UNIVERZA V LJUBLJANI

FAKULTETA ZA DRUŽBENE VEDE

David Stonič

Oblikovanje modela za ocenjevanje hibridnega ogrožanja nacionalne varnosti: primer Slovenije

Magistrsko delo

Ljubljana, 2017

UNIVERZA V LJUBLJANI

FAKULTETA ZA DRUŽBENE VEDE

David Stonič

Mentor: izr. prof. dr. Uroš Svete

Oblikovanje modela za ocenjevanja hibridnega ogrožanja nacionalne varnosti: primer Slovenije

Magistrsko delo

Ljubljana, 2017

»Svet danes nima smisla, zakaj bi ga torej slikal, kot da ga ima?«

Pablo Picasso

ZAHVALA

Zahvalil bi se mentorju dr. Urošu Svetetu za usmerjanje raziskovanja po začrtani rdeči niti skozi celotni proces.

Zahvala gre tudi Juriju, Dušanu in Viljemu za medsebojno spodbujanje v celotnem času šolanja.

Posebej bi se zahvalil podpolkovniku Lojzetu Paviču, ki me je motiviral, da sem se odpravil na to pot.

Vsekakor poti ne bi prehodil, če mi ob strani ne bi stala soproga Vesna in moja celotna družina.

Oblikovanje modela za ocenjevanja hibridnega ogrožanja nacionalne varnosti: primer Slovenije

V spremenjenem varnostnem okolju moramo razviti ustrezne koncepte in orodja za pravočasno prepoznavanje in opredelitev hibridnih groženj, da bi se lahko uspešno odzvali. Tematiko smo predstavili skozi ugotavljanje kontinuitete in diskontinuitete pojmov, ki se nanašajo na oblike varnostnih groženj in vodijo v pojav pojmov hibridna vojna, hibridne grožnje in hibridni konflikti. Identificirali smo indikatorje konvencionalnih in indikatorje nekonvencionalnih groženj. Oblikovali smo model, ki grožnje poveže z akterjem. Ovrednoteni obveščevalni podatki so vstopne informacije v izdelan model za ocenjevanje hibridne ogroženosti nacionalne varnosti. Izhodna informacija je identificirana hibridna grožnja. Hibridna grožnja državnega, nedržavnega ali posredniškega akterja je pogoj, da se lahko določi stopnjo hibridne ogroženosti nacionalne varnosti. Stopnjo hibridne ogroženosti ocenjujemo s parametri ogrožanja in stopnjujemo s petstopenjsko lestvico hibridnega ogrožanja. Ob izpolnitvi pogoja hibridne ogroženosti lahko nacionalnovarnostni sistem začne izvajati ukrepe, ki bi zmanjšali zmožnosti delovanja hibridnega akterja. Zavedanje o obstoju hibridnih groženj in njihovo identificiranje bo spodbudilo odločevalce v nacionalnovarnostnem sistemu, da bodo zagotovili ustrezno hibridno odpornost države, saj je primarna odgovornost za soočanje s hibridnimi grožnjami primarno odgovorna država in potreben je celostni vladni pristop v povezavi z Evropsko zvezo in severnoatlantskim zavezništvom.

Ključne besede: hibridne grožnje, indikatorji konvencionalnega ogrožanja, indikatorji nekonvencionalnega ogrožanja, obveščevalni podatek.

Forming of the evaluation model of the national security hybrid threats. Case study Slovenia

In the changed security environment, we have to be able to react in time and have to develop appropriate concepts and tools to detect, recognize and identify hybrid threats. We introduced the theme by determining continuity and discontinuity of concepts, that could mean some form of security/safety threats that led in formation of determining the concepts of hybrid war hybrid threat, and hybrid conflict.

We formed the model which connects the threats with the actor evaluated intelligence data are the input information to the made model for the evaluation of the national security hybrid threat. Output information is the identified hybrid threat. The hybrid threat of the state, non-state or proxy actors is the condition that enables us to determine the level of the national security.

The level of the hybrid threat is evaluated by the parameters of compromising on the five tiered scale. When the hybrid threat is detected, national security system can start with the implementation of measures, which could diminish the capability of the hybrid actor's operations.

The awareness of the hybrid threats possibility and their identification will encourage the decision makers in the national security system to insure the hybrid resilience of the state since the primary responsibility in facing hybrid threats stays with the state as a governments approach is necessary in combination with the European Union and the North Atlantic Treaty Organization.

Key words: hybrid threats, conventional threat indicators, unconventional threat indicators, intelligence data.

Kazalo

Kazalo slik

Seznam kratic

- AAP - Allied Administrative Publication
- AJP - Allied Joint Procedures
- BDP - Bruto družbeni proizvod
- CERT - Computer Emergency Response Team
- CFE TLE - Conventional Forces in Europe Treaty Limited Equipment
- COMINT - Communication Intelligence
- CYBINT - Cyber Intelligence
- DHS - Department of Homeland Security
- DOŠO - Državni operativni štab obrambe
- DNK - Deoksiribonukleinska kislina
- DNINT - Digital Network Intelligence
- DTA - Domestic Threat Analysis Division
- EU - European Union
- ELINT - Electronic Intelligence
- FISINT - Foreign Instrumentation Signals Intelligence
- GEOINT - Geospatial Intelligence
- HUMINT - Human Intelligence
- ID - Identification
- IKT - Informacijsko-komunikacijska tehnologija
- IMINT - Imagery Intelligence
- ISAF - International Security Assistance Forces
- MANPAD - Man-portable air-defense system
- MAS - Medresorska analitična skupina
- MASINT - Measurement and Signature Intelligence
- MEDINT - Medical Intelligence
- MNZ - Minstrstvo za notranje zadeve
- MO - Ministrstvo za obrambo
- MZZ - Ministrstvo za zunanje zadeve
- NATO - North Atlantic Treaty Organization
- NCKU - Nacionalni center kriznega upravljanja
- OSINT - Open Source Intelligence

- OZN - Organizacija Združenih Naodov
- RA - Republika Avstrija
- RAND - Research and Development
- ReSNV - Resolucija nacionalne varnosti
- RH - Republika Hrvaška
- RPG - Rocket Propeller Grenade
- RS - Republika Slovenija
- SI CERT - Slovenian Computer Emergency Response Team
- SIGINT - Signal Intelligence
- SNAV - Svet za nacionalno varnost
- SOCINT - Sociocultural Intelligence
- SSNAV - Sekretariat sveta za nacionalno varnost
- STRATCOM - Strategic communications
- SV - Slovenska vojska
- UVTP - Urad za varovanje tajnih podatkov
- ZDA - Združene države Amerike
- QDR - Quadrennial Defense Review
- WMD - Weapons of mass distraction

1 Uvod

Rdeča nit naloge bodo hibridne grožnje, ki transnacionalno zaposlujejo teoretike obramboslovja, vojaške zgodovinarje, vojaške strokovnjake vsekakor politike in nosilce odgovornih državniški funkcij. Hibridnost, s katero se srečujemo na obrambno varnostnem področju, je pomembna razsežnost, ki potrebuje nadaljnje raziskovanje in je ali pa bo velika prednost tistih državnih in nedržavnih akterjev, ki jo bodo znali prepoznati in preventivno ukrepati. S samimi hibridnimi grožnjami sem se tudi osebno srečal na področjih, kjer sem kot častnik Slovenske vojske deloval (Kosovo, Bosna in Hercegovina) in tudi v Afganistanu kot mednarodni civilni svetovalec na obveščevalnem področju v NATO (North Atlantic Treaty Organization) poveljstvu ISAFa (International Security Assistant Forces). Predvsem pri tem sem pridobil izkušnje. Ugotovil sem neverjetno visok nivo in prednost upornikov, ki so imeli izpopolnjen sistem strateškega komuniciranja (STRATCOM), organiziranost tega pa je pogoj, za graditev hibridne odpornosti. STRATCOM je tematika, ki se ji v tej nalogi ne bomo posvečali. V nadaljevanju uvoda bomo na kratko obdelali nekaj zgodovinskih dejstev, ki bodo nakazala smer raziskovanja.

V obdobju po drugi svetovni vojni, imenovanem hladna vojna, se je svet soočal s stalno napetostjo zaradi možnosti izbruha nove konvencionalne vojne, ki bi po vseh projekcijah vodila v za človeštvo uničujoč jedrski spopad dveh vojaškopolitičnih polov. V obdobju hladne vojne, ki se je končala s padcem berlinskega zidu, je kljub stalni prisotnosti možnega izbruha konvencionalne jedrske vojne potekalo več konfliktov. Svete (2016, 99) navaja, da tretjino teh konfliktov lahko označimo kot tradicionalne, simetrične meddržavne vojne. Ostalo so bile notranje vojne, ki so bile po svoji naravi večinoma asimetrične, kljub temu da lahko mnoge spopade umestimo med posredniške oziroma proxy vojne. Za ostale konflikte je značilna asimetričnost z gverilskim uporništvom, to so kartelni spopadi in vojne ter tudi mednarodni terorizem.

Način končanja obdobja stalnih konvencionalnih groženj in s tem hladne vojne se odraža v tako imenovani veliki strategiji ZDA (Združene države Amerike) ali Reaganovi veliki strategiji, ki vsebuje konvencionalno grožnjo odvračanja, ki je bila le nastavek za poznejše asimetrične prijeme in propad Sovjetske zveze ter Varšavskega pakta. Odvračanje ali »deterrence«. Za angleški izraz »deterrence«, ki je eden temeljnih strateških terminov na vojaškem jedrskem področju, v slovenskem strokovnem izrazoslovju še nima dogovorjene inačice. Ponujajo pa se vsaj tri možnosti: zastraševanje, odvračanje in odvračanje z zastraševanjem (Lubi 1999, 29).

Pernat (2006) zapiše, da je v splošnem pomenu odvračanje z zastraševanjem princip prepričevanja nasprotnika, da so negativne posledice zanj večje od njegove koristi. Na vojaškopolitičnem področju je odvračanje z zastraševanjem način, oziroma odnos, s katerim država drugi državi vzbuja strah pred maščevanjem in jo s tem odvrača od napada. V času hladne vojne je bil eden izmed ciljev ZDA postopno spodbujanje sprememb v Sovjetski zvezi. Kar jim je na koncu tudi uspelo s pomočjo tihe diplomacije, zaščite človekovih pravic z ekonomsko liberalizacijo in ostalih politik na področju gospodarstva.

Razpad Varšavskega pakta in s tem bipolarnosti je pripeljal do sprostitve nakopičenega konvencionalnega orožja, kar je v novonastalih državah povečalo možnost groženj. Namesto dotlej značilnega asimetričnega jedrsko konvencionalnega (ne)ravnotežja, v katerem je Nato številčno podrejenost v konvencionalnem orožju nadomeščal z jedrsko premočjo in konceptom zračno-kopenske bitke, taktičnim jedrskim orožjem in samovodljivimi izstrelki, sta se strani sporazumno odločili za simetrično konvencionalno ravnotežje. Med pogovori in pogajanji vojaških izvedencev iz 21 držav pred podpisom prvega sporazuma CFE TLE (Conventional Forces in Europe Treaty Limited Equipment) so se države sporazumele o štirih bistvenih strateških izhodiščih:

- določitev kazalnikov za opredelitev ofenzivnih sistemov,
- določitev kazalnikov za ugotavljanje števila vojakov,
- katere geografske ključe bodo uporabili pri razporejanju sil po posameznih območjih Evrope,
- kako bodo države podpisnice zagotovile učinkovit mednarodni nadzor nad izvajanjem podpisane pogodbe (Žabkar 2003, 322).

Žabkar (2003) potem predstavi, da je vsaka stran – Nato in Budimpeštanska skupina, ki je po razpustitvi Varšavskega sporazuma zajela njegove nekdanje članice – smela po podpisu sporazuma CFE TLE v Evropi obdržati po 20.000 tankov, 30.000 bojnih vozil pehote, 20.000 artilerijskih sistemov za splošno podporo, 6.800 letal in 2.000 bojnih helikopterjev.

Vendar pa je tako dosežena stabilnost, ki je temeljila na simetričnem ravnotežju konvencionalnih sil, postala nezanesljiva že leta 1998, ko so Poljska, Češka in Madžarska, ki so bile prej kot članice Budimpeške skupine vključene v seštevek z Rusko federacijo, postale članice Nata (Žabkar 2003, 323).

Uvod v nalogo lahko končamo z ugotovitvijo, da je konvencionalno ogrožanje nacionalne varnosti v Evropi bilo vse do leta 1998 nekako pod kontrolo. S širitvijo Nata proti vzhodu konvencionalne grožnje predvsem v očeh Rusije postanejo novo dejstvo.

Tudi v prihodnosti ni pričakovati veliko konfliktov, v katerih bi bile vloge sprtih strani jasne in definirane na tradicionalen način, značilen za obdobje hladne vojne (Svete in drugi 2010, 252). Svete (2016) ugotavlja, da je povečan pomen asimetričnega in tudi hibridnega vojskovanja posledica zahodne konvencionalne vojaške premoči (Svete 2016, 105).

Svete (in drugi 2010, 249) metaforično primerjajo nekonvencionalno ali asimetrično bojevanje z antičnim bojem Davida in Goljata, kjer fizično premoč nadvlada fizično šibkejši z uporabo za tisti čas nepoznane tehnologije. To je tudi bistvo pojavljanja nekonvencionalnih groženj, s katerimi konvencionalno šibkejši išče slabosti nasprotnika.

Vsekakor je o tem že 500 let pred našim štetjem pisal starokitajski vojaški teoretik Sun Cu Vu, ki je dejal, da je največja veščina, da se odpor nasprotnika zlomi brez boja. Seveda v takem primeru ne moremo govoriti o hibridnem vojskovanju prav tako ne o asimetričnem, saj oboroženih konvencionalnih konfliktov sploh ni. Lahko pa govorimo o različnih varnostno zanimivih in relevantnih pojavih.

1.1 Opredelitev predmeta proučevanja

Izraz hibrid se že dolgo uporablja na različnih področjih življenja, tako v kmetijstvu, avtomobilizmu idr. Vsekakor je hibrid nekaj, kar ni nastalo samo od sebe s pomočjo narave, ampak je spremenjeno s pomočjo človeka in moderne tehnologije. Hibrid je nekaj, kar ustvari človek s svojo tehnologijo in znanostjo, obstoječi entiteti ali izdelku doda novo lastnost pa naj bo to DNK (deoksiribonukleinska kislina) pri flori in favni ali dodaten pogon pri avtomobilu. Na varnostnem področju se pojavi pojem hibrid ob koncu prejšnjega desetletja.

Svete (2016) hibridno vojskovanje predstavi kot kombinacijo različnih konvencionalnih in nekonvencionalnih oblik/orodij vojskovanja. Škerbinc (2015) hibridno vojskovanje povezuje s sinergijskimi učinki materialnih in kognitivnih zmogljivosti ter prikrito ali odkrito agresijo z neupoštevanjem legalnih omejitev ob simultani izrabi prvin mednarodne moči za vsiljevanje lastnih strateških mednarodno nelegitimnih ciljev.

Članek »Spreminjajoča se podoba vojne«, ki ga je objavil William S. Lind (Lind in drugi 1989) izpostavi štiri generacije vojne moderne zgodovine. Za četrto pravi, da je vojna, ki vključuje celotno družbo. Hibridna vojna je potem lahko peta generacija vojskovanja. Kljub temu, da se je koncept hibridne vojne uporabljal že davno, ga je prvič zapisal leta 2006 polkovnik ameriške vojske Frank Hoffman. Bricman (2016) zapiše, da se je že v ameriški revoluciji pojavljala

kombinacija konvencionalnih in nekonvencionalnih metod za dosego političnih ciljev (Bricman 2016, 13).

Eno od pomembnih dejstev v nalogi bo opredelitev novih groženj, ki so predvsem povezane z razvojem novih tehnologij in vse večjo družbeno kompleksnostjo. Ne smemo tudi mimo dejstva, da določene grožnje, ki jih lahko uvrstimo med nekonvencionalne, obstajajo že dolgo časa, vendar jih nismo zaznavali. Nekaj takšnih groženj navaja Grizold (2005) kot nevojaške grožnje: množično nespoštovanje temeljnih človekovih pravic in svoboščin, onesnaževanje okolja posledično segrevanja ozračja, lakota, nalezljive bolezni, trgovina z drogami in belim blagom, nenadne migracije. Leta 2007 so Prezelj (in drugi 2007) pri izdelavi modela celovitega ogrožanja nacionalne varnosti republike Slovenije poleg vojaške dimenzije ogrožanja opredelili še informacijsko ogrožanje, ekonomsko ogrožanje, teroristično ogrožanje, ogrožanje organizirane kriminalitete, zdravstveno ogrožanje, okoljsko in migracijsko ogrožanje.

Pri razmišljanju o diskontinuiteti in kontinuiteti hibridnega vojskovanja si Malešič in Žabkar (2016) zastavita vprašanje, za katero menita, da je v razpravah o hibridnem vojskovanju ključno tako doma kot v tujini, in sicer v kolikšni meri gre za kontinuiteto glede na prejšnje sorodne zasnove, v kolikšni meri pa gre za pojmovanje novosti.

Malešič in Žabkar (2016) navajata Rentza in Smitha (2016), ko ugotavljata, da se vzporedno hibridnim zasnovam uporabljajo tudi druge zasnove, »nove vojne, vojskovanje četrte generacije in asimetrično bojevanje«. Četrta generacija vojskovanja v povezavi z visoko tehnologijo naj bi bilo vojskovanje šeste generacije (Malešič in Žabkar 2016, 28). V citiranem tekstu avtorja ne omenita pete generacije vojskovanja. Omenili smo že, da bi hibridno vojskovanje lahko bilo peta generacija vojskovanja, kar omenjeno besedilo posredno nakazuje.

Ray Alderman (2015) na svojem blogu zapiše, da je šesta generacija vojskovanja tista, ki lahko vpliva na sofisticirano tehnologijo, da deluje neodvisno od prostora in časa. Cigler (2016) navaja, da je šesta generacija vojskovanja stanje, ko vojna ni več nadaljevanje politike z nasilnimi sredstvi za zagotavljanje končne zmage, temveč je začetek politike za zagotovitev končnih ciljev z nevojaškimi sredstvi (Cigler 2016, 85).

Svete (2016) navaja zgodovinarja Murraya in Mansoorja (2012), ki nasprotujeta temu, da je koncept hibridnega vojskovanja novost. Tudi Malešič in Žabkar (2016) opozarjata na paradoksalnost večine avtorjev, ki da kritizirajo zasnovo hibridnega vojskovanja, da je podobno sorodnim preteklim zasnovam in navajajo njegove analitične pomanjkljivosti, hkrati pa jih uporabljajo v svojih analizah.

Ugotavljamo, da je na konceptualnem področju, ki se ukvarja s hibridnim vidikom varnosti še precej nedorečenosti. Pogled na to s stališča javnosti (laične) pa zna v tem pogledu biti še bolj

zamegljen. Svete (2016) izpostavlja, da javnost s svojim nepoznavanjem izjemno podpira vojsko, po drugi strani pa nasprotuje njenemu mednarodnemu delovanju, kar ne velja le za države z ekspedicijsko tradicijo temveč tudi za Slovenijo. Hibridnost in neenotnost v družbenem odnosu do nacionalnovarnostnih vprašanj pa je mnogo večji problem kot novi akterji, improvizirana in informacijska tehnologija ter propagandne aktivnosti (Svete 2016, 109).

Poskušali bomo nakazati ali izdelati model, ki ga bomo uporabili pri prepoznavanju in analiziranju hibridnih groženj, in empirično preizkusiti delovanje na primeru Slovenije. Za izdelavo modela bomo izhajali iz modela celovitega ocenjevanja ogrožanja nacionalne varnosti v republiki Sloveniji (Prezelj in drugi 2007) in modela, ki ponazarja stičišča hibridnih groženj (Bowers 2012).

Prezelj (in drugi 2007) je raziskal vojaške razsežnosti ogrožanja nacionalne varnosti. Identificiral je štirinajst temeljnih indikatorjev konvencionalnega ogrožanja, ki nam bodo smernica tudi pri določevanju indikatorjev nekonvencionalnega ogrožanja.

Pri prepoznavanju hibridnega ogrožanja se moramo zavedati, da mora organizacija oziroma država imeti vsaj nekaj sodobnih vojaških zmogljivosti ugotavlja Bowers (2012). Hkrati pa Bowers (2012) povzema Davida Johnsona, ki pravi, da ni dovolj, da nekdo poseduje sodobno orožje, ampak ga mora znati tudi pravilno taktično uporabljati skupaj z ostalimi zmogljivostmi kot del večje operacije. V nasprotnem lahko govorimo le o orožju in ne zmogljivosti (Bowers 2012, 41).

Do zanimivih ugotovitev je prišel tudi Vegič (2016), ki pravi, da ima hibridno vojskovanje nekaj izrazitih značilnosti: usklajena uporaba različnih oblik vojskovanja, kjer gre za kombinacijo vseh vrst vojaškega (regularnega in neregularnega) delovanja in nevojaškega delovanja, ki je praviloma najpomembnejše; prikrivanje akterjev, metod in ciljev; vse težje razlikovanje med mirom in vojno. V takšnem vojskovanju najdemo akterje in oblike delovanja, ki niso značilni za vojskovanje, prikriti značaj vojskovanja pa posledično zmanjšuje možnost zaznave, da to sploh poteka.

Oblikovani model za prepoznavanje in analiziranje hibridnih groženj bomo preizkusili na primeru Slovenije. S pomočjo javno dostopnih virov bomo poiskali morebitne grožnje v določenem časovnem obdobju in jih analizirali.

Analizirali bomo varnostne grožnje zoper Slovenijo. Analizo bomo uporabili kot izhodišče za pripravo fokusiranega intervjuja. Intervju bomo izvedli s posamezniki, ki se na državnem nivoju ukvarjajo z varnostnimi vprašanji in so tudi politični nosilci odgovornih funkcij. S

pomočjo analize groženj in analize intervjujev bomo lahko preizkusili model in potrdili oziroma ovrgli postavljeno hipotezo.

1.2 Relevantnost naloge

Visoka predstavnica Evropske unije (EU) za zunanje zadeve in varnostno politiko je 6. aprila 2016 izdala skupno sporočilo Evropskemu parlamentu in Svetu (Skupni okvir o preprečevanju hibridnih groženj – odziv Evropske unije, 2016, 3), kjer je med drugim navedeno, da je cilj hibridnih groženj izkoristiti ranljivosti države in pogosto tudi spodkopati temeljne demokratične vrednote in svoboščine. Kot prvi korak bosta visoka predstavnica in komisija sodelovali z državami članicami, da se s spremljanjem in ocenjevanjem tveganj, ki so lahko usmerjena v ranljivost EU, okrepi zavedanje o situaciji. Komisija razvija metodologije za oceno varnostnega tveganja, da bi lažje obveščala nosilce odločanja in spodbujala oblikovanje politik na podlagi tveganja na področjih, ki segajo od varnosti v letalstvu do financiranja terorizma in pranja denarja. Poleg tega bi bilo ustrezno, da države članice izvedejo raziskavo, v kateri bi opredelile področja, na katerih obstaja nevarnost za hibridne grožnje. Cilj bi bil opredeliti kazalnike hibridnih groženj, jih vključiti v mehanizme zgodnjega opozarjanja in obstoječe mehanizme za oceno tveganja ter jih po potrebi souporabljati.
Relevantnost magistrske naloge se kaže tudi v ukrepu št. 1, ki ga je izdala visoka predstavnica. Države članice, po potrebi ob podpori Komisije in visoke predstavnice, naj začnejo s pripravljati raziskavo o hibridnih grožnjah za opredelitev ključnih ranljivosti, vključno s posebnimi kazalniki, povezanimi s hibridnimi grožnjami, ki lahko potencialno vplivajo na nacionalne in vseevropske strukture in mreže. Ta naloga bi lahko pristavila del v mozaik reševanja ukrepa številka 1 Evropske komisije članicam Evropske unije (Skupni okvir o preprečevanju hibridnih groženj – odziv Evropske unije, 2016: 3─4)

1.3 Raziskovalno vprašanje in hipoteza

V teoretičnem delu naloge bomo predstavili tematiko in ob obravnavi ugotavljali kontinuiteto in diskontinuiteto pojmov, ki se nanašajo na oblike varnostnih groženj in vodijo v pojav pojmov

hibridna vojna, hibridne grožnje, hibridni konflikt. Zato si bomo zastavili raziskovalno vprašanje:

RV:1

Ali lahko s pomočjo teorije operacionaliziramo hibridno ogrožanje?

Na osnovi dognanj bomo identificirali indikatorje groženj tako konvencionalnih kot nekonvencionalnih in jih poskušali povezati v model, ki bo omogočal njihovo prepoznavanje, povezovanje z akterji in analiziranje.

V empiričnem delu naloge bomo preučili možne grožnje v Sloveniji, jih preizkusili s pomočjo modela in poskušali preveriti hipotezo:

H:1

Hibridna ogroženost nacionalne varnosti Slovenije je bistveno višja, kot jo v javnosti predstavljajo predstavniki nacionalnovarnostnega sistema.

Vzporedna analiza sklicev sveta za nacionalno varnost Slovenije (SNVS) nam pokaže, da se je SNVS v letih 2015 in 2016 veliko večkrat sestal kot v letih prej. Vsekakor je lahko logični vzrok predvsem migrantski tok, ki je potekal čez Republiko Slovenijo. Ne smemo pa izključiti možnosti, da so je na SNVS razpravljali tudi o drugih zadevah. Znano je, da se po vsaki seji stopnja ogroženosti Republike Slovenije ni spremenila in je ostala enaka─nizka.

1.4 Raziskovalne metode

Pri preučevanju bomo uporabili različne raziskovalne metode, s pomočjo katerih bomo poskušali potrditi, delno potrditi ali zavreči hipotezo, ki smo si jo zastavili, in odgovoriti na

raziskovalno vprašanje. V magistrskem delu gre pri preučevanju za interdisciplinarnost, saj bomo gradivo za nalogo črpali iz različnih znanstvenih ved:

- predvsem obramboslovja s preučevanjem teoretskih, metodoloških in empiričnih spoznanj uveljavljenih domačih teoretikov.
- Vojaških ved, katerih teorije bomo raziskovali predvsem za obrazložitev osnovnih konceptov preučevane materije, in iz vojaške zgodovine s pomočjo katere bomo preučili kontinuiteto razvoja pojma hibridnega ogrožanja. Spoznanja različnih ved bomo uporabili kot oporo pri analizi.
- Teoretični del se bo v večji meri nanašal na obramboslovje, vojaške vede, zgodovino, v empiričnem delu pa bomo predvsem z metodo analize javno objavljenih zapisov o varnostnih grožnjah dobili vpogled v poročanje o grožnjah.

V teoretičnem delu bomo s pomočjo analize primarnih pisnih virov (dokumenti, zakoni, standardni operativni postopki) in z analizo sekundarnih virov (znanstvenih in strokovnih člankov, literature, akademskih, magistrskih in doktorskih del) poskušali konceptualizirati problematiko.

