovitev pred izgradnjo modela celovitega

zaupanja državljanov v matične obveščevalno-varnostne službe smo opravili šest globinskih polstrukturiranih intervjujev. Intervjuvanci so bili:

- **nekdanji direktor OVS**, ki je želel ostati neimenovan;
- **dva takratna aktualna uslužbenca Sove**, ki morata zaradi tajnosti ostati neimenovana (avtorji doktorske disertacije ne poznamo njunih identitet);
- **dva nekdanja uslužbenca Sove**, dr. Janez Žirovnik (nekdanji sekretar v Sovi in nekdanji namestnik direktorja Sove) ter drugi nekdanji uslužbenec Sove, ki je želel ostati neimenovan;
- **takratni podpredsednik KNOVS** mag. Matej Tonin (v mandatu DZ 2014-2018).

Vnaprej strukturirana vprašanja, ki smo jih zastavili intervjuvancem, se nahajajo v prilogi doktorske disertacije (priloga 1). Intervjuje smo opravili v obdobju januar–april 2018, in sicer z nekaterimi intervjuvanci osebno, z drugimi pa preko elektronske pošte. Intervjuvancem smo po potrebi zastavili dodatna (pod)vprašanja. Stik z aktualnima uslužbencema Sove smo navezali preko tretje osebe, zato njunih identitet ne poznamo. Preden prikažemo odgovore, izpostavljamo in odgovarjamo na komentar anonimnega nekdanjega uslužbenca Sove v zvezi z vprašanji od vključno št. 2 dalje: »*Naslednja vprašanja me preveč spominjajo na to, kakšno je zaupanje javnosti v policijo in vojsko. To je v področja, o katerih je javnost veliko bolj seznanjena z vlogo in aktivnostmi teh dveh institucij, saj se z njima, predvsem s policijo, srečuje vsak dan. Kakšna vprašanja naj bi po vašem mnenju vseboval vprašalnik, s katerim bi merili zaupanje v OS* [obveščevalne službe, op. G. H.], *če pa večina državljanov ne pozna vloge teh služb, razen tega, kar prebere ali sliši v medijih. To pa so predvsem afere, ki so običajno plasirane z določenim namenom.*« Z nekdanjim uslužbencem se strinjamo, da je javnost veliko bolj seznanjena z delom policije in vojske kot pa z delom obveščevalno-varnostnih služb. Namen ankete niti doktorske disertacije ni pripraviti orodje za merjenje zaupanja, saj bi – tako kot meni tudi nekdanji uslužbenec Sove – javno mnenje o službah lahko odražalo napačno in zavajajočo oziroma izkrivljeno podobo o službah, kar so ugotovili tudi nekateri drugi intervjuvanci.

Zaradi obsežnosti zbranih odgovorov vseh šestih intervjuvancev smo posamezne odgovore strnili in jih vnesli v matriko odgovorov (tabela 4.1).

Tabela 4.1: Matrika odgovorov intervjuvancev

INTERVJUVANEC / VPRAŠANJE	Dr. Žirovnik	Anonim. nekd. uslužbenec Sove	Uslužbenec Sove 1	Uslužbenec Sove 2	Nekd. direktor OVS	Mag. Tonin
Vprašanje 1 (V1)	Ne poznam realnega stanja v službah.	Ne poznam realnega stanja v službah.	Medijska podoba precej odstopa od realnega stanja.	Medijska podoba je bistveno slabša od realnega stanja.	Medijska podoba je slabša od ocenjenega realnega stanja.	Medijska podoba služb je negativna.
Vprašanje 2 (V2)	Javnost službam zaupa.	***Glej opombo 1***	V Sloveniji je zaupanje povprečno, dobro, v tujini pa je stanje zaupanja višje. Stanje zaupanja je pomembno.	Stanje zaupanja je na sredini lestvice zaupanja državljanov v državne organe. Stanje zaupanja je pomembno.	Zaupanja v te službe ni oziroma je zelo nizko, še posebej med politiki. V tujini (predvsem na Zahodu) imajo nekoliko rezerviran odnos do zaupanja tem službam.	Zaupanje v Sloveniji in tujini je majhno, ker imajo ljudje občutek, da gre za kršenje človekovih pravic in da službe preveč posegajo v njihovo zasebnost.
Vprašanje 3 (V3)	Politika.	Na to vprašanje ne morem odgovoriti, ker nisem zasledil nobenega novinarskega prispevka na to temo.	Mediji, strankarski interesi, interesi posameznikov, tuje OVS…	Sodobnih služb se drži negativna podoba nekdanjih služb.	Odsotnost nac. interesa za učinkovit sistem in ureditev stanja, slabo stanje mediji, »samozadostnost« in naivnost politikov ter njihovo neustrezno delovanje, politiki ne sprejemajo odgovornosti, neustrezni odnosi med službami, politiki in mediji, nestrokovni in neusposobljeni kadri	Mediji in odsotnost politične volje za spremembe na področju obveščevalno-varnostnih služb.

Opomba 1: »Pri tem vprašanju mi prvič ni jasno kaj mislite pod pojmom *matična*. Tudi na sploh se mi zdi to vprašanje preveč podobno vprašanju ali državljani zaupajo n.pr. policiji in vojski. Ker je delovanje teh dveh institucij javno ni nobenega problema, da se lahko s pomočjo ankete ugotovi kakšno je zaupanje javnosti v ti dve instituciji. Delovanje OS [obveščevalnih služb, op. G. H.] pa je tajno in skrito pred očmi javnosti. Zato bi vsako merjenje zaupanja v te službe dalo izkrivljeno sliko. Posebno v Sloveniji, kjer je v nekaterih krogih še vedno prisoten duh UDBE in njene vsemogočnosti. […] Za državljane pa je pomembno le to, da se v državi počutijo varne. In za Slovenijo to, vsaj trenutno še velja.«

Tabela se nadaljuje na naslednji strani

Nadaljevanje tabele 4.1

INTERVJUVANEC / VPRAŠANJE	Dr. Žirovnik	Anonim. nekd. uslužbenec Sove	Uslužbenec Sove 1	Uslužbenec Sove 2	Nekd. direktor OVS	Mag. Tonin
(nadaljevanje V3)					v službah, neustrezno kadrovanje, pomanjkanje domoljubja, nizka stopnja varnostne kulture, pomanjkljivo znanje (politikov, medijev, javnosti).	
Vprašanje 4 (V4)	Zaupanje ne vpliva na službe, saj morajo svoje delo opravljati profesionalno in neodvisno od javnega mnenja. Glede na dejstvo, da je Slovenija (še) varna država, službe delajo dobro, kar potrjuje mojo trditev.	Če je služba uspešna pri informiranju svojih naročnikov, nezaupanje državljanov ne bi smelo imeti vpliva na njeno delovanje.	Zaupanje ima velik neposreden in posreden vpliv. Neposreden se kaže v pripravljenosti državljanov za sodelovanje s službo, posredno pa je lahko signal vladi, kaj javnost pričakuje od službe. Posredno vpliva tudi na ugled, kar pomeni tudi merilo pri oceni učinkovitosti in uspešnosti službe.	Zaupanje je izredno pomembno. Nezaupanje ne pripomore k dobremu delu. Lahko načne motivacijo, pripadnost in požrtvovalnost zaposlenih.	Pri večini državljanov neposredno ne vpliva, zelo pa pri manjšem številu državljanov, ki bi zaradi svojih specifičnih možnosti (znanje, položaj, priložnosti ipd.) lahko vplivali na delo službe (primer: razkritje identitete uslužbencev). Posredno pa vpliva kot objekt politike, ko se državljani počutijo ogrožene – reakcija ob poslabšanju varnostnih razmer ali po kriznem dogodku. Takrat bi državljani v večini odobravali manipulativne predloge politike (za uresničevanje lastnih interesov).	Zaupanje državljanov je relativno nepomembno za vsakdanje delo služb – če te delajo in delajo v skladu z zakonom, zaupanje ne bi smelo vplivati na njihovo delo. Kljub temu pa je zaupanje pomembno, saj lahko družba zaradi nezaupanja ustvari pritisk oz. ozračje, ki vpliva na politiko. Politika pa lahko z vzvodi in orodji službe še bolj omeji ali jih razpusti in na novo organizira.

Tabela se nadaljuje na naslednji strani

Nadaljevanje tabele 4.1

INTERVJUVANEC / VPRAŠANJE	Dr. Žirovnik	Anonim. nekd. uslužbenec Sove	Uslužbenec Sove 1	Uslužbenec Sove 2	Nekd. direktor OVS	Mag. Tonin
Vprašanje 5 (V5)	Varnost.	Občutek varnosti.	Učinkovitost službe, občutek varnosti, krizni pojavi, medijska pokritost, podoba uslužbencev.	Odnos politike do OVS, način imenovanja direktorja in njegove ekipe, mediji, afere, nepoznavanje pomembnosti dela OVS. Najpomembnejši dejavnik je stopnja podpore vlade.	Sodelovanje, nadzor, financiranje, regulacija dejavnosti, ocena vložka in koristi pri graditvi zaupanja, pristojnosti in odgovornost organov, relacije med njimi.	Mediji, medijska prezentacija služb, nadzorniki (npr. komisija za nadzor obveščevalnih in varnostnih služb, op. G. H.).
Vprašanje 6 (V6)	Z zagotavljanjem transparentnega delovanja in srečanji s predstavniki medijev.	S strokovnim delom, s pripravo zakonodaje o delovanju Sove in demokratičnemu nadzoru nad službo (pri tem smo iskali podporo strokovne javnosti) ter s pripravo osnovne predstavitve Sove na njeni spletni strani.	Da, predvsem na področju varovanja ugleda službe.	***Intervjuvanec ni odgovoril na vprašanje.***	Z uvedbo in izvajanjem izobraževalnega programa za uslužbence in s predlogom, da se ustanovi Svet za nacionalno varnost, s katerim bi se izboljšala komunikacija med deležniki sistema nacionalne varnosti.	1. Prizadevanje za spremembo 25. člena ZPNOVS in za uvedbo mehanizma, s katerim bi preverjali verodostojnost (predvsem Sovinih) tajnih sodelavcev (***glej opombo 2***). 2. S predlogom reorganiziranja Sove in ponovne definicije njene vloge ter

Tabela se nadaljuje na naslednji strani

Opomba 2: Predlog za spremembo se je navezoval na sporno prakso Sove pri uporabi tajnih sodelavcev za pridobitev sodnih odredb za uporabo prikritih preiskovalnih ukrepov. V skladu s 25. členom Zakona o parlamentarnem nadzoru obveščevalnih in varnostnih služb (Ur. l. RS, št. 93/07) »pooblaščena skupina [za nadzor] ne sme vpogledati v tisti del dokumentacije nadzorovane službe, iz katerega bi bilo lahko razvidno, da v postopku delujejo ali sodelujejo tajni delavci oziroma sodelavci po določbah ZKP, ZObr in ZSOVA oziroma bi bila lahko razkrita identiteta teh tajnih delavcev ali sodelavcev.« S spremembo tega člena bi parlamentarna komisija lahko vpogledala v tisti del dokumentacije, iz katerega je razvidno delo s tajnimi sodelavci, in tako imela možnost, da pomaga vzpostaviti mehanizem za preverjanje kvalitete vira (tajnega sodelavca). K temu pa je mag. Tonin dodal, da razume, »da Sova ne more nadzornikom razkriti identitete teh sodelavcev, ker potem pade celotno obveščevalno delo in koncept celotne službe,« vendar pa je po njegovem mnenju »potrebno vzpostaviti nek mehanizem, da se lahko preverja kvaliteto tega vira in da če v preteklosti ta vir ni dajal zelo uporabnih informacij, potem neka "huda" informacija ne more biti pogoj za odreditev preiskovalnega ukrepa.«

Nadaljevanje tabele 4.1

INTERVJUVANEC / VPRAŠANJE	Dr. Žirovnik	Anonim. nekd. uslužbenec Sove	Uslužbenec Sove 1	Uslužbenec Sove 2	Nekd. direktor OVS	Mag. Tonin
Vprašanje 7 (V7)	Verjetno se, ni mi znano, koliko in kako.	Službe skrbijo za svojo podobo s predstavitvijo svoje dejavnosti na spletnih straneh.	Domnevam, da se.	Zagotovo se.	V tujini imajo boljši nadzor nad službami.	V tujini k stvarem pristopajo bolj resno od nas, npr. že pri parlamentarnem nadzoru imajo drugačno sestavo komisije in strokovno pomoč, ki je pri nas nimamo.
Vprašanje 8 (V8)	*Kako:* službe kot takšne ne morejo komunicirati z javnostjo, je pa naloga politike (vlada, KNOVS), da omejeno izpostavlja določene okoliščine v zvezi z delovanjem služb.	*Kako:* prevzeti pozitivne prakse iz tujine – komunikacija preko interneta. Politika služb ne sme uporabljati za »pranje umazanega perila.«	*Ovira:* službe svojih uspehov, rezultatov in koristi ne objavljajo v medijih, zato javnost nima informacije o njihovem doprinosu.	*Kako:* služba bi morala sama skrbeti za svojo javno podobo. Vlada bi morala pojasniti pomembnost obstoja in dela služb, na ustrezen način sporočiti javnosti, da je njihovo delo pomembno za vse. Potrebna je določena mera odprtosti (pozitivne izkušnje Zahoda). Pripomogla bi tudi višja stopnja varnostne kulture, predvsem medijev.	*Kako:* izboljšati učinkovitost in strokovnost služb ter pogojev za njihovo delovanje, izoblikovati strokovno svetovalno osebje (bivši uslužbenci služb in strokovnjaki). *Ovira:* ni resne politične volje za spremembe. Spremembe mora voditi predsednik vlade z dovolj politične podpore. Predsednik vlade mora razumeti varnostne grožnje in pomembnost teh služb za pridobivanje koristnih informacij za Slovenijo.	*Kako:* reorganizirati službe in parlamentarni nadzor, dodeliti nadzornikom strokovno svetovalno osebje (bivši uslužbenci služb in strokovnjaki). *Ovira:* ni resne politične volje za spremembe. Spremembe mora voditi predsednik vlade z dovolj politične podpore. Predsednik vlade mora razumeti varnostne grožnje in pomembnost teh služb za pridobivanje koristnih informacij za Slovenijo. *Ovire:* ni političnega interesa in zaupanja, (slovenske) službe niso dovolj strokovne.

Vir: Osebni vir

4.2 Analiza odgovorov

Analiza odgovorov na V1: Intervjuvanci, ki pravijo, da poznajo realno stanje, so podali skoraj enoten odgovor, da **medijska podoba slovenskih in tujih obveščevalno-varnostnih služb odstopa od realnega stanja**. Ta podoba je **negativna** in zato **prikazuje službe v slabši luči**. Zato lahko povzamemo, da medijska podoba in medijsko poročanje o službah po mnenju intervjuvancev ne prikazuje prave podobe obveščevalno-varnostnih služb.

Analiza odgovorov na V2: Na vprašanje, kakšno je po mnenju intervjuvancev stanje zaupanja državljanov v matične obveščevalno-varnostne službe v Sloveniji in tujini, **nismo dobili enotnega odgovora**. Aktualna uslužbenca Sove menita, da je zaupanje državljanov v te službe povprečno, srednje, dobro, medtem ko je v tujini večje, mag. Tonin pa meni, da je zaupanje majhno. Nekdanji direktor OVS je svojemu odgovoru dodal, da je indikator kritičnega stanja zaupanja državljanov v matične obveščevalno-varnostne službe, ko tem službam več ne zaupajo intelektualci. Ker nismo raziskovali mnenja večjega števila intelektualcev, težko presojamo, ali je trenutno zaupanje v kritičnem stanju ali ne. Glede na odgovore intervjuvancev težko zaključimo, ali službam zaupajo, ravno tako pa na podlagi odgovorov ne moremo domnevati, koliko jim zaupajo. Namesto tega izražamo **domnevo**, da državljani tem službam **zaupajo v manjši ali srednji meri** (rezultate manjše raziskave, koliko Slovenci zaupajo slovenskim obveščevalno-varnostnim službam, predstavljamo v podpoglavju 7.1). Vsekakor pa je bilo iz odgovorov mogoče razbrati, da večjega interesa za zaupanje v te službe ni – v povezavi s tem je mag. Tonin dejal, da še ni »srečal človeka, ki bi bil izjemno navdušen nad temi službami, da bi bil izjemno pozitiven glede tega.« Na vprašanje, ali je stanje (ne)zaupanja vredno pozornosti, smo dobili le dva neposredna odgovora, da je stanje (ne)zaupanja pomembno oziroma vredno pozornosti, pri nekaterih intervjuvancih pa smo dobili posreden odgovor, da je zaupanje pomembno le v smislu, kadar vpliva na službe preko politike, kar podrobneje analiziramo pri analizi odgovorov na V4.

Analiza odgovorov na V3: Intervjuvanci so našteli več dejavnikov oziroma razlogov, zaradi katerih je stanje zaupanja takšno, kot ga ocenjujejo. Med večkrat ponovljenimi in

izpostavljenimi so **politika**, **mediji** in **preteklost, nekdanje službe oziroma nekdanja podoba služb.** Poleg naštetih so omenili tudi interese posameznikov in političnih strank, tuje obveščevalno-varnostne službe, slabo stanje služb, neustrezne kadre v službah, neustrezne odnose med službami, nizko stopnjo varnostne kulture, pomanjkljivo znanje in še nekaj drugih.

Analiza odgovorov na V4: Odgovore intervjuvancev na V4 smo med seboj lahko povezali. Ugotovili smo, da **zaupanje državljanov vpliva** na matične obveščevalno-varnostne službe, **kadar** zaradi nezadovoljstva in/ali nezaupanja **ustvari pritisk na politiko oziroma na službo preko politike**, ki lahko z ustreznimi ukrepi vpliva na delovanje služb. Takšen vpliv prepoznavamo kot posredni vpliv zaupanja državljanov na matične obveščevalno-varnostne službe. Nekdanji direktor OVS opozarja, da je to **lahko rezultat manipulacije politike**, ki izkorišča razmišljanje javnosti (ki ga ustvari/oblikuje politika s svojim poročanjem preko medijev, op. G. H.) in njenega odziva na nek dogodek, da bi dosegla spremembe v delovanju in/ali organizaciji službe oziroma nacionalnega obveščevalno-varnostnega sistema. Polovica intervjuvancev pravi, da neposrednega vpliva ni oziroma ga ne bi smelo biti, saj javno mnenje in javno zaupanje ne bi smela vplivati na delo in profesionalnost uslužbencev. Nekdanji direktor OVS meni, da zaupanje neposredno vpliva le pri manjšem delu državljanov, ki zaradi določenih specifičnih možnosti (znanje, položaj, priložnost ipd.) lahko neposredno vplivajo na samo delo službe. Aktivna uslužbenca Sove pa trdita, da nezaupanje ne pripomore k dobremu delu uslužbencev, lahko načne njihovo motivacijo, pripadnost in požrtvovalnost, na drugi strani pa državljane odbija od sodelovanja s službo. Na podlagi njunih odgovorov **domnevamo, da obstaja neposreden vpliv** zaupanja državljanov v matične obveščevalno-varnostne službe, ki se kaže kot povezava med strokovnostjo uslužbencev in zaupanjem državljanov. Državljani se ne morejo drugače seznaniti s stanjem strokovnosti uslužbencev/službe kot preko izvajalcev nadzora oziroma preko medijev, ki jih nadzorniki obveščajo. Na podlagi medijskega poročanja se oblikuje javno mnenje, ki lahko ustvari že omenjeni pritisk na službo preko politike, mediji pa so tudi sredstvo za širjenje trenutnega javnega mnenja in novic, povezanih z javnim mnenjem. Čeprav bi lahko zaključili z ugotovitvijo, da obstaja relativna neposredna povezava med učinkovitostjo službe in zaupanjem državljanov vanje, pa tega ne moremo storiti, saj

medijska podoba odstopa od realnega stanja – kot so dejali intervjuvanci – in ne daje pravih informacij o službi. Na to namiguje tudi razmišljanje nekdanjega direktorja OVS, da se za tem skriva manipulacija politike. Po našem razumevanju odgovorov nekaterih intervjuvancev državljani (domnevno) prejmejo pomanjkljive, napačne ali zavajajoče informacije, zato ustvarijo svoje mnenje na podlagi poročanja o stanju, ki je drugačno od realnega. Eden od osrednjih problemov je torej **medijsko poročanje**, saj ima relativno velik vpliv na zaupanje, hkrati pa naj ne bi temeljilo na resničnih in popolnih informacijah. Razumemo stališče aktualnih uslužbencev Sove, da javno mnenje lahko vpliva na motivacijo uslužbencev (in posledično na njihovo strokovnost), kar je po našem prepričanju človeško, vendar morajo uslužbenci zato toliko bolj poskrbeti za to, da se zavestno ogradijo od kritik, ki temeljijo na pomanjkljivih, napačnih ali celo zavajajočih informacijah (medijskega poročanja). Te kritike **ne smejo** vplivati na njihovo delo.

Analiza odgovorov na V5: Vsak intervjuvanec je navedel dejavnike glede na svoje vidike obravnavanja, zato se pri tem nismo smeli odločiti, da so vidiki nadzornikov in aktualnih uslužbencev pomembnejši. Pomembni so *vsi* vidiki in zato *vsi* dejavniki, ki so jih intervjuvanci navedli. Naša naloga pa je bila ugotoviti, kako širok je nabor teh dejavnikov, ter prepoznati, kateri dejavniki izstopajo. Trije intervjuvanci so kot pomemben dejavnik vpliva na zaupanje prepoznali **občutek varnosti pri državljanih**. Drugi dejavniki, ki so jih navedli intervjuvanci, so (nekatere dejavnike smo za lažje razumevanje in klasifikacijo združili v »skupni« dejavnik): **krizni pojavi**, **afere**, **medijska podoba** (službe in uslužbencev), **mediji**, **politika** (npr. njen odnos do služb, način imenovanja vodje službe, poročanje o službah), **učinkovitost, delovanje in pogoji za delovanje služb** (npr. vodstvo, financiranje, sodelovanje, podpora vlade), **nadzor** (vse vrste) ter **poznavanje (pomembnosti) dela obveščevalno-varnostnih služb**.

Analiza odgovorov na V6: Pet intervjuvancev (eden ni odgovoril na vprašanje) se je **z vprašanjem zaupanja posredno ukvarjalo na različne načine**. Čeprav smo ugotovili, da so bile njihove aktivnosti bolj ali manj povezane z zaupanjem v obliki vplivanja na zaupanje, domnevamo, da se nihče od njih ni ukvarjal **konkretno z zaupanjem *državljanov*** v matične obveščevalno-varnostne službe. Kot izhaja iz njihovih odgovorov, so se ukvarjali z varovanjem ugleda in izboljševanjem javne podobe *službe*, s

povečevanjem strokovnosti *uslužbencev*, z izboljševanjem *nadzora* in predlogi za reorganizacijo *službe*. V intervjujih nismo zasledili, da bi se intervjuvanci ukvarjali s temi aktivnostmi izključno ali zaradi izboljšanja zaupanja državljanov v službe. Seveda dopuščamo obstoj dejstva, da so se intervjuvanci v svoji karieri ukvarjali z zaupanjem državljanov v službe, vendar tega iz intervjujev ni mogoče razbrati. Ne zmanjšujemo pomembnosti ali vrednosti njihovih dejanj – nasprotno, intervjuvancem vsekakor dajemo priznanje za veliko in pomembno delo, ki so ga opravljali oziroma ga opravljajo –, vendar ocenjujemo, da se z zaupanjem *državljanov* najverjetneje niso ukvarjali. Razlogov, zakaj je temu tako, nismo našli, saj za to nismo imeli pravih odgovorov niti po tem nismo spraševali.

Analiza odgovorov na V7: Po mnenju intervjuvancev **se v tujini (najverjetneje) ukvarjajo s problemom zaupanja**, le trije pa so odgovorili tudi na kakšen način: 1) službe skrbijo za svojo podobo z urejanjem spletne strani, 2) parlamentarni nadzor je bolj učinkovito zastavljen in organiziran (izobraževanje nadzornikov, nudena jim je tudi strokovna pomoč/podpora). Zaradi vsebinsko pomanjkljivih odgovorov ne moremo izoblikovati mnenja, na kakšen način se s problemom zaupanja ukvarjajo v tujini.

Analiza odgovorov na V8: K izboljšanju zaupanja bi pripomoglo **poročanje vlade o delu in pomembnosti obveščevalno-varnostnih služb**, politika pa služb **ne bi smela porabljati/zlorabljati** za politične igre in spletke oziroma za »pranje umazanega perila«, menijo intervjuvanci. Na zaupanje bi po njihovem mnenju pozitivno vplivalo tudi **izboljšanje učinkovitosti in strokovnosti služb**, **organizacija ustreznega (parlamentarnega) nadzora** nad službami, ki vključuje tudi strokovnjake za svetovanje, podporo in pomoč nadzornikom glede vsebine dela, **vzpostavitev/izboljšanje zaupanja med politiko in obveščevalno-varnostnimi službami** ter **sprememba načina dela in vedênja politikov** (prevzemanje odgovornosti, kritičnost) **v odnosu do teh služb**. Med predlogi, kako izboljšati zaupanje, je bila predlagana tudi **višja stopnja varnostne kulture** – **predvsem medijev**, ki bi morali biti pri poročanju o delu matičnih obveščevalno-varnostnih služb bolj kritični in neodvisni. Službe naj bi same skrbele za svojo javno podobo z urejanjem vsebin na svojih spletnih straneh, po zgledu in dobrih praksah zahodnih držav pa naj bi se delno odprle za javnost in z njo tudi komunicirale (preko

spletnih strani), menijo nekateri intervjuvanci. **Komunikacija z javnostjo** je hkrati tudi ena izmed **ovir**, ki jih intervjuvanci prepoznavajo v procesu izboljšanja zaupanja, saj je ta zaradi tajnosti bistveno omejena. Iz navedenega razloga javnost navadno ni seznanjena z rezultati in uspehi služb, pri čemer bi morala večjo vlogo odigrati vlada. Med pomembnimi ovirami je tudi pomanjkanje politične volje za spremembe na tem področju, iz odgovorov pa je mogoče tudi zaznati, da k temu pripomore pomanjkanje znanja.

Na podlagi odgovorov na vsa vprašanja ocenjujemo, da so intervjuvanci v svojih odgovorih (verjetno podzavestno) v večji meri opisovali stanje v Sloveniji kot pa v tujini, kar smo tudi pričakovali, saj jim je stanje »doma« bližje kot pa v tisto tujini. Zato dopuščamo možnost, da vsi odgovori niso dovolj celoviti za ustrezno obravnavo in vključitev v modeliranje. Menimo, da bi lahko z večjim poudarjanjem razlike med stanjem v Sloveniji in v tujini pridobili še več podatkov. Kljub temu ocenjujemo, da smo z intervjuji dobili dovolj podatkov, ki so potrdili naše domneve, ugotovitve in izhodišča za modeliranje ter opozorili na nekatera področja, na katera prej nismo bili pozorni ali pa jih nismo imeli za relevantne. Odgovori intervjuvancev se kljub manjšim nasprotovanjem pri posameznih vprašanjih (kar je po našem prepričanju posledica različnih vlog in različnih vidikov) relativno povezujejo in skupaj kažejo na podobne dejavnike. Odgovore smo zato lahko z določenimi omejitvami uporabili pri modeliranju splošnega modela zaupanja državljanov v matične obveščevalno-varnostne službe in kasneje modela celovitega zaupanja državljanov v matične obveščevalno-varnostne službe.

5 Modeliranje celovitega zaupanja državljanov v matične obveščevalno-varnostne službe

Model celovitega zaupanja državljanov v matične obveščevalno-varnostne službe ter smernice za logistiko aplikacije tega modela predstavljajo izvirni znanstveni prispevek doktorske disertacije. Z modelom bomo »poizkušali pridobiti sposobnosti vplivati na objekt/e, na stvarnost,« (Mulej et al., 2008, str. 99) namreč »[p]odročje varnosti s svojimi storitvami […] še ne zagotavlja zaupanja, je torej potreben pogoj, ni pa tudi zadosten.« (Kovač & Trček, 2007, str. 7) Po nam znanih podatkih, pridobljenih z analizo literature, medijskih prispevkov in opravljenih intervjujev, stopnja zaupanja državljanov v matične obveščevalno-varnostne službe ni visoka. Kot izhaja iz analize literature, ki jo obravnavamo v doktorski disertaciji, in opravljenih intervjujev, bi vzpostavitev in izboljšanje tovrstnega zaupanja pozitivno vplivala ne le na nacionalni obveščevalno-varnostni sistem, temveč tudi na celotno nacionalno varnost države. Osnovo modela smo izgradili s pomočjo obravnavanih definicij in modelov zaupanja iz 3. poglavja doktorske disertacije, tako kot so splošni model zaupanja izgradili tudi Gambetta (2000) ter Schoorman, Mayer & Davis (2007). Sestavili smo ga iz splošnih in specifičnih dejavnikov, ki vplivajo na zaupanje, njihovih povezav ter odnosov (soodvisnosti) med seboj in z okoljem, njihovih sinergij in njihovih vlog (uteži) ter dejavnikov obveščevalno-varnostnega sistema. Védenje, katere dejavnike, v kolikšni meri (teža posameznih dejavnikov) in na kakšen način jih je bilo potrebno vključiti v model, smo dosegli z upoštevanjem DTS in DOMR.

Kot smo že pojasnili v uvodu doktorske disertacije, je zaupanje specifično glede na kontekst obravnave (Martin, 2014), kar sta ugotovila že Lewicki & Bunker (1996, str. 115), ki pravita, da vsaka disciplina različno pristopa k obravnavi zaupanja. Pri tem raziskovalci namenjajo premalo truda in pozornosti integraciji med seboj različnih si vidikov in s tem pojasnjevanju glavne vloge zaupanja kot pomembnega dejavnika v družbenih procesih (npr. sodelovanje, koordinacija, delovanje). Tudi drugi tuji avtorji (npr. Zand, 1972; Morgan & Hunt, 1994; Mayer et al., 1995; Kahan, 2001; Tan & Thoen, 2001; Schoorman et al., 2007; Laeequddin et al., 2010) so prepoznali tveganje »izolacije«

posameznih področno-specifičnih definicij zaupanja, torej njihovo »ne-aplikacijo« na druga področja, zato so se v teoriji izoblikovali predlogi splošnih modelov zaupanja, ki združujejo prepoznane bistvene značilnosti definicij zaupanja z različnih področij. Seveda pa se tudi ti splošni/generični modeli med seboj razlikujejo. Izgradnja modela zaupanja, ki združuje različne definicije in poglede na zaupanje, ni preprost postopek, ugotavljajo Doney et al. (1998, str. 603): »Razvoj integriranega modela zaupanja je zaradi nedoločenosti in posebnosti definicij zaupanja po številnih disciplinah in orientacijah še posebej težko.« Na področju zaupanja nismo strokovnjaki/specialisti, zato ne trdimo, da je končna struktura našega modela pravilna, upamo pa, da smo bili pri svojem delu dovolj celoviti. Z upoštevanjem pravil DTS in DOMR smo model strukturirali na podlagi sestavin, ki so z našega vidika obravnavanja pomembne in potrebne za zadostno in potrebno celovito razreševanje izbranega problema. Bosch & Nguyen (2015, str. 4) pravita: »Tudi takrat, ko vidimo, da je ''nekaj narobe s sistemom'', imamo težnjo analizirati problem z razstavljanjem sistema na manjše in manjše dele, pri čemer iščemo tisto, kar je krivo, dokler ne pričnemo izgubljati pogled na interakcije med elementi.« DTS in DOMR sta nam preprečevala pretirano posploševanje in pretirano osredotočanje na podrobnosti.

Izgradnjo končnega modela smo razdelili na dve fazi. V prvi fazi smo modelirali splošni model zaupanja državljanov v matične obveščevalno-varnostne službe, pri katerem smo vhode določili s spoznanji iz literature ter s spoznanji in z izkušnjami intervjuvancev, izhod splošnega modela pa je zaupanje v službe, vendar brez predznaka (pozitivno ali negativno, večje ali manjše ali nespremenjeno). Ta splošni model predstavlja vmesni izid doktorske disertacije, tj. model, po katerem bi zaupanje državljanov v matične obveščevalno-varnostne službe ustvarili kot podlago za netehnološki invencijsko-inovacijsko-difuzijski proces ustvarjanja in vzdrževanja celovitega zaupanja državljanov v matične obveščevalno-varnostne službe. Predstavlja prvi korak postopka dela z upoštevanjem sistematične hevristike – analizo procesa, prikaz procesa kot sistema (Mulej, 1979). Struktura splošnega modela prikazuje, kako zaupanje nastane oziroma se spreminja in kateri dejavniki vplivajo na ta proces.

V drugi fazi pa smo na podlagi zakona zadostne in potrebne celovitosti ter z uporabo DTS, DOMR, USOMID/NOVOST in TVS/MVS s postopkom modeliranja preoblikovali splošni model zaupanja v model celovitega zaupanja državljanov v matične obveščevalno-varnostne službe. Ta hkrati predstavlja poenostavljen kibernetski sistem. Vhod v drugo modeliranje (to ni vhod v model-sistem!) je bil *splošni model* zaupanja državljanov v matične obveščevalno-varnostne službe. Ta faza je hkrati predstavljala drugo in tretjo fazo postopka dela z upoštevanjem sistematične hevristike – optimizacijo in sintezo strukture procesa, tj. ustvarjanje novega procesa (Mulej, 1979). Ustvarili smo nov proces, ki ustvarja in vzdržuje dovolj celovito zaupanje državljanov v matične obveščevalno-varnostne službe.

5.1 Splošni model zaupanja državljanov v matične obveščevalno-varnostne službe

Za izhodišče za izgradnjo splošnega modela smo uporabili definicijo zaupanja, ki smo jo izoblikovali v 3. poglavju doktorske disertacije:

*Zaupanje je **psihološko stanje** oziroma **prepričanje upnika**,*
*da bo zaupnik **izpolnil upnikova pričakovanja,***
*zato je **pripravljen sprejeti tveganja in biti ranljiv,***
*saj je zaupnika **ocenil kot ustrezno entiteto**, ki je to pripravljena in sposobna storiti.*

Nato smo izbrali osrednjo tipologijo zaupanja, na kateri temelji ogrodje predlaganega modela. Odločili smo se za institucionalno zaupanje, ki ne sili v posameznika v zaupanje, temveč le ustvarja *ugodne pogoje*, da posameznik lahko oziroma lažje zaupa drugim. Ugodne pogoje razumemo kot pogoje, ki posameznika prepričajo, da mu bo okolje dolgoročno zagotavljalo pozitivno podporo za dovolj celovito zaupanje. Zaradi posebne vloge nadzora (in tudi drugih dejavnikov, kot ugotavljamo kasneje) kot *tertiusa* pa smo uporabili tudi tipologijo transakcijskega zaupanja.

Sledila je določitev osrednjih sestavin modela in njihovih povezav, ki sestavljajo ogrodje modela. Ker smo kot pomembni povezavi upoštevali zakon hierarhije zaporedja in soodvisnosti, smo lahko preverili, katere sestavine so najbolj vplivne kot izhodišča osrednjega procesa našega modela. Tako smo se že na začetku izognili upoštevanju mnenj stroke in politikov, da je najpomembnejši dejavnik (demokratični) nadzor nad obveščevalno-varnostnimi službami. Namesto tega smo s pomočjo naše delovne definicije zaupanja izhajali iz objektivnih izhodišč (potrebe in (z)možnosti) in subjektivnih izhodišč ter jih določili kot osrednji (najvplivnejši) sestavini našega modela. Za osnovne pogoje, v katerih se zaupanje ocenjuje, ustvarja, vzdržuje, zmanjšuje in spreminja v nezaupanje, sta namreč potrebna (vsaj) dva subjekta, zato tudi dve sestavini. Ti sestavini sta ***Državljan*** (upnik) in ***Matična obveščevalno-varnostna služba*** (zaupnik). Čeprav iz naslova doktorske disertacije izhaja, da model obravnava zaupanje državljanov (množina) v matične obveščevalno-varnostne službe (množina), je bilo potrebno izhajati iz državljana kot posameznika in najprej obravnavati njegovo zaupanje v posamezno tovrstno službo. Upoštevali smo, da zaupanje v posamezno službo vpliva na celoten podsistem in posredno tudi na sistem višjega reda. Pri tem smo tudi upoštevali, da selektivno zaupanje v zgolj eno službo lahko negativno vpliva na celotni nacionalni obveščevalno-varnostni sistem. Če ima en podsistem (tj. ena služba) podporo državljanov v obliki zaupanja, drugi podsistemi (službe) pa iz upravičenih ali neupravičenih razlogov ne, to lahko zamaje ravnovesje in stabilnost nacionalnega obveščevalno-varnostnega sistema, kar bi pospešilo njegovo entropijo. To bi vplivalo tudi na njegove sisteme nižjega (npr. posamezne službe) in višjega reda (sistem nacionalne varnosti). Z začetno obravnavo državljana (ednina) kot upnika in s tem osnovne sestavine zaupanja se tudi preprečuje, da bi posameznik v primeru skupinske obravnave ostal neupoštevan. Brez upoštevanja njegove vloge ciljni model doktorske disertacije namreč ne bi bil dovolj celovit – vsaj z našega vidika obravnavanja ne.

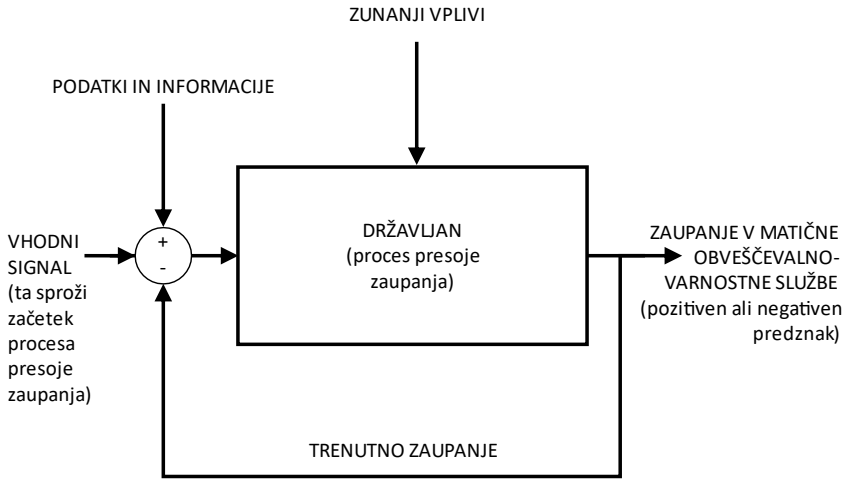
Po določitvi osrednjih dveh sestavin smo nadaljevali z oblikovanjem ogrodja oziroma koncepta splošnega modela. Ogrodje temelji na teoretskih konceptih in modelih zaupanja, ki izhajajo iz angleškega izraza *trust*: zaupanje mora temeljiti na dokazih, ki niso povsem trdni ali popolni, in na čustvih. Nevarno bi bilo obveščevalno-varnostnim službam zaupati le na podlagi dokazov (*confidence*) ali čustev oziroma slepega

prepričanja (*faith*). Da bi preprečili pojav ali zahajanje v eno ali drugo skrajnost, ki jo v teoriji sistemov poznamo kot nevarno enostranost, smo sestavini *Državljan* dodali upoštevanje vpliva čustev in razuma. S tem smo upoštevali, kot je dejal Mulej (2018, osebni vir), racionalno in iracionalno, ki tvorita podlago za zaupanje.

Pri določanju strukture ogrodja smo si pomagali z obravnavanimi modeli iz podpoglavja 3.4. Analiza je pokazala, da jim manjkajo vhodi, izhodi in povratne zveze. Ker družbeni sistemi niso zaprti sistemi in ker zaupanje z našega vidika obravnavanja ne sme biti zaprt sistem, so vhodi, izhodi in povratna zanka nujne sestavine našega modela. Pri tem je bilo potrebno upoštevati, da zaupanje lahko nastopa kot vhod in izhod.

Obe sestavini smo obravnavali kot podsistema predlaganega modela-sistema. Konceptualni model podsistema *Državljan* prikazuje slika 5.1, medtem ko konceptualnega modela podsistema *Matična obveščevalno-varnostna služba* nismo izoblikovali, saj so te službe v praksi različno izoblikovane.

Slika 5.1: Konceptualni model podsistema *Državljan*



Vir: Osebni vir

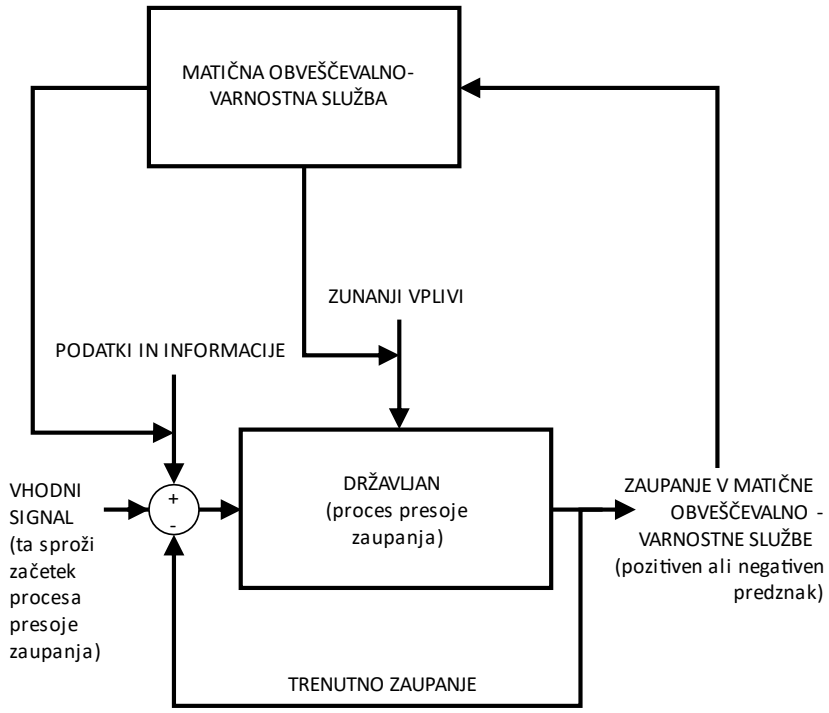
Izhajajoči iz definicije, da je zaupanje »*psihološko stanje* oziroma *prepričanje upnika*,« trdimo, da se glavni proces predlaganega modela odvija v državljanu. Ostale sestavine

modela, ki smo jih kasneje dodali, so sicer pomembne zaradi njihovega vpliva na procese v državljanu, s katerimi presoja, ali sploh oziroma koliko zaupati matičnim obveščevalno-varnostnim službam, vendar imajo vlogo vhodov v podsistem *Državljan* oziroma dejavnikov vplivanja na podsistem *Državljan*. Čeprav so procesi presoje zaupanja, ki se odvijajo v državljanu, notranji procesi podsistema *Državljan*, imajo zaradi narave zaupanja osrednjo vlogo. Te procese smo združili v enega in ga poimenovali ***proces presoje zaupanja***. Upnik z njim presoja oziroma ocenjuje, ali bo zaupnik *izpolnil upnikova pričakovanja* in ali je zaupnik *ustrezna entiteta*, ki je to pripravljena in sposobna storiti. Proces se prične, ko podsistem *Državljan* dobi signal za začetek presoje zaupanja. Ta signal lahko zavzame eno izmed različnih pojavnih oblik, npr. občutek ogroženosti zaradi terorizma, vojaških spopadov ali drugih negativnih varnostnih dogodkov, afere, izjava vlade, ministrstva ali drugega organa, ocena izvajalcev (demokratičnega) nadzora obveščevalno-varnostnih služb, pogovor z znancem o obveščevalno-varnostnih službah, medijska novica, fotografija na spletni strani, knjiga ali film z vsebino o obveščevalno-varnostnih službah, priklic spomina idr. Kljub različnim pojavnim oblikam je signal vedno *podatek*, ki sproži miselni proces v posamezniku. Nato državljan aktivno ali pasivno pridobi iz okolja tudi druge podatke ter informacije iz lastnega znanja. Podatke in informacije smo zato prepoznali kot vhod v podsistem *Državljan*. Ugotovili smo, da poleg podatkov in informacij na zaupanje vplivajo tudi stopnja trenutnega zaupanja (povratna zveza/vhod) ter zunanji vplivi. Stopnja trenutnega zaupanja vpliva na iskanje podatkov in informacij oziroma dokazov, kar je še posebej tvegano pri majhnem zaupanju ali nezaupanju, ko lahko trenutno nezaupanje postane vir lastnih dokazov (Gambetta, 1988), vpliva pa tudi na iskanje skupnih interesov med upnikom in zaupnikom. Manjše kot je zaupanje, manj bo odkritih skupnih interesov (Robbins, Judge, Odendaal & Roodt, 2009). Kadar pa državljan nima dostopa do podatkov in informacij iz okolja, pa se bo zanašal na tiste iz znanja oziroma spomina.

Osnovno ogrodje splošnega modela zaupanja državljanov v matične obveščevalno-varnostne službe tako sestavljata podsistem *Državljan* in podsistem *Matična obveščevalno-varnostna služba* (slika 5.2). To ogrodje predstavlja koncept splošnega modela zaupanja državljanov v matične obveščevalno-varnostne službe, ki smo ga

postopno dopolnili z drugimi bistvenimi in ostalimi, za boljše razumevanje problematike potrebnimi sestavinami, povezavami, vhodi in vplivi.

Slika 5.2: Koncept splošnega model zaupanja državljanov v matične obveščevalno-varnostne službe



Vir: Osebni vir

Nato so sledile dopolnitve koncepta oziroma ogrodja. Kot ugotavlja Cajner Mraović (2004), število in kakovost kontaktov državljanov z državnimi organi ter dvosmerna komunikacija neposredno vplivajo na zaupanje državljanov. Pri odnosu državljanov z matičnimi obveščevalno-varnostnimi službami smo ugotovili, da običajna dvosmerna komunikacija, na podlagi katere bi državljan pridobil želene podatke in informacije za proces presoje zaupanja, zaradi tajnosti ni vedno mogoča. Ker je tajnost nujna za zagotavljanje in uresničevanje nacionalne varnosti in interesov, obveščevalno-varnostne službe ne smejo komunicirati z državljani o občutljivih temah v »polnem obsegu« niti jim ne smejo razkriti tajnih podatkov. S tajnimi podatki se lahko seznanijo le tisti, ki imajo pravico in potrebo po seznanitvi ter so uspešno prestali varnostno preverjanje (slednji pogoj ni vedno obvezen, saj npr. v Sloveniji in tudi v tujini obstajajo izjeme, ki ne potrebujejo varnostnega preverjanja za dostop do tajnih podatkov). Državljani morajo

komunikacijo s službo zato nadomestiti z drugo aktivnostjo, ki jim bo pomagala pri procesu presoje zaupanja. Zato smo namesto komunikacije uporabili izraz ***proces pridobivanja znanja***. Ta proces je sestavljen iz različnih kognitivnih procesov, kot so zaznavanje, učenje, komuniciranje, asociiranje in sklepanje. S tem izrazom v tem kontekstu pojmujemo vse aktivnosti aktivnega in pasivnega pridobivanja podatkov in informacij o matičnih obveščevalno-varnostnih službah **od njih in od drugih subjektov**. V kontekstu institucionalnega zaupanja naj bi podatki in informacije prihajali od organizacije (Rus, 2008). Ker pa obveščevalno-varnostne službe državljanov ne seznanjajo s svojim delom na način in v tolikšni meri, kot to počnejo drugi organi javne uprave, je mogoče pričakovati, da bodo državljani manj vedeli o njihovem delu, torej jim bodo tudi težje zaupali. Takšna situacija ustvarja **situacijo negotovosti**, ki vpliva na nezaupanje (Luhmann, 1988), zato smo ob analizi literature o zaupanju spoznali, da bo upnik v primeru pomanjkanja/pomanjkljivih podatkov in informacij **iskal druge vire**. Z našega vidika obravnavanja je to pomembno dejstvo. Upoštevati smo morali, da – tudi zaradi odsotnosti ali pomanjkljivega znanja državljanov o matičnih obveščevalno-varnostnih službami – državljani pridobivajo znanje oziroma iščejo podatke in informacije pri sorodnikih, prijateljih, znancih, strokovnjakih, politikih, v medijih ter v drugih virih. V strukturi zaupanja državljanov v matične obveščevalno-varnostne službe je zato potreben vmesni členi, ***tertius***, **tretja oseba/stran**. V organizacijah in bolj kompleksnih okoljih se zaupanje oblikuje tudi po t.i. principu električnih omrežij, kot temu pravi Hosmer (1995, str. 388): Mi drugi osebi zaupamo, če jo nadzoruje tretja oseba, ki jo nadzoruje četrta oseba, četrto osebo nadzoruje peta oseba itd. Pri tem obstaja tveganje, da kadar en člen v tem omrežju popusti (navadno najšibkejši), celotno omrežje ostane brez elektrike – od tod tudi poimenovanje principa po električnih omrežjih. Tretje osebe so del principa električnih omrežjih in hkrati nastopajo kot pomemben element v transakcijskem zaupanju. Nastopajo v različnih funkcijah, v našem kontekstu predvsem kot osebe ali organizacije, ki imajo/so imele stik in/ali izkušnje z matičnimi obveščevalno-varnostnimi službami, zato imajo o njih nekatere podatke in informacije oziroma nekaj znanja. Kot **tretje osebe** smo prepoznali predvsem subjekte, ki izvajajo (demokratični) nadzor nad obveščevalno-varnostnimi službami **na podlagi predpisov** (npr. parlamentarni odbori, splošna in specializirana sodišča, ombudsmani, drugi (neodvisni) organi), in subjekte, ki izvajajo nadzor **v lastnem interesu** oziroma **v**

interesu javnosti, vendar ne na podlagi predpisov (npr. mediji, strokovna javnost, laična javnost, neodvisni preiskovalni novinarji, drugi posamezniki). Med tretje osebe za potrebe doktorske disertacije ne štejemo notranjega nadzora, saj je ta del matične obveščevalno-varnostne službe, zato nima vloge tretje osebe. Spoznali smo, da imajo prej našteti nadzorni subjekti dvojno vlogo, in sicer da:

1. zbirajo in posredujejo podatke in informacije ter da
2. z izvajanjem nadzora povečujejo gotovost državljanov o pravilnem in zakonitem delovanju nacionalnega obveščevalno-varnostnega sistema.

Predvsem zaradi druge vloge lahko nadzor pojmujemo kot **mehanizem ali sredstvo za povečanje gotovosti**. Gotovost namreč izboljšuje upnikovo prepričanje o (večji) koristi, ki jo lahko pridobi z zaupanjem v matične obveščevalno-varnostne službe.

Zaradi odsotnosti tretje strani je bil koncept splošnega modela zaupanja (slika 5.2) pomanjkljiv za nadaljnje delo, zato smo mu morali dodati druge sestavine, ki bodo podsistemu *Državljan* posredovale potrebno znanje za dovolj celovito presojo zaupanja ali pa mu vsaj omogočile pridobivanje znanja. Poleg sestavin *Državljan* in *Matična obveščevalno-varnostna služba* smo preostale sestavine modela celovitega zaupanja državljanov v matične obveščevalno-varnostne službe določili na podlagi:

1. *predhodne analize relevantnih splošnih in specifičnih modelov zaupanja*: izbira relevantnih splošnih modelov zaupanja, analiza njihovih sestavin in povezav ter izbira delov, ki jih je mogoče uporabiti za modeliranje našega modela;
2. *izbire sestavin na podlagi analize druge dostopne literature*: iskali smo sestavine, ki bi utegnile dopolniti sestavne dele iz obravnavanih splošnih in specifičnih modelov zaupanja, organizacije sistema nacionalne varnosti in nacionalnega obveščevalno-varnostnega (pod)sistema ter jih ustrezno (soodvisno) povezati. Do teh sestavin smo prišli z analizo literature, ki se navezuje na zaupanje, in z literaturo, ki se ukvarja s področjem (ocenjevanja) javnega mnenja (npr. Bernik, Malnar, Pollack, Pickel & Müller, 2014; Eurobarometer, 2015);
3. *izbire sestavin, pridobljenih z intervjuji*: zadnja faza predstavlja dopolnjevanje »mozaika« s sestavinami, ki se odražajo kot vidiki drugih specialistov, s katerimi želimo in hkrati tudi moramo sodelovati, saj le tako lahko delamo/delujemo celovito

in dosežemo celovitost. Te sestavine so delni rezultat postopka USOMID/NOVOST, saj vključuje pridobivanje in izmenjavo znanj z drugimi specialisti ter s tem različne vidike, pomembne za obravnavo našega izbranega problema;

4. *izbire drugih sestavin*: te smo določili s pomočjo lastnega znanja, izkušenj, domnev, predpostavk in spoznanj ob upoštevanju drugih izbranih sestavin.

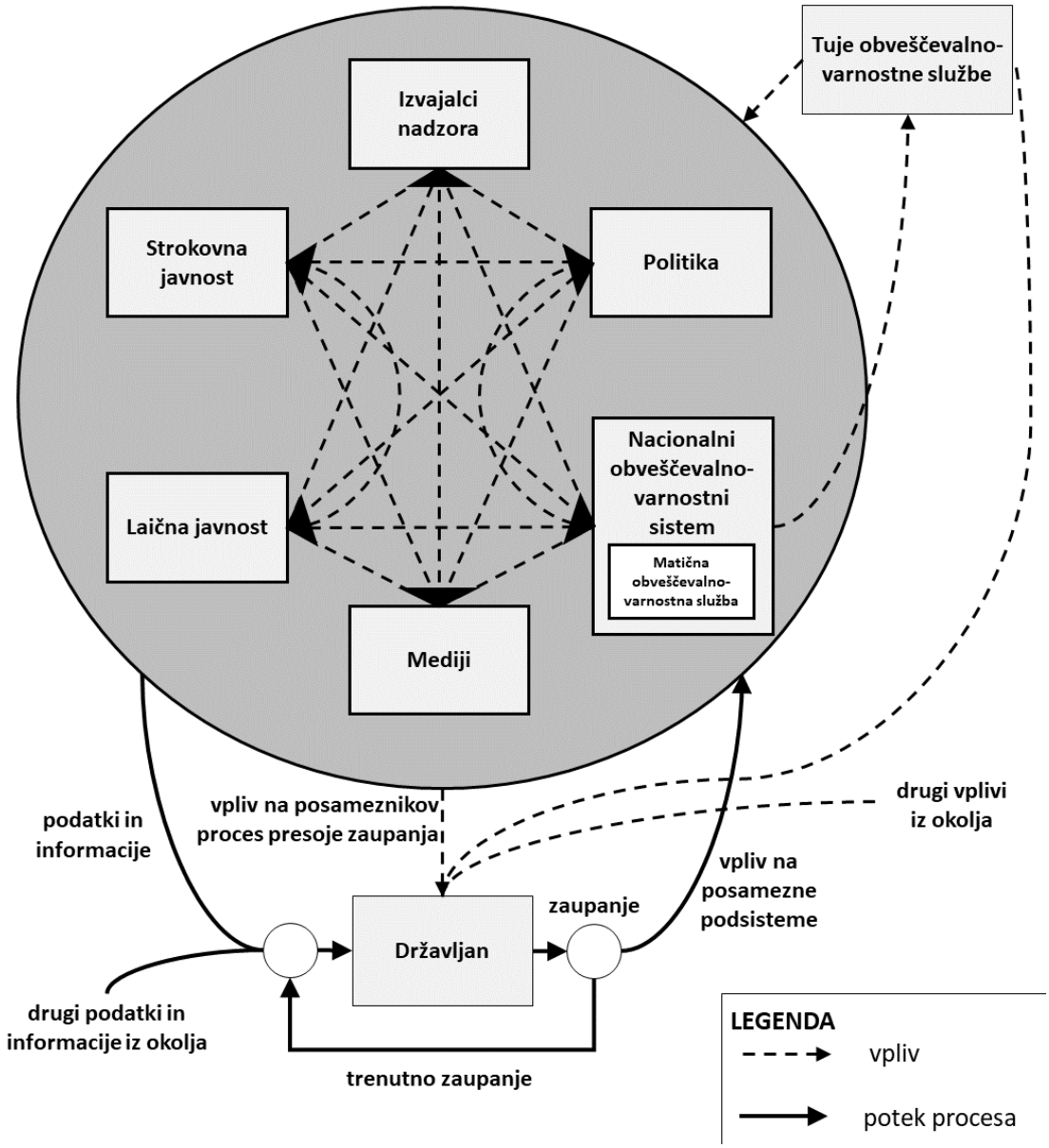
Prepoznali smo preko 110 dejavnikov, ki smo jih z našega vidika obravnavanja ocenili kot potencialne sestavine modela. V obravnavani literaturi je sicer mogoče najti tudi druge dejavnike, ki z našega vidika obravnavanja niso (bili) relevantni oziroma pomembni, zato jih tudi nismo upoštevali kot potencialne dejavnike. Kako smo vedeli, katere dejavnike, v kolikšni meri (teža posameznih dejavnikov) in na kakšen način jih poleg že določenih dveh temeljnih sestavin vključiti v model, smo dosegli z DOMR (Rosi & Mulej, 2006; Rosi & Rosi, 2011; Rosi, 2015) in z upoštevanjem DTS (Mulej, 1979; Mulej et al., 2000, 2008) oziroma z opredelitvijo dialektičnega sistema vidikov, pomembnih za naše obravnavanje izbranega problema. Ključno je bilo tudi sodelovanje z drugimi specialisti v obliki intervjujev.

Prepoznali in določili smo naslednje sestavine splošnega modela zaupanja državljanov v matične obveščevalno-varnostne službe (sestavine niso navedene v nobenem posebnem vrstnem redu): **državljan, matična obveščevalno-varnostna služba, nacionalni obveščevalno-varnostni sistem, politika, izvajalci nadzora obveščevalno-varnostnih služb, strokovna javnost, mediji**, **laična javnost** in **tuje obveščevalno-varnostne službe**. Ob upoštevanju DTS in sistematične hevristike smo naš model-sistem splošnega zaupanja državljanov v matične obveščevalno-varnostne službe najprej opredelili kot podmnožico podsistemov, šele nato pa smo podrobno opredelili posamezne podsisteme.

5.1.1 Konceptualni model povezav dejavnikov zaupanja

Naslednja slika (slika 5.3) prikazuje splošni model kot konceptualni model povezav dejavnikov zaupanja in njihove medsebojne vplive.

Slika 5.3: Splošni model zaupanja državljanov v matične obveščevalno-varnostne službe



Vir: Osebni vir

Slika 5.3 prikazuje povezave in medsebojne vplive med podsistemi. Ti podsistemi samostojno ali skupaj z drugimi podsistemi vplivajo na posameznikov proces presoje zaupanja, hkrati pa predstavljajo vire podatkov in informacij, potrebnih za proces presoje zaupanja v matične obveščevalno-varnostne službe. Zaradi preglednejše sheme smo dialektični sistem dejavnikov (podsistemov) zaradi medsebojnega vpliva in soodvisnosti povezali v krog, obarvanega s temno sivo barvo, zato vse črte, ki potekajo v/iz kroga, ponazarjajo potek podatkov in informacij oziroma vpliva v/iz enega ali več

podsistemov (odvisno od konteksta). Na enak način smo zaradi preglednosti prikazali tudi posameznikov vpliv na posamezne podsisteme – puščica je usmerjena v sivi krog, namesto v vsak podsistem posebej. Pozorni bralci bodo ugotovili, da je puščica *vpliv na posamezne podsisteme* neprekinjena, čeprav gre za vpliv in bi morala biti prekinjena, saj ponazarja (smer) potek(a) procesa in hkrati vpliv državljana. Na sliki 5.3 nismo označili, kateri podsistemi imajo pomembnejšo vlogo pri posredovanju podatkov in informacij oziroma pri vplivanju.

Kot smo že pojasnili, predstavljajo vhode v podsistem *Državljan* **podatki in informacije**, **trenutna stopnja zaupanja**, dodatno pa tudi **zaupanje v kontrolne mehanizme**.

Podatki in informacije, ki jih državljan oblikuje v znanje, navadno pridejo iz okolja (na sliki 5.3 predstavlja okolje vse, kar se nahaja zunaj podsistema *Državljan*), lahko pa pridejo tudi iz državljana, natančneje iz njegovega znanja. Če pridejo iz državljana, se ti podatki in informacije (kot obstoječe znanje) v procesu skupaj z drugimi podatki in informacijami oblikujejo v novo znanje. Za sprejem vhodov Beer (1981, str. 39) pravi, da so potrebni ustrezni receptorji, ki bodo pretvorili informacije (pravilno bi bilo »podatke«, op. G. H.) iz zunanje situacije v afektivni kanal, za njihovo zbiranje oziroma shranjevanje pa t.i. senzorni register. Ti dve komponenti sestavljata osnovno komponento kontrolnega sistema (ang. *control system*) (Beer, 1981). V našem primeru je ta komponenta »sestavni del« človeka in je sestavljena iz njegovih čutil, sposobnosti zaznavanja, obravnave podatkov in pomnjenja ter spomina. **Trenutno zaupanje** oziroma **trenutno stopnjo zaupanja** je potrebno razumeti kot stopnjo zaupanja državljanov v matične obveščevalno-varnostne službe do trenutka, preden je državljan pričel ponovno presojati zaupanje. Trenutno zaupanje nastopa v procesu presoje zaupanja kot predhodno stanje, hkrati pa bi lahko rekli, da deluje kot osnova za (ponovno) presojo zaupanja. Pri začetni izgradnji zaupanja je vrednost trenutnega zaupanja lahko »enaka 0«, zato takrat ne vpliva na proces presoje zaupanja, kasneje pa je vrednost praviloma višja ali nižja. Trenutno zaupanje ima v splošnem modelu funkcijo povratne zveze (ang. *feedback*). Povratna zveza je osnovni princip v kibernetiki in pomeni, da preteklo stanje posredno ali neposredno vpliva na novo stanje, zato bistveno vpliva na dinamiko in obnašanje sistemov (Kljajić, 1994). »Obstoj povratne zveze napravi sistem bolj zapleten

glede strukture in omogoča boljše in kvalitetnejše delovanje, oz. ji sploh omogoča delovanje. Brez povratne zveze živi organizmi sploh ne bi mogli obstati, tehnični sistemi ne bi mogli kvalitetno delovati, organizacijski sistemi bi razpadli.« (ibidem, str. 26) Poleg tega brez povratne zveze »ne bi mogli imeti izkušenj, brez tega pa bi bilo učenje nemogoče […].« (ibidem, str. 28) Izkušnje in učenje kot del procesa pridobivanja znanja sta pomembna dejavnika procesa presojanja zaupanja, zato mora biti trenutno zaupanje kot povratna zanka del podsistema *Državljan* in s tem del splošnega modela zaupanja državljanov v matične obveščevalno-varnostne službe.

Med vhode smo uvrstili tudi **zaupanje** oziroma **stanje zaupanja v kontrolne mehanizme**, ki izhaja iz generičnega modela zaupanja avtorjev Tan & Thoen (2001). V 3. poglavju smo ugotovili, da se zaupanje v drugo osebo in v kontrolne mehanizme medsebojno dopolnjujeta. Kadar je zaupanja v drugo osebo malo, mora biti več zaupanja v kontrolne mehanizme, ki bo nadomestilo manjše zaupanje v drugo osebo (in obratno) in s tem pripomoglo k preseganju praga zaupanja. Zaupanje v kontrolne mehanizme je posledica posameznikovega zaznavanja institucionalnih oziroma kontrolnih mehanizmov kot tveganj, ki vplivajo na stopnjo institucionalnega zaupanja (Laeequddin et al., 2010). To je tudi razlog, zakaj med vhode nismo uvrstili tveganja. Tveganje po našem prepričanju ni vhod, saj ga ne moremo procesirati, ima pa posreden vpliv na zaupanje preko *dojemanja tveganja*. Slednje je odvisno od državljanove kognitivne in afektivne komponente. Iz tega izhaja, da je **dojemanje tveganja odvisno od vsakega posameznika posebej**. Poleg tega tveganje kot táko ne vstopa v proces zaupanja; v proces vstopajo *podatki o tveganju*, ki jih državljan subjektivno dojema. Skupaj z zaupanjem v kontrolne mehanizme vplivajo na »izračun«, ali se splača tvegati oziroma zaupati. Zato tveganja nismo prepoznali niti določili kot vhod v sistem, temveč kot dejavnik vpliva, iz katerega prihajajo podatki in informacije. Zaupanje v kontrolne mehanizme moramo torej razumeti kot dopolnilo in ne kot nadomestek za zaupanje, s katerim se ustvarja ugodne pogoje, da bi upnik zaupal zaupniku. Ker se tveganje lahko pojavi v različnih oblikah in izhaja iz različnih okolij, poleg tega pa je njegovo zaznavanje vezano na kontekst, ga nismo dodali na sliko 5.3. V kontekstu zaupanja državljanov v matične obveščevalno-varnostne službe ima zaupanje v kontrolne mehanizme pomembno vlogo, saj je prepričanje, ki ga samostojno oblikuje državljan, zaradi malo podatkov in informacij navadno premajhno (kar je posledica

tajnosti in posebnosti delovanja obveščevalno-varnostnih služb), da bi ustvarilo prepričanje, ki bi preseglo prag zaupanja.

Izhod iz splošnega modela zaupanja državljanov v matične obveščevalno-varnostne službe je le eden: zaupanje v matične obveščevalno-varnostne službe. Vrednost izhoda je negativna (nezaupanje) ali pozitivna (zaupanje), vendar niti ta niti končni model ne predvidevata kvantifikacije vrednosti izhoda. Zaupanje kot izhod vodi v **zaupljivo vedênje** kot odraz ali »materializacijo« zaupanja. Državljan lahko zaupa ali pa ne zaupa službi, ni pa nujno, da bo to tudi pokazal in se temu ustrezno vedel. Zaupljivo vedênje ni posebej prikazano na sliki 5.3, saj ga je potrebno razumeti kot enega izmed možnih načinov vplivanja na posamezne podsisteme (puščica *vpliv na posamezne podsisteme*). Vplivanje na posamezne podsisteme je lahko neodvisno od zaupanja in s tem od zaupljivega vedênja; npr. posameznik zaupa obveščevalno-varnostni službi in to tudi vsakemu pove, vendar je podpisal peticijo za spremembo zakonodaje za zmanjšanje pooblastil tovrstnim službam. Čeprav službi zaupa, njegov podpis (vpliv) ne odraža njegove naklonjenosti službam.

V nadaljevanju smo podrobno predstavili podsisteme, ki tvorijo splošni model zaupanja državljanov v matične obveščevalno-varnostne službe.

5.1.2 Državljan

Zaradi osrednje vloge državljana in njegovega procesa presojanja zaupanja smo največ pozornosti namenili oblikovanju podsistema *Državljan*. Podsistem *Državljan* bi sicer lahko obravnavali kot podsistem kateregakoli drugega podsistema, ki se na sliki 5.3 nahaja v sivem krogu, saj so tudi uslužbenci obveščevalno-varnostnih služb in drugi uslužbenci nacionalnega obveščevalno-varnostnega sistema, politiki, nadzorniki, pripadniki strokovne javnosti in posamezniki, ki delujejo na področju medijev, državljani. Takšnega vidika obravnavanja nismo uporabili, saj smo podsistem *Državljan* obravnavali kot posameznega **državljana, ki je sicer del laične javnosti** in o matičnih obveščevalno-varnostnih službah nima veliko znanja, vednosti in informacij, zato je bolj dovzeten za

(namerno) pomanjkljive ali napačne informacije o teh službah – to velja za laično javnost na splošno.

Različni psihološki, kognitivni, afektivni in drugi procesi, ki skupaj sestavljajo presojo zaupanja, se odvijajo znotraj posameznika. Vendar sta nas nekdanji direktor OVS in mag. Tonin v intervjuju opozorila, da bi bilo potrebno podrobneje pojasniti, na kaj konkretno v zvezi z matičnimi obveščevalno-varnostnimi službami se navezuje zaupanje državljanov. Mag. Tonin je v zvezi s tem izpostavil dve vrsti zaupanja:

- splošno zaupanje, ki odraža pozitiven ali negativen odnos do služb glede na to, kakšna verjetnost obstaja po mnenju ljudi, da službe posegajo v njihovo zasebnost;
- zaupanje, da službe delajo nekaj dobrega za državo.

Pri iskanju odgovora na vprašanje, na kaj konkretno se navezuje zaupanje, smo si pomagali z modelom zaupanja v policijo (slika 3.9). Začetni sestavini prikazanega modela sta zaupanje v efektivnost policije in zaupanje v poštenost policije. Ti dve sestavini samostojno vplivata na končno zaupanje v delo policije, posredno pa preko zaupanja v vključenost policije v okolje in skupne vrednote policije in državljanov. Na primeru obveščevalno-varnostnih služb bi lahko rekli, da srednje sestavine (*Zaupanje vključenosti policije in skupne vrednote*) na primeru obveščevalno-varnostnih služb ne moremo presojati, saj se naloge obveščevalnih služb izvaja predvsem v tujini, pripadniki varnostnih služb pa se iz operativnih razlogov in zaradi tajnosti ne razkrivajo (v) javnosti. Pomembnejši sta začetni sestavini, ki sta zelo podobni temu, kar je dejal mag. Tonin, zato smo obe sestavini primerjali z vrstama zaupanja, ki ju je mag. Tonin navedel v intervjuju (tabela 5.1).

Na podlagi primerjave lahko za prvo vrstico obeh stolpcev rečemo, da sta vidika zelo podobna temu, čemur v doktorski disertaciji pravimo *ustreznost entitete*. Druga vrstica pa izraža prepričanje, vezano na pričakovanja o rezultatih, kar v doktorski disertaciji imenujemo *izpolnjevanje pričakovanj*. Ustreznost entitete in izpolnjevanje pričakovanj sta dve sestavini naše definicije zaupanja, zato ocenjujemo, da smo s tem ustrezno pojasnili, na kaj konkretno se navezuje zaupanje državljanov.

Tabela 5.1: Primerjava dveh vidikov: na kaj se navezuje zaupanje državljanov

mag. Tonin o vrstah zaupanja v obveščevalno-varnostne službe	**model zaupanja v policijo (Jackson & Bradford, 2010)**
splošno zaupanje, ki odraža pozitiven ali negativen odnos državljanov do služb glede na to, koliko službe posegajo v njihovo zasebnost	zaupanje v poštenost policije
zaupanje, da službe delajo nekaj dobrega za državo	zaupanje v efektivnost policije

Vir: Osebni vir (intervju) in Jackson & Bradford, 2010

Če našo splošno definicijo zaupanja prilagodimo zaupanju državljana v matično obveščevalno-varnostno službo, bi se ta glasila:

*Zaupanje državljana v matično obveščevalno-varnostno službo je **psihološko stanje***
*oziroma **prepričanje državljana**,*
*da bo obveščevalno-varnostna služba **izpolnila njegova pričakovanja,***
*zato je državljan **pripravljen sprejeti tveganja in biti ranljiv,***
*saj je službo **ocenil kot ustrezno entiteto**, ki je to pripravljena in sposobna storiti.*

Ker se zaupanje navezuje na tisto, kar državljan presoja pri procesu ustvarjanja oziroma oblikovanja medosebnega zaupanja (v odnosu do matične obveščevalno-varnostne službe), institucionalnega zaupanja in dispozicijskega zaupanja, smo za modeliranje podsistema *Državljan* uporabili interdisciplinarni model konstruktov zaupanja (McKnight & Chervany, 2001; glej sliko 3.2), dopolnjeni model začetne izgradnje zaupanja (povzet po McKnight et al., 1998, str. 476, dopolnjen z McKnight & Chervany, 2001 in lastnimi dopolnitvami; glej sliko 3.3), koncept kognitivnega in afektivnega zaupanja, koncept OOOD zanke (Mirzaie et al., 2012; glej sliko 3.5) in posamezne izbrane elemente iz druge obravnavane literature.

Mayer et al. (1995) pravijo, da so različni avtorji s svojimi konceptualizacijami zaupanja potrdili dejstvo, da zaupanje kot pojav ni objektivna realnost/resnica, temveč percepcija upnika, zato Brower et al. (2000) dodajajo, da je merjenje oziroma merilo zaupanja

subjektivna, individualna stvar. To potrjuje našo ugotovitev, da upnikova percepcija ali sposobnost zaznave močno vpliva na zaupanje, torej na proces presoje zaupanja. Das & Teng (2004, str. 95) celo pravita, da se večina teoretikov strinja, da je zaupanje pravzaprav zaznavanje drugih v odnosu do sebe. Zaznavanje ali percepcija vpliva na zaupanje v posameznika, to pa vpliva tudi na zaupanje v organizacijo (Schoorman et al., 2007). O pomembnosti percepcije v okviru zaupanja državljanov v matične obveščevalno-varnostne službe govori tudi Črnčec (2009, str. 14): »Potrebno je razmišljati ne le o organizacijskih spremembah, temveč o *spremembah v percepciji ljudi* [poudaril G. H.], delavcev, pripadnikov obveščevalnih struktur ter tudi razumevanju te nove potrebe znotraj obveščevalnih struktur na strani naročnikov, uporabnikov in nadzornikov obveščevalnih produktov.« Zaradi spoznanja, da percepcija pomembno vpliva na zaupanje, smo jo obravnavali, vendar le v segmentu **dejavnikov, ki vplivajo na oblikovanje percepcije**. S preobširnim obravnavanjem te tematike bi presegli okvir doktorske disertacije.

Percepcija je »čutno dojemanje predmetnega sveta; zaznavanje« (Percepcija, b. d.) oziroma proces zaznavanja, odzivanja na informacije in njihovega klasificiranja na način, da se s prepoznavanjem vzorcev iz okolja in njihove analize oblikuje mentalni model za prepoznavanje sveta okoli nas (Mohammadi & Banirostam, 2015). Tudi Vila (1994) podobno definira percepcijo kot »proces, s pomočjo katerega posameznik izbira, organizira, zbira, memorira (pomni) in interpretira informacije, zbrane s pomočjo svojih čutil.« Percepcija in mentalni model predstavljata dve različni stvari, ki sta medsebojno povezani, med njima pa poteka dvosmerna komunikacija (Mohammadi & Banirostam, 2015). Mentalni model ponazarja subjektivno sliko, ki je posledica zaznanega – podobno pravijo tudi Mulej et al. (2008), in sicer da je model ponazoritev sistema, ne objekta kot celote, zato odraža subjektivni in delni prikaz sistema. Percepcija neprestano oblikuje mentalni model z zaznavanjem okolja. V literaturi (npr. Mayer et al., 1995; Robbins et al., 2009; Pourtios, Schettino & Vuilleumier, 2013; Mohammadi & Banirostam, 2015; Yang, Penton, Köybaşı & Banissy, 2017) najdemo več dejavnikov, ki vplivajo na percepcijo, npr. učenje, znanje, spomin, pričakovanja, izkušnje, pozornost, čustva, starost, potrebe, želje/interesi, motivacija, vrednote, fizično stanje, spol, prepričanja, kako bi stvari morale biti, odnos osebe do drugih, situacija, bližina in podobnost z drugo osebo, gibanje, zvoki,

velikost, ozadje, novosti, družbeni vplivi, poznavanje problema, organizacijski kontrolni mehanizmi, prednosti, koristi in izgube. Od percepcije je odvisno, v kakšni obliki gredo ti podatki in informacije, ki jih posameznik zbira iz okolja, v nadaljnjo obravnavo v procesu presoje zaupanja. Dejali pa smo že, da posameznik pri presoji zaupanja črpa iz znanja oziroma spomina, kadar pa v njegovem znanju ni ustreznih podatkov, jih poskuša pridobiti **iz okolja**.

Analiza literature je pokazala, da je zaupanje opredeljeno tudi kot kognitivna in afektivna percepcija (Johnson & Grayson, 2005; Wan Ahmad & Mohamad Ali, 2016). Na podlagi delitve na **kognitivno** in **afektivno percepcijo** (Wan Ahmad & Mohamad Ali, 2016) smo preučili relevantnost koncepta kognitivnega in afektivnega zaupanja ter njegovo uporabo pri izgradnji našega modela. Ugotovili smo, da koncept kognitivnega in afektivnega zaupanja dopolnjuje (dopolnjeni) model začetne izgradnje zaupanja (glej sliko 3.3 oz. 3.12) z afektivno komponento, ki je v omenjenem modelu ni. S tem smo upoštevali naše izhodišče, tj. zaupanje v obliki *trust*, ki predstavlja razmerje med intelektom/razumom in med čustvi. Zato smo podsistemu *Državljan* dodali dve sestavini ter ju poimenovali ***kognitivna komponenta*** in ***afektivna komponenta***. Kognitivna komponenta, ki je v dopolnjenem modelu začetne izgradnje zaupanja označena kot *kognitivni proces*i, izhaja **iz upnikovega *intelekta***, afektivna komponenta pa izhaja **iz upnikovih *čustev***. Ti dve komponenti vplivata predvsem na medosebno zaupanje, obenem pa tudi na dispozicijsko in institucionalno zaupanje, kar smo že pojasnili.

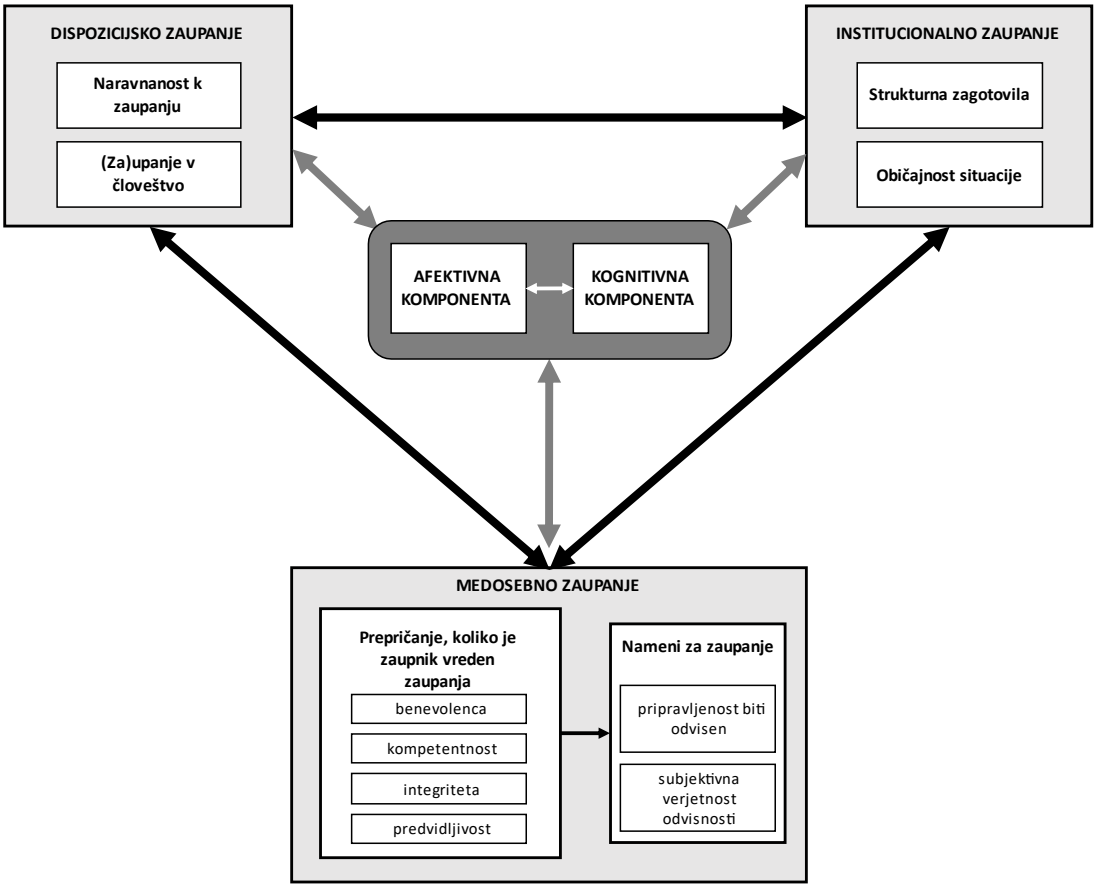
Temelj kognitivne komponente je ***kognicija***. Ta izraz med drugim označuje uporabo razuma, kategorizacijo, atribucijo in iskanje logičnih vzrokov (Varnum, Grossman, Kiatyama & Nisbett, 2010). Te aktivnosti so podobne tistim iz komponente *kognitivni procesi* na sliki 3.2. Zaupanje, ki izhaja iz kognitivne komponente, temelji na prepričanjih upnika o zanesljivosti (McAllister, 1995) in kompetentnosti upnika, torej prihaja »iz glave« (Chua et al., 2008), iz razuma. Vzpostavljeno je na podlagi znanja, ki ga posameznik pridobi z opazovanjem druge osebe in iz zaznanega ugleda druge osebe (Johnson & Grayson, 2005) oziroma z drugimi načini, ki jih v doktorski disertaciji imenujemo *proces pridobivanja znanja*. Znanje je torej temelj sestavine *kognitivna komponenta* in kognitivnega zaupanja, ki izhaja iz te komponente. S povečevanjem

kognitivnega zaupanja se povečuje tudi afektivno zaupanje (ibidem). Del kognitivne komponente so tudi upnikove izkušnje z zaupnikom (Swift & Hwang, 2013). Na podlagi navedenega lahko trdimo, da je **kognicija kot proces pridobivanja znanja pomembna za proces presoje zaupanja**. Od nje je namreč odvisno, kako bo posameznik zbral podatke in jih interpretiral ter oblikoval v znanje in prepričanje. Na drugi strani pa »predhodno znanje neposredno vpliva na kognitivne procese, ki so pomembni za učenje in ohranjanje novih informacij v sistemu spomina.« (Brod, Werkle-Bergner & Shing, 2013, str. 1) S tem ugotavljamo, da ima tudi **znanje pomembno vlogo v procesu presoje**, saj je **potrebno za izvedbo kognitivnih procesov**, ti pa **znanje dopolnjujejo z novimi podatki in informacijami**.

V povezavi s tretjimi osebami je potrebno poudariti vlogo znanja v odvisnosti upnikov (brez znanja) od tretjih oseb (z znanjem). Kadar govorimo o strokovnjakih, ki nastopajo kot tretje osebe, imajo laiki v primerjavi s strokovnjaki to pomanjkljivost, da nimajo t.i. baze znanja (Frowe, 2005), ki bi jim omogočila ustrezno procesiranje oziroma presojo zaupanja, zato so v določenih primerih lahko odvisni od strokovnjakov in od njihovega znanja. Zaradi tega obstaja tveganje, da upnik postane »žrtev« lažnih podatkov, zavajanja in vsiljevanja subjektivnega mnenja drugih, upnikova »objektivna« (tj. čim manj subjektivna) presoja pa je s tem otežena ali skoraj v celoti onemogočena.

Če na tem mestu povzamemo spoznanja iz zadnjih nekaj odstavkov, je podrobna analiza literature s področja zaupanja, ki smo jo do sedaj že večkrat navedli, pokazala, da so dispozicijsko, institucionalno in medosebno zaupanje soodvisne vrste zaupanja, da sta soodvisni kognitivna in afektivna komponenta ter da obstaja tudi soodvisnost med komponentama in vsemi tremi vrstami zaupanja. Takšen dialektični sistem (slika 5.4) predstavlja pomemben del procesa presoje zaupanja.

Slika 5.4: Soodvisnost treh vrst zaupanja in dveh komponent

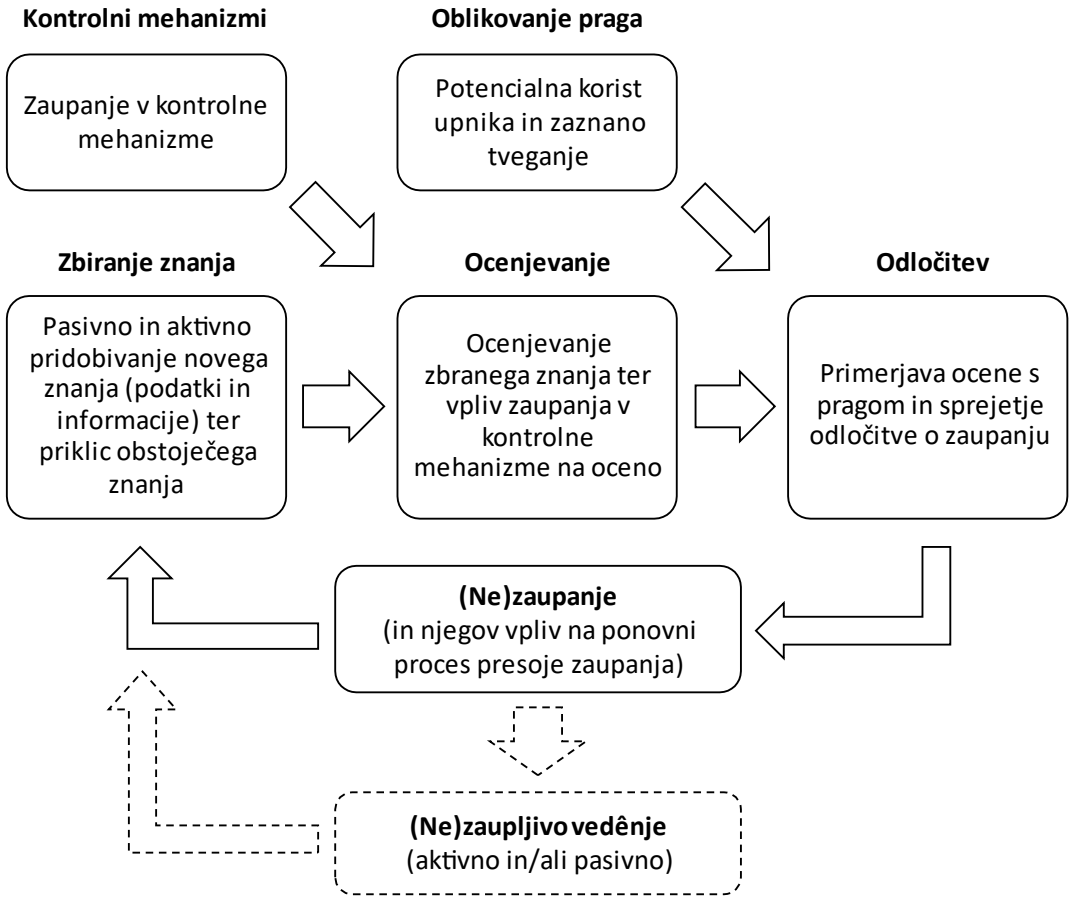


Vir: Osebni vir

Ko smo ta dialektični sistem želeli umestiti v koncept OOOD zanke (Mirzaie et al., 2012) kot izhodišče za modeliranje podsistema *Državljan*, smo ugotovili, da obstoječa struktura OOOD zanke tega ne omogoča. Prva in druga faza OOOD zanke predstavljata pridobivanje znanja od sebe in drugih, nato pa prehaja neposredno na odločitev, kar pomeni, da ne vsebuje koraka za ocenjevanje/presojo zbranih podatkov in informacij (tj. pridobljenega znanja). Podrobnejša analiza OOOD zanke je tudi pokazala, da je zaupanje po mnenju avtorjev Mirzaie et al. (2012) posledica dejanj, ki temeljijo na odločitvi posameznika, ali zaupati ali ne. Mi trdimo, da je kakršnokoli dejanje, ki izhaja iz zaupanja, (ne)zaupljivo vedênje, pri čemer ni nujno, da do takšnega vedênja sploh pride. Zato smo morali strukturo OOOD zanke ustrezno prilagoditi. OOOD zanki smo dodali dve sestavini: *Kontrolni mehanizmi* in *Oblikovanje praga*. Prva izhaja iz generičnega modela zaupanja avtorjev Tan & Thoen (2001), ki določa dve determinanti zaupanja in dve determinanti praga (glej sliko 3.13).

S postopkom modeliranja smo izoblikovali **model podsistema *Državljan*** (slika 5.5). Determinanta *Kontrolni mehanizmi* je dodana, determinanta zaupanja *Zaupanje v drugo osebo* pa je na sliki 5.5 izražena v sestavinah *Zbiranje znanja* (objektivna komponenta) in *Ocenjevanje* (subjektivna komponenta). Determinanti praga *Potencialna korist* in *Tveganje* sta združeni v enotno sestavino *Oblikovanje praga*.

Slika 5.5: Podsistem *Državljan*



Vir: Osebni vir

Ker je manjkal proces ocenjevanja zbranega znanja, smo ga dodali kot drugi korak. Sestavino OOOD zanke *Dejanje* smo preimenovali v *(Ne)zaupljivo vedênje* in ga glede na zaporedje prestavili za *(Ne)zaupanje*, saj menimo, da je takšno vedênje ***posledica*** oziroma ***odraz*** **(ne)zaupanja**. Ker (ne)zaupljivo vedênje lahko vpliva na (obstoječe) zaupanje, smo to sestavino obdržali in jo kot možno sestavino umestili na konec procesa – ob tem moramo pojasniti, da se **vpliv takšnega vedênja kaže v novi stopnji zaupanja**

in ne v obstoječi (glej povratno zanko na sliki 5.5). Zakaj smo *(Ne)zaupljivo vedênje* opredelili kot **možno sestavino** in ne kot vedno prisotno, utemeljujemo s tem, da v nekaterih primerih ne pride do izražanja (ne)zaupanja oziroma (ne)zaupljivega vedênja, zato se proces konča pri (ne)zaupanju kot prepričanju. Sestavino *Ocenjevanje* sestavljata medsebojni vpliv soodvisnosti treh vrst zaupanja in dveh komponent ter zaupanja v kontrolne mehanizme, saj gre za predvsem subjektivno oceno zbranega znanja.

Na podlagi analizirane literature, medijskih objav in intervjujev smo spoznali, da so dejavniki, ki jih državljan presoja v zvezi z matično obveščevalno-varnostno službo, **benevolenca**, **integriteta**, **kompetentnost** in **predvidljivost**, dodatno pa tudi **situacijska normalnost** in **strukturna zagotovila**. Ocenjevanje teh zaupnikovih lastnosti in dejavnikov okolja/institucije (situacijska normalnost in strukturna zagotovila) se odvija v fazi *Ocenjevanje*, ki jo predstavlja dialektični sistem na sliki 5.5. Čeprav se benevolenco, integriteto, kompetentnost in predvidljivost presoja le pri medosebnem zaupanju (zaupanje v osebe, npr. uslužbence matične obveščevalno-varnostne službe), strukturna zagotovila in običajnost situacije pa pri institucionalnem zaupanju, ugotavljamo, da ko državljan obravnava organizacije, jih vseeno presoja, čeprav ne gre za osebe. Zaupanja v službo ne moremo opredeliti kot medosebno zaupanje, saj je zaupanje v neosebne objekte opredeljeno kot institucionalno zaupanje, zato z izbranega teoretičnega vidika težko govorimo o presoji, koliko je matična obveščevalno-varnostna služba *vredna zaupanja* (kot osebnostna lastnost v kontekstu medosebnega zaupanja). Vtis, da je zaupanje v institucijo enako kot zaupanje v posameznika, je mogoče zaznati, ker upnik službi pripisuje enake lastnosti, kot jih imajo njeni uslužbenci. Enako velja tudi za druge državne organe (npr. policija, vojska, sodišča) ter družbene skupine in institucije (npr. nevladne organizacije, verske skupnosti, podjetja, politične stranke). Kljub temu so pri obravnavi obveščevalno-varnostnih služb omejitve, saj zaradi tajnosti ni možnosti obravnave posameznih uslužbencev, državljan nima dovolj znanja oziroma podatkov in informacij, prihaja pa tudi do posploševanja dejstev/mnenj (zaradi premalo znanja, vpliva medijev, hevristike idr.). Če smo prej dejali, da se službam pripisuje človeške lastnosti in da se zato zaupanje prenaša s posameznika na organizacijo oziroma z uslužbenca na matično obveščevalno-varnostno službo, pa sedaj dodajamo, da se posameznim uslužbencem navadno pripisuje tiste (posplošene) lastnosti, ki naj bi veljale

za institucijo kot enotni korpus za izvajanje obveščevalno-varnostne dejavnosti, ker njihove dejanske lastnosti (zaradi tajnosti) niso znane.

V zvezi z zaupanjem v obveščevalno-varnostno službo je eden od intervjuvancev dejal, da na tovrstno zaupanje vpliva tudi oseba, ki vodi matično obveščevalno-varnostno službo. Vodja službe javno zastopa in predstavlja službo, zato navzven deluje tudi kot njen »strelovod«. Nekdanji direktor OVS je dejal, da je (vsak) direktor obveščevalno-varnostne službe zato tudi bolj izpostavljen kritikam. Nekdanji direktor Sove, Sebastjan Selan, je pojasnil, da »[n]enapisano pravilo pravi, da če ni potrebe, naj se predstojniki obveščevalnih agencij v javnosti ne bi pojavljali. A tako se, žal, o obveščevalnih službah v javnosti govori le ob težavah.« (Mekina, 2011) Zaradi javne izpostavljenosti vodje obveščevalno-varnostne službe je o njem mogoče pridobiti več podatkov in informacij, s tem pa tudi lažje presojati zaupanje vanj. Zaradi vpliva medosebnega in institucionalnega zaupanja pa je posredno lažje presojati tudi zaupanje v matično obveščevalno-varnostno službo. Kadar posameznik presoja institucionalno zaupanje, teži k prevelikem posploševanju izrazitih in zelo izstopajočih dogodkov, v katere so vpletene organizacije in njihove vodje (Kramer, 1999). Tudi Kavčič (2015, str. 31) ugotavlja, da se »[s]plošno zaupanje v organizacije […] razvije pod vplivom percepcije vedênja in delovanja vodstva ter specifičnih srečanj (''trkov'') z organizacijo, z njenimi zaposlenimi, tehnologijo in komunikacijami.« V primeru upada medosebnega zaupanja bo zaradi soodvisnosti upadlo tudi institucionalno zaupanje – in obratno, čeprav nič od tega ni nujno. Kljub temu ne smemo pozabiti, da institucionalno zaupanje z ustvarjanjem ugodnih okoliščin pripomore, da posamezniki lažje zaupajo drugim (McKnight & Chervany, 2001) znotraj takšnih struktur, ker so del tega istega okolja (Rusu & Baboş, 2015) oziroma institucije.

Pojasnili smo že, da državljan (praviloma) ne sme/more poznati uslužbencev obveščevalno-varnostnih služb zaradi tajnosti njihove identitete, zato ne pridobiva podatkov in informacij o njihovih lastnostih neposredno od njih, temveč iz drugih virov, in zato **težje presoja zaupanje**. Ker je institucionalno zaupanje utemeljeno na informacijah, ki prihajajo od institucij (Rus, 2008) in od zaupanja vrednih posredovalcev (Toš, 2007), je pomembno, da upnik išče takšne tretje osebe, ki so verodostojne, zanesljive, vredne zaupanja. Tako je državljan odvisen od *preverjenih* (pri tem mislimo

tako zanesljivih kot tudi formalno varnostno preverjenih) tretjih oseb oziroma posrednikov, ki mu posredujejo podatke in informacije o dogajanju »onkraj zidu tajnosti«, s katerimi se sme seznaniti. Pri iskanju podatkov in informacij se zato najpogosteje naslanja npr. na medije, politiko in ostale izvajalce nadzora nad obveščevalno-varnostnimi službami.

Zaradi različne kognicije, osebnosti, dispozicijskega, institucionalnega in medosebnega zaupanja, čustev, zaznavanja tveganja, različnih izkušenj, različnega zaupanja v kontrolne mehanizme ter drugih s tem povezanih dejavnikov smo si posamezniki med seboj različni. To je tudi razlog, zakaj **ni mogoče pričakovati (niti zagotoviti), da bodo vsi državljani povsem enako presojali zaupanje**. Lahko so izpostavljeni enakim podatkom in informacijam, vendar jih bo vsak interpretiral, razumel, prioritetiziral in ocenil na drugačen način (Frowe, 2005). Poleg tega imajo državljani različno visoke prage zaupanja, drugače zaznavajo tveganja, drugače zaupajo kontrolnim mehanizmom oziroma nadzoru ipd. Tveganja namreč pomembno vplivajo na **občutek varnosti** posameznega državljana. Občutek varnosti so kot pomemben dejavnik zaupanja državljanov v matične obveščevalno-varnostne službe prepoznali in izpostavili dr. Žirovnik, nekdanji uslužbenec Sove, eden od takrat aktualnih uslužbencev Sove ter nekdanji direktor OVS. V praksi se te razlike v dojemanju tveganj in različno zastavljenih pragih zaupanja najbolj pokažejo ob dogodkih, ki so povezani z matičnimi obveščevalno-varnostnimi službami. Državljani imajo možnost posredno ali neposredno zaznati le posledice aktivnosti ali »neaktivnosti« (ta izraz ni najbolj ustrezen, pomeni pa tisto, česar služba ni naredila, bodisi zaradi malomarnosti, opustitve dolžnega ravnanja ali iz drugega razloga), ki so vsem razkrite z nekim dogodkom (npr. teroristični napadi, subverzivno delovanje, diverzije, državni udari) ali pa zanje izvejo od oseb ali organov, ki so v stiku z matičnimi obveščevalno-varnostnimi službami (npr. poročanje predsednika vlade, direktorja službe, ministra ali druge osebe o preprečitvi posameznega dejanja, vlogi službe v določenih aktivnostih ipd.). Polpreteklo zgodovino človeštva je zaznamovalo več dogodkov, zaradi katerih so matične obveščevalno-varnostne službe izgubile ugled in (s tem) zaupanje državljanov, najpogostejši razlog za to pa je bilo po našem prepričanju takšno razmišljanje državljanov: »To se je zgodilo, ker matične obveščevalno-varnostne službe niso (dobro) opravile svojega dela.« Naj navedemo le nekaj takšnih negativnih

dogodkov z negativnim vplivom na zaupanje: napad japonske vojske na Pearl Harbor v ZDA leta 1941, teroristični napadi leta 1972 v Münchnu (Olimpijske igre), leta 1993 in 2001 v ZDA (napad na Svetovni trgovinski center), leta 2002 in 2004 v Moskvi (gledališče, podzemna železnica), leta 2005 v Londonu (podzemna železnica), v zadnjih letih pa napadi v Združenem kraljestvu, Franciji, Belgiji, Nemčiji, Bosni in Hercegovini, na Danskem ter tudi drugod po svetu. Velika večina terorističnih napadov je bila izvedena na Bližnjem vzhodu, vendar mediji o tem ne poročajo. Poleg terorističnih napadov lahko poleg uvrstimo tudi razkritja »žvižgačev« o delovanju obveščevalno-varnostnih služb (npr. Manning, Snowden, pri tem ima pomembno vlogo tudi organizacija WikiLeaks), priključitev Krima Rusiji leta 2014, zastrupitev nekdanjih ruskih operativcev oziroma dvojnih agentov Aleksandra Litvinenka leta 2006 in Sergeja Skripala leta 2018, razkritje afer in spodrsljajev služb ipd. V navedenih in drugih tovrstnih primerih gre za t.i. **logiko oportunitetnega vpliva** (Mulej, 2018, osebni vir), po kateri imajo nenadni oziroma nepričakovani dogodki velik vpliv na razmišljanje, percepcijo ter počutje (in s tem na zaupanje) državljanov. Opažamo, da imajo negativni dogodki navadno večjo moč od pozitivnih, čemur Mulej (2018, osebni vir) pravi **moč negativne informacije**. En sam negativen dogodek lahko povzroči popolno izgubo zaupanja, nasprotno pa več pozitivnih dogodkov težje povrne izgubljeno zaupanje oziroma ga počasneje vzpostavi. Dokler se določen dogodek, ki je povezan z matičnimi obveščevalno-varnostnimi službami, ne zgodi, državljani o službah navadno ne razmišljajo, ker (v medijih) o njih ničesar ne zaznajo. Ko pa se dogodek zgodi, pa ima ta dogodek vpliv na razmišljanje državljanov o povezavi med službo in dogodkom. Tega **vpliva logike oportunitetnega vpliva in moči negativne informacije žal nismo mogli dokazati**, saj v zvezi s tem – po našem védenju in raziskovanju – ni literature. Kljub temu trdimo, da je to mogoče zaznati in v določeni meri tudi potrditi z analizo medijskih prispevkov in s primerjavo dobljenih rezultatov z anketo o zaupanju državljanov v te službe, nenazadnje pa tudi z razmišljanjem o lastnem odzivu ob naslednjem dogodku, ki bo povezan z (matičnimi) obveščevalno-varnostnimi službami.

5.1.3 Matična obveščevalno-varnostna služba in nacionalni obveščevalno-varnostni sistem

Zaradi vloge institucionalnega zaupanja smo namesto samostojnega podsistema *Matična obveščevalno-varnostna služba*, uporabljenega v osnovnem ogrodju splošnega modela zaupanja, ta podsistem uporabili skupaj s sestavino/(pod)sistemom *Nacionalni obveščevalno-varnostni sistem*. Ker na institucionalno zaupanje vplivajo tudi dejavniki, ki izhajajo iz drugih entitet nacionalnega obveščevalno-varnostnega sistema, te pa so med seboj povezane, smo jih v model vključili kot en sistem. V našem primeru institucionalno zaupanje državljana ne odraža le zaupanje v nacionalni obveščevalno-varnostni sistem (ta ustvarja in oblikuje strukturna zagotovila in (pogoje za presojo) običajnost(i) situacije), temveč tudi v matično obveščevalno-varnostno službo kot njegov podsistem. Posamezna služba je neločljivi del nacionalnega obveščevalno-varnostnega sistema, zato bi bilo obravnavanje službe neodvisno od preostalih sestavin nacionalnega obveščevalno-varnostnega sistema po našem prepričanju v neskladju z zakonom zadostne in potrebne celovitosti, s tem pa tudi z DTS. Kljub temu smo se morali pri obravnavi celotnega nacionalnega obveščevalno-varnostnega sistema osredotočiti na matično obveščevalno-varnostno službo, saj se nanjo navezuje upnikovo zaupanje, ter hkrati upoštevati tudi njene povezave z drugimi sestavinami nacionalnega obveščevalno-varnostnega sistema.

Oblikovanje sodobne oblike podsistema *Nacionalni obveščevalno-varnostni sistem* smo pričeli z iskanjem obstoječe strukture **splošnega** tovrstnega sistema v dostopni literaturi. Takšne literature, ki bi predstavljala ali poskušala strukturirati splošni obveščevalno-varnostni sistem, nismo našli. Ravno tako nismo našli literature, v kateri bi avtorji metodološko in sistematično pristopili k oblikovanju splošnega nacionalnega obveščevalno-varnostnega sistema. Pregled kateregakoli obveščevalno-varnostnega sistema na svetu in njegova primerjava z drugimi takšnimi sistemi namreč kaže, da se njihove strukture razlikujejo, kar je zagotovo posledica pravice do samoodločbe, ki jo priznava Mednarodni pakt o državljanskih in političnih pravicah (Organizacija združenih narodov, 1976). Skladno s tem si ljudje prosto oblikujejo svoj politični sistem ter

zasledujejo cilje, ki jih sami oziroma v njihovem imenu določi oblast. Enako si ljudje preko oblasti sami določijo in uredijo sistem, ki bo skrbel za njihovo varnost.

To je po našem prepričanju tudi razlog, zakaj smo našli le literaturo, v kateri avtorji predstavljajo obstoječo ali predlagajo novo strukturo obveščevalno-varnostnega sistema določene države (glej npr. Črnčec, 2009; Britovšek & Čretnik, 2016; Richelson, 2016) in ne neko splošno obliko tovrstnega sistema. Zaradi različne organiziranosti služb, različnega števila služb, različne delitve na vojaške, obrambne in civilne službe ter različne umeščenosti obveščevalno-varnostnih služb v državni sistem je **v praksi težko izoblikovati splošno obliko nacionalnega obveščevalno-varnostnega sistema**, ki bi jo lahko označili za splošni tovrstni sistem na globalni ravni. Izkazalo se je, da bolj kot je struktura nacionalnega obveščevalno-varnostnega sistema razvejana in več kot ima entitet, bolj je sistem kompleksen.

Ker so obveščevalno-varnostne službe po svetu različno organizirane in različno delujejo, njihovega delovanja pa zaradi tajnosti ne moremo poznati podrobno, smo posamezno službo obravnavali kot »črno škatlo« (ang. *black box*), katere notranjost ne poznamo, vemo pa, kako se izhodi iz tega sistema spreminjajo v odnosu do njegovih vhodov (Mulej et al., 2000). Čeprav struktura in organizacija službe pomembno vplivata na delovanje službe, je delovanje službe kot sistema tisto, kar državljan preučuje. Kot smo že pojasnili, naj bi državljan pri matični obveščevalno-varnostni službi presojal njeno benevolenco, integriteto, kompetentnost in predvidljivost. Obveščevalno-varnostna služba naj navzven ne bi bila predvidljiva, da se s tem prepreči odkritje njenega načina delovanja (*modus operandi*), vendar predvidljivost v kontekstu zaupanja izraža drugačno predvidljivost – državljan lahko predvidi, ali bo služba dosegla jasno znane in predvidene rezultate ob predvidenem času in na predvideni (zakoniti) način. Ti rezultati in časovni roki državljanom zaradi tajnosti niso znani, vendar govorimo o splošnih rezultatih, ki so lahko posredno zaznani (npr. odsotnost ali preprečitev terorističnih napadov in drugih posebno hudih oblik kriminala, država uspešno ščiti in uveljavlja lastne interese, krepita se moč in prepoznavnost države na zunanjepolitičnem, varnostnem, gospodarskem ali drugem področju). Rezultate dela služb lahko razkrijejo le pristojne osebe, če ocenijo, da bo to koristilo državi, službi ali drugemu državnemu/javnemu subjektu ali državnemu/javnemu

interesu. Kljub javno razkritim rezultatom dela obveščevalno-varnostne službe, ki se kažejo kot posledica poročanja državnih organov ali oblasti preko medijev ali kot zaznavanje določenega dogodka, je težko slediti njenim aktivnostim in oceniti, koliko je služba predvidljiva. Benevolence obveščevalno-varnostne službe ne moremo obravnavati enako kot benevolence »običajnega« zaupnika. Čeprav obveščevalno-varnostni službi z zakonodajo določeno poslanstvo preprečuje, da bi »ji bilo vseeno za državljane«, se poraja vprašanje, koliko njene uslužbence dejansko skrbi za državljane ter kakšno motivacijo imajo za delovanje v skladu z interesi državljanov, ki se posredno odražajo kot nacionalni interesi. Aktualni uslužbenec Sove je v intervjuju navedel, da predvsem tajnost načenja motivacijo zaposlenih, kar dodatno vpliva na njihovo benevolenco; tajnost jim onemogoča, da bi o svojem delu govorili z drugimi in tako izpolnili določene potrebe, npr. potrebo po ugledu, razumevanju in samoaktualizaciji. Enako bi lahko rekli tudi za integriteto in kompetentnost. Nacionalne obveščevalno-varnostne službe in njihovi uslužbenci naj bi delovali kompetentno (pod to uvrščamo sposobnost, strokovnost in specialnost, glej Hurley, 2012) ter v skladu z integriteto (pod to uvrščamo zanesljivost, konsistentnost in kredibilnost, glej Hurley, 2012). Kot je dejal William H. Webster, edini Američan, ki je bil direktor CIA in tudi direktor FBI, se morajo obveščevalno-varnostne službe zanašati na integriteto oziroma na tisto, kar zaznavajo kot integriteto svojih uslužbencev, zato morajo biti uslužbenci vredni zaupanja, ki jim ga izkazuje služba (Sexton, 2018). Vse to se odraža v delu in rezultatih dela obveščevalno-varnostnih služb in vpliva tudi na **ugled** služb, ki sicer ni sinonim za zaupanje; če nekoga dojemamo kot vrednega zaupanja, še ne pomeni, da ima tudi dober ugled (Kovač & Trček, 2007; Lucas, 2005). »Povezavo med zaupanjem in ugledom je težko točno definirati, predvsem ker zaupanje temelji na osebnem in subjektivnem odnosu do ciljne entitete. […] [T]orej mora obstajati zasebno znanje med izvorno in ciljno entiteto (je posledica osebne izkušnje), ki prevladuje nad ugledom. Če ne obstaja osebna izkušnja, se zaupanje oblikuje na podlagi ugleda oz. priporočil drugih.« (Kovač & Trček, 2007, str. 8) S tem se ponovno vračamo k vlogi tretjih oseb/strani v procesu presoje zaupanja.

Ugled neki osebi (ali organizaciji, op. G. H.) določi njeno družbeno omrežje in je odvisen od konteksta, zato ima lahko oseba (ali organizacija, op. G. H.) več različnih ugledov. Na ugled vplivajo tudi interakcije z drugimi in njen družbeni kapital. Kdor ima več ugleda,

ima tudi omogočen (ali pa vsaj lažji, op. G. H.) dostop do več različnih materialnih in socialnih virov, kar omogoča krepitev družbenega kapitala. Kdor pa ima več družbenega kapitala, bo tudi imel več ugleda. V tem se kaže soodvisnost med ugledom in družbenim kapitalom. Obstaja tudi tesna povezava med ugledom in vedênjem. Če vedênje zaupnika ni konsistentno z njegovim ugledom, bo to opazil upnik, ki bo spremenil svoja pričakovanja glede zaupnika, kar bo posledično vplivalo na zaupanje, to pa na odgovornost (oziroma upnikovo zaznavanje zaupnikove odgovornosti, op. G. H.) (Burke et al., 2007).

Born & Mesevage (2012) izpostavljata tudi **transparentnost**. Ta lahko po njunem mnenju odpravi mite o službah in vzpodbudi javno razpravo o njihovem delu, kar je še posebej potrebno za države, kjer je zaupanje v matične obveščevalno-varnostne službe nizko ali pa so službe zlorabile finančna sredstva (ibidem). Področje, kjer bi se po njunem (ibidem) mnenju moralo uveljaviti (večjo) transparentnost, je finančno področje služb. Pri tem se zastavlja vprašanje, kako je kljub tajnosti mogoče zagotoviti dovolj odprto in transparentno delovanje služb. Tudi Podbregar & Hibler (2006) se glede javnega delovanja in ohranjanja tajnosti sprašujeta podobno. Več transparentnosti pri delovanju obveščevalno-varnostnih služb naj bi pomagalo pri zmanjševanju sumničavosti in s tem prispevalo k povečanju zaupanja s strani državljanov. To bi sicer pozitivno vplivalo tudi na izboljšanje sodelovanja med službami in državljani, saj bi bili slednji bolj pripravljeni dati službam podatke, ki jih potrebujejo (Born & Mesevage, 2012), vendar bi na drugi strani to lahko obveščevalno-varnostne službe preveč odprlo in jih tako naredilo ranljive. Različni avtorji na podlagi raziskav in prakse (glej npr. Muna, 2008; Born & Mesevage, 2012; Matei, 2014) sicer menijo, da sodelovanje med službami in različnimi javnostmi (strokovna, medijska, laična) v obliki skupnih sestankov, konferenc, izmenjav mnenj, partnerstva s civilno sfero pri reševanju problemov prebivalstva in skupnih učnih programov prinaša pozitivne rezultate (npr. izboljša zaupanje, odpravi mite, ugibanja in govorice, (posredno) poveča proračun služb, okrepi sodelovanje med državljani, službami in politiko), vendar splošno sprejetega razmerja med odprtostjo, transparentnostjo in tajnostjo teh služb ni. Direktor ameriške obveščevalne skupnosti je februarja 2018 izdal direktivo 107, katere namen je vzpostavitev politike za zaščito človekovih pravic in transparentnost, ki bo izboljšala razumevanje in **zaupanje** v

obveščevalno skupnost, njene naloge, strukture in dejavnosti (Intelligence Community Directive 107, 2018). Ta direktiva prepoznava transparentnost kot enega od temeljev zaupanja javnosti oziroma državljanov (Coats, 2018), vendar Aftergood (2018) ugotavlja, da zgolj umikanje oznake tajnosti z dokumentov ali njihovih posameznih delov (to lahko razumemo kot omogočanje vpogleda v delo oziroma rezultate dela obveščevalno-varnostnih služb in s tem večjo transparentnost, op. G. H.) ni pripomoglo k večjemu zaupanju, kar se je po njegovem mnenju izkazalo v času takratnega predsednika ZDA, Baracka Obame.

Transparentnost bi zagotovo pripomogla k **legitimnosti** matične obveščevalno-varnostne službe, saj se legitimnost navezuje na stopnjo zaupanja državljanov v te službe (Organizacija za gospodarsko sodelovanje in razvoj, 2007). Legitimnost lahko službe pridobijo in povečajo s simbolnimi dejanji (npr. opravičila, komemoracije), s katerimi lahko utrdijo zavezanost k demokratičnim vrednotam, in z delovanjem, ki odseva družbo, ki ji služba služi (ibidem). Služba pridobi na legitimnosti oziroma na transparentnosti tudi takrat, ko npr. objavi podatke oziroma dosjeje, ki nakazujejo na sporno delovanje služb, saj bo to pri ljudeh vzbudilo občutek, da si služba želi postati bolj odprta (Matei, 2014) in da želi popraviti svoje napake ali sporne prakse. Z drugimi besedami, več odprtosti *naj bi* preneslo tudi več zaupanja. Nekdanji direktor OVS, s katerim smo opravili intervju, pravi, da je bolj kot transparentnost pomemben notranji nadzor, ki bi zagotovil pravilnost delovanja ob hkratnem preprečevanju nepotrebnih vpogledov v delovanje obveščevalno-varnostnih služb. Sam meni, da je izredno pomemben problem vprašanje nadzora nad finančnim poslovanjem in sredstvi služb, ki ostaja po njegovem mnenju enak skozi vso zgodovino.

Kot smo že pojasnili, ima pomembno vlogo tudi vodja matične obveščevalno-varnostne službe, predvsem v kontekstu medosebnega zaupanja. Bolj ko bo vodja navzven deloval po predpisih in učinkovito, bolj mu bodo državljani zaupali, s tem pa bodo zaupali tudi službi. Eden od aktualnih uslužbencev Sove je v intervjuju izpostavil, da na zaupanje vpliva tudi način imenovanja vodje službe in njegove ekipe, kar po našem mnenju nakazuje, da imajo takšne zadeve vpliv tudi znotraj organizacije. Pomemben je tudi način vodenja službe, ki se posredno kaže v rezultatih njenega dela, organizacijski klimi, odnosi

med uslužbenci, nenazadnje pa tudi v uresničevanju nacionalnih interesov in zagotavljanju nacionalne varnosti. Vodenje, ki temelji na odsotnosti ustreznega strokovnega znanja, menedžerskih kompetenc in jasnega načrta, negativno vpliva na delovanje službe, zato je v takšnih primerih mogoče pričakovati, da bodo rezultati dela slabši. Posledično se bo na posreden način (preko politike, nadzora, medijev in strokovne javnosti) zmanjšalo tudi zadovoljstvo državljanov ter s tem njihovo zaupanje.

Če povzamemo: na zaupanje ima v okviru nacionalnega obveščevalno-varnostnega sistema vpliv več dejavnikov, ki izhajajo iz njega samega, pri tem pa predvsem tisti, ki izhajajo iz matične obveščevalno-varnostne službe kot njegovega podsistema. Nekateri pomembnejši vplivi, ki smo jih prepoznali, so strukturna zagotovila in normalnost situacije, tajnost, transparentnost, odprtost, benevolenca službe/zaposlenih, integriteta službe/zaposlenih, kompetentnost službe/zaposlenih, predvidljivost službe/zaposlenih, pojav nepravilnosti in zlorab v službah ali v povezavi s službami, učinkovitost sistema, komunikacija službe z okoljem in vodja službe (predvsem benevolenca, integriteta, kompetentnost in predvidljivost vodje kot dejavniki medosebnega zaupanja). Službe po našem prepričanju ne potrebujejo (niti ne smejo) biti odprte glede vsebine dela, lahko pa javnost seznanijo z osnovami obveščevalno-varnostne dejavnosti in nekaterimi splošnimi rezultati oziroma uspehi, če s tem ne bi ogrozile svojega delovanja, osebja, sredstev ali virov.

5.1.4 Politika

Za potrebe splošnega modela zaupanja državljanov v matične obveščevalno-varnostne službe in kasneje modela celovitega zaupanja smo moral najprej opredelili izraz *Politika*. V Slovarju slovenskega knjižnega jezika pod geslom *politika* najdemo več razlag (Politika, b. d.):

- »urejanje družbenih razmer, odločanje o njih s pomočjo države in njenih organov […]«;
- »dejavnost političnih strank in njihov medsebojni odnos v boju za oblast […]«;
- »urejanje razmer in odločanje o njih na določenem družbenem področju […]«;
- »določbe, načela za tako urejanje in odločanje […].«

Izraz *politika* ima v doktorski disertaciji nekoliko bolj specifičen pomen. Zajema vse politične institucije in osebe **izvršilne in zakonodajne veje oblasti, ki določajo, urejajo, upravljajo, usmerjajo in koordinirajo (tudi) nacionalni obveščevalno-varnostni sistem in njegove podsisteme**. Podsistem *Politika* se ukvarja (tudi) s politiko obveščevalno-varnostne dejavnosti oziroma nacionalnega obveščevalno-varnostnega sistema in njegovimi prioritetami ter hkrati skrbi za izvajanje tovrstne politike. Določa nacionalne interese, cilje in prioritete nacionalne varnosti, ki spadajo pod nacionalne interese, ter jih posredno ali neposredno uresničuje in ščiti. Za podsistem *Politika* ne moremo določiti splošnih subjektov, saj je struktura tega podsistema odvisna od strukture političnega sistema obravnavane države. Iz enakega razloga nismo podsistema poimenovali *oblast*, *vlada* ali *parlament*. *Oblast* ima v določenem obsegu npr. tudi angleška kraljica, ki pa nima pristojnosti na področju obveščevalno-varnostnega sistema (razen npr. pristojnost podpisovanja zakonov s tega področja). *Vlada* je drugače strukturirana v parlamentarnih, predsedniških in pa polpredsedniških sistemih, v nekaterih državah (npr. v državah z absolutno monarhijo, kot so Kraljevina Saudova Arabija, Vatikan, Katar, Združeni arabski emirati) pa nimajo *parlamenta* v smislu, kot ga pojmujemo na Zahodu, temveč je lahko namesto tega zakonodajni subjekt v drugačni obliki ter z drugačnimi (tudi omejenimi) funkcijami. Zato ostajamo pri uporabi izraza *Politika*, ki združuje izvršilno in zakonodajno vejo oblasti v širšem pomenu (vključno s podrejenimi oziroma z njimi povezanimi organi) in ima neposreden vpliv na področju nacionalnega obveščevalno-varnostnega sistema.

Politika v splošnem smislu ima vpliv na vsa področja družbenega življenja. S predpisi in svojimi (podrejenimi) organi **oblikuje in ima pomemben vpliv na oblikovanje VKEN**. V okviru tega imamo v mislih predvsem **vladavino prava**, ki se odraža preko predpisov in mora zagotavljati upoštevanje ter zaščito človekovih pravic in svoboščin. Z vidika obravnavanja problema doktorske disertacije so predpisi pomembni predvsem zato, ker določajo in urejajo nacionalne interese (praviloma jih določa vladajoča politika), strukturo sistema nacionalne varnosti in nacionalnega obveščevalno-varnostnega (pod)sistema, delovanje služb, njihova pooblastila, pravice in svoboščine državljanov in drugih posameznikov, dopustnost posegov v te pravice in svoboščine, dostop do

informacij javnega značaja itd. Zakon kot ena izmed oblik predpisov je torej dobra osnova za vzpostavitev zaupanja državljanov v službe (Anžič & Golobinek, 2003), saj določa (Geneva Centre for the Democratic Control of Armed Forces, 2011, str. 5):

- vloge in naloge različnih varnostnih organizacij;
- določa njihove pristojnosti in omejuje njihova pooblastila;
- določa vlogo in pooblastila izvajalcev nadzora;
- zagotavlja osnovo za odgovornost s tem, ko določa jasno mejo med zakonitim in nezakonitim vedênjem (oziroma delovanjem služb, op. G. H.);
- izboljšuje javno zaupanje in krepi legitimnost vlade ter njenih varnostnih (oziroma obveščevalno-varnostnih, op. G. H.) služb.

To daje politiki **poseben**, zagotovo pa tudi **najmočnejši** položaj med vsemi sestavinami splošnega modela zaupanja državljanov v matične obveščevalno-varnostne službe. Ima posreden in neposreden vpliv na vse sestavine splošnega modela-sistema. V povezavi z zaupanjem izpostavljamo predvsem dva vidika, ki se med seboj tesno prepletata: 1) politika kot dejavnik vpliva na nacionalni obveščevalno-varnostni sistem in 2) politika kot upravljalec države (zaupnik) v očeh državljanov (upniki). Obravnava prvega vidika je s pomočjo analize literature (glej prejšnja poglavja) in opravljenih intervjujev pokazala, da politika posredno in neposredno vpliva na delo nacionalnega obveščevalno-varnostnega sistema in njegovih subjektov. Ta vpliv se kaže v določanju prioritet, smernic in ciljev nacionalnega obveščevalno-varnostnega sistema in njegovih subjektov, določanju in sprejemanju predpisov in proračuna, določanju vodilnih kadrov, usmerjanju delovanja sistema in služb, izvajanju nadzora ipd. Skladno s tem lahko rečemo, da je politika posredno in neposredno odgovorna za rezultate dela matičnih obveščevalno-varnostnih služb. Od uspešnosti delovanja nacionalnega obveščevalno-varnostnega sistema in njegovih subjektov je – ob »podpori« medijskega poročanja – odvisna tudi zunanja podoba politike, kar nas pripelje do povezave med uspešnostjo, zunanjo podobo, pričakovanji in ustreznostjo entitete. Če izhajamo iz naše definicije zaupanja in ga apliciramo na področje zaupanja v politiko, državljani od politike pričakujejo, da je sposobna izpolniti njihova pričakovanja in da jih tudi dejansko izpolnjuje ter da je politika ustrezna z vidika ustreznosti entitete. Državljani pričakujejo, da bo politika zagotovila njihovo varnost, kar uresničuje oziroma zagotavlja tudi z nacionalnim obveščevalno-

varnostnim sistemom oziroma z obveščevalno-varnostnimi službami. V zvezi s pričakovanji se vrnimo na model institucionalne učinkovitosti (Newton & Norris, 2000). Ta prikazuje, da na zaupanje vpliva razmerje med pričakovanji državljanov in učinkovitostjo/rezultati politike, zaupanje v politiko pa je rezultat njene učinkovitosti. Zaupanje ustvarja družbeni kapital, ki posredno izboljšuje učinkovitost politike, kar lahko zaupanje povečuje. Kljub temu nekateri avtorji (npr. Van de Walle et al., 2008, str. 51) ugotavljajo, da npr. nezaupanje v vlado (v našem primeru v *Politiko*, op. G. H.) in javni sektor ne predstavlja toliko odziva na to, kar vlada počne, pač pa širši upad medosebnega zaupanja. Nekatere raziskave kažejo (npr. Rothstein, 2000 v Luoma-aho, 2008), da državljani manj zaupajo institucijam, ki imajo izvoljene predstavnike, kot pa institucijam, ki imajo predstavnike s »stalnim mandatom«. Po našem prepričanju to dokazuje, da sta **za zaupanje pomembna stalnost in dolgoročnost**, ki po našem mnenju nakazujeta na **predvidljivost** in **prepričanost v kompetentnost**. Gre za izjemno pomembna dejavnika na področju delovanja obveščevalno-varnostnih služb, kar ugotavljajo tudi nekateri intervjuvanci. Pogoste spremembe politike, ciljev, usmeritev in prioritet posameznih služb ter menjave njihovih (vodilnih) kadrov ne zagotavljajo dolgoročnega dela služb. Posledično lahko predpostavljamo, da to negativno vpliva tako na javno podobo služb kot tudi na njeno delo (npr. uspešnost, tajnost, strokovnost), pri politiki pa na njeno javno podobo o sposobnosti za izpolnjevanje pričakovanj, bolj kot to pa na javno podobo ustreznosti entitete. Vprašanje, ki bi si ga morala politika zastaviti, je, ali ima dovolj znanja, izkušenj in kompetenc, da posredno vodi službo, jo usmerja in upravlja.

Poleg tega naj bi imeli organi več zaupanja, kadar imajo veliko moči in dajejo videz, da delujejo pravično, manj zaupanja pa imajo takrat, kadar imajo veliko moči in dajejo videz, da delujejo nepravično. Zato ljudje menijo, da bi morali imeti vplivni voditelji pravico oblikovati politiko in spremeniti nepravična pravila. V primeru, da jim to ne uspe, pa bodo ljudje nanje gledali izrazito negativno (Robbins et al., 2009, str. 416).

Na začetku smo določili podtezo, da *na zaupanje državljanov v matične obveščevalno-varnostne službe pomembno vpliva politika.* Do sedaj smo ugotovili, da politika pomembno in bistveno vpliva na matične obveščevalno-varnostne službe, zato smo politiko določili kot dejavnik, ki vpliva na zaupanje državljanov v službe. Politika je

pomembna tudi zaradi odnosa med državljanom oziroma družbo in politiko oziroma državo. Pri tem smo prepoznali, da ima pomembno vlogo ravno splošno zaupanje državljanov v politiko. Newton & Norris (2000) ugotavljata, da družbeno zaupanje in zaupanje v institucije delujeta v večji meri na ravni družbe in ne toliko na ravni posameznika. Obratno ima tudi posameznikovo (ne)zaupanje velik vpliv na družbeno (ne)zaupanje.

Povsem razumljivo je, da si vsaka politika želi podpore in zaupanja ljudstva, zato bo storila marsikaj, da bi se podpora in zaupanje ljudstva povečala. Žal pa sta moč in oblast in želja po še več moči in oblasti v nekaterih primerih tako močni, da posamezni politiki ali politične stranke oziroma skupine posežejo tudi po moralno in etično vprašljivih ali celo delno zakonitih oziroma nezakonitih dejanjih, da bi si povečali zaupanje. In ker imajo nekateri politiki avtoriteto in skušnjavo, da avtoriteto zlorabijo, je vsak politični sistem že v izhodišču postal sistem nezaupanja (Salminen & Ikola-Norrbacka, 2010). Zato v praksi zasledimo primere, ko se za doseganje političnih interesov, ki izhajajo iz lastnih, strankarskih, koalicijskih ali drugih podobnih interesov, manipulira z javnostjo, s tem pa z javnim mnenjem, ki ga na politika v nekaterih uporabi tudi kot orodje za ustvarjanje sprememb. Pri tem se politika lahko posluži tudi uporabe državnih ali zasebnih medijev, ki so pod vplivom politikov ali političnega vpliva. Da ima politika **vpliv na množična stališča oziroma javno mnenje**, se kaže na ravni države in na ravni posameznika (Kaase et al., 1999), vendar je potrebno razumeti, da politika ne odraža prepričanj in vrednot posameznikov (Burke et al., 2007, str. 619), temveč družbe. Po drugi strani pa lahko z vplivanjem na javno mnenje doseže, da državljani podprejo odločitve politike, s katerimi se sicer ne bi strinjali.

5.1.5 Izvajalci nadzora obveščevalno-varnostnih služb

Kot *izvajalce nadzora* zato obravnavamo tiste institucije in osebe, ki 1) **izvajajo formalni nadzor** in imajo hkrati tudi **dovoljen, utemeljen in pooblaščen dostop do tajnih podatkov** ter 2) delujejo kot **tretja oseba** v komunikaciji **med državljani in službo**. Za takšno obravnavo smo se odločili, ker imajo formalne institucije zaradi omogočenega dostopa do služb in do tajnih podatkov vpogled v delovanje službe. Poleg tega pa je

njihova naloga, da redno in sistematično spremljajo delovanje služb z namenom seznanjanja javnosti o njihovi pravilnosti delovanja. Istočasno imajo za opravljanje tovrstne funkcije tudi dovoljenje za obravnavanje tajnih podatkov. Zato bi bilo po našem prepričanju **neustrezno, če bi kot nadzor v kontekstu zaupanja obravnavali tudi medije**, saj bi to pomenilo, da bi morali kot *tertius* obravnavati nekoga, ki o pravem delovanju matične obveščevalno-varnostne službe ne more vedeti veliko, ker nima dostopa do tajnih podatkov. Z vidika nadzora je vloga medijev vsekakor pomembna, z našim vidikom obravnavanja pa jim ne zmanjšujemo te pomembnosti, vendar opozarjamo na dejstvo, da je za potrebe presoje zaupanja v tem primeru potrebna tretja stran, ki ima **omogočen dostop do potrebnih in pravih podatkov ter informacij o zaupniku**, ti pa so navadno tajni. Kljub temu se dogaja, da mediji pridobijo tajne podatke preko »stranskih kanalov«, čeprav za to nimajo dovoljenja.

Organizacija združenih narodov v poročilu o promociji in zaščiti človekovih pravic in temeljnih svoboščin pri boju proti terorizmu iz leta 2010 ugotavlja, da nadzorne institucije spodbujajo in skrbijo za zaupanje državljanov v delo matičnih obveščevalno-varnostnih služb na način, da zagotavljajo izvajanje njihovih funkcij v skladu z vladavino prava in človekovih pravic (Scheinin, 2010, str. 9). Z vidika zaupanja je nadzor nad matičnimi obveščevalno-varnostnimi službami potreben, da se prepreči slepo zaupanje in posledice, ki jih slepo zaupanje prinaša. Nekomu namreč ne zaupamo le zato, ker nam pravi, da bo nekaj zagotovo storil, temveč zato, ker na podlagi podatkov in informacij poznamo njegove značilnosti, sposobnosti, zmogljivosti ter posledice, če tega ne bo mogel opraviti (Dasgupta, 1988). Okoliščine slepega zaupanja z določenega vidika ustvarja tudi **tajnost**, vendar tajnost ne sme biti razumljena kot negativen, temveč kot pozitiven dejavnik, saj **preprečuje negativne posledice**, ki bi jih bili lahko deležni vsi državljani – posredno ali neposredno. Potrebno jo je razumeti kot »jamstvo« države, da je nekaj (dejstvo, stvar, aktivnost) širši javnosti skrito, vendar dovoljeno, utemeljeno in legitimno, hkrati pa mora takšno ostati za in zaradi uresničevanja državnih in javnih interesov. Zaradi tega je običajnim državljanom in medijem onemogočeno podrobno izvajanje nadzora matičnih obveščevalno-varnostnih služb. Običajen državljan nima dostopa do podatkov in informacij, potrebnih za ustvarjanje znanja in za presojo zaupanja, zato lahko matičnim obveščevalno-varnostnim službam težje zaupa. Iz tega

izhaja, da tajnost **bistveno otežuje** vzpostavljanje, ohranjanje in povečevanje zaupanja, zato je povsem razumljivo, da se je v (strokovni) javnosti izoblikovalo stališče, ki ga je izrazil Davison (2004): polno zaupanje državljanov je mogoče doseči le s parlamentarnim nadzorom, predvsem na področju dodeljevanja in nadzora porabe javnih sredstev. Parlamentarni nadzor (kot del sistema demokratičnega nadzora) predstavlja tretjo osebo (*tertius*), ki ima dovoljenje za dostop do tajnih podatkov in namesto javnosti oziroma v njenem imenu poizveduje ter izvršuje nadzor. Posledično je javnosti dolžan poročati o svojih ugotovitvah na način in v obsegu, ki zadostujeta potrebam javnosti. Enako velja tudi za izvršilni in sodni nadzor ter nadzor drugih organov.

Komunikacija med državljanom in matično obveščevalno-varnostno službo poteka preko *tertiusa* oziroma je v večji meri nadomeščena s komunikacijo s *tertiusom*, torej z izvajalcem nadzora. Navadno je to organ, ki deluje javno (razen kadar obravnava tajne podatke in kadar mora delovati tajno), transparentno in o opravljenem nadzoru poroča javnosti. To je **razlog, zakaj notranjega nadzora v našem modelu nismo prepoznali in določili kot *tertius***, saj zaradi tajnosti ne sme delovati javno zato o svojem delu tudi ne more poročati javnosti, hkrati pa je del službe in ne more biti tretja, neodvisna stran. Predvsem pri parlamentarnem nadzoru je pomembno, da ta javnost sproti obvešča z javnim poročanjem in javnimi zaslišanji (Born & Mesevage, 2012). S tem zagotavlja transparentnost, ki povečuje zaupanje v službe in parlamentarni nadzor (ibidem). Namesto enosmerne komunikacije mora parlament državljanom omogočiti dvosmerno komunikacijo o varnostnih vprašanjih (Born, 2003). S transparentnim, učinkovitim in ustreznim nadzorom **se zagotavlja kakovost in verodostojnost nadzora**, s tem pa **izboljšuje oziroma povečuje prepričanje o ustreznosti izvajalca nadzora**. Vsaka vrsta nadzora zato **potrebuje zaupanje s strani državljanov**, da lahko učinkovito izvaja svoje naloge in poslanstvo.

Večji del podatkov in informacij, potrebnih za presojo zaupanja, naj bi državljan neposredno ali posredno (preko medijev) prejel od nadzora, določen del podatkov in informacij pa tudi iz drugih virov. »Pomembno je, da se informacije iz formalnih in neformalnih, znotraj organizacijskih kanalov in iz okolja skladajo.« (Kavčič, 2015, str. 27) Ob tem je potrebno izpostaviti vpliv drugih virov, saj osebe »praviloma bolj verjamejo

neformalnim […] kot formalnim.« (ibidem) Podatki in informacije, ki prihajajo od izvajalca nadzora, morajo biti bolj točni, zanesljivi in resnični, kar v povezavi z možnostjo, da bo državljan večjo težo dal podatkom in informacijam iz neformalnih virov, in tveganjem, da »[n]eskladnost informacij iz različnih kanalov […] poraja dvom in posledično nezaupanje,« predstavlja težavo z vidika zaupanja državljana v nadzorne mehanizme. **Skladnost** podatkov in informacij v odnosu do zaupanja je ključna iz dveh razlogov: **zaradi prenosa znanja** 1) **z izvajalcev nadzora na državljane** in 2) kasneje **z državljanov na druge osebe**. Zato pravimo, da imajo izvajalci nadzora (in mediji) tudi funkcijo *prenosnika znanja*. »Zaupanje znanju, ki prihaja iz vira, povečuje možnost prenosa znanja, tudi če ima vir drugačne namene.« (Lucas, 2005, str. 90) S prenosom znanja se spreminja znanje drugih, kar posledično **prispeva k preoblikovanju javnega mnenja**. »Zaupanje ustvarja pogoje za povečan prenos znanja in zagotavlja njegov prenos na prejemnika v ustrezni obliki. Prejemniki znanja, ki zaupajo ponudniku znanja, so bolj nagnjeni k temu, da bodo ponudnika bolj poslušali […].« (ibidem) Vendar previdnost ni odveč, saj lahko slepo zaupanje v nadzor vodi k naivnosti državljanov, nadzoru pa omogoča, da s partikularnimi, strankarskimi ali drugačnimi interesi manipulira z javnostjo (zavajanje, selektivno poročanje, preusmerjanje pozornosti ipd.). S tem vpliva na javno mnenje, kar lahko posredno in posledično vodi v določene spremembe služb.

Nadzor je koristen, ker naj bi zaznal ali preprečil oportunistično vedênje in (nenamerne) napake zaupnika, ne da bi vplival na zaupanje, z nadzorom pa se povečuje tudi (upnikova zaznava) predvidljivost(i) zaupnikovega vedênja (Tan & Thoen, 2001). S tega vidika je nadzor lahko uporabljen tudi kot orodje za utrjevanje zaupanja. To naj bi bilo še posebej koristno v državah, kjer javnost matične obveščevalno-varnostne službe zaradi preteklosti povezuje s kršitvami človekovih pravic (npr. državah nekdanjih komunističnih in diktatorskih režimov, op. G. H.), saj lahko utrjuje zaupanje, da se podobne nepravilnosti ne bodo več dogajale (Born & Mesevage, 2012, str. 18). Seveda pa zgolj obstoj nadzora in njegovo delo ne zadostujeta, da bi državljan »brezpogojno« zaupal matičnim obveščevalno-varnostnim službam. Ugotovili smo, da imajo nadzorniki oziroma izvajalci nadzora poleg vloge ustvarjalca ugodnih pogojev, da bi državljani zaupali službam, **tudi vlogo dejavnika vpliva**, saj s svojim delom ustvarjajo **vplivne podatke in informacije, ki jih preko medijev posredujejo javnosti**. V 3. poglavju smo

pojasnili, da kadar stopnja zaupanja ne presega določenega praga, je potreben **nadzor oziroma zaupanje v nadzor**, ki nadomesti manjkajoče zaupanje ter preseže prag (Tan & Thoen, 2001). Demokratični nadzor kot del demokratične vladavine lahko izboljša zaupanje javnosti v službe le v primeru, če javnost ve, da predstavniki parlamenta oziroma drugih nadzornih organov/teles **ustrezno** nadzorujejo službe. Za to, da državljan lahko presodi ustreznost izvajanja nadzora, je **potrebno njegovo poznavanje nadzora**. V 3. poglavju smo pojasnili, da je dobro poznavanje nadzora pogoj za zaupanje državljana nadzoru.

Izvajalci nadzora kot tretje osebe imajo vlogo *nadzornega sredstva*, ki je sestavni del transakcijskega zaupanja: *transakcijsko zaupanje = zaupanje osebi + zaupanje nadzornim sredstvom* (Tan & Thoen, 2001). Če to formulo nekoliko prilagodimo za potrebe doktorske disertacije, dobimo formulo: *transakcijsko zaupanje (državljana) = zaupanje matičnim obveščevalno-varnostnim službam + zaupanje izvajalcem nadzora*. To pomeni, da je **zaupanje v nadzor nujno potrebno za transakcijsko zaupanje**, na podlagi katerega je državljan **pripravljen vstopiti v transakcijo z matično obveščevalno-varnostno službo**, torej ji **izkazovati zaupljivo** (tj. pozitivno) **vedênje** kot ***posledico* zaupanja**. *Zaupanje v nadzor* smo prepoznali kot izjemno pomemben dejavnik zaupanja državljanov v matične obveščevalno-varnostne službe, zato smo ga vključili v splošni model tovrstnega zaupanja kot del podsistema *Državljan* (glej sliko 5.5). Razlog, da je zaupanje v nadzorni mehanizem pogoj za visoko transakcijsko zaupanje, je sicer potrebno razumeti v vlogi zaupanja kot »dopolnila«, s katerim posameznik doseže ali preseže prag, ko je pripravljen zaupati, vendar ga v kontekstu doktorske disertacije vidimo predvsem v vlogi posrednika med službo in državljanom. Izvajalec nadzora je za državljane navadno edini vir (domnevno) ustreznih podatkov in informacij o matični obveščevalno-varnostni službi, od katerih je odvisno, kakšno zaupanje bo državljan izoblikoval v procesu presoje zaupanja. Če državljani viru ne zaupajo, potem ne bodo zaupali podatkom in informacijam, ki prihajajo iz vira, posledično pa ne bodo mogli izoblikovati ustreznega zaupanja v službe ali pa bo to zaupanje negativno (nezaupanje). Ponovno poudarjamo, da nadzor ne sme biti nadomestek ali dopolnilo za zaupanje, kajti če nekdo zaupa zgolj zaradi uporabe nadzora, potem v takšnem primeru ne moremo govoriti o zaupanju.