Za izdelavo modela identificiranja hibridnih groženj bomo uporabili metodo modeliranja kot poenostavitev aplikacije na hibridne grožnje.

V empiričnem delu naloge bomo uporabili študijo primera in metodo opazovanja s pomočjo analize političnega diskurza, zaznanega v elektronskih in tiskanih medijih ter analizirali delo državnih ustanov s področja varnosti. Izvedli bomo fokusiran intervju z namestnikom generalne sekretarke/svetovalcem predsednika za obrambne zadeve na Uradu predsednika RS (Republika Slovenija), s kompetentnima osebama z Ministrstva za notranje zadeve RS (MNZ) in Ministrstva za zunanje zadeve RS (MZZ), državnim sekretarjem v kabinetu predsednika vlade RS in z namestnikom direktorja oddelka za vojaško načrtovanje in vojaško politiko vojaškega odbora zavezništva Nato.

1.5 Struktura in cilj naloge

V uvodu in prvem poglavju magistrskega dela so v okviru metodološko hipotetičnega dela opredeljeni predmet preučevanja, relevantnost naloge, uporabljene raziskovalne metode,

struktura in cilj magistrskega dela ter postavljena raziskovalno vprašanje in hipoteza. Uporabljeni novi pojmi in terminologija so smiselno obrazloženi na mestih v magistrskem delu, kjer so prvič uporabljeni.

V drugem poglavju so opredeljeni temeljni koncepti, ki jih v magistrskem delu uporabljamo. Opredeljeni koncepti so konvencionalne grožnje, nekonvencionalne grožnje, hibridne grožnje. Izpostavili bomo tudi asimetrične grožnje, kibernetske grožnje ter indikatorje konvencionalnih, asimetričnih in kibernetskih indikatorjev groženj.

V tretjem poglavju bomo raziskovali informacijsko dimenzijo hibridnih varnostno zanimivih pojavov in se osredotočili na pridobivanje in vrednotenje informacij na obveščevalni sistem ter obdelali elemente nacionalnovarnostnega sistema, na katere hibridne groženje lahko vplivajo.

V empiričnem delu naloge bomo v četrtem poglavju vzpostavili metodologijo identificiranja hibridnih groženj. Izdelali bomo model ocenjevanja hibridnih grožen ter izdelali in obrazložili petstopenjsko lestvico za ocenjevanje hibridne ogroženosti.

V empiričnem delu raziskovanja bomo v petem poglavju analizirali ogroženost Slovenije. Izvedli in analizirali bomo fokusirane intervjuje in z rezultati analiz preizkusili izdelani model za prepoznavanje hibridnih groženj.

Šesto poglavje je namenjeno odgovoru na zastavljeno raziskovalno vprašanja in na potrditev oziroma zavrnitev postavljene hipoteze. Poglavje bomo končali s sklepnimi mislimi in priporočili za nadaljnje raziskovanje tematike.

Na koncu magistrskega dela so še seznam literature in drugih virov (sedmo poglavje) ter priloga.

Cilj naloge je izdelati model za prepoznavanje hibridnih groženj in ga preizkusiti na Sloveniji. Cilj naloge je tudi odgovoriti na raziskovalno vprašanje in potrditi ali zavreči postavljeno hipotezo.

2 Opredelitev temeljnih konceptov

V poglavju bomo opredelili temeljne koncepte, s katerimi se bomo v nalogi srečevali. Za lažje razumevanje se bomo sprehodili skozi generacije vojskovanja. Podrobneje bomo obdelali konvencionalne grožnje in nekonvencionalne grožnje, na koncu poglavja pa bomo definirali še hibridne grožnje. Za vse grožnje bomo iz zapisanih teoretičnih opredelitev ogrožanja izluščili indikatorje posamezne grožnje.

Omenili smo že William S. Lind (Lind in drugi 1989) in njegovo tezo o štirih generacijah vojne.

Napoleonove vojaške kampanje z mušketo opredeli kot prvo generacijo. Lind zapiše tudi, da so se zaradi tehnologije tistega časa razvile taktike linij in stolpcev. S pomočjo linij so poveljujoči lahko najbolje uporabili moč ognja. Bile so pa tudi posledica družbenih razmer in idej 18. stoletja. S stolpci so zmanjšali vpliv nizkega nivoja usposobljenosti vpoklicanih vojakov, hkrati pa so stolpci bili, energija in moč francoske revolucije.

Čeprav je danes muškete zamenjalo moderno avtomatsko orožje, so v moderni vojni še vedno prisotni sledovi prve generacije vojne, saj se na modernih bojiščih še vedno pojavlja težnja po linearnem vojskovanju. Za prvo generacijo je tudi značilno, da kljub temu, da umetnost operatike še ni bila konceptualizirana, so jo nekateri poveljniki tistega obdobja, predvsem Napoleon že uporabljali (Lind in drugi 1989, 23).

Preden nadaljujemo, bomo konceptualizirali pojem vojne, ki je preplet organiziranega nasilja, prilagojenega specifičnim zgodovinskim, socialnim, ekonomskim, tehnološkim in kulturološkim okoliščinam (Cigler 2016, 81).

Druga generacija vojne je bila odziv na puške z risanimi cevmi, mitraljeze, na neposredni ogenj, eksploziv za prodiranje in bodečo žico. Taktike so temeljile na ognju in premiku, vendar so v jedru ostale linearne. Cilj obrambe je ostal onemogočiti preboj sovražnika. Napadalci so delovali v majhnih in razpršenih linijah. Očitna razlika prve in druge generacije je bila v topništvu. Morda je najboljši povzetek druge generacije vojne francosko vodilo, ki pravi: »Topništvo osvoji, pehota zasede« (Lind in drugi 1989, 23).

Čeprav so novi koncepti v drugi generaciji vojne igrali pomembno vlogo, je bila glavna gonilna sila za spremembe tehnologija. Tehnologija se je kakovostno kazala s težjim topništvom in bombniki, z industrializacijo gospodarstva in bitko resursov, pa tudi količinsko. Prepoznava druge generacije vojskovanja sega v obdobje pruske vojske, ki je prva uvedla umetnost operatike. Spremembe so bile predvsem v novih tehnologijah in idejah. Tehnologije skozi razvoj železnice in telegrafa ideje pa so se kazale ob pruskih študijah Napoleonovih vojn (Lind in drugi 1989, 23).

Tretja generacija vojskovanja, tako kot druga, je bila rezultat prve svetovne vojne. Tretja generacija vojne se nanaša na povečanje ognjene moči na bojišču. Gonilna sila za spremembo vojne so bile tokrat ideje. Nove taktike vojskovanja so začeli razvijati Nemci že v začetni fazi prve svetovne vojne, ko so ugotovili, da v vojni resursov izgubljajo. Pojavljati so se začele taktike manevrov, napad z infiltracijo in obhodni manevri. Takšne taktične rešitve so odklon od linearnega vojskovanja. Čeprav so bili osnovni koncepti tretje generacije vojne do konca leta 1918 močno zasidrani v mišljenju poveljnikov, je operativno delovanje v drugi svetovni vojni močno spremenil razvoj tankov. Nemška vojska je razvila manevrsko vojskovanje, znano

kot »blitzkrieg« oz. bliskovita vojna. Tretja generacija vojskovanja ne temelji več na ognjeni moči in izčrpavanju, ampak na hitrosti in presenečenju. Taktično gledano je bil fokus napada prehod v sovražnikovo zaledje in uničenje od zadaj naprej – namesto »bližina in uničenje« je bil moto »obhod in uničenje«; fokus obrambe je bil usmerjen v dopuščanje sovražniku, da se približa nasprotnim položajem, sledila pa je obkolitev. Vojna tako ni več »izkazovanje moči«, kjer sile poskušajo zadržati ali prebiti linijo – tretja generacija vojskovanja je namreč nelinearna (Lind in drugi 1989, 23).

Lind (in drugi 1989) nakazuje, da bodo morali biti voditelji suvereni tako na področju umetnosti vojne kot na področju tehnologije, se pravi zahtevna kombinacija, ki zajema tako družboslovno kot naravoslovno kakovost bodočega vodje. Prednostni izzivi poveljujočih na vseh nivojih bodo izbira ciljev, ki pa bodo lahko tako politična kot kulturna in ne le vojaška odločitev, saj se bo zaradi kompleksnosti tehnologije bojišče ob zmanjševanju »škornjev na terenu« kompleksno širilo. Četrto generacijo vojskovanja bo usmerjala moderna tehnologija. V četrti generaciji, ki vključuje celotno sovražnikovo družbo, razpršenost po bojišču kliče po prilagodljivosti vojaških formacij na najnižji operativni ravni (Lind in drugi 1989, 24).

Žabkar (2004) navaja ameriškega znanstvenika Roberta Bunkerja, ki je analiziral stanje na področju vojskovanja po koncu svetovne bipolarnosti. Ugotavlja, da se bodo v času svetovne globalizacije pojavile nedržavne mednarodne organizacije, ki se bodo integrirale v določeno državo in njeno ozemlje izkoristile kot odskočno desko za napad na drugo državo. Tovrstno stanje vojskovanja je imenoval »vojne četrte epohe«.

Treba je omeniti tudi koncept večpodročnega vojskovanja (multi domain battle concept).

Tan (2016) navede generala Davida Perkinsa (poveljnika poveljstva za usposabljanje in doktrino ameriške vojske), ki pravi, »da mora vojska, ko se pripravlja za boj, na vedno bolj zapletenem in nepredvidljivem bojišču razmišljati nekonvencionalno«.

Nasprotnik bo imel učinkovita sredstva in zmogljivosti, ki jih imajo najbolj moderne države. To je bistvena razlika glede na preteklost. Kitajska, Ruska federacija, ZR Nemčija, ZDA in druge že uvajajo oz. imajo vzpostavljene kibernetske zmogljivosti. Napredne tehnološke zmogljivosti za kibernetsko in elektronsko bojevanje bodo postale vse pomembnejše in bodo segle na taktično raven. Tekmovanje za prevlado na bojišču bo tekmovanje za integracijo nove in tradicionalne zmogljivosti v sinergijskem modelu, ki je usmerjen v kognitivno zmožnost, da bo vojaška operacija izvedena kot kohezivna enota (Perkins 2016).

Koncept večpodročnega vojskovanja Jeninngs (2017) opredeli kot dominantni koncept, kateri se organizira med samo bitko na taktičnem nivoju, ob simultanem prodiranju in odrivanju kompleksne obrambe, z namenom hitre stabilizacije razmer na področju konflikta.

Slika 2.1: Tabela ponazarja razvoj asimetričnosti skozi omenjene štiri generacije vojskovanja

	1. generacija	2. generacija	3. generacija	4. generacija
čas	dogovorjen vnaprej	dogovorjen vnaprej	dogovorjen vnaprej	nenapovedan, nepredvidljiv
prostor	regionalni, lokalni	globalni	globalni	regionalni, lokalni, virtualni
taktika	linijska taktika (vojskovanje mož na moža)	"*artilerija osvaja, pehota zavzema*", naleti manjših skupin vojakov, pozicijsko vojskovanje in boj na izčrpavanje	»blitzkrieg«, »stealth« (tj. manj opazen a hiter odziv in mobilnost)	delno gverilska, delno vsebuje prvine terorističnega delovanja
akterji	državni akterji	državni akterji	državni akterji	državni in nedržavni akterji
oborožitev	muškete, bajoneti, pištole, topovi	tank, letalo, podmornica	tank, letalo, podmornica, jedrsko orožje	raketno in jedrsko orožje, informacijska tehnologija
tarče	nasprotnikova vojska	nasprotnikova vojska, tudi že civilno prebivalstvo	nasprotnikova vojska, civilno prebivalstvo	največkrat civilno prebivalstvo, razni pomembni objekti
mobilizacija	najemništvo, naborništvo, samoiniciativnost	poleg regularne vojske mobilizirana tudi civilna družba, slepo izpolnjevanje povelj	regularna vojska, revolucionarne skupine, slepo izpolnjevanje povelj	profesionalna vojska, regularna vojska, revolucionarne skupine, zasebne vojske, samoiniciativnost
cilj vojskovanja	nacionalni interesi, nacionalni konflikti	fizično uničiti nasprotnika	pridobiti nadzor nad ozemljem, uničiti nasprotnika	ustrahovanje civilnega prebivalstva; »duhovni kolaps«
številčnost nasprotnika	masovna vojska	manjša vojska	manjša vojska, enote	majhne skupine

bojne enote	konvencionalna vojska, naborniška vojska držav	konvencionalna vojska, majhne, mobilne skupine	konvencionalna vojska, majhne, hitre enote, delujejo neopazno	specializirane, majhne, visoko mobilne skupine, vozila brez posadke
teren	voda, kopno	voda, kopno, zrak	voda, kopno, zrak, pod vodno gladino	voda, kopno, zrak, pod vodno gladino

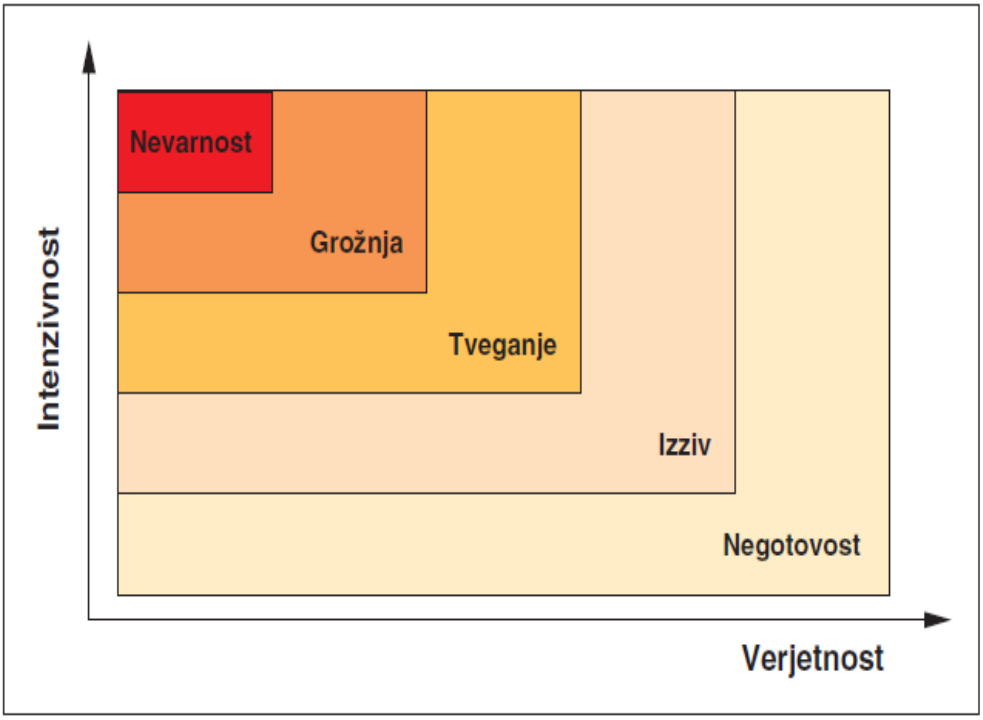
Vir: prirejeno po Kobola (2016, 64–65).

V nalogi se bomo srečevali s pojmom grožnje, pri čemer moramo specificirati, da pri grožnjah mislimo na varnostne grožnje. Prezelj (in drugi 2007) navede, da grožnje varnosti po svoji definiciji zajemajo vse družbene ali naravne pojave, ki zmanjšujejo varnost oziroma njene definicijske prvine. Da v tem smislu nadaljujemo, grožnje ogrožajo fizični obstoj prebivalstva. Grožnje motijo ali celo onemogočajo delovanje državnih ustanov in s tem onemogočajo izvajanje politične suverenosti in nemoten družbeni razvoj. Prezljeva definicija ogrožanja varnosti je zelo jasna. Kljub temu bomo za še natančnejšo obrazložitev, predvsem v delu, ki govori o družbenih in naravnih pojavih zmanjševanja varnosti, uporabili Kotnikovo razlago. Kotnikovo videnje ogrožanja nam bo pomagalo tudi pri obravnavanju kibernetskih groženj v povezavi z incidenti. Predvsem pa pri določanju oziroma selekcioniranju posameznih varnostno zanimivih pojavov v povezavi z akterji pri določanju hibridnega ogrožanja.

Kotnik (2000/2001) prikaže dva grafa, ki razmejita grožnjo z vojskovanjem in razvoj varnostno zanimivih pojavov od negotovosti do grožnje. Grafični prikaz (glej sliko 2.2) moramo razumeti samo kot bolj ali manj natančen približek realnosti, odraža pa tako kakovostno kot tudi količinsko razmerje med različnimi kategorijami varnostno zanimivih pojavov in/ali procesov, s katerimi se lahko soočijo namišljeni posameznik, družbena skupina ali država (Kotnik 2000/2001, 216).

Slika 2.2: Kategorizacija varnostno zanimivih pojavov/procesov v odvisnosti od verjetnosti in (potencialne) intenzivnosti stika s subjektom

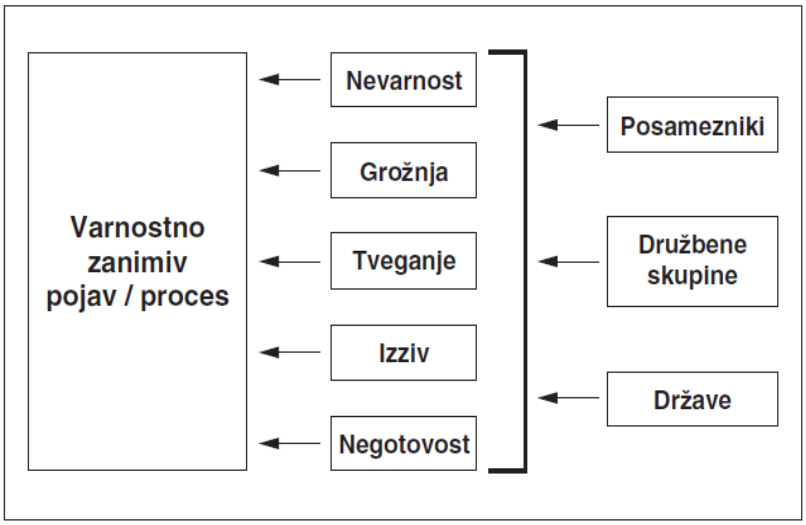
Vir: Kotnik (2000/2001, 216).



Za nas je pomemben prikaza grožnje in nevarnosti. Nevarnost lahko tolmačimo kot vojno stanje ali napad. Medtem ko so grožnje po intenzivnosti zelo visoko, pa se odmikajo od verjetnosti vojnega stanja.

Naslednji grafični prikaz nam pokaže odnos različnih subjektov do istega varnostno zanimivega pojava/procesa (glej sliko 2.3).

Slika 2.3: Odnos različnih subjektov do istega varnostno zanimivega pojava/procesa



Vir: Kotnik (2000/2001, 216).

Ugotavljamo, da se na najnižji stopnji intenzivnosti srečujemo z varnostnimi izzivi, ki lahko bodisi sami prerastejo v varnostna tveganja, bodisi jih spodbudijo kot interventni dejavnik, na naslednji stopnji pa se po preobrazbi ali spodbujenem varnostnem tveganju že lahko srečamo z varnostnimi grožnjami.

> *Ali je umestno govoriti o negotovosti, izzivu, tveganju, grožnji ali nevarnosti, je torej odvisno od verjetnosti (to je od trenutne prisotnosti/odsotnosti varnostno zanimivih pojavov/procesov) in (potencialne) intenzivnosti stika med pojavom/procesom in subjektom, ki se z njim (lahko) sooča. O varnostni negotovosti torej govorimo takrat, ko se pojavi vsaj minimalna možnost, da pride do stika med določenim varnostno zanimivim pojavom/procesom in subjektom (potencialna ogroženost), o varnostnih grožnjah in še posebej nevarnosti pa takrat, ko dejansko že prihaja do negativnega spreminjanja oz. znižanja dosežene ravni kakovosti posameznikovega in/ali družbenega življenja (realna ogroženost) (Kotnik 2000/2001, 216).*

2.1 Konvencionalne grožnje

Konvencionalne grožnje izhajajo predvsem iz oboroženih formacij neke države ali organizacije, orožja, ki ga uporabljajo, in stopnje tehnološke razvitosti tega orožja. Prezelj (in drugi 2007, 167) navaja Clausewitza, ki ugotavlja, da je vojna učinkovito politično orodje in povsem logično nadaljevanje političnih odnosov z drugimi sredstvi.

Vendar pa danes Ustanovna listina Organizacije Združenih Narodov (OZN) ne prepoveduje samo vojne, temveč tudi vsako grožnjo ali uporabo sile proti ozemeljski nedotakljivosti in politični neodvisnosti katerekoli države (Prezelj in drugi 2007, 167). Iz napisanega sledi, da je vsaka vojna modernega časa za napadalca nelegalna.

Prezelj (in drugi 2007, 170) zapiše definicijo, da vojaško ogrožanje nacionalne varnosti temelji na grožnjah z uporabo vojaških ali paravojaških oboroženih sil ali z njihovo dejansko uporabo. Bistveno pri tem je, da gre za grožnjo z uporabo ali dejansko uporabo orožja vojaških ali paravojaških institucij ali oseb. Grozi lahko država (oziroma pripadajoča vojaška ali paravojaška oborožena sila) ali militantna nedržavna organizacija.

2.1.1 Indikatorji konvencionalnih groženj

Zelo pomemben dejavnik pri razumevanju ogrožanj in njihove povezanosti pri ugotavljanju hibridnosti so indikatorji konvencionalnih groženj, ki nam osvetlijo snov, ki jo preučujemo. Predstavljeni indikatorji (povzeti po Prezelj in drugi 2007, 182) nam nakazujejo močno povezanost z nekonvencionalnimi grožnjami, ki jih bomo obdelali pozneje. Temeljni indikatorji so:

- Demonstracija vojaške sile oziroma moči, kar vključuje parade, premike enot, koncentracijo ali grupiranje sil.
- Sklepanje ofenzivnih vojaških zavezništev.
- Nespoštovanje mednarodnih varnostnih pogodb.
- Povečana sovražna vojaška dejavnost, ki vključuje vojaške vaje, vojaške aktivnosti v obmejnem pasu oziroma koncentracijo vojaških enot, vojaške kršitve meje na kopnem, zraku in morju─obmejni incidenti, povečana vojaška obveščevalna dejavnost.
- Sovražne izjave visokih predstavnikov držav z implicitno vojaško grožnjo (vključno s komentarji novinarjev in akademikov).
- Informacijska oziroma psihološka vojna.
- Povečano oboroževanje (nakupi orožja, proizvodnja, kar se še posebej nanaša na število kosov orožja in vrsto, pri čemer je poudarek na ofenzivnem orožju).
- Povečanje obrambnih izdatkov oziroma proračuna.
- Povečanje strateških rezerv (za potrebe varnostnih sil).
- Mobilizacija vojske (delna, popolna).
- Prekinitev meddržavnega sodelovanja.
- Širjenje vojaškoindustrijskega kompleksa (vključuje tudi vlaganje sredstev v proizvodne zmogljivosti za orožje za množično uničevanje).

- Operativna podpora sovražnih skupin znotraj države.
- Vojaška agresija z omejenim ali radikalnim ciljem (tudi na sporna področja).

Pri omenjenih indikatorjih izstopa informacijska (psihološka vojna), ki po našem mnenju ne spada v indikatorje konvencionalnih groženj. Prezelj (in drugi 2007) navede, da je bilo tovrstno ogrožanje zaznano pred, med in po izvedbi ogrožajočih vojaških operativnih ukrepov pri pregledu preteklih mednarodnih konfliktov. S tem se lahko strinjamo, vendar bomo ta indikator v njegovi izvirni obliki uvrstili med indikatorje nekonvencionalnega ogrožanja.

2.2 Nekonvencionalne grožnje

Nekonvencionalen navadno pomeni biti izven običajnega ali pa izven zavez, konvencij. Da grožnji pripišemo nekonvencionalnost mora izpolniti pogoje redkosti, nerazširjenosti in biti v nasprotju s prevladujočimi družbenimi pravili in normami. Nekonvencionalno lahko postane konvencionalno, ko se spremenijo okvirni pogoji (Eikenberry 2014, 1).

Ameriško ministrstvo za obrambo je leta 2014 izdelalo pregled obrambnih zmogljivosti (Defense Review-QDR). V poročilu je razširilo kategorije nekonvencionalnih groženj v prihodnjem varnostnem okolju. Med nekonvencionalne grožnje je uvrstilo teroristične organizacije, kriminalna omrežja (predvsem trgovanje z narkotiki), piratstvo, orožje za množično uničevanje in uporabo smrtonosnih bioloških sredstev. Poleg tega je QDR opredelil različne multiplicirane grožnje kot so negativni vpliv podnebnih sprememb, nadzor nad izkoriščanje naravnih virov, vladni nadzor nad urbanizacijo, širjenje naprednih tehnologij in ranljivost vojske in gospodarstva ZDA na področjih, kot sta vesolje in kibernetski prostor.

Nekonvencionalne grožnje bomo obravnavali skozi prizmo asimetričnosti, posebej bomo izpostavili kibernetske grožnje. Za asimetrične grožnje bomo ugotovili, da je novost večinoma v samem poimenovanju »asimetrije«, sama narava groženj pa seže daleč nazaj v zgodovino.

Liang in Xiangusi sta že leta 1999 zapisala v poglavju Vojaško, transvojaško in nevojaško, da lahko različne tipe in metode operacij kombiniramo, da dobimo povsem novo metodo operacije (Liang in Xiangusi 1999, 123).

Pri obravnavanju asimetričnih groženj se nam pri teoretskem preučevanju pri mnogih avtorjih pojem začne pojavljati vzporedno s hibridnimi grožnjami in asimetrično vojskovanje s hibridnim. Tu bo treba narediti ločnico in predvsem pojem grožnja ločiti od pojma vojskovanje, kar smo naredili v 2. poglavju, ko smo uporabili Kotnikovo razlago.

Osredotočili se bomo tudi na novejše grožnje. Kibernetske grožnje lahko uvrstimo med nekonvencionalne asimetrične grožnje, glede na tehnološko novost so v tej nalogi primerne za izpostavljeno. Glede na Eikenberryjevo (2014) definicijo nekonvencionalnosti se prav kibernetske grožnje spogledujejo s konvencionalnostjo. Ko bomo preučevali hibridne grožnje in hibridno vojskovanje, bomo ugotovili, da je informacijsko komunikacijska tehnologija (IKT) pomembnejši subjekt pri obravnavi hibridnega ogrožanja, saj je lahko osnovno orodje za prenašanje hibridnih groženj, orožje za kibernetsko napadanje in na drugi strani je lahko pomembni obrambni steber za odvračanje ne le kibernetskih, ampak tudi ostalih ogrožanj, ki jih združujemo v hibridne. Vsekakor je IKT predvsem pomembna za prepoznavanje indikatorjev celotnega spektra hibridnega ogrožanja, ki ga bomo v nalogi raziskali. Na kompleksnost opozarja tudi Svete (2016, 98), ki pravi, da je razvoj IKT privedel do omrežene družbe. V nadaljevanju Svete (2016, 99) opozori na transparentnost, ki daje omreženi družbi moč zaznamovanja oblik, sredstev in zmogljivosti, s katerimi sodobne države in ostali globalni akterji, ki so neodvisni od države, dosegajo svoje cilje v globalnem prostoru.