Intervjuji, ki smo jih opravili, so pokazali, da mora obstajati tudi zaupanje med izvajalci nadzora in matičnimi obveščevalno-varnostnimi službami, na zaupanju pa mora temeljiti tudi sam nadzor. Nezaupanje med obveščevalno-varnostnimi službami in izvajalci nadzora lahko vodi v selektivno, nepotrebno poostreno ali neučinkovito izvajanje nadzora ter pristransko ali neustrezno poročanje javnosti, na strani obveščevalno-varnostnih služb pa v prikrivanje določenih aktivnosti, zapiranje vase in, posledično, nelegitimno in nezakonito delovanje. Čeprav gre za pomembno področje, bi z obravnavo zaupanja med obveščevalno-varnostnimi službami in izvajalci (demokratičnega) nadzora presegli okvir doktorske disertacije, zato bralcem, ki jih to področje bolj podrobno zanima, v branje predlagamo delo avtorjev Born & Mesevage (2012).

5.1.6 Mediji

Medijev v kontekstu splošnega modela zaupanja državljanov v matične obveščevalno-varnostne službe kljub splošno sprejetemu konsenzu, da so del neformalnega nadzora, ne obravnavamo kot del izvajalcev nadzora obveščevalno-varnostnih služb, saj ne izpolnjujejo dveh kriterijev, določenih v prejšnjem podpoglavju. Kljub temu imajo mediji status »tretje« oziroma četrte osebe v verigi prenosa podatkov in informacij. Navadno oziroma laično jih razumemo kot sredstva za množično komuniciranje ali sporočanje, npr. televizija, časopis, radio, plakat, knjiga ipd. Med sredstva, ki jih najdemo na internetu oziroma na svetovnem spletu, spadajo tudi družbena omrežja (forumi, klepetalnice, Facebook, Twitter idr.), spletni video/avdio posnetki in različni zapisi posameznih uporabnikov (npr. blogi, vlogi). Zaradi bolj jasne opredelitve in kasnejše obravnave podsistema *Mediji* pojasnjujemo, da vanj ne uvrščamo le **množična komunikacijska sredstva**, temveč tudi **osebje medijskega subjekta** (npr. novinarji, samostojni raziskovalni novinarji), ki za potrebe **delovanja in uresničevanja namena oziroma nalog medijskega subjekta** (npr. televizijske postaje, časopisne hiše, spletne strani) **uporabljajo množična komunikacijska sredstva**, da podatki in informacije dosežejo ciljno publiko z namenom njihovega informiranja. Druge osebe, ki ne spadajo v to opredelitev, uporabljajo medije, ker so jim na voljo za širjenje določenih podatkov in informacij, vendar se s tem ne ukvarjajo za potrebe delovanja in uresničevanja nalog ter poslanstva medijskega subjekta, pač pa spadajo v enega od drugih podsistemov (državljani,

strokovnjaki, politiki, matične in tuje obveščevalno-varnostne službe idr.). Tako npr. obveščevalno-varnostna služba, ki preko družbenega omrežja obvešča javnost, v skladu z našim vidikov obravnavanja ni del podsistema *Medij*, temveč medije uporablja za obveščanje – takšna primera služb sta npr. NSA in GCHQ, ki uporabljata Twitter za objavljanje sporočil. Ravno tako med medije ne uvrščamo raziskovalcev ali akademikov, ki z namenom promocije svojih objav uporabljajo medije.

Glavni razlog, zaradi katerega medije prepoznavamo kot pomemben dejavnik vpliva na zaupanje državljanov v matične obveščevalno-varnostne službe, je njihov dokazan **vpliv na oblikovanje in spreminjanje javnega mnenja** (glej npr. Rose, 1962; Happer & Philo, 2013; McCombs, 2014; Xiong & Liu, 2014). Kot primer vzemimo ugotavljanje vpliva medijev na oblikovanje javnega mnenja o slovenskem sodstvu (Igličar, 2012, str. 91): »Mediji ustvarjajo pretežni del podobe sodstva v javnosti, kar posledično vpliva tudi na zaupanje državljanov v sodstvo. Zato je za dojemanje sodnega odločanja v javnosti potrebnega veliko pojasnjevanja vseh posebnosti sodnega delovanja, kar daje sodnim institucijam nove naloge in zahteva veliko občutljivosti in korektnosti ter profesionalnost novinarskega poročanja o sodnih primerih. Javnost je bila tudi vedno zainteresirana za delo sodišč, in to v dveh smereh. Po eni strani so bile najprej v ospredju osnovne informacije o sodnih odločitvah, po drugi strani pa je bila vedno izražena težnja javnosti, da sodeluje v konkretnih primerih, vsaj z navzočnostjo ali tudi neposredno pri sprejemanju odločitve.« Čeprav je citirano besedilo prispevek o medijskem poročanju o delovanju slovenskega sodstva v povezavi z zaupanjem državljanov, ga lahko uporabimo tudi za obveščevalno-varnostne službe v Republiki Sloveniji. Skoraj celotni del njihove javne podobe ustvarjajo in spreminjajo mediji, v nekoliko manjši meri pa izvajalci nadzora in vlada oziroma vodstvo države, ki svoja spoznanja in poročila javnosti navadno sporočajo ravno preko medijev. Primer dobre prakse na tem področju opisuje Florina Cristiana Matei (2014), ki je raziskovala povezavo med matičnimi obveščevalno-varnostnimi službami in mediji. Ugotovila je (ibidem), da na javno podobo služb in zaupanje vanje pozitivno vpliva *prepričljiva sposobnost*: pozitivno naravnano poročanje o delu služb, o njihovih operacijah in prispevku k nacionalni in mednarodni varnosti, da delujejo v skladu z demokratičnimi predpisi oziroma demokratičnimi usmeritvami politike.

Medijske objave so pogostokrat sprožile tudi razpravo o legalnosti uporabe HUMINT in točnosti obveščevalnih informacij, kar je v preteklosti že zmanjšalo zaupanje v matične obveščevalno-varnostne službe – tako s strani državljanov kot tudi tujih služb. Do takšnih razkritij je v večini primerov prišlo z odtekanjem podatkov, ne glede na upravičenost ali neupravičenost odtekanja ter dejanj, ki so razkrita v teh podatkih – v vsakem primeru se je zaupanje v službe zmanjšalo. Skupaj s tem je potrebno obravnavati tudi državljane, ki matičnim službam sporočijo podatke. Kadar ti državljani ugotovijo, da so bili razkriti podatki, ki so jih sporočili službi, službi ne bodo več zaupali, saj je dokazala, da ni sposobna ohraniti tajnosti. Takšni »incidenti« negativno vplivajo tudi na pridobivanje novih (in ohranjanje obstoječih, op. G. H.) tajnih sodelavcev (Althoff, 2016).

Odnos med obveščevalno-varnostnimi službami in mediji sicer zaznamujeta nasprotovanje in antipatija (Fitsanakis & Hodges, 2013). Prve delujejo tajno, zato tudi prikrivajo pridobljene podatke in informacije pred javnostjo, medtem ko mediji želijo pridobiti in razkriti ter deliti čim več podatkov in informacij (Matei, 2014), zato jim lahko medijska odmevnost in ekskluzivnost pomenita več kot pa tajnost in varnost. Kljub temu imata obe strani medsebojne koristi. Mediji preko formalnih in neformalnih kanalov od obveščevalno-varnostnih služb pridobivajo podatke in informacije, službe pa uporabljajo medije kot nosilce političnega odobravanja in legitimnosti v širšem družbenem okolju (Fitsanakis & Hodges, 2013, str. 15). Preko medijev lahko službe pridobijo zaupanje in podporo različnih družbenih slojev ter širše javnosti (Matei, 2014). A službe ne uporabljajo medijev le za ustvarjanje pozitivne podobe v medijih, temveč **tudi za manipulacijo** (glej npr. Magen, 2014; Joseph, 2017, str. 504-506) oziroma za plasiranje informacij in dezinformacij. Poleg obveščevalno-varnostnih služb uporabljajo medije za vplivanje na javno mnenje tudi politiki (Besley & Prat, 2006), gospodarstveniki, interesna združenja, posamezniki idr. Lépin (2014) pravi, da so neodvisni mediji eden izmed ključnih dejavnikov, ki vplivajo na vzdrževanje zaupanja in družbene pogodbe v demokracijah. Neodvisnost je nujno potrebna, saj mediji ne le projicirajo všečnost in kompetentnost zaupnika, temveč tudi ojačajo njegov pomen, namen oziroma bistvo (Martin, 2014, str. 49). Odvisnost in pristranskost povzročata subjektivno in usmerjeno poročanje ali prikazovanje, ki ima navadno v ozadju določen namen, interes.

Intervjuvanci, s katerimi smo spregovorili tudi o medijih, menijo, da ti s svojim nekritičnim poročanjem o matičnih obveščevalno-varnostnih službah lahko povzročijo škodo nacionalni varnosti in nacionalnim interesom. Podobno ugotavlja tudi Matei (2014, str. 95-96).

Van de Walle et al. (2008) ugotavljajo, da ima na percepcijo učinkovitosti celotnega javnega sektorja zelo velik vpliv poročanje medijev o percepciji drugih državljanov. Na mnenje državljanov o politiki vplivajo tudi škandali in afere, vendar ne nujno na dolgi rok, enako pa menijo o vplivu afer v javnem sektorju (ibidem). K vsemu temu prispeva tudi stopnja znanja državljana, ki za potrebe delovanja in uresničevanja nalog ter poslanstva medijskega subjekta, o obveščevalno-varnostni dejavnosti, nacionalnem obveščevalno-varnostnem sistemu, njegovih subjektih in ostalih s tem povezanih področjih. Moč in vpliv medijev na poročanje o institucijah javnega sektorja je na podlagi ugotovljenega pomemben dejavnik zaupanja državljanov v matične obveščevalno-varnostne službe. Če si ponovno izposodimo Igličarjeve besede (2012, str. 92) in jih uporabimo na področju zaupanja državljanov v matične obveščevalno-varnostne službe, sta družbeno dojemanje in ocenjevanje javnega mnenja odvisna od poročanja medijev, nastopov politikov in tudi od nastopov predstavnikov matičnih obveščevalno-varnostnih služb.

Pomembna naloga medijev je tudi izobraževanje in širjenje znanja. Mediji lahko pripomorejo k izobraževanju laičnih državljanov, politikov, izvajalcev nadzora in tudi drugih oseb o obveščevalno-varnostni dejavnosti, politiki in službah na več različnih načinov: časopisni članki, objavljanje prispevkov v revijah in zbornikih, radijske in televizijske oddaje, video posnetki (na spletu), blogi, spletne strani (Matei, 2014).

Kljub temu pa moramo poudariti, da sta moč in vpliv medijskega poročanja na zaupanje državljana v matične obveščevalno-varnostne službe odvisna od državljanovega znanja – predvsem od percepcije in sposobnosti kritične presoje informacij – ter od vira podatkov in informacij – neposredno od služb ali od z njimi povezanih subjektov (npr. izvajalci nadzora, politika, strokovna javnost). Dodajamo, da tudi posameznik podzavestno presoja zanesljivost vira (tako kot pri analitiki v obveščevalno-varnostnih

službah), zato ima lahko enak podatek, ki ga posreduje subjekt A, večjo težo, kot pa če ga posreduje subjekt B.

5.1.7 Strokovna javnost

Podsistem *Strokovna javnost* predstavljajo strokovnjaki za področje obveščevalno-varnostne dejavnosti oziroma dela obveščevalno-varnostnih služb in nacionalnega obveščevalno-varnostnega sistema. Ti lahko prihajajo z različnih področij, npr. pravo, človekove pravice, informatika, politologija, varstvoslovje, obramboslovje, psihologija, ekonomija, mednarodni odnosi, zgodovina, logistika, strojništvo. Ti strokovnjaki imajo določeno **znanje**, nekateri pa tudi **izkušnje**, zaradi katerega oziroma katerih je strokovnjak za državljana potencialni vir podatkov in informacij. Pri tem potrebno poudariti, da so z našega vidika obravnavanja strokovnjaki del podsistema *Strokovna javnost* le, če ti **niso zaposleni** v strukturah nacionalnega obveščevalno-varnostnega sistema. Po našem prepričanju obstajajo trije razlogi, zakaj npr. aktivnih oziroma aktualnih uslužbencev obveščevalno-varnostnih služb in drugih oseb iz nacionalnega obveščevalno-varnostnega sistema kljub znanju in izkušnjam ne moremo uvrstiti v podsistem *Strokovna javnost*. Prvi razlog: te osebe so že del podsistema *Matična obveščevalno-varnostna služba* oziroma *Nacionalni obveščevalno-varnostni sistem*. Čeprav je ena oseba v resničnem življenju lahko del več različnih podsistemov, moramo v okviru obravnavane tematike zaupanja državljanov v matične obveščevalno-varnostne službe posamezne podsisteme (in njihove podsisteme nižjega reda, v tem primeru strokovnjake) presojati predvsem z vidika pridobivanja podatkov in informacij za presojo zaupanja. Zaradi tajnosti, ki jo prepoznavamo kot drugi razlog, se uslužbenci ne smejo javno izpostavljati niti ne smejo razkriti podatkov, ki se nanašajo na njihovo delo oziroma na službo in so v skladu s predpisi označeni kot tajni. Vloga uslužbencev je v kontekstu pridobivanja podatkov in informacij za presojo zaupanja zaradi tajnosti zato zmanjšana in omejena. S tega vidika jih zato ne moremo enako obravnavati kot del strokovne javnosti. Tretji razlog pa je ozadje izraza *Strokovna javnost*: strokovna javnost je *javna* in (lahko) *deluje javno*, medtem ko za matične obveščevalno-varnostne službe tega ne moremo trditi.

Uslužbence obveščevalno-varnostnih služb in druge osebe iz nacionalnega obveščevalno-varnostnega sistema vsekakor prepoznavamo kot strokovnjake, vendar ne kot tiste, ki so del strokovne *javnosti* oziroma podsistema *Strokovna javnost*. Do neke mere bi bilo upravičeno trditi, da so te osebe del strokovne javnosti, kadar izven delovnega časa predstavljajo svoje mnenje/znanje o določeni zadevi s področja obveščevalno-varnostne dejavnosti in pri tem ne zastopajo službe niti njenih stališč, vendar jim tajnost preprečuje, da bi lahko v tej smeri povsem javno delovali. Podobno so pri svojem javnem delovanju omejeni s tajnostjo nekdanji uslužbenci tovrstnih služb in druge osebe, ki so bile nekoč del nacionalnega obveščevalno-varnostnega sistema, vendar te osebe niso več del teh podsistemov, zato spadajo v *javni* del strokovne sfere, o tajnih podatkih ne razpravljajo.

Vlogo strokovnjakov smo prepoznali kot **vir znanja**, ki lahko opozarja na nepravilnosti ali potrebne izboljšave na področju nacionalnega obveščevalno-varnostnega sistema, hkrati pa lahko **s svojim delom** (npr. medijski prispevki, izdaja publikacij in drugih oblik pisanj, projektno delo, druge aktivnosti za uzaveščanje laične javnosti) **vplivajo** na zaupanje državljanov v matične obveščevalno-varnostne službe. Slednje izvaja predvsem v smislu **širjenja znanja, pojasnjevanja določenih dogodkov in njihovih ozadij** ter **kritičnega ocenjevanja odnosa** družbe/javnosti do teh služb. Ocenjujemo, da **večina politikov, medijev in državljanov nima (dovolj) znanja** o obveščevalno-varnostnih službah, sicer bi razumeli, da je (oziroma mora biti) odnos med njimi in matičnimi obveščevalno-varnostnimi službami drugačen kot npr. odnos s policijo. Strokovnjaki imajo dovolj znanja, zato so pri svojem razmišljanju bolj kritični, s tem pa tudi bolj pomembni pri aktivnem ali pasivnem oziroma posrednem ali neposrednem ustvarjanju in povečevanju zaupanja državljanov v matične obveščevalno-varnostne službe. S tega vidika predstavljajo strokovnjaki »oddajnike« vpliva na državljane, še posebej takrat, kadar svoje mnenje izrazijo preko medijev. Nekdanji direktor OVS je v intervjuju dejal, da »do kritičnega stanja zaupanja pride takrat, kadar obveščevalno-varnostnim službam ne zaupajo več niti intelektualci oziroma tisti, ki imajo o tem nekaj znanja.« V tem smo prepoznali dodatni argument, da je znanje tisti dejavnik, ki pomembno vpliva na ustvarjanje in oblikovanje zaupanja. Čeprav bi lahko domnevali, da bi za izboljšanje javnega mnenja zadostoval vpliv strokovne javnosti, ki ima znanje, pa zgolj mnenje

strokovnjakov ne zadostuje za protiutež javnemu mnenju. Potrebne so namreč večje spremembe, predvsem na področju splošnega znanja (laične javnosti) o obveščevalno-varnostni dejavnosti in tovrstnih službah.

Na tem mestu moramo opozoriti na **osebe, ki nimajo dovolj znanja ali pa to znanje ni pravo, da bi jih lahko upravičeno imenovali *strokovnjaki*,** vendar se sami (ali pa vsaj tako mislijo) okličejo za strokovnjake ali jih zanje okličejo drugi. Tudi taki širijo svoje pomanjkljivo znanje, ki je lahko neustrezno, zmotno ali lažno, neustrezno pojasnjujejo določene dogodke in njihova ozadja ter nekritično ali pristransko ocenjujejo nekatere odnose in relacije med subjekti nacionalnega obveščevalno-varnostnega sistema z drugimi organi in z državljani.

5.1.8 Laična javnost

Laična javnost je podsistem, ki je glede na količino njegovih sestavin najbolj obsežen, saj ga sestavljajo državljani, ki niso del nacionalnega obveščevalno-varnostnega sistema, matičnih obveščevalno-varnostnih služb, politike, nadzora, strokovne javnosti niti tujih obveščevalno-varnostnih služb. V jeziku sistemske teorije je podsistem *Laična javnost* sestavljen iz več podsistemov *Državljan*. V doktorski disertaciji obravnavamo laično javnost kot skupino prebivalstva, ki o obveščevalno-varnostni dejavnosti in tovrstnih službah navadno nima (veliko) znanja niti interesa za spremljanje tega področja. Pomanjkanje ustreznega znanja je tisto, ki po našem prepričanju povzroča, da je tako obsežen podsistem mogoče usmerjati in z njim »upravljati« (oziroma manipulirati) v skladu z interesi politike, gospodarstva, interesnih skupin, vplivnih organizacij, državnih ustanov ipd. Kot ugotavljajo nekateri avtorji (Horniak, 2016), lahko politika in mediji bistveno vplivajo na oblikovanje javnega mnenja. To se »spreminja v skladu s političnimi vplivi, ki naraščajo in pojemajo po svoji moči.« (Kaase et al., 1999, str. 121-122) Ob tem je potrebno razlikovati med »nihanji in trendi v javnem mnenju. Nihanja so relativno kratkotrajna; trajajo od nekaj mesecev pa do nekaj let,« (ibidem, str. 127) zato je težje spremeniti trende javnega mnenja. Pomembnost javnega mnenja v kontekstu zaupanja zato vidimo v njegovem potencialu za doseganje družbenih sprememb, predvsem z ustvarjanjem družbenega pritiska, ki ima lahko za posledico spremembo zakonodaje,

strukture in organizacije sistemov, kadrov, financiranja matičnih obveščevalno-varnostnih služb idr.

Ocenjujemo in trdimo, da se javnost pretežno ne zanima za področje obveščevalno-varnostne dejavnosti. Z dogodki, ki vplivajo na podobo ali delo matičnih obveščevalno-varnostnih služb, se najpogosteje seznani preko medijev. Ti dogodki so lahko sami po sebi pozitivni ali negativni in jih kot take lahko obravnava tudi javnost. Mediji lahko sporočilnost dogodka popolnoma spremenijo in/ali pa ga ojačajo, zato ima lahko medijsko poročanje drugačen učinek na mnenje posameznikov in javno mnenje, kot pa zaznavanje samega dogodka brez vpletenosti medijskega poročanja. To je še posebej opazno pri poročanju o negativnih dogodkih, saj praksa in osebno zaznavanje kažeta, da nekateri mediji obravnavajo in prikazujejo tovrstne dogodke zelo pristransko, pri čemer bolj izpostavljajo nekatere razsežnosti, dele ali vidike dogodkov, jih dopolnijo z drugimi podatki in informacijami, spremenijo kontekst ipd. V zadnjih letih se je razširilo t.i. lažno poročanje (ang. *fake news*). Negativni dogodki imajo že sami po sebi večjo težo in večji vpliv na javno mnenje, medijsko poročanje pa ga lahko še bolj približa skrajnosti. O vplivu negativnih dogodkov (oziroma moči negativne informacije) in logike oportunitetnega vpliva smo govorili že v podpoglavju 5.1.2. Nekdanji direktor OVS je v intervjuju pojasnil, da so državljani ob spremembah (navadno ob poslabšanju) varnostnih razmer bolj naklonjeni sprejetju predlogov politike, kako bi odpravili posledice razmer in odpravili obstoječe nepravilnosti določenega sistema. Vendar pa naj bi se za temi predlogi skrivali predvsem lastni interesi politikov ali političnih strank. Npr. ko je administracija ameriškega predsednika Georga W. Busha (ob kasnejši podpori britanskega premierja Tonya Blaira) lažno potrdila obstoj orožja za množično uničevanje v Iranu, so državljani podprli večino predlaganih ukrepov za sankcioniranje Iraka in Sadama Huseina, ki jih je predlagala politika. Posebna nevarnost, ki smo jo prepoznali na tem področju, pa je vpliv tujih obveščevalno-varnostnih služb na medije, politiko in drugo, kar lahko vpliva na javno mnenje o matičnih obveščevalno-varnostnih službah. Njihov vpliv pojasnjujemo v naslednjem podpoglavju.

Laična javnost se (lahko) odziva tudi na spremembe, ki jih sprejme politika (npr. že omenjena sprememba zakonodaje oziroma pooblastil britanskih in francoskih

obveščevalno-varnostnih služb). Javnost (naj bi) se na odločitve politike odziva(la) na podoben način, kot deluje termostat pri tehničnih sistemih: če se zastavljena politika razlikuje od želja in pričakovanj javnosti, bo javnost zahtevala spremembe in uporabila ustrezne ukrepe, da se ta razkorak zmanjša (Wlezien, 1995). Kljub temu lahko politika z drugimi ukrepi doseže kompromis ali celo nadvlado (npr. popravek predpisov, obljube, sprejetje drugih ukrepov, odvzem pravic, prepovedi), s čimer se pritisk javnosti zmanjša oziroma ustavi. Težava nastopi, kadar javnost ne spremlja delovanja politike ali pa nima dovolj znanja ali zanimanja, da bi jo spremljala, zato je dovzetna za manipulacijo in zlorabo. Baldino (2018) pravi, da je (ustrezno in z resničnimi dejstvi, op. G. H.) informirana družba bolj ustrezna za preučevanje in odločanje o potrebah matičnih obveščevalno-varnostnih služb (to vključuje področje nalog, pooblastil, proračuna, nadzora služb ipd.). Ker laična javnost navadno predstavlja večji del neke družbe (ne glede na področje), je pomembno, da se prepreči morebitno manipuliranje takšnega večjega števila ljudi, saj lahko z volitvami, s spremembo zakonodaje ali pritiski na politiko spremeni delovanje posameznega dela ali celotnega državnega sistema – v našem primeru nacionalnega obveščevalno-varnostnega sistema oziroma sistema nacionalne varnosti.

Zato ugotavljamo, da ima podsistem *Laična javnost* v splošnem modelu zaupanja državljanov v matične obveščevalno-varnostne službe predvsem funkcijo subjekta, ki lahko posredno spremeni nacionalni obveščevalno-varnostni (pod)sistem, njegove podsisteme, lahko pa vpliva tudi na spremembo drugih podsistemov. S tega vidika se strinjamo z Wlezienom (1995), ki javnost vidi kot družbeni termostat. Ponovno poudarjamo, da je učinkovitost takšnega »termostata« odvisna predvsem od njegovega znanja, ki hkrati določa, koliko je posameznik oziroma družba kot celota dovzetna za manipulacijo s strani medijev in politike. Ker pa je ta (pod)sistem največji, ga je tudi težje spremeniti, preoblikovati ali usmeriti (v kratkem času) brez ustreznih vzvodov, večino le-teh pa imata v rokah politika in mediji oziroma oba skupaj.

5.1.9 Tuje obveščevalno-varnostne službe

Eden izmed intervjuvancev je dejal, da na zaupanje državljanov matičnim obveščevalno-varnostnim službam poskušajo vplivati oziroma vplivajo tudi tuje obveščevalno-varnostne službe. Prepoznali smo dva načina, kako lahko tuje službe vplivajo na tovrstno zaupanje:

- *Zmanjšanje zaupanja oziroma ugleda je **primarni cilj** tuje obveščevalno-varnostne službe*. S tem želi tuja služba namerno oslabiti njej tujo obveščevalno-varnostno službo.
- *Zmanjšanje zaupanja oziroma ugleda je **»stranski produkt« druge aktivnosti** tuje obveščevalno-varnostne službe*. Do upada zaupanja pride večinoma zaradi (varnostnega) dogodka ali medijskega poročanja, ki na matično obveščevalno-varnostno službo meče slabo luč zaradi njenih aktivnih ravnanj ali »neaktivnosti«.

Zagotovo obstajajo tudi drugi načini, s katerimi tuje obveščevalne službe želijo škodovati ugledu in delovanju njim tujih služb, vendar smo našteli le dva. Ker med dostopnimi viri ne najdemo znanstvenih prispevkov na to tematiko, lahko le domnevamo, s katerimi aktivnostmi in na kakšne načine poskušajo tuje službe vplivati na zaupanje. Namige o domnevni vpletenosti tujih obveščevalno-varnostnih služb v vplivanje na podobo in s tem zaupanje državljanov v matične obveščevalno-varnostne službe smo iskali tudi v medijskih objavah. V zvezi s prvim načinom vplivanja na zaupanje nismo našli nobenih objav, našli pa smo eno objavo v zvezi z drugim načinom. Primer se navezuje na vmešavanje Rusije v ameriške predsedniške volitve leta 2016. Skupno poročilo ameriških obveščevalnih služb (glej Office of the Director of National Intelligence, National Intelligence Council, 2017) pravi, da je ruska vlada za namene vplivanja na potek in rezultat volitev uporabila svoje obveščevalno-varnostne službe oziroma prikrite obveščevalno-varnostne operacije v kombinaciji s svojimi državnimi mediji, vladnimi agencijami in tretjimi osebami. V tem kontekstu je bila pozornosti deležna predvsem ruska medijska mreža *Russia Today,* danes imenovana RT, ki deluje v ZDA pod imenom *RT America* in je v lasti ruske vlade. Ta medijska mreža naj bi delovala v skladu z ruskimi nacionalnimi interesi, zato je (bila) pogosto tarča obtožb, da je rusko sredstvo za vplivanje oziroma propagando na ameriških tleh. Ob pojavu novice o ruskem vmešavanju v

ameriške predsedniške volitve je bila kritik deležna tudi ameriška obveščevalna skupnost, ki so ji očitali, da je premalo naredila, da bi preprečila aktivnosti ruskih obveščevalno-varnostnih služb. Predpostavljamo, da na podoben način tuje obveščevalno-varnostne službe uporabljajo organizacije in posameznike kot tajne sodelavce za vplivanje. Tajni sodelavec za vpliv je oseba, ki tajno sodeluje z obveščevalno-varnostno službo in je uporabljena, da s svojim vedênjem in delovanjem vpliva na odločitve odločevalcev in potek dogodkov (Šaponja, 1999). Zaradi njihovega družbenega položaja, moči ali povezav z določenimi ljudmi so lahko zelo močjo orodje obveščevalno-varnostnih služb. S svojim vedênjem in delovanjem lahko vplivajo tudi na javno mnenje, kar v kombinaciji z aferami lahko ustvari učinkovito sredstvo za delovanje proti obveščevalno-varnostnim službam (npr. za povzročanje izgube ugleda, zaupanja, posameznih tajnih sodelavcev ali celotne sodelavske mreže, tajnih lokacij, virov). Tajni sodelavci za vpliv so še posebej nevarni takrat, kadar lahko vplivajo na politike in osebe, ki so posredno ali neposredno vpletene v delo obveščevalno-varnostnih služb.

Načinov, kako tuje obveščevalno-varnostne službe vplivajo na zaupanje državljanov v matične obveščevalno-varnostne službe, je zagotovo več, zato verjetno obstaja več načinov posrednega vpliva in manj načinov neposrednega, česar pa zaradi pomanjkanja literature ne moremo raziskovati/dokazati.

5.1.10 Drugi vplivi

V tem podpoglavju so predstavljeni drugi vplivi, ki ne prihajajo iz doslej predstavljenih podsistemov. Uporabili smo le nekatere vplive, ki z našega vidika obravnavanja pomembno vplivajo na proces presoje zaupanja. Za druge vplive, ki tu niso izpostavljeni ali omenjeni, dopuščamo, da so pomembni za obravnavanje tematike doktorske disertacije z drugega vidika obravnavanja, vendar jih z našega dialektičnega sistema vidikov nismo prepoznali kot pomembne.

Iz sivega kroga, prikazanega na sliki 5.3, izhajajo tisti drugi vplivi, ki so nastali zaradi povezav in interakcij med predstavljenimi podsistemi, v določeni meri pa tudi skupaj z drugimi podsistemi, ki niso prikazani na sliki niti omenjeni v doktorski disertaciji (npr.

gospodarstvom kot sistemom, družbeno-ekonomskim sistemom, pravosodnim sistemom in drugimi podsistemi, ki so del sistema nacionalne varnosti), vendar zaradi omejitev doktorske disertacije tu niso obravnavani. Tovrstni vplivi predstavljajo **sinergije**, ki nastanejo med izpostavljenimi podsistemi, in vplivajo tako na same podsisteme kot tudi na druge, »zunanje« podsisteme (vse ostale podsisteme človekovega in družbenega življenja), v kontekstu naše raziskave pa tudi na državljana in na njegov proces presoje zaupanja.

Za lažjo obravnavo prvega takšnega vpliva se za trenutek vrnimo k dispozicijskemu zaupanju. Na prvi pogled nima večje vloge pri presoji konkretnih in specifičnih dejavnikov v zvezi z matično obveščevalno-varnostno službo, saj se osredotoča le na splošne dejavnike oseb na splošno. Sestavljeno je iz *(za)upanja v človeštvo* in *naravnanosti k zaupanju*, na kateri vplivajo odraščanje in izkušnje (Rotter, 1967; McKnight & Chervany, 2001). Odraščanje je tesno povezano z vrednotami, te pa so povezane s kulturo, etiko in normami, zato v konceptu dispozicijskega zaupanja prepoznavamo pomembnost dialektičnega sistema **VKEN** (glej Potočan & Mulej, 2006). Ker družbene vrednote in ideologije vplivajo na zaupanje v institucije (Toš, 2007), vpliva koncept VKEN tudi na institucionalno zaupanje. Da je soodvisni splet VKEN pomemben del dispozicijskega zaupanja, je mogoče posredno zaznati tudi v obravnavanem prispevku avtorjev Doney et al. (1998), ki so preučevali, kako **nacionalna kultura** vpliva na razvoj zaupanja. Iz njihovega modela nacionalne kulture in razvoja zaupanja (slika 3.10) izhaja, da nacionalna kultura vpliva na izoblikovanje norm, vrednot in predpostavk o vedênju, te pa na kognitivne procese in končno na samo zaupanje. Zato smo ocenili, da lahko koncept VKEN avtorjev Potočan & Mulej (2006) utemeljeno in upravičeno upoštevamo kot dejavnik vpliva na proces presoje zaupanja, natančneje pri dispozicijskemu zaupanju. Doney et al. (1998) so ugotovili, da kadar upnik in zaupnik izhajata iz iste kulture (to pomeni, da si delita enake norme in vrednote), obstaja večja verjetnost, da se bo med njima oblikovalo zaupanje, kadar pa se kultura razlikuje, pa bo zaupanje težje vzpostavljeno (ibidem). Iz tega izhaja, da **ima posameznikovo okolje velik vpliv** na njegovo nagnjenost k zaupanju drugih na splošno, na podlagi dialektičnega sistema treh vrst zaupanja pa ugotavljamo, da vpliva tudi na institucionalno in medosebno zaupanje. Ni pa le nacionalna kultura tista, ki vpliva na državljana in s tem njegov proces presoje

zaupanja. Tu je potrebno omeniti npr. tudi **varnostno** in **politično kulturo**, ki skupaj z nacionalno in drugimi kulturami tvorijo dialektični sistem VKEN. Z VKEN je povezan tudi naslednji vpliv, ***zaznavanje* nacionalne varnosti**. Podobno kot pri tveganju je v ospredju posameznikovo dojemanje in ne nacionalna varnost, ki se odraža v različnih stanjih in dejanjih. Neupoštevanje etike in norm, s katerimi se zagotavlja varovanje vrednot in kulturo (oziroma kulture) določene nacije/države, lahko ogrozi vrednote in kulturo (oziroma kulture). Od dojemanja nacionalne varnosti pa je odvisno tudi dojemanje tveganj in njihovo posledično sprejemanje. Vse to se, kot smo že pojasnili, odraža tudi v samem zaupanju. Naslednji tovrstni vpliv na zaupanje je **(ne)stabilnost notranjega okolja**, tj. okolja, ki ga tvorijo podsistemi v sivem krogu na sliki 5.3. Vsaka nestabilnost lahko negativno vpliva predvsem na komponente institucionalnega zaupanja, dodatno pa na zaznavanje in sprejemanje tveganj, občutek varnosti, zaznavanje, prenos podatkov in informacij itd. Izjemno pomemben vpliv ima tudi stopnja **zagotavljanja in varstva človekovih pravic**, kar še posebej pride do izraza pri kršitvah človekovih pravic s strani matičnih obveščevalno-varnostnih služb, pri pripravljanju in sprejemanju zakonodaje na področju pooblastil tovrstnih služb ter pri izvajanju (demokratičnega) nadzora nad tovrstnimi službami. Namesto tega bi lahko rekli, da na zaupanje pomembno vpliva, v kolikšni meri je neka država **pravna država**.

Drugi vplivi iz (zunanjega) okolja pa so vsi tisti vplivi, ki ne izhajajo iz podsistemov in sinergij dialektičnega sistema dejavnikov, ki ga predstavlja sivi krog na sliki 5.3, imajo pa vpliv na proces presoje zaupanja. Ti so posebej označeni na sliki 5.3, kažejo pa se v različnih pojavnih oblikah, saj izhajajo iz različnih vrst okolij (npr. nacionalno, regionalno, mednarodno varnostno okolje, delovno okolje, politično, gospodarsko, ekonomsko, geografsko, naravno in ekološko okolje). Takšen vpliv je tudi **(ne)stabilnost zunanjega okolja**, ki vpliva ne le na državljana in njegovo presojo zaupanja, temveč na celoten dialektičen sistem dejavnikov na sliki 5.3 (in s tem ponovno na državljana, vendar »z druge strani«). Tako kot pri nestabilnosti notranjega okolja ima lahko negativen vpliv na proces presoje zaupanja tudi nestabilnost zunanjega okolja. Na področju varnosti in zaznavanja varnosti ter tveganj vpliva **regionalna, mednarodna, transnacionalna in globalna varnost** na varnostno, finančno, gospodarsko, politično, gospodarsko in drugo stanje države. Enako lahko trdimo za različne **krize in katastrofe** (humanitarne,

zdravstvene, politične, podnebne, ekološke, finančne idr.) ter druge negativne dogodke in pojave, kot je npr. **korupcija** (v obveščevalno-varnostnem sistemu). Vse to posredno ali celo neposredno vpliva na dejavnike, povezane z državljanovim procesom presoje zaupanja.

Poseben vpliv, ki bi ga težko umestili v (zunanje) okolje kot prostor, saj je vezan na čas, hkrati pa bi težko rekli, da izhaja (zgolj) iz VKEN, je **preteklost**. Preteklost smo obravnavali kot pretekle dogodke, stanja in okoliščine oziroma **pretekle izide**, ki so vplivali in v večji ali manjši meri še vedno lahko vplivajo na posameznika ali del/celotno družbo na družbenem, političnem, gospodarskem, socialnem ali drugem področju. Ti pretekli izidi so »zapisani« v posameznikov spomin, v kolektivni spomin družbe ali v različne fizične, danes pa tudi digitalne oziroma virtualne zapise. Medtem ko bi z vidika družbe *preteklost* lahko razumeli kot pretekle izide z vplivom na manjši ali večji del družbe, gre pri posamezniku za dojemanje, razumevanje in obravnavanje preteklosti oziroma preteklih izidov na individualni ravni (osebne izkušnje). Vpliv preteklosti na dojemanje obveščevalno-varnostne dejavnosti in matičnih obveščevalno-varnostnih služb se kaže tudi danes, npr. v Nemčiji omemba tovrstnih služb še vedno prikliče spomine na nekdanji tajni policiji Gestapo in Stasi (Schultheis, 2019). Podobno je z državami zahodnega Balkana in držav, ki so bile nekoč pod komunističnim režimom, saj so takratne službe zaradi spornega delovanja povzročile, da ima spomin na tiste čase še danes negativen vpliv (glej npr. Fitsanakis & Hodges, 2013). Negativen vpliv, ki ga povzroči dojemanje preteklih izidov (lastnih, tujih ali obojega), lahko v kombinaciji z vplivom podsistemov *Laična javnost*, *Politika* in *Mediji* bistveno oteži vzpostavitev ali povečanje zaupanja državljanov v matične obveščevalno-varnostne službe.

5.2 Zadostno in potrebno celovito zaupanje

Model osnovnega zaupanja državljanov v matične obveščevalno-varnostne službe nima vnaprej določenega izhoda iz sistema niti usmeritve, kakšen naj bo ta izhod. Cilj doktorske disertacije pa je ustvariti model, ki bo ustvaril in vzdrževal zaupanje, natančneje takšno zaupanje, ki bo potrebno in hkrati zadostno, torej pozitivno zaupanje. To smo dosegli z izgradnjo modela celovitega zaupanja državljanov v matične

obveščevalno-varnostne službe, ki temelji na konceptu **zadostnega in potrebno celovitega zaupanja**. Ta izraz smo dobili z združitvijo izrazov *zaupanje* ter *zadostna in potrebna celovitost*, v svoji vsebini pa združuje teoretične koncepte zaupanja ter zakon zadostne in potrebne celovitosti (Mulej, 1979; Mulej & Kajzer, 1998; Mulej et al., 2000; Mulej et al., 2008). Zadostno in potrebno celovito zaupanje ni nova vrsta/zvrst ali tipologija zaupanja, temveč tista **stopnja** zaupanja, ki jo z upoštevanjem zakona zadostne in potrebne celovitosti štejemo za **celovito**. Izraz *celovitega* v naslovu doktorske disertacije tako odraža zadostno in potrebno celovitost, ki jo iščemo, opredeljujemo in uporabljamo na področju zaupanja.

Lewicki et al. (2006, str. 1016) ugotavljajo, da večina literature o zaupanju temelji na predpostavki, da zaupanje pomeni nekaj dobrega, nezaupanje pa nekaj slabega. Tudi nezaupanje je lahko kdaj koristno in potrebno, še posebej kadar moramo dvomiti v zanesljivost druge strani (ibidem). Mag. Tonin je v intervjuju dejal, da ni nič narobe, če so ljudje stalno malo nezaupljivi, ker če bi preveč zaupali, potem tem službam lahko tudi nekoliko zmanjšajo, olajšajo nadzorne mehanizme in službe vedno izkoristijo možnost, ki jih imajo, in hitro gredo preko meje. Pravi, da je neka zdrava mera nezaupanja z vidika delovanja celotne družbe dolgoročno za te službe celo koristna in da je nezaupanje državljanov do teh služb koristno za same obveščevalno-varnostne službe, ker jih sili k delovanju v skladu z zakonom in znotraj v nekih merilih. Popolno zaupanje tako omogoča možnost njegove zlorabe, popolno nezaupanje pa škodi predvsem upniku, zato je potrebno ustrezno razmerje zaupanja in nezaupanja (Lewicki et al., 2006). Laeequddin et al. (2010) ugotavljajo, da literatura ne daje odgovorov na vprašanja, koliko zaupanja je potrebnega, kje je prag zaupanja in kje so začetne, optimalne in najvišje točke zaupanja v procesu njegove izgradnje. Bijlsma & Koopman (2003) se sprašujeta, ali sploh obstaja najnižja točka zaupanja, saj je zaupanje mogoče izgraditi v vseh okoliščinah, za njegov začetek pa je vedno potreben »skok v neznano«. V obravnavani literaturi nismo našli nobenega prispevka, ki bi definiral, koliko zaupanja je potrebnega in katera stopnja je optimalna, niti izraza, ki bi to zajemal, zato smo uporabili izraz *zadostno in potrebno celovito zaupanje*.

Kot ugotavljajo nekateri avtorji (npr. Lewicki et al., 2006), mora biti med zaupanjem in nezaupanjem ustrezno ravnovesje, saj ena ali druga skrajnost ne povzročata koristi. Zaupanje in nezaupanje torej nastopata kot teza in antiteza. Njuno ravnovesje v skladu z zakonom zadostne in potrebne celovitosti naj bi zagotavljalo takšno celovitost. Vrnimo se na začetek podpoglavja 3.1, v katerem smo izbirali ustrezno terminologijo oziroma ustrezni angleški izraz za zaupanje. Ugotovili smo, da izraz *trust* pomeni pričakovanje ali prepričanje, ki temelji na **intelektu** in **čustvih** (Judge, 1999) ter nepopolnih oziroma nepojasnjenih dokazih (Hart, 1988), torej zaupanje (*trust*) temelji na ravnovesju med intelektom in čustvi. V podpoglavju 3.3 smo pojasnili, da je kognitivno zaupanje tisto, ki izhaja iz upnikovega **intelekta**, afektivno pa tisto, ki izhaja iz upnikovih **čustev**. V tem smo prepoznali **podobnost** s konceptom zadostne in potrebne celovitosti ter zaupanja v obliki angleškega izraza *trust*, ki ga je definiral Judge (1999) v odnosu do izrazov *faith* in *confidence* (glej sliko 3.1). *Faith* temelji izključno na **čustvih**, zato predstavlja **enostranski in subjektivni vidik**. Nasprotno temelji *confidence* izključno na **dokazih** in zaradi odsotnosti subjektivnih vidikov presojevalca predstavlja **objektivni vidik**, ki naj bi odražal **»absolutno, nepristransko resnico«** (tu bi sicer lahko razpravljali, ali dokaze v obliki medijskih informacij lahko prištevamo med objektivne dejavnike, vendar izhajamo iz stališča, da so dokazi tisto, kar nepristransko dokazuje del stvarnosti oziroma, kot temu pravijo v pravu, *materialno resnico*). *Trust*, ki se nahaja med *faith* in *confidence*, povezuje miselne in čustvene vidike ter omogoča dovolj stvarno obravnavo konteksta, s tem pa zadostno in potrebno celovito obravnavo zaupanja tako s čustvenega kot dokaznega vidika. To sicer ne pomeni, da je vrsta zaupanja, za katero angleški jezik uporablja izraz *trust*, že samo po sebi zadostno in potrebno celovita. Pomeni pa, da če želimo biti celoviti, moramo vključevati – tu ponovno navajamo Muleja et al. (2008, str. 80) – »vse bistvene in samo bistvene vidike v **miselno in**/ali **čustveno** sliko o obravnavanem pojavu.« Po našem prepričanju je zato vrsta zaupanja (*trust*) ustrezno izhodišče za oblikovanje zadostnega in potrebno celovitega zaupanja, saj upošteva dokaze in čustva. Pri tem moramo »zavestno in premišljeno, obenem pa tudi kar se da celovito *opredeliti*, katero *raven celovitosti* v danem primeru velja *šteti za primerno*.« (Mulej et al., 2000, str. 73)

Pri tem so pomembna tudi objektivna in subjektivna izhodišča, s katerimi posameznik izoblikuje dialektični sistem vidikov obravnavanja. Katere miselne in čustvene vidike je potrebno izbrati, presoja posameznik, zato je tudi sam odgovoren za posledice, ki jih prinaša njegova opredelitev zadostne in potrebne celovitosti. Raven celovitosti lahko celovito opredelimo tako, da »[p]oskušamo […] iskati **srednjo pot med preveč zapletenosti in poenostavljenosti** […].« (Mulej et al., 2000, str. 74) Ne smemo pretiravati v smeri celovitosti, ki je zgolj objektivna (*confidence*), niti v smeri celovitosti, ki je zgolj subjektivna (*faith*), temveč moramo upoštevati dejansko potrebo, da upoštevamo svojo soodvisnost in razvijemo svoja subjektivna izhodišča v smeri za medstrokovno ustvarjalno sodelovanje. Da bi to dosegli, so potrebni določeni specialisti in generalisti ter njihovo medsebojno sodelovanje. Vidiki bodo ustrezni, kadar bodo nastali na podlagi sodelovanja tima različnih specialistov, saj se s tem zmanjša subjektivno dojemanje stvarnosti in tako preprečuje enostranskost. To pomeni, da zadostno in potrebno celovito zaupanje lahko ustvarijo le specialisti, ki delajo interdisciplinarno po postopku USOMID/NOVOST.

Za naše potrebe definiranja zadostnega in potrebno celovitega zaupanja smo uporabili besedilo avtorjev Mulej et al. (2000, glej str. 73) in ga priredili:

Zadostno in potrebno celovito zaupanje *je premislek vsakega posameznika, s katerim se da celovito opredeliti, katero raven celovitega zaupanja velja šteti za primerno.*

Z upoštevanjem zakona zadostne in potrebne celovitosti (Mulej et al., 2008, str. 40), ki opredeljuje celovitost s štirimi sestavinami (*sistematičnost*, *sistemnost*, *dialektičnost*, *materialističnost),* lahko zadostno in potrebno celovito zaupanje opredelimo na naslednji način:

- **Posamično je potrebno obravnavati vsak podsistem sistema zaupanja (*sistematičnost*).** Če bi kateregakoli od podsistemov izpustili ali pa ga ne bi obravnavali, bi se oddaljili od zadostne in potrebne celovitosti. Obravnavati je potrebno njihove značilnosti in podrobnosti, za katere ocenimo, da so potrebne za celovito obravnavo.

- **Zaupanje je potrebno obravnavati kot celoto (*sistemnost*).** Sistem ima drugačne lastnosti kot njegovi podsistemi, saj predstavlja več kot celoto vsote njihovih posamičnih lastnosti. Potrebno je gledati tudi celotno sliko in se ne osredotočati na posamezne dele, sicer lahko zaradi posameznih delov spregledamo, kaj je glavno sporočilo, namen, bistvo celotne slike. Zaupanje je odraz celote, ne zgolj vsote (ne)zaupanja v posamezne podsisteme.
- **Upoštevati je potrebno vse soodvisnosti med podsistemi, ki vplivajo na zaupanje (*dialektičnost*).** Le upoštevanje soodvisnosti lahko pripelje do spoznanja, kako in zakaj posamezno dejanje ali stanje enega podsistema zaradi soodvisnosti vpliva na ostale podsisteme in celotni sistem. To je edini način, ki omogoča, da prepoznamo in obravnavamo nabor odzivov in reakcij, ki nastanejo kot posledica dejanja/spremembe enega podsistema. Sinergijo torej tvori(jo) soodvisnost(i), soodvisnost(i) pa lahko temelji(jo) na zaupanju, nezaupanju ali obojem. Kadar ni zaupanja niti nezaupanja, sinergije ni. Kadar je nezaupanje, je sinergija negativna, in kadar je zaupanje, je sinergija pozitivna. Zato le zaupanje prispeva k pozitivni sinergiji med podsistemi. Pozitivno zaupanje vodi v razvoj in izboljševanje trenutnega zaupanja, hkrati pa k razvoju vseh podsistemov.
- **Pri obravnavanju zaupanja moramo ostati realni (*materialističnost*).** Vsako zatiskanje oči pred stvarnostjo vodi stran od celovitosti, zato je potrebno sprejeti dejstva takšna, kot so – tudi če nekatere stvari niso ali ne bodo v skladu z našimi pričakovanji. Idealističnost vodi v zmoto in napake, ki lahko pripelje do razočaranja in s tem do neupravičenega nezaupanja, ki temelji na napačnih spoznanjih.

Pri razmisleku, katero raven celovitega zaupanja mi, avtorji doktorske disertacije, štejemo za primerno, smo upoštevali, da zadostno in potrebno celovito zaupanje zahteva pravo razmerje med čustvi in razumom ter med zaupanjem in nezaupanjem. Ker je zaupanje odvisno od konteksta in od okoliščin, zadostnega in potrebno celovitega zaupanja na splošno ne moremo konkretno opredeliti, temveč lahko podamo le svoje vidike obravnavanja v obliki okvirnih izhodišč in smernic, kdaj je zaupanje zadostno in potrebno celovito. Ta izhodišča in smernice je mogoče umestiti v posamezne sestavine celovitosti, ki smo jih obravnavali v prejšnjih alinejah:

1) **Zaupanja mora biti več od nezaupanja**. Če je nezaupanja več kot zaupanja, ne moremo govoriti o zaupanju.
2) **Obstajati mora ustrezno razmerje zaupanja in nezaupanja**. Upnik ne sme zaupniku popolnoma oziroma preveč zaupati, saj bi bil s tem izpostavljen morebitni zlorabi zaupanja in spregledu, hkrati pa upnik ne sme zaupniku zaupati nič oziroma premalo, saj bi lahko zaradi dvomov in sumničavosti povzročil škodo predvsem sebi. Ustrezno razmerje v miselnem procesu podzavestno določi upnik glede na kontekst, izbrane vidike obravnave in potrebe.
3) **Obstajati mora ustrezno razmerje čustev (subjektivnih vidikov) in dokazov (objektivnih vidikov)**. Za ustrezno vzpostavitev zaupanja so potrebna čustva in dokazi, njuno ustrezno razmerje pa v miselnem procesu podzavestno določi upnik glede na kontekst in potrebe.
4) **Obstajati mora ustrezno razmerje zaupanja in nadzora**. Nadzor (oziroma sredstva ali izvajalci nadzora) le dopolnjuje(jo) zaupanje in ga ne nadomešča(jo), hkrati pa mora(jo) obstajati zaradi zagotavljanja strukturnih zagotovil in normalnosti situacije, ki povečata upnikovo zaupanje, in ne zaradi sumničavosti ali nezaupanja upnika v zaupnika. Kadar je zaupanja manj, naj ga dopolnjuje nadzor tako, da ohranja raven zaupanja nad nezaupanjem.
5) **Upnik mora zaupati nadzoru.** Če upnik nadzoru ne zaupa, bo zaupniku manj zaupal ali pa mu sploh ne bo zaupal.
6) **Upnik naj si prizadeva pridobiti podatke in informacije, ki temeljijo na zanesljivih in preverjenih podatkih/virih**. Bolj kot bodo podatki/viri zanesljivi in preverjeni, bolj stvarno oceno bo lahko upnik ustvaril o zaupniku. Oceno zanesljivosti in preverjenosti si posameznik ustvari sam, za kar potrebuje znanje, orodja in prave podatke in informacije, poznati pa mora tudi ustrezne postopke presojanja in vrednotenja virov ter podatkov, ki prihajajo iz vira. Zavrača naj uporabo vsakih lažnih, napačnih ali zavajajočih podatkov in informacij – za prepoznavo le-teh je seveda potrebno znanje.
7) **Upnik mora upoštevati tako podatke in informacije, ki mu ustrezajo, se z njimi strinja ali jim je naklonjen, kot tudi tiste, ki mu ne ustrezajo, se z njimi ne strinja ali jim ni naklonjen.** Enostransko in selektivno obravnavanje podatkov in informacij vodi v pristranskost in s tem v enostransko celovitost, zato je ključno upoštevati vse

podatke in informacije, tudi če se z njimi ne strinjamo, nam ne ustrezajo ali pa niso v skladu z našimi pričakovanji.

8) **Upnik mora imeti ustrezno znanje o zaupniku, njegovem in lastnem okolju, tveganjih in nadzoru**. Ustrezno znanje je tisto, ki je preverjeno in temelji na zanesljivih podatkih in informacijah, hkrati pa posamezniku omogoča, da lahko suvereno, objektivno in celovito presodi oziroma oceni ustreznost potencialnega zaupnika ter njegove realne zmožnosti za uresničitev pričakovanj, da mu jasno posreduje svoje želje in da je zaupnika sposoben kritično nadzorovati v okviru uresničevanja pričakovanj.
9) **Upnikova pričakovanja, da bo njegovo zaupanje upravičeno, naj bodo realna**. Upnik mora pravilno in čim manj subjektivno oceniti, ali bo zaupnik sposoben uresničiti pričakovanja, ter vnaprej predvideti, ali bo prišlo do velikega razkoraka med pričakovanji in dejanskim stanjem. Nerealna pričakovanja vodijo v drugačno vedênje upnika in odzive na zaupnikova dejanja, ki lahko v primeru razočaranja (neupravičeno in neutemeljeno) dodatno povečajo nezaupanje. Tudi zaupnik se lahko drugače odzove na upnikovo vedênje, ki izhaja iz nerealnih pričakovanj, kot bi se sicer v primeru realnih pričakovanj.

5.3 Postopek modeliranja celovitega zaupanja državljanov v matične obveščevalno-varnostne službe

Modeliranju splošnega zaupanja državljanov v matične obveščevalno-varnostne službe je sledilo modeliranje celovitega zaupanja državljanov v matične obveščevalno-varnostne službe. S tem smo sledili realizaciji prvega dela drugega cilja doktorske disertacije: opredeliti, pojasniti in podati *smernice za logistiko izdelave* in *aplikacije* modela celovitega zaupanja državljanov v matične obveščevalno varnostne službe.

Model splošnega zaupanja državljanov v matične obveščevalno-varnostne službe smo ob upoštevanju DTS in DOMR združili s konceptom zadostnega in potrebno celovitega zaupanja ter nanj aplicirali MVS. Postopek modeliranja je bil zapleten, saj smo se morali vedno znova opominjati, da mora biti model celovitega zaupanja državljanov v matične

obveščevalno-varnostne službe osredotočen na zaupanje državljanov. Le tako smo lahko ostali znotraj opredeljenega okvirja doktorske disertacije. Proces izgradnje modela celovitega zaupana državljanov v matične obveščevalno-varnostne službe smo zato opravili v več fazah, ki so predstavljene v naslednjih podpoglavjih (izhod, povratna zanka, struktura, procesi, vhod, vplivi), dodali pa smo tudi smernice za delovanje modela. Te besedno prikazujejo, kako naj bi model-sistem deloval v praksi.

Ker je podsistem *Državljan* del podsistema *Laična javnost*, ga v modelu celovitega zaupanja nismo več navajali in obravnavali posamično, podsistem *Laična javnost* pa smo preimenovali v **podsistem *Državljani***. Ta ostaja enak podsistemu *Laična javnost*, ki smo ga obravnavali pri splošnem modelu zaupanja državljanov v matične obveščevalno-varnostne službe, le da je dobil drugačno ime, s katerim smo se približali naslovu doktorske disertacije in našemu subjektu raziskovanja – državljanom.

Modela nismo matematično prikazali, ker nimamo za to ustreznega znanja, zato je nedeterminističen. V nasprotju z matematiko družboslovje ni eksaktna veda, zato spremenljivk v našem modelu nismo mogli ustrezno matematično določiti. Tudi sicer je model v matematiki primer prehajanja od splošnega h konkretnemu, nasprotno pa je model v nematematičnih vedah (npr. družboslovju, op. G. H.) nekaj, kar posplošuje konkretno (Mulej, 1979). Dodatni razlog, zakaj našega modela ne moremo matematično opredeliti, pa je koncept VKEN (Potočan & Mulej, 2006). Zaradi spreminjajočih človeških dejavnikov (posameznik, družba) sestavin modela nismo hierarhično razporedili glede na matematične (številčne) vrednosti, temveč le opisno, besedno. Nenazadnje je med matematičnimi in besednimi modeli pomembna razlika le v »preciznosti izraza o postavkah in odnosih med njimi [tj. besedami ali matematičnimi simboli, op. G. H.]« (McGrath, Nordlie & Vaughan, 1973 v Mulej, 1979, str. 128), zato smo poskušali sestavine modela in povezave med njimi opredeliti zadostno in potrebno celovito. Pri tem smo si pomagali z izbiro najpomembnejših funkcij modela. Kljub temu modeliramo zato, »da bi [mi in drugi raziskovalci, strokovnjaki, op. G. H.] pridobili preglednost, možnost uporabiti matematični izraz in metode obravnavanja, možnost uporabiti statistiko, računalniško obdelavo podatkov, možnost preskusiti verjetno obnašanje pred (običajno zelo drago) uporabo v praksi.« (Mulej, 1979, str. 130)

5.5.1 Izhod in povratna zanka

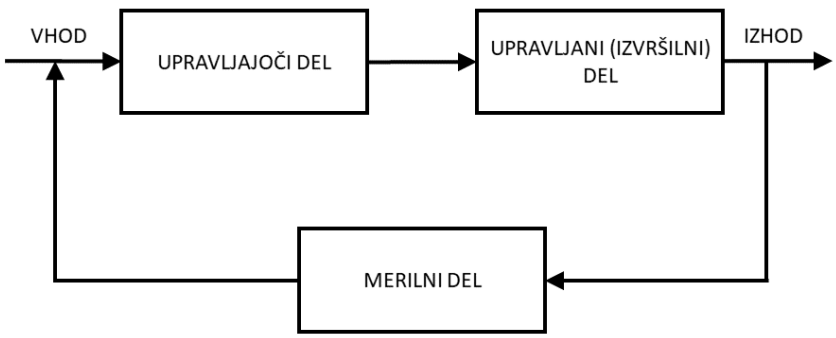
Na začetku drugega modeliranja smo najprej določili izhod. Razlog za takšen postopek je izhodišče našega raziskovanja, da bo izhod iz modela zaupanje s pozitivnim predznakom. Bistvo takšnega izhoda je vzdrževanje zaupanja in njegovo ohranjanje na tolikšni ravni, da ga je več kot nezaupanja. S tem tudi posredno prispeva k učinkovitemu zagotavljanju nacionalne varnosti in uresničevanju nacionalnih interesov preko matičnih obveščevalno-varnostnih služb. Zgolj pozitivno zaupanje kot izhod samo po sebi nima nobenega posebnega učinka na ostale podsisteme in okolje, dokler ostane v posamezniku kot *prepričanje* in se ne manifestira v okolje. V takšnem primeru ima zaupanje učinek oziroma vpliv le na ponovno presojo zaupanja, ko ta nastopi v vlogi vhoda kot trenutno zaupanje. Če ostali podsistemi (*Politika*, *Matična obveščevalno-varnostna služba* idr.) zaradi državljanovega neizkazovanja zaupanja tega ne zaznajo, potem je neupravičeno pričakovati, da bodo podsistemi imeli podatke o državljanovi stopnji zaupanja. Zato je **ključno**, **da se iz zaupanja razvije zaupljivo vedênje**, da podsistemi zaznajo stanje ali spremembo zaupanja. Zaupljivo vedênje se lahko kaže kot izražanje mnenja v javnomnenjskih raziskavah, dajanje pobud za spremembo zakonodaje, aktivno delovanje v interesnih skupinah, sodelovanje s službami, objavljanje prispevkov v medijih idr. Če zaupljivo vedênje ni vidno drugim podsistemom, potem ne bo mogoče vzpostaviti povratne zanke znotraj teh podsistemov in izvesti prilagoditve zaznani stopnji zaupanja državljanov. V jeziku MVS to pomeni, da brez zaupljivega vedênja podsistemi ne morejo zaznati sprememb neposredno iz vira (vendar ne zaradi lastne krivde ali nesposobnosti), zato se ne morejo pravočasno in ustrezno prilagoditi spremembam, saj pridejo do podatkov preko drugih virov in kasneje, ko je prilagajanje tedaj že preteklim spremembam navadno oteženo, omejeno ali nemogoče. Ne trdimo, da se morajo državljani aktivno udejstvovati pri izkazovanju zaupanja, saj ti niso dolžni izražati svojega mnenja. Kljub temu menimo, da lahko z jasnim **izražanjem** zaupljivega vedênja bistveno pripomorejo k zagotavljanju lastne viabilnosti in viabilnosti nacionalnega obveščevalno-varnostnega sistema. Naloga politike, nacionalnega obveščevalno-varnostnega sistema in strokovne javnosti je, da mnenje spremljajo in merijo ter nanj sproti reagirajo, zato jim bo jasno izražanje zaupljivega vedênja v veliko pomoč.

Z odločitvijo za izhod modela-sistema zaupanje s pozitivnim predznakom, smo določili tudi element modela-sistema v središču našega obravnavanja – *Državljani*. Zaupanje, ki predstavlja izhod podsistema *Državljani*, hkrati predstavlja tudi povratno zanko za državljane in za ostale podsisteme. Državljanom služi kot osnova pri procesu presoje zaupanja (*predhodno zaupanje*), medtem ko ostalim sistemom predstavlja stanje o zadovoljstvu državljanov s storitvami, ki jih zanje opravljajo matične obveščevalno-varnostne službe in drugi z njimi povezanimi podsistemi.

5.3.2 Struktura

Strukturo modela-sistema smo morali pripraviti v skladu s smernicami za ustvarjanje zadostnega in potrebno celovitega zaupanja. Predviden vhod v modeliranje je bil vhod v obliki elementarnega kibernetskega sistema (kot sistem z izbranega vidika obvladovanja). Mulej (1979) deli kibernetske sisteme na elementarne in kompleksne; prvih ni mogoče razstaviti na kibernetske sisteme nižjega reda, druge pa sestavlja več elementarnih kibernetskih sistemov z zapletenimi medsebojnimi povezavami. Vsak elementarni sistem vsebuje **upravljajoče** organe, **izvajalne** oziroma **upravljane** (izvršne) organe in **merilne** organe (ibidem), kot to prikazuje slika 5.6. V doktorski disertaciji smo za omenjene organe uporabili izraz *podsistem*.

Slika 5.6: Elementarni kibernetski sistem



Vir: Mulej, 1979, str. 101

Upravljajoči podsistem na podlagi »informacij vhoda in po nekem osnovnem programu, ki ga ima v svojem spominu, aktivira v izvajalnem programu niz aktivnosti,« **upravljani** oziroma **izvršni podsistem** predela »dobljene informacije v konkretne akcije, s katerimi se sistem vključuje v okolje ali vpliva na okolje,« **merilni podsistem** pa »meri aktivnosti izvajalnega organa in ugotovitve sporoča upravljajočemu organu.« (Mulej, 1979, str. 101, 102) Vsi ti trije sistemi delujejo sinergijsko, sicer elementarni sistem najverjetneje ne bi obsta(ja)l. Ker smo želeli (in želimo), da naš predlagani model obstaja in obstane, smo morali v splošnem modelu zaupanja državljanov v matične obveščevalno-varnostne službe prepoznati upravljajoči, upravljani in merilni podsistem. Predhodna analiza splošnega modela zaupanja državljanov v matične obveščevalno-varnostne službe je pokazala, da je njegova struktura kompleksna in precej drugačna od splošnih struktur organizacijskih enot, skupin ali drugih strukturiranih pojavnih ali miselnih slik oziroma sistemov. Ker obstajata dva osrednja subjekta, sta zato tudi dva »centra« modela-sistema. Pojavila se je dilema, ali zaradi te dvojnosti sploh lahko prepoznamo (ali apliciramo) strukturo Mulejevega (1979) elementarnega kibernetskega sistema na splošni model zaupanja državljanov v matične obveščevalno-varnostne službe, saj bi takšen sistem imel na prvi pogled dva podobna elementarna kibernetska sistema. Izkazalo se je, da obstajata **(vsaj) dva paralelna elementarna kibernetska sistema**.

Iskanje razrešitve prepoznanega problema smo pričeli z iskanjem odgovora na vprašanje: »Kateri podsistem analizira trenutno stopnjo zaupanja državljana oziroma državljanov v matične obveščevalno-varnostne službe?« Upravljajoči podsistem skupaj z informacijami vhoda na podlagi lastnih/internih predpisov, določil, programov ali katerega drugega podobnega zapisa določi izvršitelju, kako naj procesira vhod, da bo izoblikoval in v okolje posredoval izhod/zaupanje (pozitivno ali negativno), medtem ko merilni podsistem kvantitativno ali kvantitativno meri izhod/zaupanje. V osnovnem modelu zaupanja je upravljajoči tisti podsistem, ki **analizira** podatke **o *stanju sistema*** (o njegovi strukturi, organizaciji ali delovanju) **in hkrati** podatke o tem, **koliko in kakšno zaupanje *ustvarja*** trenutno stanje sistema (informacije dobi od merilnega podsistema). Brez podatkov o stanju sistema bi težko vedeli, zakaj sistem ustvarja takšno (ne)zaupanje, brez podatkov o količini in vrsti zaupanja pa ne bi vedeli, ali ustvarja zaupanje ali nezaupanje in koliko tega ustvarja. Odgovor na prej zastavljeno vprašanje, kateri podsistem analizira trenutno

stopnjo zaupanja državljana oziroma državljanov v matične obveščevalno-varnostne službe, bi moral biti *Državljan*, *Politika* in *Nacionalni obveščevalno-varnostni sistem* (vključno s podrejenimi službami). Predvsem slednji podsistem je tisti, **ki bi ga *moralo* zanimati, kakšno je trenutno stanje zaupanja**, saj so mu državljani zaupali pomembno nalogo – da bo namesto njih opravil določene naloge in s tem izpolnil njihova pričakovanja, po drugi strani pa je nacionalni obveščevalno-varnostni podsistem na podlagi »družbene pogodbe« preko matičnih obveščevalno-varnostnih služb dolžan izvajati del nalog, ki jih za državljane opravlja država. To ne pomeni, da državljan ne potrebuje podatkov o stanju sistema in o tem, koliko zaupanja ustvarja – ravno nasprotno. Državljan jih nujno potrebuje, saj je tudi od teh podatkov odvisno, v katero smer se bo spremenil rezultat državljanove presoje zaupanja kot izhod podsistema *Državljan*, vendar so ti podatki zaradi zagotavljanja servisa državljanom bolj pomembni za državo oziroma nacionalni obveščevalno-varnostni sistem in njemu podrejene službe.

Naslednje vprašanje, ki smo si ga zastavili, se je glasilo: »Kateri podsistem odredi akcijo oziroma odziv glede na pridobljene podatke?« Izvajalni (izvršilni) podsistem se odzove na informacijo o trenutnem stanju sistema in **se odzove z ustrezno akcijo**, bodisi s povečanjem ali z zmanjšanjem zaupanja ali pa stanja sploh ne spremeni. Poleg spremembe/ohranjanja stopnje zaupanja se lahko kaže – ali pa ne –tudi **(ne)zaupljivo vedênje** (odraz ali *materializacija* zaupanja), ki izhaja iz akcije, odziva. Po našem prepričanju ni le podsistem *Državljan* tisti, ki se navadno odzove na informacije, temveč **bi se morali** na informacije o trenutnem stanju sistema in ostale podatke in informacije **odzvati tudi drugi podsistemi**. Medtem ko se državljan na to odzove z (ne)zaupanjem oziroma z (ne)zaupljivim vedênjem, se drugi podsistemi odzovejo z akcijo, ki poveča ali zmanjša oziroma na določen način vpliva na zaupanje ali pa tudi ne. Odziv pa je odvisen od vrste, pomembnosti in teže pridobljenih podatkov in informacij, zato bi bilo neustrezno posploševati, kakšen bi ta moral biti.

Merilni podsistem elementarnega kibernetskega sistema mora biti v modelu celovitega zaupanja tisti podsistem, ki **zazna novo stanje**, izhajajoče iz izvedenih akcij, **ali nespremenjeno stanje**, informacijo o tem pa mora posredovati v upravljalni podsistem. Za merilni podsistem bi ravno tako lahko rekli, da ga predstavljata del podsistema

Državljan ter *Izvajalci nadzora*, *Strokovna javnost* in v določeni meri nekateri podsistemi nacionalnega obveščevalno-varnostnega sistema. Vsi ti podsistemi imajo nalogo, da prenesejo informacijo o akcijah izvajalnih organov do upravljajočega dela. S tem mu dajo vedeti, kakšne akcije so izvedli izvajalni podsistemi glede na informacijo, pridobljeno ali od državljana/državljanov ali od drugih podsistemov iz paralelnega elementarnega kibernetskega sistema. Posebno vlogo pri tem imajo po našem prepričanju mediji, ki bi morali skrbeti (oziroma naj bi skrbeli) za hitrost, natančnost in vpliv teh informacij, razlog za to pa smo obrazložili v podpoglavju o podsistemu *Mediji*. Merilni podsistem z določenega vidika obravnavanja predstavljajo tudi tuje obveščevalno-varnostne službe, ki zagotovo spremljajo (tudi) odnos javnosti oziroma državljanov do matičnih obveščevalno-varnostnih služb, vendar so z našega vidika obravnave del okolja in posebnih sistemov, zato jih ne smemo obravnavati enako kot del istega (matičnega) elementarnega kibernetskega sistema.