Na osnovi preučene teorije nekonvencionalnega ogrožanja bomo izpostavili indikatorje, ki jim za uporabo v modelu dodamo še indikatorje kibernetskih groženj.

Asimetrične grožnje so posledica iskanja poti šibkejših z namenom spoprijeti se z močnejšim. Svete (in drugi 2010, 247) ugotavlja, da opredeljevanje asimetričnih groženj in virov ogrožanja z namenom prizadeti tehnološko razvite in velike sile terminološko in kontekstualno ni nov pojav, ampak da je zgodovinsko primerljiv. Se pa strinjajo, da je asimetrično ogrožanje onstran pričakovanj varnostnih mehanizmov nasprotnika.

Prezelj (in drugi 2007) ugotavlja kako so različna ogrožanja tesno linearno, nelinearno in transnacionalno povezana. Potem navede, da lahko povišanje stopnje nevojaških ogrožanj, kot so migracije, ekonomsko ogrožanje, zdravstveno in informacijsko ogrožanje, stopnjevanje kriminala, porast terorizma vpliva na intenzivnost vojaškega ogrožanja.

V tem podpoglavju se srečamo s prehajanjem pojmov in problematiko razmejitve med njimi. Vegič (2016, 77) naleti na koncept hibridno in asimetrično ter ugotovi, da je predvsem zaradi še vedno pomanjkljive konceptualizacije termina hibridno težko postaviti ločnico med obema pojmoma. Potem Vegič navede Sveteta (in druge, 2010), da asimetrijo razume podobno kot Lonsdale (2008), delovanje, organiziranje in razmišljanje, ki je drugačno od nasprotnikovega in ima za cilj maksimizirati relativno moč, izkoristiti nasprotnikovo šibkost in si pridobiti večjo svobodo delovanja. Vendar opozarja, da se ta ne nanaša le na merljive in materialistične kazalce moči, temveč tudi na neprimerljivost sodelujočih v konfliktih, ki se kaže pri uporabi sredstev in metod.

Pojem asimetrija v vojaškem smislu se prvič pojavi leta 1997 v reviji Quadrennial Defense Review in kot smo ugotovili to ni nič novega, kot tudi niso novi ostali strateški pristopi (spopadi nizke intenzivnosti, nevojne vojaške operacije, strategija posrednega nastopanja, gverilsko vojskovanje, terorizem) (Svete in drugi 2010, 248). Dodamo lahko še specialno vojno, ki je lahko z vidika širine spektra konfrontacije kot nekonvencionalna vojna totalna vojna, ki poteka na nižjih ravneh (Žabkar 2003, 122). Med nekonvencionalne oziroma asimetrične grožnje Britovšek in Čretnik (2016) uvrščata tudi ilegalne migracije in kibernetske grožnje.

Resolucija o strategiji nacionalne varnosti Republike Slovenije (ReSNV-1) v točki Vojaške grožnje opredeljuje: »da se bodo vojaške grožnje v prihodnje odražale predvsem v obliki lokalnih in regionalnih nestabilnosti, ki lahko hitro presežejo svoj lokalni oziroma regionalni okvir…..«. Morda ni prav posrečeno, da v isti točki nadaljuje o posledicah vojn in v dokument vpelje asimetrijo in tudi hibridnost. »… kot posledica vojn, oboroženih spopadov in spopadov nizke intenzivnosti na kriznih žariščih bo naraščala verjetnost groženj asimetrične narave«. Potem opredeli, da bo bojišče prihodnosti poleg kopnega, morja in zraka obsegalo tudi kibernetsko okolje in vesolje. »V prihodnosti se nasprotniki ne bodo pojavljali samo v obliki držav, temveč tudi v različnih nedržavnih ali nadnacionalnih oblikah. Zaradi neizenačenih konvencionalnih vojaških zmogljivosti, ki jih posedujejo različni subjekti v mednarodnem varnostnem okolju, bo postala pomembna nova oblika vojaškega ogrožanja varnosti, hibridno bojevanje, ki poleg konvencionalnih vključuje tudi uporabo terorističnih, kriminalnih in drugih neregularnih oblik delovanja, informacijske tehnologije ter različnih gospodarskih in drugih sredstev.«

Potočnik (2016, 17) navede, da doktrina Nata (AAP-06 2013, 2–A–20) opredeljuje asimetrično grožnjo kot grožnjo, ki izhaja iz morebitne uporabe različnih sredstev ali metod z namenom preslepiti ali izničiti sovražnikovo moč, pri čemer izkorišča njegove slabosti za doseganje neproporcionalno pomembnega rezultata.

Žabkar (2003, 112) na osnovi primera bojevanja Združenih držav Amerike proti teroristični mreži Al Kaida po dogodkih leta 2001 izpelje naslednjo razširjeno definicijo asimetrije, v kateri izhaja iz tega, da imata konfrontirani strani različne ranljive točke, pri čemer tista stran, ki takšno točko prva odkrije pri nasprotniku in nato nanjo usmeri svoj udar, pridobi odločilno prednost.

Ne glede na to, da smo ugotovili, da je asimetričnost pri vojskovanju obstajala že davno v preteklosti, Svete (in drugi 2010, 252) zapiše, da je pri sodobnih oboroženih konfliktih pri asimetričnosti očitna njena neizjemnost in da je tako postala prevladujoče okolje, v katerem se odvijajo sodobne operacije, ki jih izvajajo oborožene sile, obveščevalne službe, zasebna

varnostna podjetja in druge varnostne strukture. Zato so konflikti po koncu hladne vojne postali bolj kompleksni kot kadar koli prej v zgodovini vojskovanja.

2.2.1 Indikatorji nekonvencionalnih groženj

Asimetričnost običajno zajema taktike in strategije nekonvencionalnega vojskovanja, šibkejši nasprotnik pa poskuša z uporabo določene strategije zmanjšati pomanjkljivosti v svojih vrstah (Ancker in drugi 2003, 18–25). Vendar pa se asimetrija ne nanaša samo na kvantitativne indikatorje temveč tudi na neprimerljivost, neenakost in različnost sodelujočih v spopadu (Svete 2002, 12).

Škerbinc (2015, 8) piše o značilnostih hibridnega vojskovanja. To, pravi, da je kombinirana uporaba konvencionalnih, specialnih, neregularnih sil in plačancev. Konvencionalne indikatorje smo že izpostavili. Asimetričnost poleg specialnih, neregularnih sil in plačancev najdemo v nadaljevanju Škerbinčeve razlage, ko izpostavi intenzivno uporabo propagande, izvajanje psiholoških operacij in zavajanj, agresivne ekonomske pritiske, ustvarjanje in uporabo »petokolonašev«, ofenzivno kibernetsko delovanje, prevrate, ustvarjanje in izkoriščanje družbenih kriz, državne udare, teroristične akcije, gverilo, akcije prikrivanja in prebega.

Gologranc (2015) pri preučevanju razmerja šibki/močnejši med akterji asimetričnosti izpostavi pet faktorjev, in sicer so to vojaški, politični, mednarodni, ekonomski in informacijsko komunikacijski. Vojaški nas pri določanju indikatorjev asimetričnih groženj ne zanima. Izpostavimo pa lahko indikatorje ostalih štirih faktorjev, ki jih Gologranc obdela. Indikatorji, kot so politični cilji in interesi, podpora ljudstva, vrsta političnega režima, zavezniki, mednarodno pravo, ekonomske sankcije, ekonomska moč, psihološko vojskovanje in IKT.

Med asimetrične indikatorje bomo uvrstili tudi »ekonomsko bojevanje«. Kopač (in drugi 2007) navede več avtorjev, ki ga utemeljujejo kot sredstvo za doseganje nacionalnih interesov. Kopač (in drugi 2007, 60) izpostavi, da ekonomsko bojevanje zajema postopke za slabljenje in motenje nasprotnikovega gospodarstva. Indikatorje lahko po Kopaču (in drugih 2007, 62) opredelimo kot ekonomsko varnost prebivalstva, notranjo stabilnost države, razvojno uspešnost države, izpostavljenost ekonomskemu bojevanju, stopnjo vključenosti v mednarodne ekonomske odnose in zunanjo stabilnost, prosperiteto in stabilnost mednarodnega okolja. Omenit velja povezanost notranjega slabenja gospodarstva zaradi domačih menedžerjev, ki se jih preganja kot gospodarski kriminal.

Prezelj (in drugi 2007, 88) izpostavi indikatorje terorističnega ogrožanja in kot odraz števila terorističnih napadov, števila žrtev terorističnih napadov, števila groženj terorističnih napadov ter delujoče teroristične in ekstremistične skupine na območju neke države.

Že omenjeni organizirani kriminal obdelata Meško in Dobovšek (in drugi 2007, 119) in predlagata naslednje indikatorje organizirane kriminalitete, ki izhajajo iz kaznivih dejanj: umor, huda telesna poškodba, protipravni odvzem prostosti, ugrabitev, zvodništvo, neupravičena proizvodnja in promet z mamili, odvzem motornega vozila, izsiljevanje, ponarejanje denarja, pranje denarja, tihotapstvo, dajanje podkupnin in hudodelsko združevanje.

Že omenjena Liang in Xiangusi v svoji knjigi Unrestricted warfare navedeta različne vrste vojskovanja, ki jih lahko razumemo tudi kot indikatorje. Omenita atomsko vojskovanje, diplomatsko vojskovanje, mrežno vojskovanje, poslovno vojskovanje, bio-kemično vojskovanje, obveščevalno vojskovanje, vojskovanje za surovine, ekološko vojskovanje, psihološko vojskovaje, ekonomsko vojskovaje, vesoljsko vojskovanje, taktično vojskovanje, regularno vojskovanje, elektronsko vojskovanje, tihotapsko vojskovanje, sankcijsko vojskovanje, gverilsko vojskovanje, narkotično vojskovanje, medijsko vojskovanje, teroristično vojskovanje, virtualno vojskovanje (odvračanje) in ideološko vojskovanje (Liang in Xiangusi 1999, 123).

Izpostavimo še indikatorje migracijskega ogrožanja kot jih vidi Kopač (in drugi 2007). Regularne migracije izpostavi z indikatorjem migracijskega gibanja oziroma selitvenega prirasta prebivalstva. Najprimernejši indikator za ilegalne migracije je količinski glede na število ljudi, ki so nezakonito prestopili mejo določene države. Kopač izpostavi še prisilne migracije, za katere je najprimernejši indikator prav tako izražen v številu beguncev v določeni državi.

2.2.2 Kibernetske grožnje

V današnji informacijski dobi je delovanje informacijskega sistema za državo in družbo ključnega pomena. Že omenjena ReSNV-1 grožnje opredeljuje zaradi odvisnosti od neprekinjenega in zanesljivega delovanja informacijskih sistemov. Širitev različnih oblik kibernetske kriminalitete, kibernetskega vojskovanja/informacijskega bojevanja in kibernetskega terorizma, zlasti kibernetskih vdorov in napadov državnih in nedržavnih subjektov, ki jih prostorsko in časovno ne bo mogoče omejiti. Opredeljuje tudi odzive na kibernetske grožnje in zlorabo informacijskih tehnologij in sistemov z nacionalno strategijo odzivanja, v katero bosta v največji možni meri vključena javni in zasebni sektor. Predvideva ustanovitev nacionalnega koordinacijskega organa za kibernetsko varnost (CERT). Opredeljuje tudi dejavnosti na področju interneta in kako omejiti širjenje nelegalnih vsebin, kot so: poveličevanje, opravičevanje ali vzpodbujanje terorizma, širjenje rasne in verske nestrpnosti

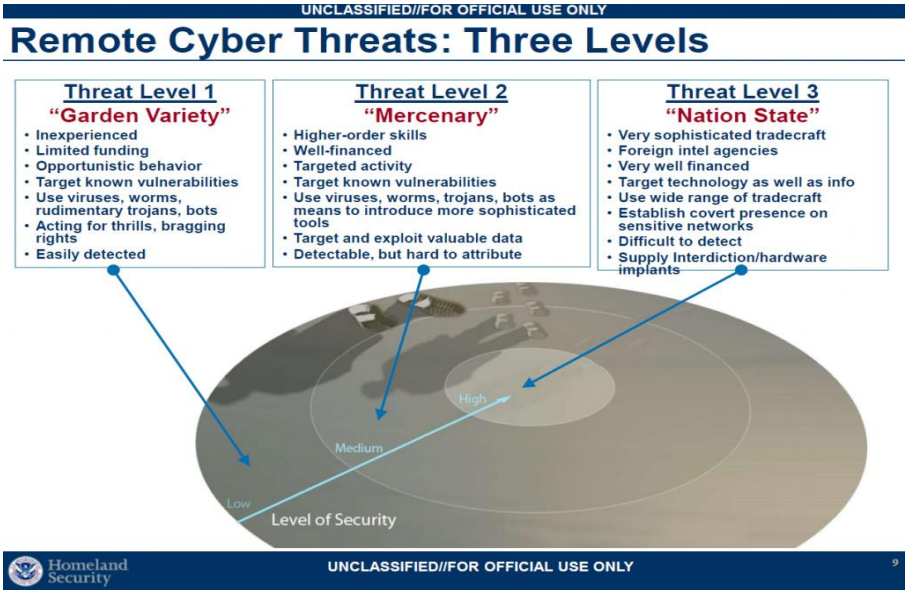
ter ksenofobije, z zlorabo izdelovanje eksploziva in z izdelava in razširjanje gradiva, ki prikazuje spolne zlorabe otrok.

Pomembno je poudariti, da je medresorska delovna skupina za pripravo strategije kibernetske varnosti oblikovala predlog, po katerem vlogo Nacionalnega organa za kibernetsko varnost prevzame Urad Vlade RS za varovanje tajnih podatkov. Ta predlog je na svoji seji potrdil tudi Strateški svet Sveta za razvoj informatike. Na 116 seji Vlade RS, dne 5. januarja 2017, je Vlada RS določila, da Urad Vlade RS za varovanje tajnih podatkov, najpozneje do 31. januarja 2017 pripravi pravno podlago, ki bo osnova za prevzem pristojnosti Nacionalnega organa za kibernetsko varnost in jo posreduje v potrditev Vladi. To odločitev je vlada sprejela po sprejetju Strategije kibernetske varnosti dne 25. februarja 2016. Ta med ukrepi na strateški ravni predvideva vzpostavitev nacionalnega organa za kibernetsko varnost (v strategiji opredeljenega kot osrednja koordinacija ali CERT). Vlada RS je na svoji 129. redni seji dne 6. aprila 2017 sprejela sklep o dopolnitvi Sklepa o ustanovitvi, nalogah in organizaciji Urada Vlade RS za varovanje tajnih podatkov. S tem sklepom je določila strokovne naloge in organizacijo UVTP-ja na področju kibernetske varnosti.

Bratuša (2011, 26) navede, da kitajska vojaška stratega Qiao Liang in Wang Xiangsui (1999) prva omenjata asimetrično kibernetsko bojevanje. V knjigi avtorja opišeta načine, kako lahko Kitajska z uporabo kibernetskega bojevanja in ostalih taktik asimetričnega bojevanja konkurira vojaško močnejšim državam, kot so evropske države in ZDA. Babič (2016) dodaja, da se kibernetske grožnje kažejo kot orožje držav v asimetričnem bojevanju, v hekerskih napadih, kot tehnološko vohunstvo, kibernetska minska polja in mreže vohunskih (računalniško-informacijskih) postaj.

Prezelj (v Malešič 2002, 59) zaznava kompleksnost sodobnega ogrožanja varnosti, na to vplivajo intenzivnost informatizacije, povezovalni procesi globalizacije, nastajanje novih držav po hladni vojni in tudi razvoj človekove zavesti. S pojavom novih tehnologij, ki so poleg komuniciranja omogočile tudi opravljanje vsakodnevnih nalog v kibernetskem prostoru, so se istočasno pojavile tudi nevarnosti oziroma grožnje pri uporabi teh orodij. Trije stebri kibernetskih groženj, kot jih razumejo v ZDA, so predstavljeni v izvorni obliki (glej sliko 2.4).

Slika 2.4: Stebri kibernetskih groženj



Vir: DHS Office of Intelligence and Analysis, Domestic Threat Analysis Division (DTA) (2009, 9).

Raziskovalci so v sklopu RAND-a (Research and development corporation) že pred petnajstimi leti pripravili nekaj črnih scenarijev glede kibernetskega prostora in s tem povezanih varnostnih groženj tako za posameznega uporabnika, organizacijo in družbo kot celoto. V nadaljevanju so naštete tiste, ki so se dejansko že zgodile oziroma se vidijo njihovi zametki.

Povzeto po The Future of the Information Revolution in Europe 2001, 71–72:

- Povečana družbena in posameznikova odvisnost od računalnikov in komunikacijskih sistemov postavi te sisteme v vlogo specifičnih tarč za napade.
- Povečan obseg zbranih podatkov glede nakupovalnih navad, vzorcev uporabe mobilnih naprav, gibanja, nakupov s kreditnimi karticami itd. občutno zmanjšuje raven naše zasebnosti.
- Strojna in programska oprema postane samo replicirajoča in povzroči verižno reakcijo, ki je neobvladljiva.
- Naraščajoča odvisnost razvitega sveta od računalnikov in komunikacijske tehnologije ustvari asimetrijo varnostnih groženj v primerjavi z drugimi regijami in kulturami. Postanemo bistveno bolj ranljivi od tradicionalnih družb.
- Naraščajoča kompleksnost omrežij pripelje do katastrofalnih prekinitev v delovanju informacijskih sistemov in tudi največji strokovnjaki s področja IKT teh težav in napak ne razumejo.

Gorman in Carr (v Dokl, 2012) ugotavljata, da se kibernetskih groženj še vedno ne zavedamo dovolj. Bistvena težava je v tem, da se še vedno ne zavedamo, da imajo kibernetske grožnje zaradi uporabe IKT izreden vpliv na ostale segmente. Posledice kibernetskih groženj je treba preučevati tudi iz psiho-socialnega vidika, ne pa samo iz materialnega. Napad na večjo ustanovno – organizacijo, ki je bistvenega pomena za varnost in stabilnost (državno ali gospodarsko) družbe, lahko zamaje ugled celotne ureditve in stabilnost sistema. Ključna infrastruktura ni samo v lasti države, temveč je velik delež v zasebni lasti. Na primer v ZDA je kar 80 odstotkov ključne infrastrukture v zasebni lasti. Evropska komisija v predlogu koncepta kibernetske obrambe na osnovi svojih raziskav ugotavlja, da je za 95 odstotkov vseh incidentov na področju kibernetske varnosti kriv človeški faktor oziroma človeška napaka. Zaradi navedenega je še toliko pomembnejša ozaveščenost uporabnikov, kar imenujemo »kibernetska higiena«, hkrati pa je treba imeti ozko specialistično usposobljen kader s področja kibernetske varnosti, ki ga je treba nenehno uriti z vajami in izobraževati.
Kibernetske grožnje različni avtorji razlagajo na različne načine. V osnovi pa lahko kibernetske grožnje razdelimo na dva dela, na namerne in nenamerne.

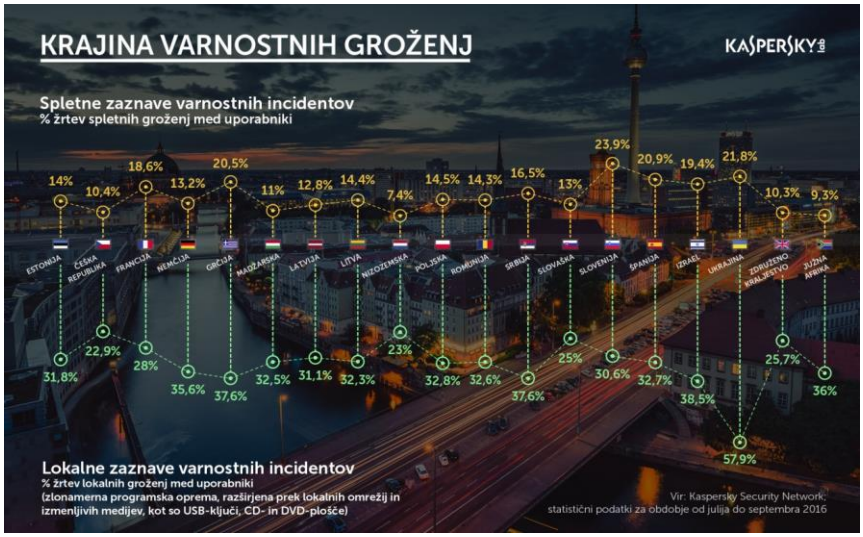
Dunn (2005) kibernetske grožnje v primeru namernih dejanj razdeli po naravi na dva različna pola in z njimi povezana scenarija.

- Nestrukturirane kibernetske grožnje so naključne in relativno omejene. Bistvo nestrukturiranih groženj je delovanje nasprotnika z omejenimi sredstvi in te grožnje so praviloma kratkoročno usmerjene. Izvajalci imajo omejena finančna sredstva, orodja, znanje, veščine in tehnološke pripomočke. Nestrukturirane kibernetske grožnje ne morejo ogroziti državne varnosti oziroma kritične informacijske infrastrukture, lahko pa takšni napadi povzročijo precejšnjo škodo.
- Strukturirane kibernetske grožnje so znatno bolj metodične, organizirane in bolje podprte z vsemi resursi. V to raven kibernetskih groženj spadajo tuje obveščevalne službe, kriminalna dejanja, gospodarsko vohunjenje, kibernetsko vojskovanje/informacijsko bojevanje, kibernetski terorizem in vključenost profesionalnih hekerjev.

Po podatkih Kaspersky Security Network (glej sliko 2.5) za obdobje od julija do septembra 2016 je po številu uporabnikov, ki so se soočili z lokalnimi varnostnimi incidenti, na prvem mestu Ukrajina (57,9 odstotka uporabnikov), sledijo ji Izrael (38,5 odstotka) ter Srbija in Grčija

(vsaka s 37,6 odstotka). Zaskrbljujoče pa je dejstvo, da ima najvišje število spletnih varnostnih incidentov Slovenija (23,9 odstotka), sledijo Ukrajina (21,8 odstotka) ter Španija in Grčija.

Slika 2.5: Analiza krajina varnostnih groženj s statistiko spletne in lokalne zaznave varnostnih incidentov 2016



Vir: Kaspersky (2016).

Vendar pa se moramo pri tej analizi zavedati, da jo je naredilo eno največjih podjetij na svetu, ki se ukvarja z izdelavo varnostnih programov za zaščito IKT in ima torej poslovni interes za prikazati čim večjo ogroženost IKT.

2.2.3 Indikatorji kibernetskih groženj

Indikatorje kibernetskih groženj bomo povzeli po Svetetu (in drugih 2007), ki (glej sliko 2.6) prikaže antropogene indikatorje glede na namen in uporabljena sredstva, in jih dopolnili glede na teorijo predelanih vsebin. Vsekakor je turbolentnost tako samih groženj kot z njimi povezanih indikatorjev v kibernetskem svetu visoka glede na »svetlobni« razvoj IKT in s tem samega kibernetskega prostora.

Slika 2.6: Antropogeni indikatorji ogrožanja informacijske varnosti

VIR	NAMEN	INDIKATORJI
Hekerji, krekerji	Izziv, ego, uporništvo	hacking, sistemski vdori, neavtorizirani vstopi v sistem

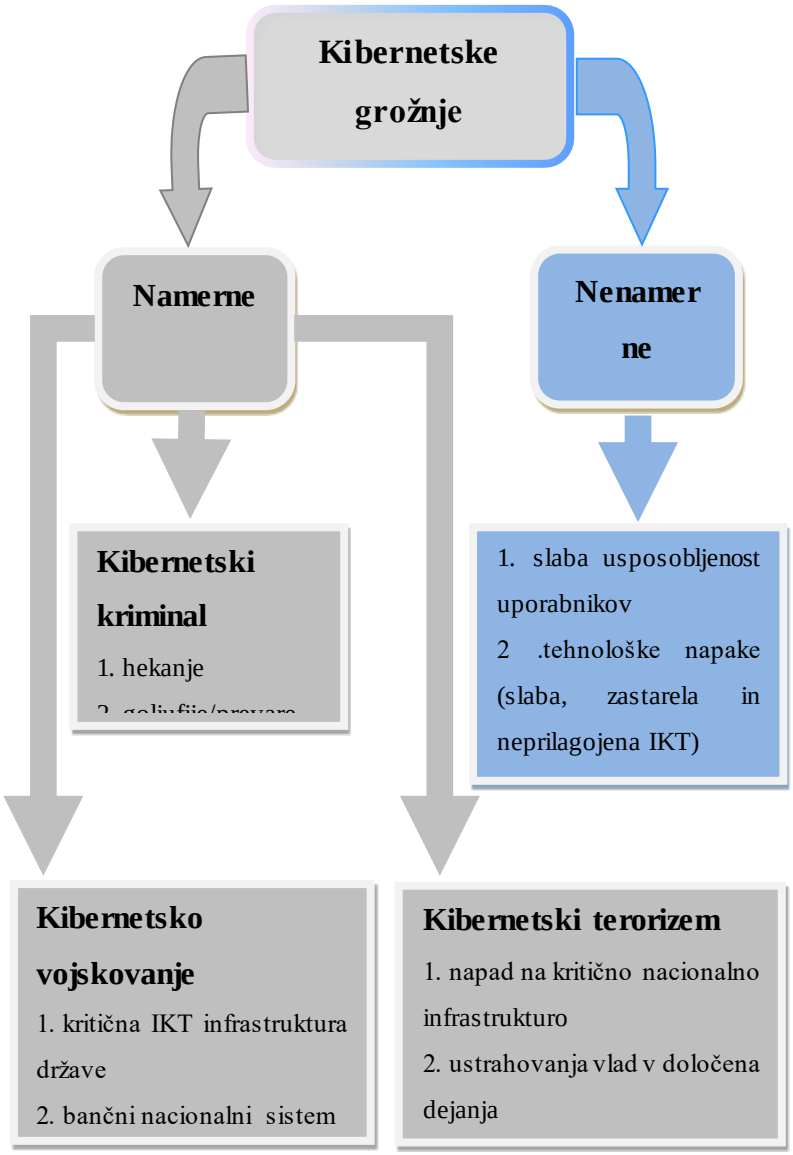
Računalniški kriminal	Uničevanje informacij, pridobitništvo, (finančno) neavtorizirano spreminjanje podatkov	Računalniški kriminal, prevare, informacijsko podkupovanje, »spoofig«, sistemski vdor
Terorizem	Izsiljevanje, uničevanje podatkov, izkoriščanje, maščevanje	Informacijsko bojevanje, sistemski napad (denial of service), vdori v sisteme, nepooblaščeno spreminjanje sistemov
Industrijsko vohunjenje (družbe, tuje vlade, drugi vladni interesi)	Konkurenčna prednost, ekonomsko vohunjenje	Ekonomsko izkoriščanje, kraja podatkov─informacij, vdori oziroma kršitve zasebnosti, vdori v sistem, nepooblaščeni dostopi v sistem (do zaupnih podatkov, zakonsko zaščitenih in/ali tehnološko povezanih informacij
Insajderji oziroma zaposleni (slabo izobraženi, nepazljivi, nepošteni, zahrbtni, odpuščeni)	Radovednost, ego, obveščevalna dejavnost, finančna korist, maščevanje, namerne napake pri vnosu podatkov, programske napake	Napad na zaposlene, izsiljevanje, brskanje po zasebnih podatkih, zloraba računalnikov, prevara in kraja, informacijsko podkupovanje, vnos ponarejenih─uničenih podatkov, prisluškovanje, zahrbtna koda (virusi, logične bombe, trojanski konji), prodaja osebnih podatkov, sistemske napake oziroma hrošči, vdor v sisteme, sistemska sabotaža, nepooblaščeni vstop v sistem

Vir: Svete (2007, 36).

To je načelna delitev pojavnih oblik kibernetskih groženj (glej sliko 2.7), iz katerih lahko izvlečemo dodatne antropogene indikatorje kibernetskega ogrožanja. Kibernetske grožnje in z njimi povezan razvoj orodij, metod, tehnik se vsakodnevno spreminja in dopolnjuje zaradi neverjetnega razvoja IKT. Grožnje smo ločili na namerne in nenamerne. Nenamerne imajo prav

tako negativne posledice za varnostni sistem, vendar nas ob hibridnosti in izpostavljanju indikatorjev ne zanimajo.

Slika 2.7: Diagram kibernetskih groženj



Iz diagrama (glej sliko 2.7) lahko izluščimo dodatne antropogene indikatorje kibernetskih groženj: viktimizacija, kršenje avtorskih pravic, vdori v kritično IKT infrastrukturo (bančno, zdravstveno, sodno, obrambno), z ustrahovanjem in izrabo IKT izisliti podporo terorizmu.

2.3 Hibridne grožnje

Skozi preučeno teorijo ugotavljamo, da je hibridnost novi pojem za lažje razumevanje starih pojavov. Kljub temu bomo poskušali izluščiti teoretike, ki so se v svojih delih lotili smiselnosti uporabe pojma hibridna grožnja. Najprej bi navedli uvodne besede članka litvanskega generalmajorja Edvardasa Mažeikisa, direktorja Urada za standardizacijo v zvezi Nato.

> *Preden začnem govoriti o hibridnih grožnjah, bi vas rad vprašal: Ali so namere in metode, uporabljene za hibridno vojskovanje, nove? Ali je to nova ali stara definicija? Seveda je stara, stara je kot Zemlja in vojne na njej. Lahko omenim tipičen primer hibridnega vojskovanja še iz antičnih časov, primer trojanskega konja. Lahko omenim na primer začetek druge svetovne vojne in napad nacistov na Poljsko ali pa zimsko vojno leta 1939 s Finsko. Ali, ko so nacisti organizirali napad na lastno radijsko postajo preoblečeni v uniforme poljske vojske. Napad Sovjetske zveze na lastno mejno postojanko (štirje mrtvi, devet ranjenih) na meji s Finsko s poznejšo obsodbo Fincev za storjeno dejanje, kar je pripeljalo do spremembe vlade na Finskem (Mažeikis 2017, 5).*

Malešič in Žabkar (2016) povzameta Lanoszka in zapišeta, da uradna ameriška opredelitev hibridno grožnjo prepoznava kot vsakega nasprotnika, ki sočasno in prilagojeno uporablja mešanico konvencionalnih, neregularnih, terorističnih in kriminalnih sredstev ali dejavnosti na območju operacije, pri čemer hibridna grožnja ni ena entiteta, ampak je kombinacija državnih in nedržavnih akterjev (Lanoszka v Malešič in Žabkar 2016, 26). Definicija omejuje hibridne grožnje na območje operacije, kar morda ni prav posrečeno, saj s tem ne priznava hibridnega ogrožanja v mirnodobnem času. Priznava pa tako državne kot nedržavne akterje. Podobno razmišljajo tudi Britanci, vojskovanje je trajnostni element mednarodnega sistema, čeprav se njegov značaj spreminja skozi čas. Značilnost tega razvoja je pojav ─ nekateri trdijo, ponovni pojav ─ spojine ali hibridnih groženj. To stanje nastane, kjer se države ali nedržavni akterji odločijo, da bodo izkoristili vse načine vojskovanja s sočasno uporabo naprednega konvencionalnega orožja, neregularne taktike, terorizma in kriminala, z namenom destabilizirati obstoječi red. S tem grozijo državni in nedržavni akterji, ki imajo dostop do nekaterih sofisticiranih orožij in sistemov, običajno nastopajo skupaj z rednimi silami. Konflikti so vedno bolj značilna mešanica tradicionalne in netradicionalne taktike, decentraliziranega načrtovanja in izvedbe državnih ali nedržavnih akterjev, ki lahko uporabljajo preprosto in zapleteno tehnologijo na popolnoma nov način (Fleming 2011, 35).

Thiele (2016) pravi, da je vojskovanje kameleon in da je enaindvajseto stoletje čas dinamičnega strateškega okolja, v katerem lahko nasprotnik deluje s hibridnimi sredstvi tako na ohranjanje političnega ravnotežja kot na vojsko in s tem na celotno družbo. Agresijo s hibridnimi grožnjami lahko državni in nedržavni akterji izvajajo po celotnem spektru konvencionalne in

nekonvencionalne linije delovanja in vključijo diplomacijo, vojaško in gospodarsko razsežnost konflikta. Vsaka grožnja ima pred sabo cilj in Thiele (2016) jih povezuje s kibernetskimi, kritičnimi informacijskimi sistemi, motnjami kritičnih storitev kot so oskrba z energijo in finančnimi storitvami, s čemer se zmanjša zaupanje v državne institucije in socialno kohezijo. Zaradi omenjenega je prav javnost postala privlačna tarča (Thiele 2016, 3).

Mažeikis (2017) pri definiranju hibridne grožnje izhaja iz že znanega akterja in pravi, da mora imeti država ali nedržavni akter zmogljivosti in očitno željo, da uporabi hibridno strategijo. To storijo z aktivnostmi, ki včasih dosežejo raven prave vojaške akcije in se lahko izvajajo tudi v daljših časovnih obdobjih (Maželkis 2017, 6).

Na tem mestu se prvič srečamo s terminom hibridna strategija. Če definiramo strategijo kot načrt ciljev, podciljev in nalog za uresničitev dodeljenega poslanstva, potem lahko hibridno vojskovanje dobi povsem novo razsežnost, ki pa ni realna.

Fleming (2011) navede, da je značilnost hibridnih ogrožanj decentralizirano poveljevanje in kontrola, razpršene vojaške in nevojaške aktivnosti, kombinacija tradicionalnih, neregularnih, terorističnih in razrvanih kriminalnih metod. S Flemingom se lahko strinjamo in potem poskušamo ugotoviti, ali lahko govorimo o hibridnosti, ko je ta zapisana. Ali lahko govorimo o doktrinarnosti? Ko govorimo o hibridnih grožnjah, govorimo o vsem, ki državi s pomočjo regularnih in neregularnih sil, kriminalnih združb, (ki so predvsem v državah z visoko stopnjo koruptivnosti), podjetij, (ki so zdavnaj prerasla nacionalne okvirje) ali terorističnih organizacij pomagajo, da vpliva na drugo državo s ciljem, spremembe družbenega reda, z ozemeljskim ciljem s ciljem ekonomske osamitve in drugo. Hibridne grožnje vodijo k totalnim grožnjam. Morda pretiravamo, ko zapišemo, da je stalna napetost blokovskega spopada, ki je zaznamovala 45-letno zgodovino, dobila naslednika, ki je nedoločljiv, njegova smer ogrožanja ni le morska, kopenska ali zračna, ampak tudi virtualna in vesoljska. Če pretiravamo oziroma nas vodi misel zarote, se je grožnja s pomočjo farmacevtske industrije naselila že v fetus. Hibridno ogrožanje je stanje, ko človeka, družbo ali svet določene interesne skupine (nedoločljivih oblik in organiziranosti) držijo v stalni negotovosti. Negotovost je stanje, ki bo človeka motiviralo kot potrošnika prihodnosti, potrošnika v omreženi družbi. Zato ne moremo govoriti ne o hibridni strategiji, ne o doktrinarnih načelih hibridnega vojskovanja, zato težko govorimo o pojmu hibridna vojna. Lahko govorimo o hibridnih grožnjah, ki jih je treba identificirati in se proti njim uspešno odzvati, še preden preidejo v konvencionalni ali asimetrični konflikt in v vojno. Svete (2016) omenja Martina van Crevelda, izraelskega vojaškega teoretika, ki je že v osemdesetih letih 20. stoletja predvidel zaton konvencionalnih konfliktov med rednimi nacionalnimi oboroženimi silami držav in vzpon konfliktov nizke intenzitete z glavnimi igralci

v obliki raznih milic, kriminalnih skupin in paravojaških sil predvsem v razvijajočem se svetu. Svete (2016) potem navede, da so ta Creveldova predvidevanja napad na clausevistično pozicioniranje zahodne vojaške organizacije, saj gre predvsem za odnos med politiko in vojsko ter njeno vlogo v vojnah, ki je izrazito ločena od mirnodobnega časa. Za razliko od današnjega časa, ko je ravno obratno in vojnih napovedi ni več, sama vojska pa ob morebitnih konfliktih vse manj nalog opravli sama, ampak jih prenese na druge nacionalnovarnostne strukture ali celo na zasebna vojaška podjetja (Svete 2016, 100).

Evropska komisija se prav tako distancira od pojma hibridna vojna in zapiše, da se opredelitve hibridnih groženj razlikujejo in morajo ostati prilagodljive. Da se lahko odzovejo na njihovo spremenljivo naravo, naj bi pojem zajemal kombinacijo prisilnih in subverzivnih dejavnosti, konvencionalnih in nekonvencionalnih metod (npr. diplomatskih, vojaških, gospodarskih, tehnoloških), ki jih državni in nedržavni akterji lahko usklajeno uporabljajo za doseganje posebnih ciljev, pri čemer pa razmere ne dosežejo praga za uradno razglasitev vojne. Navadno je poudarek na izkoriščanju ranljivosti tarče in ustvarjanju dvoumnosti, da se ovirajo procesi odločanja. Obsežne dezinformativne kampanje, uporaba družbenih medijev za nadzor politične pripovedi ali za radikalizacijo, novačenje in usmerjanje posredniški akterjev so lahko sredstva za hibridne grožnje (Skupni okvir o preprečevanju hibridnih groženj – odziv Evropske unije 2016, 2).

Podobno distanco od pojma vojne je pri raziskovanju asimetričnosti zapisal Krunič (1997), ko je zavrnil pojem specialna vojna in razvil teorijo neposrednega nastopanja, ki jo države uporabljajo za reševanje konfliktov, da bi se izognile vojnemu stanju.

Ducaru (2016) se pri poglavju zgodnjega odkrivanja hibridnih groženj nekako distancira od pojma hibridna vojna in zapiše, da je posebno pozornost treba posvetiti zgodnjemu odkrivanju hibridnih groženj saj gre za poseben izziv in ni rečeno, da se bodo pretekle izkušnje v novih pogojih ponavljale. Stopnja predvidljivosti je nizka. Informacijski tokovi so predvidoma nezanesljivi (celo namenoma, kljub uporabi zavajajočih medijev, dvojnosti propagande, idr.). Nato mora biti sposoben zaznati zgodnje indikatorje razvijanja hibridnih groženj, to mora spoznati že na politični ravni in ravnati tako, da se hibridna grožnja ne razvije v vojaški konflikt, ampak da se jo zadrži na blažji ravni.

Cruceru (2014) navaja ameriška vojaška teoretika že omenjenega Franka G. Hoffmana in Jamesa N. Mattisa, ki v članku Future warefare (2005) definirata pojma hibridna grožnja in hibridna vojna. Po njunem mnenju državni in nedržavni akterji razvijajo nove kapacitete in možnosti (tehnološke kombinacije in nepričakovane taktike) za dosego strateških prednosti pri izogibanju direktne vojaške konfrontacije s silami ZDA. Gre za hibridno grožnjo, mešanico

vojaških in nevojaških virov in operacij, terorizma, gverilske taktike, kriminala in spletnih napadov, ki lahko ogrozijo varnostne interese ZDA in drugih zaveznikov.

Hibridni nasprotnik želi delovati na mnogih področjih in zbrati taktične učinke, pridobiti podporo medijev in voditi informacijske operacije z namenom spodkopati sovražnikovo voljo za nadaljevanje kompleksnih konfrontacij. Ta nov tip nasprotnika sili Američane in njihove zaveznike, da sočasno sledijo širokemu spektru groženj, da bi se lahko uspešno upirali različnim nasprotnikom med kompleksnimi in zamegljenimi spopadi na vojaškem in nevojaškem področju, kar je srž hibridne vojne (Cruceru 2014, 235).

Ni naključje, da pri poglavju hibridne grožnje v zadnjem delu navajamo utemeljitelja pojma hibridnosti v povezavi z varnostjo Franka G .Hoffmana, ki je svoje razmisleke objavil leta 2007 v delu Conflict in the 21st Century: The Rise of Hybrid Wars. V tej knjigi avtor izpostavlja da možni nasprotniki ZDA in druge sile svojo strategijo in operativni položaj nenehno prilagajajo in s tem ustvarjajo tipološko mešanico, ki jo je težko tipizirati in poraziti. Glavni izziv so državni in nedržavni akterji, ki se odločijo uporabiti taktike in tehnologije, ki najbolj ustrezajo njihovemu okolju in kulturi. Najverjetneje bodo prihodnje vojne izkoriščale razlike med nasprotniki, metodami in sredstvi za večstranske ali hibridne spopade. V času hibridnih konfrontacij bodo nasprotniki uporabljali dostop do modernih vojaških naprav, da bi podprli upornike, teroriste in kriminalne združbe, kot tudi nekatere države, ki lahko kombinirajo visokotehnološke vojaške naprave s terorističnimi akcijami in spletnimi vojaškimi operacijami, uperjenimi proti ekonomskim in finančnim tarčam (Hoffman 2007, 26).

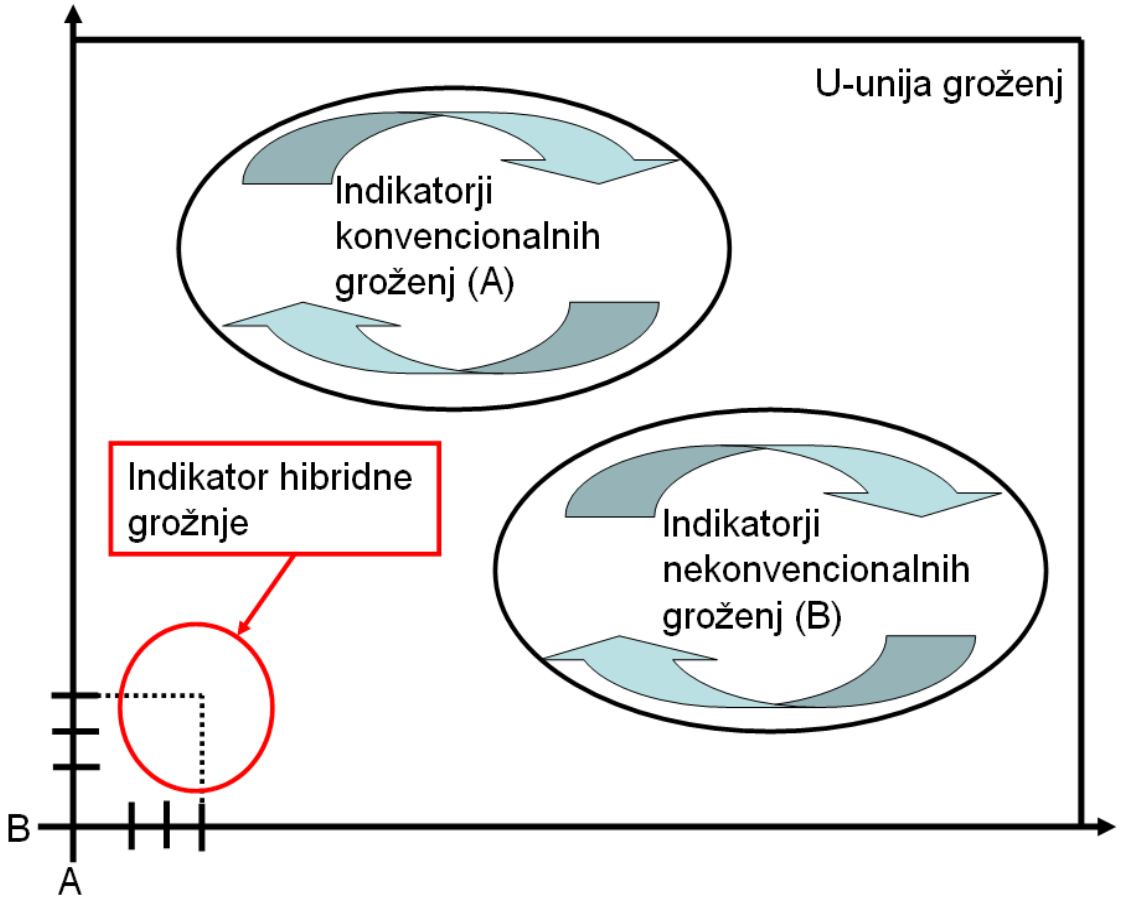
Lahko govorimo o posredniški vojni, kot nam je znana iz obdobja hladne vojne, ali o posredniškem delegiranju nalog državnih akterjev nedržavnim v okviru iste države. Lahko zapišemo, da na osnovi hibridnih groženj lahko predvidevamo različne oblike napadov na taktičnem nivoju, ki imajo tudi strateške posledice v obliki spremembe političnega sistema ali vodijo v neki družbi celo do vojnega stanja, ki pa ga ne moremo imenovati hibridna vojna. Dopuščamo možnost, da govorimo o hibridni vojni v podobnem smislu kot o hladni vojni, ki nikoli ni postala »vroča«, vendar je kljub temu bilo veliko konfliktov ali tako imenovanih posredniških vojn. Hibridna vojna je pojem, ki ga lahko uporabljamo v enakem smislu kot hladna vojna. Naj to našo tezo podkrepim z besedami Iztoka Simonitija: »postmoderni svet ni več tako lahko razložljiv in morda obvladljiv, kakor je bil prejšnji. Prejšnji interpretativni obrazci preprosto niso več uporabni. Znanost, stroka in politika so v trenutku, ko je potrebna zrelost in odločnost, da bi reagirali na številne realne vojne, vse postale nekakšne sirote hladne vojne« (Simoniti 2001, 25).

Za konec podpoglavja navedimo še tezo, ki sta jo je zapisala Richmond in Mitchel, ko sta iz hibridne vojne predlagala hibridni mir, ki naj bi bil mešanica različnih družbenih stanj konfliktnosti. V hibridnem miru je zabrisana meja med zunanjo in notranjo varnostjo, med diplomacijo in silo ter med informacijo in dezinformacijo (Richmond in Mitchel v Cigler 2016, 88). S tezo hibridni mir kot izpeljanko iz hibridne vojne v smislu pred vojnega stanja se ne moremo strinjati. Hibridni mir lahko razumemo kot stanje, ko so se prenehale konvencionalne sovražnosti in se nadaljuje hibridno ogrožanje, katerega cilj je počakati ugodnejši politični trenutek za nadaljevanje vojne, ki mora imeti tudi konvencionalno noto.

2.3.1 Indikatorji hibridnih groženj

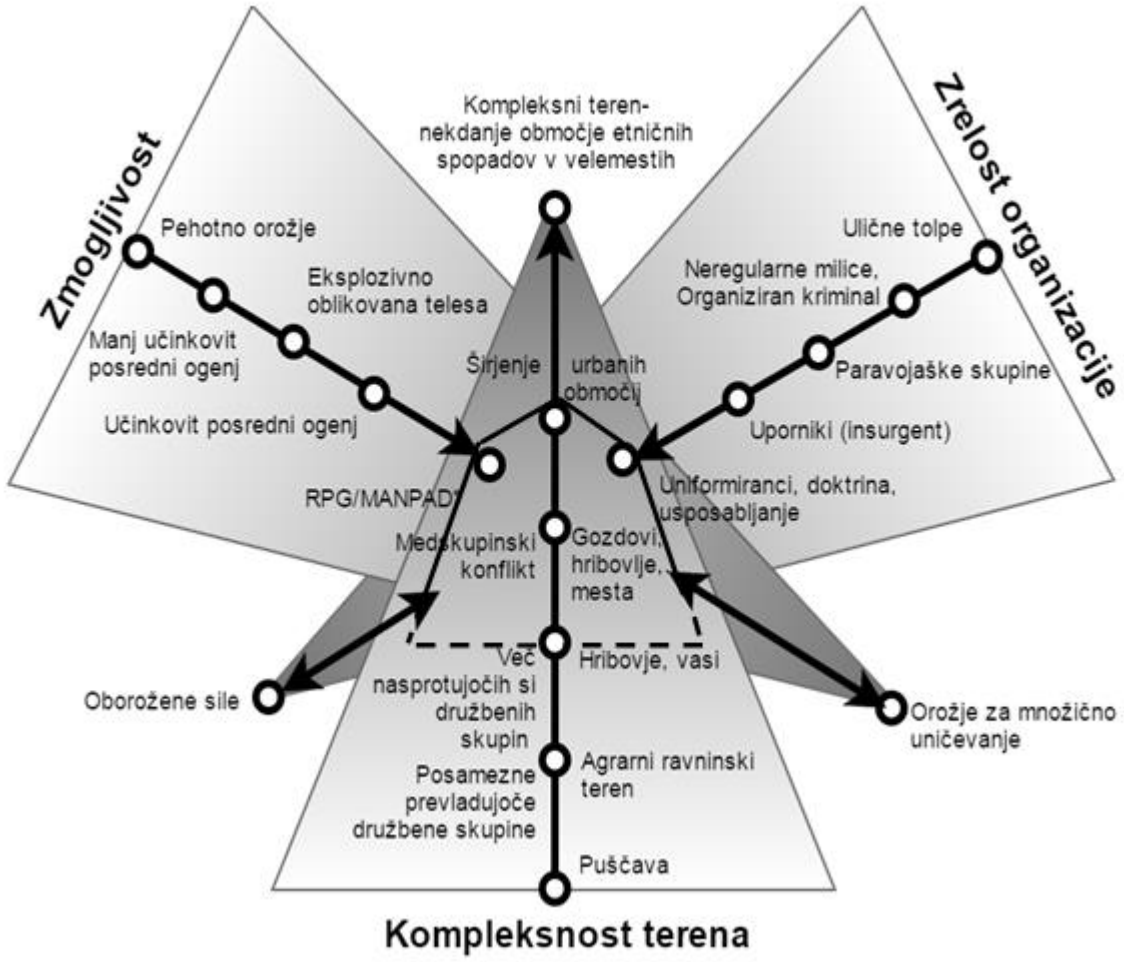
Pri določanju indikatorjev hibridnih groženj na osnovi že predelanih teoretikov in empiričnih opredelitev nekonvencionalnih indikatorjev pridemo do paradoksa. Ali lahko določimo indikatorje hibridnih groženj ali le povežemo že preučene indikatorje konvencionalnih in nekonvencionalnih groženj in jih kot celoto predstavimo kot hibridne indikatorje? Dilemo najlažje prikažemo v obliki slike (glej sliko 2.8), prikazuje nam množico indikatorjev konvencionalnih in množico indikatorjev nekonvencionalnih groženj. Obe množici skupaj nam predstavljata unijo groženj. Puščice nam ponazarjajo dinamičnost in stalnost groženj. Matematika nas uči, da za obstoj unije potrebujemo najmanj dve množici, v našem primeru množico A (konvencionalni indikatorji) in množico B (nekonvencionalni indikatorji), da dobimo unijo U (grožnje). Logični zapis unije množic: $a \in A \cup B \Leftrightarrow ((a \in A) \vee (a \in B))$. Pomen te primarne obrazložitve se kaže v dejstvu, da potrebujemo vsaj en par iz različnih množic v uniji, ki ga bomo uporabili pri modelu prepoznavanja hibridnih groženj. Da lahko izpostavimo indikatorje hibridnih groženj v uniji groženj, potrebujemo vsaj en kartezični produkt množice A in množice B, logični zapis: $A \times B = \{(a,b); a \in A \wedge b \in B\}$. Kartezični par indikatorjev je dovolj, da lahko ogrožanje poimenujemo hibridno.

Slika 2.8: Indikatorji hibridnih groženj, poenostavljeni z unijo množic in kartezičnim produktom



Indikatorje hibridnih groženj lahko poenostavimo tudi kot križišče hibridnih groženj, ki ga je razvil Bowers (2012). Grožnje nam predstavi skozi tri faktorje in sicer zmogljivost, kompleksnost terena in zrelost določenega akterja. Stičišče vseh treh faktorjev imenuje »sweet spot«, v prevodu smo to poimenovali območje hibridnega ugodja (glej sliko 2.9):

Slika 2.9: Križišče hibridnih groženj



Vir: prirejeno po Bowers (2012, 42).

*RPG (Rocket propelled grenade)/MANPAD (Man-portable air-defense system)

Pri določanju zmogljivosti se Bowers (2012) vpraša kje lahko organizacija pridobi zmogljivosti in znanje za uporabo. V več primerih je bilo videno, da so orožje, trening in vzdržnost lahko pridobljeni iz vojska tako imenovanih propadlih državah, »failed states«. Po propadu države pripadniki vojske lahko odložijo uniformo in se združijo s hitro ustanovljeno organizacijo za hibridno ogrožanje. Še naprej uporabljajo obstoječe vojaške zmogljivosti, vendar so odvezani obveznosti podpiranja izžetega državnega aparata (Bowers 2012, 41). Na enak način lahko potencialni akter pridobi orožje za množično uničevanje (WMD), ki pa ga je težko vzdrževati, razen če posredniškega akterja ne sponzorira država, najpogosteje druga.

Primernost akterja, da postane hibridni akter, Bowers (2012, 43) definira s stopnjo organiziranosti in kohezije, razvitostjo vodenja, odzivnostjo na notranje vodenje in na sponzorsko državo, s stopnjo podpore prebivalstva in s stopnjo do katere je akter predan ciljem ob učinkoviti strategiji.

Pri Bowersu opazimo, da se je pri razvijanju modela osredotočil na nedržavne akterje in morebitne posredniške nedržavne in posredniške državne akterje. Kar je razumljivo glede na dejstvo, da država z vzpostavljenimi državnimi institucijami poseduje oborožene sile, v okviru katerih ima specialne sile, razvito infrastrukturo na področju IKT, zmožnosti ekonomskega vpliva v regiji in razvito diplomatsko mrežo, s tem pa tudi vse možnosti hibridnega ogrožanja. Pomembno je omeniti ekstremne ideologije, ki v bistvu zadržujejo razvoj zrelosti hibridnega akterja. Ekstremne ideologije ovirajo akterja od primernega nivoja pragmatizma in s tem odrivajo skrbništvo države sponzorja, saj akter, ki sprejema ukaze od boga, težko uresničuje strateške cilje sponzorske države (Bowers 2012, 44).