Prepoznana paralelna elementarna kibernetska sistema bi morala biti soodvisna in tvoriti določene sinergije, **ki ustvarjajo zadostno in potrebno celovito zaupanje**, zato je bilo potrebno njuno delovanje preoblikovati v sinergijsko sodelovanje, kar bi zagotovili z izgradnjo modela kibernetskega sistema celovitega zaupanja državljanov v matične obveščevalno-varnostne službe. Ker mora biti v skladu s konceptom zadostnega in potrebno celovitega zaupanja več zaupanja kot nezaupanja, je ključno, da je izhod pozitiven, vendar model-sistem s tem ne sme popolnoma odpraviti nezaupanja, saj bi s tem nastalo »slepo zaupanje«. Kljub temu smo z upoštevanjem DTS in DOMR ter nejasno opredeljenih in spreminjajočih se dejavnikov okolja želeli zagotoviti, da bo izhod iz modela celovitega zaupanja državljanov v matične obveščevalno-varnostne službe zaupanje s pozitivnim predznakom (večje zaupanje).

Pred nadaljevanjem smo si namesto vprašanja »Zakaj *morajo* državljani zaupati matičnim obveščevalno-varnostnim službam?« zastavili vprašanje »Zakaj državljani *potrebujejo* matične obveščevalno-varnostne službe?« Pri iskanju odgovora smo bili osredotočeni na skrito ozadje – soodvisnost in pozitivno sinergijo med tema dvema elementarnima kibernetskima sistemoma. Preprost odgovor, do katerega smo prišli in čigar bistvo najdemo v tem, kar je osrednji del DOMR (glej poudarjeno in primerjaj z Rosi

& Rosi, 2011), se glasi: Državljani **potrebujejo** te službe, ker državljani **nimajo pravih *znanj, vednosti, talentov, vrednot, čustev in možnosti*,** da bi zmogli opravljati naloge, ki jih opravljajo matične obveščevalno-varnostne službe. V tem odgovoru se po našem prepričanju skriva tudi odgovor, zakaj državljani *morajo* zaupati tovrstnim službam:

*Ker jim zaradi pomanjkanja znanj, vednosti, talentov, vrednot, čustev in možnosti **ne preostane nič drugega, kot da izvajanje nalog prepustijo oziroma zaupajo službam, ki so temu kos**, saj če tega državljani ne bi storili, bi bili kot družba in kot posamezniki **podvrženi pospešeni entropiji**.*

Zaupanje ne sme biti razumljeno kot prepričanje, da je državljan kot upnik nemočen in šibek, temveč da ima kljub položaju možnost, da zaščiti lastne interese in potrebo po varnosti. Zadostno in potrebno celovito zaupanje prinaša korist tudi zaupniku, saj mu daje določeno priznanje (povečevanje ugleda in dobrega imena), da je ustrezen subjekt za izpolnitev pričakovanj, in mu daje potrebno podporo za izvajanje nalog, hkrati pa ga omejuje pri morebitni prekoračitvi »pooblastil«, ki mu jih je dal upnik. Ker je okolje preveč kompleksno, da bi bili državljani sposobni sami preživeti v njem (Rosi, 2019, osebni vir), morajo izpolnitev pričakovanj (oziroma te naloge) nase prevzeti službe. S tem se prenese del zagotavljanja in vzdrževanja **samo-preživetja** oziroma **viabilnosti** državljanov z njih na matične obveščevalno-varnostne službe. Model-sistem, za katerega želimo, da **preživi** v realnem okolju, je potrebno modelirati tako, da »se zmore *prilagajati spremenljivim* okoliščinam,« (Mulej et al., 2000, str. 369) zato smo pri modeliranju celovitega zaupanja državljanov v matične obveščevalno-varnostne službe uporabili Beerovo različico teorije viabilnih sistemov (TVS) (Beer, 1984).

TVS je sicer splošen izraz za teorijo, ki preučuje viabilne sisteme, s katero se je poleg Stafforda Beera intenzivno ukvarjal tudi Eric Schwarz. Zato moramo poudariti, da v doktorski disertaciji izraz TVS uporabljamo za organizacijsko *teorijo*, ki jo je razvil Stafford Beer. V okviru te teorije je isti avtor razvil *model* viabilnih sistemov (MVS). Tudi Mulej et al. (2000) v svojem delu ločijo teorijo viabilnega sistema od modela viabilnega sistema. Temelja raziskovanja in oblikovanja viabilnih sistemov oziroma definiranja viabilnosti kot

lastnosti sistemov predstavljata Beerovi knjigi *Brain of the Firm* (1972) in *The Heart of Enterprise* (1979).

Sistemi so viabilni, kadar so sposobni neodvisnega obstoja (Beer, 1984), zagotavljanja svojega preživetje (Schwaninger, 2006 a) in soočanja z notranjo in zunanjo raznolikostjo (Leonard, 2008). Viabilnost sistema odraža sposobnost vzdrževanja ravnovesja med spremembo in kontrolo – če je sistem viabilen, se bo v kratkem roku prilagodil okolju, vendar bo hkrati ohranjal tudi dolgoročno vključenost v okolje (MacGregor Adams, 2011). To izhaja iz principa viabilnosti, ki pravi, da je za viabilne sistem potrebno vzdrževati ravnovesje med avtonomijo in integracijo podsistemov ter med stabilnostjo in prilagajanjem (Beer, 1979, 1981 v MacGregor Adams, 2011, str. 133). Vzpostavljanje in ohranjanje takšnega ravnovesja je seveda kompleksna naloga. Viabilni sistem mora imeti **potencial** za odzivanje na nepredvidljive, nepričakovane ali nove dogodke, pojave, okoliščine (Mulej et al., 2000). To pomeni, da mora biti pripravljen na več različnih stanj in dogodkov, ki lahko pripeljejo do takšnih stanj. Če ni pripravljen, se najverjetneje ne bo ustrezno odzval na določen dogodek ali stanje, posledično pa sistem ne bo oziroma ni sposoben zagotavljati svojega preživetja. Zato je **prilagodljivost** oziroma **sposobnost odzivanja na znane in neznane dogodke** ključni atribut viabilnih sistemov (Espejo & Reyes, 2011). Na viabilnost močno vpliva princip **raznolikosti**, tj. število različnih elementov v odnosu do skupka znanih oziroma določljivih elementov (Ashby, 1957, str. 126). Beer (1981, str. 403; 1984, str. 10) opredeljuje raznolikost kot število vseh možnih stanj elementov sistema. Sistem ima lahko več dimenzij, vsaka dimenzija pa ima lahko več različnih možnih stanj, zato je raznolikost drugačna že v vsaki od teh dimenzij (Godsiff, 2010, str. 95). Del sistema, ki je odgovoren za odzivanje, mora prepoznati ta stanja in se nanje odzvati, če želi doseči sprejemljiv rezultat in ohraniti viabilnost sistema (ibidem). Na podlagi tega je nastal Ashbyev **zakon zadostne in potrebne celovitosti**, ki pravi, da »lahko raznolikost uniči raznolikost.« (Ashby, 1957, str. 207) To velja v primeru, ko »ima ''obvladovalec'' potrebno in zadostno raznolikost – to je sposobnost vzdrževati izide nekega položaja znotraj zaželenih okvirov (množice ciljev), če (in samo če!) ima sposobnost *proizvesti odzive na vse motnje*, ki bi se utegnile pojaviti in spraviti njegove izide izven ciljne množice.« (Mulej et al., 2000, str. 369) V jeziku vsakodnevnega življenja to pomeni, da več kot imamo znanja o možnih različnih stanjih, ki se nam ali npr. naši

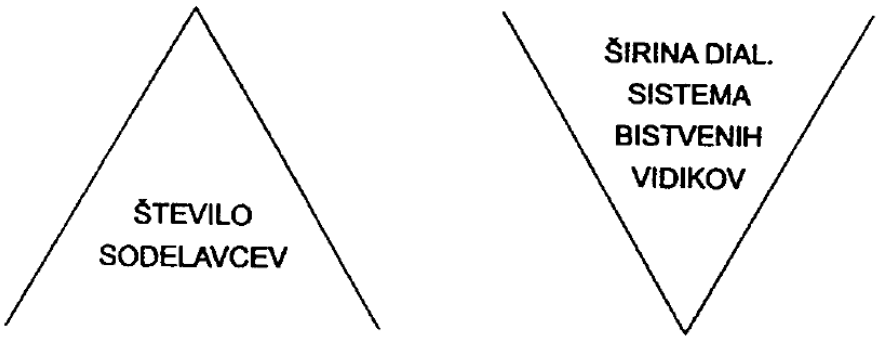
organizaciji lahko zgodijo, ter kompetenc, orodij in metod, da se nanje odzovemo, bolj ustrezno se lahko na ta stanja pripravimo in odzovemo – to še posebej velja za nenavadne, nevsakdanje, urgentne in krizne situacije. Praktičen primer: če se zavedamo in pridobimo znanje, kje, na kakšen način, kdaj in zakaj lahko v našem domu pride do požara, bomo imeli več različnih možnosti (metode, orodja), da se na morebitni pojav požara pripravimo in nanj ustrezno reagiramo. Tudi v tem primeru lahko vidimo, kako z raznolikostjo (več različnih metod in orodij za preprečevanje in gašenje požara ter izogibanje in zmanjševanje njegovih posledic) uničimo raznolikost (različni načini in razsežnosti požara idr.), da bi **ohranili lastno viabilnost** (zdravje, življenje). Sistem, ki je oziroma naj bi bil viabilen, mora zato težiti k ohranjanju lastne viabilnosti s čim večjo, predvsem pa zadostno in potrebno raznolikostjo.

TVS med drugim tudi zagotavlja sistemski vpogled v strukturo organizacije (Hawrood, 2012), tj. njene elemente in odnose med njimi (soodvisnosti, hierarhijo, komunikacijo itd.). Kot pravi Jackson (2009, str. S28), je MVS preprost način prikaza, kako kibernetski zakoni in načela podpirajo delovanje kompleksnih sistemov. »[M]enedžerjem in njihovim svetovalcem [omogoča], da izdelajo politiko in razvijejo organizacijske strukture v jasnem razumevanju rekurzij, v katerih naj bi delovali, in da oblikujejo regulativni sistem v okviru tistih rekurzij,« ki upoštevajo »temeljne kanone kibernetike.« (Beer, 1984, str. 17) Kaj je rekurzija, pojasnjujemo nekoliko kasneje. Neustrezna struktura namreč ne omogoča učinkovitega prilagajanja navzven in navznoter, ravno nasprotno – otežuje ali celo onemogoča pridobivanje vseh potrebnih podatkov in informacij iz okolja ter njihovo uporabo za namene delovanja in preživetja sistema. S tem določa tudi uspeh ali neuspeh organizacij, ki ga Beer prepozna kot funkcijo njihove sposobnosti soočati se z okoljem, zunanjim svetom in njihovimi uporabniki (Pickering, 2002). Pickering (ibidem, str. 7) dodaja, da je oblikovanje informacijskih tokov tisti dejavnik, ki odloča, kako hitro se organizacija sooča z dogajanjem v svojem okolju in svetu.

Menedžment organizacije je tisti, ki odreja, usmerja, koordinira in spremlja delovanje organizacije. Ta je odvisen od podatkov in informacij, ki prihajajo od spodaj navzgor. Obenem organizacijska in ukazovalna hierarhija potekata od zgoraj navzdol (Mulej et al., 2008). Slika 5.7 prikazuje, da je zaradi velikega števila prejetih podatkov in informacij

širina bistvenih vidikov pri vrhu organizacije večja. Kljub temu je »*raznolikost managementa* […] mnogo *nižja* od raznolikosti organizacije kot celote,« (Mulej et al., 2000, str. 371) saj je število stanj, ki jih zaznavajo preostali deli organizacije, bistveno večje od števila stanj, ki jih zaznava menedžment. Izenačitev raznolikosti v praksi normalno ni izvedljiva (ibidem, str. 374), vendar si mora menedžment prizadevati, da bi se njegova raznolikost menedžmenta približala raznolikosti preostale oziroma celotne organizacije, saj bi tako lažje vplival na okolje oziroma na organizacijo glede na spremembe v okolju. Beer je to v svojih delih poskušal doseči z **ojačevalci** in **blažilci** v strukturah MVS, ki bi uravnali število in pretok podatkov in informacij med organizacijskimi enotami. Prvi povečajo vpliv menedžmenta na okolje, drugi pa zmanjšajo vplive iz okolja (Mulej et al., 2000, str. 373). Blažilci menedžmentu omogočijo, da pridobi zgolj bistveno, a kljub temu realno sliko o okolju, brez odvečnih informacij in drugega nepotrebnega »balasta«.

Slika 5.7: Širina števila udeležencev in širine sistema vidikov



Vir: Mulej et al., 2008, str. 69

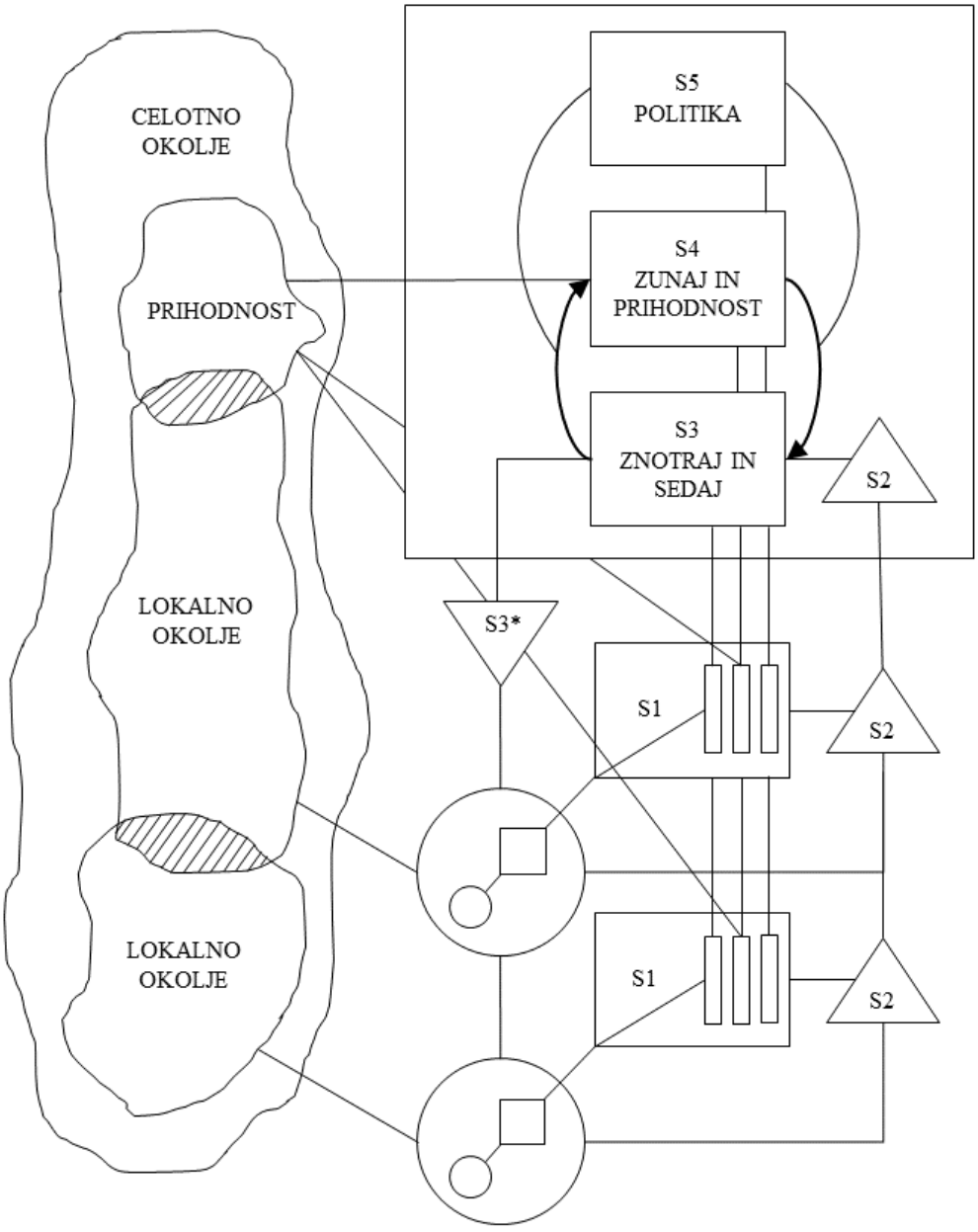
DTS upošteva razlike med menedžmentom in organizacijo v raznolikosti, zato tisto, čemur Mulej pravi »bistveni vidiki«, z določenega vidika obravnavanja predstavlja splet in sinergijo vseh različnih, vendar pomembnih in bistvenih vidikov o organizaciji in okolju potrebnih za odločanje, do katerih menedžment pride preko blažilcev. Z ojačevalci pa lahko doseže, da se ukazi in naloge, ki jih delegirajo in ki temeljijo na prejetih podatkih in informacijah, vrnejo po hierarhiji navzdol in nato v ojačani obliki v okolje.

To brez ustrezne strukture organizacije ni mogoče, zato je Beer predlagal posebno strukturo sistema, ki zagotavlja viabilnost – MVS (slika 5.8). Ta je sestavljen iz petih podsistemov, brez katerih ne more biti viabilen (Beer, 1984), vsak pa predstavlja ključno funkcijo za preživetje: implementacija (Sistem 1 – S1), koordinacija (Sistem 2 – S2), nadzor (Sistem 3 – S3 in Sistem S3* – S3*), razvoj (Sistem 4 – S4) in politika (Sistem – S5) (Espejo & Gill, 1997). Vloge teh podsistemov so:

- **Sistem 1 (S1)**: upravljanje osnovnega podsistema (Schwaninger, 2006 a). S1 predstavlja operativne enote (Hildbrand & Bodhanya, 2015) ali operativne funkcije in deluje v okolju, hkrati pa se mu tudi prilagaja. Pri svojem delovanju je avtonomen, vendar deluje v skladu s smernicami/pravili S5 ter usmeritvami S3.
- **Sistem 2 (S2)**: koordinacija podsistemov, zmanjševanje nihanj (oscilacij) med njimi (Schwaninger, 2006 a). S2 je zadolžen za nemoteno delovanje sistema (Hildbrand & Bodhanya, 2015). V resničnem življenju ga najdemo v obliki informacijskih sistemov, operativnih načrtov, urnikov, skupin, internih enot za storitve in podporo, standardov vedênja, baz znanja (Schwaninger & Scheef, 2016). Preko njega poteka komunikacija med S1 in S3.
- **Sistem 3 (S3)**: operativno upravljanje kolektivnih podsistemov (Schwaninger, 2006 a). S3 je torej zadolžen za upravljanje operativnih enot (S1). Njegove naloge so vzpostavitev splošnega optimalnega razmerja med osnovnimi enotami (S1), zagotavljanje sinergij in dodeljevanje sredstev osnovnih enotam (Schwaninger & Pérez Ríos, 2008). Deluje po principu »tu in sedaj« oziroma »znotraj in sedaj«, osnovnim enotam pa določa cilje, se z njimi pogaja o sredstvih in od njih terja določeno mero odgovornosti (Pérez Ríos, 2012).
- **Sistem 3* (S3*)**: kanal za kontrolo in spremljanje (Schwaninger, 2006 a), ki povezuje S3 in S1 ter analizira informacije, ki potekajo na relaciji S1-2-3 (Schwaninger & Pérez Ríos, 2008). S3 preko S3* pridobiva informacije, ali S1 dobiva ukaze in naloge preko S2 in ali jih razume, hkrati pa S3* služi kot alternativni vir za preverjanje informacij, ki potekajo iz S1 v S3 (Mulej et al., 2000). S3 lahko z njim nagradi ali sankcionira S1 ter s tem uravnava ustreznost delovanja S1. Kot pravi Pérez Ríos (2012, str. 113), služi S3* kot alarm, ki obvesti S3 o neustreznosti delovanja S1. Kadar S3 ne reši ali ne more rešiti teh težav in je ta alarm še vedno aktiviran, gre informacija o tem

naravnost do S5, ki mora nato rešiti problem – to naj bi se zgodilo v izjemnih, redkih primerih (ibidem).

Slika 5.8: Struktura MVS



Vir: Prilagojeno po Beer, 1984, str. 15

- **Sistem 4 (S4)**: dolgoročno upravljanje, odnos do okolja (Schwaninger, 2006 a). V nasprotju s podsistemom S3 je S4 usmerjen v prihodnost, zato ima strateškoanalitično funkcijo viabilnega sistema. Raziskuje potencialne priložnosti za delovanje (npr. strateško upravljanje, raziskave in razvoj, ustvarjanje novih

zmogljivosti, znanja) (Schwaninger & Scheef, 2016). S4 je ključen za viabilnost sistema oziroma njegovo prilagajanje spremembam, ki so povezane z okoljem (Hildbrand & Bodhanya, 2015), saj se osredotoča na vrsto stanj, s katerimi bi se sistem lahko srečal/soočil v prihodnosti. Do teh stanj pride s pridobivanjem podatkov iz okolja, ki jih preoblikuje v informacije, potrebne za odločitve in (re)akcije ter prilagajanje notranjega okolja zunanjemu.

- **Sistem 5 (S5)**: normativno upravljanje, korporativni etos (Schwaninger, 2006 a), glavna avtoriteta sistema (Pérez Ríos, 2012). Njegova naloga je ohranjati ravnotežje med sedanjostjo (S3) in prihodnostjo (S4), med notranjo (S3) in zunanjo usmerjenostjo (S4); skrbi za moderiranje in skladnost interakcij med S3 in S4 (Schwaninger & Pérez Ríos, 2008). Predstavlja najvišje vrednote, norme in pravila sistema (ibidem), zato »pooseblja« identiteto sistema ter s tem predstavlja njegovo »dušo« (Brocklesby & Cummings, 1996).

S1, S2 in S3 (ter S3*) skupaj predstavljajo **operativni menedžment** sistema (Schwaninger, 2006 a). Nekateri pomembni odnosi med temi podsistemi vključujejo pogajanja o ciljih in virih, odgovornost, upravljanje s cilji, nadzor nad finančnimi sredstvi, interveniranje (Schwaninger & Scheef, 2016). S3 ima pomembno vlogo še v eni drugi funkciji. Skupaj s podsistemom S4 namreč tvori »**homeostat** [poudaril G. H.], tj. telo vzajemne prilagoditve, ki si prizadeva za stabilnost viabilnega sistema« (ibidem, str. 5). Homeostat označimo s S3-4. S3 pokriva področje znotraj sistema in trenutno stanje sistema, S4 pa področje zunaj sistema in stanje v prihodnosti. Združevanje teh dveh vidikov omogoča, da se sistem glede na trenutno stanje ustrezno prilagodi verjetnemu (!) okolju v bližnji ali daljni prihodnosti. Brez informacije o prihodnosti je prilagajanje neznanemu lahko potratno s časovnega, finančnega, kadrovskega, materialnega ali katerega drugega vidika, saj upravljalec sistema ne ve, čemu in kako naj se prilagodi. Enako si upravljalec sistema ne more pomagati pri prilagajanju sistema, če ima informacijo o prihodnosti, nima pa vpogleda v trenutno stanje sistema. Zato pravimo, da je prilagajanje sistema možno le s homeostatom S3-4, ki zajema obe področji: znotraj in sedaj (S3) ter zunaj in v prihodnosti (S4). Schwaninger & Scheef (2016) namreč pravita, da če sistem ni viabilen oziroma ni v skladu s TVS, potem nima povezave med S3 in S4. Če sistem nima

homeostata, ne more biti stabilen (ibidem) niti viabilen. Sistem, ki ni viabilen, pa je, kot že rečeno, podvržen hitrejši entropiji.

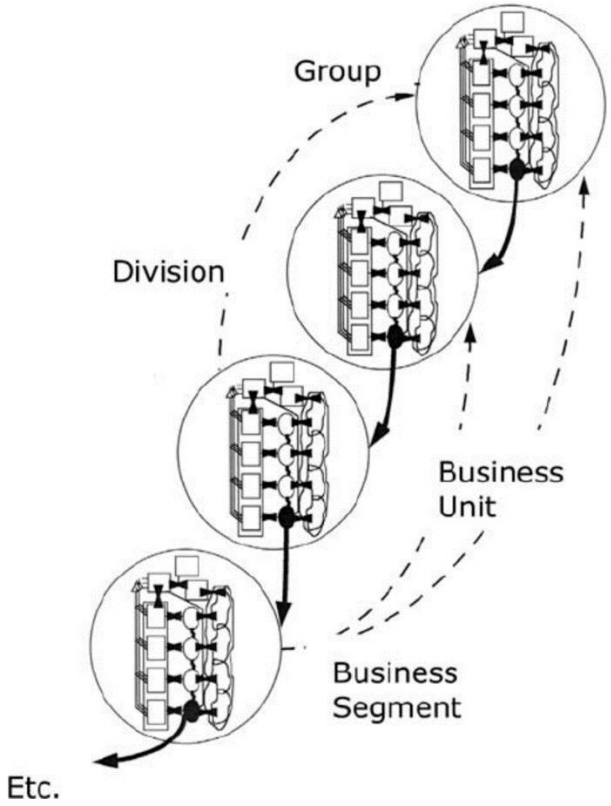
Pri tem je podsistem S5 izredno pomemben, saj skrbi za ublažitev medsebojnih interakcij in informacij podsistemov S3 in S4, ki predstavljata diametralno nasprotni si funkciji (S3 – kratkoročne, S4 – dolgoročne). Zaradi tega S5 spominja na koordinatorja, ki spremlja in uravnava delovanje homeostata S3-4. Brez S5 sistem težko išče in vzdržuje ustrezno ravnovesje med podatki in informacijami o sedanjem ter prihodnjem stanju. Ker S5 določa in ponotranja vrednote, norme in pravila sistema, ima najboljši pregled nad tremi različnimi stanji sistema: v kakšnem stanju *je* sistem (te informacije zagotavlja S3), v kakšnem stanju *je lahko oziroma bi moral biti* sistem glede na stanje v okolju (te informacije zagotavlja S4) in v kakšnem stanju ***bi moral biti*** **sistem glede na njegovo poslanstvo**. Slednje dovolj dobro pozna le S5, ki ve, s kakšnim namenom je bil sistem ustvarjen, zakaj deluje, h kateremu cilju prispeva in kako pripomore k uresničevanju poslanstva sistema na višji ravni rekurzije, katerega podsistem je S5 skupaj s S3 in S4.

Vračamo se k izrazu ***rekurzija***, ki je bil omenjen v enem od prejšnjih odstavkov. Ta izhaja iz besede *rekurz* oziroma latinskega izraza *recurrere*, kar pomeni *teči nazaj*, beseda *rekurzivno* pa »nanašajoče na samega sebe« (Novak, b. d.). Rekurzija je pravzaprav ponavljanje lastnosti strukture viabilnega sistema (Mulej et al., 2000), pri čemer določen podsistem nastopa kot S1 sistema višjega reda, hkrati pa je z določenega vidika obravnavanja tudi sam sistem, ki ga sestavljajo podsistemi na nižji ravni hierarhije. Tako sistem S3-4-5 predstavlja metasistem, ki je hkrati S1 na višji ravni rekurzije. Za lažje razumevanje principa rekurzije bralcem predlagamo, naj najprej pogledajo štirikotnik na sliki 5.8, v katerem so S3, S4 in S5, nato pa S1 (štirikotnik), znotraj katerega so trije manjši pokončni pravokotniki (ti predstavljajo S3, S4 in S5 na nižji ravni rekurzije). Slika 5.9 prikazuje enako, le da je posplošena za namene lažjega prikaza in razumevanja rekurzije.

Rekurzijo lahko najdemo na vseh ravneh izbranega viabilnega sistema. Vsak del oziroma enota viabilnega sistema je z določenega vidika obravnavanja kopija celote, v katero je vgrajena, saj ima vse funkcije za obvladovanje procesov, za katere obstaja določen namen (Schwaninger, 2006 b). Zato Beer (1984, str. 14) pravi, da je S1 vedno viabilni

sistem. Rekurzija podsistemov in njihovih odnosov je ena od temeljnih značilnosti Beerove TVS in njegovega MVS. Vsak viabilni sistem je namreč del več kot enega sklopa rekurzivnih odnosov (Leonard, 2000), kar kaže na to, da vsi podsistemi izpolnjujejo ista načela (Schwaninger, 2006 a).

Slika 5.9: Struktura z nekaj ravnmi rekurzije



Vir: Schwaninger, 2006 a, str. 961

S tem zaključujemo zelo kratek povzetek in predstavitev TVS in MVS, saj ocenjujemo, da bo to bralcem zadostovalo za okvirno pojasnjevanje bistva povezav med preživetjem sistema, viabilnostjo, raznolikostjo, kompleksnostjo, strukturo, organizacijo, prilagajanjem in delovanjem (notranjega okolja) sistema. Vse to se navezuje tako na področje obveščevalno-varnostne dejavnosti, ki predstavlja vsebinsko plat modela celovitega zaupanja državljanov v matične obveščevalno-varnostne službe, kot na strukturo in delovanje modela z vidika izbranih sistemskih teorij. Ključno je, da bralci doktorske disertacije razumejo ozadje našega razmišljanja: določenemu (pod)sistemu ni treba prevzeti vse kompleksnosti nase, temveč jo lahko v celoti ali delno prevzamejo drugi (pod)sistemi, kadar in če je to mogoče oziroma dopustno in če s tem ne ogrozi

lastne viabilnosti. V kontekstu izbranega problema doktorske disertacije državljani ne prevzemajo kompleksnosti varnostnega okolja v celoti, temveč večji del te kompleksnosti na podlagi »družbene pogodbe« nase prevzemajo organi sistema nacionalne varnosti. To je tudi razlog, zakaj smo za strukturiranje uporabili tudi MVS.

MVS namreč nismo aplicirali na celotni model splošnega zaupanja državljanov v matične obveščevalno-varnostne službe, temveč le na nacionalni obveščevalno-varnostni sistem in matične obveščevalno-varnostne službe kot rekurzijo nižjega reda. MVS je pomemben za **zagotavljanje viabilnosti nacionalnega obveščevalno-varnostnega sistema in njegovih podsistemov** (med drugim tudi matičnih obveščevalno-varnostnih služb) **ter s tem viabilnosti državljanov**, ki so večji del svoje kompleksnosti prenesli na državo, zato bi lahko zaradi aplikacije MVS **posredno vzdrževali viabilnost podsistema *Državljan***. Nacionalni obveščevalno-varnostni sistem se mora odzivati na spremembe zunanjega in notranjega okolja (varnostne grožnje, incidenti in pojavi na nacionalni, regionalni in globalni ravni, stopnja globalizacije, spremembe in dogodki v ekonomiji, gospodarstvu, kulturi, mednarodni politiki idr.), če želi uresničevati svojo nalogo pri zaščiti in uresničevanju nacionalnih interesov, med katere spada tudi nacionalna varnost.

Glede na izbrane vidike obravnave in izbrani osrednji problem doktorske disertacije dajemo v kontekstu ohranjanja viabilnosti nacionalnega obveščevalno-varnostnega sistema in njegovih služb/podsistemov večji poudarek *zaupanju* kot dejavniku okolja nacionalnega obveščevalno-varnostnega sistema in zato manjši poudarek drugim dejavnikom. V literaturi, medijih in javnosti nismo zasledili stališča, da se **mora** nacionalni obveščevalno-varnostni sistem **odzvati** tudi na **stopnjo zaupanja in vsako spremembo zaupanja državljanov**, vendar se nam to zdi pomembno. Schreier (2005, str. 147) namreč pravi: »Izgradnja zaupanja je stvar, ki zahteva veliko več pozornosti, saj je zaupanje javnosti ključno za vsako uspešno zasnovo delujočih in odgovornih obveščevalno-varnostnih služb v demokratični družbi.« Ugotavljamo, da zaupanje odraža prepričanje državljanov v obliki misli, besed ali dejanj, ki imajo potencial, da posredno ali neposredno vplivajo na delovanje matičnih obveščevalno-varnostnih služb in nacionalnega obveščevalno-varnostnega sistema. Neupoštevanje stopnje zaupanja lahko vodi do negativnih posledic, ki bi se najbolj odražale pri kreiranju informacij za odločevalce, saj

bi te sčasoma postale skromne, pomanjkljive, netočne ali napačne. Posledično bi bile sprejete neustrezne odločitve, ki bi lahko bile tudi v neskladju z nacionalnimi interesi. Čeprav ne moremo trditi, da ima neupoštevanje spremembe ali dejavnika okolja, kot je npr. pojav nove teroristične organizacije, enake posledice kot neupoštevanje stopnje zaupanja državljanov v matične obveščevalno-varnostne službe, hkrati tudi ne moremo trditi, da je neupoštevanje stopnje zaupanja glede na potencialne posledice manj pomembno od neupoštevanja pojava nove teroristične organizacije.

Matična obveščevalno-varnostna služba ima z vidika nacionalnega obveščevalno-varnostnega sistema kot viabilnega sistema vlogo subjekta, ki prvi pride v stik z okoljem in subjekti iz okolja (S1). Državljani so del okolja nacionalnega obveščevalno-varnostnega sistema, zato imajo prav oni prvi stik s tem sistemom preko njegovih operativnih enot, tj. matičnih obveščevalno-varnostnih služb. V 3. poglavju doktorske disertacije smo pojasnili, da sta institucionalno in medosebno zaupanje tesno povezana, zato lahko nezaupanje določeni osebi vpliva na nezaupanje organizaciji, katere del je ta oseba. Če uporabimo analogijo: nezaupanje v S1 negativno vpliva na zaupanje v metasistem S3-4-5 in organizacijo v celoti. Za ohranjanje viabilnosti sistema in njegovih podsistemov je nujno sodelovanje vseh podsistemov (ob hkratnem zagotavljanju avtonomije vseh S1), zato je ob nezaupanju v en podsistem potrebno odzivanje celotnega sistema – takšno je namreč delovanje sistema v skladu s TVS in MVS, ki zagotavlja viabilnost sistema. Vendar če se sistem odzove na spremembo zaupanja, da ostane viabilen, zaupanje državljanov pa ostane nizko ali pa ga (več) ni, bo sistem izgubil potrebno podporo državljanov, njegova entropija pa bo zato hitrejša. Zato je pomembno, da je njegovo delovanje in prilagajanje takšno, da poleg lastne viabilnosti ohranja tudi zaupanje. Od tod smo izpeljali:

ohranjanje viabilnosti nacionalnega obveščevalno-varnostnega sistema in obveščevalno-varnostnih služb

=

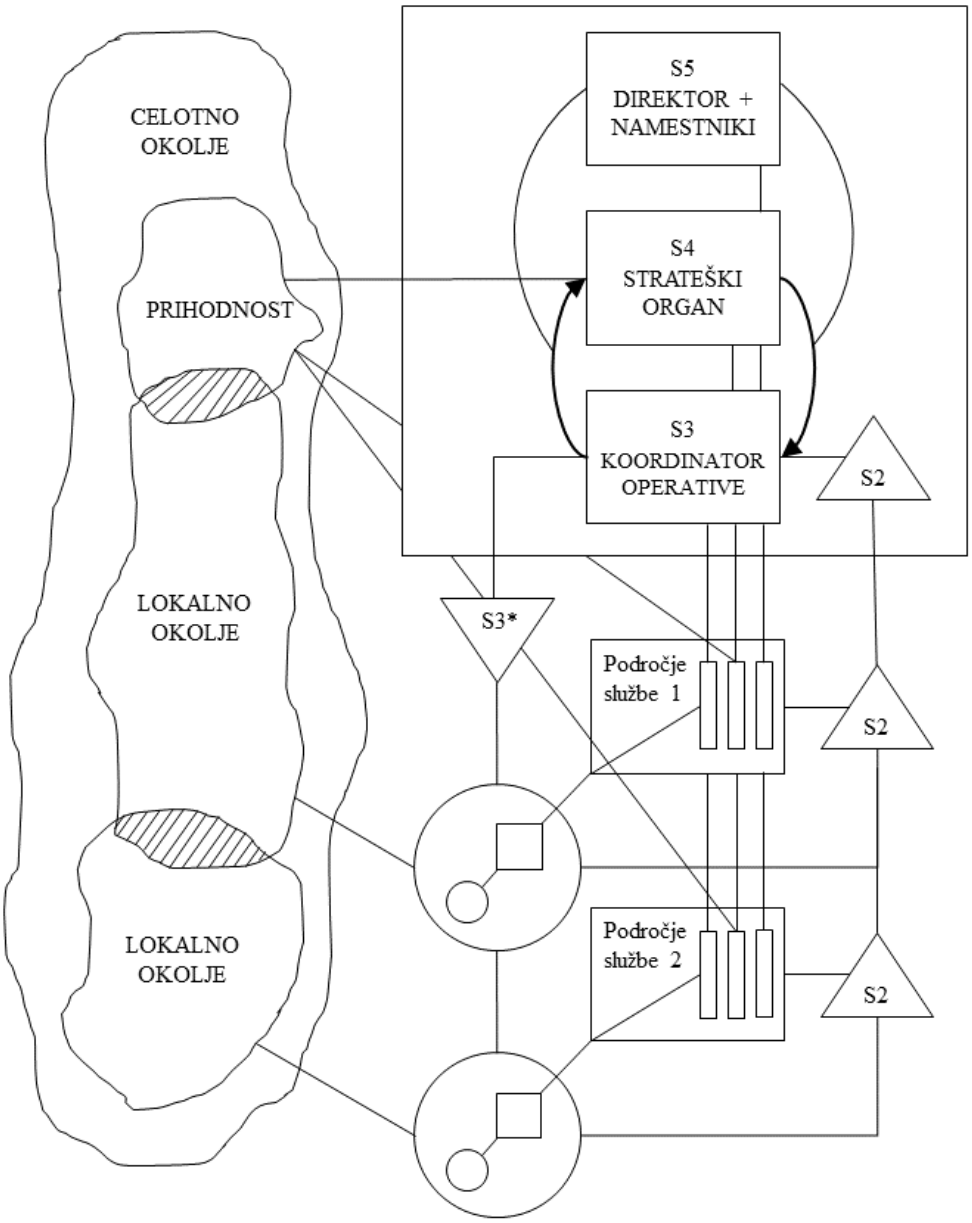
ohranjanje celovitega zaupanja državljanov v matične obveščevalno-varnostne službe in nacionalni obveščevalno-varnostni sistem

Ob upoštevanju dejstva, da MVS lahko zagotovi strukturno osnovo za viabilnost obveščevalno-varnostnih služb, smo po analizi literature, ki obravnava TVS in MVS (Beer, 1981, 1984, 1985; Beckford, 1995; Brocklesby & Cummings, 1996; Espejo & Gill, 1997; Pickering, 2002; Devine, 2005; Schwaninger, 2006 a, 2006 b, 2009, 2010; Leonard, 2008; Jackson, 2009; Espejo & Reyes, 2011; Pérez Ríos, 2012; Hildbrand & Bodhanya, 2015; Schwaninger & Scheef, 2016; Walker, 2017; Orengo, 2018), izoblikovali **model viabilne obveščevalno-varnostne službe**, ki (bi vsaj v teoriji morala) zagotavlja(ti) podlago za njeno viabilnost. Strukturo modela prikazuje slika 5.10, sestavljen pa je iz naslednjih podsistemov:

- S1: **področje službe** predstavlja organizacijsko enoto obveščevalno-varnostne službe, ki opravlja določeno funkcijo in je samostojna zaradi specifične narave svojega dela (npr. operativno in tehnično zbiranje podatkov, analitika, protiobveščevalni oddelek/sektor, varnostni oddelek/sektor, logistika, mednarodno sodelovanje, arhiv ipd.). Te organizacijske enote so pri svojem delovanju avtonomne, vendar delujejo v skladu s predpisi ter odredbami in usmeritvami vodstva službe (S5).
- S2: **informacijski sistem, drugi komunikacijski kanali in srečanja** (npr. sestanki, pogovori, simpoziji, kolegiji), preko katerih teče komunikacija in izmenjava podatkov ter informacij med več S1 ter med S1 in S3. Komunikacija, ki poteka preko informacijsko-komunikacijske tehnologije, je šifrirana/kriptirana in zaščitena s posebnimi protokoli za obravnavo tajnih podatkov.
- S3: **koordinator operative**, ki skrbi za usklajeno (so)delovanje vseh področij službe, delitev finančnih, materialnih in kadrovskih sredstev, izvajanje skupnih projektov/operacij, predvsem pa za uresničevanje prioritet in ciljev službe. Pri tem tesno sodeluje s strateškim organom, ki daje priporočila in smernice za prihodnje delo, hkrati pa upošteva predpise ter odredbe in usmeritve vodstva službe (S5).
- S4: **strateški organ** ima lahko različne oblike. Po našem prepričanju bi bila najbolj ustrezna oblika *kolegij* (npr. predstavnikov (ali vodij) posameznih področij službe). Na sejah takšnega organa bi namreč vsi imeli možnost izraziti svoje vidike na v odnosu do področja, ki ga vodijo. Skupaj bi – vsak s svojega vidika obravnavanja – prepoznavali trende in spremembe v okolju in odločali, kako bi se bilo najbolj primerno nanje odzvati in se jim prilagoditi.

- S5: **direktor in namestniki (vodstvo službe)** je oziroma so normativna in vodstvena avtoriteta obveščevalno-varnostne službe, organ za normativno upravljanje, ki skrbi za uresničevanje smernic za delovanje službe, določenih s strani oblasti (politike). Skrbi za ravnotežje (in kompromise) med koordinatorjem operative in strateškim organom ter upoštevanje bistva, usmeritev, predpisov, etičnih in moralnih načel ter vizije in ciljev službe. To pripomore k ravnovesju službe in ohranjanju njene viabilnosti v odnosu do spremenljivega (varnostnega) okolja.

Slika 5.10: Viabilna obveščevalno-varnostna služba

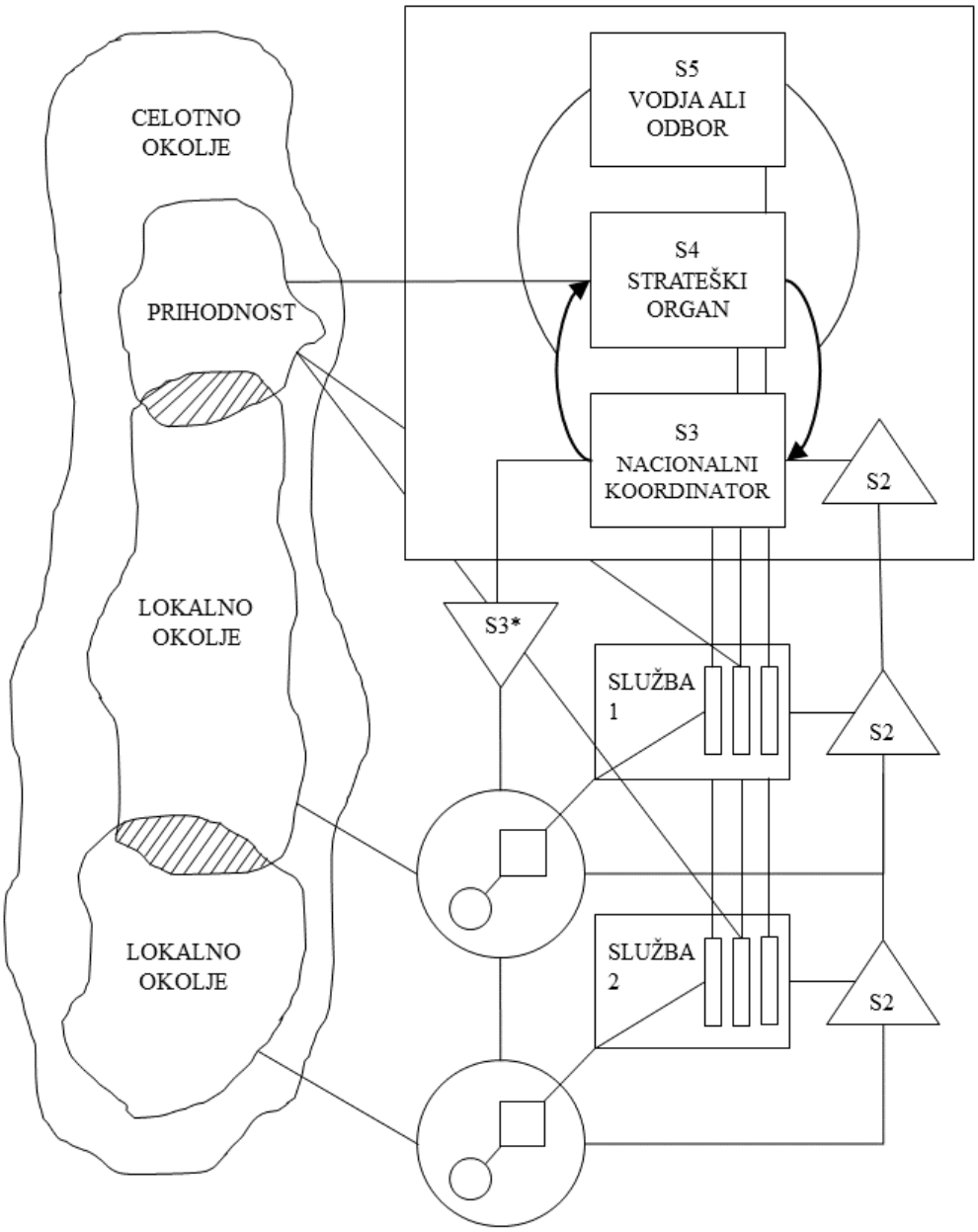


Vir: Osebni vir

Viabilna obveščevalno-varnostna služba je na višji ravni rekurzije podsistem S1 **viabilnega nacionalnega obveščevalno-varnostnega sistema**. Njegovo strukturo (model) prikazuje slika 5.11. Podsistemi viabilnega nacionalnega obveščevalno-varnostnega sistema so:

- S1: **službe**, ki pokrivajo svoje (s predpisi) določeno področje dela (npr. civilna, obrambna, vojaška služba ali pa obveščevalna služba, varnostna služba, obveščevalno-varnostna služba). Vsaka služba je – tako kot področja oziroma organizacijske enote službe pri rekurziji nižjega reda – avtonomna in neodvisna od drugih služb.
- S2: **informacijski sistem, drugi komunikacijski kanali in srečanja** (npr. sestanki, pogovori, simpoziji, kolegiji), preko katerih teče komunikacija in izmenjava podatkov ter informacij med službami. Komunikacija, ki poteka preko informacijsko-komunikacijske tehnologije, je šifrirana/kriptirana in zaščitena s posebnimi protokoli za obravnavo tajnih podatkov.
- S3: **nacionalni koordinator**, ki skrbi za usklajeno (so)delovanje vseh služb, delitev finančnih, materialnih in kadrovskih sredstev, izvajanje skupnih projektov/operacij, v katere so vključene različne službe, predvsem pa za uresničevanje skupnih prioritet in ciljev različnih služb ter nacionalnih interesov in prioritet. Pri tem tesno sodeluje s strateškim organom, ki daje priporočila in smernice za prihodnje delo za celotni nacionalni obveščevalno-varnostni sistem. Nacionalni koordinator je **organ**, ki ga vodi predstojnik/vodja.
- S4: **strateški organ**, ki ga sestavljajo predstavniki (vodje) služb. Skupaj prepoznavajo dejavnike, trende in spremembe v okolju ter določajo skupno ali usklajeno odzivanje oziroma prilagajanje služb navedenemu. Strateški organ sodeluje z nacionalnim koordinatorjem.
- S5: **vodja ali odbor** je normativna in vodstvena avtoriteta nacionalnega obveščevalno-varnostnega sistema. S5 je posredno ali neposredno odgovoren zakonodajni ali izvršni veji oblasti (odvisno od državne ureditve). Skrbi za uresničevanje smernic za delovanje celotnega sistema, za ravnotežje (in kompromise) med nacionalnim koordinatorjem in strateškim organom in za delovanje podsistemov v skladu s predpisi, etičnimi in moralnimi načeli, usmeritvami politike ter nacionalnimi interesi.

Slika 5.11: Model viabilnega nacionalnega obveščevalno-varnostnega sistema



Vir: Osebni vir

Vodstvo službe (vodja ali odbor) bi lahko sodelovalo na srečanjih strateškega organa viabilne obveščevalno-varnostne službe. Vendar to ne bi pomenilo, da je vodstvo/odbor del strateškega organa oziroma S4, temveč da gre za **komunikacijo** in **sodelovanje** med S4 in S5. Ti dve funkciji je potrebno ločiti, čeprav ima v praksi vodstvo/odbor pomembno besedo pri določanju prihodnjih ciljev, nalog in prioritet, vendar se o tem navadno odloča na podlagi informacij, ki jih pripravijo drugi – S4. Na tem mestu kot zanimivost dodajamo, da Beer in tuji avtorji (med njimi večina tistih, ki smo jih obravnavali v tem podpoglavju)

funkcijo sistema S4 imenujejo *intelligence*, kar v angleškem izrazoslovju pomeni tudi *obveščevalna informacija* in pa *obveščevalna zvrst* kot ena od treh zvrsti obveščevalno-varnostne dejavnosti (obveščevalna, protiobveščevalna in varnostna zvrst), odvisno od konteksta uporabe (Hribar, 2016).

Ker lahko nacionalni obveščevalno-varnostni sistem predstavlja **S1 in tudi S4**, odvisno od vidika obravnave, to predstavlja hkrati **posebnost in omejitev**, zaradi katere nismo mogli nadaljevati z izgradnjo strukture viabilnega sistema nacionalne varnosti. Nacionalni obveščevalno-varnostni sistem preko svojih podsistemov s podatki iz okolja ustvarja informacije o prihodnjem (predvidenem) stanju, da se sistem nacionalne varnosti lahko pravočasno in ustrezno prilagodi okolju. Obveščevalna, protiobveščevalna in varnostna dejavnost delujejo tudi operativno v okolju, zato so lahko zaradi narave dela hkrati tudi S1. Glavni kriterij, na podlagi katerega bi lahko presodili, kam uvrščamo nacionalni obveščevalno-varnostni sistem (v S1 ali S4), je **presoja oziroma odločitev**, komu oziroma čemu je sistem podrejen, ali delovanju ***za operativno uresničevanje etosa***, ki ga pooseblja S5, ali delovanju ***za informacijsko podporo*** S5. Ker je ta presoja v domeni oblasti, ki ima možnost in moč spreminjati državne sisteme, nismo začeli z izgradnjo viabilnih sistemov na področju nacionalnega varnostnega sistema.

Strukturo splošnega modela zaupanja državljanov v matične obveščevalno-varnostne službe (slika 5.3) smo zato dopolnili z modeloma viabilne obveščevalno-varnostne službe (slika 5.10) in viabilnega nacionalnega obveščevalno-varnostnega sistema (slika 5.11). S tem smo zadostili pogoju, da je vhod v modeliranje elementarni kibernetski sistem, saj imata podsistema *Državljani* in *Matična obveščevalno-varnostna služba* vse ustrezne sestavine elementarnega kibernetskega sistema, ki se istočasno ujemajo s sestavinami MVS, hkrati pa celotnega splošnega modela zaupanja ni mogoče razstaviti na kibernetske sisteme nižjega reda. Z aplikacijo Beerove strukture MVS smo ustvarili ustrezne strukturne pogoje za zagotavljanje viabilnosti dveh podsistemov splošnega modela zaupanja državljanov v matične obveščevalno-varnostne službe, *Matična obveščevalno-varnostna služba* in *Nacionalni obveščevalno-varnostni sistem*, s tem pa pozitiven vpliv na podsistem *Državljani*.

Ostali podsistemi (*Politika*, *Izvajalci nadzora obveščevalno-varnostnih služb*, *Mediji* in *Strokovna javnost*) so ravno tako pomembni elementi modela in hkrati nastopajo kot dejavniki vpliva, vendar jih nismo preoblikovali. Podsistemov *Politika* in *Mediji* nismo preoblikovali zaradi naše ocene, da morebitna nova struktura bi sicer zagotavljala njihovo viabilnost, ki bi omogočala izvajanje njihovih osrednjih funkcij, vendar zaradi tega ne bi bistveno vplivala na državljanov proces presoje zaupanja niti ne bi imela neposredne ali pomembnejše posredne povezave z zaupanjem državljanov v matične obveščevalno-varnostne službe. Podsistema *Strokovna javnost* pa se ne da prestrukturirati z MVS, saj gre za množico nepovezanih strokovnjakov, posameznikov, zato ni strukturiran kot organizacija. Prestrukturiranje nacionalnega obveščevalno-varnostnega (pod)sistema in njegovih služb ter drugih organov je bilo nujno potrebno zaradi zagotovitve vseh dejavnikov, ki neposredno pozitivno vplivajo na državljanovo institucionalno in medosebno zaupanje v odnosu do matičnih obveščevalno-varnostnih služb. Z viabilno strukturo se po našem prepričanju lahko zagotovi in izboljša *strukturna zagotovila* ter *običajnost situacije,* ki povečujejo državljanovo institucionalno zaupanje, hkrati pa prispeva k zagotavljanju *kompetentnosti*, *integritete*, *predvidljivosti* služb in njihovih uslužbencev, s čimer se lahko poveča državljanovo *medosebno zaupanje*. Vzdrževanje viabilnosti namreč od podsistemov zahteva nenehno prilagajanje, za kar je med drugim potrebno tudi pridobivanje in osveževanje znanja, ustrezno opravljanje svojega dela, učinkovito vodenje podsistemov, primerno razdeljevanje sredstev, delegiranje nalog idr.

V osnovnemu modelu je kljub vsem dopolnitvam in spremembam manjkala sestavina, ki bi pripomogla k celovitemu uresničevanju 8. smernice za ustvarjanje zadostnega in potrebno celovitega zaupanja (*Upnik mora imeti ustrezno znanje o zaupniku, njegovem in lastnem okolju, tveganjih in nadzoru*). Pred tem smo ugotovili, da večina politikov, medijev in državljanov nima (dovolj) znanja o obveščevalno-varnostnih službah ali pa je to znanje pomanjkljivo in da so zato bolj dovzetni za (namerno) pomanjkljive ali napačne informacije o matičnih obveščevalno-varnostnih službah. Ker ima znanje pomembno vlogo v procesu presoje zaupanja, bi takšno stanje modela brez komponente, ki bi zagotavljala ustrezno znanje, vodilo v vse prej kot v izboljšanje zaupanja. V povezavi s podajanjem znanja smo omenili strokovnjake, ki nastopajo kot tretje osebe, od katerih so državljani v določenih primerih lahko odvisni na področju pridobivanja znanja. In

čeprav smo ugotovili, da so strokovnjaki (podsistem *Strokovna javnost*) vir znanja, ki hkrati opozarja na nepravilnosti ali potrebne izboljšave in ki pojasnjuje določene dogodke in njihova ozadja ter kritično ocenjuje delo služb, pa ti strokovnjaki v trenutni strukturi modela celovitega zaupanja po našem mnenju ne zadostujejo za ustrezno distribucijo znanja in s tem uresničevanje prej omenjene 8. smernice za ustvarjanje zadostnega in potrebno celovitega zaupanja, saj niso vsi strokovnjaki tudi učitelji. Zato smo dodali nov podsistem – ***Izobraževalni sistem***. Ta ima nekaj skupnih sestavin s podsistemom *Strokovna javnost*, in sicer **visokošolske učitelje/akademike**. Ker niso vsi iz podsistema *Strokovna javnost* tudi učitelji, strokovnjaki, ki niso učitelji, ne spadajo v podsistem *Izobraževalni sistem*. Naloga podsistema *Izobraževalni sistem* je skrb za prilagojeno in ustrezno izobraževanje različnih struktur državljanov o obveščevalno-varnostni dejavnosti, v okviru tega tudi o matičnih obveščevalno-varnostnih službah. Osrednje je osnovno znanje, ki služi kot podlaga za izoblikovanje ustrezne **varnostne kulture**. Brez ustreznega znanja ne moremo pričakovati, da se bo izboljšala varnostna kultura, zato tudi ne moremo pričakovati, da se bo stanje na področju zaupanja v te službe bistveno spremenilo. Z znanjem bi namreč odpravili velik dejavnik, ki negativno vpliva na zaupanje državljanov v matične obveščevalno-varnostne službe – **strah**. Po našem prepričanju strah izhaja iz prepričanja v obstoj možnosti zlorabe moči in pooblastil, ki jih imajo obveščevalno-varnostne službe, saj si nihče ne želi biti opazovan proti svoji volji. Vsaka nezakonita uporaba pooblastil za spremljanje, opazovanje in sledenje osebam pomeni tudi hudo kršitev posameznikove zasebnosti in njegovih človekovih pravic, zato je potrebno državljane prepričati in jim dokazati, da je strah povsem odveč. Izhajali smo iz spoznanja, da **strah povzroča nezaupanje, izhaja pa največkrat iz nevednosti in neznanja** (»strah pred neznanim«). V uvodu doktorske disertacije smo tudi pojasnili našo predpostavko, da če državljani o obveščevalno-varnostnih služb nimajo ustreznih preverjenih, resničnih in zanesljivih znanj, s katerimi lahko samostojno, utemeljeno in kritično pristopijo k individualni obravnavi in izgradnji zaupanja, bodo na zaupanje bistveno vplivali drugi dejavniki, kar bo ustvarilo družbeni vpliv, ki bo usmerjal zaupanje državljanov v matične obveščevalno-varnostne službe. Ljudje, ki nimajo izkušenj iz določene situacije, lahko pridobijo strah tudi z branjem ali poslušanjem negativnih informacij in z opazovanjem, takšen strah pa je lahko enak tistemu, kot ga doživlja oseba, ki ima določene izkušnje (Makashvilia, Kaishauri &

Azmaiparashvili, 2014, str. 185). Kot smo že večkrat omenili, državljani po naših izkušnjah in védenju o službah nimajo veliko znanja, zaupanje pa je med drugim odvisno tudi od znanja (Marková, Linell & Gillespie, 2008), zato lahko pride do dvojega: 1) zaupanje upade zaradi pomanjkanja znanja, ali pa 2) državljani pridobijo napačno ali pomanjkljivo znanje, ki vodi v napačna spoznanja in strah, ta pa v upad zaupanja. Za slednji primer so pogosto odgovorni mediji, ki namerno poročajo o zadevah, s katerimi se med ljudmi širi strah in nezaupanje (Milton, 2008), ali pa prikazujejo dejansko stanje v drugačni obliki. Podoben vpliv sta imela neznanje in strah na zaupanje v policijo (glej npr. Bradford & Jackson, 2010). Kot ugotavlja Layard (2005), sta strah in zaupanje povezana, saj stopnja zaupanja v družbi kaže povezavo s stopnjo strahu v družbi. S tem okvirno utemeljujemo, zakaj je bilo potrebno dodati podsistem *Izobraževalni sistem* osnovnemu modelu, da bi lahko dosegli zadostno in potrebno celovito zaupanje. Ta podsistem je z vidika ustvarjanja in vzdrževanja zadostnega in potrebno celovitega zaupanja soodvisen z ostalimi podsistemi.

Podobno kot pri osnovnem modelu zaupanja državljanov v matične obveščevalno-varnostne službe so vsi podsistemi (razen podsistema *Tuje obveščevalno-varnostne službe*), ki vplivajo na podsistem *Državljani* in ta od njih pridobiva podatke in informacije, med seboj soodvisni. Velika večina povezav med soodvisnimi podsistemi je odvisna od njihove komunikacije. Miltonova (2008, str. 9) pravi, da zaupanje izhaja iz pristne komunikacije, zato je komunikacija nujen element našega modela. Z njo se utrjujejo povezave, posredujejo podatki in informacije ter vzdržujejo ustrezni odnosi, potrebni za zaupanje. Pravočasna, zanesljiva, točna in iskrena komunikacija po našem prepričanju zagotavlja, da prihaja do pozitivnih sinergij, s čimer upočasnjuje entropijo celotnega modela oziroma modela-sistema, posredno pa se zagotavljajo tudi vsi pogoji za uresničevanje smernic za ustvarjanje zadostnega in potrebno celovitega zaupanja.

5.3.3 Procesi

Prepoznali smo naslednje temeljne procese modela celovitega zaupanja državljanov v matične obveščevalno-varnostne službe:

a) Zbiranje podatkov in informacij ter presoja zaupanja

Ta proces se odvija v posameznih državljanih znotraj podsistema *Državljani* in je osrednji proces modela, saj so državljani naš osrednji subjekt/objekt raziskovanja. Postopek zbiranja podatkov in informacij ter presoje zaupanja smo podrobno opisali v podpoglavju 5.1.2 (slika 5.5).

b) Spremljanje in merjenje zaupanja

Izvajajo ga podsistemi *Politika*, *Nacionalni obveščevalno-varnostni sistem* in *Strokovna javnost*. Politika mora spremljati in meriti zaupanje, ker je zadolžena za urejanje, upravljanje, usmerjanje in koordiniranje nacionalnega obveščevalno-varnostnega sistema in njegovih podsistemov. Stopnja zaupanja ji pove, kako so državljani zadovoljni s storitvami obveščevalno-varnostnih organov, te informacije pa mora nato uporabiti za ustrezno prilagajanje njihovega delovanja. Iz enakega razloga mora zaupanje spremljati in meriti tudi nacionalni obveščevalno-varnostni sistem, ki je z vidika matičnih obveščevalno-varnostnih služb kot sistem višjega reda oziroma višja raven rekurzije odgovoren za viabilno delovanje svojih avtonomnih podsistemov. Razlog, zakaj mora strokovna javnost spremljati in meriti zaupanje, je nekoliko drugačen od tistega, zakaj morata enako početi politika in nacionalni obveščevalno-varnostni sistem: da kritično spremlja zadovoljstvo in zaupanje državljanov v povezavi z ukrepi, ki jih sprejmeta politika in nacionalni obveščevalno-varnostni sistem. Ta dva sistema zaradi političnih, individualnih ali drugih partikularnih vplivov/interesov/razlogov nista pripravljena spremeniti stanja ali pa tega ne moreta storiti. Strokovna javnost v tem primeru služi kot tretja stran, ki s kritične distance – ker ni neposredno vpletena v situacijo – presoja stanje in sprejete ukrepe ter predlaga, kaj bi bilo potrebno storiti, popraviti, odpraviti ali preprečiti. Je svetovalec in hkrati nadzornik nad strokovnostjo, smotrnostjo in tudi zakonitostjo ukrepanja politike in nacionalnega obveščevalno-varnostnega sistema pri spremembah, potrebnih za vzdrževanje ali spremembo zaupanja državljanov v matične obveščevalno-varnostne službe.

V doktorski disertaciji sicer nismo predlagali ali izoblikovali nobenega orodja za merjenje zaupanja, vendar menimo, da bi ustrezno sestavljena anketa zadoščala za pridobitev podatkov o stopnji zaupanja državljanov v matične obveščevalno-varnostne službe.

c) Izobraževanje

Izobraževanje drugih oziroma posredovanje znanj s področja obveščevalno-varnostne dejavnosti je eden izmed procesov, ki mu znanstvena in strokovna literatura, akademska sfera in strokovna javnost po našem prepričanju ne posvečajo dovolj pozornosti. Proces presoje zaupanja brez (ustreznega) znanja ne more biti celovit in čim manj subjektiven, zaradi tega pa je težje zagotoviti visoko zaupanje državljanov v matične obveščevalno-varnostne službe. To razmišljanje, ki je povezano z izobraževanjem, smo razdelili na dva vidika.

Prvi vidik se nanaša na vsebino znanja. Osnovno znanje s področja obveščevalno-varnostne dejavnosti lahko zagotovi le ustrezen izobraževalni sistem, bodisi državni ali podprt s strani države. To znanje bi moralo biti osnovno, saj ni potrebe za poglobljeno znanje, zato menimo, da velike spremembe obstoječih izobraževalnih sistemov (ali programov) ne bi bile smiselne. Vsekakor pa bi bilo potrebno zagotoviti ustrezen način za pridobivanje ustreznega znanja, ki bi zagotavljal osnovno poznavanje obveščevalno-varnostne dejavnosti in tovrstnih služb. S tem bi se zmanjšalo ali celo preprečilo, da bi prišlo do zmotnih prepričanjih o službah in njihovih nalogah, pooblastilih ter aktivnostih. To znanje bi postopno odpravilo nezadovoljstvo, dvome in strah, posredno pa tudi preprečilo morebitno škodo, ki bi jo zaradi neznanja in s tem nezaupanja lahko utrpel nacionalni varnostni sistem in njegovi podsistemi. Vse drugo znanje, ki dopolnjuje osnovno, pa lahko državljanom posredujejo bodisi matične obveščevalno-varnostne službe, nacionalni obveščevalno-varnostni sistem, strokovna javnost (preko medijev) in mediji preko spletnih strani, zgibank, poročil, tiskovnih konferenc, znanstvenih in strokovnih konferenc, neformalnih ali formalnih izobraževanj za širšo javnost, okroglih miz ipd. Za izobraževanje zato ni zadolžen le *Izobraževalni sistem*, temveč so v ta proces vpleteni tudi podsistemi *Politika*, *Nacionalni obveščevalno-varnostni sistem*, *Matična obveščevalno-varnostna služba* in *Strokovna javnost*.

Prepričano smo, da bi moral podsistem *Politika* kot nosilec varnostne in tudi izobraževalne politike poskrbeti za ustrezno izobrazbo državljanov ne le na področju varnosti na splošno, temveč predvsem na področju varnostne kulture. Zato menimo, da bi morala biti izobraževalna politika, ki bi dvignila raven varnostne kulture, povečala

splošno razgledanost na področju varnosti in izboljšala samozaščitno ravnanje državljanov, eden od dolgoročnih nacionalnih interesov.

Drugi segment znanja pa se nanaša na področje kritičnega razmišljanja. Ustrezno znanje samo po sebi ni zagotovilo, da bo državljan ustrezno presodil zaupanje, saj je lahko podvržen zavajanju in zmotnim ali pomanjkljivim podatkom in informacijam s strani tujih obveščevalno-varnostnih služb pa tudi politike, medijev, strokovne javnosti, izobraževalnega sistema, nadzora in drugih državljanov. Kritično razmišljanje in z njim povezana kritična distanca do dogodkov državljanu omogočata, da iz procesa presoje zaupanja izloči vse subjektivne, vsiljene, napačne, zavajajoče ali druge s tem povezane podatke in informacije. Znanje in veščine s področja kritičnega razmišljanja je mogoče pridobiti tako s formalnim kot neformalnim izobraževanjem, pri tem pa ima strokovna javnost pomembno nalogo, da spremlja in preko medijev kritično ocenjuje aktualne in pretekle dogodke, aktivnosti, politiko in druge vsebine s področja obveščevalno-varnostne dejavnosti. Ne pozabimo, da je strokovna javnost *tertius*, ki ima pri procesu presoje zaupanja v okoliščinah, ko je o zaupniku malo podatkov in informacij, pomembno vlogo, saj upnik veliko znanja pridobi ravno od nje.

č) Izvajanje nadzora

V uvodu smo izpostavili dokaj razširjeno prepričanje, da je demokratični nadzor najboljše (ali celo edino) zagotovilo, da bodo službe delovale demokratično in da se bo s tem povečalo zaupanje državljanov v matične obveščevalno-varnostne službe. Vendar je demokratični nadzor le eden izmed dejavnikov, ki vplivajo na zaupanje. Potrebno ga je izvajati, pri tem pa izvajalcem nadzora zagotoviti vso podporo za opravljanje njihovega dela, predvsem strokovno podporo, kadar ti nimajo dovolj znanja. Izvajalci nadzora so tako kot strokovnjaki *tertius*, vendar s to razliko, da imajo podatke in informacije o dogajanju »onkraj zidu tajnosti«, zato so pomemben vir podatkov in informacij za medije in državljane. V podpoglavju 5.3.6 so predstavljene konkretne smernice za ustrezno izvajanje (demokratičnega) nadzora obveščevalnih in varnostnih služb, ki so v skladu s smernicami za ustvarjanje zadostnega in potrebno celovitega zaupanja, drugih konkretnih smernic pa v doktorski disertaciji nismo navedli, saj o izvajanju

demokratičnega nadzora obstaja veliko javno dostopne literature (glej npr. Wills et al., 2011; Wills, 2012; Born, 2013; Cole, Fluri & Lunn, 2015; Schierkolk, 2018).

d) Poročanje

Poročanje se kot temeljni proces pojavlja na različnih mestih v modelu. Predvsem pri podsistemih, ki spadajo pod okrilje državne uprave, mora biti poročanje pravočasno, natančno in v okviru potrebe po védenju (slednje je vezano predvsem na tajnost podatkov). Pri poročanju državljanom je ključno, da je poročanje objektivno, brez vrednostnih sodb, realno in v okviru dovoljenega; potrebno je upoštevati tajnost podatkov, nacionalne interese in biti pozoren na tuje interese ter z njimi povezane aktivnosti tujih obveščevalno-varnostnih služb. *Izvajalci nadzora* so poleg politike in delno tudi nacionalnega obveščevalno-varnostnega sistema ter matičnih obveščevalno-varnostnih služb tisti, ki lahko (omejeno) poročajo o dogajanju »onkraj zidu tajnosti«. Ker je podsistemov, ki bi lahko poročali o tem, malo, je ključno, da njihovo poročilo doseže čim večji krog državljanov (npr. s pomočjo medijev). Pri tem pa lahko trčimo na različna načela in pravice, kot so pravica do *osebne varnosti* (glej npr. 3. člen Splošne deklaracija o človekovih pravicah in 5. člen EKČP), pravica *dobiti informacijo javnega značaja*, ki jo pozna večina Zahodnih držav (pri tem obstajajo tudi omejitve do dostopa, ki so odvisne od nacionalnih predpisov), *tajnost podatkov,* princip *potrebe po védenju* (ang. *need-to-know*), načelo *javnega interesa in* načelo *nacionalnega interesa*. Ta načela in pravice se v nekaterih primerih med seboj izključujejo, ključne pa so izkušnje, znanje in tudi poznavanje prava.