Če na kratko obrazložimo še faktor terena po Bowersu (2012). Zanj je teren tretji faktor, ki omogoča zrelo in zmogljivo hibridno grožnjo, ki lahko doseže uspeh proti moderni vojaški organizaciji. Termin teren se uporabi v geografskem in demografskem smislu. Skoraj nazorno je, da je kompleksnost terena kritični faktor, ki onemogoča hibridnemu nasprotniku, da bi se moderni oboroženi sili uspešno uprl. Bolj je teren geografsko in demografsko enostaven, lažje se prednost moderne tehnologije, konvencionalne moči in številčnosti ljudstva izkoristi v boju proti hibridnemu akterju (Bowers 2012, 45).

Ugotovili smo, da državni akterji imajo zmožnosti hibridnega ogrožanja, vendar je pri ugotavljanju tega pomembno definirati namero. Namera državnega akterja bo predvsem glede legalnosti ostala zakrita in zato težko določljiva.

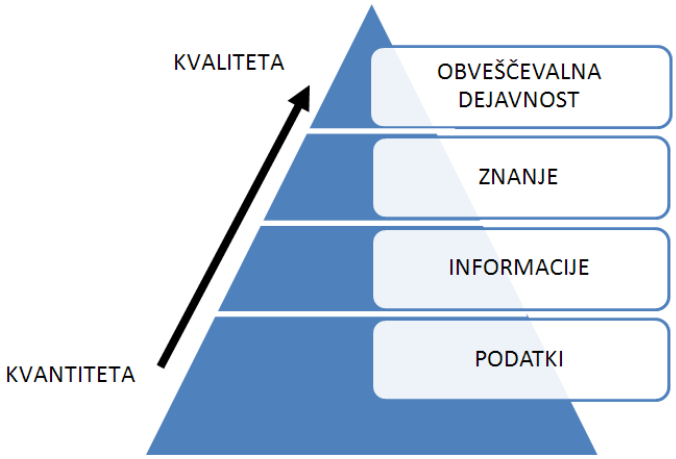
3 Informacijsko-obveščevalna razsežnost hibridnih varnostno zanimivih pojavov

V današnji omreženi družbi, virtualni družbi, družbi kjer mrgoli informacij ni več izziv pridobiti informacije ampak znati informacije diferencirati. Izluščiti prave informacije je pomembno tako v življenju vsakega posameznika, ki se mora odločiti recimo v kateri trgovini bo kupil živež za družino, kot za institucije, ki se ukvarjajo z varnostjo. Za učinkovito rabo oblikovanega modela za prepoznavanje hibridnih groženj bomo potrebovali verodostojne preverjene informacije. Zato bomo v tem poglavju obdelali pridobivanje in vrednotenje informacij. Teoretično bomo opredelili tudi organiziranost obveščevalnih služb.

3.1 Pridobivanje in vrednotenje informacij

Za lažje razumevanje bomo predstavili obveščevalno-informacijsko piramido (glej sliko 3.1).

Slika 3.1: Obveščevalno-informacijska piramida



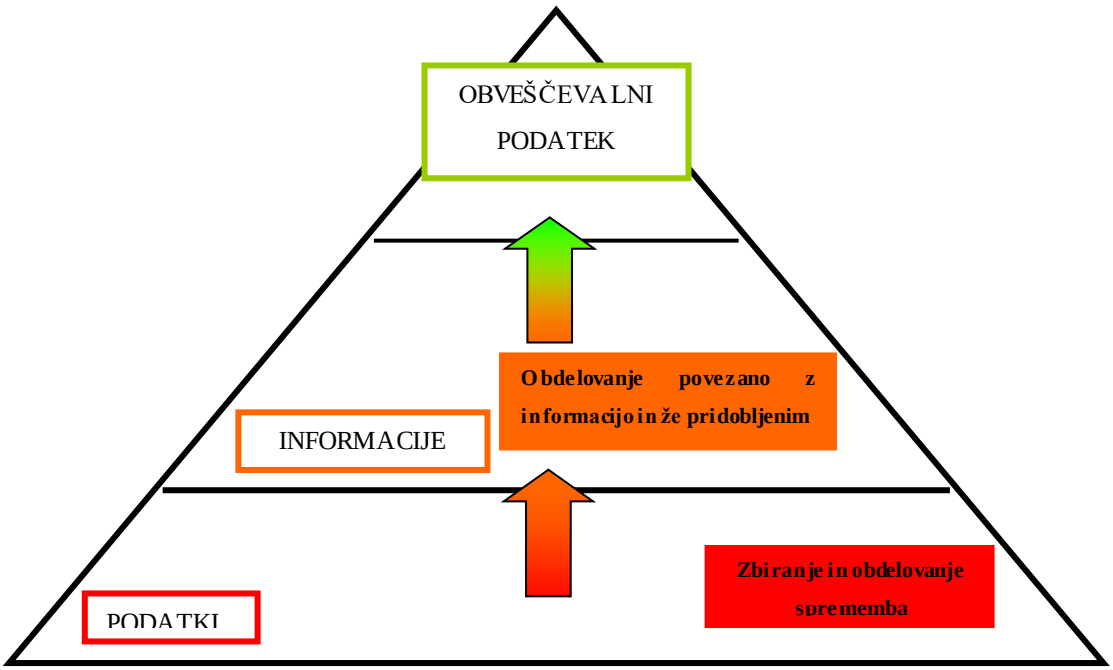
Vir: prirejeno po Jéquier in Dedier (v Črnčec 2009, 35).

Iz piramide je razvidno, da se kakovost informacij glede na količino nesorazmerno viša. Izluščene in kakovostne informacije se pridobivajo z obveščevalno dejavnostjo (ang. Intelligence). Črnčec (2009, 34) definira obveščevalno dejavnost na tri načine. Obveščevalna dejavnost se nanaša na zgornjo plast informacijske piramide, zmožnost sprejemanja ocen in koherentno prilagajanje okoliščinam. Lahko se nanaša na dejavnosti, povezane s pridobivanjem podatkov nacionalnih obveščevalnih struktur in širše (britanska uporaba) –na industrijsko podjetje ali katero koli drugo družbeno organizacijo.

Zavezniška doktrina (AJP 2.0) razloži razliko med podatkom, informacijo in obveščevalnim podatkom in sicer, da ima informacija posebno vrednost, kadar lahko iz nje izdelamo določene zaključke. To pa je lahko tudi rezultat njene povezave s kakšno drugo informacijo, ki smo jo že predhodno pridobili, ali pa povezava pridobljene informacije s predhodnimi izkušnjami. Sami po sebi imajo podatki, pridobljeni s pomočjo različnih senzorjev, manjšo uporabno vrednost. Podatki, zbrani s pomočjo senzorjev, postanejo informacije, ko so primerno predelani v ustrezen format. Informacija je sama po sebi dejstvo ali niz dejstev. Če pa jo povežemo z že znano informacijo oziroma umestimo v okvir predhodno znanih dejstev, bo nastal nov niz dejstev, ki jih imenujemo obveščevalni podatek. Obveščevalni podatek se od informacije razlikuje po tem, da nastane kot rezultat v procesu subjektivne ocene, ni popolnoma nedvoumen in je odprt za spremembe. Povezovanje enega niza informacij z drugim ali ocenjevanje informacij s primerjavo že zbranih dejstev in informacij v bazah podatkov ter ugotovitvami, ki

jih izdela analitik, so vrh v izdelavi obveščevalnih podatkov iz informacij. Razmerje med podatki, informacijami in obveščevalnimi podatki je prikazano na sliki (glej sliko 3.2), ki za osnovo uporabi že prikazano obveščevalno-informacijsko piramido.

Slika 3.2: Razmerje med informacijo in obveščevalnim podatkom



Vir: prirejeno po (AJP 2.0, 2003, 26).

Slika 3.2 nam nazorno prikaže (sistem semaforja od rdeče prek oranžne v zeleno), kako množica podatkov z obdelavo prehaja v informacijo. Z nadaljnjo analizo in primerjavo z že pridobljenimi informacijami preide v analiziran in ovrednoten obveščevalni podatek. Obveščevalni podatek je material, ki ga lahko uporabimo za ocenjevanje ogrožanja.

Črnčec (2009, 35) nam potrjuje hibridnost okolja tudi v obveščevalni dejavnosti, saj zapiše, da bolj ko postaja družba kompleksna, večje so potrebe po obveščevalni dejavnosti v javnem in zasebnem sektorju, na ravni nacionalnih obveščevalnih služb, mednarodnih korporacij in nacionalnih podjetij. In citira Argella: »V preteklosti je bila obveščevalna dejavnost v pristojnosti države. V večjih industrializiranih državah se razmere spreminjajo, ker multinacionalke in nacionalne korporacije delujejo na obveščevalnem področju na isti ravni kot državne institucije« (Agrell v Črnčec 2009, 35).

V nadaljevanju bomo predstavili še senzorje, s katerimi lahko pridobivamo podatke. V samo uporabo senzorjev predvsem z vidika legalnosti se za potrebe te naloge ne bomo spuščali.

Podatki se zbirajo s pomočjo virov, lahko jim rečemo tudi senzorjev. Vire združujemo v zvrsti pridobivanja podatkov. V angleškem jeziku temu pravimo »collection«, v slovenščini imamo daljši izraz – zbiranje podatkov v obveščevalni dejavnosti. Šaponja (1999) opredeli tri ključne discipline:

- operativne discipline (zbiranje podatkov z operativnim delom),
- tehnične discipline (zbiranje podatkov z uporabo tehničnih sredstev),
- disciplina zbiranja javno dostopnih podatkov (Šaponja 1999, 84).

Črnčec (2009) tudi navede Šaponjo (1999) in pojasni, da se operativne discipline nanašajo posredno ali neposredno na operativno delovanje. Kot primer navaja: tajno sodelovanje, tajni odkupi predmetov ali podatkov, tajno sledenje in opazovanje, tajno fotografiranje in video snemanje, tajno prisluškovanje telekomunikacijam, tajno prisluškovanje in snemanje pogovorov, nadzorovanje računalniških sistemov bank, preverjanje pisem in drugih pošiljk, delovanje pod krinko, sodelovanje s drugimi partnerskimi službami. Šaponja (1999) navede, da v okviru tehničnih disciplin s tehničnimi sistemi zbiramo podatke in discipline so ločene od operativnega dela: zbiranje podatkov s sredstvi za strateški nadzor telekomunikacij oziroma za prisluškovanje, z uporabo različnih načinov fotografiranja iz zraka ali vesolja, z uporabo različnih radarskih sistemov in naprav za merjenje različnih količin na daljavo. Opredeli tudi disciplino zbiranja javno dostopnih podatkov, zanje pravi, da jih zbirajo v manjšem obsegu, vendar že napove, da se njihov pomen v prihodnosti zaradi bliskovitega tehnološkega razvoja povečuje. Sem predvsem spada zbiranje podatkov iz elektronskih medijev, računalniških in podatkovnih omrežij, načrtno spremljanje tiska, strokovne literature in najem strokovnjakov za izdelavo različnih raziskav (Šaponja v Črnčec 2009, 89).

Združena obveščevalna doktrina (AJP 2.0) opredeli, da so informacije, predelane v obveščevalne podatke, zbrali »viri« in »agencije«. Vir zavezniška doktrina opredeli »v besedišču obveščevalne dejavnosti oseba ali stvar, od katere je mogoče pridobiti informacije«. Vir lahko zbira informacije slučajno pri klepetu v kavarni ali pa jih zbira načrtno na podlagi podrobnih zahtev, kot je na primer slikovno snemanje programirane poti poleta brezpilotnega letala. Vir je primarni izvor informacije, ki lahko poseduje informacijo ali pa njegova aktivnost nakazuje na obstoj informacije. Zbiralec je oseba ali sistem, ki prejme informacijo od vira. Edina sprememba informacije na katero lahko vpliva vir, je njena oblika. To je lahko na primer prevod iz enega jezika v drugega v primeru verbalnega zbiranja informacij ali pa pretvorba slike iz vizualne oblike v digitalni signal prek satelita. Vir nima kapacitete in zmožnosti za obdelavo informacij.

Agencija je opredeljena kot »pri obveščevalni dejavnosti organizacija ali posamezniki, ki se ukvarjajo z zbiranjem in/oziroma obdelavo podatkov«. Agencija je lahko sposobna zbirati in obdelovati informacije ali pa jih je sposobna samo zbirati in jih mora v obdelavo pošiljati neki drugi agenciji. Kot primer: na eni strani spektra ustreznih agencij so pehotne izvidniške enote, ki poročajo o dejavnostih nasprotnika na različnih lokacijah, na drugi strani pa velike vladne službe, ki prejemajo informacije od širokega kroga virov in izvajajo zelo obsežno procesiranje informacij z namenom, da izdelujejo obveščevalne podatke, ki so nacionalnega strateškega pomena.

AJP 2.0 opredeli obveščevalne vire:

Pridobivanje obveščevalnih podatkov s pomočjo zvez (SIGINT ─ Signal Intelligence) so obveščevalni podatki, pridobljeni s prestrezanjem komunikacij (COMINT ─ Communication Intelligence) in drugih elektronskih emisij (ELINT ─ Electronic Intelligence).

Pridobivanje obveščevalnih podatkov s pomočjo slikovnega materiala (IMINT ─ Imagery Intelligence) pomeni »obveščevalne podatke, pridobljene s senzorji, ki so lahko nameščeni na kopnem, morju in zraku oziroma so nameščeni na vesoljskih plovilih«.

Obveščevalna dejavnost s pomočjo človeških virov (HUMINT ─ Human Intelligence) pomeni »kategorijo obveščevalne dejavnosti, ki izhaja iz zbiranja in posredovanja informacij s pomočjo človeških virov«. HUMINT lahko dosežemo v prikritih (tajnih) ali v neprikritih operacijah. Prikrite operacije izvajajo obveščevalne agencije.

Pridobivanje podatkov s pomočjo javnih virov OSINT (Open Source Intelligence) pomeni »pridobivanje obveščevalnih podatkov iz javno dostopnih informacij kot tudi drugih informacij brez stopnje tajnosti, ki imajo omejeno javno distribucijo in dostopnost«.

Črnčec (2009) navede še FISINT (Foreign Instrumentation Signals Intelligence) zbiranje podatkov iz tujih elektromagnetnih virov. MASINT (Measurement and Signature Intelligence), ki se nanaša na pridobivanje podatkov z vsemi drugimi sredstvi, z merjenjem in odtisom, ki niso SIGINT (Črnčec 2009, 90).

Omeniti je treba še MEDINT (Medical Intelligence), ki se ukvarja predvsem z zbiranjem, analiziranjem in interpretacijo tujih zdravstvenih zmogljivosti, biološko znanstvenih in prostorskih informacij predvsem za potrebe strateškega planiranja zdravstvenih operacij, ki so tesno povezane tako z vojaškim kot civilnim sektorjem. GEOINT (Geospatial Intelligence) je analiza in vizualni prikaz geoprostorskih dejavnosti, povezanih z varnostjo. V razvoju sta tudi novejša načina pridobivanja podatkov CYBINT (Cyber Intelligence)/DNINT (Digital Network Intelligence), ki se ukvarjata s pridobivanjem podatkov iz kibernetskega prostora in SOCINT (Sociocultural Intelligence), ki se ukvarja s sistematičnim spremljanjem okolja, ljudi in družbe.

Pomemben dejavnik pri omenjeni transformaciji podatka v informacijo in obveščevalni podatek je vrednotenje tako informacije kot vira. Za namene obveščevalne dejavnosti temu pravimo ocenjevanje informacije z vidika zanesljivosti vira in verodostojnosti informacije. Ocena je ovrednotenje, kako zanesljiv je vir in kako verjetno je, da je informacija, ki prihaja od vira, točna in zanesljiva. Pridobljene informacijo ne smemo vzeti kot resnične same po sebi. Za to obstaja veliko razlogov, vključno z namernim zavajanjem, zaradi katerega informacija lahko ni zanesljiva ali popolnoma točna. Proces ocenjevanja pomeni, da je vsak del informacije ali obveščevalnega podatka posebej opredeljen z alfanumeričnimi ocenami. Z njimi določamo stopnjo zaupanja, ki jo lahko prisodimo informaciji ali obveščevalnemu podatku.
Sprejeti standardi vrednosti za ocenjevanje stopenj zanesljivosti virov in kredibilnosti informacij so navedeni v razpredelnici (glej sliko 3.3).

Slika 3.3: Vrednosti zanesljivosti in kredibilnosti informacije

Zanesljivost vira		Kredibilnost informacije	
A	Popolnoma zanesljiva	1	Potrjena s strani drugega vira
B	Po navadi zanesljiva	2	Verjetno resnična
C	Komaj zanesljiva	3	Morda resnična
D	Ne vedno zanesljiv	4	Dvomljiva
E	Nezanesljiv	5	Neverjetna
F	Zanesljivosti ni mogoče oceniti	6	Resničnosti ni mogoče presoditi

Vir: AJP 2.0 (2003, 31).

3.2 Obveščevalni sistem

Obveščevalni sistem, ki je del sistema notranje varnosti v okviru nacionalnovarnostnega sistema, smo izpostavili predvsem zaradi njegove odločilne vloge pri pridobivanju in vrednotenju informacij, ki jih potrebujemo za zaznavanje morebitne hibridne ogroženosti. Obveščevalni sistem deluje v okviru obveščevalno-varnostnih služb in Slovenske vojske. Kot smo omenili je prepotreben za pridobivanje informacij in hkrati ranljiv in dovzeten za morebitno hibridno ogrožanje, predvsem tujih obveščevalnih služb. Ostale elemente nacionalnovarnostnega sistema in njihovo izpostavljenost hibridnim grožnjam bomo obdelali v naslednjem podpoglavju.

Obveščevalni sistem je ožji pojem obveščevalne skupnosti. Črnčec (2009) pravi, da so obveščevalno-varnostne službe organizirane in oblikovane v obveščevalno-varnostni sistem ali skupnost, ki obsega predvsem obliko in način organiziranja, usklajevanja, usmerjanja in nadzorovanja obveščevalnih služb (Črnčec 2009, 39).

V tem podpoglavju se bomo orientirali na način organiziranja obveščevalnega sistema in podali tudi misli teoretika glede organizacije obveščevalnega sistema v Sloveniji, ki nam bo že nakazal okvirje, v katerih se bomo gibali ko bomo poskušali potrditi zastavljeno hipotezo.

Črnčec (2009) navaja Hadžovića, ki zapiše, da je obveščevalni sistem lahko centraliziran, decentraliziran ali integriran. Pri centralizirani ureditvi v obveščevalni dejavnosti so naloge in pristojnosti decentralizirane, zbiranje, vrednotenje in distribucija pa se izvaja centralizirano s pomočjo centralne enote. Pozitivno pri tem sistemu je trdnost vodstva, negativnost pa se kaže pri kritičnem ocenjevanju določene problematike. Prav nasprotno je v decentraliziranem sistemu, kjer vsaka enota zase načrtuje, zbira, vrednoti in posreduje obveščevalne podatke. Tak sitem je primeren za resorsko delovanje saj je v vsakem resorju druga specializirana obveščevalna služba. V tem sitemu vsaka služba oblikuje svojo oceno in se s tem izgublja celotna slika. Lahko pride tudi do tekmovalnosti, podvajanja in neracionalnosti. Tak sistem kliče po neusklajenosti in pomanjkanju usmeritev (Hadžović v Črnčec 2009, 39).

Velika nevarnost pri tem sistemu je »cirkularna« informacija. Cirkularna informacija pomeni, da različne agencije uporabljajo isti vir, od katerega se pridobi informacija. Taka informacija je v bistvu ena, potrjena pa je iz različnih virov (ki v bistvu niso različni). Za lažjo razumljivost bomo navedli primer. Vir je podal verbalno informacijo HUMINT operaterju. SIGINT enota je od istega vira prestregla signal mobilnega telefona, ko je podajal enako informacijo novinarju. Novinar je naredil prispevek, ki so ga obdelali OSINT analitiki.

Po drugi strani pa Črnčec (2009) navede, da ima lahko decentraliziran sistem tudi ogromno prednost predvsem pri kritičnem ocenjevanju in odločanju, saj ima končni odločevalec na voljo več podatkov in možnosti. Vendar Črnčec (2009) zapiše, da bi integriran sistem bil najprimernejši, saj je zasnovan na sodelovanju in usklajevanju med službami in na tak način lahko zagotavlja načela, okvire, oblike in metode obveščevalnega delovanja kot enotne obveščevalne politike (Hadžović v Črnčec 2009, 39).

Črnčec (2009) navede, da je organiziranost obveščevalnih služb v Sloveniji *sui generis* saj bi težko našli podobno v svetu. Črnčec (2009) naprej citira Anžiča: »Gre za rešitve, ki jih strokovno ne morem sprejeti. Prepričan sem, da gre za politične in ne strokovne rešitve« (Anžič v Črnčec 2009, 38). Navedimo še naslednji Anžičev citat: »Gre za politično odločitev, da ima država osrednjo obveščevalno in varnostno službo hkrati« (Anžič v Črnčec 2009, 38).

Navedena citata Anžiča smo izpostavili predvsem ob predpostavki, ki smo si jo zadali ob oblikovanju hipoteze.

Na koncu podpoglavja nakažimo še smer možne spremembe obveščevalno-varnostnega sistema, ki ga raziščeta Britovšek in Čretnik (2016). Izpostavita, da morajo majhne države, kot je Slovenija, glede na grožnje in finančne ter kadrovske omejitve slediti modelom organiziranosti obveščevalno-varnostnega sistema, ki omogočajo učinkovito in ekonomično opravljanje tako obveščevalnih kot tudi varnostnih nalog (Britovšek in Čretnik 2016, 328). Britovšek in Čretnik izdelata tri modele reorganizacije obveščevalno-varnostnega sistema. V prvem modelu predvidevata združitev obveščevalnih in varnostnih nalog s civilnega in obrambnega področja v enotno Obveščevalno-varnostno službo. Z drugim in tretjim modelom predvidevata združitev obveščevalnih nalog (z zbiranjem in analiziranjem podatkov o razmerah v tujini) v enotno Obveščevalno službo. Ker gre pri obveščevalnih nalogah za podporo tako zunanji (MZZ) kot tudi obrambni politiki (MO), bi bilo optimalno, da je služba organizirana pod Vlado RS. Drugi model predvideva prenos civilnih varnostnih nalog pod policijo oz. bi lahko bila znotraj policije ustanovljena organizacijska enota za nacionalno varnost (npr. Varnostna služba), ki bi opravljala in združevala obveščevalno-varnostne naloge (protiteroristične in protiobveščevalne naloge). Vsem trem modelom je skupna okrepitev obveščevalnega sektorja SV znotraj Generalštaba SV. Obveščevalni sektor SV bi v celoti prevzel vojaške obveščevalne naloge (spremljanje vojaških groženj, razmer na MOM, bojiščih in kriznih žariščih) in bi s svojimi ocenami in ugotovitvami redno podpiral enote, poveljnike in poveljstva SV ter ostale organe Ministrstva za obrambo. Za optimalno opravljanje nalog bi Obveščevalni sektor SV moral okrepiti analitični del in izkoristiti obveščevalne zmogljivosti, ki jih premore SV. Obveščevalni sektor SV bi s svojimi ugotovitvami in ocenami podpiral Obveščevalno-varnostno službo ali Obveščevalno službo in sodeloval z njo.

3.3 Vpliv hibridnih groženj na elemente nacionalnovarnostnega sistema

Zagotavljanje nacionalne varnosti Republike Slovenije temelji na delovanju obrambnega sistema, sistema notranje varnosti ter sistema varstva pred naravnimi in drugimi nesrečami kot podsistemov sistema nacionalne varnosti, vključuje pa tudi zunanjepolitične, gospodarske, informacijske in druge dejavnosti, ki neposredno vplivajo na nacionalno varnost (ReSNV-1).

Elementi nacionalnovarnostnega sistema, ki jih navedena resolucija navaja, so obrambni sistem, sistem notranje varnosti in sistem varstva pred naravnimi in drugimi nesrečami.

Glede hibridne ogroženosti lahko na osnovi predelanih teoretičnih vsebin ugotovimo, da sta elementa nacionalnovarnostnega sistema obrambe in notranje varnosti vsekakor lahko podvržena hibridnim grožnjam, kar pa ne moremo trditi za tretji element varstva pred naravnimi in drugimi nesrečami.

Za potrebe naloge bomo preučili tudi subjekte sistema nacionalne varnosti, ki so prav tako lahko podvrženi hibridnim grožnjam. Na najvišjem nivoju je državni zbor, kot zakonodajni organ predstavlja politično raven upravljanja sistema. Z državnim proračunom omogoča delovanje nacionalnovarnostnega sistema, določa politiko na obveščevalnem področju, zakonske okvire in dolgoročne smernice razvoja nacionalnovarnostne politike, strateške smeri zunanje obrambne, notranjevarnostne, gospodarske, obveščevalne in varnostne politike ter drugih politik. Predsednik republike je prvi in najuglednejši predstavnik države v tujini in ima v sistemu nacionalnevarnosti izjemno vlogo kot poveljnik obrambnih sil. Poleg tega je med rednimi prejemniki obveščevalnih informacij (Žirovnik 2003, 128).

Vlada republike Slovenije je nosilka izvršilne oblasti in skrbi za uresničevanje nacionalnovarnostne politike in delovanje sistema nacionalne varnosti na vseh področjih in ravneh (Žirovnik 2003, 126).

Svet za nacionalno varnost je bil ustanovljen skladno z Zakonom o vladi in deluje pri vladi. Je političnoposvetovalni organ, ki je pristojen za usklajevanje nacionalnovarnostne politike in za usmerjanje in usklajevanje dejavnosti, ki se izvajajo za uresničevanje interesov in ciljev nacionalne varnosti. Naloge SNAV so: svetuje vladi glede sprejemanja aktov in ukrepov, svetuje ministrstvom pri ukrepih in aktih ministrstev, usklajuje mnenja in ukrepe ministrstev, državnih organov in drugih organizacij. Pred obravnavo usklajuje mnenja ministrstev in drugih državnih organov glede aktov Državnega zbora Republike Slovenije, ki se nanašajo na nacionalno varnost, ugotavlja in ocenjuje varnostna tveganja, ogrožanje države ter ukrepe in usmeritve za zagotavljanje nacionalne varnosti. Vlada v SNAV imenuje: predsednika vlade (predsednik SNAV), ministre za obrambo, notranje zadeve, zunanje zadeve, finance, pravosodje in direktorja Slovenske obveščevalno-varnostne agencije. Predsednik SNAV lahko povabi k sodelovanju pri delu SNAV predsednika Državnega zbora RS, predstavnika največje opozicijske stranke ter druge ministre in strokovnjake s področja nacionalne varnosti. V vojni se SNAV preoblikuje v državni operativni štab obrambe (DOŠO), ki operativno usklajuje vojaško in civilno obrambo ter ukrepe zaščite in reševanja (Kure 2009, 31–33). SNAV že kar

nekaj časa vodi predsednik vlade, kar kaže na pomen in prednostno vlogo organa ter vprašanj, ki jih obravnava (Odlok o Svetu za nacionalno varnost, 2014).

Sekretariat SNAV (SSNAV), ki ga imenuje vlada, operativno usklajuje aktivnosti za delovanje SNAV, usklajuje izvedbo stališč in opravlja druge naloge. Strokovna in administrativno-tehnična dela za sekretariat SNAV opravlja služba, ki jo določi vlada. SSNAV sestavljajo: svetovalec predsednika vlade za nacionalno varnost (vodi sekretariat), direktor Slovenske obveščevalno-varnostne agencije (namestnik vodje), generalni sekretar vlade, generalni direktor Policije, načelnik Generalštaba Slovenske vojske, generalni direktor Obveščevalnovarnostne službe Ministrstva za obrambo, državni sekretarji, poveljnik Civilne zaščite Republike Slovenije in direktor Službe Vlade Republike Slovenije za zakonodajo. Predsednik SNAV lahko določi, da svetovalec predsednika vlade za nacionalno varnost spremlja izvrševanje odločitev vlade glede uresničevanja nacionalnih interesov in ciljev na področju nacionalne varnosti (Odlok o Svetu za nacionalno varnost, 2014).

Omeniti moramo tudi nacionalni center za krizno upravljanje (NCKU) Center deluje neprekinjeno in zagotavlja prostorske, tehnične, informacijske in telekomunikacijske pogoje za delo Vlade Republike Slovenije (v nadaljnjem besedilu: vlada) v skladu z zakonom v izrednem in vojnem stanju ter ob pojavih ali dogodkih oziroma krizah v državi oziroma v regionalnem ali strateškem okolju, ki lahko pomembno ogrozijo nacionalno varnost. Ministrstvo za obrambo zagotavlja kadrovske, materialne, prostorske, finančne in druge pogoje za delo centra (Uredba o organizaciji in delovanju NCKU, 2006).

Naloge centra so:

- zagotavlja informacijske in komunikacijske povezave za izmenjavo podatkov in informacij;
- zagotavlja informacijske in komunikacijske povezave za izmenjavo podatkov in informacij skladno s sprejetimi mednarodnimi obveznostmi države;
- zagotavlja prenos odločitev za izvajanje ukrepov za pripravljenost, povelja za izvajanje mobilizacije in drugih ukrepov, načrtovanih za odzivanje na krizne pojave in dogodke;
- opravlja naloge državnega centra upravnih zvez;
- opravlja druge naloge v skladu z navodili ministra za obrambo, ki pa ne smejo omejevati zgornjih nalog (Uredba o organizaciji in delovanju NCKU, 2006).

V NCKU deluje tudi Medresorska analitična skupina (MAS), ki jo imenuje vlada. Zagotavlja strokovno in analitično podporo vladi v izrednem in vojnem stanju ter ob krizah. Deluje v stalni ali razširjeni sestavi, odvisno od razmer. Neprekinjeno delovanje se vzpostavi, ko je potreba po celovitem spremljanju varnostnega položaja, v vojnem ali izrednem stanju in ob dogodkih ali

razmerah, ki presegajo zmožnosti enega resorja in zahtevajo usklajeno delovanje več državnih organov (Vuga-Bernšak 2016, 21).

4 Metodologija identificiranja hibridnih groženj

Kot smo v nalogi nakazali, je bistvena potreba pri identificiranju hibridnih groženj potreba po verodostojnih in preverjenih informacijah. Do uporabnih informacij pridemo s pomočjo obveščevalnih metod. Žabkar (2004) pravi, da gre pri obveščevalni metodi za fuzijo več različnih metod, kot so opazovanje, indukcija, dedukcija, analiza in sinteza.

Ob pridobitvi obveščevalnih podatkov nam predstavljeni indikatorji konvencionalnega in nekonvencionalnega ogrožanja nakažejo grožnjo, s pomočjo modela jo povežemo z akterjem in lahko predpostavimo hibridno ogroženost. Kljub predpostavki o hibridnem ogrožanju in verodostojnosti podatkov, ki so jih indikatorji zaznali, še vedno govorimo o subjektivnosti. Za objektivno razlago identificiranih hibridnih groženj bi se morali tematike lotiti s pomočjo ekspertize. Kar bi pomenilo, da se na osnovi znanih informacij pojavijo vprašanja na zapletene procese, kar samo hibridno ogrožanje je. Zato bi morali izbrati ekspertno skupino ozko specializiranih strokovnjakov. Žabkar (2004) navede, da ima taka skupina intuicijo in znanje, da na hiter način pride do skupinskega strokovnega mnenja in ocene. Ta mnenja in ocene se potem analizirajo s pomočjo statističnih in drugih znanstvenih metod. Le tako lahko pridemo do objektivne ocene oziroma do ekspertne presoje.

4.1 Model ocenjevanja hibridnih groženj

Že sam naslov poglavja vsebuje besedno zvezo ocenjevanje hibridnih groženj, kar nakazuje na dejstvo, ki ga je zapisal Prezelj (in drugi 2007), da natančno merjenje ogrožanja nacionalne varnosti ni mogoče. Gre za sklepanje, kjer lahko pride do razlike med objektivnim ogrožanjem in zaznanim ogrožanjem in ne za natančno kvantitativno merjenje (Prezelj 2007, 14).

Model bomo poenostavili s pomočjo diagrama (glej sliko 4.1), kjer se bomo osredotočili na indikatorje hibridnega ogrožanja na način kot smo ga poenostavili v podpoglavju 2.3.1 (Indikatorji hibridnega ogrožanja). Ovrednoteni obveščevalni podatek vstavimo v model. V

primeru, da kateri od indikatorjev zazna grožnjo, to grožnjo povežemo z akterjem in časovno premico. Ko se na isti časovni premici pojavita vsaj dve identificirani grožnji, ki nista iz istega indikatorskega polja (konvencionalnega ali nekonvencionalnega), lahko začnemo ocenjevati, ali identificirani akter hibridno ogroža. To pomeni, da naredimo novo entiteto, ki jo podrobneje spremljamo. Model je sestavljen iz indikatorskih polj, časovno opredeljenih vektorjev groženj, akterjev in časovne premice, ki posameznega akterja povezuje z vektorjem grožnje.
V indikatorski polji vstavimo vse identificirane indikatorje konvencionalnih in nekonvencionalnih groženj. Akterje sproti dodajamo z identificiranim legalnim ali nelegalnim nazivom. Modri vektor predstavlja posamezno identificirano grožnjo. Zelena časovna premica pomeni, da ni zaznane grožnje, oranžna, da je grožnja zaznana z enega od indikatorskih polj, rdeča pomeni hibridno ogroženost. Akterje ločimo v dve primarni skupini: državni in nedržavni akterji. Iz primarno nastavljenih entitet se lahko oblikujeta dve novi entiteti in sicer posredniške države in posredniški nedržavni akterji. V diagramu (glej sliko 4.1) vektor grožnje, ki povezuje isto grožnjo z dvema akterjema, obarvamo v črno, tako izločimo iz državnega akterja posredniškega državnega ali posredniškega nedržavnega akterja.

V nadaljnjem razvoju modela bi lahko diagram pretvorili v delujočo aplikacijo. Navedimo najenostavnejši primer povezovanja podatkov s prednastavljenimi identitetami v posameznih tabelah.
Potrebovali bi bazo podatkov (MySQL) in povezane funkcije z algoritmi za uspešno delovanje.

Baza podatkov bi vsebovala tabelo Obveščevalni podatek, kjer bi definirali dve polji z naslednjimi vnosi:

- (ID, INDIKATORSKO POLJE) vnosi v tabelo: 1 ─ konvencionalne grožnje, 2 ─ nekonvencionalne grožnje.

Druga tabela: Državni akterji bi vsebovala naslednja polja:

- (ID, DRŽAVNI AKTER) vnosi v tabelo: 1 ─ državni akterji, 2 ─ posredniški državni akterji, 3 ─ ne državni akterji, 4 ─ posredniški nedržavni akterji.

Tretja tabela: Države bi vsebovala naslednja polja:

- (ID, ID DRŽAVNEGA AKTERJA, IME DRŽAVE) vnosi v tabelo: 1 ─ id, 2 ─ id državnega akterja, 3 ─ ime države.

Četrta tabela: Grožnje bi vsebovala naslednja polja:

- (ZAPOREDNI ID, ID GROŽNJE, ID INDIKATORSKEGA POLJA, ID DRŽAVNEGA AKTERJA, ID DRŽAVE, DATUM, ČAS, NASLOV GROŽNJE, OPIS GROŽNJE, STOPNJA, ID SEKTORJA ZA OBVEŠČANJE).

Peta tabela: Aktivnost bi vsebovala naslednja polja:

- (ZAPOREDNI ID, ID KONVENCIONALNE GROŽNJE, ID NEKONVENCIONALNE GROŽNJE, DATUM, ČAS, NASLOV, OPIS, STOPNJA, ID OBVEŠČENEGA SEKTORJA)

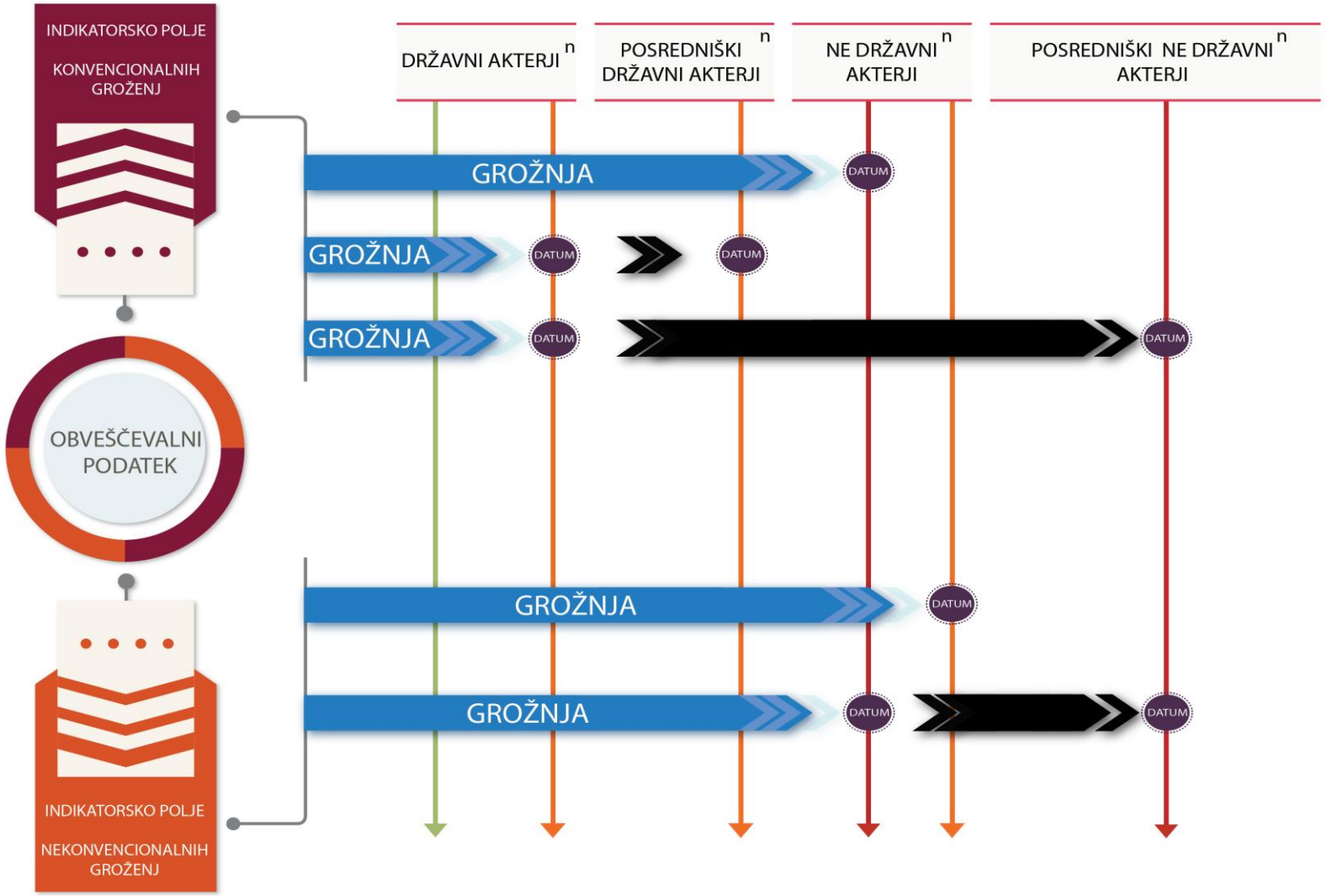
Šesta tabela: Sektorji bi vsebovala naslednja polja:

- (ID SEKTORJA, NASLOV, OPIS, KONTAKTNA OSEBA, ...).

Pri vnosu posamezne grožnje v sistem bi izpolnili vnosna polja za tabelo Grožnje.
Po vnosu bi sistem sprožil funkcijo, ki bi preverila povezave vnesene grožnje z obstoječimi. Pri funkciji bi se določili izbrani algoritmi za prepoznavanje medsebojnih povezav med grožnjami, ki bi nato sprožili aktivnost, v kolikor bi glede na prednastavljeni algoritem prišlo do ujemanja. Algoritmi bi preverili, ali pride do ujemanja obveščevalnega podatka konvencionalne grožnje z nekonvencionalno grožnjo za posameznega državnega akterja. V primeru ujemanja se sproži obvestilo ID sektorju, ki je zadolžen za posamezno grožnjo.

Za večjo varnost bi to temeljilo na decentralizirani »blockchain« tehnologiji, kjer bi bili podatki porazdeljeni medmrežno, saj bi bila tako ranljivost najmanjša. Mreža bi uporabljala javni in zasebni ključ kriptografije za dostop in pretakanje informacij digitalnih sredstev.

Slika 4.1: Diagram modela prepoznavanja hibridne ogroženosti



4.2 Stopnjevanje hibridne ogroženosti

Osnova za stopnjevanje hibridne ogroženosti je dejstvo, da so grožnje identificirane s pomočjo poenostavljenega modela. To pomeni, da je znan akter, ki ogroža, in da obstaja kartezični par groženj. Z ocenjevanjem hibridnih groženj želimo priti do stanja, da lahko načrtujemo ukrepe za zmanjševanje hibridnih groženj.

Za načrtovanje ukrepov moramo oceniti naslednje parametre. Predvsem je treba določiti vzrok oziroma namero morebitnega akterja hibridnega ogrožanja. Oceniti moramo zmožnosti akterja. Oceniti in določiti stopnjo hibridne ogroženosti.

Vzrok oziroma namero določimo subjektivno, z neprekinjenim spremljanjem stanja pri hibridnem akterju. Za spremljanje uporabljamo diplomatsko mrežo, agentsko mrežo, to storimo z izmenjavo obveščevalnih podatkov in skrbnim spremljanjem tako lokalnih kot državnih medijev.

Za ocenjevanje zmogljivosti hibridnega akterja lahko uporabimo Bowersov model križišča hibridnih groženj (glej sliko 2.9). S pomočjo Bowersovega modela lahko napovemo, katera izmed obstoječih ali novonastajajočih organizacij ali držav lahko v prihodnosti razvije elemente za hibridno ogrožanje. Kar zadeva organizacijsko zrelost, ni pričakovati, da bi se morebitni hibridni akter kar na enkrat pojavil, Bowers (2012, 47) prihodnost definira z desetletjem. Bolj verjetno je, da se hibridni akterji rekrutirajo/razvijejo iz že obstoječih oboroženih skupin ali iz vojaške in varnostne infrastrukture v posebnih skupinah propadlih držav. Če se določena skupina približuje križišču hibridnih groženj, tedaj se obveščevalno dejavnost in planiranje usmeri v tisto določeno skupino ali območje. Ti poskusi lahko presežejo načrtovanje ukrepov zoper določeno skupino, ki bi se znala razviti v odkrito hibridno grožnjo. Bolj učinkovito bi bilo usmeriti vse sile v onemogočanje hibridnim akterjem, da bi dosegli točko hibridnega ugodja.

Za določanje stopnje ogroženosti v Sloveniji na obrambnem področju se uporablja trinivojska stopnja. Nizka, ki pomeni, da akter razpolaga z omejenimi zmožnostmi in ni indikatorjev o nameri. Srednja pomeni, da obstaja stopnja ogroženosti in je akter nakazal namero, da bo napadel vendar za to ni potrjenih indikatorjev. Pri visoki stopnji ogroženosti dodamo še potrjene indikatorje.

Zaradi kompleksnosti hibridnega ogrožanja bi bilo treba izdelati več kot trinivojsko stopnjo hibridne ogroženosti. Za izhodišče določitev stopenj hibridnega ogrožanja lahko uporabimo naslednje parametre ogrožanja:

- kvantitativnost posameznih groženj,
- rzličnostt groženj (hibridnost groženj),
- zmožnosti hibridnega delovanja akterja,
- ugotovljeno namero.

Vsakemu parametru ogrožanja določimo stopnjo ogrožanja na petnivojski lestvici. Povprečje štirih parametrov ogrožanja uporabimo, da določimo, do katere stopnje nas hibridni akter ogroža. Petnivojsko določanje stopnje hibridne ogroženosti lahko povzamemo po britanski lestvici, ki jo uporablja MI5 za ocenjevanje teroristične ogroženosti.

- Prva stopnja ─ nizka ogroženost.
- Druga stopnja ─ zmerna ogroženost.
- Tretja stopnja ─ precejšnja ogroženost.
- Četrta stopnja ─ resna ogroženost.
- Peta stopnja ─ visoka ogroženost.

V nadaljevanju se bomo posvetili posameznemu parametru ogrožanja.

- ✓ **Parameter kvantitativnosti posameznih groženj;**

Kvantitativnost groženj določamo numerično v povezavi s časovno razsežnostjo pojavljanja groženj posameznega akterja. Razmerje pojavljanja posamezne grožnje opazujemo na hibridni časovni premici v določenem časovnem intervalu (časovni interval se določi glede na obdobje ocenjevanja ogroženosti). Za določanje stopnje ogroženosti po parametru kvantitativnosti groženj je pomembno število različnih groženj in pojavljanje posamezne grožnje v določenem časovnem intervalu. Najenostavnejše za določanje stopnje ogroženosti po parametru kvantitativnosti groženj je da se vse grožnje (G) seštejejo in delijo s 5 (nivoji ogroženosti), da dobimo stopnjo ogroženosti parametra kvantitativnosti groženj (G : 5 = stopnja ogroženosti). Za kompleksnejše in s tem natančnejše določanje tega parametra bi bilo treba v nadaljnjem raziskovanju izdelati matematični model. Za določanje stopnje parametra kvantitativne ogroženosti izdelamo vrednostno matriko (glej sliko 4.2), ki nam prikazuje ocenjevanje ogroženosti parametra kvantitativnosti.

Slika 4.2: Matrika ocenjevanja ogroženosti za parameter kvantitativne ogroženosti

Stopnje ogroženosti	Vrednost kvocienta grožnje
Prva stopnja – nizka ogroženost	$\leq 1,5$
Druga stopnja – zmerna ogroženost	1,6 do 2,5
Tretja stopnja – precejšnja ogroženost	2,6 do 3,5
Četrta stopnja – resna ogroženost	3,6 do 4,5
Peta stopnja – visoka ogroženost	$4,6 \geq$

- ✓ **Parameter različnosti groženj (hibridnost groženj)**;

Različnost groženj prav tako lahko določimo numerično. Več je različnih z indikatorji prepoznanih groženj, višja je stopnja hibridne ogroženosti. Vendar moramo različnost ocenjevati v povezavi z obsegom ogrožanja. Pri tem vidiku bomo uporabili ponderiranje. Višja je utež (ponder) večji je obseg grožnje. Kot primer lahko navedemo demografsko okolje, »grožnjo, ki se nanaša na lokalno okolje, nasproti grožnje, ki ogroža celotno družbo«, ali institucionalno »ogrožanje IKT varnostnega podjetja nasproti ogrožanja IKT Ministrstva za notranje zadeve«.

Uteži bomo določili za tri različne obsege ogrožanja. Nacionalni obseg, kritična infrastruktura ali glavno mesto ter lokalni obseg. Uteži določimo v matriki (glej sliko 4.3). Posamezne ponderirane grožnje med seboj seštejemo in delimo s 5 (nivoji ogroženosti). Za določitev stopnje ogroženosti uporabimo že predstavljeno matriko (glej sliko 4.2).

Slika 4.3: Matrika določitve uteži

Obseg ogrožanja	Utež
Nacionalni	0,5
Kritična infrastruktura ali glavno mesto	0,3
Lokalni	0,2

Za računanje bi lahko uporabili matematično formulo za računaje ponderirane aritmetične sredine (glej sliko 4.4), kjer nam (x) predstavlja število groženj za določen obseg in (p) utež. Vsekakor se ta parameter ogrožanja lahko raziskuje naprej in se prav tako izdela matematični model s primernimi algoritmi.

Slika 4.4: Primer formule za računanje ponderirane aritmetične sredine

$$\overline{x} = \frac{\sum_{i=1}^{n} x_i p_i}{\sum_{i=1}^{n} p_i} = \frac{x_1 p_1 + x_2 p_2 + \cdots + x_n p_n}{p_1 + p_2 + \cdots + p_n}$$

Vir: Calculat.

- ✓ **Zmožnosti hibridnega delovanja akterja;**

Subjektivna ocena zmožnosti hibridnega ogrožanja z upoštevanjem terena, zrelosti in zmogljivosti opravimo s pomočjo sinteze vseh treh elementov, ki smo jih predstavili z Bowersovim modelom (glej sliko 2.9). Stopnjo ogroženosti po parametru zmožnosti hibridnega delovanja akterja smo oblikovali glede na tri ključne spremenljivke hibridnih groženj (glej sliko 4.5), kompleksnost terena, zrelost organizacije in zmogljivost ter njeno napredovanje proti območju hibridnega ugodja.

Slika 4.5: Matrika določitve stopenj ogroženosti parametra zmožnosti

Stopnja dosega hibridnega ugodja	Stopnja ogroženosti
Vse tri ocene (kompleksnost terena, zrelost organizacije in zmogljivost) v področju hibridnega ugodja.	5 – visoka ogroženost
Zmogljivost in zrelost organizacije v področju hibridnega ugodja.	4 – resna ogroženost
Zmogljivost ali zrelost organizacije v področju hibridnega ugodja.	3 – precejšnja ogroženost
Zmogljivost za izdelavo eksplozivih teles in z možnostjo učinkovitega posrednega ognja. Zrelost organizacije na nivoju upornikov in	2 – zmerna ogroženost

paravojaških skupin. Kompleksnost terena sestavljajo agrarni ravninski del in prevladujoče družbene skupine.	
Organiziran kriminal, ulične tolpe, pehotno orožje, manj učinkovit posredni ogenj, puščavski teren, stepe.	1 – nizka ogroženost

- ✓ **Parameter ugotavljanja namere;**

Subjektivna ocena ugotovljene namere akterja s pomočjo analize je najzahtevnejša oblika ocenjevanja, zanjo potrebujemo znanje, tako strokovno kot znanstveno in izkušnje. Za ta del je nujno potrebna že omenjena ekspertna skupina. Na nivoju države Slovenije bi to lahko bila skupina MAS, ki deluje v okviru NCKU. Za ocenjevanje namere izdelamo matriko (glej sliko 4.6).

Slika 4.6: Matrika za ocenjevanje namere hibridnega akterja

Namere ni mogoče določiti.	1 – nizka ogroženost
Namera je delno določljiva.	2 – zmerna ogroženost
Namera je določljiva na daljše časovno obdobje (5 do 10 let).	3 – precejšna ogroženost
Namera je določljiva na krajše časovno obdobje (1 do 5 let).	4 – resna ogroženost
Namera je določljiva na zelo kratko obdobje do enega leta.	5 – visoka ogroženost

5 Ogroženost Slovenije

Kot smo v nalogi že ugotavljali, je ocena ogroženosti Slovenije nizka že zadnjih 25 let, vsekakor pa v zadnjem desetletnem obdobju. Dokument, ki bi opredeljeval tako stopnje kot oceno ogroženosti v Sloveniji, ni javno dostopen,. To stanje je z vidika preventive nerazumno. Za primer vzemimo v podpoglavju 4.2 navedeno spletno stran britanske obveščevalne službe MI5, ki poleg obrazložitve stopenj ogroženosti državljanom tudi svetuje, kako prepoznati določene

indikatorje groženj, kako postopati in obveščati. V Sloveniji se za določanje stopnje ogroženosti uporablja tristopenjska lestvica in glede na to, da ni dostopna, jo Prezelj (in drugi 2007) definira kot univerzalni sistem ocenjevanja ogroženosti na obrambnem področju. Univerzalnost gre v tem kontekstu razumeti kot širše sprejeto, vendar ne nujno točno. Vse tri stopnje, nizko, srednjo in visoko, smo že obdelali (glej podpoglavje 4.2). Za izdelan model bomo uporabljali petstopenjsko lestvico.

5.1 Analiza varnostnih groženj v Sloveniji

Izdelava celovite analize varnostnih groženj (ob analizi medijev) v Republiki Sloveniji bi bila preobsežna in ne bi zasledovala ciljev te naloge. Zato se bomo osredotočili le na nekatere indikatorje, ki bodo nakazali na morebitno hibridno ogrožanje. Ko se sprehodimo skozi javno dostopne vire (medije), se »grožnje« največkrat pojavljajo v povezavi z geopolitičnim prostorom, kjer Slovenija leži. To ugotovitev lahko podkrepimo z besedami vrhovnega poveljnika obrambnih sil, predsednika RS Boruta Pahorja, ki je podal mnenje v državnem zboru RS glede ocene pripravljenosti Slovenske vojske. Predsednik se osredotoči na zahodni Balkan, kamor spada tudi Slovenija. Navede da sta stabilnost in mir v regiji zahodnega Balkana za slovensko varnost vitalnega pomena. Da še vedno obstajajo odprta bilateralna vprašanja in zastoji pri gospodarskem, političnem in mednarodnem razvoju nekaterih držav in so dejavnik tveganja. Pravi tudi, da se to tveganje lahko naglo poveča ob morebitnem ponovnem zaostrovanju begunske in migrantske krize v regiji.