S poročanjem javnosti se izboljšujeta tudi transparentnost in sodelovanje z državljani. V zvezi s tem je Lohaus (2015) dejal: »Aktivno vključevanje javnosti po razkritjih gradi zaupanje, ščiti viabilnost pomembnih zmogljivosti.« Meni (ibidem), da zanikanje in nepotrjevanje informacij lahko naredita več škode kot dobrega. Kljub temu je potrebno razumeti, da obveščevalno-varnostne službe ne morejo komentirati zadev, ki so tajne. Pomemben je hiter odziv in pa dialog, ki ga služba vzpostavi z državljani. Komunikacija je namreč nujna za vzpostavitev in ohranitev zaupanja med upnikom in zaupnikom – med državljani in matičnimi obveščevalno-varnostnimi službami.

e) Svetovanje in nudenje strokovne pomoči

Pri tem procesu ne gre za pomoč, ki jo matične obveščevalno-varnostne službe nudijo državnim organom in drugim subjektom javnega ali zasebnega sektorja na področju protiobveščevalne in varnostne dejavnosti, temveč za pomoč, ki jo strokovna javnost preko svojih ekspertov nudi drugim podsistemom. S tem se povečuje strokovnost matičnih obveščevalno-varnostnih služb in drugih oseb nacionalnega obveščevalno-varnostnega sistema, na drugi strani pa krepi zaupanje med strokovno javnostjo in nacionalnim obveščevalno-varnostnim sistemom ter matičnimi obveščevalno-varnostnimi službami, politiko in izvajalci nadzora. Matične obveščevalno-varnostne službe bi morale biti bolj odprte za novo znanje in koncepte, s katerimi lahko nadgradi svoje delovne procese, opremo in sredstva, znanje ter nekatera druga področja. Ozko delovanje specialistov namreč ne zadostuje za celovito delovanje, zato je tudi na tem področju potrebno sodelovanje specialistov »z obeh strani« skupaj generalisti, kot to določa DTS. Pridobivanje novega znanja in potreba po svetovanju na specifičnih področjih obveščevalno-varnostne dejavnosti je še posebej ključna za izvajalce nadzora, saj ti nimajo vedno dovolj ali pa pravega znanja, potrebnega za učinkovito izvajanje nadzora, na kar je v intervjuju opozoril tudi mag. Tonin.

f) Preprečevanje plasiranja dezinformacij in vplivov tujih obveščevalno-varnostnih služb.

Delovanje tako specifičnega procesa lahko zagotavljajo le obveščevalno-varnostne službe, ki morajo biti za to ustrezno usposobljene in opremljene (materialno, kadrovsko ter finančno). Neizvajanje tega procesa lahko poveča možnost, da je izid državljanove presoje zaupanja napačen in posledično škodljiv za matične obveščevalno-varnostne službe in posredno za celotni nacionalni varnostni sistem.

5.3.4 Vhodi

Kljub identifikaciji dveh elementarnih kibernetskih sistemov smo presodili, da je za določanje vhodov modela-sistema ključen podsistem *Državljan*, saj predstavlja osrednji subjekt našega raziskovanja, ki je zaradi človeške narave tudi najbolj občutljiv in nepredvidljiv. Prepoznali smo naslednje vhode podsistema *Državljan*, ki hkrati

predstavljajo tudi vhode modela-sistema celovitega zaupanja državljanov v matične obveščevalno-varnostne službe:

- **Podatki in informacije o podsistemih/iz podsistemov**. Ti predstavljajo osnovno materijo za proces presoje zaupanja, za oblikovanje praga zaupanja in za ostale potrebe podsistema.
- **Dezinformacije in vplivi tujih obveščevalno-varnostnih služb**.
- **Drugi podatki in informacije o okolju/ki prihajajo iz okolja**. Ti vplivajo na vse postopke procesa presoje zaupanja. Državljani iz njih pridobivajo znanje o službah, ostalih podsistemih, zaznanem tveganju, vplivih in drugih dejavnikih, ki lahko vplivajo na proces presoje zaupanja.
- **Trenutna stopnja zaupanja** državljanov v matično obveščevalno-varnostne službe (izhodišče za ponovno presojo zaupanja).

Ker je za obliko in vsebino vhodov iz prve alineje odgovoren dialektični sistem podsistemov (*Politika*, *Izvajalci nadzora*, *Mediji*…), lahko ti podsistemi vplivajo na oblikovanje vhodov iz prve alineje na način, da bodo sledili smernicam za ustvarjanje zadostnega in potrebno celovitega zaupanja. Podsistemi ne morejo ustvariti ali preprečiti pojava vhodov iz tretje in četrte alineje, lahko pa vplivajo na zaznavanje teh vhodov. Vhodi iz tretje alineje niso zaželeni, saj so škodljivi, zavajajoči in zato povzročajo upad zaupanja. Da bi dosegli celovito zaupanje, morajo matične obveščevalno-varnostne službe preprečiti, da ti vhodi pridejo do državljana, če pa že pridejo, pa je naloga dialektičnega sistema podsistemov, da ima državljan dovolj znanja, da zazna škodljive vhode in jih ne upošteva pri presoji zaupanja.

5.3.5 Vplivi

Na podlagi analizirane literature v prejšnjih poglavjih, opravljenih intervjujev in lastnega znanja ugotavljamo, da so podsistemi ***Politika***, ***Izvajalci nadzora***, ***Mediji*** in ***Državljani*** (ne nujno v tem vrstnem redu) tisti podsistemi, ki imajo največji vpliv na celoten proces zaupanja in na državljana.

Politika ima vpliv zaradi možnosti in moči, da posredno ali neposredno vpliva na vsa področja nacionalnega obveščevalno-varnostnega sistema oziroma krovnega sistema nacionalne varnosti (pa tudi na vsa področja družbenega življenja). Z usmerjanjem, določanjem prioritet in vplivom na izvajanje obveščevalno-varnostne dejavnosti posredno vpliva na njihovo učinkovitost in javno podobo ter njihove rezultate. V tem kontekstu velja dodati, da ima politika predvsem velik vpliv na delovanje ter določanje ogrodja, prioritet in proračuna nacionalnega obveščevalno-varnostnega sistema. Politika ima možnost vplivanja na vse tri vrste zaupanja: dispozicijsko (z oblikovanjem etike in morale preko predpisov, vzgoje, sankcioniranjem, nagrajevanjem in drugimi ukrepi), institucionalno (npr. s predpisi, skrbjo nad upoštevanjem in izvajanjem predpisov ter družbenega reda, s sankcioniranjem in nagrajevanjem, z oblikovanjem družbe in družbenega reda) ter medosebno zaupanje (posredovanje podatkov in informacij o zaupniku in/ali vplivanje na širjenje ali vpliv drugih informacij – tudi preko medijev).

Podsistem ***Izvajalci nadzora*** je vpliven zaradi možnosti nadzorovanja skoraj vseh področij delovanja matičnih obveščevalno-varnostnih služb, hkrati pa ima status (domnevno) zanesljivega in relevantnega vira informacij o stanju in delovanju matičnih obveščevalno-varnostnih služb. Ker so informacije moč, lahko s poročanjem o delovanju služb iz prve roke ustvarijo (pomemben) prvi vtis o situaciji. To lahko pomeni nizko ali visoko zaupanje že v samem izhodišču presoje zaupanja. Zaradi njihove funkcije so lahko tudi medijsko odmevni, kar še dodatno poveča domet in vpliv njihovega poročanja.

Podsistem ***Mediji*** služi kot **prenašalec, ojačevalec ali blažilec vpliva** podatkov in informacij politike, izvajalcev nadzora, nacionalnega obveščevalno-varnostnega sistema, njegovih podsistemov in pa strokovne javnosti, po drugi strani pa je lahko tudi **vir vpliva**. Zadnje velja predvsem takrat, kadar novinarji z raziskovalnim delom razkrijejo določen incident, nepravilnost, stanje ali področje službe. Vpliv medijev je velik predvsem zaradi velikega dometa njihovega poročanja in hitrosti obveščanja javnosti. Usmerjenost vpliva je odvisna predvsem od vsebine poročanja.

Spoznali smo, da podsistem ***Državljani*** pravzaprav ni (primarni) izvor vpliva, temveč je predvsem **ojačevalec** vpliva, ki ga ustvarijo drugi podsistemi. Vpliv, ki ga državljani

ustvarjajo z javnim mnenjem in trendov, nastane na podlagi mnenja večine, to pa se oblikuje na podlagi podatkov in informacij, ki jih državljani pridobijo predvsem od vplivnih podsistemov. Če so ti negativni, je večja verjetnost, da bo tudi javno mnenje negativno.

Poseben položaj med podsistemi, ki imajo vpliv, ima podsistem ***Tuje obveščevalno-varnostne službe***. Zaradi nepoznavanja zmogljivostih tujih služb, njihovih aktivnosti, metod delovanja ipd. ne moremo trditi, kakšen vpliv imajo. O obstoju njihovega vpliva ne dvomimo, ne moremo pa ga oceniti, saj se tuje službe med seboj razlikujejo. Razlikujejo se tudi družbe, v katerih tuje službe delujejo, in interesi služb, ki so usklajeni z njihovimi nacionalnimi politikami in prioritetami, zato je lahko rezultat njihovega dela/vpliva od države do države povsem različen.

Iz podobnih razlogov nismo mogli določiti najbolj vplivnih zunanjih dejavnikov, saj so si družbe po svetu različne, zato se zaradi različnih VKEN razvijejo tudi različni odzivi na posamezne incidente, pojave, razkritja in drugo. Ker je bil naš cilj ustvariti model, ki ga bo mogoče aplicirati na katerokoli državo, smo sklenili, da pustimo to področje dovolj široko odprto in da ne bomo določali (preveč) specifičnih dejavnikov.

Za vse vplive velja, da jih je potrebno omejiti, da ne bi bili izkoriščeni za zlorabo ali partikularne interese in jih predvsem usmeriti v doseganje pozitivnih rezultatov. Kako izkoristiti vplive notranjih podsistemov, smo predlagali s smernicami za delovanje modela, oblikovanimi s pomočjo DTS, DOMR, TVS/MVS in smernicami za ustvarjanje zadostnega in potrebno celovitega zaupanja.

5.3.6 Smernice za delovanje modela

Smernice in izhodišča za ustvarjanje zadostnega in potrebno celovitega zaupanja smo aplicirali na področje zaupanja državljanov v matične obveščevalno-varnostne službe in tako izoblikovali nekaj specifičnih smernic za podsisteme. Te smernice bi bilo potrebno upoštevati, da bi lahko obravnavani podsistemi skupaj z drugimi podsistemi vzpostavili in zagotavljali celovito zaupanje državljanov v matične obveščevalno-varnostne službe.

Poudarjamo, da te smernice niso zagotovilo za dosego *popolnega* zaupanja, temveč za dosego *celovitega* zaupanja. Potrebno jih je razumeti kot *priporočila* za delovanje podsistemov pri izvajanju temeljnih procesov. Smernice bi pripomogle k ustvarjanju psihološkega stanja oziroma prepričanja upnika, da je zaupnik ustrezna entiteta in da bo izpolnil njegova pričakovanja, hkrati pa da bi bil upnik pripravljen sprejeti tveganja in biti ranljiv. Na eni strani bi zato pripomogle k ustvarjanju in vzdrževanju dispozicijskega, institucionalnega in medosebnega zaupanja, na drugi strani pa k objektivni presoji zaupanja. Ali bo s tem doseženo celovito zaupanje, je odvisno predvsem od objektivnih in subjektivnih izhodišč vsakega posameznika ali posameznice, ki aplicira smernice, kasneje pa model v prakso.

Politika:

- posredno zagotavljanje učinkovitosti matičnih obveščevalno-varnostnih služb (podpora: finančna, kadrovska, organizacijska, koordinacijska);
- redno spremljanje in merjenje stanja zaupanja državljanov v matične obveščevalno-varnostne službe in ustrezno ukrepanje v primeru upada zaupanja;
- opozarjanje na vpliv tujih obveščevalno-varnostnih služb;
- prizadevanje za resnično, ažurno in verodostojno poročanje o stanju in dogodkih, povezanih z matičnimi obveščevalno-varnostnimi službami (razen če to preprečujejo tajnost oziroma nacionalni ali varnostni interesi);
- objavljanje informacij (obveščanje), ki temeljijo na preverjenih in zanesljivih podatkih (iz ravno takšnih virov);
- dajanje pojasnil, zakaj je potrebno zaupati matičnim obveščevalno-varnostnim službam;
- predstavljanje sistema, ki zagotavlja učinkovitost matičnih obveščevalno-varnostnih služb;
- določanje smernic in okvirov za transparentno in zakonito izvajanje obveščevalno-varnostne dejavnosti;
- zagotavljanje avtonomije in kontinuitete dela matičnih obveščevalno-varnostnih služb (predpisi, resolucije, strategije, dolgoročne smernice);

- tesno sodelovanje z vodstvom in predstavniki nacionalnega obveščevalno-varnostnega sistema ter matičnih obveščevalno-varnostnih služb;
- določanje predpisov, pooblastil in okvirov za delovanje izvajalcev nadzora;
- določanje okvirov za transparenten postopek izbire kompetentnih izvajalcev nadzora;
- zagotavljanje avtonomije in izogibanje oviranju izvajalcev nadzora pri njihovem delu;
- izpostavljanje uspehov in dosežkov matičnih obveščevalno-varnostnih služb (kadar je to mogoče in če se s tem nikogar/ničesar ne ogroža);
- seznanjanje javnosti s stanjem nacionalnega, regionalnega ter mednarodnega varnostnega okolja;
- spreminjanje/prilagajanje izobraževalnega sistema, da bi državljani pridobili vsaj osnovno znanje o obveščevalno-varnostni dejavnosti, nacionalnem obveščevalno-varnostnem sistemu in matičnih službah;
- sodelovanje z mediji na področju obveščanja in poročanja;
- skrb za vzpostavitev izobraževalnih aktivnosti za ustrezno medijsko poročanje (delavnice, okrogle mize, projekti, strokovna srečanja idr.);
- uvajanje in urejanje politike na področju »žvižgačev«;
- sprejemanje ustreznih ukrepov za izboljšanje in vzdrževanje ustrezne varnostne kulture;
- sodelovanje z ostalimi podsistemi/deležniki modela-sistema zaupanja državljanov v matične obveščevalno-varnostne službe.

Matična obveščevalno-varnostna služba:

- strokovno, etično, legitimno, legalno delovanje in izvrševanje predpisanih nalog;
- pravočasno preprečevanje pretresov in afer, izogibanje napakam in pravočasna zajezitev ali zmanjšanje nastale škode;
- sodelovanje z izvajalci nadzora, njihovo upoštevanje in neoviranje njihovega dela;
- zagotavljanje tajnosti lastnih operativnih zadev, osebja, nalog, metod idr. med potekom izvajanja nadzora;
- preprečevanje izvajalcem nadzora, da bi izvršili morebitne kršitve predpisov ali prekoračitev pooblastil pri izvajanju nadzora;

- odpravljanje napak, pomanjkljivosti, kršitev in nepravilnosti, ki jih odkrije nadzor, ter sprejemanje odgovornosti zanje;
- izboljševanje transparentnosti z upoštevanjem navodil, smernic in ugotovitev politike, vodstva nacionalnega obveščevalno-varnostnega sistema, izvajalcev nadzora in strokovne javnosti;
- javno priznanje kredibilnosti izvajalcev nadzora, kadar je nadzor ustrezno izveden;
- posredovanje informacij javnosti v tolikšni meri in pod takimi pogoji, da s tem ne ogrožajo svojega delovanja ali delovanja drugih služb, tajnosti, nacionalne varnosti in nacionalnih interesov, da pri tem vendar zadostijo javnim interesom (kadar je to mogoče oziroma dopustno);
- seznanjanje javnosti s stanjem nacionalnega, regionalnega in mednarodnega varnostnega okolja;
- sodelovanje z mediji, organiziranje in izvajanje srečanj/delavnic z mediji na temo ustreznega poročanja o delu služb;
- vzpostavljanje in vzdrževanje dialoga z javnostjo (tudi s pomočjo medijev oziroma sredstev za obveščanje);
- objavljanje periodičnih poročil za politiko, vodstvo nacionalnega obveščevalno-varnostnega sistema, izvajalce nadzora in javnost (vendar ne istih poročil za vse subjekte);
- oblikovanje (interaktivne) spletne strani z osnovnimi informacijami o službi, njenih nalogah in pristojnostih;
- dajanje informacij javnega značaja, kadar je to mogoče/dopustno in v skladu s predpisi;
- izogibanje zavajanju javnosti pri pojasnjevanju dogodkov, povezanih z matičnimi obveščevalno-varnostnimi službami (kadar je to mogoče);
- preprečevanje vpliva in delovanja tujih obveščevalno-varnostnih služb ter opozarjanje na njihov vpliv;
- sodelovanje z ostalimi podsistemi/deležniki modela-sistema zaupanja državljanov v matične obveščevalno-varnostne službe.

Nacionalni obveščevalno-varnostni sistem:

- posredovanje informacij javnosti v tolikšni meri in pod takimi pogoji, da niso ovirane niti ogrožene matične obveščevalno-varnostne službe niti nacionalna varnost in nacionalni interesi;
- seznanjanje javnosti s stanjem nacionalnega, regionalnega in mednarodnega varnostnega okolja;
- pripravljanje smernic za transparentno in zakonito delovanje subjektov nacionalnega obveščevalno-varnostnega podsistema;
- spremljanje zaupanja državljanov v matične obveščevalno-varnostne službe;
- spremljanje delovanja matičnih obveščevalno-varnostnih služb, predvsem na področju strokovnosti, zakonitosti in potrebnosti delovanja;
- zagotavljanje ustreznih pogojev za avtonomno delovanje matičnih obveščevalno-varnostnih služb;
- vzpostavljanje notranjega ravnovesja in ravnovesja z okoljem (v skladu s TVS in MVS);
- koordiniranje matičnih obveščevalno-varnostnih služb pri skupnih ali podobnih zadevah;
- spremljanje in zagotavljanje delovanja sistema za komunikacijo med matičnimi obveščevalno-varnostnimi službami;
- skrb za usklajevanje prioritet politike z nalogami in cilji matičnih obveščevalno-varnostnih služb;
- skrb za implementacijo potrebnih rešitev ali sprememb;
- opozarjanje javnosti na delovanje in vpliv tujih obveščevalno-varnostnih služb;
- spremljanje in koordiniranje odpravljanja napak, pomanjkljivosti, kršitev in nepravilnosti v matičnih obveščevalno-varnostnih službah, ki jih odkrijejo pričujoči sistem, politika, izvajalci nadzora, ali službe same;
- javno priznanje kredibilnosti izvajalcev nadzora, kadar je nadzor ustrezno izveden;
- izpostavljanje uspehov in dosežkov matičnih obveščevalno-varnostnih služb (kadar je to mogoče in s tem nikogar/ničesar ne ogroža);
- objavljanje periodičnih publikacij (poročila, bilteni, zgibanke) s področja varnostne kulture, obveščevalno-varnostne dejavnosti, protiobveščevalne zaščite in drugih področij, ki bi pripomogla k uzaveščanju državljanov;

- sodelovanje z ostalimi podsistemi/deležniki modela zaupanja državljanov v matične obveščevalno-varnostne službe.

Izvajalci nadzora:

- izvajanje zakonitega, strokovnega, neodvisnega, nepristranskega in učinkovitega nadzora;
- delovanje v okviru danih pooblastil in predpisov;
- redno, objektivno, nepristransko in pravočasno poročanje o delu matičnih obveščevalno-varnostnih služb;
- izogibanje vrednostnim sodbam, »aferaštvu«, selektivnemu, pristranskemu, zavajajočemu ali pomanjkljivemu poročanju;
- posvetovanje s politiko, vodstvom matičnih obveščevalno-varnostnih služb in vodstvom nacionalnega obveščevalno-varnostnega sistema pred poročanjem javnosti o incidentih, napakah in aferah (namen je poiskati ustrezen način informiranja javnosti, ki bo najmanj škodljiv za službe in njihov ugled ter s tem zaupanje vanje);
- izpostavljanje uspehov in dosežkov matičnih obveščevalno-varnostnih služb, predvsem pa doseženih izboljšav ali odpravljenih pomanjkljivosti, napak ali kršitev (kadar je to mogoče in s tem nikogar/ničesar ne ogroža);
- zavedanje svojega položaja v »verigi zaupanja« in vpliva na državljane ter preprečevanje izkoriščanja in zlorabe takšnega vpliva;
- sodelovanje z mediji;
- medsebojno usklajevanje z drugimi izvajalci nadzora – predvsem z namenom, da ne preobremenijo služb (npr. z istočasno izvedenimi nadzori);
- pridobivanje usposobljenega kadra oziroma usposabljanje obstoječih nadzornikov, ki jim državljani zaupajo oziroma javnost zanje meni, da so kredibilni, strokovni, nepristranski in neodvisni;
- posvetovanje s strokovnjaki oziroma strokovno javnostjo, kadar je potrebno posebno znanje;
- izkazovanje spoštovanja in zaupanja do nadzorovanih subjektov in javnosti;

- sodelovanje z ostalimi podsistemi/deležniki modela-sistema zaupanja državljanov v matične obveščevalno-varnostne službe.

Mediji:

- objektivno in neškodljivo poročanje o ugotovitvah izvajalcev nadzora in izjavah politike, predstavnikov matičnih obveščevalno-varnostnih služb ter predstavnikov nacionalnega obveščevalno-varnostnega sistema;
- objavljanje novic, ki temeljijo na preverjenih dejstvih in podatkih iz zanesljivih virov;
- spoštovanje tajnosti in posebnosti ter občutljivosti obveščevalno-varnostnega področja;
- upoštevanje novinarske etike, ki je usklajena s spoštovanjem tajnosti, nacionalne varnosti in nacionalnih interesov;
- spoštovanje zaposlenih v matičnih obveščevalno-varnostnih službah, izvajalcev nadzora in politikov ter njihovega dela;
- izogibanje »aferaštvu« in selektivnemu, pristranskemu, zavajajočemu ali pomanjkljivemu poročanju;
- poročanje o preverjenih podatkih, ki temeljijo na preverjenih in zanesljivih virih;
- kritično preiskovanje delovanja matičnih obveščevalno-varnostnih služb, nacionalnega obveščevalno-varnostnega sistema, politike in izvajalcev nadzora;
- zavestno izogibanje izkoriščanju čustvenega ali drugega ranljivega stanja posameznika ali skupine oziroma družbe, manipulacije z njim/-i ter namernemu in načrtnemu oblikovanju javnega mnenja z neetičnim potvarjanjem ali prilagajanjem dejstev, zavajanjem, podpihovanjem ipd.;
- sodelovanje in posvetovanje s strokovnjaki oziroma strokovno javnostjo, kadar je potrebno posebno znanje za ustrezno medijsko poročanje ali delovanje;
- sodelovanje z ostalimi podsistemi/deležniki modela-sistema zaupanja državljanov v matične obveščevalno-varnostne službe.

Strokovna javnost:

- kritično spremljanje in/ali preučevanje/raziskovanje delovanja matičnih obveščevalno-varnostnih služb, nacionalnega obveščevalno-varnostnega sistema, politike in izvajalcev nadzora;
- seznanjanje javnosti z aktualnimi, relevantnimi in verodostojnimi podatki o delu matičnih obveščevalno-varnostnih služb, nacionalnega obveščevalno-varnostnega sistema, politike in izvajalcev nadzora;
- seznanjanje javnosti s stanjem ožjega in širšega varnostnega okolja;
- objavljanje prispevkov in raziskav s področja obveščevalno-varnostne dejavnosti;
- strokovno in objektivno argumentiranje dogodkov, okoliščin in dejstev, ki so povezani z obveščevalno-varnostno dejavnostjo doma in po svetu;
- spodbujanje kritičnega razmišljanja in kritične distance do aktualnih dogodkov (incidenti, afere, pojavi…), akterjev, okoliščin, dela matičnih obveščevalno-varnostnih služb, izvajalcev nadzora, politike itd.;
- spremljanje in raziskovanje področja zaupanja v matične obveščevalno-varnostne službe (ter tudi v izvajalce nadzora, politiko idr.);
- spremljanje in merjenje zaupanja državljanov v matične obveščevalno-varnostne službe ter analiziranje in ustrezne (nedvoumna) predstavitve dobljenih rezultatov;
- posredovanje rezultatov merjenja zaupanja državljanov v matične obveščevalno-varnostne službe politiki in vodstvu nacionalnega obveščevalno-varnostnega sistema;
- sodelovanje s politiko, izvajalci nadzora, nacionalnim obveščevalno-varnostnim sistemom in matičnimi obveščevalno-varnostnimi službami pri oblikovanju politik, smernic in standardov ter na področju razvoja znanj, kadrov, opreme in zmogljivosti;
- oblikovanje in izvedba izobraževanja politikov, izvajalcev nadzora, medijev in državljanov o obveščevalno-varnostni dejavnosti in zaupanju v tovrstne službe;
- oblikovanje in izvedba izobraževanja/usposabljanja ali sodelovanje z vodstvom služb pri izobraževanju/usposabljanju pripadnikov matičnih obveščevalno-varnostnih služb, kadar te potrebujejo specifična znanja;
- javno priznavanje kredibilnosti izvajalcev nadzora, kadar je nadzor po mnenju strokovne javnosti ustrezno izveden;

- argumentirano komentiranje uspehov in dosežkov matičnih obveščevalno-varnostnih služb, ki jih izpostavijo politika, predstavnik nacionalnega obveščevalno-varnostnega sistema ali izvajalci nadzora;
- kritično preučevanje aktualnih predpisov, smernic in prioritet na področju obveščevalno-varnostne dejavnosti;
- kritično preučevanje preteklosti, pojasnjevanje razlike med preteklostjo in sedanjostjo ter izpostavljanje preteklih dobrih in slabih praks;
- organizacija javnih posvetov, okroglih miz, konferenc in drugih javnih dogodkov na temo aktualnih oziroma perečih vprašanj, ki zadevajo tudi delovanje matičnih obveščevalno-varnostnih služb in nacionalnega, regionalnega ter mednarodnega varnostnega okolja;
- sodelovanje z ostalimi podsistemi/deležniki modela zaupanja državljanov v matične obveščevalno-varnostne službe.

Izobraževalni sistem:

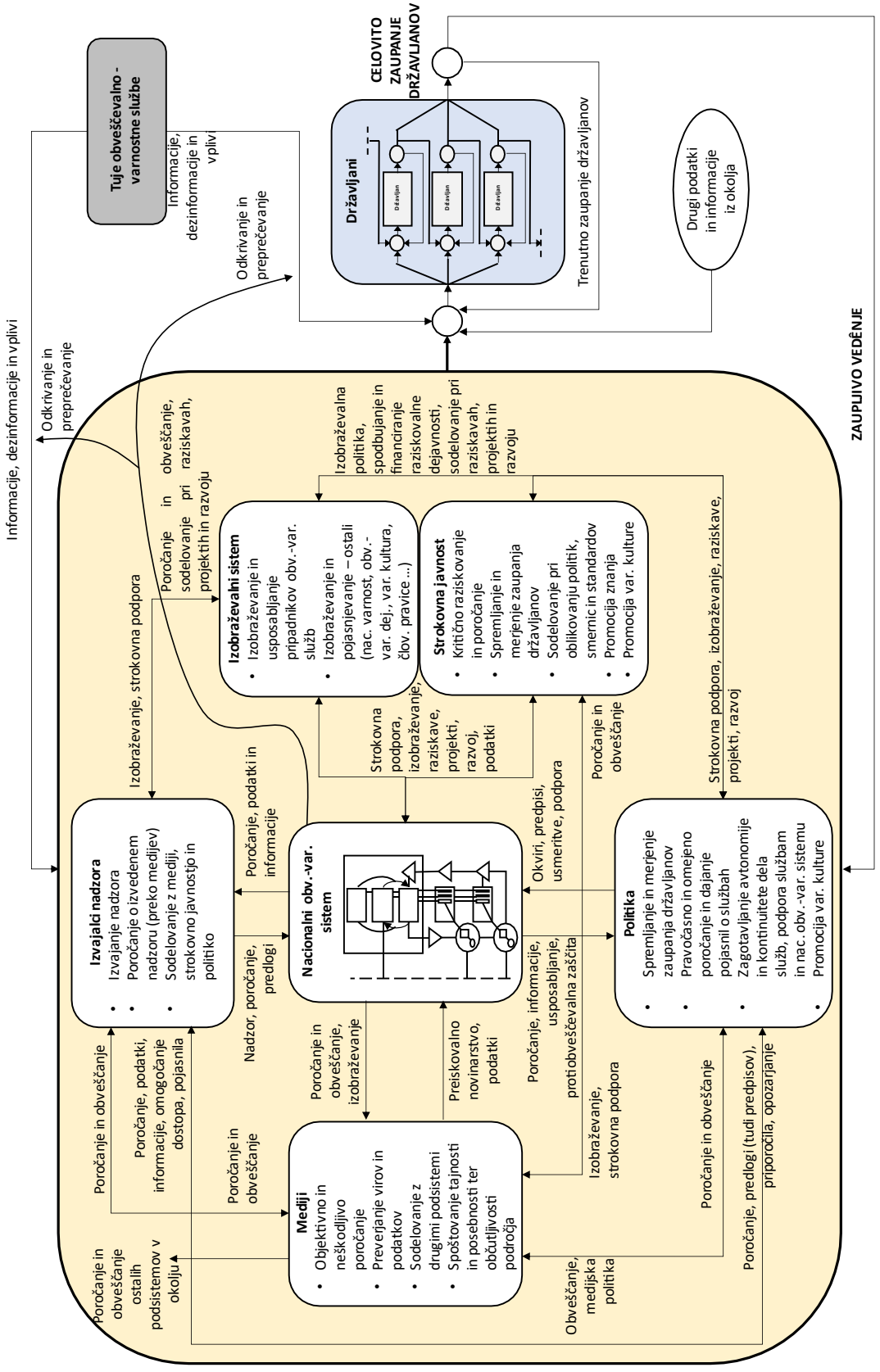
- izobraževanje politike, izvajalcev nadzora, medijev in državljanov;
- izobraževanje in usposabljanje pripadnikov matičnih obveščevalno-varnostnih služb, ko potrebujejo specifična znanja (informacijska tehnologija, strojništvo, elektrotehnika, psihologija, tuji jeziki, ekonomija, kulturologija idr.);
- posredovanje (državljanom) osnov o obveščevalno-varnostni dejavnosti, ključnih subjektih, ki izvajajo to dejavnost, njihovih pooblastilih in nalogah ter njihovi pomembnosti za obstoj in delovanje države;
- pojasnjevanje (državljanom) pomena in pomembnosti zaupanja v matične obveščevalno-varnostne službe;
- pojasnjevanje državljanom konkretnih posledic zaupanja in nezaupanja (ponazarjanje s praktičnimi primeri iz javno dostopne literature, novic, prakse ipd.);
- pojasnjevanje (državljanom) možnosti zlorabe služb za določene interese;
- spodbujanje kritičnega razmišljanja;
- opozarjanje na posledice prevelikega zanašanja na čustva (še posebej slepega zaupanja) ali na dokaze (dezinformiranje, zavajanje, manipulacija);

- predstavljanje (državljanom) organov za nadzor matičnih obveščevalno-varnostnih služb, njihovih vlog in nalog;
- izpostavljanje pomembnosti izvajalcev nadzora;
- izpostavljanje pomembnosti znanja pri ustvarjanju mnenja;
- izpostavljanje pomembnosti vidikov in dela strokovne javnosti;
- opozarjanje na vplive tujih obveščevalno-varnostnih služb;
- pojasnjevanje človekovih temeljnih pravic in svoboščin in meja delovanja matičnih obveščevalno-varnostnih službe na tem področju.

5.4 Model celovitega zaupanja državljanov v matične obveščevalno-varnostne službe

Na podlagi rezultatov dela, predstavljenega v prejšnjem podpoglavju, smo izgradili model celovitega zaupanja državljanov v matične obveščevalno-varnostne službe, ki ga prikazuje sika 5.12. Širše gledano ga sestavljajo tri sestavine: podsistem *Državljani*, podsistem *Tuje obveščevalno-varnostne službe* in *dialektični sistem podsistemov*, ki vplivajo na državljane (*Politika*, *Izvajalci nadzora*, *Strokovna javnost*, *Izobraževalni sistem*, *Mediji* in *Nacionalni obveščevalno-varnostni sistem*) in jim posredujejo informacije. Izmed vseh sestavin na sliki 5.12 je slednja največja in je zaradi boljše preglednosti obarvana z rumeno barvo. Te tri sestavine tvorijo dialektični sistem, ki ga prikazujemo z modelom celovitega zaupanja državljanov v matične obveščevalno-varnostne službe. Podsistem *Državljani* je sestavljen iz več podsistemov *Državljan*, kjer gre za medsebojni vpliv z lastnim zaupanjem in zaupljivim vedênjem. Ti različni medsebojni vplivi in zaupljiva vedênja skupaj tvorijo zaupanje javnosti. Prekinjena črta nakazuje, da je državljanov v podsistemu več, vendar smo jih za lažje razumevanje delovanja podsistema prikazali le nekaj.

Slika 5.12: Model celovitega zaupanja državljanov v matične obveščevalno-varnostne službe



Vir: Osebni vir

Državljani prejmejo podatke in informacije od tretje sestavine modela (tj. dialektičnega sistema podsistemov z vplivom ter podatki in informacijami), tujih služb in iz okolja ter jih vsak pri sebi skupaj s trenutno (individualno in družbeno) stopnjo zaupanja preoblikujejo (glej sliko 5.5) v celovito zaupanje. Do takšnega zaupanja pride, ker podsistemi v prej omenjenem sistemu med seboj sodelujejo na načine, ki jih določajo specifične smernice za delovanje modela iz podpoglavja 5.3.6. Smernice smo oblikovali ob upoštevanju teorij zaupanja, posebnosti obveščevalno-varnostnega področja, TVS/MVS, DTS in DOMR. Tuje obveščevalno-varnostne službe predstavljajo sestavino, ki negativno vpliva na proces presoje zaupanja državljanov in na delovanje celotnega sistema, obarvanega z rumeno barvo in njegovih podsistemov. Njihovo delovanje odkrivajo in preprečujejo (ali pa izkoriščajo – vendar tega nismo označili na sliki niti o tem nismo pisali) matične obveščevalno-varnostne službe. Ostale podsisteme v rumenem polju smo že posebej predstavili, le da v tem modelu delujejo v skladu z že omenjenimi smernicami za delovanje modela oziroma za ustvarjanje celovitega zaupanja državljanov v matične obveščevalno-varnostne službe.

Matične obveščevalno-varnostne službe na sliki 5.12 niso prikazane tako kot ostali podsistemi, temveč kot podsistemi S1 nacionalnega obveščevalno-varnostnega (pod)sistema. S tem se ne oddaljujemo od naslova doktorske disertacije ali od zastavljenega koncepta, temveč:

- upoštevamo, da zaupanje v posamezno službo vpliva na celoten podsistem in posredno tudi na sistem višjega reda ter da selektivno zaupanje v zgolj eno službo lahko negativno vpliva na celotni nacionalni obveščevalno-varnostni sistem;
- omogočamo, da nacionalni obveščevalno-varnostni (pod)sistem prevzame pomemben delež odgovornosti za zagotavljanje avtonomnosti, zakonitosti, legitimnosti, strokovnosti in (zadostne in potrebne) transparentnosti matičnih obveščevalno-varnostnih služb. S tem se povečata institucionalno (strukturna zagotovila in običajnost situacije) in medosebno zaupanje državljanov (integriteta, benevolenca, kompetentnost, predvidljivost, posledično pa tudi pripravljenost biti odvisen);
- omogočamo, da nacionalni obveščevalno-varnostni (pod)sistem prevzame pomemben del procesa vzpostavljanja in vzdrževanja stikov med službami in

državljani (obveščanje javnosti, neposredna komunikacija, dajanje pojasnil, dajanje informacij javnega značaja, organizacija dogodkov za javnost ipd.), koordinacijo ter zagotavljanje učinkovitejšega sodelovanja in komuniciranja tovrstnih služb med seboj ter z drugimi podsistemi in ostalimi deležniki.

S tega vidika predstavlja *Nacionalni obveščevalno-varnostni sistem* pomemben podsistem, ki skrbi za pravočasno, učinkovito in ustrezno delovanje matičnih obveščevalno-varnostnih služb zunaj in znotraj nacionalnega obveščevalno-varnostnega sistema ter njihovo sodelovanje z drugimi podsistemi zunaj in znotraj nacionalnega obveščevalno-varnostnega podsistema. Avtonomija matičnih obveščevalno-varnostnih služb, ki je povezana predvsem z njihovim delo(krogo)m, je še vedno nujno potrebna za izvajanje osnovnih procesov – brez tega ne bi bilo podlage za vzpostavitev in vzdrževanje zaupanja. Obstoj viabilnega sistema, ki »bdi« nad delovanjem in avtonomijo matičnih obveščevalno-varnostnih služb, namreč še ne pomeni odvzem odgovornosti službam, temveč jim omogoča nemoteno in ustrezno delovanje. Z vidika zaupanja je *Nacionalni obveščevalno-varnostni sistem* vmesnik in neke vrste »okolje«, ki zagotavlja ustrezne pogoje za razvoj celovitega zaupanja. Ostali podsistemi, kot so *Politika*, *Izvajalci nadzora*, *Strokovna javnost*, *Izobraževalni sistem* in *Mediji*, morajo posamično in skupaj z drugimi podsistemi usklajeno sodelovati na takšen način, da to »okolje« še naprej ostane ustrezno za razvoj celovitega zaupanja.

6 Logistika aplikacije modela in programoteka

Po predhodnih empiričnih raziskavah zaupanje v matične obveščevalno-varnostne službe ni visoko, zato ga je potrebno povečati in izdelati logistiko aplikacije modela, ki bo presegala metode odnosov z javnostmi. Zaradi narave dela obveščevalno-varnostnih služb je potrebno zagotoviti kontinuiteto njihovega dela, kar zahteva tudi kontinuiteto celovitega zaupanja. To lahko dosežemo le s celovitim modelom, z ustrezno logistiko aplikacije ter programoteko za samo aplikacijo. Z izrazom *logistika aplikacije* označujemo zadostno in potrebno celovito podprt postopek aplikacije oziroma uvedbe izbrane rešitve v prakso v skladu s programoteko (tj. model postopkov oziroma programov, kot jo opredeljujejo Mulej et al., 2000, str. 203). *Logistika aplikacije* ni nov pojem in je bil uporabljen tudi na drugih področjih (glej npr. Nu, 2009). Razložimo jo lahko kot opis logističnega procesa za aplikacijo nečesa (npr. stvar, proces, tehnologija, model) v/na izbrani subjekt/objekt, ustreznejša pa je opredelitev kot **zadostno in potrebno celovito podprt postopek aplikacije oziroma uvedbe izbrane rešitve v prakso v skladu s programoteko**. Da gre nedvomno za logistiko, potrjuje tudi definicija, da je logistika »znanstvena disciplina, ki interdisciplinarno in multidisciplinarno preučuje in uporablja zakonitosti planiranja, organiziranja, vodenja in kontrole tokov materiala, ljudi, energije in informacij v sistemih.« (Kramar, 2014, str. 64) Programoteka, v skladu s katero se aplicira model v prakso, je »dovolj celovito urejena zbirka podatkov, posvečena okvirnim programom za delovne postopke ustvarjalnih delovnih procesov. Uporabimo jo lahko (tudi in predvsem) za delo, ki ga ne narekujejo stroji, ampak lastna ustvarjalnost in izkušenost sodelavcev […].« (Mulej et al., 2008, str. 92)

Določen model je lahko dobro zastavljen in bi v praksi lahko prinesel pozitivne rezultate, vendar jih najverjetneje ne bi prinesel zaradi neustrezne aplikacije – vsaj ne v takšni meri. Modeli reform obveščevalno-varnostnih služb v tujih državah ne bodo nujno prinesli želenega uspeha, dokler bodo uporabljeni le kot grobi načrti, pravi Schreier (2005), saj imajo na modele prevelik vpliv zgodovinski, politični, strukturni, družbeni, lokalni in drugi specifični dejavniki (kar smo v disertaciji označili kot VKEN, op. G. H.). Preden se model aplicira v prakso, ga morajo uvajalci usvojiti in razumeti, saj bi nerazumevanje in

»šablonsko« prenašanje njegovih vsebin prineslo več negativnih kot pa pozitivnih posledic v praksi. Model je potrebno preučiti in se osredotočiti ne zgolj na njegovo strukturo, temveč tudi na okolje, v katerega se vpeljuje. Vse to je dokaz, da nista pomembni le vsebina in struktura modela, temveč tudi njegova aplikacija ob upoštevanju notranjega in zunanjega okolja.

Prepričani smo, da je od logistike aplikacije odvisno, kako uspešen oziroma učinkovit bo določen model v praksi. V našem primeru je od logistike aplikacije odvisno, kako uspešen bo model celovitega zaupanja državljanov v matične obveščevalno-varnostne službe v praksi, v ciljni državi. Potrebo po celoviti logistiki aplikacije potrjuje tudi praksa, o kateri smo že pisali v doktorski disertaciji in iz katere je razvidno, da države različno pristopajo k razreševanju različnih problemov znotraj obravnavane problematike, npr. z zakonodajo, parcialnimi ali začasnimi ukrepi, reorganizacijami, kadrovskimi, finančnimi ali drugimi ukrepi, redko pa zasledimo sistemski pristop k njihovem razreševanju. Veliko se izpostavlja tudi potrebo po dostopnosti obveščevalno-varnostnega sistema za javnost in transparentnost služb, s tem pa vključevanje javnosti oziroma državljanov v posredno oblikovanje nacionalnega obveščevalno-varnostnega sistema. »Zaradi vključevanja javnosti se poveča legitimnost odločitev in njihova socialna sprejemljivost. S tem se preprečuje nastajanje nesoglasij in sporov v družbi. […] Večja stopnja legitimnosti ima za posledico lažje izvajanje odločitev v praksi, saj subjekti sprejete odločitve boljše razumejo in jih podpirajo, kar vse zmanjšuje odtujenost državljanov od državne uprave.« (Igličar, 2009, str. 631) Tudi s tem, kar pravi Igličar, lahko ponovno utemeljimo našo trditev, da ima premalo ali nič znanja negativen vpliv na zaupanje državljanov v matične obveščevalno-varnostne službe. »Česar ne poznamo, je za nas na videz bolj kompleksno« (Rosi, 2019, osebni vir), zato se temu ljudje navadno težje približajo, nekateri imajo celo odpor do neznanega. »Za razumevanje in sprejemljivost predpisov v javnosti oziroma tako imenovani volilni bazi kaže povečati sodelovanje javnosti pri pripravi predlogov predpisov. S tem se poveča zaupanje javnosti, saj je prav nezaupanje javnosti pogosto eden izmed glavnih razlogov za čezmerno izdajanje predpisov.« (Igličar, 2009, str. 632) Participacija državljanov pri ustvarjanju zakonodaje je tako le eden od različnih dejavnikov, ki (lahko) povečajo zaupanje, ne pa edini. Naš model vsako obliko pozitivne

participacije državljanov, ki ima za posledico vzpostavljanje ali povečevanje celovitega zaupanja, prepoznava kot zaupljivo vedênje.

Participacijo javnosti – ne le državljanov, temveč tudi nevladnih organizacij, lobistov, aktivistov za človekove pravice, političnih strank, drugih strokovnjakov, zagovornikovposebnih interesov idr. – je kot pomemben element pri vnašanju sprememb oziroma reorganizaciji ali reformi obveščevalni-varnostnega sistema prepoznal tudi Schreier (2005). Kot pravi (ibidem, str. 154), je reformo potrebno opraviti na dveh različnih ravneh:

1. **Psihološka raven:** preseči kulturo strahu in skrivnostnosti z vzpostavitvijo zaupanja in več transparentnosti.
2. **Odgovornosti in nadzor:**
   - izboljšanje mehanizmov odgovornosti, zakonodajnega in pravosodnega nadzora nad obveščevalno-varnostnimi službami v okviru vladavine prava;
   - vodenje reforme mora priti z vrha, potrebna je močnejša vključenost izvršilne veje oblasti, ki mora dati z jasne smernice za sprejemanje in določanje odgovornosti ter koordiniranje služb;
   - vključevanje družbe v reformo, koordinacija in promocija pa bosta bolj učinkoviti, če bodo vanju vključeni vsi, tudi javnost, mediji in ostali podsistemi.

Med drugim opozarja (ibidem), da na reforme močno vplivajo mednarodne strukture, ki reformam ne smejo nasprotovati, sicer ne bodo prinesle želene viabilnosti in trajnosti. Treverton (2008, str. 44-47) predlaga, da bi bilo pri spremembi obveščevalno-varnostnega sistema potrebno prestrukturirati službe, povečati njihove vire, izboljšati sistem njihovega menedžmenta, izboljšati uporabo tehnologije in s tem produktivnost služb, izboljšati njihovo sodelovanje z drugimi organizacijami z ustanovitvijo koordinacijskih teles ali ustanovitvijo vodilnega organa, spremeniti predpise, izboljšati vodstvo služb, izboljšati politiko, ki jo službe uresničujejo, ter spremeniti kulturo s spodbudami in usposabljanjem posameznikov, ki povzročijo spremembe njihovega vedênja, za kar pa je potreben zagon z vrhov matičnih obveščevalno-varnostnih služb (in politike, op. G. H.).

OECD izpostavlja še en pomemben vidik. Izkušnje izvajalcev reforme varnostnega sektorja na Kosovu in v Sierra Leone kažejo, da je potrebno natančno in predhodno načrtovanje postopkov reforme, sicer pride do težkih zapletov, ter da je potrebno uporabiti multidisciplinarni team posameznikov z različnimi znanji (Organizacija za gospodarsko sodelovanje in razvoj, 2007). Z upoštevanjem DTS in USOMID/NOVOST smo sledili ne le navedenim priporočilom izvajalcev reforme, temveč tudi konceptu celovitosti, ki ga je mogoče doseči le s sodelovanjem generalistov in specialistov. Na drugi strani pa OECD opozarja na nujno vključenost posameznikov v mehanizme nadzora, ki jim lahko zaupajo tudi matične obveščevalno-varnostne službe. Kot navaja OECD (ibidem, str. 147), reforma obveščevalno-varnostnega sistema pogosto »*vključuje širitev kroga ljudi, ki jim službe zaupajo, da izvajajo nadzor. Zgodnje izkušnje pri odpiranju zunanjemu pregledu bodo ključnega pomena; naglica pri uvajanju odprtega nadzora nad posamezniki in institucijami, ki nimajo zaupanja ali niso kompetentni, pa bo verjetno kontraproduktivna. Koristno bi bilo delovati v fazah, kjer nadzor najprej izvajajo ugledni, nepristranski posamezniki (npr. kakšen sodnik, parlamentarec, akademik ali podobna oseba), preden se vloga razširi na širše institucije. Morda bi bilo koristno počakati* [s širjenjem nabora izvajalcev nadzora, op. G. H.]*, da reformni ukrepi ustvarijo sodstvo ali zakonodajno vejo oblasti, ki bo lahko izvajala kompetenten in odgovoren nadzor*.« Za učinkovito reformo sta potrebna tudi **odprta razprava** (s poudarkom, da morajo biti »reformirane« službe učinkovito nadzorovane, da ne postanejo orodje političnih ali drugih interesov) ter *učinkovit menedžment občutljivih zadev*, npr. kdo je ustrezen za delo v tovrstnih službah (prevladati morajo selekcijski postopki, kriteriji, predpisi in nadzor, ne pa politična pripadnost) (ibidem).

Omenili smo le nekaj mnenj, idej in predlogov, ki jih zasledimo v literaturi, kako spremeniti obveščevalno-varnostni sistem in s tem posredno izboljšati zaupanje državljanov v matične obveščevalno-varnostne službe. Navedene in druge predloge smo uporabili kot pomoč pri oblikovanju logistike aplikacije oziroma programoteke. Ta je nastala ob upoštevanju sistematične hevristike (Mulej, 1979), pravil DTS (Mulej, 1979; Mulej et al., 2000), DOMR (Rosi & Mulej, 2006; Rosi & Rosi, 2011; Rosi, 2015) in invencijsko-inovacijskega difuzijskega managementa (Mulej et al., 2008).

Programoteko sestavljajo **osnovni oziroma povezovalni program** (model splošnega, okvirnega postopka ustvarjalna miselnega dela), ki povezuje delne programe, in **delni programi** (posamezni koraki določenega dela programa). Osnovni program je mogoče primerjati s postopkom NOVOST (glej Mulej et al. 2000, str. 208, 210) in tudi z delom procesa razreševanja kompleksnih problematik z uporabo DOMR (glej Rosi, 2015). Pri osnovnem programu in pri povezovalnih programih nismo opredelili tistih stopenj v postopku oziroma posamičnih procesih aplikacije modela, ki vodijo v ustavitev postopka in prekinitev aplikacije (npr. ni odločitve, ni dejanja, ni podatkov). Razlog za to je v **odločitvi politike**, da se trenutno stanje sistema spremeni, zato (binarne) možnosti oziroma izbire, ali nekaj storiti ali ne, nismo predvideli, saj smo izhajali iz domnevne želje politike, da *se* stanje *spremeni* – na bolje.

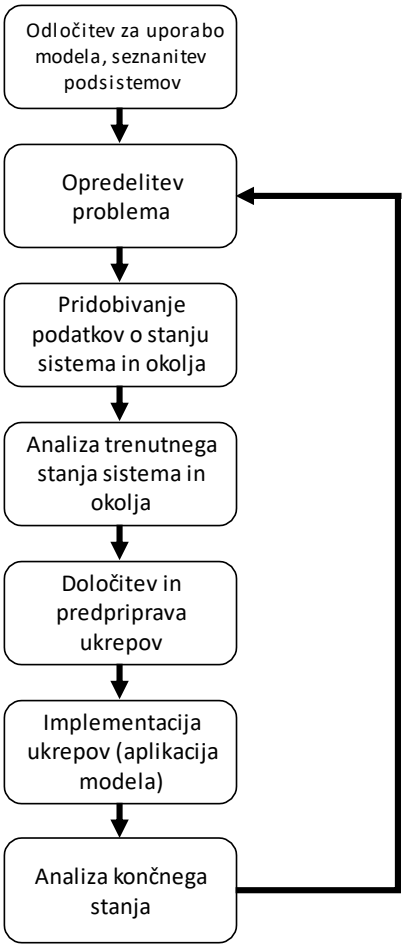
6.1 Osnovni program

Osnovni program logistike aplikacije modela, ki ga prikazuje slika 6.1, je razdeljen na 1 + 6 korakov. Prvi korak, *Korak 0*, sicer ni del postopka NOVOST, vendar smo ga dodali, ker je po našem mnenju potreben za začetek postopka NOVOST, ki se začne s korakom 1.

- **Korak 0**: Izbira in **odločitev politike za uporabo modela** celovitega zaupanja državljanov v matične obveščevalno-varnostne službe, **seznanitev** ostalih podsistemov z bistvom modela, **povabilo** ostalim podsistemom k sodelovanju pri nadaljnjih postopkih.
- **Korak 1**: Skupna **opredelitev problema –** obstoječi sistem ne omogoča dovolj celovitega zaupanja državljanov v matične obveščevalno-varnostne službe.
- **Korak 2**: **Pridobivanje podatkov** o trenutnem stanju sistema, njegovih podsistemov, njihovih povezavah, sinergijah in trenutnem stanju okolja (pri tem sodelujejo vsi podsistemi po korakih postopka NOVOST).
- **Korak 3**: **Analiza** trenutnega stanja sistema in okolja – iskanje kritičnih točk, pomanjkljivosti in razsežnosti problema, razlogov za odsotnost celovitega zaupanja in priložnosti s pomočjo modela celovitega zaupanja državljanov v matične obveščevalno-varnostne službe.
- **Korak 4**: **Določitev in predpriprava ukrepov**.

- **<u>Korak 5</u>**: **Implementacija ukrepov** (aplikacija modela).
- **<u>Korak 6</u>**: **Analiza končnega stanja** po implementaciji ukrepov in odločitev za morebitne nove ukrepe (dopolnjevanje, izboljševanje, vzdrževanje) – postopek sistematične hevristike: analiza (novega) procesa, optimizacija (novega) procesa in sinteza strukture (novega) procesa oziroma ustvarjanje (povsem) novega procesa (glej Mulej, 1979).

Slika 6.1: Osnovni program programoteke – logistike aplikacije celovitega modela zaupanja državljanov v matične obveščevalno-varnostne službe



Vir: Osebni vir

Pred korakom 1 je potrebno, da se politika odloči za uporabo modela celovitega zaupanja državljanov v matične obveščevalno-varnostne službe. Brez javnega spoznanja, da nekaj ni v redu, in odločitve, da se to spremeni, ni mogoče začeti postopka, zato je **politična volja** najpomembnejši dejavnik za samo logistiko aplikacije. Po odločitvi za

uporabo modela je potrebno ostale podsisteme obvestiti o nameri in jih seznaniti z bistvom modela ter odločitvijo politike za njegovo uporabo. Ob tem jih politika povabi k sodelovanju pri nadaljnjih postopkih aplikacije modela. Temu sledi skupna **opredelitev problema** v skladu s postopkom USOMID/NOVOST: *obstoječi sistem ne omogoča dovolj celovitega zaupanja državljanov v matične obveščevalno-varnostne službe*. S tem se predvsem politika pa tudi drugi podsistemi zavestno opredelijo, da trenutno stanje ne zadovoljuje želja, potreb oziroma nacionalnih interesov, zato je potrebno spremeniti sistem. Z vidika DTS je korak 1 tisti, ki v logistiki aplikacije modela predstavlja temelj uresničevanja 4. sestavine DTS (*materialističnost*): soočenje z resnico, prenehanje metanja peska v oči in sprejetje realnega stanja obliki, kakršno je.

Korak 2 predvideva zbiranje podatkov o trenutnem stanju sistema, njegovih podsistemih, njihovih povezavah, sinergijah, trenutnem stanju okolja, njegovih zmogljivostih itd. Namen tega koraka je pridobiti čim več *verodostojnih* in *zanesljivih* podatkov, ki bi jih bilo mogoče uporabiti v koraku 3. Tudi pri tem koraku (in kasneje pri korakih 3, 4 in 5) sodelujejo vsi podsistemi.

Korak 3 je kompleksen, saj zahteva dosledno, natančno in objektivno analizo zbranih podatkov ob upoštevanju vseh sestavin DTS. Od tega koraka je odvisno, kako bo tekel nadaljnji postopek, s tem pa uspešnost korakov 4 in 5. Koraka 1 ne smemo zamenjati s korakom 2 niti s korakom 3, saj gre pri koraku 2 za postopek zbiranja podatkov o trenutnem stanju z namenom kasnejše analize, pri koraku 3 pa za proces analize oziroma ugotavljanja stanja na podlagi zbranih podatkov, medtem ko pri koraku 1 le opredelimo problem in izhodišča, iz katerih izhaja logistika aplikacije modela.

Pri koraku 4 se oblikuje različne možne razrešitve problema, ki so v skladu z modelom celovitega zaupanja državljanov v matične obveščevalno-varnostne službe.

Te razrešitve so aplicirane v koraku 5, **da bi z njimi sistem postal podoben modelu** – s tem se želi subjekt, ki model aplicira, približati celovitosti sistema. Čeprav govorimo o aplikaciji modela, ga na sistem apliciramo z razreševanjem problemov, tj. z različnimi ukrepi. Razrešitve bi se morale v praksi razlikovati od države do države, razrešitve

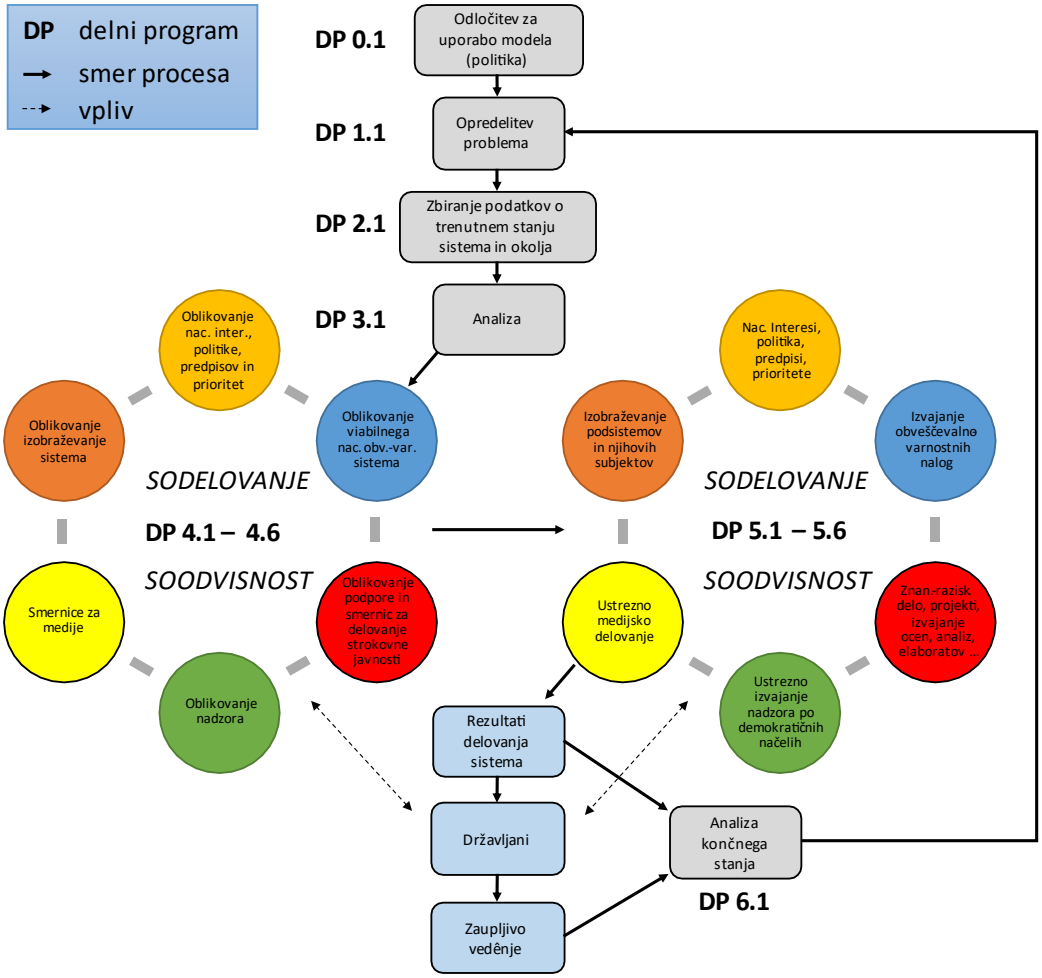
problema so lahko tudi različnega obsega, predviden čas aplikacije pa je ravno tako lahko različen. Vse je v veliki meri odvisno predvsem od kompleksnosti problema in dejanske in zaznane kompleksnosti aplikacije razrešitev.

V koraku 6 se pregleda rezultate celotnega procesa in preveri uspešnost »novega« sistema. Preveri se, kaj bi bilo mogoče izboljšati, kaj odstraniti, spremeniti, zamenjati. To je mogoče izvedeti na podlagi novega stanja sistema oziroma na podlagi podatkov in informacij, ki govorijo o novem sistemu. Pridobljeni podatki in informacije vstopijo v korak 1 kot povratne informacije o trenutnem stanju sistema, torej kot izhodišče/vhod za ponovno aplikacijo modela. Aplikacija modela namreč **ni enkratno dejanje**, temveč **ponavljajoči se postopek**. Ponavljanje aplikacije ne sme postati rutinski postopek, sicer lahko proces preide iz izboljševanja (rast in utrjevanje zaupanja), v stagniranje in propadanje, kar vodi v **pospešeno entropijo**. Vsaka nadaljnja aplikacija upočasnjuje entropijo sistema, ne more pa je popolnoma zaustaviti.

6.2 Delni programi

Slika 6.2 predstavlja potek posameznih delnih programov (v nadaljevanju: DP) znotraj osnovnega programa. DP 0 je posebnost, saj mora delovati le takrat, ko se model prvič aplicira na realni sistem. Predstavlja **zavestno odločitev in namero** politike (korak 0), da spremeni trenutno stanje, vendar problema, ki povzroča trenutno stanje, še ni dovolj celovito opredelila – za to potrebuje druge podsisteme. Od takrat dalje je namreč mogoče razumeti, da je odločitev za uporabo modela že sprejeta in je ni več potrebno ponovno sprejemati, saj so odločevalci videli pozitivne rezultate aplikacije modela.

Slika 6.2: DP logistike aplikacije celovitega modela zaupanja državljanov v matične obveščevalno-varnostne službe



Vir: Osebni vir

DP 0

1. Vhodne povezave	DKUM, ProQuest, drugi viri, ki razpolagajo z besedilom o modelu celovitega zaupanja državljanov v matične obveščevalno-varnostne službe
2. Vhodni dokument in informacije	Besedila o modelu celovitega zaupanja državljanov v matične obveščevalno-varnostne službe, podatki in raziskave o trenutni stopnji zaupanja državljanov v matične obveščevalno-varnostne službe
3. Vhodna informacijska dejavnost	Pridobivanje podatkov, mnenj, ocen
4. Temeljni proces obravnavanega dela celotnega procesa	**Osnovna analiza modela** (struktura, podsistemi, povezave, okolje, vhodi, izhodi) **in seznanitev z njegovimi značilnostmi ter skritimi ozadji, razmišljanje in diskusija, odločitev za uporabo modela**
5. Izhodna informacijska dejavnost	Obveščanje, seznanjanje, sporočanje
6. Izhodni dokument in informacije	Resolucija/strategija/namera o vzpostavitvi celovitega zaupanja državljanov v matične obveščevalno-varnostne službe, dokumenti s pojasnilom za odločitev, pozivi in vabila podsistemom za sodelovanje
7. Izhodne povezave	Strokovna javnost, nacionalni obveščevalno-varnostni sistem (matične obveščevalno-varnostne službe), izvajalci nadzora, izobraževalni sistem, mediji, državljani, na koncu DP 1

DP 1

1. Vhodne povezave	DP 0, strokovna javnost, nacionalni obveščevalno-varnostni sistem (in službe), izvajalci nadzora, izobraževalni sistem, mediji, državljani, kasneje tudi DP 6
2. Vhodni dokument in informacije	Resolucija/strategija/namera o povečanju zaupanja državljanov v matične obveščevalno-varnostne službe
3. Vhodna informacijska dejavnost	Branje, razmišljanje, pogovor, sestanek/seja, diskusija, anketa
4. Temeljni proces obravnavanega dela celotnega procesa	**Opredelitev problema** (v skladu s postopkom USOMID/NOVOST, DOMR): obstoječi sistem ne omogoča dovolj celovitega zaupanja državljanov v matične obveščevalno-varnostne službe
5. Izhodna informacijska dejavnost	Oblikovanje bistva zaznanega problema
6. Izhodni dokument in informacije	Opredeljeni problem, dokument z opredeljenim problemom
7. Izhodne povezave	DP 2, strokovna javnost, nacionalni obveščevalno-varnostni sistem (matične obveščevalno-varnostne službe), izvajalci nadzora, izobraževalni sistem, mediji, državljani

DP 2

1. Vhodne povezave	DP 1, politika, strokovna javnost, nacionalni obveščevalno-varnostni sistem (matične obveščevalno-varnostne službe), izvajalci nadzora, izobraževalni sistem, mediji, državljani
2. Vhodni dokument in informacije	Poročila, analize, ocene, napovedi, primerjave, bilance, ugotovitve, materialno stanje, kadrovsko stanje, rezultati delovne uspešnosti, število incidentov, ocena ogroženosti, varnostna ocena okolja idr.
3. Vhodna informacijska dejavnost	Razmišljanje, prebiranje, poslušanje, gledanje, iskanje, brskanje, poizvedovanje, posredovanje, pisanje, govorjenje, fotografiranje, snemanje
4. Temeljni proces obravnavanega dela celotnega procesa	**Ustanovitev osrednje (medresorske) skupine za oblikovanje zbirke podatkov, zbiranje podatkov o trenutnem stanju sistema, njegovih podsistemov, njihovih povezavah, sinergijah in trenutnem stanju okolja** (v skladu s postopkom USOMID/NOVOST, DOMR)
5. Izhodna informacijska dejavnost	Oblikovanje zbirke podatkov
6. Izhodni dokument in informacije	Zbirka podatkov o trenutnem stanju sistema in okolja
7. Izhodne povezave	Politika, strokovna javnost, nacionalni obveščevalno-varnostni sistem (matične obveščevalno-varnostne službe), izvajalci nadzora

DP 3

1. Vhodne povezave	Skupina za oblikovanje zbirke podatkov (glej DP 2)
2. Vhodni dokument in informacije	Zbirka podatkov
3. Vhodna informacijska dejavnost	Dostop do zbranih podatkov in njihovo pregledovanje
4. Temeljni proces obravnavanega dela celotnega procesa	**Analiza podatkov o trenutnem stanju sistema in okolja** (v skladu s postopkom USOMID/NOVOST, DOMR): iskanje kritičnih točk, pomanjkljivosti in razsežnosti problema ter razlogov za odsotnost celovitega zaupanja
5. Izhodna informacijska dejavnost	Oblikovanje ugotovitev na podlagi opravljene analize
6. Izhodni dokument in informacije	Poročilo (predlog: uporaba oznake stopnje tajnosti)
7. Izhodne povezave	Politika, strokovna javnost, nacionalni obveščevalno-varnostni sistem (matične obveščevalno-varnostne službe), izvajalci nadzora

DP 4.1., 4.2, 4.3, 4.4, 4.5 in 4.6 potekajo istočasno, posamično in skupaj. Ob tem je ključno upoštevanje njihove soodvisnosti ter soodvisnosti oblikovanih predlogov za razrešitev problema od predlogov za druge podsisteme, zato je sodelovanje nujno. Le na takšen način se je mogoče približati zadostni in potrebni celovitosti.