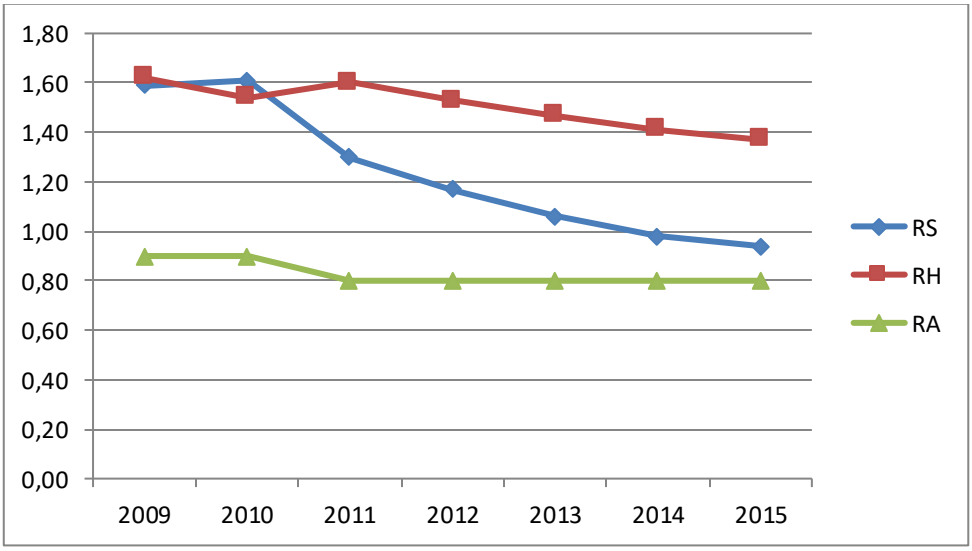
Preverimo indikator konvencionalnega ogrožanja, in sicer protestne diplomatske note. Ob migrantski krizi, ko sta Slovenska policija in Slovenska vojska postavljali žično ograjo na schengenski meji, je bilo do decembra 2015 slovenskim diplomatom predanih pet diplomatskih not.

Naslednji indikator konvencionalnega ogrožanja je povečanje proračuna za obrambo. Tu bi predvsem opozorili na razmerje sredstev namenjenih za obrambo. Kot primer analizirajmo BDP (bruto družbeni proizvod), namenjen za obrambo RS, vojaške zaveznice Republike Hrvaške (RH) in vojaško nevtralne Republike Avstrije (RA),(glej sliko 5.1). Grafični prikaz razmerja poudari (glej sliko 5.2).

Slika 5.1: Razmerje % BDP, namenjenega za obrambo RS, RH in RA

LETO (%BDP)	2009	2010	2011	2012	2013	2014	2015	Skupaj
RS	1,59	1,61	1,30	1,17	1,06	0,98	0,94	8,65
RH	1,62	1,54	1,60	1,53	1,47	1,41	1,37	10,54
RA	0,90	0,90%	0,80	0,80	0,80	0,80	0,80	5,8

Slika 5.2: Grafični prikaz razmerja % BDP, namenjenega za obrambo med RS, RH in RA

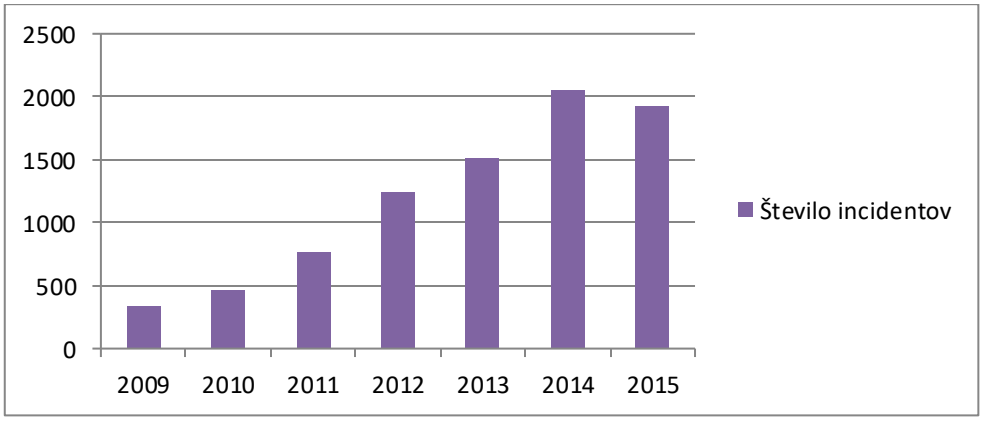


V nadaljevanju poglejmo nekonvencionalni ekonomski indikator. Osredotočili se bomo na nekaj ključnih podjetij, ki so nacionalno pomembna. Mercator, ki povezuje poleg trgovske verige tudi slovensko prehrambno industrijo. Koncern Agrokor je tudi s pomočjo hrvaških in ruskih bank uspel prevzeti lastništvo Mercatorja. Naslednje strateško podjetje je Petrol. V Petrolu imajo tuje banke več kot 15-odstotni delež. Naslednja povezava, ki smo jo analizirali, je povezava madžarskega podjetja MOL in hrvaške Ine ter češke banke. Československa obhodni bank je lastnica 12,8 odstotka Petrola. MMC RTV Slo je 23. januarja 2015 poročal o namenu MOL, da s pomočjo omenjene banke pride do skoraj 13-odstotnega lastništva Petrola. Omenimo še Ljubljanske mlekarne, ki so od jeseni 2012 v lasti francoske skupine Lactalis. Ta se je oktobra 2012 za prevzem 50,3-odstotnega deleža v družbi dogovorila z NFD Holdingom, Factor banko, skladom KD Delniški Dohodkovni, KD Banko in Savo, delež pa nato v začetku leta 2013 prenesla pod okrilje družbe Dukat, ki je del skupine Lactalis. Omenimo še področje

zavarovalništva, kjer je tuje podjetje Adris Grupa za RS druga največja lastnica skupine druge največje zavarovalniške skupine v Sloveniji Sava Re in tudi lastnica hrvaške zavarovalnice Croatia osiguranje. Ko pogledamo delniške knjige Save Re, ne lastništvo Croatie osiguranja in ne Adrisa uradno ni razvidno. Že več let se namreč skrivata za fiduciarnimi računi tujih bank. Do marca letos (2017) je Croatia osiguranje priznavala, da obvladuje nekaj manj kot desetodstotni delež, takrat pa so javnost prek Zagrebške borze obvestili, da je pridobila dodatnih (okoli) pet odstotkov delnic. Skupaj ima torej v lasti nekaj manj kot 15 odstotkov Save Re.

Za analizo kibernetskih incidentov uporabimo poročilo SI – CERT, ki od leta 2011 pripravlja letna poročila o informacijskih/kibernetskih incidentih v RS. Število incidentov narašča, čeprav je v zadnjih letih opaziti trend stagniranja na številki okoli 2000. Pri teh poročilih se moramo zavedati dejstva, da je po podatkih različnih organizacij in študij, prijavljenih samo 10 odstotkov varnostnih incidentov v informacijskih sistemih. Veliko incidentov (groženj/napadov) je takšne vrste, da uporabniki tega sploh ne zaznajo oziroma ne vejo, da so bili napadeni.

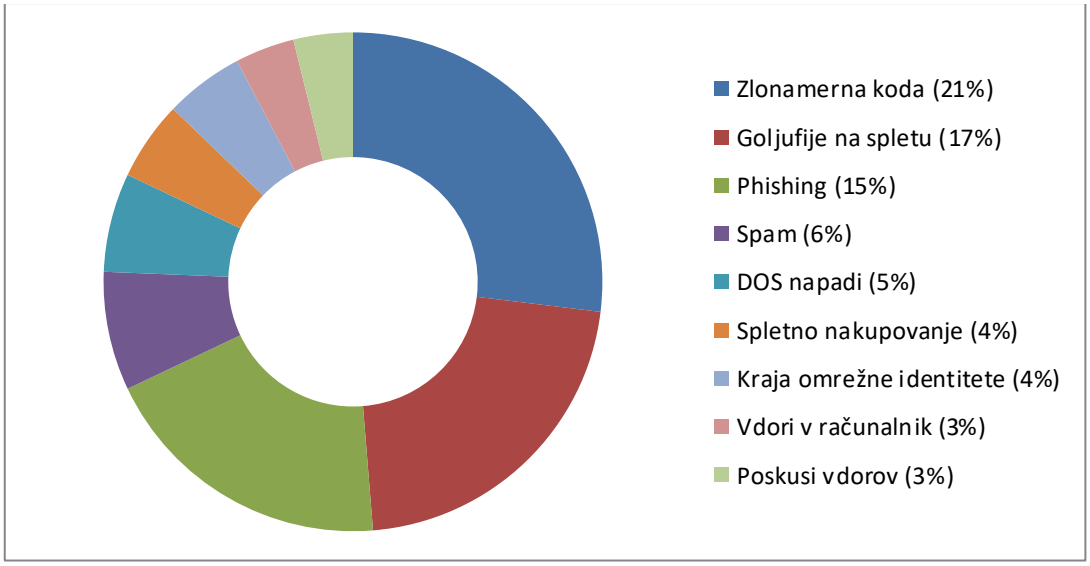
Slika 5.3: Graf kibernetskih incidentov v letih 2009 – 2015



Vir: Letno poročilo omrežne varnosti (SI – CERT, 2015).

Ko razčlenimo incidente za leto 2015, ugotovimo, da se je SI – CERT pri reševanju spletnih incidentov v kibernetskem prostoru pretežno ukvarjal z škodljivo zlonamerno kodo (21 %), goljufijami na spletu (17 %), s phishingom (15 %), spamom (6 %), DDoS napadi (5 %) in spletnim nakupovanjem (4 %). Zabeležena je bila tudi kraja omrežne identitete v štirih odstotkih in skeniranje/poskušanje vdora v treh odstotkih.

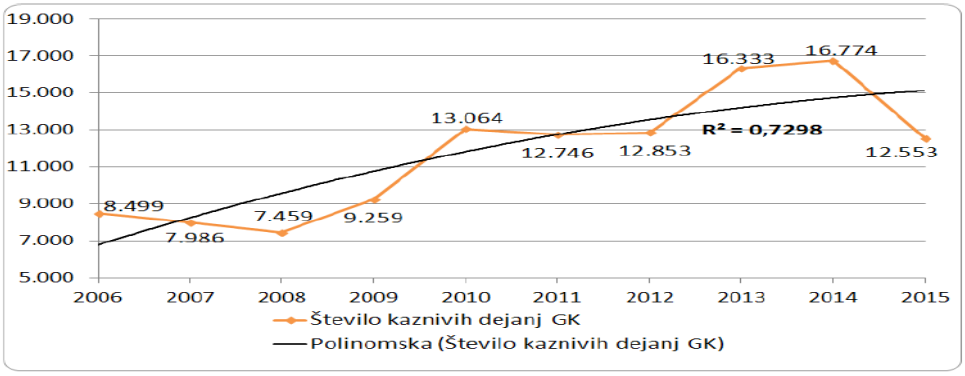
Slika 5.4: Grafična ponazoritev najpogostejših incidentov v letu 2015



Poglejmo še indikator tujih obveščevalnih služb. Indikator je predvsem z vidika tajnosti podatkov težko analizirati. Omenimo zadevo, ki je v letu 2015 polnila medije. Objavljeni so bili posnetki pogovora med državnimi zastopniki v povezavi z arbitražnim postopkom. Zanimivo je, da so novico objavili srbski mediji. Za kritike je bil ta dogodek tudi znak slabega dela slovenskih obveščevalcev oziroma protiobveščevalcev, ki prisluškovanja niso preprečili. Omenjeno afero so objavili mediji in le špekuliramo lahko, da so vdori tujih obveščevalnih služb stalnica.

Indikator gospodarski kriminal. Na sliki 5.6, ki je povzeta iz letnega poročila o delu Slovenske policije, nakazuje polinomsko naraščanje gospodarske kriminalitete v Republiki Sloveniji.

Slika 5.5: Gospodarska kriminaliteta v obdobju 2006 – 2015



Vir: Letno poročilo o delu policije 2015 (2016, 19).

Indikator, organizirani kriminal. Policija se je na področju organizirane kriminalitete usmerila predvsem v odkrivanje in preiskovanje organiziranih oblik čezmejne kriminalitete, ki v veliki

meri izhaja ali je tesno povezana z območjem jugovzhodne Evrope in Zahodnega Balkana. Za odkrivanje in preiskovanje delovanja organiziranih kriminalnih združb je bilo v sodelovanju s tujimi varnostnimi organi izvedenih več skupnih preiskav. Obravnavanih je bilo 387 (382) ali za 1,3 odstotka več kaznivih dejanj kot leto prej, ki so bila posledica organizirane kriminalne dejavnosti. Ovadenih je bilo 245 (260) ali za 5,8 odstotka manj oseb. Posledica sprememb migracijskih poti in izvajanja prikritih preiskovalnih ukrepov je bilo povečanje števila zaznanih kaznivih dejanj prepovedanega prehajanja meje ali ozemlja države z 31 na 62. Velja omeniti, da morajo biti za opredelitev organizirane kriminalne dejavnosti izpolnjena štiri obvezna in najmanj dve od sedmih variabilnih (izbirnih) meril. Obvezna merila so obstoj skupine vsaj treh ljudi, delovanje v daljšem časovnem obdobju, pridobivanje premoženjske koristi in/ali družbene moči ter izvrševanje uradno pregonljivih kaznivih dejanj. Variabilna merila so uporaba nasilja in/ali korupcije, delovanje na mednarodni ravni, sodelovanje pri pranju denarja, notranja pravila ravnanja ter delitev vlog in nalog med člani skupine, podjetniški način delovanja ter vplivanje na medije, gospodarstvo, državno upravo in/ali politiko (Letno poročilo o delu policije 2015, 2016, 35).

5.2 Analiza intervjujev

Za prikaz delovanja modela za ocenjevanje hibridnih groženj bomo nadaljevali preizkus. Z delno opravljeno analizo varnostnih groženj smo ugotovili, da grožnje obstajajo. Kljub analizi in ugotovljenem stanju se zavedamo, da s tovrstno analizo varnostnih groženj, za katero smo podatke pridobili iz javno dostopnih virov, na izdelanem modelu preizkusa ne moremo izvesti. Kot smo ugotovili pri izdelavi modela, potrebujemo analizirane in ovrednotene obveščevalne podatke, s pomočjo katerih lahko povežemo indikatorje groženj z akterji. Pri sami izdelavi raziskovalnega načrta smo že prišli do enake ugotovitve. Zato smo oblikovali fokusirane intervjuje (glej prilogo), s pomočjo katerih smo od strokovnih in političnih nosilcev funkcij v nacionalnovarnostnem sistemu poskušali pridobiti njihovo videnje hibridnosti v povezavi z varnostjo. Z analizo intervjujev pričakujemo dovolj verodostojnih podatkov, da bi potrdili analizirane grožnje in s tem dobili odgovor na zastavljeno hipotezo.

Izvedli smo fokusirane intervjuje z naslednjimi intervjuvanci.

- Vprašanja za brigadirja Miho Škerbinca, namestnika direktorja oddelka za vojaško načrtovanje in vojaško politiko vojaškega odbora zavezništva Nato, smo poslali po

elektronski pošti 23. maja 2017 ob 18. uri in 18 minut, odgovore smo prejeli 23. maja 2017 ob 21. uri in 57 minut.

- Intervju z Boštjanom Šeficem, državnim sekretarjem MNZ, je bil opravljen v prostorih Ministrstva za notranje zadeve, Litostrojska 54, 25. maja 2017, od 09. do 11. ure.
- Intervju z Matejem Marnom, generalnim direktorjem Direktorata za skupno zunanjo in varnostno politiko MZZ, je bil opravljen v prostorih MZZ, Prešernova cesta 25, 29. maja 2017, od 14.30 do 15.30.
- Intervju z mag. Urošem Krekom, namestnikom generalne sekretarke/svetovalcem predsednika republike za obrambne zadeve, je bil na Uradu predsednika Republike Slovenije, Erjavčeva 17, Ljubljana, 2. junija 2017 od 11. do 12. ure.
- Vprašanja za dr. Erika Kopača, državnega sekretarja, pristojnega za nacionalno varnost v kabinetu predsednika vlade RS, smo poslali 13. junija 2017 ob 10.30. odgovore smo prejeli 13. junija 2017 ob 16,51.

Vprašanja za posameznega intervjuvanca so v prilogi. Zvočni posnetki intervjujev in transkript odgovorov so v originalu pri avtorju magistrskega dela.

Analiza intervjujev je pokazala, da so hibridne grožnje poznan termin. Stroka se zaveda pomena in značilnosti. Naloga stroke je, da pojem hibridno bolj približa nosilcem pomembnejših funkcij v nacionalnem varnostno-obrambnem sistemu RS.

Sklepati je, da iz izvedenih intervjujev Slovenija ni hibridno ogrožena na način, kot so pojem intervjuvanci na političnih dolžnostih razumeli. Analiza intervjujev je tudi pokazala, da hibridne grožnje ne obravnavajo pristojni organi, ki se ukvarjajo z ogroženostjo Slovenije. Pozitivni premik je narejen pri ocenjevanju terorističnih groženj, tako v smislu ustanovitve stalne delovne skupine, koordinatorja in večstopenjske lestvice ogroženosti.

Na najvišjem organu nacionalnovarnostnega sistema se groženj v povezavi s hibridnostjo zavedajo zato bomo citirali dr. Kopača: »Hibridne grožnje so ena izmed tem, katere se bodo v bližnji prihodnosti obravnavale na nivoju SSNAV. Pomembno je, da Slovenija novo dimenzijo prepozna in jo ustrezno vključi v strateške in doktrinarne dokumente, kar se bo posledično odražalo v prilagoditvah v graditvi obrambnih zmogljivosti. Na začetku vlogo SSNAV vidimo predvsem v koordinaciji opredelitve koncepta hibridnega ogrožanja ter postavitvi smernic za nadaljnje ukrepanje na tem področju. Ali bo SSNAV v prihodnje prevzel operativno-koordinatno vlogo pri odzivanju na tovrstna ogrožanja, pa bo pokazal čas. Pri tem bi opozorili, da je v tem trenutku SSNAV posvetovalno telo« (intervju z dr. Kopačem, 13. junija 2017).

Intervjuvanci se strinjajo, da bi bila potrebna koordinacijska skupina, ki bi usmerjala delo obveščevalnih služb, v njej bi se zbirali vsi obveščevalni podatki (all source intelligence) in določala bi stopnjo ogroženosti republike Slovenije. Strinjali so se tudi glede vključevanja javnosti, ta bi morala biti bolj obveščena o stopnjah ogroženosti, o preventivi in kurativi.

Vsi intervjuvanci menijo, da je treba zagotoviti ustrezno odpornost države. Za soočanje s hibridnimi grožnjami je potreben celosten vladni pristop, zato je za to primarno odgovorna država. Glede na to, da je vsebina povezana z dolgoročno oceno groženj in podrejena strategiji nacionalne varnosti, je pomembno, da delo na »hibridnem konceptu« poteka vzporedno z obnovo Resolucije o strategiji nacionalne varnosti in Obrambne strategije. Prizadevati si je treba, da bodo aktivnosti glede hibridnega ogrožanja potekale tesno povezane z aktivnostmi, ki že potekajo tako na ravni Nata kot EU.

Mnenju intervjuvancev glede odpornosti države in tesni povezanosti z EU in Natom, dodajmo še ugotovitev Fägerstena (2016), ki piše o hibridni odpornosti (hybrid resilience). Hibridno odpornost na nacionalni ravni je glede na različnost in stalnost hibridnih groženj težko vzdrževati. Z rastjo nacionalnih soodvisnosti raste tudi soodvisnost pri graditvi hibridne odpornosti in ni omejena le na trenutno obstoječe soodvisnosti (Fägersten 2016, 115). Intervjuvance skrbi politična razdeljenost družbe, ki je idealen poligon za delovanje tujih obveščevalnih služb. Vsi so enotnega mnenja, da bi v primeru konkretne vojaške ogroženosti RS politika pozabila na delitve in podobno kot leta 1991 stopila skupaj.

Skrb vzbuja dejstvo, ki se v neki meri nanaša na že omenjeno koordinacijsko skupino, da intervjuvanci niso seznanjeni z bilateralnimi dogovori o izmenjavi obveščevalnih podatkov. Zatorej lahko špekuliramo, da teh dogovorov ni. Politični del intervjuvancev je tudi pozdravil projekt vlade RS, imenovan P-7 (Sistem kriznega upravljanja in vodenja v RS), in z njim vzpostavitev MAS, ki je tudi za v tej nalogi izdelani model ključen element.

6 Zaključek in priporočila

Z obravnavo teoretičnih vsebin smo izpostavili indikatorje konvencionalnih in nekonvencionalnih ogrožanj. Dokazali smo, da so indikatorji hibridnega ogrožanja le kombinacija indikatorjev konvencionalnega in nekonvencionalnega ogrožanja in ne novo

dejstvo. Prišli smo do pomembnega spoznanja, da so hibridne grožnje dokazljive ter se distancirali od pojma hibridna vojna. Določili smo možne akterje hibridnega ogrožanja. Tako smo operacionalizirali hibridno ogrožanje in oblikovali model za ocenjevanja hibridnega ogrožanja nacionalne varnosti. S tem smo pritrdilno odgovorili na raziskovalno vprašanje, RV 1: Ali lahko s pomočjo teorije operacionaliziramo hibridno ogrožanje?

V nadaljnjem raziskovanju se izdelani model lahko razvije v računalniško aplikacijo ob ustrezni določitvi algoritmov, ki bi obveščevalne podatke s pomočjo indikatorjev groženj povezali z enim ali več akterji. Izdelana aplikacija bi bila osnova analitikom za izdelavo subjektivnih analiz hibridnega ogrožanja. Slabost izdelanega modela je povezava kibernetskih groženj z akterji. Določanje akterjev pri kibernetskem ogrožanju je in bo velik izziv. Nakazali smo tudi možno pot razvoja modela v aplikacijo.

V nadaljevanju raziskovanja smo skozi nekatere indikatorje analizirali ogroženost Slovenije. Izvedli smo fokusirane intervjuje z namenom, da bi odgovorili na zastavljeno hipotezo H 1. Hibridna ogroženost nacionalne varnosti Slovenije je bistveno višja, kot jo v javnosti predstavljajo državne institucije.

Hipoteza je bila zastavljena precej provokativno, glede na dejstvo, da se o hibridni ogroženosti s strani državnih institucij javno še ne razpravlja. Z analizo groženj po naključno izbranih indikatorjih smo model tudi preizkusili. Izjema pri omenjanju hibridnih groženj je predsednik RS Borut Pahor, ki je v svojem mnenju o stanju pripravljenosti Slovenske vojske za leto 2015 (glej podpoglavje 5.1) govoril tudi o hibridnih tveganjih in zapisal, da se bo Slovenija morala zaradi novih oblik ogrožanja varnosti nanje pripraviti v konceptualnem, sistemskem in organizacijsko-kadrovskem smislu.

Zato moramo hipotezo zavreči. Kljub temu, da hipoteze nismo potrdili, je naloga v tem pogledu dosegla svoj cilj.

Pri določanju stopnje ogroženosti bodo državne ustanove, ki so vključene v nacionalnovarnostni sistem, morale biti tudi zaradi hibridnih groženj predvsem veliko bolj transparentne.

Med potrjevanjem hipoteze smo ugotovili, da bi bilo treba graditi hibridno odpornost države. Državljani RS morajo v vsakem trenutku vedeti kakšna je stopnja ogroženosti Slovenije, kako indikatorji ogrožanja prepoznati oziroma kateri so. Na ta način bo lahko država prišla do pomembnih informacij na primarni ravni, ki jih tudi zaradi kadrovske podhranjenosti, pomakanja finančnih sredstev, neustrezne organiziranosti ali celo rutinskega opravljanja operativnega dela zaposlenih v nacionalnovarnostnem sistemu, predvsem v podsistemu notranje varnosti, spregleda.

Kot so tudi intervjuvanci poudarili, je treba preseči zgodovinsko motivirane delitve in se s skupnim ciljem, zagotavljanjem varnostne blaginje državljanov, spopasti s hibridnimi grožnjami. Za dosego cilja je potreben že omenjeni univerzalni politični konsenz na področju varnosti, ki s pomočjo šolskega sistema vključuje preventivno varnostno indoktrinirane državljane in državljanke. Celotni nacionalnovarnostni sistem z vsemi specialističnimi resursi, predvsem iz obveščevalnega sektorja, ki vključuje elemente Ministrstva za notranje zadeve, Ministrstva za zunanje zadeve, Slovenske obveščevalno-varnostne agencije, Obveščevalno-varnostne službe Ministrstva za obrambo in vojaške obveščevalno-varnostne organe Slovenske vojske. Prav pri teh je nujno potrebna zakonska ureditev, ki bi se začela s primarnim aktom, Zakonom o obrambi, ki v sedanji obliki opredeljuje obveščevalno dejavnost le Obveščevalno-varnostni službi Ministrstva za obrambo in Slovenski obveščevalno-varnostni agenciji. Sprememba bi omogočila reorganizacijo obveščevalno-varnostnega sistema, kot smo omenili na koncu podpoglavja 3.2. S tem bi vzpostavili pogoje za rast hibridne odpornosti. Pri graditvi hibridne odpornosti je nujno čezmejno sodelovanje. Okvir takega sodelovanja je že nastavljen v okviru skupne zunanje in varnostne politike EU v tesnem sodelovanju z Natom in ob vzpostavitvi hibridne fuzijske celice (Hybrid fusion cell). Podpora Slovenije temu projektu tudi s kadri bi bil korak naprej pri graditvi nacionalne hibridne odpornosti.

Hibridne grožnje ne poznajo meja, ne razlikujejo med vojaškim in civilnim. To pa je tudi razlog, da preučevanje in iskanje rešitev za prepoznavanje in preprečevanje hibridnih groženj ne more biti usmerjeno samo naloga vojaške organizacije, ampak se morajo s tem problemom soočiti vsi, ki so tako ali drugače vključeni v nacionalnovarnostni sistem. Prav tako, kot smo že omenili, je to naloga prav vsakega varnostno osveščenega državljana. Zavedati se namreč moramo, da živimo v časih, ko se vojne ne odvijajo na oddaljenih bojiščih, ampak med nami. Zato bo vedno več pozornosti in finančnih sredstev treba namenjati tudi oboroženim silam, njihovi opremi, kadru, oborožitvi in usposabljanju. Že skoraj zgodovinsko dejstvo je, da ljudstvo, ki ne hrani svoje vojske, hrani tujo.

Z izdelanim modelom bomo lažje prepoznali hibridne grožnje. Potem bo treba okrepiti ustrezno nacionalno odpornost in zagotoviti, da bomo pripravljeni odgovoriti, s hitro oceno in učinkovitim odločanjem. S krepitvijo konvencionalnih zmogljivosti brez ustreznih nekonvencionalnih mehanizmov ne bomo mogli zgraditi kredibilnega odziva. Ob zgodnjem prepoznavanju groženj bo potrebna krepitev sinergije med strategijami in delovanjem resorjev. Ker je krepitev nacionalnih odpornosti ena izmed ključnih komponent uspešnega odvračanja in obrambe pred hibridnimi grožnjami in izzivi, mora Slovenija poglobiti obstoječe in vzpostaviti nove mehanizme in koordinacijo na nacionalnem nivoju.

Prav na koncu bi zapisal misel. Imeti samostojno državo so bile stoletja sanje naših dedov. Poti, ki so nas pripeljale do uresničitve sanj leta 1991, so bile različne. Nekateri so se borili z besedo, drugi v španski državljanski vojni, nekateri v Galiciji, tretji v vojski Avstro-ogrske monarhije ali Kraljevine Italije. Poti so bile v okviru različnih držav in vladarjev tudi politične. Borili so se s pesmijo, borili so se za severno mejo, bili so partizani, bili so domobranci. Nekateri v teritorialni obrambi, nekateri v jugoslovanski armadi. Različnost teh poti nas dela velike in močne. Različnost teh poti nas je pripeljala do države, do Slovenske vojske. Različnost nas povezuje in ne razdružuje. Lahko bi dejali, da smo do sanj prišli na hibriden način. Tudi na hibriden način lahko vse kar smo dosegli, izgubimo.

7 Literatura

1. Alderman, Ray. 2015. *Sixth generation warfare: manipulating space and time.* Dostopno prek: http://mil-embedded.com/guest-blogs/sixth-generation-warfare-manipulating-space-and-time/ (5. april 2017).

2. Ancker, J. Clinton in Michael D. Burke. 2003. *Doctrine for asymetric warfare*. Dostopno prek: http://www.au.af.mil/au/awc/awcgate/milreview/ancker.pdf (7. april 2017).
3. Anžič, Andrej. 1996. *Vloga varnostnih služb v sodobnih parlamentarnih sistemih-nadzorstvo*. Ljubljana: ČZP Enotnost.
4. --- 1997. *Varnostni sistem Republike Slovenije*. Ljubljana: Uradni list RS.
5. Bricman, Urban. 2016. Sirski konflikt skozi prizmo hibridne vojne. Diplomsko delo. Ljubljana: FDV.
6. Britovšek, Jaroš in Aleš Čretnik. 2016. Obveščevalno-varnostni sistem Republike Slovenije: reorganizacija in sistemske rešitve. *Varstvoslovje* 18 (3). Ljubljana: Univerza v Mariboru, Fakulteta za policijsko-varnostne vede.
7. Berzinš, Janis. 2014. *Russia's new Generation Warfare in Ukraine*: Implications for Latvian Defense Policy. Dostopno prek: http://www.naa.mil.lv/~/media/NAA/AZPC/Publikacijas/PP%2002-2014.ashx (31. marec 2016).
8. Babič, Drago. 2013. *Tradicionalno proti netradicionalnemu*. Opredelitev asimetričnega ogrožanja varnosti. Zaključna naloga. Maribor: VŠT.
9. Bowers, O. Christopher. 2012. *Identifying Emerging Hybrid Adversaries*. U.S. Army War College. Dostopno prek: http://indianstrategicknowledgeonline.com/web/hybrid%20Bowers.pdf (28. marec 2017).
10. Bratuša, Tomaž. 2011. *Asimetrično bojevanje in strategija posrednega nastopanja v kibernetski vojni*. Magistrsko delo. Maribor: Univerza v Mariboru, Fakulteta za varnostne vede.
11. Calculat.org. *Ponderirana aritmetička sredina.* Dostopno prek: http://www.calculat.org/hr/prosjek/ponderirana-aritmeticka-sredina.html (18. maj 2017).
12. Cigler, Mirko. 2016. *Hibridna varnost*. V Konvencionalna in hibridna varnost: Vzorci (dis)kontinuitete, ur. Marjan Malešič, 75–95. Ljubljana: Fakulteta za družbene vede.
13. Cruceru, Valerică. 2014. On contemporary warfare: Short review of specific concepts. *Military Art and Science, Revista academiei forţelor terestre* 3 (75)/2014: 231–237. Dostopno prek: http://www.armyacademy.ro/reviste/rev3_2014/CRUCERU.pdf (17. junij 2017).
14. Črnčec, Damir. 2009. *Obveščevalna dejavnost v informacijski dobi*. Ljubljana: Defensor d.o.o.

15. Deep, Alex. 2015. *Hybrid War*: Old Concept, New Techniques. Dostopno prek: http://smallwarsjournal.com/jrnl/art/hybrid-war-old-concept-new (15. marec 2017).
16. Department of Defense. *Quadrennial defense review 2014*. Dostopno prek: http://archive.defense.gov/pubs/2014_Quadrennial_Defense_Review.pdf (10. april 2017).
17. *DHS Office of Intelligence and Analysis, Domestic Threat Analysis Division* (DTA) (2009, 9). Dostopno prek: https://info.publicintelligence.net/Bamford_ICSJWG_Fall_2009.pdf (15. april 2017).
18. Dokl, Jure. 2012. *Kibernetska varnost omrežij*. Magistrsko delo. Ljubljana: FDV.
19. Ducaru, Dimitru Sorin. 2016. *The cyber dimension of modern hybrid warfare and its relevance for NATO*. Europolity 10 (1). Dostopno prek: http://europolity.eu/wp-content/uploads/2016/07/Vol.-10.-No.-1.-2016-editat.7-23.pdf (18. junij 2017).
20. Dunn, Myriam. 2005. *A Comparative Analysis of Cyber Security Initiatives Worldwide*. Geneva: International telecommunication union. Dostopna prek: https://www.itu.int/osg/spu/cybersecurity/docs/Background_Paper_Comparative_Analysis_Cybersecurity_Initiatives_Worldwide.pd (7. april 2017).
21. Eikenberry, W. Karl. 2014. Thoughts on unconvencional threts and terrorism. Hoover institution. Dostopno prek: http://www.hoover.org/sites/default/files/fw_hoover_foreign_policy_working_group_unconventional_threat_essay_series/201411%20-%20Eikenberry.pdf (17. junij 2017)
22. Evropska komisija. 2016. Skupno sporočılo evropskemu parlamentu ın svetu. *Skupni okvir o preprečevanju hibridnih groženj*. Dostopno prek: http://eur-lex.europa.eu/legal-content/SL/TXT/PDF/?uri=CELEX:52016JC0018&from=EN (7. april 2017).
23. Fägersten, Björn. 2016. *Forward Resilience in the Age of Hybrid Threats: The Role of European Intelligence*. Forvard Resilience (Daniel S. Hamilton, editor). Centre For Transatlantic Relations. Washington D.C. Dostopno prek: http://transatlanticrelations.org/wp-content/uploads/2017/02/Forward_Resilience_Full-Book.pdf (30. junij 2017).
24. Fleming, P. Brian. 2011. *The hybrid threat concept: Contemporary war, military planning and the advent of unrestricted operational art*. Monograph. Kansas: School of advanced Military studies. United States army command and General Staff College.
25. Hoffman, Frank. 2006. *Lessons from Lebanon*: Hezbollah and Hybrid Wars. Dostopno prek: http://www.fpri.org/article/2006/08/lessons-from-lebanon-hezbollah-and-hybrid-wars/ (1. marec 2107).

26. --- 2007. *Conflict in the 21st Century*: *The Rise of Hybrid Wars*. Arlington – Virginia: Potomac Institute for Policy Studies.
27. Gologranc, Gal. 2015. *Statistična ocena faltorjev prevlade šibkejšega nad močnejšim v slovenski osamosvojitveni vojni*. Magistrsko delo. Ljubljana: FDV.
28. Grizold, Anton. 2005. *Slovenija v spremenjnem varnostnem okolju: k razvoju obrambno-zaščitnega sistema: izzivi in spobude.* Ljubljana: FDV
29. Hadžović, Sead. 1988. *Problemi organizacije nacionalnih obaveštajnih sistema u savremenim uslovima međunarodnih kretanja*. Beograd: 13. Maj.
30. Hundley, O. Richard, Robert H. Anderson, Tora K. Bikson, Maarten Botterman, Jonathan Cave, C. Richard Neu, Michelle Norgate in Renee Cordes. 2001. The future of the information revolution in Europe. Natıonal defense research institute. Santa monica: RAND.
31. Jennings A., Nathan. 2017. *Realign the Army for Multi-Domain Battle*. Association of United States Army. Dostopno prek: https://www.ausa.org/articles/realign-army-multi-domain-battle#.WO--tv8IVgI.facebook (29. junij 2017).
32. Kobola, Mitja. 2016. *Asimetrično vojskovanje – vrste in primeri skozi zgodovino ZDA*. Diplomsko delo. Ljubljana: FDV.
33. Kokalj, Mirjam. 2006. Slovenska *obveščevalno-varnostna agencija kot samostojna vladna služba.* Diplomsko delo. Ljubljana: FDV.
34. Krunić, Zoran. 1997. *Strategija posrednega nastopanja*. Unigraf. Ljubljana.
35. Kotnik-Dvojmoč, Igor. 2000 ─ 2001. Varnostna tveganja in grožnje v sodobnem svetu. *Ujma 14 ─15*. Ljubljana: Minstrstvo za obrambo. URSZR.
36. Kure, Ina. 2009. *Koordinacija med obveščevalno varnostnimi subjekti*. Diplomsko delo. Ljubljana: FDV.
37. Liang, Qiao in Wang Xiangsui. 1999. *Unrestricted Warfare*. Beijing: PLA Literature and Arts Publishing House.
38. Lind, S. William, Heith Nightengale, John F. Schmitt, Joseph W. Sutton in Hary I.Wilson. 1989. *The Changing Face of War: into the Fourth Generation*. Marine Corps Gazette 73 (10). Dostopno prek: https://www.mca-marines.org/files/The%20Changing%20Face%20of%20War%20-%20Into%20the%20Fourth%20Generation.pdf (20. marec 2017).
39. Lubi, Darko. 1999. *Jedrsko širjenje po Hladni vojni*. Znanstvena knjižnica. Ljubljana: FDV.

40. Ministrstvo za notranje zadeve, Policija, Služba generalnega direktorja policije, Sektor za odnose z javnostmi in Sektor za razvoj in sistemske naloge, Oddelek za načrtovanje in analitiko. 2016. *Letno poročilo o delu policije 2015*. Ljubljana.
41. Malešič, Marjan, 2002. *Nacionalna in mednarodna varnost*. Ljubljana: FDV.
42. Malešič, Marjan in Anton Žabkar. 2016. Konvencionalno ali hibridno vojskovanje? 1.nad. Vloga Ruske federacije v sirski vojni. *Revija Obramba*. Ljubljana: Založba Defensor d.o.o..
43. Mattis N. James in Frank Hoffman. 2005. Future Warfare: The Rise of Hybrid Wars. *Proceedings Magazine*. US Naval Institute. Dostopno prek: http://milnewstbay.pbworks.com/f/MattisFourBlockWarUSNINov2005.pdf (28. maj 2017).
44. Mažeikis, Edvardas. 2017. *Hybrid threats: overcoming ambiguity, building resilience*. Dostopno prek: http://www.tspmi.vu.lt/doc/1554-edvardas-mazeikis-hybrid-threatsdocx (29. maj 2017).
45. NATO. 2014. *Wales Summit Declaration*. Dostopno prek: http://www.nato.int/cps/en/natohq/official_texts_112964.htm (17. april 2017).
46. NATO, Public Diplomacy Division. 2017. *Defense Expenditure of NATO Countries (2009-2016).* Dostopno prek: http://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2017_03/20170313_170313-pr2017-045.pdf (1. junij 2017).
47. NATO Standardisation Agency. 2003. *AJP – 2.0 Skupna zavezniška obveščevalna, protiobveščevalna in varnostna doktrina.* Stanag 2190. Brussels: NATO Standardisation Agency.
48. *Odlok o Svetu za nacionalno varnost*. Ur. l. RS 76/2014 (22. oktober 2014).
49. Pahor, Borut. 2016. *Mnenje predsednika Republike Slovenije Boruta Pahorja o stanju pripravljenosti Slovenske vojske*. Dostopno prek: http://www.up-rs.si/up-rs/uprs.nsf/objave/C81C1823FEC78751C1257FA90030FFB7?OpenDocument (20. maj 2017).
50. Perkins, David, G. 2016. *Multi-Domain Battle: Joint Combined Arms Concept for 21st Century*. Association of the United States Army. Dostopno prek: https://www.ausa.org/articles/multi-domain-battle-joint-combined-arms-concept-21st-century (28. junij 2017).
51. Pernat, Staša. 2006. Analiza *zunanje politike in zunanjepolitične strategije Združenih držav Amerike*. Diplomsko delo. Ljubljana: FDV.

52. Potočnik, Viktor. 2016. Fourth generation warfare. Part 1: Geopolitical framework to Slovenian security. *Sodobni vojaški izzivi* 18 (2). Ljubljana: Generalštab Slovenske vojske.
53. Prezelj, Iztok, ur., Svete Uroš, Kopač Erik, Meško Gorazd in Dobovšek Bojan, Kraigher Alenka in Berger Tatjana, Grošelj Klemen. 2007. *Model celovitega ocenjevanja ogrožanja nacionalne varnosti Republike Slovenije.* Ljubljana: Ministrstvo za obrambo, Direktorat za obrambne zadeve, Sektor za civilno obrambo.
54. Prezelj, Iztok. 2006. *Teroristično ogrožanje nacionalne in mednarodne varnosti.* Varstvoslovje, 8. Ljubljana: Univerza v Mariboru, Fakulteta za policijsko-varnostne vede.
55. Regionalna obala. 2014. *V tujih rokah že kar nekaj (uspešnih) slovenskih podjetij.* Dostopno prek: http://regionalobala.si/novica/v-tujih-rokah-ze-kar-nekaj-uspesnih-slovenskih-podjetij- (25. maj 2017).
56. Regionalna obala. 2015. *Zaradi žice ob meji: Že peta hrvaška diplomatska nota Sloveniji.* Dostopno prek: http://www.regionalobala.si/novica/zaradi-zice-ob-meji-ze-peta-hrvaska-diplomatska-nota-sloveniji (25. maj 2017).
57. *Resolucija o strategiji nacionalne varnosti Republike Slovenije* (ReSNV-1). Ur. l. RS 27/2010 (26. marec 2010).
58. RTV Slovenija, MMC. 2015. *Mol naj bi skozi zadnja vrata na tiho vstopal v Petrol. Madžari to zanikajo.* Dostopno prek: https://www.rtvslo.si/gospodarstvo/mol-naj-bi-skozi-zadnja-vrata-na-tiho-vstopal-v-petrol-madzari-to-zanikajo/356438 (25. maj 2017).
59. Security service MI5. *Threat levels*. Dostopno prek: https://www.mi5.gov.uk/threat-levels (13. maj 2017).
60. Simoniti, Iztok. 2001. *Človek, država in vojna*. V človek, država in vojna, ur. Luard Evan, Iztok Simoniti in Anton Grizold, 15 ─ 82. Ljubljana: FDV.
61. SiolNet. 2016. *Potrjeno: Hrvati v naskoku na drugo največjo zavarovalniško skupino v Sloveniji.* Dostopno prek: http://siol.net/posel-danes/novice/potrjeno-hrvati-v-naskoku-na-drugo-najvecjo-zavarovalnisko-skupino-v-sloveniji-416987 (25. maj 2017).
62. Siolnet. 2015. *To so najodmevnejše afere slovenskih obveščevalcev*. Dostopno prek: http://siol.net/novice/slovenija/to-so-najodmevnejse-afere-slovenskih-obvescevalcev-389567 (5. junij 2017).
63. Sipri. 2015. Milex-data 1988-2014. Dostopno prek: http://www.sipri.org/research/armaments/milex/milex_database/milex-data-1988-2014 (1. junij 2017)

64. Svete, Uroš. 2016. Hibridni konflikti v omrežni družbi. V *Konvencionalna in hibridna varnost:* Vzorci (dis)kontinuitete, ur. Marjan Malešič, 97 ─ 112. Ljubljana: FDV.
65. --- 2006. Nacionalno varnostni vidik ogrožanja informacijske infrastrukture. *Varstvoslovje* 8. Ljubljana: Univerza v Mariboru, Fakulteta za policijsko-varnostne vede.
66. --- 2002. *Vloga in pomen informacijske tehnologije v sodobnem asimetričnem vojskovanju.* Magistrsko delo. Ljubljana: FDV.
67. Svete, Uroš, Damijan Guštin in Vladimir Prebilič. Asimetrija in vojaška organiziranost: slovenske izkušnje. V Mednarodne razsežnosti varnosti Slovenije, ur. Marjan Malešič, 247 ─ 280. Ljubljana: FDV.
68. Svete, Uroš, Damjan Guštin, Janja Vuga, Rok Zupančič in Jelena Juvan. 2015. *The Small State Facing Asymmetric Enviroment*. Prague: Institute of international relations.
69. Šaponja, Vladimir. 1999. *Taktika dela obveščevalno varnostnih služb.* Ljubljana: MNZ, VPVŠ.
70. Šefic, Boštjan. 2004. Svet za nacionalno varnost in njegova vloga v sistemu nacionalne varnosti Republike Slovenije. *Dnevi varstvoslovja. Slovenski dnevi varstvoslovja.* Lobnikar Branko (ur.). Ljubljana: Fakulteta za policijsko-varnostne vede.
71. Škerbinc, Miha. 2015. KAJ JE TO: hibridno vojskovanje. *Revija Obramba*. Ljubljana: Založba Defensor d.o.o..
72. *Uredba o organizaciji in delovanju Nacionalnega centra za krizno upravljanje*. Ur. l. RS, št. 9/2006 (19. januar 2006).
73. Tan, Michaele. 2016. *The multi-domain battle.* Dostopno prek: http://www.defensenews.com/articles/the-multi-domain-battle (29. junij 2017).
74. The cyber dimension of modern hybrid warfare and its relevance for NATO. Dostopno prek: http://europolity.eu/wp-content/uploads/2016/07/Vol.-10.-No.-1.-2016-editat.7-23.pdf (8. maj 2017).
75. Theile, D. Ralph. 2016. Hybrid Threats – And how to counter them. *ISPSW Strategy Series: Focus on Defense and International Security* 448. Berlin.
76. *Treaty on conventional armed forces in Europe*. Dostopno prek: http://www.osce.org/library/14087?download=true (15. marec 2017).
77. Urad Vlade RS za varovanje tajnih podatkov. 2017. *Nacionalni organ za kibernetsko varnost*. Novica, dostopno prek: http://www.uvtp.gov.si/si/medijsko_sredisce/novica/article/729/1360/ (16. maj 2017).

78. Urad Vlade RS za varovanje tajnih podatkov. 2017. *Sklep o dopolnitvi Sklepa o ustanovitvi, nalogah in organizaciji Urada Vlad Republike Slovenije za varovanje tajnih podatkov*. Novica, dostopno prek: http://www.uvtp.gov.si/si/medijsko_sredisce/novica/article/729/1361/ (16. maj 2017).
79. Vegič, Vinko. 2016. Pojav in konceptualizacija hibridnega vojskovanja. *Sodobni vojaški izzivi* 18 (1). Ljubljana: Generalštab Slovenske vojske.
80. Vlada RS. *P-7: Sistem kriznega upravljanja in vodenja v Republiki Sloveniji. Dostopno prek:* http://www.vlada.si/teme_in_projekti/projektna_pisarna/p7_posodobljen_sistem_kriznega_upravljanja_in_vodenja/ (5. junij 2017).
81. Vuga-Beršnak, Janja in Anica Ferlin. 2016. Krizno upravljanje in vodenje v Republiki Sloveniji: predlog strukture KUV pri vladi RS. Upravljanje kompleksnih kriz v Republiki Sloveniji. *Zbornik* (ur. Vuga-Beršnjak), MORS, e-knjiga 9─32.
82. Žabkar, Anton. 2003. *Marsova dediščina: Temelji vojaških ved 1. knjiga.* Ljubljana: FDV.
83. Žabkar, Anton. 2004. *Marsova dediščina: Metode in smeri razvoja 2. knjiga.* Ljubljana: FDV.
84. Žirovnik, Janez. 2003. Slovenska obveščevalno-varnostna agencija v sistemu nacionalne varnosti Republike Slovenije. *Dnevi varstvoslovja. Slovenski dnevi varstvoslovja*. Pagon Milan (ur.). Ljubljana: Višja policijsko-varnostna šola.

Priloga: Vprašanja iz intervjujev

Brigadir Miha Škerbinc, namestnik direktorja oddelka za vojaško načrtovanje in vojaško politiko vojaškega odbora zavezništva NATO:

1. Kaj razumete pod terminom hibridne grožnje?

   V nalogi sem določil 4 parametre za ocenjevanje hibridne ogroženosti:

- kvantitativnost posameznih groženj,
- raznolikost groženj (hibridnost groženj),

- zmožnosti hibridnega delovanja akterja,
- ugotovljeno namero.

2. Ali bi vi še dodali še kak parameter oziroma ga odvzeli?
3. Kaj menite o oboroževanju in modernizaciji oboroženih sil na zahodnem Balkanu?
4. Ali ima Slovenija podpisane pogodbe o bilateralni izmenjavi obveščevalnih podatkov in če jih ima, s kom?
5. Kibernetske grožnje sem uvrstil v nekonvencionalne grožnje. Ali menite, da se spogledujejo s konvencionalnostjo?
6. Kje se zbirajo obveščevalni podatki (SOVA, OVS, bilaterala, diplomatska mreža, NATO, EU), kdo koordinira, vrednoti in distribuira obveščevalne podatke?
7. Ali je Slovenija kot članica zavezništva posredniška (proxy) država?
8. Ali vidite migracije kot grožnjo in na kakšen način?
9. Bipolarnost slovenske politike in družbe ali vas to skrbi in na kakšen način?
10. Ali menite, da je Slovenija hibridno ogrožena? Če da, kdo in kako jo ogroža?

Boštjan Šefic, državni sekretar MNZ:

1. Kaj razumete pod terminom hibridne grožnje?
2. Ali se kot državni sekretar … počutite varno?
3. Ali menite, da je Slovenija hibridno ogrožena? Če da, kdo in kako jo ogroža?
4. Ali ima Slovenija podpisane pogodbe o bilateralni izmenjavi obveščevalnih podatkov in če jih ima, s kom?
5. Kje se zbirajo obveščevalni podatki (SOVA, OVS, bilaterala, diplomatska mreža, NATO, EU)?
6. Kdo koordinira delo obveščevalnih služb?
7. Kdo vrednoti in distribuira obveščevalne podatke?
8. Ali imate dostop do obveščevalnih podatkov?
9. Kdo določa stopnjo ogroženosti v Sloveniji?
10. Kaj posamezna stopnja ogroženosti pomeni v preventivi in kurativi?
11. Kdo je pristojen za obravnavanje posameznih groženj z vidika hibridnosti v okviru SNAV?

12. Stopnja varnostne ogroženosti RS je vselej nizka. Ali se je politika pripravljena soočiti s kolateralno škodo?
13. Ali je Slovenija kot članica zavezništva posredniška država?
14. Ali vidite migracije kot grožnjo in na kakšen način?
15. Bipolarnost slovenske politike in družbe – ali vas to skrbi in na kakšen način?

Matej Marn, generalni direktor Direktorata za skupno zunanjo in varnostno politiko MZZ:

1. Kaj razumete pod terminom Hibridne grožnje?
2. Ali se kot direktor direktorata za skupno zunanjo in varnostno politiko počutite varno?
3. Ali menite, da je Slovenija hibridno ogrožena? Če da, kdo in kako jo ogroža?
4. Ali ima Slovenija podpisane pogodbe o bilateralni izmenjavi obveščevalnih podatkov in če jih ima, s kom?
5. Ali diplomatska mreža izdeluje obveščevalne podatke?
6. Kdo vrednoti in distribuira obveščevalne podatke?
7. Ali imate dostop do obveščevalnih podatkov?
8. Kdo določa stopnjo ogroženosti v Sloveniji?
9. Kdo je pristojen za obravnavanje posameznih groženj z vidika hibridnosti v okviru SNAV? Ali vi sodelujete v SNAV, če ne, kdo z MZZ?
10. Stopnja varnostne ogroženosti RS je vselej nizka. Ali se je politika pripravljena soočiti s kolateralno škodo?
11. Kdo izdeluje varnostno oceno za naše diplomate in po kateri lestvici?
12. Kaj posamezna stopnja ogroženosti pomeni v preventivi in kurativi?
13. Ali je Slovenija kot članica zavezništva posredniška država?
14. Ali vidite migracije kot grožnjo in na kakšen način?
15. Kako je diplomacija spremljala/spremlja migrantski tok z vidika obveščanja matice?
16. Bipolarnost slovenske politike in družbe – ali vas to skrbi in na kakšen način?

Mag. Uroš Krek, namestnik generalne sekretarke/svetovalec predsednika RS za obrambne zadeve:

1. Kaj razumete pod terminom hibridne grožnje?
2. Ali se kot državni sekretar … počutite varno?
3. Ali menite, da je Slovenija hibridno ogrožena? Če da, kdo in kako jo ogroža?
4. Ali ima Slovenija podpisane pogodbe o bilateralni izmenjavi obveščevalnih podatkov in če jih ima, s kom?
5. Kje se zbirajo obveščevalni podatki (SOVA, OVS, bilaterala, diplomatska mreža, NATO, EU)?
6. Kdo koordinira delo obveščevalnih služb?
7. Kdo vrednoti in distribuira obveščevalne podatke?
8. Ali imate dostop do obveščevalnih podatkov?
9. Kdo določa stopnjo ogroženosti v Sloveniji?
10. Kaj posamezna stopnja ogroženosti pomeni v preventivi in kurativi?
11. Kdo je pristojen za obravnavanje posameznih groženj z vidika hibridnosti v okviru SNAV?
12. Stopnja varnostne ogroženosti RS je vselej nizka. Ali se je politika pripravljena soočiti s kolateralno škodo?
13. Ali je Slovenija kot članica zavezništva posredniška država?
14. Ali vidite migracije kot grožnjo in na kakšen način?
15. Vojaški obveščevalci so izvzeti iz obveščevalnega cikla in po zakonu o obrambi ne smejo delati?
16. Bipolarnost slovenske politike in družbe ─ ali vas to skrbi in na kakšen način?

Dr. Erik Kopač, državni sekretar, pristojen za nacionalno varnost v kabinetu predsednika vlade RS:

1. Kaj razumete pod terminom hibridne grožnje?
2. Ali se kot državni sekretar … počutite varno?
3. Ali menite, da je Slovenija hibridno ogrožena? Če da, kdo in kako jo ogroža?
4. Ali ima Slovenija podpisane pogodbe o bilateralni izmenjavi obveščevalnih podatkov in če jih ima, s kom?
5. Kje se zbirajo obveščevalni podatki (SOVA, OVS, bilaterala, diplomatska mreža, NATO, EU)?

6. Kdo koordinira delo obveščevalnih služb?
7. Kdo vrednoti in distribuira obveščevalne podatke?
8. Ali imate dostop do obveščevalnih podatkov?
9. Kdo določa stopnjo ogroženosti v Sloveniji?
10. Kaj posamezna stopnja ogroženosti pomeni v preventivi in kurativi?
11. Kdo je pristojen za obravnavanje posameznih groženj z vidika hibridnosti v okviru SNAV ali SSNAV?
12. Stopnja varnostne ogroženosti RS je vselej nizka. Ali se je politika pripravljena soočiti s kolateralno škodo?
13. Kako vidite vlogo MAS?
14. Ali je Slovenija kot članica zavezništva posredniška država?
15. Ali vidite migracije kot grožnjo in na kakšen način?
16. Kdo koordinira delo obveščevalnih služb?
17. Bipolarnost slovenske politike in družbe ali vas to skrbi in na kakšen način?