DP 4.1 (za politiko)

1. Vhodne povezave	DP 3, 4.2, 4.3, 4.4., 4.5 in 4.6
2. Vhodni dokument in informacije	Predlogi, smernice, dobre prakse, analize, poročila, statistike, ocene, ugotovitve, strokovna in znanstvena literatura, mednarodni dokumenti
3. Vhodna informacijska dejavnost	Analiziranje, primerjanje, vrednotenje, razvrščanje
4. Temeljni proces obravnavanega dela celotnega procesa	**Oblikovanje nacionalnih interesov, politike, predpisov in prioritet (v skladu s postopkom USOMID/NOVOST, DOMR):** • oblikovanje okvirjev in postopkov za spremljanje in nadzorovanje dela nacionalnega obveščevalno-varnostnega sistema in njegovih podsistemov pri zasledovanju nacionalnih interesov ter upoštevanju predpisov in prioritet; • oblikovanje postopkov za spremljanje in merjenje zaupanja državljanov; • oblikovanje predpisov za zagotavljanje avtonomije in kontinuitete dela služb; • oblikovanje predpisov s področja pooblastil matičnih obveščevalno-varnostnih služb; • oblikovanje predpisov, proračuna in drugih sredstev ter določitev aktivnosti in smernic za podporo nacionalnemu obveščevalno-varnostnemu sistemu (materialno, finančno, kadrovsko, tehnološko, medijsko); • oblikovanje strategije in ključnih smernic za promocijo varnostne kulture; • oblikovanje predpisov s področja varnostnega preverjanja (tudi izvajalcev nadzora); • oblikovanje predpisov in določitev smernic za podporo strokovne javnosti (materialno, finančno, kadrovsko, tehnološko, medijsko); • oblikovanje predpisov in postopkov za spremljanje izvrševanja in upoštevanja medijske politike; • oblikovanje predpisov, ki urejajo področje »žvižgačev«; • oblikovanje predpisov in postopkov za spremljanje rezultatov politike izobraževanja; • oblikovanje postopkov, priporočil, smernic in načrtov za pravočasno in ustrezno poročanje zainteresiranim javnostim ter dajanje pojasnil o matičnih obveščevalno-varnostnih službah in nacionalnem obveščevalno-varnostnem sistemu; • drugo.
5. Izhodna informacijska dejavnost	Oblikovanje, urejanje, distribucija, obveščanje
6. Izhodni dokument in informacije	Izoblikovani nacionalni interesi, politike, predpisi, načrti in prioritete
7. Izhodne povezave	DP 4.2, 4.3, 4.4., 4.5, 4.6 in na koncu 5.1

DP 4.2 (za nacionalni obveščevalno-varnostni sistem in matične obveščevalno-varnostne službe)

1. Vhodne povezave **2. Vhodni dokument in informacije**	DP 3, 4.1, 4.3, 4.4., 4.5 in 4.6 Predlogi, smernice, dobre prakse, analize, poročila, statistike, ocene, ugotovitve, strokovna in znanstvena literatura, mednarodni dokumenti
3. Vhodna informacijska dejavnost	Analiziranje, primerjanje, vrednotenje, razvrščanje
4. Temeljni proces obravnavanega dela celotnega procesa	**Oblikovanje viabilnega nacionalnega obveščevalno-varnostnega sistema (v skladu s postopkom USOMID/NOVOST, DOMR in TVS/MVS):** • določitev ustreznih podsistemov in zagotovitev ustreznih zmogljivosti (finančne, kadrovske, materialne idr.); • določitev pogojev za avtonomno delovanje vseh podsistemov nacionalnega obveščevalno-varnostnega sistema; • razmejitev pristojnosti različnih matičnih obveščevalno-varnostnih služb ter preprečevanje prekrivanja/podvajanja njihovega delokroga; • oblikovanje predpisov in usposabljanja za izvajanje obveščevalno-varnostnih nalog na strokoven, etičen, legitimen način; • oblikovanje strategije za pridobitev novega, mlajšega in strokovnega kadra za dolgoročno zaposlitev; • oblikovanje ukrepov, usposabljanja in dejavnikov delovnega okolja za učinkovitejše zagotavljanje tajnosti zadev in aktivnosti znotraj matičnih obveščevalno-varnostnih služb; • oblikovanje smernic za učinkovito koordiniranje matičnih obveščevalno-varnostnih služb in skupnih operacij (tudi z drugimi, zunanjimi organi izven nacionalnega obveščevalno-varnostnega sistema); • priprava smernic in priporočil za usklajevanje prioritet politike z nalogami in cilji matičnih obveščevalno-varnostnih služb; • določitev ključnih aktivnosti in prioritet na področju promocije varnostne kulture; • oblikovanje postopkovnika, priporočil in dobrih praks za odpravljanje napak, pomanjkljivosti, kršitev in nepravilnosti, ki jih odkrije nadzor; • oblikovanje aktivnosti in smernic za promocijo in spodbujanje sprejemanja odgovornosti za odkrite napake, pomanjkljivosti, kršitve in nepravilnosti; • oblikovanje sistema nagrajevanja in motiviranja uslužbencev matičnih obveščevalno-varnostnih služb; • predlogi ukrepov za izboljšanje zaščite identitete uslužbencev matičnih obveščevalno-varnostnih služb pred razkritjem;

	• priprava gradiva za uzaveščanje državljanov o obveščevalno-varnostni dejavnosti in z njo povezanimi aktualnimi problemi; • oblikovanje načrta in gradiv za opozarjanje javnosti na vpliv tujih obveščevalno-varnostnih služb; • oblikovanje strategije za vzdrževanje ugleda služb in vzdrževanje stikov z drugimi podsistemi; • vzpostavitev sistema in postopkov za spremljanje stanja zaupanja državljanov v matične obveščevalno-varnostne službe; • priprava ukrepov za transparentno delovanje služb skupaj s politiko, izvajalci nadzora in strokovno javnostjo; • priprava strategije, načrta in konkretnih ukrepov za sodelovanje s politiko, mediji, strokovno javnostjo, izobraževalnim sistemom, izvajalci nadzora in državljani (dialog, skupne aktivnosti); • oblikovanje strategije obveščanja javnosti o lastnih aktivnostih in stanjem varnosti okolja (npr. periodična poročila, spletna stran); • drugo (odvisno od države/okolja).
5. Izhodna informacijska dejavnost	Oblikovanje, urejanje, distribucija, obveščanje
6. Izhodni dokument in informacije	Model viabilnega nacionalnega obveščevalno-varnostnega sistema
7. Izhodne povezave	DP 4.1, 4.3, 4.4., 4.5, 4.6 in na koncu 5.2

DP 4.3 (za strokovno javnost)

1. Vhodne povezave	DP 3, 4.1, 4.2, 4.4., 4.5 in 4.6
2. Vhodni dokument in informacije	Predlogi, smernice, dobre prakse, analize, poročila, statistike, ocene, ugotovitve, strokovna in znanstvena literatura, mednarodni dokumenti
3. Vhodna informacijska dejavnost	Analiziranje, primerjanje, vrednotenje, razvrščanje
4. Temeljni proces obravnavanega dela celotnega procesa	**Oblikovanje podpore in smernic za delovanje strokovne javnosti oziroma njenega znanstvenoraziskovalnega dela, kritičnega ocenjevanja delovanja podsistemov in opozarjanja/spodbujanja laične javnosti** (v skladu s postopkom USOMID/NOVOST, DOMR): • smernice za strokovno, nepristransko in etično znanstveno-raziskovalno delo, izvedbo projektov in drugih podobnih znanstveno-raziskovalnih aktivnosti – samostojno in skupaj z drugimi podsistemi modela-sistema; • nabor ukrepov za spodbujanje podsistemov k javni razpravi o aktualnih temah in problemih s področja obveščevalno-varnostne dejavnosti; • oblikovanje konceptov za izvedbo konferenc, okroglih miz, diskusij in drugih podobnih (javnih) srečanj z namenom

	iskanja razrešitev za aktualne/pogoste/izpostavljene probleme; • nabor ukrepov za širjenje in promocijo znanja o obveščevalno-varnostnem področju; • osnutek sistema in aktivnosti za raziskovanje, spremljanje in merjenje zaupanja državljanov v matične obveščevalno-varnostne službe; • nabor ukrepov za spodbujanje kritičnega razmišljanja in kritične analize aktualnih dogodkov (incidenti, afere, varnostni pojavi …), akterjev, okoliščin, dela matičnih obveščevalno-varnostnih služb, izvajalcev nadzora, politike itd.; • oblikovanje strategij, smernic, ukrepov in spodbud za multidisciplinarno povezovanje in znanstveno-raziskovalne dejavnosti; • oblikovanje smernic za sistemski pristop k raziskovanju; • drugo (odvisno od države/okolja).
5. Izhodna informacijska dejavnost	Oblikovanje, urejanje, distribucija, obveščanje
6. Izhodni dokument in informacije	Smernice in ukrepi za podporo in učinkovito delovanje strokovne javnosti
7. Izhodne povezave	DP 4.1, 4.2, 4.4., 4.5, 4.6 in na koncu 5.3

DP 4.4 (za medije)

1. Vhodne povezave	DP 3, 4.1, 4.2, 4.3., 4.5 in 4.6
2. Vhodni dokument in informacije	Predlogi, smernice, dobre prakse, analize, poročila, statistike, ocene, ugotovitve, strokovna in znanstvena literatura, mednarodni dokumenti
3. Vhodna informacijska dejavnost	Analiziranje, primerjanje, vrednotenje, razvrščanje
4. Temeljni proces obravnavanega dela celotnega procesa	**Oblikovanje smernic za ustrezno medijsko delovanje** (v skladu s postopkom USOMID/NOVOST, DOMR): • oblikovanje strategije in smernic za vzpostavitev kritičnih, objektivnih, etičnih in neodvisnih medijev; • oblikovanje smernic za objektivno poročanje in uporabo nepristranskega jezika/izrazoslovja; • oblikovanje novinarskega kodeksa; • organizacija usposabljanja za delovanje v skladu z novinarskim kodeksom; • oblikovanje načrta za vzpostavitev/okrepitev vloge organa/organov za presojo delovanja medijev v skladu z novinarskim kodeksom (razsodišča, komisije …); • oblikovanje smernic za ustrezno vrednotenje podatkov in informacij z namenom zmanjšanja lažnega, napačnega ali pomanjkljivega poročanja;

	• prepoznava in določitev konkretnih potreb ter ukrepov za sodelovanje z vsemi podsistemi, ki so vključeni v ta model-sistem; • ugotovitev potreb po pridobitvi znanja/usposabljanju tistih, ki medijsko pokrivajo področje nacionalne varnosti, o organizaciji nacionalne varnosti (vključno z izvajalci nadzora), nacionalnih interesih, tajnosti in tajnih podatkih ter vlogi medijev; • drugo (odvisno od države/okolja).
5. Izhodna informacijska dejavnost	Oblikovanje, urejanje, distribucija, obveščanje
6. Izhodni dokument in informacije	Smernice in ukrepi za ustrezno medijsko delovanje
7. Izhodne povezave	DP 4.1, 4.2, 4.3., 4.5, 4.6 in na koncu 5.4

DP 4.5 *(za izobraževalni sistem)*

1. Vhodne povezave	DP 3, 4.1, 4.2, 4.3., 4.4 in 4.6
2. Vhodni dokument in informacije	Predlogi, smernice, dobre prakse, analize, poročila, statistike, ocene, ugotovitve, strokovna in znanstvena literatura, mednarodni dokumenti
3. Vhodna informacijska dejavnost	Analiziranje, primerjanje, vrednotenje, razvrščanje
4. Temeljni proces obravnavanega dela celotnega procesa	**Preoblikovanje izobraževalnega sistema** (v skladu s postopkom USOMID/NOVOST, DOMR): • oblikovanje učnih načrtov in vsebin za izobraževanje politike, izvajalcev nadzora, medijev in državljanov o področju nacionalnega obveščevalno-varnostnega sistema in obveščevalno-varnostne dejavnosti (splošno), o človekovih pravicah in temeljnih svoboščinah (v povezavi z nacionalno varnostjo), o vrstah in funkcijah nadzora matičnih obveščevalno-varnostnih služb in o zaupanju v te službe; • oblikovanje učnih načrtov in vsebin za izobraževanje in usposabljanje pripadnikov matičnih obveščevalno-varnostnih služb, ko potrebujejo specifična znanja (informacijska tehnologija, strojništvo, elektrotehnika, psihologija, tuji jeziki, ekonomija, kulturologija idr.); • oblikovanje učnih metod in delovnih navad za spodbujanje kritičnega razmišljanja in delovanja; • oblikovanje metod za spremljanje in merjenje stopnje znanja s tega področja; • sodelovanje izobraževalnega sistema z ostalimi podsistemi pri kreiranju promocije in diseminacije znanj (predvsem z mediji); • drugo (odvisno od države/okolja).
5. Izhodna informacijska dejavnost	Oblikovanje, urejanje, distribucija, obveščanje
6. Izhodni dokument in informacije	Smernice in ukrepi za preoblikovanje izobraževalnega sistema

7. Izhodne povezave	DP 4.1, 4.2, 4.3., 4.4, 4.6 in na koncu 5.5

DP 4.6 (za izvajalce nadzora)

1. Vhodne povezave **2. Vhodni dokument in informacije**	DP 3, 4.1, 4.2, 4.3., 4.4 in 4.5 Predlogi, smernice, dobre prakse, analize, poročila, statistike, ocene, ugotovitve, strokovna in znanstvena literatura, mednarodni dokumenti
3. Vhodna informacijska dejavnost	Analiziranje, primerjanje, vrednotenje, razvrščanje
4. Temeljni proces obravnavanega dela celotnega procesa	**Oblikovanje smernic in ukrepov za vzpostavitev in ustrezno izvajanje zakonitega, strokovnega, neodvisnega, nepristranskega in učinkovitega nadzora** (v skladu s postopkom USOMID/NOVOST, DOMR): • oblikovanje politik, smernic in navodil za redno, objektivno, nepristransko in pravočasno poročanje o delu matičnih obveščevalno-varnostnih služb; • sodelovanje pri oblikovanju predpisov za varnostno preverjanje izvajalcev nadzora (z možnostjo izjem); • priprava etičnega kodeksa za delo izvajalcev nadzora; • oblikovanje učnih vsebin (skupaj z drugimi podsistemi) za objektivno, omejeno, pravočasno in neškodljivo poročanje o delu matičnih obveščevalno-varnostnih služb oziroma nacionalnega obveščevalno-varnostnega podsistema; • oblikovanje učnih vsebin (skupaj z drugimi podsistemi) s področja veljavnega pravnega reda, človekovih pravic in svoboščin in upoštevanja tega pri izvajanju nadzora; • prepoznava in določitev konkretnih potreb in ukrepov za sodelovanje z vsemi podsistemi, ki so vključeni v ta model-sistem; • oblikovanje ukrepov za pridobivanje in posodabljanje znanj, potrebnih za učinkovito in ustrezno izvajanje nadzora; • oblikovanje strategije za pridobivanje usposobljenega kadra/usposabljanje obstoječih izvajalcev nadzora, ki jim javnost, politika in službe zaupajo; • določitev navodil in smernic za sodelovanje z drugimi izvajalci nadzora (v katerih primerih, na kakšen način idr.) • drugo (odvisno od države/okolja).
5. Izhodna informacijska dejavnost **6. Izhodni dokument in informacije**	Oblikovanje, urejanje, distribucija, obveščanje Smernice in ukrepi za vzpostavitev ter ustrezno izvajanje zakonitega, strokovnega, neodvisnega, nepristranskega in učinkovitega nadzora
7. Izhodne povezave	DP 4.1, 4.2, 4.3., 4.4, 4.5 in na koncu 5.6

Tako kot DP 4.1., 4.2, 4.3, 4.4, 4.5 in 4.6 tudi DP 5.1, 5.2, 5.3, 5.4, 5.5 in 5.6 potekajo istočasno, posamično in skupaj v sodelovanju in z upoštevanjem njihove soodvisnosti ter soodvisnosti vseh implementiranih ukrepov za razrešitev problema.

DP 5.1 (za politiko)

1. Vhodne povezave **2. Vhodni dokument in informacije**	DP 4.1, 5.2, 5.3, 5.4, 5.5 in 5.6 Izbrani/določeni predlogi nacionalnih interesov, politik, predpisov, načrtov in prioritet
3. Vhodna informacijska dejavnost	Sprejemanje, razvrščanje, posredovanje
4. Temeljni proces obravnavanega dela celotnega procesa	**Implementacija nacionalnih interesov, politik, predpisov in prioritet in aktivnosti, ki spremljajo njihovo realizacijo**: • spremljanje in nadzorovanje dela nacionalnega obveščevalno-varnostnega sistema in njegovih podsistemov pri zasledovanju nacionalnih interesov in upoštevanju predpisov in prioritet; • spremljanje in merjenje zaupanja državljanov ter ustrezno ukrepanje v primeru upada zaupanja; • poudarjanje pomena zaupanja državljanov v matične obveščevalno-varnostne službe; • implementacija predpisov za področje pooblastil matičnih obveščevalno-varnostnih služb; • zagotavljanje avtonomije in kontinuitete dela služb; • nudenje podpore (finančne, kadrovske, materialne, organizacijske, komunikacijske, koordinacijske…) nacionalnemu obveščevalno-varnostnemu sistemu (in njegovim podsistemom); • promocija varnostne kulture; • uvedba varnostnega preverjanja izvajalcev nadzora (z možnostjo izjem); • ureditev in nadzor izvajanja politike in predpisov na področju delovanja medijev; • ureditev in nadzor izvajanja politike in predpisov na področju »žvižgačev«; • ureditev in nadzor izvajanja politike in predpisov na področju nadzora obveščevalno-varnostnih služb; • opozarjanje na vpliv tujih obveščevalno-varnostnih služb; • podpora strokovni javnosti in izobraževalnemu sistemu (materialna, finančna, kadrovska, tehnološka, medijska …); • ureditev in nadzor izvajanja medijske politike (izogibanje cenzuri); • spremljanje rezultatov politike izobraževanja in usposabljanja; • pravočasno, objektivno in resnično poročanje in dajanje pojasnil o nacionalnem obveščevalno-varnostnem sistemu, njegovih podrejenih službah in varnostnih dogodkih (kadar je to mogoče in dovoljeno); • izpostavljanje uspehov matičnih obveščevalno-varnostnih služb in celotnega nacionalnega obveščevalno-varnostnega sistema (kadar je to mogoče in dovoljeno); • drugo (odvisno od države/okolja).

5. Izhodna informacijska dejavnost	Sprejemanje in izdajanje zakonskih in podzakonskih aktov, zapovedovanje, predpisovanje, napotitev, poročanje, obveščanje, opozarjanje, sporočanje, ukazovanje, odrejanje, delegiranje, tolmačenje
6. Izhodni dokument in informacije	Posamični dokumenti za implementacijo nacionalnih interesov, politik, predpisov, načrtov in prioritet (npr. zakonski in podzakonski akti, usmeritve, navodila, priporočila, strategije, resolucije), izjave za javnost/medije
7. Izhodne povezave	DP 5.2, 5.3, 5.4, 5.5, 5.6, na koncu DP 6, vsi podsistemi

DP 5.2 (za nacionalni obveščevalno-varnostni sistem in matične obveščevalno-varnostne službe)

1. Vhodne povezave	DP 4.2, 5.1, 5.3, 5.4, 5.5 in 5.6
2. Vhodni dokument in informacije	Izbrani/določeni predlogi za vzpostavitev viabilnega nacionalnega obveščevalno-varnostnega sistema (zakonski in podzakonski akti, navodila, smernice, usmeritve, primeri dobre prakse ipd.)
3. Vhodna informacijska dejavnost	Obravnava predlogov (tj. navodil, smernic, usmeritev in drugih dokumentov, prioritet), sestanki, seje, izobraževanja in usposabljanja
4. Temeljni proces obravnavanega dela celotnega procesa	**Vzpostavitev viabilnosti in vzdrževanje viabilnega nacionalnega obveščevalno-varnostnega sistema v praksi**: • vzpostavitev in zagotavljanje ustreznih pogojev za avtonomno delovanje matičnih obveščevalno-varnostnih služb; • izvajanje in nadzorovanje izvajanja obveščevalno-varnostnih nalog na strokoven, etičen, legitimen način; • pridobivanje novega, mlajšega in strokovnega kadra za dolgoročno zaposlitev; • zagotavljanje tajnosti lastnih zadev in aktivnosti ter nadzorovanje izvajanja tega; • koordiniranje matičnih obveščevalno-varnostnih služb in skupnih operacij (tudi z drugimi, zunanjimi organi izven nacionalnega obveščevalno-varnostnega sistema); • usklajevanje prioritet politike z nalogami in cilji matičnih obveščevalno-varnostnih služb; • delovanje na področju zagotavljanja nacionalnih interesov in varovanja ustavne ureditve ter nacionalne varnosti, promocija varnostne kulture; • odpravljanje napak, pomanjkljivosti, kršitev in nepravilnosti, ki jih odkrije nadzor, ter sprejemanje odgovornosti zanje; • primerno nagrajevanje in motiviranje uslužbencev matičnih obveščevalno-varnostnih služb za njihovo delo; • zaščita identitete uslužbencev matičnih obveščevalno-varnostnih služb pred razkritjem;

	• opozarjanje javnosti na vpliv tujih obveščevalno-varnostnih služb; • vzdrževanje ugleda služb, vzdrževanje stikov z drugimi podsistemi – predvsem z javnostjo (z vidika zaupanja); • spremljanje stanja zaupanja državljanov v matične obveščevalno-varnostne službe; • vzpostavitev ustrezne stopnje transparentnosti delovanja skupaj s politiko, izvajalci nadzora in strokovno javnostjo; • sodelovanje s politiko, mediji, strokovno javnostjo, izobraževalnim sistemom, izvajalci nadzora in državljani (dialog, skupne aktivnosti); • izogibanje zavajanju pri komunikaciji z drugimi podsistemi (razen v izjemnih primerih, ko to dopušča zakonodaja); • obveščanje javnosti o lastnih aktivnostih in stanju varnosti okolja (npr. periodična poročila, spletna stran) – kolikor je to dovoljeno in potrebno; • promocija lastnih dosežkov in aktivnosti – kolikor je to dovoljeno in potrebno; • objava gradiva (zgibanke, spletni oglasi, video posnetki, drugo tiskano gradivo) za uzaveščanje državljanov o obveščevalno-varnostni dejavnosti in s tem področjem povezanimi aktualnimi problemi; • drugo (odvisno od države/okolja).
5. Izhodna informacijska dejavnost	Poročanje, obveščanje, posredovanje in plasiranje podatkov, informacij, dezinformacij in drugih gradiv, tiskovne konference, seje, sestanki, simpoziji, konference
6. Izhodni dokument in informacije	Podatki, informacije in dezinformacije (pisno, ustno, zvočno, slikovno ali video gradivo), poročila, zapisniki, elaborati, operativno gradivo, druga vrsta dokumentacije oziroma gradiv
7. Izhodne povezave	DP 5.1, 5.3, 5.4, 5.5, 5.6, na koncu DP 6, vsi podsistemi

DP 5.3 (za strokovno javnost)

1. Vhodne povezave	DP 4.3, 5.1, 5.2, 5.4, 5.5 in 5.6
2. Vhodni dokument in informacije	Predlogi za podporo (in razvoj) strokovne javnosti, strategije, načrti
3. Vhodna informacijska dejavnost	Zbiranje podatkov in informacij, analiza predlogov, predpisov, strategij in načrtov
4. Temeljni proces obravnavanega dela celotnega procesa	**Znanstveno-raziskovalno delo, kritično ocenjevanje in opozarjanje/spodbujanje laične javnosti**: • izvedba znanstveno-raziskovalnega dela, projektov in drugih podobnih znanstveno-raziskovalnih aktivnosti – samostojno in skupaj z drugimi podsistemi; • spodbujanje podsistemov (predvsem državljanov) k javni razpravi o aktualnih temah in problemih s področja obveščevalno-varnostne dejavnosti;

	• organizacija konferenc, okroglih miz, diskusij in drugih podobnih (javnih) srečanj z namenom iskanja razrešitev za aktualne/pogoste/izpostavljene probleme; • aktivno širjenje in promocija znanja z obravnavanega področja; • raziskovanje, spremljanje in merjenje zaupanja državljanov v matične obveščevalno-varnostne službe; • posredovanje rezultatov merjenja zaupanja državljanov v matične obveščevalno-varnostne službe, politiki in vodstvu nacionalnega obveščevalno-varnostnega sistema; • kritično preučevanje/raziskovanje delovanja matičnih obveščevalno-varnostnih služb, nacionalnega obveščevalno-varnostnega sistema, politike in izvajalcev nadzora; • seznanjanje javnosti z aktualnimi, relevantnimi in verodostojnimi podatki o delu matičnih obveščevalno-varnostnih služb, nacionalnega obveščevalno-varnostnega sistema, politike, izvajalcev nadzora ter tudi medijev in izobraževalnega sistema; • seznanjanje javnosti s stanjem ožjega in širšega varnostnega okolja ter stopnjo (zaznavanja) varnostne kulture; • strokovna in objektivna argumentacija dogodkov, okoliščin in dejstev povezanih z obveščevalno-varnostno dejavnostjo doma in po svetu; • spodbujanje kritičnega razmišljanja in kritične distance do aktualnih dogodkov (incidenti, afere, varnostni pojavi …), akterjev, okoliščin, dela matičnih obveščevalno-varnostnih služb, izvajalcev nadzora, politike itd.; • sodelovanje s politiko, izvajalci nadzora, nacionalnim obveščevalno-varnostnim sistemom in matičnimi službami pri oblikovanju politik, smernic in standardov ter razvoju znanj, kadrov, opreme in zmogljivosti; • argumentirano komentiranje uspehov in dosežkov matičnih obveščevalno-varnostnih služb, ki jih izpostavijo politika, predstavnik nacionalnega obveščevalno-varnostnega sistema ali izvajalci nadzora; • argumentirano in konstruktivno komentiranje neuspehov in napak matičnih obveščevalno-varnostnih služb, ki jih izpostavijo politika, predstavnik nacionalnega obveščevalno-varnostnega sistema ali izvajalci nadzora; • kritično preučevanje aktualnih predpisov, smernic, navodil in prioritet na področju obveščevalno-varnostne dejavnosti (tudi tujih); • kritično preučevanje preteklosti na področju obveščevalno-varnostne dejavnosti v nacionalnem, regionalnem in mednarodnem okolju, pojasnjevanje razlik med preteklostjo in sedanjostjo ter izpostavljanje dobre in slabe prakse iz preteklosti; • drugo (odvisno od države/okolja).

5. Izhodna informacijska dejavnost	Obveščanje/poročanje, založniška dejavnost/objavljanje v revijah in drugih virih, posredovanje, poučevanje, izobraževanje, usposabljanje, izvedba sestankov, delavnic, izobraževalnih dogodkov, okroglih miz, konferenc ipd.
6. Izhodni dokument in informacije	Poročila, rezultati analiz in raziskav, projektna dokumentacija, načrti, elaborati, znanstveni in strokovni prispevki, promocijsko gradivo, pojasnila, izjave za medije, ocene
7. Izhodne povezave	DP 5.1, 5.2, 5.4, 5.5, 5.6, na koncu DP 6, vsi podsistemi

DP 5.4 (za medije)

1. Vhodne povezave	DP 4.4, 5.1, 5.2, 5.3, 5.5 in 5.6
2. Vhodni dokument in informacije	Zakonski in podzakonski predpisi, strategije, resolucije, podatki in informacije o drugih podsistemih in od njih, tiskovne konference, izjave za javnost, sestanki, odprte seje, magnetogrami, zvočni/slikovni/video posnetki, druga zaznana dejstva in ostali pridobljeni podatki
3. Vhodna informacijska dejavnost	Zbiranje/pridobivanje, analiziranje, primerjanje, vrednotenje, razvrščanje, posredovanje
4. Temeljni proces obravnavanega dela celotnega procesa	**Ustrezno medijsko delovanje:** • objektivno poročanje in uporaba nepristranskega jezika/izrazoslovja; • izogibanje (prepoved) zavajanja javnosti z lažnimi novicami, pol-resnicami, s prilagajanjem dejstev, podpihovanjem ipd.; • izogibanje »aferaštvu« in selektivnemu, pristranskemu ali pomanjkljivemu poročanju; • izogibanje želji po ekskluzivnosti, kadar bi to povzročilo škodo obveščevalno-varnostnemu organu/organom, drugemu državnemu organu s področja nacionalne varnosti, nacionalni varnosti ali drugim nacionalnim interesom; • ustrezno vrednotenje podatkov in informacij; • poročanje o preverjenih podatkih in informacijah, ki temeljijo na preverjenih in zanesljivih virih; • objektivno in neškodljivo poročanje o ugotovitvah izvajalcev nadzora in izjavah politike, predstavnikov matičnih obveščevalno-varnostnih služb ter predstavnikov nacionalnega obveščevalno-varnostnega sistema; • upoštevanje specifičnosti in občutljivosti področja obveščevalno-varnostne dejavnosti z vidika nacionalne varnosti in nacionalnih interesov; • spoštovanje instituta tajnosti (izjeme: javni interes, kazniva dejanja idr., odvisno od predpisov); • upoštevanje novinarskega kodeksa, ki mora biti usklajen s spoštovanjem tajnosti, nacionalne varnosti in nacionalnih interesov; • spoštovanje zaposlenih v matičnih obveščevalno-varnostnih službah in nacionalnem obveščevalno-

	varnostnem sistemu, izvajalcev nadzora, strokovne javnosti, oseb iz izobraževalnega sistema in politikov ter njihovega dela; • kritično preiskovanje delovanja matičnih obveščevalno-varnostnih služb, nacionalnega obveščevalno-varnostnega sistema, politike, izobraževalnega sistema, strokovne javnosti in izvajalcev nadzora; • sodelovanje in posvetovanje z drugim podsistemom ali s strokovnjaki, kadar je potrebno posebno znanje za ustrezno medijsko poročanje/delovanje; • sodelovanje z ostalimi podsistemi modela-sistema; • preprečevanje nedovoljenih ali spornih poskusov škodljivega vpliva na medije in njihovo poročanje s strani politike, matičnih obveščevalno-varnostnih služb, drugih podsistemov, interesnih skupin ipd. • drugo (odvisno od države/okolja).
5. Izhodna informacijska dejavnost	Medijsko poročanje, distribucija, prikazovanje
6. Izhodni dokument in informacije	Novice, podatki, informacije, fotografije (tisk, televizija, radio, medmrežje/internet/splet)
7. Izhodne povezave	DP 5.1, 5.2, 5.3, 5.5, 5.6, na koncu DP 6, vsi podsistemi

DP 5.5 (za izobraževalni sistem)

1. Vhodne povezave	DP 4.5, 5.1, 5.2, 5.3, 5.4 in 5.6
2. Vhodni dokument in informacije	Predpisi s področja izobraževanja (s strani politike, pristojne za izobraževanje) in drugi akti, usmeritve za učne vsebine, podatki, informacije in dezinformacije iz drugih podsistemov, sredstva (finančna, kadrovska, materialna, druga), znanstvena in strokovna literatura, praksa in izkušnje, znanje, učni načrti, objave v medijih
3. Vhodna informacijska dejavnost	Zbiranje potrebnih in ustreznih podatkov, informacij, drugih gradiv in znanj, učenje, opazovanje
4. Temeljni proces obravnavanega dela celotnega procesa	**Izobraževanje podsistemov in njihovih subjektov**: • izobraževanje politike, izvajalcev nadzora, medijev in državljanov; • izobraževanje in usposabljanje pripadnikov matičnih obveščevalno-varnostnih služb, ko potrebujejo specifična znanja (informacijska tehnologija, strojništvo, elektrotehnika, psihologija, tuji jeziki, ekonomija, kulturologija idr.); • predstavitev osnov obveščevalno-varnostne dejavnosti, ključnih subjektov, ki izvajajo to dejavnost, njihovih pooblastil, nalog in njihove pomembnosti za obstoj in delovanje države državljanom; • pojasnitev pomena in pomembnosti zaupanja v matične obveščevalno-varnostne službe državljanom;

	• pojasnitev konkretnih posledic zaupanja in nezaupanja in njihova ponazoritev s praktičnimi primeri iz javno dostopne literature, novic, prakse državljanom ipd.; • spodbujanje kritičnega razmišljanja in delovanja; • predstavitev organov za nadzor obveščevalno-varnostnih služb, njihove vloge in nalog državljanom; • izpostavitev pomembnosti izvajalcev nadzora, znanja pri ustvarjanju mnenja in vidikov ter dela strokovne javnosti; • opozarjanje na vplive tujih obveščevalno-varnostnih služb; • predstavitev človekovih temeljnih pravic, svoboščin in meja delovanja matičnih obveščevalno-varnostnih služb na tem področju; • spremljanje in merjenje stopnje znanja s tega področja; • povezovanje državljanov s subjekti (npr. obiski institucij, predavanja strokovnjakov iz podsistemov, izobraževanja, ki jih vodijo strokovnjaki iz podsistemov); • drugo (odvisno od države/okolja).
5. Izhodna informacijska dejavnost	Poučevanje, izobraževanje, usposabljanje, sestanki, organizacija delavnic, izobraževalnih dogodkov, okroglih miz, konferenc ipd., založniška dejavnost
6. Izhodni dokument in informacije	Znanstvena in strokovna literatura, drugo (periodično) gradivo, praksa in izkušnje, zgibanke, video posnetki, avdio posnetki, znanje, novi/posodobljeni učni načrti, analize, poročila
7. Izhodne povezave	DP 5.1, 5.2, 5.3, 5.4, 5.6, na koncu DP 6, vsi podsistemi

DP 5.6 (za izvajalce nadzora)

1. Vhodne povezave	DP 4.6, 5.1, 5.2, 5.3, 5.4 in 5.5
2. Vhodni dokument in informacije	Predpisi in drugi akti (tudi predlogi/osnutki), navodila in smernice za vzpostavitev in ustrezno izvajanje zakonitega, strokovnega, neodvisnega, nepristranskega in učinkovitega nadzora, dobre prakse
3. Vhodna informacijska dejavnost	Pridobivanje podatkov in informacij, obravnava (osnutkov/predlogov) predpisov, analiza gradiv, primerjava, izmenjava mnenj, analiza dobrih praks
4. Temeljni proces obravnavanega dela celotnega procesa	**Vzpostavitev in ustrezno izvajanje zakonitega, strokovnega, neodvisnega, nepristranskega in učinkovitega nadzora**: • redno, objektivno, nepristransko in pravočasno poročanje o delu matičnih obveščevalno-varnostnih služb; • iskanje ustreznega načina informiranja javnosti, ki bo najmanj škodljiv za matične obveščevalno-varnostne službe in njihov ugled ter s tem zaupanje državljanov vanje; • prizadevanje za spoštovanje pravnega reda ter človekovih pravic in svoboščin; • izogibanje vrednostnim sodbam, »aferaštvu«, selektivnemu, pristranskemu, zavajajočemu ali

	pomanjkljivemu poročanju (še posebej, kadar gre za poročanje preko medijev); • izpostavljanje uspehov in dosežkov matičnih obveščevalno-varnostnih služb ter izboljšav ali odpravljenih pomanjkljivosti, napak ali kršitev (kadar je to mogoče in se s tem nikogar/ničesar ne ogroža); • sodelovanje z mediji, politiko, nacionalnim obveščevalno-varnostnim sistemom (in njegovimi subjekti), strokovno javnostjo, izobraževalnim sistemom in državljani, predvsem pa z matičnimi obveščevalno-varnostnimi službami; • pridobivanje in posodabljanje znanj, potrebnih za učinkovito in ustrezno izvajanje nadzora; • primerjanje lastne prakse s prakso v tujini in iskanje dobrih praks; • mednarodno sodelovanje s tujimi izvajalci nadzora (izmenjava mnenj, izkušenj, dobrih praks); • pridobivanje usposobljenega kadra/usposabljanje obstoječih izvajalcev nadzora, ki jim javnost, politika in službe zaupajo; • medsebojno usklajevanje z drugimi izvajalci nadzora (predvsem časovna usklajenost izvajanja nadzorov in izogibanje hkratnim nadzorom); • drugo (odvisno od države/okolja).
5. Izhodna informacijska dejavnost	Izvajanje nadzora, obveščanje, poročanje, opozarjanje, sodelovanje
6. Izhodni dokument in informacije	Zapisnik o opravljenem nadzoru, poročila o opravljenem nadzoru, priporočila, smernice, navodila, kazenske ovadbe, predpisi o organizaciji, delu, pooblastilih in nalogah izvajalcev nadzora, izjave za javnost
7. Izhodne povezave	DP 5.1, 5.2, 5.3, 5.4, 5.5, na koncu DP 6, vsi podsistemi

DP 6

1. Vhodne povezave	DP 5.1, 5.2, 5.3, 5.4, 5.5 in 5.6, strokovna javnost, politika, nacionalni obveščevalno-varnostni sistem (matične obveščevalno-varnostne službe), izobraževalni sistem, mediji, državljani, tuje obveščevalno-varnostne službe, zaupljivo vedênje, okolje
2. Vhodni dokument in informacije	Rezultati analiz/primerjav/javnomnenjskih raziskav, poročila, poslovni rezultati, medijske objave, javni nastopi, dogodki
3. Vhodna informacijska dejavnost	Zbiranje podatkov in informacij
4. Temeljni proces obravnavanega dela celotnega procesa	**Analiza končnega stanja aplikacije modela oziroma delovanja sistema in optimizacija ter sinteza strukture novega procesa (v skladu s postopkom USOMID/NOVOST, DOMR)**:

	• analiza delovanja in rezultatov dela posameznih podsistemov glede na zastavljene cilje, okoliščine, predpise, smernice, načrte, prioritete, nacionalne interese ipd.; • analiza vplivov posameznih podsistemov na druge podsisteme; • analiza sodelovanja, komunikacije in soodvisnosti med podsistemi; • analiza zaznanega/izmerjenega zaupljivega vedênja in stopnje izmerjenega zaupanja državljanov v matične obveščevalno-varnostne službe; • analiza zaznanega in odkritega dela in vpliva tujih obveščevalno-varnostnih na obravnavane podsisteme ter na zaupanje državljanov v matične obveščevalno-varnostne službe; • optimizacija (novega) procesa; • sinteza strukture (novega) procesa oziroma ustvarjanje (povsem) novega procesa; • drugo (odvisno od države/okolja).
5. Izhodna informacijska dejavnost	Oblikovanje povratne informacije o učinkovitosti novega stanja sistema in prepoznanih težav/problemov glede na zaznano zaupljivo vedênje državljanov in stopnjo njihovega zaupanja
6. Izhodni dokument in informacije	Povratna informacija (poročilo, rezultat analize, primerjave), predlagane spremembe za procese ali model, nova struktura modela
7. Izhodne povezave	DP 1, politika

Postopek se nato ponovi v enakem zaporedju (od DP 1 do DP 6). Namen takšnega cikličnega ponavljanja ni v konstantnem izboljševanju procesa v neskončnost, temveč v doseganju celovitega zaupanja državljanov v matične obveščevalno-varnostne službe. To pomeni, da je delovanje določenega podsistema lahko manj uspešno ali na trenutke celo škodljivo (npr. nekompetentni izvajalci nadzora, afere v matičnih obveščevalno-varnostnih službah, pristransko delovanje medijev, neučinkovito izobraževanje), vendar sistem kljub temu živi in deluje v smeri razvoja ter viabilnosti. Za učinkovitost in uspešnost sistema je ključno, da si DP sledijo v točno določenem zaporedju ter da DP 4.1–DP 4.6 in DP 5.1–DP 5.6 potekajo istočasno in v skladu z USOMID/NOVOST, DST, DOMR ter TVS/MVS. Če izvajalci aplikacije tega okvirnega zaporedja in načina aplikacije ne bodo vsaj okvirno upoštevali, ne bodo mogli doseči celovitega zaupanja državljanov v matične obveščevalno-varnostne službe, ker ne bodo izpolnili vseh potrebnih kriterijev za dvig in vzdrževanje celovitega zaupanja.

Državljanov in njihovega procesa presoje zaupanja nismo opredelili kot DP, saj jih k temu procesu ne moremo prisiliti. Da pa bi delovali tako, kot si želimo, lahko nanje in na njihovo vedênje vplivamo z ostalimi podsistemi. V »idealnih« okoliščinah bi DP za podsistem *Državljani* opredelili tako:

1. Vhodne povezave	Strokovna javnost, politika, nacionalni obveščevalno-varnostni sistem (matične obveščevalno-varnostne službe), izobraževalni sistem, mediji, tuje obveščevalno-varnostne službe, drugi državljani – rezultati njihovega delovanja in njihovi vplivi
2. Vhodni dokument in informacije	Medijski prispevki (časopis, splet, televizija, radio), besede druge osebe, dejanja druge osebe, tiskovne konference, izjave za javnost, pisno gradivo (poročila, knjige, elaborati, ocene, strokovni in znanstveni članki), fotografije, video posnetki, spomin, trenutno zaupanje
3. Vhodna informacijska dejavnost	Pasivno in aktivno zbiranje podatkov in informacij (znanja) z uporabo čutil in s priklicem iz spomina
4. Temeljni proces obravnavanega dela celotnega procesa	**Presoja zaupanja v matične obveščevalno-varnostne službe in druge podsisteme v tistem segmentu, ko njihovo delovanje, značilnosti ali obstoj vpliva na zaupanje v matične obveščevalno-varnostne službe**
5. Izhodna informacijska dejavnost	Zaupljivo vedênje: posredno ali neposredno izražanje zaupanja v matične obveščevalno-varnostne službe z besedami in dejanji
6. Izhodni dokument in informacije	Besede (govor, pogovor neposredno z osebo/osebami), pisni zapis (klasična ali elektronska pošta, zapis na spletu, v časopisu, preko telefonskega sporočila ali aplikacije ipd.), zvočni posnetek, video posnetek, dejanje (podpis peticije, protest, bojkot, udeležba dogodkov, izkazovanje podpore preko spletnih omrežij, materialna ali finančna podpora, ravnanje, opustitev ravnanja ipd.)
7. Izhodne povezave	Strokovna javnost, politika, nacionalni obveščevalno-varnostni sistem (matične obveščevalno-varnostne službe), izvajalci nadzora, izobraževalni sistem, mediji, drugi državljani

Celotna logistika aplikacije modela celovitega zaupanja državljanov v matične obveščevalno-varnostne službe je kljub relativno natančno opredeljeni programoteki okvirna, zato so okvirni tudi osnovni program in delni programi. Vsako približevanje togosti in oddaljevanje od okvirnosti bi preprečilo doseganje celovitega zaupanja. Razlog se skriva v VKEN, ki delajo družbe med seboj različne, zato so si tudi države med seboj različne. Čeprav so v tem poglavju navedeni programi dokaj precizno določeni in opisani, po našem prepričanju še vedno dopuščajo dovolj gibkosti in manevrskega prostora za prilagojeno aplikacijo modela glede na ciljni subjekt – državo.

7 Dejavniki logistike aplikacije modela na Republiko Slovenijo

S končno obliko modela celovitega zaupanja državljanov v matične obveščevalno-varnostne službe ter z izdelano logistiko aplikacije modela smo poiskali dejavnike logistike aplikacije modela na Republiko Slovenijo, ki je predstavljala naš testni objekt za preverjanje uporabnosti/ustreznosti modela. Republiko Slovenijo smo izbrali, ker poznamo strukturo in delovanje njenega sistema nacionalne varnosti, nacionalnega obveščevalno-varnostnega (pod)sistema, državnega ustroja, politike, družbe, medijev, strokovne javnosti, izobraževalnega sistema in drugih dejavnikov, relevantnih za obravnavo zaupanja državljanov v matične obveščevalno-varnostne službe. Naš namen je bil pridobiti povratne informacije o uporabljenih dejavnikih/sestavinah modela in identificirati ključne dejavnike logistike aplikacije predlaganega modela na Republiko Slovenijo. Da bi bila identifikacija navedenih dejavnikov bolj učinkovita, smo predhodno preverili, kakšno je zaupanje slovenskih državljanov v slovenske obveščevalno-varnostne službe.

7.1 Zaupanje slovenskih državljanov v slovenske obveščevalno-varnostne službe

Podatkov o tem, koliko slovenski državljani zaupajo slovenskim obveščevalno-varnostnim službam, je zelo malo, nekatere (posredne) podatke pa je bilo potrebno pridobiti s pomočjo analize že izvedenih raziskav in z lastno raziskavo. Po nam znanih in dostopnih podatkih obstaja le ena javno dostopna raziskava, ki konkretno sprašuje o zaupanju Slovencev v slovenske obveščevalno-varnostne službe, natančneje v Sovo. Raziskava slovenskega javnega mnenja leta 2012 (glej Kurdija et al., 2016) je med drugim merila tudi zaupanje Slovencev v Sovo (ne pa tudi v OVS). V raziskavi je sodelovalo 1034 anketirancev (N = 1034). Slika 7.1 prikazuje rezultate raziskave.

Slika 7.1: Zaupanje Slovencev v obveščevalno-varnostne službe v letu 2012

	Kako zaupate:	sploh nič	le malo	precej	v celoti	ne vem
		1	2	3	4	8
i)	sodiščem	27,7	46,1	19,0	1,9	5,3
j)	policiji	10,1	35,0	45,3	7,2	2,5
k)	evropski valuti evru	8,6	40,4	41,2	6,1	3,7
l)	humanitarnim organizacijam (Rdeči križ, Karitas, Unicef ...)	23,0	41,1	27,3	6,3	2,3
m)	Varuhu človekovih pravic	11,7	38,1	35,4	5,9	8,9
n)	Slovenski obveščevalno varnostni agenciji (SOVA)	20,2	37,7	13,8	1,1	27,1
o)	sindikatom	26,1	41,8	22,8	2,5	6,8

Vir: Kurdija et al., 2012, str. 140

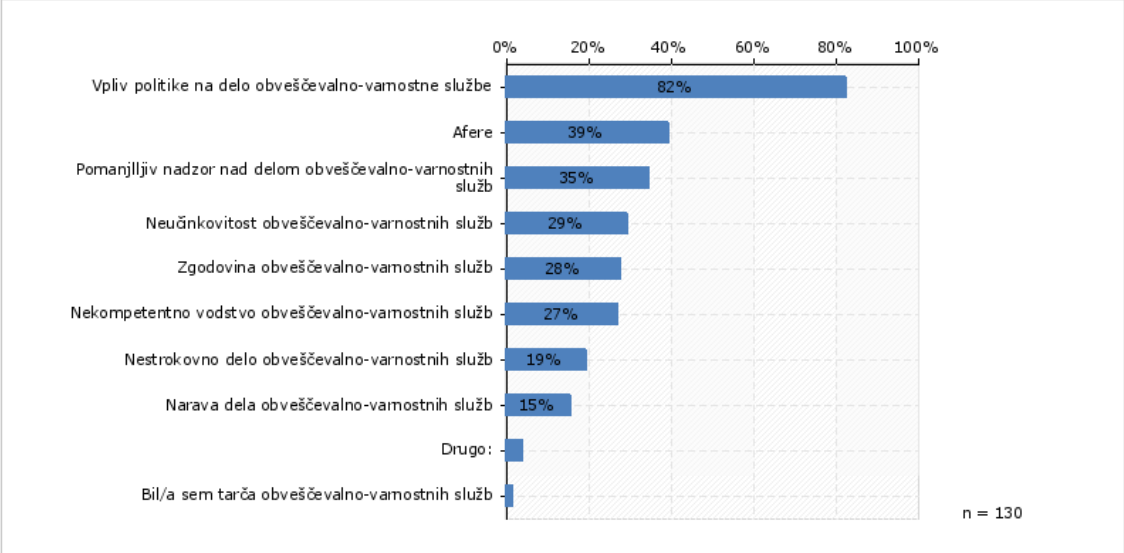
Petina anketirancev (20,2 %) sploh ni zaupala Sovi, 37,7 % anketirancev ji je malo zaupalo, 13,8 % ji je precej zaupalo, 1,1 % ji je v celoti zaupalo, 27,1 % pa je odgovorilo »ne vem«. Lahko bi rekli, da je več kot polovica anketirancev izrazila nizko stopnjo zaupanja v Sovo.

Ker drugih rezultatov v zvezi z zaupanjem v tovrstne službe ni bilo, smo leta 2016 izvedli spletno anketiranje z orodjem 1ka (https://www.1ka.si/). Spletna anketa je bila aktivna med 22. 6. 2016 in 22. 9. 2016. Povezava do ankete je bila posredovana naslove elektronske pošte znancev avtorja doktorske disertacije, študentov in zaposlenih Fakultete za logistiko UM ter študentov Fakultete za varnostne vede UM. Spletno povezavo do ankete je objavil tudi doktorski kandidat in soavtor te doktorske disertacije na svojem uporabniškem profilu družbenega omrežja Facebook. Spletno povezavo je odprlo 815 ljudi, od katerih je 295 ljudi (36 %) anketo izpolnilo v celoti. Anketa, ki se nahaja v prilogi doktorske disertacije (Priloga 2), se razlikuje od ankete, ki so jo uporabili v predstavljeni raziskavi slovenskega javnega mnenja. Sestavljena je iz šestih vprašanj in razdeljena na dva sklopa: vsebinski sklop (prvo in drugo vprašanje) in demografski sklop (tretje, četrto, peto in šesto vprašanje). Na prvo, tretje, četrto, peto in šesto vprašanje so anketiranci odgovarjali z izbiro enega izmed ponujenih odgovor, na drugo vprašanje pa z izbiro enega ali več odgovor (z možnostjo vpisa svojega odgovora). Anketiranci, ki so odgovorili na prvo vprašanje z »Da«, so nato odgovorili le še na vprašanja iz demografskega sklopa, anketiranci, ki so odgovorili na prvo vprašanje z »Ne«, pa so odgovorili tudi na vseh preostalih šest vprašanj, saj je bilo drugo vprašanje (»Zakaj ne?«)

ponujeno le anketirancem, ki so na prvo vprašanje odgovorili »Ne«. Vsi odgovori anketirancev so v prilogi doktorske disertacije (Priloga 3).

Na vprašanje »Ali zaupate slovenskim obveščevalno-varnostnim službam?« je 165 anketirancev (56 %) odgovorilo »Da«, 130 anketirancev (44 %) pa »Ne«. Teh 130 anketirancev je na vprašanje »Zakaj ne?« odgovorilo, kot prikazuje slika 7.2.

Slika 7.2: Rezultati odgovorov na vprašanje, zakaj anketiranci ne zaupajo slovenskim obveščevalno-varnostnim službam



Vir: Osebni vir

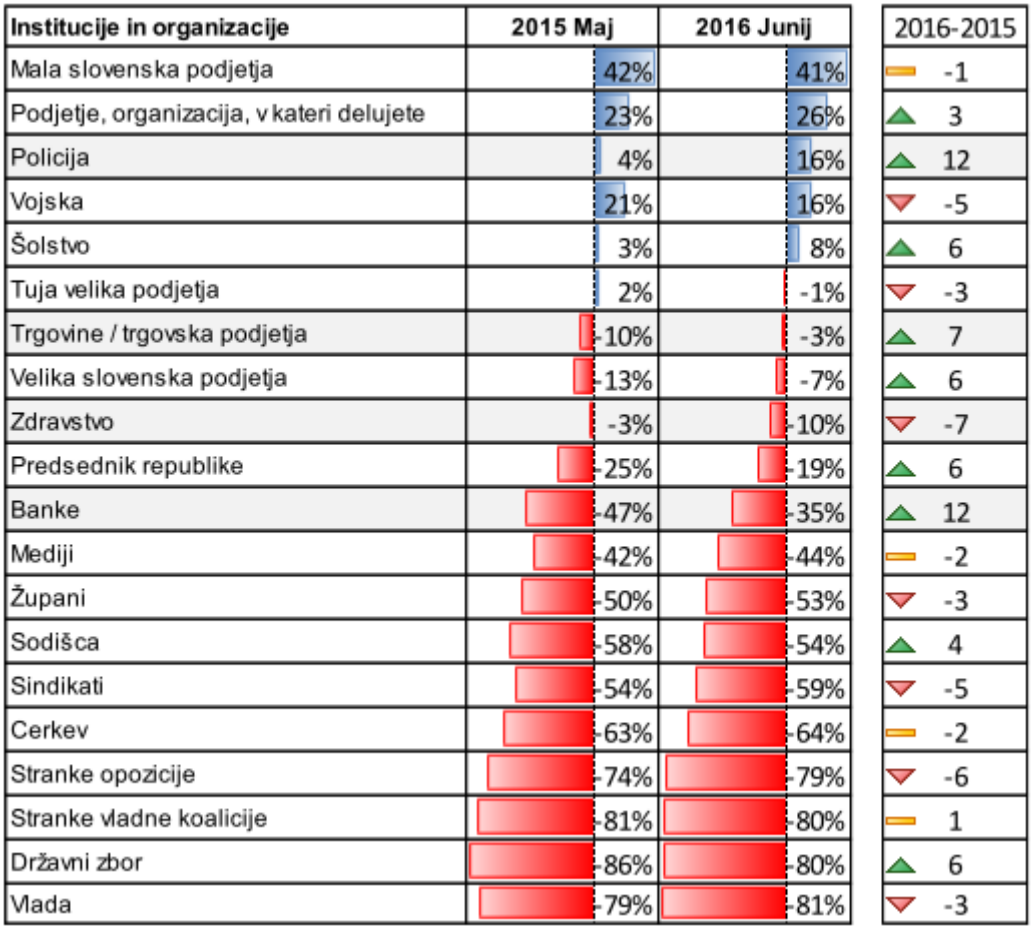
Nekateri anketiranci so pri odgovoru »Drugo« navedli nekatere druge razloge oziroma mnenja (odgovori niso lektorirani):

- »politični nadzor opozocije glede na pozicijo, pomanjkanje vednosti varuha človekovih pravic kakšna je njena/njegova vloga pri nadzoru teh služb«;
- »ker so povsod sami šalabajzi na vodilnih položajih, predvidevam da je tudi pri obveščevalno-varnostnih službah tako«;
- »ne poznam njihovega dela«;
- »prekomplicirani postopki, ki onemogočajo ukrepanje v realnem času«;
- »ne zaupam jim«.

Pri moških anketirancih (n = 138) jih 73 (52,9 %) zaupa slovenskim obveščevalno-varnostnim službam, 65 (47,1 %) pa ne. Pri ženskih anketirankah (n = 157) pa jih 92 (58,6 %) zaupa službam, 65 (41,4 %) anketirank pa službam ne zaupa. Kljub majhni razliki v številu in odstotkih pri odgovorih bi lahko rekli, da bistvene razlike pri zaupanju v slovenske obveščevalno-varnostne službe med spoloma ni. Pri delitvi anketirancev po starosti smo se osredotočili na največji dve skupini, in sicer na tiste med 21. in 35. letom starosti ter tiste med 36. in 55. letom starosti. Rezultati ankete so pokazali, da v starostni skupini 21-35 let (n = 205) 124 anketirancev (60,5 %) službam zaupa, 81 (39,5 %) pa je takšnih, ki službam ne zaupa. V starostni skupini 36-55 let (n = 65) je 28 anketirancev (43,1 %) takšnih, ki službam zaupa, 37 (56,9 %) pa takšnih, ki službam ne zaupa. Zaradi številčno neenake zastopanosti med starostnima skupinama ne moremo z zanesljivostjo trditi, kdo bolj ali manj zaupa slovenskim obveščevalno-varnostnim službam niti zakaj v posamezni starostni skupini prevladuje število tistih, ki zaupajo, oziroma tistih, ki ne zaupajo, saj smo imeli premalo anketirancev v starostni skupini 36-55 let, da bi to lahko statistično dokazali.

Raziskava javnega mnenja, ki jo je izvedlo podjetje Valicon v obdobju 2015-2016, je pokazala, da imajo Slovenci nizko stopnjo zaupanja v politične stranke, Vlado RS, Državni zbor RS, sodišča in zdravstvo (slika 7.3). Čeprav to ni razvidno iz rezultatov, domnevamo, da je bilo zaradi slabega zaupanja v politiko, različnih afer in omenjenega razkritja operativca Sove s strani avstrijskega veleposlaništva septembra 2015 nizko tudi zaupanje v slovenske obveščevalno-varnostne službe.

Slika 7.3: Stopnja zaupanja v institucije in organizacije (maj 2015–junij 2016)



Institucije in organizacije	2015 Maj	2016 Junij	2016-2015
Mala slovenska podjetja	42%	41%	-1
Podjetje, organizacija, v kateri delujete	23%	26%	3
Policija	4%	16%	12
Vojska	21%	16%	-5
Šolstvo	3%	8%	6
Tuja velika podjetja	2%	-1%	-3
Trgovine / trgovska podjetja	-10%	-3%	7
Velika slovenska podjetja	-13%	-7%	6
Zdravstvo	-3%	-10%	-7
Predsednik republike	-25%	-19%	6
Banke	-47%	-35%	12
Mediji	-42%	-44%	-2
Župani	-50%	-53%	-3
Sodišča	-58%	-54%	4
Sindikati	-54%	-59%	-5
Cerkev	-63%	-64%	-2
Stranke opozicije	-74%	-79%	-6
Stranke vladne koalicije	-81%	-80%	1
Državni zbor	-86%	-80%	6
Vlada	-79%	-81%	-3

* n = 510 (maj 2015) in 524 (junij 2016)

Vir: Valicon, 2016, str. 2

Memedijeva (2015) je ugotovila, da je zaupanje v demokratične institucije med slovenskimi študenti razmeroma nizko. Najmanj zaupajo vladi in parlamentu, bolj pa zaupajo sodiščem, policiji, Slovenski vojski in varuhu človekovih pravic. Ugotovila je tudi (ibidem), da večina študentov, ki so sodelovali v raziskavi, pravi, da se je njihovo zaupanje zmanjšalo tekom študija. Razlogi za zmanjšanje zaupanja so predvsem korupcija, afere, pridobljeno znanje, boljše poznavanje sistema/institucij/procesov in dejanja institucij, razlogi za povečanje pa boljše poznavanje sistema/institucij/procesov, pridobljeno znanje ter stik z nosilci funkcij oziroma institucijami (ibidem). Zanimiv je tudi rezultat raziskave, ki jo je opravil Van de Walle (2007), da se je zaupanje Slovencev v javno upravo v letih 1999-2001 zmanjševalo s starostjo in z višjo izobrazbo. Igličar (2012, str. 97) je opazil, da je »[n]a splošno […] zaznati trend zmanjševanja zaupanja slovenske

javnosti v vse državne institucije in tudi v sodstvo. Slovensko javno mnenje, z nekaj izjemami, bolj zaupa civilnodružbenim ustanovam kot osrednjim državnim organom.« Če je mogoče slovenske obveščevalno-varnostne službe uvrstiti med institucije, ki zagotavljajo red in fizično nedotakljivost sistema (glej v Kaase et al., 1999, str. 313), med katere spadata policija in vojska, potem bi bilo mogoče sklepati, da te službe uživajo relativno višjo stopnjo zaupanja kot pa ostale državne institucije. Toš (v Kaase et al., 1999) namreč ugotavlja, da je za institucije reda značilna višja raven zaupanja. Vendar so rezultati slovenskega javnega mnenja iz leta 2012 pokazali, da je zaupanje Slovencev v Sovo manjše od zaupanja v policijo in Slovensko vojsko (glej Kurdija et al., 2012, str. 140 in 141). Zato domnevamo, da Sova ne uživa enakega zaupanja slovenske javnosti kot policija in Slovenska vojska, kar verjetno velja tudi za OVS.

Zakaj je temu tako, nismo zasledili v nobenem nam dostopnem viru, domnevamo pa, da je razlog večplasten. Ugled slovenskih obveščevalno-varnostnih služb je bil v zgodovini samostojne Republike Slovenije zaradi afer pogosto načet. Veliko število afer nakazuje na to, da ali službe niso dovolj strokovne oziroma kompetentne, da zaradi določenih razlogov iz službe »uhajajo« podatki, da se je politika prepogosto vmešavala v delo obveščevalno-varnostnih služb ali pa da mediji ne poročajo ustrezno oziroma z ustreznimi nameni. V zadnjih letih se v zvezi z obveščevalno-varnostno dejavnostjo v večji meri poroča o Sovi, o OVS in policiji pa zelo malo. Za primer medijskega poročanja o Sovi navajamo prispevek v časopisu Dnevnik iz leta 2007, ki trdi, da je »[v] prvih štirih mesecih tega leta […] Sova z lastno aktivnostjo zbrala za skoraj 50 odstotkov manj informacij. To pomeni, da je Sova iz lastnih virov, z mrežo sodelavcev, s posebnimi metodami ipd. skoraj za polovico manj uspešna kot v enakem obdobju lani. Takšen padec uspešnosti potrjuje opozorila poznavalcev obveščevalne skupnosti, da takšna afera škoduje predvsem sami tajni službi, saj sta omajana njen ugled in kredibilnost, tajni sodelavci pa ji ne zaupajo več.« (Praprotnik, 2007) Težko ocenjujemo, ali so podatki iz neuradnih virov, kot pravi avtor prispevka, resnični, vsekakor pa lahko z gotovostjo trdimo, da takšen prispevek bistveno pripomore k zmanjšanju zaupanja v Sovo in njene uslužbence – predvsem na način, kot ga navaja tudi avtor članka, da tajni sodelavci službi ne zaupajo več in z njo ne želijo več sodelovati. Kot pravi Podbregar (2018, str. 96), je dr. Janez Drnovšek maja 2007 v dveh televizijskih intervjujih na vprašanje, ali kot predsednik države zaupa Sovi,

odgovoril: »Jaz sem Sovi zaupal v vseh letih, ko sem bil predsednik vlade, do nedavnega. […] [V]em, da je bila pomembna tudi za Nato, za EU, da je bilo vzpostavljeno sodelovanje z največjimi državami, partnersko sodelovanje, in da so predsedniki teh držav večkrat izrekli priznanje, češ, da je služba kvalitetna, da je veliko pripomogla k širši varnosti. In da je del širšega evropskega in varnostnega sistema. In to je bilo tisto, kar smo sistematično gradili skozi ta leta, moram reči, da sedaj, v zadnjih mesecih, odkar je prišlo do sprememb v Sovi, nimam več tega občutka, ampak nasprotno, da se je po zelo hitrem postopku ta institucija razmontirala, izničila, zapravljeno zaupanje […].« Kot kaže, je bilo zaupanje v Sovo v tistem obdobju izgubljeno oziroma porušeno.

Popolnoma drugačno stanje prikazuje sporočilo za javnost nekdanjega predsednika Vlade RS dr. Mira Cerarja, v zvezi z anonimnimi očitki o korupciji in slabem stanju v Sovi, o katerem je bila javnost preko medijev na podlagi t.i. anonimk seznanjena leta 2016 (»Premier dr. Cerar izrazil nadaljnje zaupanje direktorju Sove Klemenčiču« [Sporočila za javnost], 2016): »*[P]remier poudarja, da je Sova v zadnjem letu bistveno okrepila svoje dejavnosti. Prav tako uživa opazen ugled pri drugih državah in uspešno sodeluje s partnerskimi službami številnih držav […]. Dejavnosti Sove so z vidika države posebej pomembne zlasti v času sodobnih varnostnih groženj, kot so terorizem in množične migracije, ter zapletenih privatizacijskih postopkov. […] Ob tem pa opozarja, da so se v preteklosti več let v Sovi uveljavljale nekatere neprofesionalne prakse. Direktor Sove Klemenčič […] se mora tako soočati z nepotističnimi, klientelističnimi in nekaterimi drugimi nesprejemljivimi praksami, ki jih je začel prekinjati z uveljavljanjem profesionalnega delovanja. […] Neprofesionalno pisanje javnih anonimnih obtožb je v popolnem nasprotju s profesionalnimi načeli obveščevalno-varnostne dejavnosti, ki omogočajo ustrezne kanale za morebitne pritožbe oziroma opozorila na posamezne nepravilnosti ali celo nezakonitosti, ocenjuje premier. Hkrati izpostavlja, da ravno tovrstne prakse krnijo ugled oziroma skušajo diskreditirati Sovo, kar gre na škodo celotni državi.*«

Tudi v letu 2019 je prišlo do nove afere glede zaposlovanja določenih oseb, ki so bile blizu takratnemu predsedniku vlade, Marjanu Šarcu, vendar je vsebina te afere z našega vidika nepomembna, saj želimo bralce opozoriti na dejstvo, kako je tudi ta afera vplivala na

ugled in javno podobo matične obveščevalno-varnostne službe, izvajalce nadzora, medije in politike. Vpleteni podsistemi so nedvomno izgubili določeno stopnjo zaupanja s strani državljanov, saj je njihovo medijsko (predvsem pa javno) delovanje, medsebojno obtoževanje in različno sklicevanje na enako pravno podlago povzročilo, da so v očeh drugih postali manj kompetentni, nestrokovni in brez integritete.

Da gre za nekompetentnosti služb, o kateri se je v medijih pogosto pisalo ob pojavu afer, lahko beremo tudi v komentarjih bralcev spletnih člankov. Mnenje posameznikov (oziroma javnosti) kaže, da imajo oziroma so imeli državljani različne razloge za takšno mnenje. Nekateri se sklicujejo na polpreteklo zgodovino, drugi na strokovnost, tretji na politiko, menimo pa, da je v vseh primerih prisotno pomanjkanje ustreznega znanja o področju dela služb tako na strani državljanov kot tudi medijev in tudi politikov. Pojavi se tudi vprašanje, ali so komentatorji novic pomislil na namen objave neke novice, na morebitno drugačno stanje, kot je bilo prikazano na ostala dejstva in okoliščine ali pa na morebitno zavajanje/dezinformiranje javnosti. Z osnovnim in ustreznim znanjem o obveščevalno-varnostnih službah bi lahko ustrezno oblikovali svoje mnenje in kritičen pogled na situacijo, v nobenem primeru pa svojih ugotovitev ali ugotovitev drugih laikov ne bi smeli posploševati niti delati prehitrih zaključkov. Za zaupanje in ugled je še posebej škodljivo, kadar državljan nima nikakršnega znanja ali pa je to pomanjkljivo ali napačno, svoje mnenje pa nato širi preko javnih občil oziroma medijev. Vsakdo ima pravico do svojega mnenja in do njegovega izražanja, ob tem pa je potrebno upoštevati tudi to, kar je v pesmi *Apel in čevljar* zapisal dr. France Prešeren: »Le čevlje sodi naj Kopitar!« Pomanjkanje znanja v kombinaciji z napačnimi ali pomanjkljivimi podatki in informacijami negativno vpliva na mnenje/zaupanje posameznika in družbe v matične obveščevalno-varnostne službe. Drugi dejavnik pa je vpogled v realno stanje. Ker večina državljanov nima vpogleda v delo tovrstnih služb, bi moral biti za pojasnjevanje stanja znotraj služb pristojen in odgovoren mehanizem za nadzor obveščevalnih in varnostnih služb. Kot kaže analiza slovenskih medijskih prispevkov in posamičnih izjav ter dejanj nekaterih izvajalcev nadzora matičnih obveščevalno-varnostnih služb, je njihova strokovnost, pristranskost in dobronamernost pod vprašajem, kar opazi in izrazi tudi slovenska javnost.

Vrnimo se k iskanju podatka, koliko Slovenci zaupajo slovenskim obveščevalno-varnostnim službam. Rezultati naše, metodološko sicer nereprezentativne ankete kažejo, da nekaj več kot polovica anketirancev zaupa slovenskim obveščevalno-varnostnim službam, slaba polovica pa ne. Če naše ugotovitve združimo z rezultati raziskave javnega mnenja iz leta 2012 (glej Kurdija et al., 2012), lahko ugotovimo podobno stanje: nekaj več kot polovica anketirancev službam zaupa, 20,2 % jim ne, ostali pa so odgovorili z »ne vem«. Intervjuvanca, s katerima smo opravili intervju in sta bila v času opravljanja intervjuja aktualna uslužbenca Sove, menita, da je trenutno zaupanje v slovenske obveščevalno-varnostne službe »povprečno, dobro« oziroma »nekje na sredini lestvice zaupanja državljanov v različne državne organe.« S tem **okvirno ugotavljamo**, da je **zaupanje Slovencev v slovenske obveščevalno-varnostne službe zmerno**. Za metodološko ustrezno oceno oziroma potrditev bi morali opraviti ustrezne meritve v skladu z ustreznim znanstvenim pristopom in orodji, za takšno ocenjevanje pa je potrebna vključenost raziskovalcev z drugih področij.

7.2 Teoretična aplikacija modela na Republiko Slovenijo

Model, ki smo ga izoblikovali v 5. poglavju in ustvarili programoteko za njegovo aplikacijo, smo teoretično aplicirali na Republiko Slovenijo kot sistem, ki ima svoje lastnosti, posebnosti, strukturo, podsisteme idr. ter ga oblikuje tudi okolje, v katerem se nahaja, in ostali vplivni dejavniki. Na ta način smo želeli najti dodatne ali posebne dejavnike logistike aplikacije modela. Ker nimamo in nismo imeli zakonodajne ali izvršilne moči, smo logistiko aplikacije modela lahko le teoretično simulirali. Aplikacija je potekala postopno ter v skladu z osnovnim programom in njegovimi DP. Podpoglavja v nadaljevanju predstavljajo posamezne DP.

7.2.1 DP 0: Odločitev za uporabo modela in seznanitev podsistemov o odločitvi

Izhodišče za uporabo modela je naša doktorska disertacija. Njeno končno obliko bi morali poslati odločevalcem na najvišji ravni v Republiki Sloveniji (Vlada, DZ, predsednik republike) in se z njimi po potrebi tudi sestati, v kolikor bi želeli od nas pojasnila ali odgovore na njihova vprašanja glede modela in njegove aplikacije. Odločevalce bi bilo

potrebno **z argumenti in dejstvi prepričati**, da je model **nujen** za viabilno delovanje nacionalnega obveščevalno-varnostnega sistema, s tem pa tudi za učinkovito uresničevanje nacionalnih interesov Republike Slovenije ter njene nacionalne varnosti. Na podlagi tega bi se morala **izoblikovati politična interes in volja** za uporabo modela, ki bi morala obstajati predvsem na najvišji ravni upravljanja države (Vlada, DZ, predsednik republike). Odločitev za uporabo modela bi morala biti enotna. V primeru nestrinjanja z uporabo modela je njegova uporaba že v izhodišču obsojena na propad, saj bi tisti subjekti, ki se z modelom ne bi strinjali, posredno ali neposredno onemogočali njegovo aplikacijo. V tej fazi bi zadostovala le trdna politična volja za spremembo oziroma uporabo modela, ne pa tudi strinjanje/soglasje matičnih obveščevalno-varnostnih služb, medijev, izobraževalnega sistema, strokovne javnosti in drugih podsistemov. Kljub temu bi takšno strinjanje bistveno pripomoglo k aplikaciji modela, vendar je bistvenega pomena le odločitev vodstva, ki nato s predpisi uveljavi svojo voljo oziroma odločitev za uporabo modela in tako postane *nacionalni interes*. Spremembe morajo namreč potekati od vrha navzdol in ne obratno.

Politični vrh (Vlada, DZ, predsednik republike) bi nato moral skupaj izoblikovati pisno namero in načrt (npr. resolucija, bela knjiga) za vzpostavitev celovitega zaupanja državljanov v matične obveščevalno-varnostne službe. V njem bi pojasnili svojo odločitev za aplikacijo modela ter dolgoročne koristi, ki bi jih tak model prinesel, in se zavezal k njegovi implementaciji. O takšnem dokumentu bi politični vrh moral obvestiti javnost in druge podsisteme, ki jih obravnavamo v modelu, in nato pozvati vse relevantne podsisteme k sodelovanju pri implementaciji modela: parlamentarne politične stranke, delovna telesa DZ, ki bi lahko sodelovala na tem področju, Svet za nacionalno varnost (v nadaljevanju: SNAV) in sekretariat Sveta za nacionalno varnost (v nadaljevanju: SSNAV), Sovo, OVS, Policijo, ministrstvo, pristojno za notranje zadeve, ministrstvo, pristojno za zunanje zadeve, ministrstvo, pristojno za obrambo, ministrstvo, pristojno za pravosodje, ministrstvo, pristojno za medije, ministrstvo, pristojno za finance, ministrstvo, pristojno za javno upravo, ministrstvo, pristojno za izobraževanje, Urad Vlade RS za varovanje tajnih podatkov (v nadaljevanju: UVTP), Upravo za informacijsko varnost, Ustavno sodišče RS, Vrhovno sodišče RS, Varuha človekovih pravic, Informacijskega pooblaščenca, vse slovenske univerze, njihove članice in druge visokošolske zavode, ki bi lahko

sodelovali, (izobraževalne) zavode in druge (izobraževalne) ustanove, ki bi lahko sodelovale na tem področju, nevladne organizacije, ki bi lahko sodelovale na tem področju, vse slovenske medije (javne in zasebne), strokovnjake s področja nacionalne varnosti, obveščevalno-varnostne dejavnosti, varnostnih ved, politologije, obramboslovja, prava (ustavnega, kazenskega, procesnega, upravnega ipd.), človekovih pravic, demokratičnega nadzora obveščevalno-varnostnih služb, izobraževanja, znanosti, zunanjih zadev in mednarodnih odnosov, sistemske teorije, nenazadnje pa tudi vse zainteresirane državljane Republike Slovenije. Pri obveščanju bi morali sodelovati slovenski mediji, tako javni kot zasebni (kolikor bi bilo to mogoče).

Sodelovanje bi moralo biti **omogočeno vsem, in sicer nekaterim neposredno, drugim pa zaradi tajnosti posredno**, hkrati pa bi moralo biti **transparentno, sledljivo, strokovno, konstruktivno** in **dovolj jasno opredeljeno**. Tako bi npr. državni organi sodelovali v medresorskih skupinah in s pisnimi predlogi, nevladne organizacije in državljani z udeležbo na sestankih, posvetih, okroglih mizah in pisnimi predlogi, strokovna javnost z oblikovanjem predlogov predpisov, konkretnih ukrepov, študijami ipd. Pod določenimi pogoji bi bilo sodelovanje omejeno ali izvedeno posredno, če bi sodelovanje nepoklicanih oseb lahko povzročilo škodo določenim organom, državnim interesom ali državni varnosti (npr. kjer so prisotni tajni podatki).

Trije dejavniki, pri katerih bi lahko zaznali težave, so a) **vzpostavitev** in **kontinuiteta politične volje**, b) **dosledno upoštevanje vseh sodelujočih** in c) **spoštovanje določil (»pravil igre«)**. V slovensko kulturo je žal že skoraj zakoreninjena delitev na »naše in vaše«, ki bi lahko povzročila selektivno upoštevanje dogovorjenega in mnenja drugih, predvsem tistih, s katerimi se ne strinjajo. Navedeno ni v skladu s sistemskimi teorijami, ki smo jih obravnavali in vključili v model, zato bi bila aplikacija modela otežena. Navedene težave je mogoče odpraviti z **dosledno** uporabo DTS in DOMR, predvsem v smislu poudarjanja pomembnosti vsakega posameznika in skupine ter sinergij, ki jih je mogoče doseči s sodelovanjem. Z USOMID/NOVOST bi se še dodatno okrepilo in utemeljilo njegovo pravilnost in potrebnost.

7.2.2 DP 1: Opredelitev problema

Politični vrh bi moral skupaj z ostalimi povabljenimi prepoznati problem ter ga enotno in dovolj jasno izpostaviti: *obstoječa ureditev v Republiki Sloveniji ne omogoča dovolj celovitega zaupanja državljanov v matične obveščevalno-varnostne službe*. Zato bi bilo predhodno obravnavati problem znotraj posameznega subjekta političnega vrha, šele nato pa s skupno odločitvijo stopiti pred ostale subjekte in skupaj z njimi ustrezno definirati model. Postopek bi moral potekati v skladu z USOMID/NOVOST in DOMR: najprej posamično razmišljanje, nato kroženje zapisov, sledi skupinsko obravnavanje in na koncu sprejem skupne odločitve – v tem primeru definicije. Podsistemi bi si nato izmenjali zapise in nanje podali svoje predloge, nato pa bi jih kasneje skupaj obravnavali npr. predstavniki posameznih podsistemov, ki bi sprejeli končno opredelitev problema.

Lahko bi rekli, da je opredelitev problema, ki jo ponujamo, »vsiljena« in da nakazuje na to, kateri problem bi moral biti prepoznan. Naš namen je, da odločevalce usmerimo v realen problem, ki smo ga že prepoznali namesto njih, potrebno pa je, da ga spoznajo in razumejo tudi sami. S tem upoštevamo vse štiri sestavine DTS. Brez tega ni mogoče doseči politične volje in razumevanja, ki sta nujno potrebna za nadaljnjo aplikacijo modela. Politični vrh bi moral za takšno opredelitvijo problema stati, se je zavedati in problem prepoznati kot resničen in vpliven (4. sestavina DTS, *materialističnost*). Zainteresirani, ki bi bili povabljeni k sodelovanju oziroma k opredelitvi problema, bi morali delovati konstruktivno in s ciljem, da se stanje izboljša, saj bi s tem v večji ali manjši meri pridobili vsi, seveda vsak na svojem področju. Ključnega pomena je, da se pri opredelitvi problema upošteva mnenja vseh sodelujočih. S tem bi se zagotovilo participacijo vseh deležnikov ter povečevalo možnosti za doseganje sinergij, do katerih lahko pride le pri sodelovanju generalistov in specialistov.

Opredeljeni problem bi bil kasneje vključen v akt ali dokument, ki bi izražal tudi razlog in namen političnega vrha in vključenih podsistemov za razreševanje problema ter določil cilj(e). S končno verzijo dokumenta bi morali biti nato seznanjeni tudi ključni podsistemi oziroma sestavine predlaganega modela: strokovna javnost, nacionalni obveščevalno-

varnostni sistem (in matične obveščevalno-varnostne službe), izvajalci nadzora, izobraževalni sistem, mediji ter državljani.

7.2.3 DP 2: Pridobivanje podatkov o stanju sistema in okolja

Pri tretjem koraku bi zbiranje podatkov potekalo v skladu s postopkom USOMID/NOVOST in DOMR: najprej samostojno znotraj subjekta (posamično, kroženje zapisov, skupinsko, oblikovanje končne zbirke podatkov), nato s kroženjem in dopolnjevanjem podatkovnih zbirk, kasneje pa skupinsko. Podatki bi se nanašali na dejstva in zaznavo dejstev in okoliščin (mnenja, ocene, zaznave), povezanih s trenutnim sistemom/stanjem sistema, ki vpliva na zaupanje državljanov v matične obveščevalno-varnostne službe. Pri samostojnem zbiranju podatkov znotraj posameznega subjekta nismo prepoznali težav, prepoznali pa smo jih pri kroženju in skupinski obravnavi. Npr. kroženje podatkov obveščevalno-varnostnih služb je zaradi tajnih podatkov lahko omejeno ali nemogoče, saj mediji ne bi smeli imeti dostopa do tajnih podatkov. Tako npr. Sova, OVS in Policija ne bi prostovoljno delili svojih podatkov z mediji ali strokovno javnostjo. Vprašanje je torej, kako naj drugi dopolnijo podatkovne zbirke, če do njih nimajo dostopa? Vidiki državljanov, medijev, strokovne javnosti in izobraževalnega podsistema so lahko drugačni od vidikov politike, izvajalcev nadzora in nacionalnega obveščevalno-varnostnega sistema, zato bi bilo napačno, če bi morali zaradi tajnosti opustiti uporabo postopka USOMID/NOVOST in DOMR. S tem bi namreč tvegali, da izpustimo katerega od pomembnih ali vplivnih vidikov/podatkov.

Da bi se izognili tej težavi, bi morala Vlada RS **ustanoviti poseben organ**, ki bi v imenu vseh sodelujočih deležnikov/podsistemov izvajal aplikacijo modela. Organ bi bil lahko oblikovan kot skupina, v kateri bi sodelovali predstavniki iz vsakega podsistema državne in javne uprave ter izven njiju (podobno kot so izbrani oziroma imenovani člani Državnega sveta RS ali sodniki porotniki delovnega in socialnega sodišča ter okrožnih sodišč). Menimo, da bi bilo to bolj učinkovito in transparentno kot pa medresorska skupina, saj bi se vzpostavila povezava ne le med državnimi organi, temveč tudi s preostalim javnim zasebnim/nevladnim sektorjem. Tako bi se povečala tudi transparentnost in zaupanje v subjekte. Osebe, ki bi sodelovale v tem organu, bi morale

biti varnostno preverjene, saj bi imele zaradi posebne in pomembne vloge dostop tudi do tajnih, osebnih in drugih varovanih ali občutljivih podatkov.

V slovenskem prostoru bi bilo v skladu z navedenim smiselno izoblikovati delovno telo, npr. **neodvisno komisijo**, ki bi jo ustanovil DZ in bi ocenila trenutno stanja zaupanja v slovenske obveščevalno-varnostne službe z namenom vzpostavitve sistema celovitega zaupanja državljanov v matične obveščevalno-varnostne službe (v nadaljevanju: **komisija**). Ker slovenski sistem ni usklajen z našim predlaganim modelom, ne moremo obravnavati slovenskih sodelujočih subjektov tako, kot so v modelu definirani podsistemi. Komisijo bi sestavljali 1 do 3 demokratično izvoljeni predstavniki za vsako področje, ki v predlaganem modelu nastopa kot podsistem: politika (Vlada, DZ, predsednik republike oziroma njegov urad, Državni svet RS, ministrstvo, pristojno za izobraževanje, ministrstvo, pristojno za notranje zadeve, ministrstvo, pristojno za obrambo), slovenski nacionalni obveščevalno-varnostni sistem (Sova, OVS, Policija, SNAV, SSNAV), organi za nadzor obveščevalnih služb (KNOVS, Računsko sodišče, Varuh človekovih pravic, Informacijski pooblaščenec, Vrhovno sodišče RS, Sektor proračunske inšpekcije), strokovna javnost (visokošolski učitelji, raziskovalci, nekdanji uslužbenci obveščevalno-varnostnih služb, Inštitut za demokratični nadzor nad oboroženimi silami – DCAF, Transparency International, druge organizacije in strokovnjaki), izobraževalni sistem (organi ministrstva, pristojnega za šolstvo, Zavod RS za šolstvo, Nacionalna agencija za kakovost v visokem šolstvu, javne in zasebne univerze v RS), mediji (nacionalni in zasebni tiskani, televizijski, radijski in spletni mediji), državljani. Med deležniki, ki bi jih bilo smiselno in potrebno umestiti v komisijo, so tudi predstavniki UVTP, SI CERT, Uprave za informacijsko varnost ter nekaterih drugih državnih in javnih institucij, vendar bi bilo potrebno te organizacije delno ali v celoti reorganizirati v skladu s predlaganim modelom viabilnega nacionalnega obveščevalno-varnostnega sistema, šele nato pa v drugi aplikaciji modela vključiti predvidene podsisteme.

Komisija bi v DP 2 zbirala podatke o trenutnem stanju sistema v Republiki Sloveniji in njegovih podsistemov, o njihovih povezavah, sinergijah in trenutnem stanju okolja (gre za različne vrste gradiv s podatki, npr. poročila, analize, ocene, napovedi, primerjave, bilance, ugotovitve, evidence, rezultati, lahko pa tudi mnenja, priporočila, predlogi).

Podatke bi organu posredovali vključeni deležniki (podsistemi in njihovi subjekti, tj. organizacije in posamezniki) po opravljenem kroženju zbranih podatkov znotraj posameznih podsistemov.

Naslednja naloga komisije bi bila priprava zbirke podatkov v skladu s postopkom USOMID/NOVOST in DOMR. Postopek bi zagotovil kroženje podatkov v dopolnjevanje, nato ponovno zbiranje dopolnjenih podatkov ter nato skupinsko obravnavo vseh zbranih podatkov. Izvajanje in upoštevanje postopka bi nadzirala komisija. Na podlagi končne zbirke podatkov bi se kasneje izvedlo analizo o stanju sistema, podsistemov idr. Tisti del podatkov, ki bi se navezovali na delovanje obveščevalno-varnostnega sistema ter ostalih deležnikov in bi bili označeni s stopnjo tajnosti, bi bilo zato potrebno obravnavati in shranjevati ločeno od ostalih vrst podatkov v skladu z veljavnimi predpisi, ki urejajo obravnavo tajnih podatkov. Z ustrezno metodološko podporo tako iz javne uprave kot znanstveno-raziskovalnega sektorja bi se lahko vzpostavilo učinkovit informacijski sistem za zbiranje podatkov, ki bi bil tudi ustrezno zaščiten pred morebitnimi nepooblaščenimi vdori. Zaradi tajnih in občutljivih podatkov bi imeli dostop do končne zbirke vseh podatkov poleg članov komisije le politika, nacionalni obveščevalno-varnostni sistem, matične obveščevalno-varnostne službe in izvajalci nadzora. Tu bi morala politika poskrbeti za ustrezno obveščanje izobraževalnega sistema, medijev in strokovne ter splošne javnosti o dogajanju, izsledkih (za javnost) in pa zagotavljanju transparentnosti. Strokovna javnost, mediji, izobraževalni sistem, državljani in ostali pa zaradi zagotavljanja tajnosti ne bi imeli dostopa do celotne zbirke podatkov. Ob tem bi morali biti vsi deležniki, predvsem pa tisti člani, ki bi bili del predlaganega organa, poučeni, da je namen zbiranja podatkov skupna korist in ne partikularni interesi političnih strank, interesnih skupin, medijev, vplivnih posameznikov ipd.

7.2.4 DP 3: Analiza zbranih podatkov

Komisija bi nato v skladu s postopkom USOMID/NOVOST in DOMR analizirala podatke o trenutnem stanju sistema in okolja (iskanje kritičnih točk, pomanjkljivosti in razsežnosti problema ter razlogov za odsotnost celovitega zaupanja), pri čemer bi podatke najprej analiziral vsak podsistem posebej, nato posamezno z zapisi drugih podsistemov

(kroženje) in kasneje skupinsko. Kroženje bi potekalo preko članov komisije, ki bi na koncu oblikovala ključne ugotovitve in jih objavila kot končno poročilo. V skladu s slovenskimi predpisi, ki urejajo varovanje tajnih podatkov, bi končno poročilo analize vsebovalo javni in tajni del. Revidirano poročilo brez tajnih podatkov bi bilo javno objavljeno in posredovano vsem deležnikom, celotno poročilo s tajnimi podatki pa bi prejeli tisti, ki imajo potrebo po seznanitvi s konkretnimi tajnimi podatki v poročilu in imajo dostop do tajnih podatkov ustrezne stopnje tajnosti. To končno poročilo bi služilo kot izhodišče za določitev in pripravo ukrepov za podsisteme predlaganega modela.

V prvi fazi aplikacije modela bi morali nacionalni in zasebni mediji poročati v skladu z dogovorom, ki bi ga predhodno sprejela komisija. Cilj takšnega dogovora mora biti, da se o analizi poroča ustrezno, nepristransko, transparentno, neškodljivo in pravočasno. Tukaj bi imeli ključno in odgovorno vlogo predvsem mediji. Na takšen način bi se izognili morebitnim negativnim posledicam za posamezne podsisteme in samo logistiko aplikacije modela.

7.2.5 DP 4: Določitev in priprava ukrepov

Vsak izmed podsistemov bi opravil aktivnosti, določene v ustreznemu DP (DP 4.1 za politiko, DP 4.2 za nacionalni obveščevalno-varnostni sistem in matične obveščevalno-varnostne službe, DP 4.3 za strokovno javnost itd.). V skladu z USOMID/NOVOST bi morali posamezni podsistemi izhajati le iz podatkov, ki so bili posredovani komisiji (glej DP 2), oziroma iz analize (glej DP 3). Zbiranje dodatnih podatkov in iskanje ostalih virov bi namreč pomenilo odstopanje od predpisane logistike aplikacije modela celovitega zaupanja državljanov v matične obveščevalno-varnostne službe in zato možnost, da se bo model oddaljil od zadostne in potrebne celovitosti.

Kot smo že navedli v enem od prejšnjih poglavij, morajo DP 4.1., 4.2, 4.3, 4.4, 4.5 in 4.6 potekati istočasno (vsi podsistemi hkrati), najprej posamično, nato pa skupaj, ključno pa je sodelovanje med posameznimi subjekti/podsistemi v tistih korakih, pri katerih je to mišljeno (kroženje predlogov, skupno obravnavanje). Ključno je tudi, da podsistemi v fazi kroženja predlogov sodelujejo med seboj in upoštevajo druge predloge (ni nujno, da jih

sprejmejo, zadostuje, da jih vzamejo v obzir in premislek). Pri tem mora izmenjava (dopolnjenih) predlogov ukrepov potekati preko komisije oziroma njenih članov. Za izvedbo DP 4 (4.1, 4.2, 4.3 …) morajo vsi deležniki skupaj s političnim vrhom določiti rok, znotraj katerega bodo opravili predpisane aktivnosti. Pri samostojnem in medsebojnem delovanju pa bi morali podsistemi upoštevati predpise s področja tajnih podatkov, če bi jih obravnavali pri svojem delu.

V slovenskem prostoru bi se pri tej fazi aplikacije modela soočili še z enim dejavnikom oziroma izzivom, in sicer z oblikovanjem slovenskega viabilnega nacionalnega obveščevalno-varnostnega sistema. Izoblikovalo se je več predlogov za spremembo slovenskega obveščevalno-varnostnega sistema, ki jih lahko opazimo v medijih, pisnih delih, medijskem poročanju ali javnih zapisih posameznikov, vendar nobeden od predlogov ne vključuje principa viabilnosti po Beeru. Npr. Britovšek & Čretnik (2016) ugotavljata, da se o predlogih za reorganizacijo slovenskega obveščevalno-varnostnega sistema razpravlja že vrsto let. Tudi sama predlagata spremembe za izboljšanje dela slovenskih obveščevalno-varnostnih služb, ki se soočajo s finančnimi in kadrovskimi omejitvami. Potrebo po izboljšanju dela izpeljujeta iz negativne medijske izpostavljenosti teh služb zaradi različnih afer in napak. Tudi Podbregar(glej npr. Podbregar 2011a, 2019) predlaga spremembe in ugotavlja, da smo »[v] Sloveniji […] tako v SOVI kot v OVS MORS gradili hibridni organizaciji za izvajanje obveščevalno-varnostne dejavnosti. Torej, ena organizacijska struktura izvaja obveščevalne in varnostne ter protiobveščevalne naloge. V EU so uveljavljeni različni modeli in moram povedati, da je tudi pri nas po letu 1991 med poznavalci ves čas prisotna razprava o tem, da je treba sedanji hibridni model spremeniti. […] V zadnjih letih se morda pojavlja podvajanje zakonsko predpisanih obveščevalnih nalog med SOVA in OVS MORS, kar pa je nujno treba urediti.« (Podbregar, 2012, str. 43-44) Na strani politike pa so poslanci poslanske skupine *Nova Slovenija – krščanski demokrati* (NSi) zaradi domnevne slabe kadrovske in finančne situacije obveščevalno-varnostnih služb, sprememb vodstva služb in afer leta 2016 predlagal reformo slovenskega obveščevalno-varnostnega sistema ter oblikovanje nove, sodobne službe. Državni zbor RS je na njihov predlog zato sprejel *Priporočilo v zvezi z zagotavljanjem učinkovitejšega dela obveščevalno-varnostnega sistema RS zaradi spremenjenih varnostnih razmer v soseščini in mednarodnem okolju* (Državni zbor, 2016).

O smotrnosti, ekonomičnosti, racionalnosti in drugih vidikih delovanja trenutne organizacije slovenskega obveščevalno-varnostnega sistema v doktorski disertaciji ne razpravljamo niti ne dajemo konkretnih predlogov za njegovo spremembo v skladu s TVS/MVS, saj bi za to potrebovali predvsem več podatkov o trenutnem stanju – teh pa zaradi nedostopnosti in tudi tajnosti nimamo. Nobeden od prej navedenih in drugih predlogov k razreševanju izbranega problema v slovenskem prostoru, ki smo jih zasledili, ne pristopa tudi z vidika celovitega zaupanja državljanov v matične obveščevalno-varnostne službe. Za to je za oblikovanje viabilnega nacionalnega obveščevalno-varnostnega sistema, ki smo ga izoblikovali, potrebno tesno sodelovanje tudi z obveščevalno-varnostnimi službami znotraj države in drugimi relevantnimi subjekti, predvsem pa s politiko. Pri kasnejših aplikacijah našega predlaganega modela, ki potekajo kot izboljšanje trenutnega stanja, je sistem že izoblikovan in politične spremembe niso več tako vplivne kot na začetku, vendar je njen vpliv še vedno največji.

Oblikovanje konkretnih smernic za posamezne podsisteme bi moralo potekati v skladu s postopkom USOMID/NOVOST, zato konkretnih smernic v tem primeru ne moremo dati. Za to so pristojni posamezni subjekti podsistemov skupaj, ki naj postopajo v skladu s splošnimi smernicami, navedenimi v podpoglavju 6.2. Dva dejavnika, ki ju v tej fazi prepoznavamo kot vplivna, se navezujeta predvsem na zagotavljanje odločevalske avtonomije podsistemov znotraj postopka USOMID/NOVOST. Prvi je **zagotavljanje spoštovanja predlogov drugih deležnikov**, namesto neutemeljenega kritiziranja ali nasprotovanja zaradi nasprotnih ideologij, prepričanj, stališč. Drugi dejavnik pa je **(prevladujoči) vpliv partikularnih interesov posameznikov in skupin**, ki otežuje sprejemanje še tako preprostih odločitev. Takšni vplivi so v slovenskem prostoru žal stalnica. Menimo, da bi tudi v primeru aplikacije modela ti vplivi predstavljali ne le izziv, temveč oviro. Drugačni pogledi in interesi so običajni, ne smejo pa prevladati nad večino, zato je to mogoče preseči le z doslednim upoštevanjem pravil in zakonitosti USOMID/NOVOST in DOMR. Ob tem ne moremo mimo **nujne in potrebne depolitizacije** medijev, nadzora, šolstva in drugih vidikov družbenega življenja, ki so neločljivi del predlaganega modela. Prepletenost politike z ostalimi podsistemi povečuje tveganje, da odločitve, sprejete znotraj posameznih podsistemov v okviru postopka NOVOST ne bodo strokovne, argumentirane, sinergijske in predvsem celovite, temveč nestrokovne,

pavšalne in enostranske – takšne, ki pospešujejo entropijo. Da bi omejili te vplive, je ključnega pomena, da se v postopek NOVOST vključi vse potrebne deležnike znotraj podsistema in zagotovi enakost vseh strani/podsistemov.

Komisija bi na koncu tega DP zbrane predloge pregledala in jih dopolnila v skladu s postopkom USOMID/NOVOST. Pri pripravi ukrepov bi bilo zagotovo potrebno vključiti tudi pravnike (zakonodajno-pravne službe, pravnike za državno upravo, ustavno pravo, človekove pravice in temeljne svoboščine, delovno pravo idr.), ki bi poskrbeli, da so predlogi ukrepov legitimni in tudi legalni ter usklajeni z obstoječimi pravnimi temelji (Ustava RS, pravni red EU, nacionalni zakonski in podzakonski predpisi). S pomočjo pravnikov bi se lahko zagotovilo hitrejše in učinkovitejše sprejemanje potrebnih ukrepov.

7.2.6 DP 5: Implementacija ukrepov

Tako kot DP 4.1., 4.2, 4.3, 4.4, 4.5 in 4.6 morajo tudi DP 5.1, 5.2, 5.3, 5.4, 5.5 in 5.6 potekati istočasno, posamično in skupaj v sodelovanju ter z upoštevanjem njihove soodvisnosti ter soodvisnosti vseh implementiranih ukrepov za razrešitev problema. Implementacijo ukrepov bi spremljala in koordinirala komisija na podlagi sodelovanja z vsemi podsistemi. Prioriteta implementacije ukrepov je odvisna od vrste ukrepov, zato mora potekati hierarhično. Npr. najprej bi bili sprejeti ukrepi, ki spreminjajo obstoječe ali uvajajo nove predpise na nacionalni ravni. Te bi sprejel DZ na podlagi predlogov predpisov, ki jih pripravi Vlada v sodelovanju s komisijo oziroma posameznimi podsistemi. Pričakuje se, da pri sprejemanju predpisov v DZ RS ne bi smelo biti večjih težav ali zapletov, saj naj bi bil del politike, ki sprejema predpise, zastopan v komisiji, predlogi predpisov pa s tem že predhodno usklajeni in neformalno »potrjeni«. Nato bi bili sprejeti ukrepi na nacionalni ravni in znotraj organizacij (npr. odredbe, navodila, pravilniki, notranji akti, strategije, smernice), ki zahtevajo predhodno sprejetje krovnih predpisov, nato pa ukrepi, ki so vezani na aktivnosti, izvršene na podlagi predhodno sprejetih predpisov. Sprejemanje predpisov mora vedno potekati v okviru obstoječih predpisov in pooblastil, ki zadevajo posamezne podsisteme oziroma njihove subjekte. Pomembno vlogo pri zagotavljanju zakonitosti imajo nadzorni organi, predvsem pa

sodišča. Tudi pri delnih procesih je zato pomembna vloga pravnikov, da zagotovijo učinkovito implementacijo ukrepov ter spremljajo pravne plati pri sami implementaciji, kjer je to potrebno (predvsem na področju nacionalnih interesov, politik, predpisov/prioritet in aktivnosti, ki spremljajo njihovo realizacijo, ter vzpostavitvi in ustreznem izvajanju zakonitega, strokovnega, neodvisnega, nepristranskega in učinkovitega nadzora).

V slovenskem sistemu bi v tej fazi oziroma po njej prišlo do korenitih sprememb vseh podsistemov:

- preoblikovali bi se nacionalni interes, politike, predpisi in prioritete (npr. sprememba Resolucije o strategiji nacionalne varnosti, zakonodaje s področja obveščevalno-varnostnih služb, nadzornih organov in medijev, sprememba prioritet dela obveščevalno-varnostnih služb itd.);
- reorganizacija slovenskega obveščevalno-varnostnega sistema, ki bi bil (pre)strukturiran v viabilen nacionalni obveščevalno-varnostni sistem (možnost ustanavljanja novih ter ukinjanja ali spreminjanja obstoječih organov);
- sprememba manjšega dela slovenskega izobraževalnega sistema (učni načrti javnih in zasebnih višje- in visokošolskih zavodov), uvedba novih učnih metod;
- okrepljeno sodelovanje med državnimi strukturami, subjekti viabilnega slovenskega obveščevalno-varnostnega sistema, strokovno javnostjo ter izobraževalnim sistemom;
- okrepljeno delovanje strokovne javnosti na področju znanstveno-raziskovalnega dela, ki bi delovala bolj proaktivno in v skladu z novimi smernicami;
- vzpostavitev novih smernic in ukrepov za izvajanje zakonitega, strokovnega, neodvisnega, nepristranskega in učinkovitega nadzora slovenskih obveščevalno-varnostnih služb in ostalih subjektov novega slovenskega obveščevalno-varnostnega sistema;
- sprememba medijskega poročanja in delovanja novinarjev na področju spremljanja obveščevalno-varnostne dejavnosti v RS;
- boljša uzaveščenost državljanov o pomeni in delu slovenskih obveščevalno-varnostnih struktur.

Zaradi ocenjene kompleksnosti sprememb, do katerih bi prišlo v tej fazi aplikacije modela, ne moremo oceniti, kakšne bi bile druge posledice in spremembe v državi in družbi, zato tudi ne moremo podati nadaljnjih ocen.

7.2.7 DP 6: Analiza končnega stanja

Analiza končnega stanja je zadnji in dolgotrajen postopek modela, ki preuči delovanje sistema in poišče njegove prednosti, slabosti, priložnosti in tveganja. Za učinkovito analizo bi bilo potrebno skupaj z ustreznimi strokovnjaki pripraviti kriterije za ocenjevanje uspešnosti posameznih parametrov (sodelovanje, komunikacija, realizacija ipd.). Ti parametri bi kazali učinkovitost aplikacije oziroma delovanja modela. Iskanje in predlaganje ključnih kriterijev in vsebin za posamezne podsisteme bi potekalo v skladu s postopkom USOMID/NOVOST, najprej v podsistemih, nato pa v komisiji, ki bi na koncu tudi potrdila kriterije. Vsekakor pa bi morali biti med prednostnimi kriteriji ocenjevanja uspešnosti in učinkovitosti modela tudi takšni, ki bi nakazovali na stopnjo zaznanega zaupljivega vedênja in izmerjenega zaupanja državljanov v slovenske obveščevalno-varnostne službe. Pri oblikovanju kriterijev bi bilo smiselno vključiti tudi strokovnjake oziroma organizacije iz javne uprave, znanstveno-raziskovalnega sektorja in zasebnega sektorja (podjetja), ki delujejo ali raziskujejo področje merjenja in spremljanja javnega mnenja/zaupanja.

Komisija bi nato s celotnim končnim poročilom o analizi postopka seznanila politiko in ključne organe slovenskega viabilnega nacionalnega obveščevalno-varnostnega sistema, ostale podsisteme in zainteresirano javnost pa z delnim in revidiranim končnim poročilom. Nekatere ugotovitve bi zaradi zagotavljanja nacionalnih interesov in nacionalne varnosti morale ostati tajne.

Izhodišče za nadaljnje izboljšave procesa so predlogi za optimizacijo vsebinskih delov ali celotnega procesa ali pa z optimizacijo samega postopka. Teh predlogov ne smemo enačiti s predlogi za implementacijo ukrepov iz DP 3. Novo stanje in spoznanje, kaj bi bilo mogoče ali potrebno izboljšati pri aplikaciji modela, pripeljejo do ponovitve obravnave ključnega problema (DP 1), s katerim se ponovno, vendar v drugačnem obsegu sooča

sistem. Po implementaciji ukrepov bi se postopno pričeli kazati pozitivni rezultati podsistemov in celotnega sistema, ki pozitivno ali negativno vplivajo na državljane, saj sta model in logistika aplikacije zasnovana tako, da bi morali biti ti vplivi pozitivni (pod pogojem, da so vsi prejšnji koraki in DP izpeljani v skladu z DTS, DOMR in USOMID/NOVOST). Na podlagi pozitivnih rezultatov bi državljani RS postopno izkazovali zaupljivo vedênje do slovenskih obveščevalno-varnostnih služb. Proces izgradnje zaupanja je dlje trajajoči proces, zato bi se bolj obsežni in konkretni rezultati po naši oceni lahko pokazali šele po preteku daljšega časovnega obdobja (nekaj let).

Kakšno bi bilo končno stanje teoretične aplikacije modela na Slovenijo kot vzorčni primer, ne moremo ugibati. Prvi razlog je že omenjena ocenjena kompleksnost sprememb, do katerih bi prišlo v DP 5, zaradi katere bi težko ocenjevali prihodnje aktivnosti znotraj logistike aplikacije. Drugi razlog pa dejstvo, da je na koncu DP 5 in v DP 6 potrebno sodelovanje vseh podsistemov (preko komisije) v skladu z USOMID/NOVOST, kolektivnih odločitev pa ne moremo predvideti – tudi zaradi prvega razloga.

7.3 Spoznanja iz teoretične aplikacija modela na Republiko Slovenijo in prepoznani dejavniki

Na podlagi izvedene teoretične aplikacije smo našli vplivne dejavnike in prišli do novih spoznanj o tem, katere dele logistike aplikacije bi bilo potrebno spremeniti in ali dopolniti, da bi bil model ustrezno apliciran v ciljno okolje (nekatera spoznanja oziroma dejavnike smo že omenili v prejšnjem podpoglavju):

- Na aplikacijo modela bistveno vplivajo trije dejavniki: a) **vzpostavitev** in **kontinuiteta politične volje in interesa** za uporabo modela, b) **dosledno upoštevanje vseh sodelujočih** v procesu aplikacije modela in c) **spoštovanje določil (»pravil igre«)**. Prvi dejavnik je bistvenega pomena, saj brez političnega interesa tudi ni mogoče izvesti kasnejših odločitev na najvišji ravni odločevalcev v državi, ki najbolj vplivajo na potek in vsebino logistike aplikacije. Podsistem *Politika* je zato po našem prepričanju **najbolj vplivna in najpomembnejša sestavina** modela in same logistike aplikacije modela. Dosledno upoštevanje vseh sodelujočih v procesu aplikacije modela in

spoštovanja določil je mogoče doseči le z doslednim upoštevanjem DTS, DOMR in USOMID/NOVOST. Težava je tudi v izbiri upoštevanja DTS, DOMR in USOMID/NOVOST. Menimo, da bi morala v tem primeru stran, ki ima največji interes za aplikacijo modela, prevzeti iniciativo in skrbeti za to, da se bo tako pravila kot zakonitosti omenjenih sistemskih teorij in metodologij ustrezno upoštevalo. V tem primeru je po našem prepričanju to podsistem *Politika*.

- Vpliv politike kot največji od relevantnih vplivov je žal pogosto uporabljen ali zlorabljen za partikularne vplive. S tem se povečujeta subjektivnost in enostranskost v postopku USOMID/NOVOST, oba pa vodita v hitrejšo entropijo sistema. S tega vidika bi bilo potrebno okrepiti mehanizme za nadzor politike in preprečevanje njenega vpliva (depolitizacija), kjer ga ne bi smelo biti. To bi prispevalo k večji avtonomiji sodelujočih pri postopku USOMID/NOVOST in bolj celovitim razrešitvam problemov.
- Da bi se ohranilo tajnost podatkov in hkrati zagotovilo sodelovanje vseh deležnikov – tudi tistih, ki sicer nimajo dostopa do tajnih podatkov –, smo predlagali, da se v okviru DP 2 ustanoviti poseben **neodvisen organ** oziroma **komisijo**. To bi sestavljali 1 do 3 demokratično izvoljeni predstavniki za vsako področje, ki v predlaganem modelu nastopa kot podsistem. Predstavnik vsakega podsistema bi nastopal kot *posrednik* na prvem mestu in šele nato kot *posameznik z mandatom, ki mu ga je podelil podsistem*. Na takšen način bi se omogočilo izvedbo postopka USOMID/NOVOST preko predstavnikov, obenem pa zagotovilo, da se ostali subjekti preko predstavnika vključijo v sodelovanje s svojimi znanji in subjektivnimi vidiki.
- Pred oblikovanjem oziroma ustanovitvijo komisije v DP 2 je pri prvi obravnavi potrebno na podlagi konsenza med odločevalci in strokovnjaki strokovno definirati, kateri subjekti so del katerega podsistema, ki jih opredeljuje naš predlagani model, in kateri subjekti bodo vključeni v poseben organ. Na primeru Republike Slovenije se je izkazalo, da postopka ni bilo mogoče izpeljati v skladu s prvotno verzijo logistike aplikacije, ker stanje/obstoj/ureditev subjektov v državi in model nista primerljiva. Poseben organ se je zato izkazal tudi kot rešitev, ki državo, na katero se želi aplicirati model, ne sili v to, da bi subjekte v prvi aplikaciji modela popolnoma zmanjšala ali spremenila na takšen način, da bi bili (popolnoma) enaki tistim v modelu. Vseeno pa

bi bilo verjetno potrebno reorganizirati nekatere subjekte, šele nato pa v drugi aplikaciji modela vključiti predvidene podsisteme, kot to določa predlagani model.

8 Razprava

Zaupanje državljanov v matične obveščevalno-varnostne službe, ki smo ga predstavili v doktorski disertaciji, je po našem prepričanju eden izmed pomembnih dejavnikov nacionalne varnosti, ki posredno posega tudi v širše delovanje družbe in države na splošno. Raziskava, s katero smo preučili zaupanje (splošno) kot področje raziskovanja in koncept, dejavnike obveščevalno-varnostne dejavnosti, ki vplivajo na zaupanje, dejavnike zaupanja ter poiskali gradnike/sestavine zaupanja in kasneje modele zaupanja državljanov v matične obveščevalno-varnostne službe, je **potrdila** dejstvo, da gre pri tovrstnem zaupanju za **kompleksno področje**. Ugotovili smo, da zaradi vloge subjektov nadzora, strokovne javnosti, medijev, javnosti in tajnosti ter številnih dejavnikov vpliva, ki izvirajo iz sistema in okolja, med državljani in matičnimi obveščevalno-varnostnimi službami ne gre za klasičen odnos zaupanja. Izkazalo se je, da na zaupanje med omenjenima entitetama **vpliva bistveno več drugih entitet** in ne samo tretje osebe. Poleg tega gre za izjemno posebne okoliščine, saj državljani kot upniki ne morejo komunicirati s službami kot z upniki na način, kot bi si želeli. Seveda je podobno tudi pri drugih večjih organizacijah, kjer ne vzpostavljamo osebnih odnosov, vendar so te organizacije dovolj odprte ali pa delujejo toliko javno, da se državljani lahko sami prepričajo o njihovi benevolenci, integriteti, kompetentnosti in predvidljivosti ter o situacijski normalnosti in strukturnih zagotovilih. Obveščevalno-varnostne službe pa delujejo tajno, previdno in zaprto, zato je preverjanje njihove benevolence, integritete, kompetentnosti in predvidljivosti brez *tertiusa* (ki mu zaupa, ki ima vpogled v območje »onkraj zidu tajnosti«) praktično nemogoče. S tem z veliko stopnjo gotovosti **potrjujemo, da gre pri zaupanju državljanov v matične obveščevalno-varnostne službe za posebno obliko zaupanja, ki ni povsem primerljiva z ostalimi v obravnavani literaturi o zaupanju**, zato lahko **potrdimo prvo podtezo**.

Pri preverjanju **druge podteze** smo ugotovili, da teze nismo potrdili zaradi posebnosti tovrstnega zaupanja, temveč zaradi necelovitega pristopa k obravnavanju zaupanja v družbenih sistemih. Čeprav gre pri zaupanju državljanov v matične obveščevalno-varnostne službe za posebno obliko zaupanja, to **ne pomeni**, da na druge vrste zaupanja

(npr. zaupanje v policijo, vojsko, pravosodni sistem) ne vpliva enako ali večje število specifičnih dejavnikov, **temveč da jih (nam javno dostopna) literatura ne prepoznava toliko**, čeprav je jasno, da gre pri katerem koli podobnem družbenem pojavu za kompleksen dialektični sistem mnogih vplivov. Ne moremo trditi, da politika, preteklost, mediji, družbene razmere, stopnja znanja ipd. nimajo vpliva na zaupanje v policijo ali vojsko, pač pa da teh dejavnikov nam javno dostopna literatura ne obravnava. Krivično bi bilo, če bi trdili, da so bili avtorji v doktorski raziskavi omenjene literature s teh področij pri svojem delu pomanjkljivi ali pristranski, saj je jasno, da so predmet raziskovanja obravnavali v skladu s ciljem svoje raziskave. Model, ki ga predlagamo v disertaciji, sestavljajo politika, mediji, izvajalci nadzora, nacionalni obveščevalno-varnostni sistem (katerega del so tudi matične obveščevalno-varnostne službe), strokovna javnost, izobraževalni sistem, državljani in tuje obveščevalno-varnostne službe. Ti podsistemi se na prvi pogled ne razlikujejo od ostalih (podobnih) podsistemov, ki jih prepoznavajo drugi modeli, le da se naš pomembno razlikuje od drugih zaradi medsebojnih relacij, prepoznanih skritih ozadjih teh vplivov/dejavnikov, tajnosti in pa prepoznane vloge in pomembnosti znanja in izobraževanja. Čeprav smo tuje obveščevalno-varnostne službe v doktorski disertaciji obravnavali le z enega, predvsem negativnega vidika, še ne pomeni, da matične obveščevalno-varnostne službe ne bi smele sodelovati z njimi, saj brez partnerskih služb in izmenjave podatkov in informacij z njimi ne bi mogli v celoti uresničevati svojega poslanstva. V doktorski disertaciji jih obravnavamo zgolj z vidika posrednega ali neposrednega, namernega ali nenamernega povzročanja škode zaupanju državljanov v matične obveščevalno-varnostne službe. Schreier (2005) tuje obveščevalno-varnostne službe in sisteme vidi kot dobre referenčne točke za oblikovanje reform obveščevalno-varnostnega sistema. Pri tem opozarja, da reforme ne bodo uspele, dokler so uporabljene zgolj kot togi programi, na drugi strani pa različne zgodovinske, politične, strukturne in družbene značilnosti (v doktorski disertaciji uporabljamo kratico VKEN, op. G. H.) zahtevajo specifične strategije za reforme, za katere pa mora politika ustvariti potreben dialog z deležniki (ibidem, str. 154). Na podlagi prepoznanih specifičnih dejavnikov in njihovih dokazanih specifičnih vplivov **smo potrdili drugo podtezo**, da na zaupanje državljanov v matične obveščevalno-varnostne službe vpliva več specifičnih dejavnikov, kot jih prepoznava obravnavana literatura za druga sorodna

področja, vendar obenem poudarjamo, da smo do tega prišli le ob upoštevanju DTS, DOMR in USOMID/NOVOST.

Pomembno je bilo tudi spoznanje, ki smo ga v doktorski disertaciji dokazali, da drugi subjekti vplivajo na *situacijsko normalnost* in *strukturna zagotovila* ter tudi na npr. na *oblikovanje praga* in *zaupanje v kontrolni mehanizem* (izvajalce nadzora). Schreier (2005) je dejal, da vzpostavitev zaupanja potrebuje veliko pozornosti, saj je ključno za uspešno delovanje in odgovornost obveščevalno-varnostnih služb v demokratičnih družbah. Nadalje pravi (ibidem), da zgolj zakonodaja, ki vzpostavlja nadzor matičnih obveščevalno-varnostnih služb, ni dovolj, na kar smo opozorili tudi sami in to dokazali v doktorski disertaciji. »*Šele takrat, ko bodo državljani začutili, da te institucije delujejo pošteno, zakonito, odgovorno in pregledno, bo mogoče preseči zapuščino strahu in samovolje. Bolj nevarne pomanjkljivosti, ki so skupne vsem državam, so korupcija, organizirani kriminal in sistemski kronizem. Te spodkopavajo javno zaupanje, spodbujajo splošni cinizem in pomanjkanje spoštovanja zakonov – kar posledično spodkopava prizadevanja za oblikovanje delujočega gospodarstva in odvrača naložbe. Preveč politične in gospodarske moči ostaja v rokah pokvarjenih politikov in uradnikov, povezanih z organiziranim kriminalom, ki zlorabljajo obveščevalne in varnostne službe ter izkoriščajo etnične napetosti, da bi se obdržali na oblasti. Preveč obveščevalnih in varnostnih služb je neposredno ali posredno vpletenih v korupcijo in organizirani kriminal. Obstajajo celo primeri, ko se službe uporabljajo kot instrumenti za zadovoljevanje ekonomskih interesov političnega establišmenta.*« (ibidem, str. 147) Na to smo v doktorski disertaciji opozorili tudi mi, saj smo s preučevanjem strukture politike, njenih povezav z ostalimi podsistemi in njenimi potencialnimi vplivi dokazali, da politika z usmerjanjem, določanjem prioritet in vplivom na izvajanje obveščevalno-varnostne dejavnosti posredno in pomembno vpliva na učinkovitost, rezultate dela in javno podobo obveščevalno-varnostnih služb ter s tem na zaupanje državljanov v matične obveščevalno-varnostne službe. Na podlagi tega smo **potrdili tudi tretjo podtezo**.

Kompleksnost koncepta zaupanja državljanov v matične obveščevalno-varnostne službe ter razsežnosti možnih posledic pomanjkanja ali zlorabe tovrstnega zaupanja sta dva izmed vidnejših in vplivnejših razlogov, zakaj zaupanje državljanov v matične

obveščevalno-varnostne službe prepoznavamo kot enega ključnih dejavnikov delujočega in učinkovitega obveščevalno-varnostnega sistema, ki bistveno prispeva ne le k ugledu in dolgoročni stabilnosti obveščevalno-varnostnih služb, temveč tudi k ohranjanju nacionalne varnosti. V doktorski disertaciji smo zato razvili model, ki bi to zaupanje ponovno vzpostavil in ga vzdrževal ter obnavljal, predvsem pa nadgrajeval z ustreznimi pristopi in orodji, dolgoročno pa prispeval k viabilnosti matičnih obveščevalno-varnostnih služb, družbe in države.

V doktorski disertaciji smo predstavili zasnovo, potek, rezultate, ugotovitve in zaključke naše raziskave, s katero smo poiskali rešitev za izboljšanje zaupanja državljanov v matične obveščevalno-varnostne službe. Pričakujemo, da bi se predlagani model lahko uporabil v katerikoli demokratični državi, saj je bil oblikovan na način, da bi ga bilo mogoče uporabiti v vseh različnih okoljih in aplicirati kljub specifikam določenega okolja. Kljub temu ne trdimo, da je model univerzalen recept za rešitev problema tovrstnega zaupanja. Ustvarjen je tako, da zaupanje povečuje in ga vzdržuje na takšni ravni, kot je potrebno za določen sistem (v določeni državi). Opozarjamo, da model ni sredstvo za zavajanje ali doseganje napačnega zaznavanja s strani državljanov, temveč za doseganje boljših delovnih rezultatov vseh deležnikov, ustvarjanje ugodnejšega okolja za zaupanje in za uresničevanje vzajemnih koristi. Model kljub vsemu *ne garantira* boljših delovnih rezultatov subjektov, ki so kot sestavine vključeni vanj, temveč le posredno in neposredno ustvarja boljše pogoje za to. Uspešnost uporabe oziroma aplikacije modela pa je odvisna od tistih, ki ga bodo uporabili in na kakšen način ga bodo uporabili.

Primarni cilj modela je, da ponovno vzpostavi in vzdržuje celovito zaupanje državljanov v matične obveščevalno-varnostne službe. To lahko doseže s pozitivnim vplivom na presojo zaupanja znotraj vsakega državljana posebej in posledično na javno zaupanje. Na takšen način vzpostavi in dolgoročno vzdržuje celovito zaupanje v matične obveščevalno-varnostne službe, kar bi lahko imelo več pozitivnih učinkov na nacionalno varnost. Primarni cilj je mogoče predstaviti kot sklop več sekundarnih ciljev:

- vzpostaviti osnovno izobraževanje državljanov za pridobivanje osnovnega znanja in kritično razmišljanje/presojo;
- vzpostaviti odnose in komunikacijo med vsemi sestavinami modela;

- izboljšati transparentnost delovanja obveščevalno-varnostnih služb, izvajalcev nadzora in politike;
- izboljšati transparentnost, strokovnost in integriteto oseb v obveščevalno-varnostnih službah, politiki, medijih, nadzoru, strokovni javnosti in izobraževalnem sistemu;
- izboljšati strokovnost in smotrnost nadzora obveščevalnih služb;
- izboljšati znanje (o obveščevalno-varnostni dejavnosti) državljanov in vseh oseb, ki so vključeni v sistem;
- izboljšati kakovost informacij, ki jih obveščevalno-varnostne službe pripravijo za odločevalce;
- pripraviti ustrezne informacije za strokovno in splošno javnost (ter medije);
- izboljšati nacionalno varnost in varnostno kulturo;
- idr.

Uresničitev sekundarnih ciljev lahko po našem prepričanju pozitivno vpliva na presojo zaupanja državljanov. Državljani bi prepoznali več koristi od služb zaradi boljšega znanja, zaznanih boljših rezultatov (ki jih posredujejo mediji, politika, službe same ali nadzor) in manjšega števila negativnih dogodkov. Državljani bi do teh informacij prišli preko medijev, politike, služb samih ali pa izvajalcev nadzora, ki bi pri poročanju upoštevali posebnosti tega področja (tajnost, občutljivost, tveganja) in smernice za ustrezno poročanje. Zaradi usklajenega in učinkovitejšega nadzora – ki bi mu državljani s pomočjo modela tudi bolj zaupali – pa bi zaznali manj tveganj s strani matičnih obveščevalno-varnostnih služb, saj bi bilo manj zlorab pooblastil, nepravilnosti pri delu in drugih podobnih negativnih dejavnikov/vplivov. Vse skupaj bi pozitivno vplivalo na oblikovanje običajnosti situacije in na strukturna zagotovila (institucionalno zaupanje), da bodo pričakovanja državljanov kot upnikov izpolnjena s strani matičnih obveščevalno-varnostnih služb.

Ponovno poudarjamo, da tudi s predlaganim modelom celovitega zaupanja državljanov v matične obveščevalno-varnostne službe, izoblikovano logistiko aplikacije in programoteko **ni mogoče zagotoviti, da bodo vsi ljudje enako presojali zaupanje**. Z modelom želimo doseči, da bo med državljani **več zaupanja kot nezaupanja** v matične

obveščevalno-varnostne službe, hkrati pa mora obstajati **ustrezno razmerje** zaupanja in nezaupanja. Tega ne moremo matematično ali generično določiti, saj je to odvisno od vsakega posameznika oziroma konkretnega primera posebej. Razrešitev problema, ki ga obravnavamo, državljanom ne vsiljuje zaupanja, temveč jih spodbuja k temu, da bi zaupali. Vsak državljan ima pravico zaupati ali ne zaupati matičnim obveščevalno-varnostnim službam.

Večji sistem je nemogoče prilagoditi čisto vsakemu posamezniku, temveč ga je potrebno prilagoditi večini, zato je treba spremljati mnenje večine. V doktorski disertaciji nismo predlagali podrobno izdelanega načina, kako spremljati in meriti zaupanje, saj menimo, da je njegovo oblikovanje v domeni strokovnjakov z drugih področij (metodologija, statistika, javno mnenje in merjenje javnega mnenja). Mayer et al. (1995) pravijo, da so različni avtorji s svojimi konceptualizacijami zaupanja potrdili dejstvo, da zaupanje kot pojav ni objektivna realnost/resnica, temveč percepcija upnika, zato Brower et al. (2000) dodajajo, da je merjenje oziroma merilo zaupanja subjektivna, individualna stvar. V zvezi s tem spomnimo na odgovor oziroma komentar v intervjuju z nekdanjim uslužbencem Sove, ki je vprašal, kako lahko državljani ocenjujejo nekaj, o čemer ne vedo veliko ali vedo napačne stvari. Drugi intervjuvanec pa je dejal, da bi »vsako merjenje zaupanja v te službe dalo izkrivljeno sliko,« saj je delovanje obveščevalno-varnostnih služb »tajno in skrito pred očmi javnosti.« Pomisleki na strani intervjuvancev so po našem prepričanju za trenutne razmere (tj. v času pisanja doktorske disertacije) upravičeni, pričakovani in povsem utemeljeni. Pričakujemo pa, da bi se to **v razmerah, ko je model apliciran, spremenilo oziroma izboljšalo,** saj predvideva pridobitev znanja, na čigar podlagi bi dobili bolj realno oceno/sliko zaupanja v javnosti. Informacije o stanju zaupanja državljanov v matične obveščevalno-varnostne službe so nedvomno pomembne za delovanje sistema v skladu z modelom, saj ne prikažejo zgolj posameznih, subjektivnih vidikov, temveč so kolektiven odraz javnosti, zato bi bilo oblikovanju ustreznega načina za merjenje in spremljanje zaupanja potrebno nameniti posebno pozornost, čas in sredstva. Mnenje večine se navadno ugotavlja z anketiranjem, pri katerem je mogoče z ustreznimi izračuni določiti, kolikšen mora biti interval statističnega zaupanja, da so rezultati reprezentativni za določeno populacijo. To pomeni, da morajo javnomnenjske raziskave kazati, da je med državljani več zaupanja v matične obveščevalno-varnostne

službe kot pa nezaupanja. Čeprav je naš cilj, da z modelom dosežemo celovito zaupanje, bi bilo na podlagi ravnokar pojasnjenega naivno predvidevati in verjeti, da bo *vsak* državljan (bolj) zaupal službam (kot pa jim ne zaupal). Ob tem bi morali državljane opozoriti, da vedno obstaja možnost napak in zlorab, le da jih naš predlagani model poskuša čimbolj zmanjšati in hkrati zmanjšati njihov vpliv, kar smo želeli doseči z uporabo ustreznih sistemskih teorij, metodologij in metod (DTS, DOMR, USOMID/NOVOST, TVS/MVS).

Model z vključevanjem ostalih podsistemov v preoblikovanje celotnega sistema zagotovo spodbuja državljanov čut za odgovornost, s širjenjem ustrezne stopnje znanja pa povečuje razumevanje koncepta zakonitosti ter spoštovanja vladavine prava, človekovih pravic in svoboščin. Pričakujemo, da bi omogočal tudi sodelovanje javnosti in zainteresiranih posameznikov pri razreševanju občutljivih vprašanj, povezanih z obveščevalno-varnostno dejavnostjo. Čeprav bi s predlagano komisijo omejili neposredno sodelovanje vsakemu posamezniku posebej (to namreč preprečuje že princip tajnosti), je sodelovanje kljub temu omogočeno in usklajeno z metodologijo USOMID/NOVOST in z zastopanjem.

Model sam po sebi ni dovolj za doseganje želenih rezultatov, potrebna je njegova **pravilna aplikacija**. Da bi bil model ustrezno apliciran, smo podrobno opredelili logistiko aplikacije modela, tj. zadostno in potrebno celovito podprt postopek aplikacije oziroma uvedbe modela v prakso v skladu s programoteko. Logistika ima pomembno vlogo, saj v postopku aplikacije modela združuje različne znanstvene discipline z namenom načrtovanja, organiziranja, vodenja in kontrole tokov materiala, ljudi, energije in informacij. Tako aplikacijo kot **programoteko** smo razvili v skladu s DTS, DOMR in USOMID/NOVOST. Programoteko smo z uporabo izoblikovane logistike aplikacije teoretično aplicirali na Republiko Slovenijo in s tem poiskali vplivne dejavnike. S prepoznanimi dejavniki smo ugotovili, kaj bi bilo potrebno spremeniti in dodati, da bi bilo mogoče model aplicirati brez večjih zapletov. Čeprav smo del teoretične aplikacije izvedli na podlagi predvidevanj in domnev, se je že v postopku strukturiranja delnih procesov z vpeljevanjem USOMID/NOVOST pokazalo, da model in aplikacija **med podsisteme vnašata sodelovanje in komunikacijo**. Sinergije, do katerih pride ob tem,

prinašajo boljše rezultate za vse strani. Z izboljšanjem lastnega delovanja ter z izboljšanjem medsebojnega sodelovanja, komunikacije, koordinacije ter pravočasnega in učinkovitega odzivanja na notranje in zunanje dejavnike se postopno zmanjšuje in odvrača negativne dejavnike, ki vplivajo na delovanje in obstoj podsistemov. Na podlagi tega lahko **potrdimo osrednjo tezo doktorske disertacije**, da izdelava in ustrezna logistika aplikacije modela celovitega zaupanja državljanov v obveščevalno-varnostne službe **omogočata upočasnitev entropije** obveščevalno-varnostnega podsistema in sistema nacionalne varnosti, ki sta z vidika obravnavane problematike doktorske disertacije osrednja (pod)sistema.

S tem zaključujemo našo raziskavo in dokazujemo, da model zaupanja državljanov v matične obveščevalno-varnostne službe predstavlja izvirni znanstveni prispevek na področju delovanja in izboljšanja nacionalnega obveščevalno-varnostnega podsistema oziroma sistema nacionalne varnosti, ki lahko v praksi prispeva k razvoju na omenjenih področjih.

8.1 Omejitve in možnosti nadaljnjega razvoja modela

Model in ima nekaj omejitev, ki jih je potrebno upoštevati. Prvič, model temelji le na izbranih konceptih in modelih zaupanja ter se naslanja na definicijo zaupanja, ki smo jo sami predlagali na podlagi razpoložljive literature in našega razumevanja zaupanja. Model je zato potrebno obravnavati v okviru izbranih teorij in v kontekstu, saj bi obravnava osrednjega problema z uporabo drugih teorij lahko pripeljala do drugačnih vidikov. To ne pomeni, da je predlagani model povsem napačen ali pravilen, pač pa da je z našega vidika obravnavanja utemeljen.

Drugič, model je splošno strukturiran in vključuje le določene vsebinsko zaokrožene, za naš vidik preučevanja pomembne podsisteme. Uvajanje dodatnih podsistemov bi po naši oceni prispevalo k preveč ozko usmerjenemu modelu, zaradi česar bi izgubil možnost aplikacije na najširši krog obstoječih sistemov po svetu. Kljub temu je mogoče in hkrati potrebno model prilagoditi okolju, v katerem se nahaja sistem, saj model ne predvideva podrobnejših delitev posameznih podsistemov. Model je torej mogoče bolj podrobno

prilagoditi točno določeni državi, ni pa ga mogoče podrobno prilagoditi in razčleniti za vse države na splošno. Obenem bo model potrebno nadgrajevati tudi zato, ker se bo zaradi spreminjanja družbe spreminjal posameznik (in obratno), kar pomeni, da se bodo spreminjale tudi VKEN. S tem se bo spreminjalo tudi varnostno okolje.

Tretjič, predstavljen model je le teoretičen in ni bil preizkušen v praksi. Aplikacija modela na Republiko Slovenijo je potekala teoretično, predvsem zaradi iskanja vplivnih dejavnikov, na podlagi katerih bi lahko izboljšali logistiko aplikacijo modela, in ne toliko zaradi iskanja hipotetičnih rezultatov/izidov za Republiko Slovenijo. Zaradi splošnosti in raznolikosti obstoječih obveščevalno-varnostnih sistemov po svetu bi težko preverili ustreznost predlaganega modela zgolj na podlagi teoretičnih hipotez, kot je to v navadi. Zato nismo testirali veljavnosti modela, saj bi morali strukturo predlaganega modela oblikovati tako, da bi bila enaka ali podobna obstoječim podsistemom. Cilj naše raziskave je bil predlagati *nov* model, ki bi vzpodbudil širšo razpravo o zaupanju državljanov v matične obveščevalno-varnostne službe. S tega vidika je stvar diskusije, ali je verzijo modela, ki je nadgrajena na podlagi spoznanj iz teoretične aplikacije, že mogoče aplicirati na realni sistem ali ga je treba na teoretični ravni razvijati še naprej oziroma nadgraditi.

Četrtič, za uporabo in aplikacijo modela mora obstajati politična volja. Ker so si tako politični sistemi kot kulture družb različni, nismo predpostavljali, kako je mogoče doseči politično voljo. Kljub temu menimo, da bi bilo potrebno sodelovanje vseh podsistemov iz predlaganega modela, da se najprej doseže skupni (tudi politični) konsenz, iz katerega bo izhajala tudi politična volja za aplikacijo modela.

Petič, bistvenega pomena je, da se za aplikacijo modela uporabi posebne smernice in priporočila, ki smo jih razvili v skladu z izbranimi sistemskimi teorijami in njihovimi metodologijami za inoviranje in aplikacijo inovacij (DTS, DOMR, USOMID/NOVOST). Te namreč med drugim upoštevajo zakon zadostne in potrebne celovitosti in preprečujejo, da bi aplikacija modela kaj izpustila ali prepustila naključju. Tako bi se sistem, na katerega bi bil model apliciran, bolj približal zadostni celovitosti – enako pa tudi zaupanje.

Šestič, model bi zagotovo lahko izboljšali s sodelovanjem večjega števila strokovnjakov z različnih področij. Ocenjujemo, da bi bilo potrebno sodelovanje strokovnjakov s področja zaupanja, prava, menedžmenta, nacionalne varnosti, varstvoslovja, obramboslovja, politologije, javne uprave, psihologije, pedagogike, andragogike, sociologije, novinarstva, komunikologije, odnosov z javnostmi, informacijskih sistemov, teorije sistemov, metodologije, statistike in drugih relevantnih področij. Po našem prepričanju nudi predlagani model v tej obliki veliko izhodišč za nadaljnje raziskovanje doslej še relativno skromno raziskanega področja. Služi pa lahko predvsem kot podlaga za skupni dialog med politiko, prakso, znanostjo, izobraževalnim sistemom in zainteresirano javnosti, v katero smer in na kakšen način je potrebno skupaj delovati na področju povrnitve in vzdrževanja zaupanja državljanov v obveščevalne službe.

Navajamo tudi nekaj vprašanj (in s tem predlogov), ki bi jih bilo v okviru prihodnjih raziskav potrebno nasloviti za bolj podrobno raziskovanje in razvijanje modela:

- Katero znanje je »ustrezno znanje«, ki ga državljani potrebujejo, da lahko ustrezno presojajo zaupanje?
- Kdo, kdaj in kako pogosto bi bilo treba obveščati javnost? Kako je s koordinacijo in morebitno centralizacijo obveščanja javnosti v pomembnih obveščevalno-varnostnih zadevah?
- Kaj bi moralo biti tajno v postopku aplikacije modela in kako bi to vplivalo na zaupanje državljanov, če bi bili zaradi zadev, ki bi bile tajne, omejeni v procesu aplikacije?
- Kakšno bi moralo biti merjenje zaupanja in kako pogosto?
- Kako vzpostaviti in utrditi sodelovanje med sestavinami (podsistemi) predlaganega modela?
- Koliko finančnih/proračunskih, kadrovskih, materialnih in sredstev je potrebno nameniti za aplikacijo modela in vzdrževanje celovitega zaupanja državljanov v matične obveščevalno-varnostne službe?
- Kakšno vlogo imajo pri tem mednarodne varnostne organizacije in mednarodni akti (konvencije, protokoli, predpisi ipd.)?

- Kako ustrezno prekiniti s preteklostjo/zgodovino in v kolikšni meri? Koliko preteklosti je »potrebno obdržati pri življenju« za ustrezne oziroma normalne kulturne, vzgojne, izobraževalne in druge podobne namene?

Zaključek

V celotni doktorski raziskavi in pri pisanju doktorske disertacije smo iskali odgovor na vprašanje, ki nas je vseskozi gnalo in motiviralo: *Zakaj naj bi državljani zaupali oziroma zakaj morajo zaupati matičnim obveščevalno-varnostnim službam?* Šele na samem koncu smo prišli do dovolj jasnega in strnjenega odgovora, ki se po našem prepričanju glasi takole:

Državljani **morajo** zaupati matičnim obveščevalno-varnostnim službam, saj z zaupanjem **prenesejo del zagotavljanja lastne viabilnosti na službe**. Služba, ki ne zaznava zaupanja, bo slabše opravljala svoje naloge in poslanstvo, s tem pa ogrozila ne le lastno viabilnost, temveč tudi viabilnost državljanov in celotne države. Državljani s celovitim zaupanjem pokažejo troje:

- vzdržujejo lastno viabilnost z zaupanjem določenih nalog matičnim obveščevalno-varnostnim službam;
- službi nudijo ustrezno podporo za zagotavljanje nalog, ki koristi njihovi lastni viabilnosti, viabilnosti služb, viabilnosti drugih, tj. celotne družbe (družbena odgovornost) in s tem viabilnosti države;
- preprečujejo, da bi prišlo do zlorabe ali oškodovanja njihove lastne viabilnosti.

Če takšnega zaupanja ni, državljani **največjo škodo posredno** povzročimo službi, družbi in državi, predvsem pa jo **povzročamo sami sebi**.

Seznam literature in virov

Аслан Масхадов скорее жив, чем мёртв [NTV.ru]. (2002). Najdeno 3. februarja 2018 na spletnem naslovu: https://www.ntv.ru/novosti/2132/

ФСБ предотвратила антироссийские действия ЦРУ [NTV.ru]. (2003). Najdeno 3. februarja 2018 na spletnem naslovu: https://www.ntv.ru/novosti/9113

Aftergood, S. (2018, 3. april). *DNI Says Build Trust in Intelligence Through Transparency.* Najdeno 10. aprila 2018 na spletnem naslovu: https://fas.org/blogs/secrecy/2018/04/trust-transparency/

Agent. (b. d.). V *Slovar slovenskega knjižnega jezika.* Najdeno 2. februarja 2018 na spletnem naslovu: http://bos.zrc-sazu.si/cgi/neva.exe?name=ssbsj&tch=14&expression=zs%3D366

Althoff, M. (2016). Human Intelligence. V M. M. Lowenthal & R. M. Clark, *The 5 Disciplines of Intelligence Collection* (str. 45-80). Thousand Oaks, CA: CQ Press.

Anžič, A. (1996). Nadzorstvo nad obveščevalnimi službami. *Teorija in praksa,* 33 (2), str. 194-207.

Anžič, A. (1997). *Varnostni sistem Republike Slovenije.* Ljubljana: Uradni list Republike Slovenije.

Anžič, A. (2000). Tajnost: vrednota in zlo. *Teorija in praksa,* 37 (5), str. 849-863.

Anžič, A. & Golobinek, R. (2003). Slovenski model parlamentarnega nadzorstva nad obveščevalnimi in varnostnimi službami. *Teorija in praksa,* 40 (6), str. 1058-1073.

Arnott, D. C. (2007). Trust - current thinking and future research. *European Journal of Marketing,* 41 (9/10), str. 981-987.

Ashby, W. R. (1957). *The Introduction to Cybernetics (Second Impression).* London: Chapman & Hall Ltd.

Atribucija. (b. d.). V *Termania.* Najdeno 21. decembra 2016 na spletnem naslovu: http://www.termania.net/slovarji/terminoloski-slovar-vzgoje-in-izobrazevanja/3474347/atribucija

Baldino, D. (2018, 30. maj). Accountability is key to building trust in Australia's. *The Conversation*. Najdeno 31. januarja 2019 na spletnem naslovu:

http://theconversation.com/accountability-is-key-to-building-trust-in-australias-intelligence-community-95426

Baynard, D., Bell, A., Broekhof, M., Chitnis, A., Gruenberg, L. & Wastcoat, S. (2013). *How Can We Trust Intelligence Agencies? (Draft).* Cambridge: The Wilberforce Society. Najdeno 27. januarja 2017 na spletnem naslovu: http://thewilberforcesociety.co.uk/wp-content/uploads/2015/07/Intelligence-2.pdf

Beckford, J. L. (1995). *Towards a Participative Methodology for Viable System Diagnosis*. Najdeno 5. januarja 2018 na spletnem naslovu: http://beckfordconsulting.com/Papers/ParticipativeVSM.doc.pdf

Beer, S. (1981). *Brain of the Firm. Second Edition.* Chichester, New York, Brisbane, Toronto: John Wiley & Sons.

Beer, S. (1984). The Viable System Model: Its Provenance, Development, Methodology and Pathology. *The Journal of the Operational Research Society,* 35 (1), str. 7-25.

Beer, S. (1985). *Diagnosing the System for Organizations.* Chichester: Wiley.

Benevolenca. (b. d.). V *Slovar slovenskega knjižnega jezika.* Najdeno 7. julija 2017 na spletnem naslovu: http://bos.zrc-sazu.si/cgi/a03.exe?name=sskj_testa&expression=ge=benevolenca

Bernik, I., Malnar, B., Pollack, D., Pickel, G. & Müller, O. (2014). Politična kultura in demokratične vrednote v novih demokracijah. V N. Toš (ur.), *Vrednote v prehodu VIII.: Slovenija v srednje in vzhodnoevropskih primerjavah* (str. 435-582). Ljubljana; Wien: Univerza v Ljubljani, Fakulteta za družbene vede, IDV – CJMMK; Edition Echoraum.

Besley, T. & Pratt, A. (2006). Handcuffs for the grabbing hand?: media capture and government accountability. *American economic review,* 96 (3), 720-736.

Bijlsma, K. & Koopman, P. (2003). Introduction trust within organisations. *Personnel Review,* 32 (5), str. 543-555.

Bochel, H. & Defty, A. (2017). Parliamentary Oversight of Intelligence Agencies: Lessons from Westminster. V A. W. Neal (ur.), *Security in a Small Nation: Scotland, Democracy, Politics* (str. 103-124). Cambridge, UK: Open Book Publishers.

Boon, S. D. & Holmes, J. G. (1991). The dynamics of interpersonal trust: Resolving uncertainty in the face of risk. V R. A. Hinde & J. Groebel, *Cooperation and prosocial behaviour* (str. 190-211). Cambridge: Cambridge University Press.

Born, H. (2003). *Parliamentary oversight of the security sector: Principles, mechanisms and practices.* Geneva: Inter-Parliamentary Union; Geneva Center for the Democratic Control of Armed Forces.

Born, H. (2013). *Parliamentary oversight of the security sector.* Brussels: European Parliament, Office for Promotion of Parliamentary Democracy.

Born, H. & Geisler Mesevage, G. (2012). Introducing Intelligence Oversight. V H. Born & A. Wills (ur.), *Overseeing Intelligence Services: A Toolkit* (str. 3-22). Geneva: The Geneva Centre for the Democratic Control of Armed Forces (DCAF).

Born, H. & Leigh, I. (2005). *Making Intelligence Accountable: Legal Standards and Best Practice for Oversight of Intelligence Agencies.* Oslo: Publishing House of the Parliament of Norway.

Born, H. & Leigh, I. (2007). *Democratic Accountability of Intelligence Services.* Geneva: Geneva Centre for the Democratic Control of Armed Forces.

Born, H. & Mesevage, G. G. (2012). Introducting Intelligence Oversight. V H. Born & A. Wills (ur.), *Overseeing Intelligence Services: A Toolkit* (str. 3-24). Geneva: Geneva Centre for the Democratic Control of Armed Forces.

Bosch, O. & Nguyen, N. (2015). *Systems thinking for everyone: The journey from theory to making an impact.* Kingston, ACT: Think2Impact Pty Ltd.

Boyce, C. & Neale, P. (2006). *Conducting In-Depth Interviews: A Guide for Designing and Conducting In-Depth Interviews for Evaluation Input.* Watertown, MA: Pathfinder International.

Brezovšek, M. & Črnčec, D. (2004). Tajnost v demokraciji. *Teorija in praksa,* 41 (3-4), str. 506-523.

Britovšek, J. & Čretnik, A. (2016). Obveščevalno-varnostni sistem Republike Slovenije: reorganizacija in sistemske rešitve. *Varstvoslovje,* 18 (3), str. 325-348.

Brocklesby, J. & Cummings, S. (1996). Designing a Viable Organizational Structure. *Long Range Planning,* 29 (1), str. 49-57.

Brod, G., Werkle-Bergner, M. & Shing, Y. L. (2013). The Influence of Prior Knowledge on Memory: A Developmental Cognitive Neuroscience Perspective. *Frontiers in Behavioral Neuroscience,* 7 (139), str. 1-13.

Brower, H. H., Schoorman, F. D. & Tan, H. H. (2000). A model of relational leadership: the integration of trust and leader–member exchange. *Leadership Quarterly*, 11 (2), str. 227-250.

Burke, C. S., Sims, D. E., Lazzara, E. H. & Salas, E. (2007). Trust in leadership: A multi-level review and integration. *The Leadership Quarterly*, 18 (2007), str. 606-632.

Cajner Mraović, I. (2004). Community Policing Action Strategy in Croatia. V M. Hadžić (ur.), *The Role of Parliament in Security Sector Reform in the Countries of the Western Balkans: Collection of Papers and Discussions* (str. 95-105). Belgrade: Centre for Civil-Military Relations.

Camén, C., Gottfridsson, P. & Rundh, B. (2011). To trust or not to trust? Formal contracts and the building of long-term relationship. *Management Decision*, 49 (3), str. 365-383.

Chua, R. J., Ingram, P. & Morris, M. W. (2008). From the Head and the Heart: Locating Cognition- and Affect-Based Trust in Managers' Professional Networks. *The Academy of Management Journal*, 51 (3), str. 436-452.

Clark, R. M. (2007). *Intelligence Analysis: A Target-Centric Approach.* Washington (D.C.): CQ Press.

Coats, D. (2018, 22. marec). *Memorandum - Issuance of Updated Intelligence Community Directive 107 on Civil Liberties, Privacy, and Transparency*. Najdeno 7. aprila 2018 na spletnem naslovu: https://assets.documentcloud.org/documents/4421360/ICD-107-MEMO.pdf

Cole, E., Fluri, P. & Lunn, S. (2015). *Oversight and Guidance: Parliaments and Security Sector Governance.* Geneva: DCAF.

Corritore, C. L., Kracher, B. & Wiedenbeck, S. (2003). On-line trust: concepts, evolving themes, a model. *International Journal of Human-Computer Studies*, 58, str. 737-758.

Creed, D. W. & Miles, R. E. (1996). Trust in Organizations: A Conceptual Framework Linking Organizational Forms, Managerial Philosophies, and the Opportunity Costs of Controls. V R. M. Kramer & T. R. Tyler (ur.), *Trust in Organizations:*

Frontiers of Theory and Research (str. 16-38). Thousand Oaks, London, New Delhi: Sage Publications.

Črnčec, D. (2003). Obveščevalno-varnostna služba Ministrstva za obrambo kot conditio sine qua non obveščevalno varnostne skupnosti Republike Slovenije. V M. Pagon (ur.), *Dnevi varstvoslovja 2003* (str. 1-13). Ljubljana: Visoka policijsko-varnostna šola.

Črnčec, D. (2009). *Obveščevalna dejavnost v informacijski dobi.* Ljubljana: Defensor.

Das, T. K. & Teng, B.-S. (2004). The RIsk-Based View of Trust: A Conceptual Framework. *Journal of Business and Psychology*, 19 (1), 85-116.

Davison, M. G. (2004). Opening of the Conference - Mark G. Davison, Deputy Head of the OSCE Mission to Serbia and Montenegro. V M. Hadžić, *The Role of Parliament in Security Sector Reform in the Countries of the Western Balkans: Collection of Papers and Discussions* (str. 14-15). Belgrade: Centre for Civil-Military Relations.

Dedijer, S. (2005). Obveščevalna knjižnica v obveščevalnem živčnem sistemu Slovenije? *Organizacija znanja*, 20 (3), str. 124-129.

Delhey, J. & Newton, K. (2003). Hwo trusts? The Origin of social trust in seven societies. *European Societies*, 5 (2), str. 93-173.

Deutsch, M. (1958). Trust and Suspicion. *Journal of Conflict Resolution*, str. 265-279.

Dialog. (b. d.). *Slovar slovenskega knjižnega jezika.* Najdeno 26. aprila 2017 na spletnem naslovu: http://bos.zrc-sazu.si/cgi/a03.exe?name=sskj_testa&expression=ge=dialog

Doney, P. M., Cannon, J. P. & Mullen, M. R. (1998). Understanding the influence of national culture on the development trust. *Academy of Management Review*, 23 (3), str. 601-620.

Drucker, P. F. (1967). *The effective executive.* New York: Harper & Row.

Državni zbor. (2016). *Priporočilo v zvezi z zagotavljanjem učinkovitejšega dela obveščevalno-varnostnega sistema RS, EPA: 1269 - VII.* Ljubljana: Državni zbor. Najdeno 3. marca 2017 iz https://www.dz-rs.si/wps/portal/Home/deloDZ/zakonodaja/izbranZakonAkt?uid=C1257A70003EE749C1257FF100440E17&db=kon_akt&mandat=VII&tip=doc#

Dvoršek, N. & Podbregar, I. (2012). Analitika v obveščevalno-varnostni dejavnosti. V I. Podbregar (ur.), *Obveščevalno-varnostna dejavnost: procesi, metode, nadzor* (str. 137-272). Ljubljana: Fakulteta za varnostne vede.

Ebert, T. (2007). Interdisciplinary Trust Meta-Analysis: Analysis of High Rank Trust Articles between 1966 and 2006. V *Discussion Papers in Business Administration 2007-1.* Munich: University of Munich, Munich School of Management. Najdeno 13. julija 2017 na spletnem naslovu: https://core.ac.uk/download/pdf/12162438.pdf

Ebo, A. (2008). Local Ownership and Emerging Trends in SSR: A Case Study of Outsourcing in Liberia. V T. Donais (ur.), *Local Ownership and Security Sector Reform* (str. 149-167). Zürich, Berlin: LIT Verlag.

Ehrman, J. (2009). Toward a Theory of CI: What are We Talking About When We Talk about Counterintelligence? *Studies in Intelligence*, 53 (2), str. 5-20.

Espejo, R. & Gill, A. (1997). *The Viable System Model as a Framework for Understanding Organizations.* Najdeno 3. novembra 2017 na spletnem naslovu: https://www.researchgate.net/profile/Raul_Espejo/publication/265740055_The_Viable_System_Model_as_a_Framework_for_Understanding_Organizations/links/54dc62140cf23fe133b14526/The-Viable-System-Model-as-a-Framework-for-Understanding-Organizations.pdf

Espejo, R. & Reyes, A. (2011). *Organizational Systems: Managing Complexity with the Viable System Model.* Berlin, Heidelberg: Springer-Verlag.

Eurobarometer. (2015). *Standard Eurobarometer 83 – Spring 2015: "Public opinion in the European Union".* Najdeno 20. septembra 2016 na spletnem naslovu: http://ec.europa.eu/public_opinion/archives/eb/eb83/eb83_publ_en.pdf

Evropska komisija. (2014). *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Enlargement Strategy and Main Challenges 2014-15. COM(2014) 700 final. {SWD(2014) 307 final}.* Bruselj: Evropska komisija.

Evropska komisija. (2017). *White paper on the future of Europe: Reflections and scenarios for the EU27 by 2025.* Bruselj: Evropska komisija.

Faith. (b. d.). V *Online Etymology Dictionary.* Najdeno 2016. decembra 19 na spletnem naslovu: http://www.etymonline.com/index.php?term=faith

Faulkner Rogers, J. (2013, 11. oktober). Public opinion and the Intelligence Services. *YouGov.co.uk*. Najdeno 7. avgusta 2017 na spletnem naslovu: https://yougov.co.uk/news/2013/10/11/british-attitudes-intelligence-services/

Ferš, D. (2002). From Security and Intelligence Service to Slovene Intelligence and Security Agency. *National Security and the Future*, 2 (3), str. 61-80.

Fink Hafner, D., Krašovec, A. & Kustec Lipicer, S. (2002). *Dejavniki v oblikovanju (ne)zaupanja v Državni zbor: Zaključno poročilo.* Ljubljana: Fakulteta za družbene vede, Inštitut za družbene vede, Center za politološke raziskave, Center za raziskovanje javnega mnenja in množičnih komunikacij.

Fitsanakis, J. & Hodges, K. A. (2013). Sense of Trust: Restoring Public Faith in Southern European and Balkan Intelligence Agencies in an Age of Austerity. *Journal of Mediterranean and Balkan Intelligence*, 1 (1), str. 15-32.

Flexon, J. L., Lurigio, A. J. & Greenleaf, R. G. (2009). Exploring the dimensions of trust in the police among Chicago juveniles. *Journal of Criminal Justice*, 37 (2009), str. 180-189.

Frankovič, M. & Preston, M. (1993). Sodobni obveščevalni sistemi (Analiza primerov ZDA, Izraela in Avstrije). *Teorija in praksa*, 30 (11-12), str. 1277-1284.

Fraumann, E. (1997). Economic Espionage: Security Missions Redefined. *Public Administration Review*, 57 (4, Jul. – Aug., 1997), str. 303-308.

Frelih, P. (2017, 10. februar). Zoran Krunić: "Povprečen Slovenec občuduje Jamesa Bonda, zgraža pa se nad UDBO". *Russia Beyond the Headlines - si.rbth.com*. Najdeno 6. avgusta 2017 na spletnem naslovu: https://si.rbth.com/politics_and_society/2017/02/10/zoran-krunic-povprecen-slovenec-obcuduje-jamesa-bonda-zgraza-pa-se-nad-udbo_699498

Friedrich, R. & Luethold, A. (2008). And They Came In and Took Possession of Reforms: Ownership and Palestinian SSR. V T. Donais (ur.), *Local Ownership and Security Sector Reform* (str. 191-213). Zürich, Berlin: LIT Verlag.

Frowe, I. (2005). Professional Trust. *British Journal of Educational Studies*, 53 (1), str. 34-53.

Fukuyama, F. (1995). *Trust: Social Virtues and the Creation of Prosperity.* New York: Free Press.

G. C. & T. H. (2015, 7. september). Sova zalotena pri vohunjenju za Avstrijci. Grims: Preusmeritev pozornosti zaradi beguncev. *Rtvslo.si*. Najdeno 4. oktobra 2017 na spletnem naslovu: https://www.rtvslo.si/crna-kronika/sova-zalotena-pri-vohunjenju-za-avstrijci-grims-preusmeritev-pozornosti-zaradi-beguncev/373400

Gambetta, D. (1988). Can we trust? V D. Gambetta (ur.), *Trust: Making and Breaking Cooperative Relations* (str. 213-237). Oxford: Basil Blackwell Ltd.

Ganesan, S. (1994). Determinants of Long-Term Orientation in Buyer-Seller Relationships. *Journal of Marketing*, 58 (2), str. 1-19.

Gendron, A. (2005). Just War, Just Intelligence: An Ethical Framework for Foreign Espionage. *International Journal of Intelligence and CounterIntelligence*, 18 (3), str. 398-434.

Geneva Centre for the Democratic Control of Armed Forces. (2011). *Intelligence Legislation Model: The Netherlands. Intelligence and Security Services Act, 2002.* Geneva: Geneva Centre for the Democratic Control of Armed Forces.

Gentry, J. A. (2008). Intelligence Failure Reframed. *Political Science Quarterly*, 123 (2), str. 247-270.

Gidman, W., Ward, P. & McGregor, L. (2012). Understanding public trust in services provided by community pharmacist relative to those provided by general practitioners: a qualitative study. *BMJ Open*, 2, str. 1-11.

Gill, P. (2007). Evaluating intelligence oversight committees: The UK Intelligence and Security Committee and the 'war on terror'. *Intelligence and National Security*, 22 (1), str. 14-37.

Gill, P. (2009). Security intelligence and human rights: Illuminating the “heart of darkness”? *Intelligence and National Security*, 24 (1), str. 78-102.

Gill, P. & Phythian, M. (2006). *Intelligence in an Insecure World.* Cambridge; Malden: Polity Press.

Godsiff, P. (2010). Service Systems and Requisite Variety. *Service Science*, 2 (1-2), str. 92-101.

Godson, R. (2011). *Dirty Tricks or Trump Cards: U.S. Covert Action & Counterintelligence.* New Brunswick; London: Transaction Publishers.

Goerner, S. J., Dyck, R. G. & Lagerroos, D. (2008). *The New Science of Sustainability: Building a Foundation for Great Change.* Chapel Hill, North Carolina: Triangle Center for Complex Systems.

Goldman, Z. K. & Rascoff, S. J. (2016). Introduction. V Z. K. Goldman & S. J. Rascoff (ur.), *Global intelligence oversight: governing security in the tewnty-first century* (str. xvii-xxxi). Oxford: Oxford University Press.

Goldsteen, R., Schorr, J. K. & Goldsteen, K. S. (1989). Longitudinal study of appraisal at Three Mile Island: Implications for life event research. *Social Science and Medicine*, 28 (4), 389-398.

Grobman, G. M. (2005). Complexity theory: a new way to look at organizational change. *Public Administration Quarterly*, 29 (3), str. 350-382.

Happer, C. & Philo, G. (2016). The Role of the Media in the Construction of Public Belief and Social Change. *Journal of Social and Political Psychology*, 1 (1), 321-336.

Hardy, K. & Williams, G. (2016). Executive Oversight of Intelligence Agencies in Australia. V Z. K. Goldman & S. J. Rascoff (ur.), *Global intelligence oversight: governing security in the tewnty-first century* (str. 315-342). Oxford: Oxford University Press.

Hart, K. (1988). Kinship, Contract, and Trust: The Economic Organization of Migrants in an African City Slum. V D. Gambetta (ur.), *Trust: Making and breaking cooperative relations* (str. 176-193). Oxford: Blackwell.

Hawrood, S. A. (2012). The management of change and the Viplan Methodology in practice. *The Journal of the Operational Research Society*, 63 (6), str. 748-761.

Heintzman, R. & Marson, B. (2005). People, service and trust: is there a public sector service value chain? *International Review of Administrative Sciences*, 71 (4), str. 549-575.

Hevristika. (b. d.). V *Slovar slovenskega knjižnega jezika.* Najdeno 18. septembra 2017 na spletnem naslovu: http://bos.zrc-sazu.si/cgi/a03.exe?name=sskj_testa&expression=ge=hevristika

Hildbrand, S. & Bodhanya, S. (2015). Guidance on applying the viable system model. *Kybernetes*, 44 (2), str. 168-201.

Hočevar, B. (2011, 3. februar). Kaj je obveščevalno-varnostna dejavnost? *Delo*. Najdeno 10. oktobra 2017 na spletnem naslovu: http://www.delo.si/novice/slovenija/kaj-je-obvescevalno-varnostna-dejavnost.html

Hoffman, L. J., Lawson-Jenkins, K. & Blum, J. (2006). Trust beyond security: an expanded trust model. *Communications of the ACM*, 49 (7), str. 94-101.

Hosmer, L. T. (1995). Trust: The Connecting Link between Organizational Theory and Philosophical Ethics. *The Academy of Management Review*, 20 (2), str. 379-403.

Hribar, G. (2013). *Metode protiobveščevalnega delovanja: študija arhivskega gradiva Republike Slovenije* (magistrska naloga). Ljubljana: Fakulteta za varnostne vede.

Hribar, G. (2016). The foundations of counterintelligence: definition and principles. V T. Ivanuša & I. Podbregar (ur.), *The Anatomy of Counterintelligence* (str. 24-42). Sharjah: Bentham Science Publishers.

Hribar, G., Podbregar, I. & Ivanuša, T. (2014). OSINT: A »Grey Zone«? *International Journal of Intelligence and CounterIntelligence*, 27 (3), str. 529-549.

Hulnick, A. S. (2005). Indications and Warning for Homeland Security: Seeking a New Paradigm. *International Journal of Intelligence and CounterIntelligence*, 18 (4), str. 593-608.

Hurley, R. F. (2006). The Decision to Trust. *Harward Business Review*, 84 (9), str. 55-62.

Hurley, R. F. (2012). *The Decision to Trust: How Leaders Create High-Trust Organizations.* San Francisco, CA: Jossey-Bass.

Hurley, R. F. (b. d.). Managing Trust: Creating the New Loyalty. Najdeno 17. avgusta 2017 na spletnem naslovu: www.drbobhurley.com/pdf/trusthbr1.pdf

Huxley, J. (2015). *An Exploratory Analysis and Synthesis of the Viability of Groups with Salient Social Identities Using Stafford Beer's VSM Model* (doktorska disertacija). Portsmouth: Portsmouth University.

Igličar, A. (1987). Država blaginje, civilna družba in pravna država. *Družboslovne razprave*, 4 (5), str. 62-67.

Igličar, A. (2009). Preobražanje pravnih institucij v sodobnih demokracijah. *Teorija in praksa*, 46 (5), str. 625-640.

Igličar, A. (2012). Sodstvo kot družbeni podsistem in javnost. *Zbornik znanstvenih razprav*, 72, str. 79-115.

Intelligence Community Directive 107. (2018, 28. februar). Office of the Director of National Intelligence. Najdeno 5. marca 2018 na spletnem naslovu: https://www.dni.gov/files/documents/ICD/ICD-107.pdf

International Organization for Standardization. (2009). *ISO 31000:2009 - Risk Management.* Geneva: International Organization for Standardization.

Ivanko, Š. (2007). *Raziskovanje in pisanje del: metodologija in tehnologija raziskovanja in pisanja strokovnih in znanstvenih del.* Kamnik: Cubus image.

Ivanuša, T. (2013). *Kibernetika varnostnih sistemov.* Ljubljana: Zavod za varnostne strategije pri Univerzi Maribor.

Ivanuša, T. (2015). *The Cybernetics of Security and Defense Systems.* New York: Nova Publishers.

Ivanuša, T., Mulej, M., Pečan, S., Tičar, B. & Podbregar, I. (2009). *Pandemija: upravljanje in obvladovanje omejitve gibanja.* Ljubljana: Zavod za varnostne strategije pri Univerzi Maribor.

Ivanuša, T., Podbregar, I. & Hribar, G. (2016). *Topografija protiobveščevalne dejavnosti.* Harlow: Pearson Education Ltd.

Jackson, J. & Bradford, B. (2010). What is trust and confidence in the police? *Policing: a journal of policy and practice*, 4 (3), str. 241-248.

Jackson, M. C. (2009). Fifty Years of Systems Thinking for Management. *The Journal of the Operational Research Society*, 60 (Supplement 1), str. S24-S32.

Johnson, D. & Grayson, K. (2005). Cognitive and affective trust in service relationships. *Journal of Business Research*, 58 (2005), str. 500-507.

Johnson, W. R. (2009). *Thwarting Enemies at Home and Abroad: How to Be a Counterintelligence Officer.* Washington, D.C.: Georgetown University Press.

Johnston, R. (2005). *Analytic Culture in the U.S. Intelligence Community: An Ethnographic Study.* Washington, DC: The Center for the Study of Intelligence, Central Intelligence Agency.

Joseph, P. (2017). *The SAGE Encyclopedia of War: Social Science Perspectives.* SAGE Publications, Inc.: Thousand Oaks.

Judge, W. Q. (1999). *The Leader's Shadow, Exploring and Developing Executive Character.* Thousand Oaks, London, New Delhi: SAGE Publications.

Kaase, M., Newton, K. & Toš, N. (1999). *Zaupanje v vlado.* Ljubljana: Liberalna akademija, Znanstvena knjižnica FDV.

Kahan, D. M. (2001). Trust, Collective Action, and Law. *Boston University Law Review*, 81 (2), str. 333-347.

Kaptein, S. P. (1998). *Ethics Management: Auditing and Developing the Ethical Content of Organizations.* Dodrecht, Boston, London: Kluwer Academic Publishers.

Kaufman, S. B. (2017). How does IQ relate to personality? *Mensa World Journal*, 57, str. 8-9.

Kavčič, B. (2015). Zaupanje. *Zavarovalniški horizonti: revija za zavarovalništvo in aktuarstvo*, 11 (1), str. 23-40.

Kenning, P. (2008). The influence of general trust and specific trust on buying behaviour. *International Journal of Retail & Distribution Management*, 36 (6), str. 461-476.

Kljačić, M. (1994). *Teorija sistemov.* Kranj: Moderna organizacija - FOV Kranj.

Knapp, M. (2007). *Spying for Peace: Explaining the Absence of the Formal Regulation of Peacetime Espionage.* Chicago: University of Chicago. Najdeno 2. oktobra 2015 na spletnem naslovu: http://research.policyarchive.org/8193.pdf

Knez, M. & Mulej, M. (2011). Celovit menedžment logistike - ključni vir konkurenčnosti. *Embalaža, okolje, logistika*, 61, str. 54-57.

Knežević, L. (2015). CG: "provjetravanje" obavještajne službe. *Obris.org.* Najdeno 12. julija 2017 na spletnem naslovu: http://obris.org/svijet/cg-provjetravanje-obavjestajne-sluzbe/

Knightley, P. (1986). *The Second Oldest Profession: The Spy as Bureaucrat, Patriot, Fantasist and Whore.* London: André Deutsch.

Kocsis, K. (2007). *Reform in Intelligence-Security Services in Transition Countries*. Najdeno 3. April 2016 na spletnem naslovu: http://www.dcaf.ch/content/download/34351/523919/version/1/file/REFORM-IN-INTELLIGENCE.pdf

Kontekst. (b. d.). V *Slovar slovenskega knjižnega jezika.* Najdeno 4. julija 2017 na spletnem naslovu: http://bos.zrc-sazu.si/cgi/a03.exe?name=sskj_testa&expression=kontekst&hs=1

Koren, B. (2012). Metode zbiranja podatkov v obveščevalno-varnostni dejavnosti. V I. Podbregar (ur.), *Obveščevalno-varnostna dejavnost: procesi, metode, nadzor* (str. 45-135). Ljubljana: Fakulteta za varnostne vede.

Kovač, D. & Trček, D. (2007). Metode in modeli zaupanja v porazdeljenih sistemih. V B. Zajc & A. Trost (ur.), *Zbornik Šestnajste mednarodne Elektrotehniške in računalniške konference ERK 2007, 24.-26. september 2007, Portorož, Slovenija* (str. 7-10). Ljubljana: Somaru.

Kramar, U. (2014). *Osnove logistike: skripta za predmet (prva izdaja).* Celje: Fakulteta za logistiko, Univerza v Mariboru.

Kramer, R. M. (1999). Trust and distrust in organizations: Emerging Perspectives, Enduring Questions. *Annual Review of Psychology*, 50, str. 569-98.

Krapež, A. (2015). *Logistika obveščevalnih dejavnosti na ekonomsko poslovnem področju* (doktorska disertacija). Celje: Fakulteta za logistiko.

Križman, A. (2009). Vpliv predhodnikov zaupanja na sodelovanje med podjetji v zunanji logistični oskrbi. *Management*, 4 (4), str. 329-350.

Kuloğlu, G., Gül, Z. & Erçetin, Ş. Ş. (2014). Counter-Intelligence as a Chaotic Phenomenon and Its Importance in National Security. V S. Banerjee, Ş. Ş. Erçetin & A. Tekin (ur.), *Chaos Theory in Politics* (str. 171-188). Dordrecht, Heidelberg, New York, London: Springer.

Kurdija, S. et al. (2016). Slovensko javno mnenje 2012/1. V N. Toš (ur.), *Vrednote v prehodu X.: Slovensko javno mnenje 2010-2016* (str. 133-188). Ljubljana, Dunaj: Univerza v Ljubljani, Fakulteta za družbene vede, IDV, CJMMK; Edition Echoraum.

Laeequddin, M., Sahay, B. S., Sahay, V. & Waheed, K. A. (2010). Measuring trust in supply chain partners' relationships. *Measuring Business Excellence*, 14 (3), str. 53-69.

Lahneman, W. J. (2010). The Need for a New Intelligence Paradigm. *International Journal of Intelligence and CounterIntelligence*, 23 (2), str. 201-225.

Lane, C. (1998). Introduction: Theories and Issues in the Study of Trust. V C. Lane & R. Bachmann (ur.), *Trust Within and Between Organizations: Conceptual Issues and Empirical Applications* (str. 1-30). Oxford: Oxford University Press.

Langhorst, M. & Nieke, S. (2015, 3. december). *Nachrichtendienste: "Was wir brauchen, ist Vertrauen"*. Najdeno 10. novembra 2016 na spletnem naslovu:

https://www.baks.bund.de/de/aktuelles/nachrichtendienste-was-wir-brauchen-ist-vertrauen

Layard, R. (2005). *Happiness: Lessons from a new science.* London: Penguin.

Leonard, A. (2008). Integrating Sustainability Practices Using the Viable System Model. *Systems Research and Behavioral Science*, 25, str. 643-654.

Lépine, P. (2014). Intelligence Gathering in Democracies: Breaking the Social Contract? V D. Čaleta & P. Shemella (ur.), *Intelligence and Combating Terrorism - New Paradigm and Future Challenges* (str. 25-41). Ljubljana; Monterey: Institute for Corporative Security Studies; Center for Civil-Military Relations, Naval Postgraduate School.

Lester, G. & Jackson, B. A. (2009). Weighing Organizational Models for a New Domestic Intelligence Agency. V B. A. Jackson (ur.), *The Challenge of Domestic Intelligence in a Free Society: A Multidisciplinary Look at the Creation of a U.S. Domestic Counterterrorism Intelligence Agency* (str. 123-147). Santa Monica: RAND Corporation.

Lewicki, R. J. & Bunker, B. B. (1996). Developing and Maintaining Trust in Work Relationships. V R. Kramer & T. R. Tyler (ur.), *Trust in organizations: Frontiers of theory and research* (str. 114-139). Thousand Oaks, CA: Sage.

Lewicki, R. L., Tomlinson, E. C. & Gillespie, N. (2006). Models of Interpersonal Trust Development: Theoretical Approaches, Empirical Evidence, and Future Directions. *Journal of Management*, 32 (6), str. 991-1022.

Lewin, J. E. (2003). An empirical investigation of the effects of downsizing on buyer–seller relationships. *Journal of Business Research*, 56 (4), str. 283-293.

Little, L., Marsh, S. & Briggs, P. (2007). Trust and Privacy Permissions for an Ambient World. V R. Song, L. Korba & G. Yee (ur.), *Trust in E-Services: Technologies, Practices and Challenges* (str. 259-322). Hershey, London, Melbourne, Singapore: Idea Group Publishing.

Lohaus, P. (2015, 21. julij). The intelligence community should build public trust,. *AEI.org*. Najdeno 31. januarja 2019 na spletnem naslovu: https://www.aei.org/articles/the-intelligence-community-should-build-public-trust-not-just-transparency/

Lowenthal, M. (2014). *Intelligence: From secrets to policy. 6th edition.* Washington, DC: CQ Press.

Lowenthal, M. M. (2009). *Intelligence: From Secrets to Policy.* Washington DC: CQ Press.

Lucas, M. (2005). The impact of trust and reputation on the transfer of best practices. *Journal of Knowledge Management*, 9 (4), str. 87-101.

Luhmann, N. (1988). Familiarity, Confidence, Trust: Problems and Alternatives. V D. Gambetta (ur.), *Trust: Making and Breaking Cooperative Relations* (str. 94-107). Oxford: University of Oxford, Department of Sociology.

Luoma-aho, V. (2008). Sector reputation and public organisations. *International Journal of Public Sector Management*, 21 (5), str. 446-467.

M.B. (24. marec 2015). Pahor: Potrebno odpraviti vsak dvom, da je v tem primeru prišlo do morebitnih nezakonitosti. *Demokracija.si.* Najdeno 24. junija 2016 na spletnem naslovu: http://www.demokracija.si/fokus/pahor-potrebno-odpraviti-vsak-dvom-da-je-v-tem-primeru-prislo-do-morebitnih-nezakonitosti

MacDonald, J. & Stokes, R. J. (2006). Race, Social Capital, and Trust in the Police. *Urban Affairs Review*, 41 (3), str. 358-375.

MacGregor Adams, K. (2011). Systems principles: Foundation for the SoSE methodology. *International Journal of System of Systems Engineering*, 2 (2/3), str. 120-155.

Mack, A. (1975). Why Big Nations Lose Small Wars: The Politics of Asymmetric Conflict. *World Politics*, 27 (2), str. 175-200.

Magen, C. (2014). Media Strategies and Manipulations of Intelligence Services: The Case of Israel. *The International Journal of Press/Politics*, 20 (2), str. 247-265.

Makarovič, J. (2004). Zaupanje: odprtost kot zdravilo in kot strup. *Teorija in praksa*, 41 (1-2), str. 377-386.

Makashvilia, M., Kaishauri, N. & Azmaiparashvili, T. (2014). The role of knowledge in overcoming snake fear. *Procedia - Social and Behavioral Sciences*, 152, str. 184-187.

Makovec, U. (2016, 3. september). Intervju: Damir Črnčec, strokovnjak za varnostna vprašanja. "Koliko multikulturalizma je v Katarju, ki financira džamijo v Sloveniji? Nič.". *Siol.net*. Najdeno 2. januarja 2017 na spletnem naslovu: https://siol.net/novice/slovenija/koliko-multikulturalizma-je-v-katarju-ki-financira-dzamijo-v-sloveniji-nic-425115

Marková, I., Linell, P. & Gillespie, A. (2008). Trust adn Distrust in Society. V I. Marková & A. Gillespie (ur.), *Trust and Distrust: Sociocultural perspectives* (str. 3-27). Charlotte: Information Age Publishing.

Martin, D. (2014). Towards a model of trust. *Journal of Business Strategy*, 35 (4), str. 45-51.

Martins, N. (2002). A model for managing trust. *International Journal of Manpower*, 23 (9), str. 754-769.

Matei, F. C. (2014). The media's role in intelligence democratization. *International Journal of Intelligence and Counterintelligence*, 27 (1), str. 73-108.

Mayer, R. C., Davis, J. H. & Schoorman, F. D. (1995). An Integrative Model of Organizational Trust. *The Academy of Management Review*, 20 (3), str. 709-734.

McAllister, J. (1995). Affect- and Cognition-Based Trust as Foundations for Interpersonal Cooperation in Organizations. *The Academy of Management Journal*, 38 (1), str. 24-59.

McCombs, M. (2014). *Setting the Agenda: Mass Media and Public Opinion. Second Edition.* Cambridge; Malden: Polity Press.

McKnight, D. H. & Webster, J. (2001). Collaborative Insight or Privacy Invasion? Trust Climate as a Lens for Understanding Acceptance of Awareness Systems. V C. L. Copper, S. Cartwright & P. C. Earley (ur.), *The International Handbook of Organizational Culture and Climate* (str. 533-555). Chichester: John Wiley & Sons Ltd.

McKnight, D. H., Cummings, L. L. & Chervany, N. L. (1998). Initial trust formation in new organizational relationships. *Academy of Management Review*, 23 (3), str. 473-490.

McKnight, H. D. & Chervany, N. L. (2001). Trust and Distrust Definitions: One Bite at a Time. *Trust in Cyber-societies*, 2246, str. 27-54.

Media. [b. d.] https://www.wordsinspace.net/course_material/fmt/DefinitionsOfMedia.pdf

Mekina, B. (2011, 14. april). Sebastjan Selan: "Približno polovica ministrstev pridobiva ali uporablja naše informacije". *Mladina*. Najdeno 9. marca 2015 na spletnem naslovu: http://www.mladina.si/53711/sebastjan-selan-priblizno-polovica-ministrstev-pridobiva-ali-uporablja-nase-informacije/

Memedi, S. (2015). *(Ne)zaupanje v temeljne institucije demokratične ureditve med mladimi: primer Slovenije* (magistrsko delo). Ljubljana: Fakulteta za družbene vede.

Mensa Slovenija. (b. d.). *Kaj je IQ (inteligenčni kvocient) [O Mensi]*. Najdeno 7. maja 2018 na spletnem naslovu: https://www.mensa.si/

Miller, A. H. (1974). Political Issues and Trust in Government: 1964-1970. *The American Political Science Review*, 68 (3), str. 951-972.

Milton, A. (2008). *Why are fear and distrust spiralling in twenty-first century Britain?* Najdeno 7. maja 2019 na spletnem naslovu: https://www.jrf.org.uk/file/37798/download?token=0wf2uQ7N&filetype=viewpoint

Mirzaie, K., Fesharaki, M. N. & Daneshgar, A. (2011). A Thought Structure for Complex Systems Modeling Based on Modern Cognitive Perspectives. *International Journal of Computer Science Issues*, 8 (3), str. 182-187.

Mirzaie, K., Fesharaki, M. N. & Daneshgar, A. (2012). Trust modeling based on Capra cognitive framework. *Procedia – Social and Behavioral Sciences*, 32, str. 197-203.

Mohammadi, S. & Banirostam, T. (2015). A Perceptual Meta-model based on the Ontology of Mental Models. *The International Journal of Humanities & Social Studies*, 3 (11), str. 122-128.

Mookerji, R. K. (1988). *Chandragupta Maurya and his times.* Delhi, Varanasi, Patna, Bangalore, Madras: Motilal Banarsidass.

Morgan, R. M. & Hunt, S. D. (1994). The Commitment-Trust Theory of Relationship Marketing. *Journal of Marketing*, 58 (3), str. 20-38.

Mulej et al. (2000). *Dialektična in druge mehkosistemske teorije: podlage za celovitost in uspeh managementa.* Maribor: Ekonomsko-poslovna fakulteta.

Mulej et al. (2008). *Invencijsko-inovacijski management z uporabo dialektične teorije sistemov (podlaga za uresničitev ciljev Evropske unije glede inoviranja).* Ljubljana: Korona plus, d.o.o., Inštitut za inovativnost in tehnologijo.

Mulej, M. (1979). *Ustvarjalno delo in dialeketična teorija sistemov.* Celje: Razvojni center.

Mulej, M. (1994). *Teorije sistemov.* Maribor: Ekonomsko-poslovna fakulteta.

Mulej, M. & Kajzer, Š. (1998). Ethics of interdependence and the law of requisite holism. V M. Rebernik & M. Mulej (ur.), *STIQE '98: proceedings of the 4th International Conference on Linking Systems Thinking, Innovation, Quality, Entrepreneurship and Environment, Maribor, Slovenia, December 6-9, 1998* (str. 129-140). Maribor: Institute for Entrepreneurship at Faculty of Business Economics.

Mun, J., Shin, M. & Jung, M. (2011). A goal-oriented trust model for virtual organization creation. *Journal of Intelligent Manufacturing*, 22 (2011), str. 345-354.

Muna, R. (2008). Local Ownership and the Experience of SSR in Indonesia. V T. Donais (ur.), *Local Ownership and Security Sector Reform* (str. 233-251). Zürich, Berlin: LIT Verlag.

Newton, K. & Norris, P. (2000). Confidence in Public Institutions: Faith, Culture or Performance? V S. J. Pharr & R. D. Putnam (ur.), *Disaffected Democracies: What's Troubling the Trilateral Countries?* (str. 52-73). Princeton, New Jersey: Princeton University Press.

Novak, G. (b. d.). *Rekurzija v Pythonu*. Najdeno 5. marca 2019 na spletnem naslovu: http://www.nauk.si/materials/6337/out/#state=1

Nu, Y.-N. (2009). *Techno-economic analysis of single-pass maize biomass harvest systems* (magistrska naloga). Ames, Iowa: Iowa State University.

Office of the Director of National Intelligence, National Intelligence Council. (2017). *Background to "Assessing Russian Activities and Intentions in Recent US Elections": The Analytic Process and Cyber Incident Attribution.* Najdeno 27. februarja 2018 na spletnem naslovu: https://www.dni.gov/files/documents/ICA_2017_01.pdf.

Office, N. S. (2015). *AAP-06, Edition 2015, NATO Glossary of Terms and Definitions (English and French).* Bruselj: NATO Standardisation Office.

Olmedilla, D., Rana, O. F., Matthews, B. & Nejdl, W. (2006). Security and Trust Issues in Semantic Grids. V C. Goble, C. Kesselman & Y. Sure (ur.), *Semantic Grid: The Convergence of Technologies* (str. 1-11). Dagstuhl: Internationales Begegnungs- und Forschungszentrum für Informatik, Schloss Dagstuhl. Najdeno 22. septembra 2016 na spletnem naslovu: http://drops.dagstuhl.de/volltexte/2006/408/pdf/05271.OlmedillaDaniel.Paper.408.pdf

Olson, J. M. (2001). The Ten Commandments of Counterintelligence. *Studies in Intelligence*, 45 (5), str. 38-63.

Organizacija za gospodarsko sodelovanje in razvoj. (2005). *DAC Guidelines and Reference Series: Security System Reform and Governance.* Pariz: OECD Publishing.

Organizacija za gospodarsko sodelovanje in razvoj. (2007). *OECD DAC Handbook on Security System Reform: Supporting Security and Justice.* Paris: OECD Publishing.

Organizacija združenih narodov. (1948). *Splošna deklaracija človekovih pravic.* New York: Organizacija združenih narodov.

Organizacija združenih narodov. (1976). *Mednarodni pakt o državljanskih in političnih pravicah.* New York: Organizacija združenih narodov.

Pagon, M., Banutai, E. & Bizjak, U. (2011). Organizational culture in European public administration institutions: new and traditional values, fear, and resistance to change [objavljen povzetek prispevka na konferenci]. V *Sessions [Elektronski vir] / Sixth International Conference on Interdisciplinary Social Sciences, 11-13 July, 2011.* New Orleans: [s. n.].

Paliszkiewicz, J. O. (2011). Trust Management: Literature Review. *Management*, 6 (4), str. 315-331.

Parlamentarna skupščina Sveta Evrope. (2005). Report Doc. 10567 - 2 June 2005. Democratic oversight of the security sector in member states. V *Documents - Working papers, 2005 Ordinary Session (Third Part), 20-24 June 2005. Volume V, Documents 10566-10615* (str. 13-28). Strasbourg: Council of Europe Publishing.

Percepcija. (b. d.). V *Slovar slovenskega knjižnega jezika.* Najdeno 31. avgusta 2017 na spletnem naslovu: http://bos.zrc-sazu.si/cgi/neva.exe?name=ssbsj&tch=14&expression=zs%3D49526

Pérez Ríos, J. M. (2012). *Design and Diagnosis for Sustainable Organizations: The Viable System Method.* Berlin, Heidelberg: Springer-Verlag.

Phythian, M. (2005). Still a Matter of Trust: Post-9/11 British Intelligence and Political Culture. *International Journal of Intelligence and CounterIntelligence*, 18 (4), str. 653-681.

Phythian, M. (2013). *Understanding the Intelligence Cycle.* Oxon; New York: Routledge.

Pickering, A. (2002). Cybernetics and the Mangle: Ashby, Beer and Pask. *Social Studies of Science*, 32 (3), str. 413-427.

Podbregar, I. (2008). Nekateri elementi obveščevalne dejavnosti. V I. Podbregar (ur.), *Vohunska dejavnost in gospodarstvo: znanstvena monografija* (str. 21-71). Ljubljana: Fakulteta za varnostne vede.

Podbregar, I. (2011 a). Pred reinženiringom nacionalnovarnostnega sistema - priložnosti za Slovensko vojsko. *Sodobni vojaški izzivi*, 13 (2), str. 15-25.

Podbregar, I. (2011 b, 9. september). Veliki brat je že neviden. *Finance*, 2, str. 15.

Podbregar, I. (2012). Uvod v obveščevalno-varnostno dejavnost. V I. Podbregar (ur.), *Obveščevalno-varnostna dejavnost: procesi, metode, nadzor* (str. 20-44). Ljubljana: Fakulteta za varnostne vede.

Podbregar, I. (2018). Voditelj in neposredno nadrejeni vodja. V T. Logar (ur.), *Janez Drnovšek* (str. 84-97). Ljubljana: Cankarjeva založba.

Podbregar, I. & Hibler, J. (2006). Obveščevalno-varnostna dejavnost in odnosi z javnostmi. V B. Lobnikar (ur.), *7. slovenski dnevi varstvoslovja, Raznolikost zagotavljanja varnosti: zbornik prispevkov* (str. 27-30). Ljubljana: Fakulteta za policijsko-varnostne vede.

Podbregar, I. & Ivanuša, T. (2008). *Obveščevalna dejavnost na področju zdravstva - MEDINT.* Ljubljana: Zavod za varnostne strategije pri Univerzi Maribor.

Podbregar, I. & Ivanuša, T. (2010). Javni viri in analitika v obveščevalni dejavnosti. *Revija za kriminalistiko in kriminologijo*, 61 (2), str. 191-198.

Podbregar, I., Hribar, G. & Ivanuša, T. (2015). Intelligence and the Significance of a Secret Agent's Personality Traits. *International Journal of Intelligence and CounterIntelligence*, 28 (3), str. 520-539.

Podbregar, I., Mulej, M., Pečan, S., Podbregar, N. & Ivanuša, T. (2010). *Informacije kot »bojna« podpora kriznemu odločanju, krizni komunikaciji in delovanju.* Ljubljana: Zavod za varnostne strategije pri Univerzi Maribor.

Politika. (b. d.). V *Slovar slovenskega knjižnega jezika.* Najdeno 17. novembra 2019 na spletnem naslovu: https://fran.si/iskanje?View=1&Query=politika

Potočan, V. & Mulej, M. (2006). Systemic Understanding of Trust and Ethics of Interdependence in Innovative Business. V *ISA 2006 Congress "The quality of social existence in a globalising world" [Elektronski vir] / XVI World Congress of Sociology, International Convention Centre Durban, South Africa, 23-29 July 2006* (str. 9). Malvern: Naren Bhimsan.

Pourtios, G., Schettino, A. & Vuilleumier, P. (2013). Brain mechanisms for emotional influences on perception and attention: What is magic and what is not. *Biological Psychology*, 92 (2013), str. 492-512.

Praprotnik, R. (24. maj 2007). Neuradno: Sovi padla storilnost skoraj za polovico. *Dnevnik*. Najdeno 10. oktobra 2016 na spletnem naslovu: https://www.dnevnik.si/247410

Premier dr. Cerar izrazil nadaljnje zaupanje direktorju Sove Klemenčiču [Sporočila za javnost]. (2016). Najdeno 30. septembra 2016 na spletnem naslovu: http://www.vlada.si/predsednik_vlade/sporocila_za_javnost/a/premier_dr_cerar_izrazil_nadaljnje_zaupanje_direktorju_sove_klemencicu_176

Prezelj, I. (2002). Konceptualizacija nacionalnih varnostnih interesov. *Teorija in praksa*, 39 (4), str. 621-637.

Prunckun, H. (2012). *Counterintelligence Theory and Practice.* Lanham, MD: Rowman & Littlefield.

Purg, A. (1995). *Obveščevalne službe.* Ljubljana: Enotnost.

Purg, A. (2002). *Primerjalni obveščevalni sistemi.* Ljubljana: Visoka policijsko-varnostna šola.

Raab, C. D. (2017). Security, Privacy and Oversight. V A. W. Neal (ur.), *Security in a Small Nation: Scotland, Democracy, Politics* (str. 77-102). Cambridge, UK: Open Book Publishers.

Rădoi, M. & Lupu, A. (2017). Understanding Institutional Trust. What Does It Mean to Trust the Health System? V A. Maturo, Š. Hošková-Mayerová, D. T. Soitu & J. Kacprzyk (ur.), *Recent Trends in Social Systems: Quantitative Theories and Quantitative Models* (str. 11-22). Cham: Springer International Publishing AG Switzerland.

Ragin, C. C. (2007). *Družboslovno raziskovanje: enotnost in raznolikost metode.* Ljubljana: Fakulteta za družbene vede.

Resolucija o strategiji nacionalne varnosti Republike Slovenije. *Ur. l. RS*, št. 27/2010.

Richelson, J. (2018). *The U.S. Intelligence Community.* New York: Routledge.

Ritchey, T. (1998). *Fritz Zwicky, Morphologie and Policy Analysis*. 12 str. Najdeno 20. septembra 2017 na spletnem naslovu:

https://www.researchgate.net/publication/267794873_Fritz_Zwicky_Morphologie_and_Policy_Analysis

Ritchey, T. (2011). *Wicked Problems - Social Messes: Decision Support Modelling with Morphological Analysis.* New York: Springer.

Robbins, S. P., Judge, T. A., Odendaal, A. & Roodt, G. (2009). *Organisational Behaviour: Global and Southern African Perspectives. 2nd Edition.* Cape Town: Pearson Education.

Robinson, P. (2009). The Viability of a Canadian Foreign Intelligence Service. *International Journal*, 64 (3), str. 703-716.

Rosario, E., Hartlyn, J. & Morgan, J. (2006). Performance Still Matters: Explaining Trust in Government in the Dominican Republic. *Political Science Publications and Other Works*. Najdeno 6. februarja 2017 na spletnem naslovu: http://trace.tennessee.edu/utk_polipubs/11/

Rose, A. M. (1962). The study of the influence of the mass media on public opinion. *Kyklos*, 15 (2), str. 465-484.

Rosi, B. (2004). *Prenova omrežnega razmišljanja z aplikacijo na procesih v železniški dejavnosti* (doktorska disertacija). Maribor: Univerza v Mariboru.

Rosi, B. (2015). *Innovation in systems thinking: the application of dialectical network thinking in resolving complex problems.* New York: Nova Science Publishers.

Rosi, B. & Mulej, M. (2006). The dialectical network thinking - a new systems theory concerned with management. *Kybernetes*, 35 (7/8), str. 1165-1178.

Rosi, B. & Rosi, M. (2011). Razreševanje problemov z uporabo (mehko)sistemskega razmišljanja kot potenciala družbeno odgovorne ustvarjalnosti ljudi. *Naše gospodarstvo*, 57 (1-2), str. 61-71.

Rotter, J. B. (1967). A new scale for the measurement of interpersonal trust. *Journal of Personality*, 35 (4), str. 651-665.

Rousseau, D. M., Sitkin, S. B., Burt, R. S. & Camerer, C. (1998). Not So Different After All: A Cross-Discipline View of Trust. *Academy of Management Review*, 23 (3), str. 393-404.

Rus, A. (2008). Zaupanje in ekonomska uspešnost. *Teorija in praksa*, 45 (1-2), str. 72-92.

Rusu, R. & Baboş, A. (2015). Organizational trust between institutional and interpersonal trust. *Buletin Ştiinţific*, 2 (40), str. 175-180.

Salminen, A. & Ikola-Norrbacka, R. (2010). Trust, good governance and unethical actions in Finnish public administration. *International Journal of Public Sector Management*, 23 (7), str. 647-688.

Salo, J. & Karjaluoto, H. (2007). A conceptual model of trust in the online environment. *Online Information Review*, 31 (5), str. 604-621.

Salovey, P. & Mayer, J. D. (1990). Emotional intelligence. *Imagination, cognition and personality*, 9, str. 185-211.

Sawers, J. (2010, 28. oktober). Sir John Sawers's speech – full text. *The Guardian*. Najdeno 29. septembra 2017 na spletnem naslovu: https://www.theguardian.com/uk/2010/oct/28/sir-john-sawers-speech-full-text

Scheinin, M. (2010). *Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism.* New York: Organizacija združenih narodov.

Schierkolk, N. Y. (2018). *International standards and good practices in the governance and oversight of security services.* Tbilisi: DCAF.

Schiffman, L., Thelen, S. T. & Sherman, E. (2010). Interpersonal and political trust: modeling levels of citizens' trust. *European Journal of Marketing*, 44 (3/4), str. 369-381.

Schlenker, B. R., Helm, B. & Tedeschi, J. T. (1973). The effects of personality and situational variables on behavioral trust. *Journal of Personality and Social Psychology*, str. 419-427.

Schoorman, F. D., Mayer, R. C. & Davis, J. H. (2007). An Integrative Model of Organizational Trust: Past, Present, and Future. *Academy of Management Review*, 32 (2), str. 344-354.

Schreier, F. (2005). Democratic Oversight and Control of Intelligence in South East Europe: An Analysis of the Stability Pact Self-Assessment Studies. V E. Cole, T. Donais & P. H. Fluri (ur.), *Defence and Security Sector Governance and Reform in South East Europe Self-Assessment Studies: Regional Perspectives* (str. 137-154). Baden-Baden: Nomos Verlagsgesellschaft.

Schultheis, E. (2019, 8. februar). World's biggest intelligence headquarters opens in Berlin. *The Guardian.* Najdeno 9. februarja 2019 na spletnem naslovu:

https://www.theguardian.com/world/2019/feb/08/worlds-biggest-intelligence-headquarters-opens-berlin-germany-bnd

Schwaninger, M. (2006 a). Design for viable organizations - The diagnostic power of the viable system model. *Kybernetes*, 35 (7/8), str. 955-966.

Schwaninger, M. (2006 b). Theories of Viability: a Comparison. *System Research and Behavioral Science*, 23, str. 337-347.

Schwaninger, M. (2010). Model-based management (MBM): a vital prerequisite for organizational viability. *Kybernetes*, 39 (9/10), str. 1419-1428.

Schwaninger, M. & Pérez Ríos, J. (2008). System dynamics and cybernetics: A synergetic pair. *System Dynamics Review*, 24 (2), str. 145-174.

Schwaninger, M. & Scheef, C. (2016). A Test of the Viable System Model: Theoretical Claim vs. Empirical Evidence. *Cybernetics and Systems*, 47 (7), str. 544-569.

Security Service - MI5. (2007). *Intelligence, Counter-Terrorism and Trust.* Najdeno 12. novembra 2016 na spletnem naslovu: https://www.mi5.gov.uk/fa/node/404

Sexton, S. (2018, 15. marec). Former CIA and FBI Director Calls for Renewed Trust in Beleaguered. *Salzburg Global Seminar*. Najdeno 31. januarja 2019 na spletnem naslovu: https://www.salzburgglobal.org/news/latest-news/article/former-cia-and-fbi-director-calls-for-renewed-trust-in-beleaguered-intelligence-agencies.html

Shaw, E. D., Ruby, K. G. & Post, J. M. (1998). The insider threat to information systems. *Security Awareness Bulletin*, 2 (98), str. 22-47.

Sims, M. C. & Stephens, M. (2011). *Living Folklore: An Introduction to the Study of People and Their Traditions. Second Edition.* Logan, Utah: Utah State University Press.

Sinnigen, W. G. (1962). The Origins of the frumentarii. *Memoirs of the American Academy in Rome*, 27, str. 212-224.

Six, F. E. (2007). Building interpersonal trust within organizations: a relational signalling perspective. *Journal of Management Governance*, 11, str. 285-309.

Sotlar, A. (2012). Nadzor nad obveščevalno-varnostno dejavnostjo. V I. Podbregar (ur.), *Obveščevalno-varnostna dejavnost: Procesi, metode, nadzor* (str. 437-488). Ljubljana: Fakulteta za varnostne vede.

Svet Evrope. (1950). *Evropska konvencija o varstvu človekovih pravic in temeljnih svoboščin.* Rim: Svet Evrope.

Svet Evrope. (1999). *Recommendation 1402 (1999). Control of internal security services in council of Europe.* Strasbourg: Svet Evrope.

Svet Evrope. (2009). *Armed Forces and Security Services: What Democratic Controls?* Strasbourg: Svet Evrope.

Swift, P. E. & Hwang, A. (2013). The impact of affective and cognitive trust on knowledge sharing and organizational learning. *The Learning Organization*, 20 (1), str. 20-37.

Šaponja, V. (1999). *Taktika dela obveščevalnovarnostnih služb.* Ljubljana: Ministrstvo za notranje zadeve, Visoka policijsko-varnostna šola.

Šarotar Žižek, S. & Mulej, M. (2015). Znanost, celovitost, navidezna celovitost, zadostna in potrebna celovitost. V S. Šarotar Žižek (ur.), *Osebna celovitost človeka* (str. 9-18). Maribor: IRDO, Inštitut za razvoj družbene odgovornosti.

Šifrer, J. (2008). Obveščevalna dejavnost v procesu kriznega upravljanja. V I. Podbregar (ur.), *Vohunska dejavnost in gospodarstvo* (str. 151-184). Ljubljana: Fakulteta za varnostne vede.

Tan, Y. & Thoen, W. (2001). Toward a generic model of trust for electronic commerce. *International Journal of Electronic Commerce*, 5 (2), str. 61-74.

Taylor, S. A. (2007). The Role of Intelligence in National Security. V A. Collins (ur.), *Contemporary Security Studies* (str. 248-267). Oxford: Oxford University Press.

Toš, N. (2007). (Ne)zaupanje v institucije: potek demokratične institucionalizacije v Sloveniji (1991– 2006). *Teorija in praksa*, 44 (3-4), str. 367-395.

Toš, N. & Hafner-Fink, M. (1997). *Metode družboslovnega raziskovanja*. Ljubljana: Fakulteta za družbene vede.

Treverton, G. F. (2008). *Reorganizing U.S. Domestic Intelligence: Assessing the Options.* Santa Monica, CA: RAND Corporation.

Tucker, A. W. (1983). The Mathematics of Tucker: A Sampler. *The Two-Year College Mathematics Journal*, 14 (3), str. 228-232.

Tversky, A. & Kahneman, D. (1974). Judgement under Unvertainty: Heuristics and Biases. *Science*, 185 (4157), str. 1124-1131.

Tyler, T. R. & Huo, Y. J. (2002). *Trust in the law: encouraging public cooperation with the police and courts.* New York: Russell Sage Foundation.

Umpleby, S. A. (1991). Comparing conceptual systems: A strategy for changing values as well as institutions. *Cybernetics and Systems*, 22 (4), str. 515-529.

Umpleby, S. A. (1997). Cybernetics of conceptual systems. *Cybernetics & Systems*, 28 (8), str. 635-651.

Uslaner, E. M. (2004). Trust and Social Bonds: Faith in Others and Policy Outcomes Reconsidered. *Political Research Quarterly*, 57 (3), str. 501-507.

Valicon. (2016). *Sporočilo za medije: Valicon ogledalo Slovenije 2016.* Ljubljana: Valicon. Najdeno 18. avgusta 2017 na spletnem naslovu: www.valicon.net/files/Sporocilo%20za%20javnost%202016-06-17.pdf

Van de Walle, S. (2007). Determinants of Confidence in the Civil Service: An International Comparison. V K. Schedler & I. Proeller (ur.), *Cultural Aspects of Public Management Reform* (str. 171-201). Amsterdam: Elsevier.

Van de Walle, S., Van Roosbroek, S. & Bouckaert, G. (2008). Trust in the public sector: is there any evidence for a long-term decline? *International Review of Administrative Sciences*, 1, str. 47-64.

Varnum, N. E., Grossman, I., Kitayama, S. & Nisbett, R. (2010). The Origin of Cultural Differences in Cognition: The Social Orientation Hypothesis. *Current Directions in Psychological Science*, 19 (1), str. 9-13.

Verovati. (b. d.). V *Slovar slovenskega knjižnega jezika.* Najdeno 5. januarja 2017 na spletnem naslovu: http://bos.zrc-sazu.si/cgi/neva.exe?name=ssbsj&tch=14&expression=zs%3D84113

Vila, A. (1994). *Organizacija in organiziranje.* Kranj: Moderna organizacija, Fakulteta za organizacijske vede.

Wallace, R. (2009). A Time for Counterespionage. V J. E. Simms & B. Gerber (ur.), *Vaults, Mirrors & Masks: Rediscovering U.S. Counterintelligence* (str. 101-124). Washington, D.C.: Georgetown University Press.

Wan Ahmad, W. N. & Mohamad Ali, N. (2016). Trust perceptions in using persuasive technologies. *2016 3rd International Conference On Computer And Information Sciences (ICCOINS)*, str. 49-53.

Warner, M. (2009). Building a Theory of Intelligence Systems. V G. F. Treverton & W. Agrell (ur.), *National Intelligence Systems: Current Research and Future Prospects*

(str. 11-37). Cambridge, New York, Melbourne, Madrid, Cape Town, Singapore, Sao Paolo, Delhi: Cambridge University Press.

Washington Post Staff. (2017, 20. marec). Full transcript: FBI Director James Comey testifies on Russian interference in 2016 election. *Washington Post*. Najdeno 20. marca 2017 na spletnem naslovu: https://www.washingtonpost.com/news/post-politics/wp/2017/03/20/full-transcript-fbi-director-james-comey-testifies-on-russian-interference-in-2016-election/?utm_term=.182e0d811f73

Wilkinson, D. & Birmingham, P. (2003). *Using Research Instruments: A Guide for Researchers.* London: RoutledgeFalmer.

Williams, M. (2001). In Whom We Trust: Group Membership as an Affective Context for Trust Development. *The Academy of Management Review*, 26 (3), str. 377-396.

Wills, A. (2012). Financial Oversight of Intelligence Services. V H. Born & A. Wils (ur.), *Overseeing Intelligence Services: A Toolkit* (str. 151-178). Geneva: DCAF.

Wills, A., Born, H., Scheinin, M., Wiebusch, M. & Thornton, A. (2011). *Parliamentary Oversight of Security and Intelligence Agencies in the European Union.* Brussels: European Parliament.

Winkler, I. (2005). *Spies Among Us: How to Stop Spies, Terrorists, Hackers and Criminals You Don't Even Know You Encounter Every Day.* Indianapolis: Whiley Publishing.

Wlezien, C. (1995). The Public as Thermostat: Dynamics of Preferences for Spending. *American Journal of Political Science*, 39 (4), str. 981-1000.

Xiong, F. & Liu, Y. (2014). Opinion formation on social media: An empirical approach. *Chaos: An Interdisciplinary Journal of Nonlinear Science*, 24 (013130), str. 1-8.

Yang, T., Penton, T., Köybaşı, Ş. L. & Banissy, M. J. (2017). Social perception and aging: The relationship between aging and the perception of subtle changes in facial happiness and identity. *Acta Psychologica*, 179 (2017), str. 23-29.

Zakon o Slovenski obveščevalno-varnostni agenciji. *Ur. l. RS*, št. 81/06 – uradno prečiščeno besedilo.

Zand, D. E. (1972). Trust and managerial problem solving. *Administrative Science Quarterly*, 17 (2), str. 229-239.

Zaupanje. (b. d.). V *Slovar slovenskega knjižnega jezika.* Najdeno 27. oktobra 2016 na spletnem naslovu: http://bos.zrc-sazu.si/cgi/a03.exe?name=sskj_testa&expression=zaupanje&hs=1

Zucker, L. G. (1985). Production of Trust: Institutional Sources of Economic Structure, 1840-1920. V L. L. Cummings & B. Staw (ur.), *Research in Organizational Behavior (Vol. 8)* (str. 53-111). Greenwich: JAI Press.

Ženko, Z. & Mulej, M. (2009). Poučevanje teorije sistemov kot prispevek za pot v inovativno družbo. *Mednarodno inovativno poslovanje - Journal of Innovative BUsiness and Management,* 1 (1). Najdeno 5. junija 2016 iz http://journal.doba.si/letnik_1-2009-st-1/poucevanje-teorije-sistemov-kot-prispevek-za-pot-v-inovativn

Žirovnik, J. (2016). *Procesni model presojanja posegov obveščevalnih služb v komunikacijsko zasebnost kot logistični izziv* (doktorska disertacija). Celje: Fakulteta za logistiko.

Priloge

Priloga 1: Vprašanja za intervju

Vir: Osebni vir

1. Kako ocenjujete trenutno medijsko podobo tujih in slovenskih obveščevalno-varnostnih služb v primerjavi z realnim stanjem?
2. Kakšno je po vašem mnenju stanje zaupanja državljanov v matične obveščevalno-varnostne službe v Republiki Sloveniji in v tujini? Se vam zdi stanje sploh vredno pozornosti?
3. Kdo je po vašem prepričanju odgovoren za takšno stanje?
4. Pojasnite, prosim, zakaj in koliko po vašem mnenju (ne)zaupanje državljanov **neposredno** oziroma **posredno** vpliva na matične obveščevalno-varnostne službe (učinkovitost, uspešnost, ugled…).
5. Kateri so po vašem mnenju tisti dejavniki, ki vplivajo na zaupanje državljanov v matične obveščevalno-varnostne službe (splošno)? Kateri se vam zdijo pomembnejši od drugih?
6. Ali ste se z vprašanjem zaupanja kakorkoli ukvarjali v času, ko ste opravljali/opravljate funkcijo direktorja obveščevalno-varnostne službe/uslužbenca obveščevalno-varnostne službe/člana KNOVS? Kaj je bilo na tem področju narejeno?
7. Ali (oziroma koliko in kako) se po vašem védenju s tem problemom ukvarjajo v tujini?
8. Kako bi bilo po vaše mogoče izboljšati tovrstno zaupanje? Kakšne bi bile prednosti in koristi (če sploh) ter za koga? Kje vidite pri tem ovire ali težave?

Priloga 2: Anketa

Vir: Osebni vir

Q1 - Ali zaupate slovenskim obveščevalno-varnostnim službam?

◯ Da

◯ Ne

IF (1) Q1 = [2]

Q2 - Zakaj ne?

Možnih je več odgovorov

☐ Vpliv politike na delo obveščevalno-varnostne službe

☐ Nekompetentno vodstvo obveščevalno-varnostnih služb

☐ Nestrokovno delo obveščevalno-varnostnih služb

☐ Narava dela obveščevalno-varnostnih služb

☐ Neučinkovitost obveščevalno-varnostnih služb

☐ Zgodovina obveščevalno-varnostnih služb

☐ Pomanjkljiv nadzor nad delom obveščevalno-varnostnih služb

☐ Afere

☐ Bil/a sem tarča obveščevalno-varnostnih služb

☐ Drugo:

Q3 - Spol:

◯ Moški

◯ Ženski

Q4 - V katero starostno skupino spadate?

- ◯ do 20 let
- ◯ 21 - 35 let
- ◯ 36 - 55 let
- ◯ 56 - 65 let
- ◯ 65 let ali več

Q5 - Kakšna je vaša najvišja dosežena formalna izobrazba?

- ◯ Manj kot srednja šola
- ◯ Srednja šola
- ◯ Višja šola
- ◯ Visoka šola (VS/UN)
- ◯ Specializacija
- ◯ Magisterij
- ◯ Doktorat

Q6 - Kakšen je vaš trenutni status?

- ◯ Dijak/inja
- ◯ Študent/ka
- ◯ Zaposlen/a
- ◯ Brezposeln/a
- ◯ Upokojenec/ka
- ◯ Drugo:

Priloga 3: Rezultati ankete

Vir: Osebni vir

Q1	**Ali zaupate slovenskim obveščevalno-varnostnim službam?**			
	Odgovori	**Frekvenca**	**Odstotek**	**Kumulativa**
	1 (Da)	165	56%	56%
	2 (Ne)	130	44%	100%
Veljavni	Skupaj	295	100%	

Q2	**Zakaj ne?**		
	Podvprašanja	**Navedbe**	
		Frekvence	%
Q2a	Vpliv politike na delo obveščevalno-varnostne službe	107	29%
Q2b	Nekompetentno vodstvo obveščevalno-varnostnih služb	35	10%
Q2c	Nestrokovno delo obveščevalno-varnostnih služb	25	7%
Q2d	Narava dela obveščevalno-varnostnih služb	20	5%
Q2e	Neučinkovitost obveščevalno-varnostnih služb	38	10%
Q2f	Zgodovina obveščevalno-varnostnih služb	36	10%
Q2g	Pomanjkljiv nadzor nad delom obveščevalno-varnostnih služb	45	12%
Q2h	Afere	51	14%
Q2i	Bil/a sem tarča obveščevalno-varnostnih služb	2	1%
Q2j	Drugo:	5	1%
	SKUPAJ		100%

Q2j_text	Q2 (Drugo:)	
	Odgovori	**Frekvenca**
	politični nadzor opozocije glede na pozicijo, pomanjkanje vednosti varuha človekovih pravic kakšna je njena.njegova vloga pri nadzoru teh služb	1
	ker so povsod sami šalabajzi na vodilnih položajih, predvidevam da je tudi pri obveščevalno.varnostnih službah tako.	1
	ne poznam njihovega dela	1
	prekomplicirani postopki, ki onemogočajo ukrepanje v realnem času	1
	ne zaupam jim	1
Veljavni	Skupaj	5

Q3	Spol:		
	Odgovori	**Frekvenca**	**Odstotek**
	1 (Moški)	138	47%
	2 (Ženski)	157	53%
Veljavni	Skupaj	295	100%

Q4	V katero starostno skupino spadate?		
	Odgovori	**Frekvenca**	**Odstotek**
	1 (do 20 let)	21	7%
	2 (21 - 35 let)	205	69%
	3 (36 - 55 let)	65	22%
	4 (56 - 65 let)	3	1%
	5 (65 let ali več)	1	0%
Veljavni	Skupaj	295	100%

Q5	Kakšna je vaša najvišja dosežena formalna izobrazba?		
	Odgovori	**Frekvenca**	**Odstotek**
	1 (Manj kot srednja šola)	1	0%
	2 (Srednja šola)	125	42%
	3 (Višja šola)	17	6%
	4 (Visoka šola (VS/UN))	118	40%
	5 (Specializacija)	2	1%
	6 (Magisterij)	30	10%
	7 (Doktorat)	2	1%
Veljavni	Skupaj	295	100%

Q6	Kakšen je vaš trenutni status?		
	Odgovori	**Frekvenca**	**Odstotek**
	1 (Dijak/inja)	2	1%
	2 (Študent/ka)	154	52%
	3 (Zaposlen/a)	115	39%
	4 (Brezposeln/a)	11	4%
	5 (Upokojenec/ka)	3	1%
	6 (Drugo:)	10	3%
Veljavni	Skupaj	295	100%

Q6j_text	Q6 (Drugo:)		
	Odgovori	**Frekvenca**	**Odstotek**
	študent/zaposlen	1	0%
	študent; sin, vnuk, bratranec, stric, moozikant, prijatelj grivastih in svetlečih bodočih doktorjev obrambnih ved.	1	0%
	samozaposlena / izredna študentka mag	1	0%
	samozaposlena	3	1%
	prekerc	1	0%
	s.p.	1	0%
	na porodniški	1	0%
Veljavni	Skupaj	9	3%

Delovni življenjepis študenta

ZAPOSLITVE:

- **Koordinator (2018–v teku)**
  Primož Repnik s.p., Kamnik

- **Namestnik vodje penziona (2018)**
  Primož Repnik s.p., Kamnik

- **Asistent (visokošolski sodelavec) (2017–2018)**
  Univerza v Mariboru, Fakulteta za organizacijske vede, Kranj

- **Asistent (visokošolski sodelavec) (2014–2017)**
  Univerza v Mariboru, Fakulteta za logistiko, Celje

IZOBRAZBA:

- **Magister varstvoslovja**
  Fakulteta za varnostne vede, 2013

- **Diplomirani varstvoslovec (UN)**
  Fakulteta za varnostne vede, 2011

OSEBNA BIBLIOGRAFIJA (COBISS):

šifra raziskovalca 37588

Univerza v Mariboru

Fakulteta za logistiko

IZJAVA O AVTORSTVU IN ISTOVETNOSTI TISKANE IN ELEKTRONSKE OBLIKE DOKTORSKE DISERTACIJE

Ime in priimek študenta: **Gašper Hribar**
Študijski program: **Logistika sistemov (3. bolonjska stopnja)**
Naslov doktorske disertacije: **Model celovitega zaupanja državljanov v matične obveščevalno-varnostne službe: logistika aplikacije**
Mentor: **red. prof. dr. Bojan Rosi**
Somentor: **red. prof. dr. Iztok Podbregar**

Podpisani študent**:**

- izjavljam, da je zaključno delo rezultat mojega znanstvenoraziskovalnega dela;
- izjavljam, da sem pridobil vsa potrebna soglasja za uporabo podatkov in avtorskih del v zaključnem delu in jih v zaključnem delu jasno in ustrezno označil;
- na Univerzo v Mariboru neodplačno, neizključno, prostorsko in časovno neomejeno prenašam pravico shranitve avtorskega dela v elektronski obliki, pravico reproduciranja ter pravico ponuditi zaključno delo javnosti na svetovnem spletu preko DKUM in drugih informacijskih zbirk in ponudnikov; seznanjen sem, da bodo dela deponirana/objavljena v DKUM dostopna široki javnosti pod pogoji licence Creative Commons BY-NC-ND, kar vključuje tudi avtomatizirano indeksiranje preko spleta in obdelavo besedil za potrebe tekstovnega in podatkovnega rudarjenja in ekstrakcije znanja iz vsebin; uporabnikom se dovoli reproduciranje brez predelave avtorskega dela, distribuiranje, dajanje v najem in priobčitev javnosti samega izvirnega avtorskega dela, in sicer pod pogojem, da navedejo avtorja in da ne gre za komercialno uporabo;
- dovoljujem objavo svojih osebnih podatkov, vezanih na zaključek študija (ime, priimek, leto zaključka študija, naslov zaključnega dela) na spletnih straneh Univerze v Mariboru in v publikacijah Univerze v Mariboru;
- izjavljam, da je tiskana oblika zaključnega dela istovetna elektronski obliki zaključnega dela, ki sem jo oddal za objavo v DKUM;
- izjavljam, da sem seznanjen s pogoji Proquest-a za oddajo in javno objavo doktorske disertacije v podatkovni zbirki ProQuest Dissertations & Theses Global (http://contentz.mkt5049.com/lp/43888/382619/PQDTauthoragreement.pdf).

Kraj in datum:_____ Podpis študenta/-ke:_____